الرقم التسلسلي: .....

جامعة سعيدة – الدكتور مولاي الطاهر
كلية الحقوق والعلوم السياسية

أطروحة

مقدمة لنيل شهادة

دكتوراه العلوم

الشعبة: الحقوق

التخصص: قانون عام

من طرف:

حفيظة رفاس

عنوان الأطروحة:

دور السياسة الجنائية للمشرع الجزائري في مكافحة جرائم التكنولوجيا الحديثة

أطروحة مناقشة بتاريخ 2020/06/24 أمام لجنة المناقشة المشكلة من:

الرقم	اللقب والاسم	الرتبة	المؤسسة	الصفة
01	أ.د/ لريد محمد أحمد	أستاذ التعليم العالي	جامعة سعيدة – د. مولاي الطاهر	رئيسا
02	د/ بن عيسى أحمد	أستاذ محاضر "أ"	جامعة سعيدة – د. مولاي الطاهر	مشرفا ومقررا
03	د/ عثماني عبد الرحمن	أستاذ محاضر "أ"	جامعة سعيدة – د. مولاي الطاهر	عضوا مناقشا
04	د/ رابحي لخضر	أستاذ محاضر "أ"	جامعة الأغواط - عمار ثليجي	عضوا مناقشا
05	د/ ديدوني بلقاسم	أستاذ محاضر "أ"	جامعة الأغواط - عمار ثليجي	عضوا مناقشا
06	د/ ونوقي نبيل	أستاذ محاضر "أ"	المركز الجامعي بريكة - أحمد بن عبد الرزاق حمودة	عضوا مناقشا

السنة الجامعية: 2019-2020

بسم الله الرحمن الرحيم

"... وَمَا تَوْفِيقِيٓ إِلَّا بِٱللَّهِ ۚ عَلَيْهِ تَوَكَّلْتُ وَإِلَيْهِ أُنِيبُ."

سورة هود - الآية 88 -

"... إنّي رأيتُ أنّه ما كَتَبَ أحَدُهُم في يَومِهِ كِتاباً

إلا قالَ في غَدِهِ لوغُيِّرَ هذا لَكانَ أَحسن...

ولَو زُيِّدَ ذاكَ لَكانَ يُستَحسن...

ولَو قُدِّمَ هذا لكانَ أفضل...

ولو تُرِكَ ذاكَ لَكانَ أجمل...

وهذا مِن أعظَمِ العِبر

وهو دَليلٌ على استيلاءِ النّقْصِ على جُملَةِ البَشر..."

العماد الأصفهاني

إهـــــــــداء

إلى من جعل المولى عز وجل الجنة تحت قدميها...
إلى من ضحت من أجلي بشبابها...
إلى من رعتني بحبها وعطفها
وحبتني منذ نعومة أظافري بعنايتها واحتوتني بحنانها...
بفضل من الله ثم بفضل تفانيها ودعائها
وصلت إلى ما أصبو إليه من نجاح وتوفيق وما أتطلع إليه من آمال وأحلام...
إلى أمي أولا، إلى أمي ثانيا ثم إلى أمي أبدا...
أهدي ثمرة جهدي الذي تكلل بهذا البحث المتواضع...
وأنا على يقين تام أني لن أوفي حقها مهما قلت...
نعم إلى أمي بصمت، لأن صمت الكلمات أبلغ أمام فيض فضلها...
فلها مني البر والحسنى ما حييت ودعائي لها بالعافية وحسن الخاتمة.

وحيدتك وسندك...حفيظة

شكر وعرفان

إلهي لا يطيب الليل إلا بشكرك...، ولا النهار إلا بطاعتك...، ولا اللحظات إلا بذكرك...، ولا الآخرة إلا بعفوك... ولا تطيب الجنة إلا برؤيتك...

إلى من راهنوا على فشلها وقيل لها: لا تكثري من البحث والتفكير حتى لا تظلي، فأبت بعد أن عرفت جيدا أن خير حمد لله على نعمة العقل هو استخدامه.

في مثل هذه اللحظات يتوقف اليراع ليفكر قبل أن يخط الحروف ليجمعها في كلمات...، تتبعثر الأحرف وعبثا نحاول تجميعها في سطور، سطور كثيرة تمر في الخيال...، ولا يبقى لنا في نهاية المطاف إلا قليلا من الذكريات...، تتناثر الكلمات حبرا وحبا على صفائح الأوراق، لكل من علمني، ولمن أزال غيمة جهل مررت بها برياح العلم، لكل من أعاد رسم ملامحي وتصحيح عثراتي...، إلى من جعل الحياة ألطف بكلماته... بأفعاله...، بمبادراته اللامتوقعة...

فواجب علينا شكرهم ونحن نخطو خطوتنا الأولى في غمار الحياة، ونخص بالشكر والعرفان إلى كل من أشعل شمعة في دروب عملنا، إلى من وقف على المنابر وأعطى من حصيلة فكره لينير دربنا...، أسمى عبارات الامتنان لمن حملوا أقدس رسالة...

يعجز قلمي ويتلعثم لساني عن تسطير عبارات الشكر والامتنان إلى أستاذي الفاضل الدكتور أحمد بن عيسى الذي لا تستوفي لا الكلمات ولا العبارات حق شكره، أين تفضل بالإشراف على هذا العمل ولم يبخل عنا بشيء سواء في الماجستير أو الدكتوراه، فكان لتشجيعه لنا بالكتابة ولمؤازرته دون كلل أو ملل وكذا توجيهاته الصائبة الأثر البالغ في بناء الموضوع جزاه الله عنا كل خير وجعل الله بكل حرف صدقة جارية عنه، وله منا كل الاحترام والتقدير...

إلى الأساتذة الكرام من الابتدائي إلى ما بعد التدرج، نختص بالشكر منهم الدكتور بن أحمد الحاج الذي تفضل بالإشراف على بداية هذا العمل، والدكتور لريد محمد أحمد الذي تفضل بالإشراف على رئاسة لجنة المناقشة، ومد لنا يد العون في مشوارنا الجامعي من الليسانس إلى ما بعد التدرج...، كما نتقدم بعواطف الشكر والامتنان للأساتذة الكرام بقبولهم المشاركة في تقييم ومناقشة هذه الأطروحة.

إلى الجد والجدة لأمي لرعايتهما وتربيتهما لي...، إلى الوالد، إلى طبيب العائلة والأب الذي لم يبخل بمساعداته وتوجيهاته؛ الدكتور حاجي بوعلام...، إلى عبد الرزاق وبراهيمي يونس.

تفيض نفسي شكرا وتقديرا إلى عمال مديرية الأشغال العمومية لولاية سعيدة وعلى رأسهم مديرها؛ السيد سي بلخير خالد بن الوليد، إلى أساتذة وعمال كلية ومكتبة الحقوق بجامعة سعيدة...

الشكر موصول لأفراد العائلة...، إلى كل صديقاتي، زميلاتي وزملائي كل باسمه...

إلى أولئك الذين أسدوا لنا العون من قريب أو من بعيد وتجاوزهم خط القلم سهوا لشكرهم ...شكرا.

ر. حفيظة...

مقدمة

وفرت التكنولوجيا الحديثة للإنسان نمط حياة جديدا ومتطورا ومتسارعا يحمل معه العديد من التحديات لاسيما في المجال التشريعي والقانوني، فهذه التكنولوجيا تفرض على الإنسان مواكبة تطورها السريع وحقيقة أنها تأتي بالجديد دائما، والعالم الآن يشهد ثورة في تكنولوجيا المعلومات والاتصالات التي أتت بعد ثورة صناعية أسهمت بشكل كبير في تطور الإنسان وتغير أسلوب حياته فنتيجة للتكنولوجيا الحديثة أصبح العالم عبارة عن قرية صغيرة وذلك لتأمينها إمكانية التواصل بسهولة ويسر وسرعة كبيرة بين مجتمعاته بلا حدود جغرافية ولا زمنية، وقد خلف استخدامها آثارا إيجابية مكن الانسان من قفزة حضارية نوعية مست مختلف القطاعات واستطاعت بذلك أن تقدم خدمات جليلة للأمم والشعوب.

الآن وقد أصبحت التكنولوجيا الحديثة عنصرا فاعلا أساسيا في جميع مناحي الحياة وأصبح استخدامها واسعا ومنتشرا طفت إلى السطح العديد من صور الإجرام المستحدثة والمرتبطة ارتباطا وثيقا بالتكنولوجيا الحديثة وبيئتها، وهذا راجع أساسا إلى طبيعة النفس البشرية، حيث يستغل بعض الأشرار المخترعات العلمية وما تقدمه من وسائل متقدمة في معالجة المعلومات والتواصل السريع والواسع النطاق في ارتكاب العديد من الجرائم المستحدثة والواقعة أساسا في بيئة رقمية افتراضية ومتعلقة حصرا بها.

كما أن للتكنولوجيا الحديثة جانبا بناء؛ إلا أن لها أيضا جانبا هداما حمل معه بعض الانعكاسات السلبية التي تولدت نتيجة للاستخدام السيئ للأنظمة المعلومات والاتصالات، واستغلالها على نحو غير شرعي بقصد إلحاق الأذى والإضرار بمصالح الأفراد والجماعات أو بقصد المتعة، فظهرت بذلك صورا مستحدثة من الجرائم اصطلح على تسميتها جرائم التكنولوجيا الحديثة.

وقد فرضت جرائم التكنولوجيا الحديثة نفسها كظاهرة سلبية على الأفراد والمجتمعات والحكومات ككل وذلك راجع أساسا إلى التقدم الكبير والتطور السريع والتوسع الشاسع للآفاق التكنولوجية الذي وصلت إليه هذه الأخيرة، فبدأ التأثير السلبي لهذا الإجرام واضحا ومهددا للأفراد والجماعات والأموال والحكومات على حد سواء، ولتدارك هذا الخطر صارت عملية المكافحة لجرائم التكنولوجيا الحديثة ضرورة حتمية، يجب التصدي لها خاصة وأن الدول قد وجدت نفسها عاجزة عن أداء واجبها الدستوري والقانوني لحماية الأفراد وتحقيق الأمن والاستقرار المنوط بها، ومما فاقم الوضع وجود فراغ قانوني معتبر لمواجهة هذه الظاهرة، فما كان منها سوى الإسراع إلى احتواء هذا النوع الجديد والخطير من الإجرام بسد الفراغ القانوني لمكافحته وذلك بتعديل قوانين العقوبات القائمة الخاصة بها وإصدار قوانين أخرى جديدة تتصدى لمختلف أنواع الإجرام المتصل بالتكنولوجيا الحديثة.

ظهرت الجريمة كظاهرة اجتماعية بظهور الإنسان وارتبطت ارتباطا وثيقا به فهي تعكس الواقع وتستجيب لتطوره، فأصبحت بذلك الوجه السلبي الذي يتنقل عبر العصور التي يتطور فيها الإنسان، وعليه فإن الأخذ بالآليات العلمية الحديثة يؤثر تأثيرا كبيرا في ظاهرة الإجرام، ونتيجة لظهور ثورة تقنية المعلومات، برزت ظاهرة إجرامية غير معتادة رافقت المسار التاريخي الذي مرت به هذه التقنية نشأة وتبلورا فتطورا، وشكلت بذلك انعكاسا حتميا لاستفادة المجرمين من المعطيات التي استحدثها هذا التطور التكنولوجي فكان من البديهي أن تظهر أنماطا جديدة من الجرائم التي لم تكن معهودة في السابق، ومجرم الأمس ليس بمجرم اليوم خاصة أن الإجرام في استمرار وتطور مستمر في عصرنا الحالي أين انفجرت فيه ثورة تكنولوجيات المعلومات والاتصالات نتيجة تطور تقنيات ووسائل معالجة المعلومات والاتصال التي جعلت العالم في حالة وجود إلكتروني متقارب بشكل كبير ومفتوحا للعموم ألغى معه آليا

المعالم الجغرافية والحدود السياسية للدول؛ هاته التقنية هي سلاح ذو حدين يمكن أن تسخر للمنفعة كما يمكن أن يساء استخدامها من قبل بعض المجرمين التي ساعدتهم وشجعتهم على تفاقم حجم جرائمهم بأقل جهد مع انخفاض احتمال كشف أمرهم؛ وتمثلت بداياتها بجرائم الاعتداء على البرامج والمعلومات المخزونة في الحاسبات الآلية والاستعمال غير المشروع لها.

ومع هذا التطور المستمر لكل من تكنولوجيا المعلومات وتكنولوجيا الاتصالات وصولا إلى اندماجهما معا بما عرف بتقنية المعلومات الحديثة أو التقنية الحديثة أو تكنولوجيا المعلومات والاتصالات وما نتج عنها من شبكات ووسائط إلكترونية، والتي مثلت قفزة حضارية نوعية في حياة الأفراد والدول، إلا أن هذا الجانب الإيجابي المشرق لهذه التكنولوجيا لم ينف الانعكاسات السلبية التي أفرزتها إساءة استخدام هذا التطور الذي أضفى طبيعة خاصة على جرائم كانت تقليدية قبل ظهور هذه التكنولوجيا وأدى إلى ظهور أنماط مستحدثة من الأفعال الجرمية، فتم توظيف تقنية المعلومات الحديثة في الاحتيال على المصارف واعتراض بطاقات الائتمان واستخدامها غير المشروع، والابتزاز والسطو على البنوك إلكترونيا والتزييف والتزوير، والاحتيال الإلكتروني، وتدمير الحاسبات البنكية...إلخ، ووجد العابثون من ذوي النزعة الإجرامية ضالتهم في استغلال هذه التقنية وتحقيق مآربهم عن طريقها، بدءا من جرائم الاعتداء على حق الانسان في شرفه وسمعته واعتباره وحقه في حرمة حياته الخاصة، وفي سلامة الجسم والحياة، عروجا بالجرائم الأخلاقية والإخلال بالآداب العامة، وصولا إلى الإرهاب والتجسس بالإضافة إلى تهديد أمن الدولة.

من هنا تحول الإنسان إلى هدف من أهداف مجرمي التقنية الحديثة، بعد أن أتاحت الثورة الرقمية تحقيق أغلب صور الاعتداء على الأشخاص من جنح بسيطة إلى جنايات كبرى وبأبسط الأساليب، وبات التوافق بين السياسة الجنائية وحق الأفراد في سلامة أبدانهم وحريتهم وشرفهم من كل أذى يحيط بهم مطلبا أساسيا لمواجهة الإجرام التكنولوجي الحديث في ظل انتشار وسائل تقنية المعلومات والاتصالات والتوسع في مجالات استخدامها، والتي لم يقتصر أثرها على الأفراد، بل امتد أثر الاستخدام الإجرامي لها ليطال المصلحة العامة بوجه عام، سيما وقد بات العمل الحكومي يعتمد على التطبيقات اللامحدودة لتقنية المعلومات الحديثة للتحكم في أنظمة البنية التحتية وتقديم الخدمات العامة عبر نظم المعلومات الإلكترونية التي شكلت نظم الإدارة والرقابة والإشراف والتحكم بالمرافق المختلفة والقطاعات العسكرية والأمنية.

ولم يقف خطر الاستخدام الإجرامي لتقنية المعلومات الحديثة على أمن الحكومات والدول عند حد الاعتداءات سالفة الذكر، بل نمت وازدهرت في العصر الرقمي أفعال التجسس والتهديد والترويع وإثارة الفتنة وتبادل معلومات التطرف ونشر الأفكار الإرهابية عبر وسائل تقنية المعلومات الحديثة، واتخذت أبعادا جديدة وآفاقا أرحب مع تطور الأجهزة والشبكات ووسائل الاتصال.

وهكذا وجد العالم نفسه أمام ظاهرة جرمية نمت وتطورت بنماء وتطور أجنحة تقنية المعلومات الحديثة وتباينت التعبيرات والاصطلاحات المستخدمة للدلالة عليها تباينا رافق مسيرة نشأة وتطور تلك التقنية، وأحاط بها الكثير من التساؤلات التي تتعلق بتحديد ماهيتها باعتبارها جريمة مستحدثة ومتميزة عن باقي الجرائم الكلاسيكية من خلال موضوعها، طبيعتها وخصائصها، وتعددت المحاولات الرامية إلى تحديد صورها المختلفة وأنماط السلوك الإجرامي والأفعال المكونة له، والبحث في كيفية مواجهتها من خلال تطبيق النصوص القائمة التي وضعت في وقت سابق على ظهور تقنية المعلومات الحديثة، دون قياس أو إخلال بمبدأ الشرعية الجنائية وتباينت اتجاهات الدول المختلفة في التعامل معها والعمل على خلق إطار قانوني لها، يقوم على تصنيفها وضبطها وخلق العقوبات الرادعة اللازمة لحماية البشر من تأثيرها وحماية النشاطات بكافة أنواعها.

حيث خلق هذا النوع من الجرائم تحديا كبيرا للفقه والقضاء فاقتنعوا بضرورة مواكبة هذا التطور الملحوظ في جرائم التكنولوجيا الحديثة ومواجهتها تشريعيا بقواعد قانونية غير تقليدية، والجدير بالذكر أن التشريعات العربية لم تتطرق إلى موضوع جرائم التكنولوجيا الحديثة إلا فيما ندر، ولعل السبب في ذلك أن الثورة التي أفرزتها تقنية المعلومات في البلدان العربية قد بدأت منذ نهاية العقد الأخير من القرن الماضي عكس البلدان المتقدمة التي اعتمدت على هذه الأخيرة منذ عقدين من الزمن أو أكثر، والجدير بالذكر أن ثمة تباين كبير بشأن الاصطلاحات المستخدمة للدلالة على هذه الظاهرة الجرمية الناشئة في البيئة الرقمية، وهو تباين رافق مسيرة نشأة وتطور ظاهرة الإجرام المتصلة بالتكنولوجيا الحديثة، غير أن اختيار الاصطلاح يتعين أن يزاوج بين البعدين التقني والقانوني، فإذا عدنا للحقيقة الأولى المتصلة بولادة وتطور تقنية المعلومات نجد أنها تشمل فرعين جرى بحكم التطور تقاربهما واندماجهما وهما الحوسبة والاتصال، أما المنطق الثاني لدقة اختيار الاصطلاح، فيتعين أن ينطلق من أهمية التمييز بين الاصطلاحات المنتمية لما يعرف بأخلاقيات التقنية وبين ما يعرف بإجرام هذه التقنية، وهو ما يجيب التساؤل الرئيسي بشأن الحدود التي ينتهي عندها العبث، وتلك التي تبدأ عندها المسؤولية الجنائية، أما المنطق الثالث الهام من وجهة نظرنا هو أن يكون الاصطلاح قادرا على أن يعبر بقدر الإمكان عن حدود محله، فيكون شاملا لما يعبر عنه، فلا يعبر عن الجزء ليعني الكل، ومن هنا فكل اصطلاح وصف الظاهرة بدلالة إحدى الجرائم المتصلة بالتكنولوجيا الحديثة كان قاصرا على الإحاطة الشمولية بالمعبر عنه، كاصطلاح جرائم التكنولوجيا الحديثة وهي تعابير واسعة الدلالة تحيط بأكثر ما تحتوي عليه هذه الظاهرة المستحدثة.

ولما كان ظهور تقنية المعلومات الحديثة بالشكل الراهن يرجع إلى حداثة العهد بها، والتي ما إن انتشرت إلا وأدى ذلك إلى انتشار الجرائم المصاحبة لها، وبهذا الوضع أصبح المشرع أمام أفعال جرمية لم تكن لتدور بخلده أنها واقعة بأي حال من الأحوال خاصة وأن التطور المستمر لكل من تكنولوجيا المعلومات وتكنولوجيا الاتصالات أدى إلى عدم تبلور مفهوم واضح لماهية تقنية المعلومات الحديثة وجرائمها، وعدم التوصل إلى نموذج واحد متفق عليه في تحديد أنماط السلوك الإجرامي والأفعال المكونة له لهذه الجرائم التي بدأت بالظهور مع بدايات ثورة تكنولوجيا المعلومات، والتي نمت وتطورت بتطورها إلى أن وصلنا إلى مرحلة اندماج تكنولوجيا المعلومات وتكنولوجيا الاتصالات، ذلك أن الفقه والأنظمة القانونية في بلدان العالم قاطبة لم تتفق على صور محددة يندرج في إطارها ما يسمى بجرائم تكنولوجيا المعلومات الحديثة، الأمر الذي يستتبع تعذر إيجاد فهم مشترك لهذه الظاهرة الجرمية ويثير إشكالية حول مدى كفاية نصوص قوانين العقوبات القائمة لمواجهتها دون قياس أو إخلال بمبدأ الشرعية الجنائية، وهي نصوص وضعت في وقت سابق على ظهور تقنية المعلومات الحديثة.

تعود مشكلة البحث إذن إلى ما يتميز به من صفة فنية ومفردات ومصطلحات جديدة كالبرامج والبيانات التي تشكل محلا للاعتداء أو تستخدم كوسيلة للاعتداء، معظم مستندات موضوع جرائم التكنولوجيا الحديثة عبارة عن تسجيلات إلكترونية تتم عبر شبكات الاتصال المعلوماتي، ذات طبيعة خاصة ومتميزة، وذلك راجع إلى عدة عوامل منها طبيعة المال المعلوماتي، وحداثة ظهور الوسائل التكنولوجية وتقنيات تشغيلها، ولهذا أصبح لا يكفي أن يكون الباحث مختصا في القانون، بل يتعين عليه أيضا أن يكون ملما بالجوانب الفنية والتقنية لهذه الوسائل والإنترنت ليتمكن من إيجاد الحلول للتحديات والمشاكل القانونية التي تثيرها هذه الأخيرة.

ونظرا لخطورة هذه الظاهرة الإجرامية عمدت العديد من الدول إلى سن مجموعة من المراسيم والقوانين التي تدين مرتكبي الجريمة المتصلة بالتكنولوجيا الحديثة، كونها تلحق أضرارا جسيمة بالمؤسسات والحكومات والأشخاص، وعلى هذا الأساس تحاول الدولة حماية مواطنيها على غرار الجزائر التي سعت إلى حماية أفرادها من خلال مجموعة من الآليات والأجهزة والقوانين.

على هدي ما سبق تثور الإشكالية التالية:

– ما مدى نجاعة سياسة المشرع الجزائري في مكافحة جرائم التكنولوجيا الحديثة؟

على ضوء الإشكالية المتبناة، تثير هذه الدراسة العديد من التساؤلات الفرعية التي يمكن من خلالها الإلمام بالمحتوى العام للبحث، والتي يمكن اجمالها أساسا فيما يلي:

– ماهي أهم التحولات التي طرأت على مسرح الجريمة والإجرام في ظل بيئة رقمية افتراضية؟

– ما هي آليات وأساليب المشرع الجزائري لمكافحة جرائم التكنولوجيا الحديثة؟

لا أحد ينكر أن موضوع التكنولوجيا الحديثة والجرائم المتصلة بها هو من المواضيع المستحدثة كليا، وبالتالي فإن البحث فيه لا يخلو من صعوبات جمة ترجع إلى حداثة استخدام تكنولوجيا المعلومات وما تتسم به من صبغة علمية بحتة غريبة في تصورنا على رجال القانون، فالفهم الحقيقي لظاهرة جرائم تكنولوجيا المعلومات الحديثة يستلزم بالضرورة الإلمام الكامل بتكنولوجيا المعلومات الحديثة بكل محتوياتها ونظم تشغيلها، وبالتالي تكريس وقت طويل للإحاطة بالجوانب الفنية والتقنية لهذه التكنولوجيا، فمن الصعب على رجل القانون أن يبحث في الجوانب القانونية دون الإلمام الكافي بالجوانب الفنية للموضوع محل البحث، فالتقنية الحديثة عالم متجدد ومتغير باستمرار وينمو بشكل كبير وواسع، ويحتوي على كم هائل من الرموز الأجنبية والمصطلحات العلمية الكثيرة التي تحتاج إلى شخص متخصص في هذا المجال لمعرفة المقصود بها.

فضلا عن ذلك افتقار المكتبة العربية إلى الدراسات التي تعالج من وجهة النظر القانونية الفنية التقنية للمشاكل الناجمة عن تكنولوجيا المعلومات الحديثة بشكل عام، والصعوبة الأكثر تعقيدا بالنسبة للباحث الجزائري هي أنه يفتقر للأرضية التي ينطلق منها في بحثه نظرا للفراغ التشريعي، وكذا ندرة التطبيقات القضائية في هذا المجال نظرا لحداثة هذا الموضوع على الساحة القانونية العربية.

هذه الدراسة هي محاولة لتبيان الأحكام العامة لجريمة تقنية المعلومات الحديثة وملامح إطارها القانوني ودراسة الأحكام الموضوعية للجرائم الناشئة عن استخدام هذه التقنية الحديثة بدءا من جرائم الاعتداء على حق الانسان في سلامة الجسم والحياة؛ وفي شرفه وسمعته وعدم مضايقته وحقه في حرمة حياته الخاصة، مرورا بالجرائم الجنسية، وانتهاء بالإرهاب والتجسس وتهديد أمن الدولة، وستتم دراسة الأحكام الموضوعية لهذه الجرائم من خلال بحث مدى كفاية النصوص الواردة في قانون العقوبات الجزائري وملاءمتها في الانطباق على هذه الجرائم، مع العرض لما ورد في نصوص القوانين الحديثة ذات الصلة.

تكمن أهداف موضوع البحث من الناحية النظرية والعلمية باعتباره يلامس كثيرا مصالح المجتمع وعلى وجه الخصوص المصارف من خلال التعامل الإلكتروني والسحب من الأرصدة بواسطة البطاقة الممغنطة أو الدفع الإلكتروني، وأيضا المساس بالحياة الخاصة عن طريق التسجيل وغيرها من المجالات التي تدخل في استعمال الوسائل والوسائط التكنولوجية التي أصبحت تستخدم من طرف المنظمات الإرهابية.

فمن الناحية العلمية تثير التكنولوجيا الحديثة باعتبارها علم المعالجة الآلية للمعطيات مشكلات قانونية عديدة، إذ يساء ارتكاب الجريمة عن بعد من ناحية، أو تكون محلا للاعتداء عليها من ناحية أخرى، مما يثير مسألة تكييف الاعتداء، وما إذا كان يشكل جريمة أم لا، بالإضافة إلى ما تثيره مشكلة الاختصاص القضائي والقانون الواجب تطبيقه على الجرائم المرتكبة عبرها، حتى أنها تثير مسألة التنازع الإيجابي أو السلبي في الاختصاص فيما لو وقعت الجريمة في محكمتين قضائيتين أو أكثر داخل الدولة الواحدة علاوة على ذلك فإن الإجراءات الجزائية المتبعة في ملاحقة جرائم التكنولوجيا الحديثة تثير الكثير من المشكلات القانونية، بدءا بمرحلة الإستدلال وجمع الأدلة حتى صدور الحكم الجزائي، لاسيما فيما يتعلق بمسألة إثبات هذه الجرائم، ومدى شرعية الأدلة المتحصل عليها وقبولها لدى القاضي الجزائي.

أما من الناحية النظرية فتبرز أهمية الدراسة في معرفة مدى كفاية النصوص الحالية لمنع جرائم التكنولوجيا الحديثة وردع مرتكبيها، ومدى الحاجة إلى خلق نصوص قانونية جديدة للحد من هذه الظاهرة، وإبراز خطورة الاستخدام السلبي للتكنولوجيا الحديثة والكشف على أنواع الجرائم الناجمة عنها، إضافة إلى محاولة إعطاء نظرة شاملة عن أهم الإجراءات الإحترازية التي اتبعتها الجزائر تصديا لجرائم التكنولوجيا الحديثة حفاظا على أمنها في العالم الرقمي، من خلال الوقوف على أهم القوانين والتشريعات التي سنتها للقضاء على هذه الجرائم معاقبة مرتكبيها.

تتجلى أهمية موضوع البحث من الأهمية البالغة لجرائم التكنولوجيا الحديثة في ظل الغزو التكنولوجي الهائل من خلال تحديد مميزات هذه الجرائم وانعكاسات الاستخدام السيئ لتكنولوجيا المعلومات، فموضوع هذه الجرائم من المواضيع التي فرضت نفسها على المستوى الوطني والدولي على حد سواء، والتي ينبغي على المشرع مواجهتها بتشريعات حاسمة لمكافحتها وعقاب مرتكبيها.

كما تظهر أهمية هذا الموضوع في الدور الذي تلعبه تقنية المعلومات الحديثة في حياتنا اليومية، وتأثيراه على مظاهر هذه الحياة في جميع مجالاتها، ومدى الحاجة لبحث ظاهرة جرائم هذه التقنية والعمل على خلق إطار قانوني لها يقوم على تصنيفها وضبطها وخلق العقوبات اللازمة والرادعة لحماية الأفراد والجماعات سواء الطبيعية أو المعنوية من تأثيرها، وحماية النشاطات بكافة أنواعها ذلك أن التكنولوجيا والقانون متلازمان وكل منهما يخدم الأخر، فجرائم تقنية المعلومات الحديثة تعني تأثير هذه التكنولوجيا وأدواتها على القوانين الجزائية، حيث تبرز أهمية البحث في الوقوف على هذه الظاهرة الجرمية التي نمت بنماء تقنية المعلومات وتطورت بتطورها فظهرت على السطح جرائم لم تكن موجودة في السابق، كما ظهرت طرق حديثة لارتكاب الجرائم التقليدية.

وفي هذا الصدد لا يمكن إنكار جهود الفقه العربي الذي أولى لظاهرة جرائم تقنية المعلومات الحديثة اهتماما خاصا منذ بداياتها، إلا أن المسار التاريخي الذي مرت به تقنية المعلومات الحديثة نشأة، تبلورا وتطورا، قد انعكس على طبيعة الدراسات الفقهية التي تناولت ظاهرة جرائم هذه التقنية بالبحث سواء في بلداننا العربية وحتى في البلدان المتقدمة، بحيث أدت الحقبة الزمنية التي سبقت مرحلة اندماج تكنولوجيا المعلومات والاتصالات وظهور تقنية المعلومات الحديثة إلى توجه غالبية هذه الدراسات إلى تسليط الضوء على أمن المعلومات والجانب الاقتصادي لظاهرة جرائم تقنية المعلومات الحديثة دون إيلاء الاهتمام اللازم للجرائم التي تستهدف الأشخاص والحكومات، ومن هنا تتبلور أهمية هذا الموضوع بشكل خاص، كونه محاولة لتسليط الضوء على هذه الجرائم التي ندرت الدراسات بشأنها ولا تزال بحاجة ماسة إلى ما يتناولها من بحث ودراسة.

بالإضافة إلى محاولة الوقوف على أهم النقاط الأساسية للتعرف على مفهوم جرائم التكنولوجيا الحديثة مع إبراز أنماطها وكذا التعرف على الجهود التي تبذلها السلطات الجزائرية للحد من تداعيات انتشار هذه الجرائم.

وقع الاختيار على هذا الموضوع لعاملين أساسين هما العامل الذاتي؛ ويتمثل في وجود خلفية لدى الباحثة حول موضوع الإجرام المتصل بالتكنولوجيا الحديثة، وميولها لدراسة المواضيع التي تتسم بالتطور المستمر عبر الزمن، إضافة إلى ما لقيته من تشجيع في هذا الميدان أساسا من طرف الأستاذ المشرف الدكتور أحمد بن عيسى وبعض الزملاء وكذا بعض الزملاء وأفراد العائلة المحيطة والعامل الموضوعي؛ حيث يظهر أن الموضوع محل البحث من المواضيع الراهنة والدائمة، وذلك نظرا لارتباطه بالعالم الافتراضي المتطور والمتجدد، الذي أدى بدوره إلى ظهور العديد من المشكلات العويصة في المجال القانوني، مما كان سببا في ظهور العديد من الفجوات والثغرات، الأمر الذي ألزم رجال القانون مواجهتها والتصدي لها بوضع الحلول الملائمة لها، كما أن حداثة الجريمة بحد ذاتها أوجبت التمعن فيها لمنع أي اعتداء كان من شأنه الحاق الضرر بمصالح الآخرين، بالإضافة إلى افتقار مكتبتنا الجزائرية لهذا النوع من الدراسات مما نتج عنه ندرة الكتابات في هذا المجال.

تتمثل مشكلة البحث الرئيسية في المواجهة التشريعية الماسة بسرية المعلومات الإلكترونية، وذلك من خلال دراسة الأحكام القانونية الخاصة بالجرائم المتصلة بالتكنولوجيا الحديثة، وفحص قدرة النصوص العقابية القائمة على توفير الحماية القانونية اللازمة لسرية هذه المعلومات الإلكترونية، وبحكم انتماء هذه الدراسة إلى الدراسات الوصفية، حتم اعتمادنا المنهج الوصفي، وهو المنهج الذي يختص بدراسة الظواهر كما هي في الواقع بوصفها وصفا دقيقا وموضوعيا، وذلك حسب طبيعة الموضوع محل البحث، لأننا بصدد وصف وتحليل ظاهرة تطور جرائم التكنولوجيا الحديثة من خلال تعريفها وبيان موضوعاتها وأهم مميزاتها ومراحل تطورها وأسبابها ووسائل ارتكابها...إلخ، إضافة إلى التعرف على أهم القوانين والتشريعات التي أقرها التشريع الجزائري للتصدي لظاهرة انتشار جرائم التكنولوجيا الحديثة بغية عرض مضامين المواد القانونية ذات الصلة بالموضوع وتحليلها والوقوف على مواطن القصور واللبس والغموض ثم نقترح سبل مكافحتها.

استندنا في بحثنا هذا إلى مراجع قيمة لكوكبة من الباحثين الذين تناولوا تحليل مواضيع ذات علاقة بعدد من مباحث هذا المؤلف ومطالبه، على الرغم من حداثة موضوع الدراسة، وفيما يلي قائمة بأهم أطروحات الدكتوراه في الجامعات الجزائرية.

دراسة بشرى زلاسي، 2013، "المعطيات الحديثة للحاسب الإلكتروني (الكمبيوتر) وحجيتها في الإثبات المدني" (أطروحة دكتوراه في الحقوق قسم القانون الخاص، كلية الحقوق، بن عكنون، جامعة الجزائر1، 2013)، حصرت الباحثة موضوع دراستها في مجال التصرفات القانونية المدنية، وبينت أن قوة المعطيات الإلكترونية في إثبات هذه التصرفات يتطلب تدخلا تشريعيا لضبطها وتحديد مدى حجيتها، وإحاطتها بضمانات خاصة –تقنية –، هذه الضمانات التي تعد الحجر الأساسي لحجيتها ويعول عليها في التكفل بإقرار صحتها ومصداقيتها في الإثبات لتصبح بذلك دليلا يبعث على الطمأنينة في استخدامه والتعامل به.

دراسة براهيمي جمال، 2018، "التحقيق الجنائي في الجرائم الإلكترونية" (أطروحة دكتوراه في الحقوق قسم القانون الخاص كلية الحقوق، بن عكنون، جامعة الجزائر1، 2013)، أرجعت الدراسة الجرائم الالكترونية من الأنماط الإجرامية الجديدة التي أفرزتها تكنولوجيات الإعلام والاتصال الحديثة، فهي تختلف تماما عن الجرائم التقليدية، في ذاتية أركانها وأساليب ارتكابها والبيئة الافتراضية واللامادية التي ترد عليها وخصوصية مرتكبيها، مما جعلها ظاهرة غريبة عن نصوص القانون الجزائي التقليدي بشقيه الموضوعي

والإجرائي، من ثمة فأية محاولة إخضاع هذا النمط الإجرامي الجديد لإجراءات التحقيق والإثبات المألوفة سيؤدي حتما إلى عدم الوفاء بمتطلبات مبدأ الشرعية الإجرائية، وينجر عنه عقبات كثيرة أمام سلطات التحقيق.

دراسة بن طالب ليندا، 2019، "الدليل الإلكتروني ودوره في الإثبات الجنائي، دراسة مقارنة" (أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2019)، استهدفت دراسة الدليل الإلكتروني ودوره في الإثبات الجنائي دراسة مقارنة بين عدة تشريعات وأنظمة قانونية، وبدأت هنا الدراسة بالبحث في ذاتية الدليل الإلكتروني والوقوف عند محله وعرض أهم إجراءات وأساليب التحقيق التقليدية والمستحدثة لجمعه، ثم التطرق إلى حجية الدليل الإلكتروني في الإثبات الجنائي لإظهار قوته الإستدلالية، ومن ثمة تسليط الضوء على أهمية دور القاضي الجزائي في قبول هذا الدليل والإقتناع به، مع إظهار فعالية ونجاعة التعاون الدولي في هذا المجال.

فهذه الدراسات وغيرها التي توافرت لنا قد تناولت الجرائم المتصلة بالتكنولوجيا الحديثة بشكل عام، لم تتطرق لبيان الأحكام الخاصة لكل جريمة في ضوء قانون عربي مستحدث لمكافحتها، مع أن بعض القوانين كانت قد صدرت في هذا المجال ولتأخر المشرع العربي في بعض الدول الأخرى في إصدار مثل تلك القوانين، بالإضافة إلى أن الدراسات التي تناولت الجانب الموضوعي تزيد بكثير عن تلك التي تناولت الجانب الإجرائي.

وجديد هذه الدراسة أنها لا تتناول الموضوع بشكل عام فحسب، بل تتناوله بالشرح لبيان الأحكام الخاصة لأهم تلك الجرائم تقليدية كانت أو مستحدثة، مع عدم إغفال ما يخص الجانب الإجرائي، وعليه تسعى هذه الدراسة البحثية على بسط القول في وسائل ارتكاب جرائم التكنولوجيا الحديثة، وأركان هذه الجرائم المرتكبة عبر الوسائط التقليدية والآلية، كما تذهب هذه الدراسة إلى تعريف هذه الجرائم وعلى مناقشة تصنيفات جرائمها وأنواعها تكون فيه المعطيات أو المعلومة هدفا أو أداة لارتكابها بصورة مستحدثة وفقا للدافع الجرمي، كما تناقش النظريات الحديثة التي تحاول تفسير السلوك الجرمي في العالم الافتراضي وصعوبة كشف الجرائم المرتكبة في ربوعه. لذلك تعد هذه الدراسة من طائفة الدراسات التي تنصب على الجرائم المستحدثة، وهو أحوج ما يحتاج إليه المشرع للاستفادة منها عند وضع تنظيم قانوني لاسيما في ظل غياب هذا التنظيم على جرائم التكنولوجيا الحديثة، بما يسهم في تطوير الرؤى التشريعية وكذلك القضائية.

إنطلاقا مما سبق سنحاول بحث هذا الموضوع من خلال بابين، الباب الأول: سنتناول فيه تبيان الأحكام العامة لجريمة تكنولوجيا المعلومات الحديثة وملامح إطارها القانوني، عبر الإنطلاق بداية من التعريف بتقنية المعلومات الحديثة وأجنحتها ومحاولة الإحاطة بجوانبها الفنية والتقنية، وتحديد ماهية الجرائم التي تثيرها هذه التكنولوجيا وطبيعتها وموضوعها وصورها المختلفة، ومعرفة خصائصها وسمات مرتكبيها وأركانها والإشكاليات التي يطرحها ركنها الشرعي، حيث سنبين بداية ماهية ومقبولية ومبررات استخدام اصطلاح جرائم التكنولوجيا الحديثة أو جرائم التقنية الحديثة، ومن ثم سنتناول من خلال الفصل الأول المدلول العام لتكنولوجيا المعلومات الحديثة والجرائم الناشئة عنها، ونخصص المبحث الأول منه لعرض مفهوم تكنولوجيا المعلومات الحديثة والإطلال على عوالمها من أجهزة وبرمجيات ومعطيات وشبكات معلومات بحدود حاجة القانونيين وغير المختصين تقنيا للإحاطة بالتكنولوجيا التي أثرت على السلوك، وبيان خصائصها وسمات مرتكبيها من خلال استعراض المحاولات الفقهية المختلفة لتعريفها، وما نتج عن إساءة

استخدام وسائلها العديد من الجرائم التي نحن بصدد بحثها ودراستها ثم نخصص الفصل الثاني لتحديد تصنيف جرائم تكنولوجيا المعلومات الحديثة، سواء المتعلقة بتقنية الاتصالات الحديثة، أم تلك الجرائم ذات الصبغة المالية.

ومن ثم سوف نتناول بالبحث في الباب الثاني آليات مكافحة جرائم التكنولوجيا الحديثة، فنعرض في الفصل الأول الأحكام الموضوعية لمكافحة جرائم التكنولوجيا الحديثة، بحيث نستعرض آفاق مكافحة جرائم التكنولوجيا الحديثة في المبحث الأول ونعرج إلى دور الأجهزة الأمنية في التصدي لجرائم التكنولوجيا الحديثة في المبحث الثاني، ونعرض في الفصل الثاني التحقيق وإثبات جرائم التكنولوجيا الحديثة حيث سنتناول في هذا الإطار إجراءات جمع الدليل الإلكتروني في المبحث الأول ونخلص في المبحث الثاني إلى حجية الدليل الرقمي في إثبات جرائم التكنولوجيا الحديثة.

الباب الأول: ماهية جرائم التكنولوجيا الحديثة

شكل التقدم التكنولوجي الكبير، وتطور وسائل الاتصال والتواصل المتنوعة، وانفتاح العالم على بعضه، واعتماده على إرسال شتى أنواع البيانات، ووصولها للأشخاص الخاطئين أو المنافسين إجراما معاصرا أو ما اصطلح عليه بجرائم التكنولوجيا الحديثة ويعتبر تحديا كبيرا يقف في وجه استقرار منظومة القيم التي تتحكم في سير المجتمعات.

فتعد الثورة التكنولوجية وبخاصة ثورة الاتصالات أهم التطورات التي يعيشها العالم اليوم، كما تعتبر هذه الثورة المحرك الأساسي في التطورات الحاصلة في الوقت الحالي، إلا أنها ليست المحرك الوحيد في هذه التطورات إذ ساهم التطور الكبير في تكنولوجيا الأجهزة الإلكترونية بصورة كبيرة في تسارع معدلات التقدم في مجال الاتصالات والمعلومات.

وقد كان من نتاج التطور في الجانبين ظهور أدوات واختراعات وخدمات جديدة في مختلف المجالات، ولقد نتج عن الثورة التكنولوجية تلك ظهور نوع جديد من المعاملات يسمى المعاملات الإلكترونية تختلف عن المعاملات التقليدية التي نعرفها من حيث البيئة التي تتم فيها هذه المعاملات، ويقصد بالمعاملات الإلكترونية كل المعاملات التي تتم عبر تجهيزات إلكترونية مثل أجهزة الحاسوب، شبكة الإنترنت، ومؤخرا عن طريق الأجهزة الإلكترونية الذكية، وتتكون تلك المعاملات من عدد من المكونات الأساسية يهيمن فيها طرح مكون أساسي وهو الجزء الخاص بجرائم تلك المعاملات أو بمعنى أدق القواعد القانونية الجنائية التي تحكم الأفعال التي تتم من خلال التكنولوجيا الحديثة.

والعقل الجرمي للإنسان لم ينفك يتطور مع تطور تلك الوسائل المساعدة وأضحى يستعمل المتاح منها لارتكاب الجرائم وإنطلاقا من كون البشر قادرين على التأقلم بسرعة مع محيطهم وظروف الحياة تمكن الفرد من الاستعانة بشتى السبل الموضوعة بين يديه بغية تطوير أسلوبه الجرمي وابتداع وسائل جديدة لتنفيذ جرائمه، وعليه مكنت الثورة الرقمية للمجرم المعلوماتي تسخير الفضاء الكوني لتحقيق أغلب صور الاعتداءات من جنح بسيطة إلى جنايات كبرى، إما كفاعل أصلي أو كفاعل معنوي وبأبسط الأساليب من خلال التلاعب ببرمجة البيانات التي تكون أحيانا عن بعد وبضغطة زر واحدة[1].

وعليه سنحاول دراسة هذا الباب في فصلين:

الفصل الأول: المحددات المفاهيمية لجرائم التكنولوجيا الحديثة

الفصل الثاني: أهم الجرائم المرتكبة باستخدام التكنولوجيا الحديثة

[1] محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، ص32. محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، ط2، 2004، ص43.

الفصل الأول: المحددات المفاهيمية لجرائم التكنولوجيا الحديثة

أبرز القرن العشرين ثورة من نوع آخر تتعلق بوسائل الاتصال والتواصل وكسب المعلومة نتيجة التقدم الذي أحدثه العلماء والمكتشفون لوسائل التكنولوجيا، ولعل جرائم التكنولوجيا الحديثة واحدة من التغييرات الكبيرة التي طرأت نتيجة التزاوج بين وسائل الاتصال والتواصل وبين التكنولوجيا الحديثة، وما صاحبه من تأثير في شكل الجريمة وسلوك المجرم ونظرا لما تتمتع به هذه التقنية من طابع دولي فكان ذلك مساعدا لانتشارها إلى حد كبير[1]، وإن كان من إيجابيات هذا التطور أنه قد ساهم في تسهيل الحياة البشرية وفي مختلف المجالات، إلا أن له في الجانب المقابل وجه مظلم حيث ما لبث أن ظهرت سلبيات هذا التطور نتيجة الاستخدام غير المشروع لهذه الوسائل والاعتداء على القيم والحقوق والمصالح المحمية.

فقال تشارلز بيرسي سنو في هذا الشأن أن التكنولوجيا شيء خبيث، تمنحك هبات عظيمة بيد وتطعنك في ظهرك باليد الأخرى فتنبأ عن مستقبل التكنولوجيا، وأثرها في كل مناشط حياتنا الحالية والمستقبلية، ويجب القول هنا إن كان لكل شيء فوائده فإن له مضاره إذا أسيء استخدامه على غير الوجه الصحيح، لذا يجب التنبيه والتحذير من أن التقدم التكنولوجي الحادث والسريع يتبعه تقدم هائل في عالم الجرائم بكافة أنواعها.

ولعل مصطلح جرائم التكنولوجيا الحديثة من المصطلحات التي رافقت هذا التطور، ولقد ظهرت عدة محاولات جادة لأجل تحديد المقصود بهذه الجريمة وبيان المدلول الذي تمتاز به عن غيرها من السلوكيات المجرمة، وعادة ما لا يضع المشرع التعريف الذي يحدد المقصود منها ويترك الأمر للفقه أو القضاء لأن هذا النوع من الجرائم لا يزال في تزايد باضطراد كبير مع تطور الوسائل المساعدة للحياة ومع كل ابتكار جديد يتمكن العقل البشري من التوصل إليه.

من هنا نجد تباينا كبيرا بشأن الاصطلاحات المستخدمة للدلالة على الظاهرة الإجرامية الناشئة عن التكنولوجيا الحديثة وهو تباين رافق نشأة وتطور ظاهرة الإجرام المتصلة بتقنية المعلومات، فاصطلح عليها مثلا اصطلاح إساءة استخدام الكومبيوتر مرورا باصطلاح احتيال الكومبيوتر، فاصطلاحات الجريمة المرتبطة بالكمبيوتر، فجرائم التقنية العالية، إلى جرائم الحاسوب أو الاختراقات فجرائم الإنترنت والكمبيوتر وأيضا اصطلح عليها الجريمة المعلوماتية ثم الجريمة السبرانية.

فبغية ضبط المصطلح وجب علينا التطرق للتطور التكنولوجي الذي حدث وأدى إلى ظهور التكنولوجيا الحديثة وما ارتبط بها من سلوكيات إجرامية، ثم نتطرق إلى مختلف المصطلحات والتسميات التي أطلقت على هذه السلوكيات المجرمة، ومن ثم نعرج إلى أهم الخصائص التي ميزت هذه الأخيرة التي تعددت صورها وأشكالها، وعليه حاولنا تقسيم هذا الفصل إلى مبحثين:

المبحث الأول: مفهوم جرائم التكنولوجيا الحديثة

المبحث الثاني: ارتكاب جرائم التكنولوجيا الحديثة

[1] B. Etter, Computer Crime, Australian Institute of Criminology, 4th National Outlook Symposium on Crime in Australia – New Crimes of New Responses, Australian Institute of Criminology, Canberra, 2001, p02.

المبحث الأول: مفهوم جرائم التكنولوجيا الحديثة

يشهد العالم عصرا جديدا يطلق عليه المفكر الأمريكي ألفن توفلر العصر المعلوماتي أو عصر ثورة المعلومات، وقد نشأت هذه الثورة من جمع طفرتين هي طفرة الاتصالات وطفرة تقنية المعلومات. فلا يخفى أن العالم شهد خلال النصف الثاني من القرن العشرين تطورات علمية هائلة، وكانت متلاحقة مما يصعب في كثير من الأحيان مسايرتها أو متابعتها عن كثب، ولعل أهم تلك التطورات التي شهدتها البشرية فضلا عن الاكتشافات العلمية الهائلة في مختلف المجالات تطور وسائل التكنولوجيا، فقد أدى ظهورها وانتشارها إلى إحداث ثورة حقيقية في نقل المعلومات لاسيما بعد ظهور الإنترنت، وكان من نتيجة ذلك أنه ساد الإعتقاد بأننا على أعتاب حضارة جديدة تكون الغلبة فيها لمجتمع المعلومات بدلا عن المجتمع الصناعي الذي مرت به البلدان المتقدمة في القرن التاسع عشر وبدايات القرن العشرين، وإذا كان المجتمع الصناعي يهتم أساسا بتحويل المادة أو الطاقة من صورة لأخرى، فإن مجتمع المعلومات يقوم بتحويل البيانات أو المعطيات –وهي غير ملموسة– من شكل إلى آخر وذلك بمعالجتها بواسطة إحدى وسائل التكنولوجيا الحديثة كالحاسب الآلي.

فاعتبرت الكثير من الدراسات أن استخدام الوسائل الإلكترونية والقدرة على التبادل الرقمي للمعلومات والخدمات –سواء عبر الأجهزة الإلكترونية الذكية أو الحواسيب الآلية– من أبرز الأسس المعرفية التي يقوم عليها مجتمع المعلومات وسبب من أسباب رواج التجارة الإلكترونية وانتشار نوع معاصر من الجرائم تعددت خصائصه وأصنافه.

وبما أن الجريمة ظاهرة اجتماعية تعكس الواقع، وتتفاعل مع متغيراته، وتستجيب لتطوره، فإن الأخذ بالآليات العلمية الحديثة يؤثر تأثيرا كبيرا على ظاهرة الإجرام[1]، فتعتبر الجريمة المرتكبة عبر الإنترنت بواسطة وسائل التكنولوجيا المبتكرة من الآثار السلبية التي خلفتها التقنية العالية، إذ أخذت هذه الظاهرة الإجرامية حيزا كبيرا من الدراسات من أجل تحديد مفهومها مما أنجر عنه وضع عدة مصطلحات للدلالة عليها.

يجمع أغلب الكتاب والمحللين الاجتماعيين على اختلاف خلفياتهم على أن المجتمع قد شهد تحولا جذريا منذ ثمانينيات القرن الماضي، وهم يحددون أصل هذا التحول في النظم الآلية لمعالجة وتخزين وبث المعلومات ويرون أن الإنسانية أقبلت على حضارة جديدة تتأسس على المعرفة، تؤدي فيها المعلومات دور المادة الخام الأولية ويتعاظم فيها دورها كمورد استراتيجي وهي أكثر أهمية حتى من مصادر المعادن والطاقة ورأس المال، فنتيجة ثورة تقنية المعلومات برزت ظاهرة جرمية غير معتادة رافقت خط المسار التاريخي الذي مرت به هذه الأخيرة نشأة، تبلورا وتطورا، وشكلت انعكاسا حتميا لاستفادة المجرمين من المعطيات التي استحدثها هذا التطور التكنولوجي وتمثلت بداياتها أساسا بجرائم الاعتداء على البرامج والمعلومات المخزونة في الحاسبات الآلية والاستعمال غير المشروع لها التي تختلف عن الجرائم التقليدية في أطرافها، مكانها وموضوعها، والتي تعتبر من الجرائم المستحدثة كونها تطال الكيان المنطقي للأجهزة بما تشمله من برامج ومعطيات، ونظرا إلى حجم المخاطر وهول الخسائر الناجمة عنها باعتبارها تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة كونها جريمة تنشأ في الخفاء وتشيع فقدان الثقة بالتقنية وتهدد إبداع العقل البشري فقد جعلت العالم يؤكد على خطورتها.

---

[1] André Vitalis, Informatique, Pouvoir et Libertés, Economica, 1981, p22.

إنطلاقا مما سبق يمكن الذهاب إلى القول إن التطرق إلى مفهوم جرائم التكنولوجيا الحديثة تكتنفه صعوبة خاصة وذلك يرجع إلى أن هذا النمط من الإجرام من الأنماط المستحدثة التي رافقت التطور التكنولوجي الحديث، هذا من جهة، ومن جهة أخرى فإنها تتسم بتعدد تسمياتها والمصطلحات الدالة عليها، كما أن استعراض الطبيعة القانونية الخاصة لهذه الجرائم كونها تطال في اعتداءاتها المعلومات ومعطيات الحاسب والأجهزة الذكية يثير صعوبات أخرى، بالإضافة إلى أن تحديد خصائص هذا النمط وتمييزه عن غيره من الأصناف الأخرى من الإجرام يثير مسائل قانونية على قدر من الأهمية التي تباينت بتطور هذا النوع من الجرائم.

المطلب الأول: تعريف جرائم التكنولوجيا الحديثة

أدى ظهور الحاسب الآلي والأجهزة الإلكترونية الذكية وانتشارها إلى إحداث ثورة حقيقية في المعلومات، وبدأ الحديث عن مجتمع المعلومات والمعلوماتية وغيرها من المصطلحات الجديدة ومن هنا ساد الإعتقاد بأننا على أعتاب حضارة جديدة تماما تكون الغلبة فيها لمجتمع المعلومات كبديل للمجتمع الصناعي الذي مرت به المجتمعات المتقدمة خلال القرن الماضي.

وقد ترتب على انتشار الوسائل الإلكترونية في مجالات الحياة المختلفة أن ظهر في الواقع حامل جديد إن جاز التعبير للمعلومات يختلف جذريا عن الحامل الورقي التقليدي السائد حتى وقت قريب، وكان من نتيجة ذلك أن بدأت المستندات الورقية التقليدية تتراجع رويدا ليحل محلها تدريجيا الدعامات الجديدة للمعلومات كنتيجة طبيعية لانتشار الحاسب خصوصا في البنوك وشركات التأمين والشركات الكبرى والمؤسسات الحكومية، مثال ذلك الأشرطة الممغنطة وأسطوانات الفيديو والدعامات المثقبة بأنواعها المختلفة والميكروفيلم.

أبرز القرن العشرين إذن ثورة من نوع آخر تتعلق بوسائل الاتصال وكسب المعلومة نتيجة التقدم الذي أحدثه العلماء والمكتشفون لوسيلتين هما جهاز الكمبيوتر والأجهزة الإلكترونية الذكية ووسيلة أخرى لكسب المعلومة والاتصال ألا وهي الإنترنت أو الشبكة العنكبوتية، ويعبر عنه الفقهاء بقرن المعلوماتية نتيجة تدفق هذه المعلومات وانسيابها ووفرتها، إلا أن استخدامها غير المشروع حتم ظهور نوع جديد من الجرائم وهي إحدى التغيرات الكبيرة التي طرأت نتيجة التزاوج بين وسائل الاتصال والتكنولوجيا الحديثة وما صاحبه من تأثير في شكل الجريمة وسلوك المجرم لم يكن يعرفها القانونيون من قبل.

وعليه يمكن القول إن التطرق إلى تعريف جرائم التكنولوجيا الحديثة تكتنفه صعوبة خاصة، ويرجع ذلك إلى أن هذه الجرائم من الجرائم المستحدثة التي رافقت التطور التكنولوجي الحديث، وذلك لاتصالها بجانب تقني وفني بحت يتمثل في النظام المعلوماتي بشقيه المادي والمعنوي، وتباينت الاجتهادات الفقهية في وضع تعريف هذا النوع من الجرائم، مما أصبح يشكل تحديا كبيرا أمام القواعد القانونية التقليدية في تحديد تعريف دقيق لها، فالتكنولوجيا الجرمية كظاهرة إجرامية حديثة ذات طبيعة خاصة صعبت من التوصل إلى اتفاق حول مصطلح موحد يعبر عن هذه الظاهرة المستحدثة.

ولقد حاولت العديد من الأعمال الأكاديمية وضع تعريف لجرائم التكنولوجيا الحديثة فذهبت إلى القول على أنها تلك الجرائم التي تقع على الأشخاص والأموال وتلك التي تمس المصلحة العامة بواسطة وسائل التكنولوجيا الحديثة عن طريق شبكة

الإنترنت سواء داخل البلاد أو خارجها، ومن النادر جدا أن يتضمن جزء التعريفات في هذه الأبحاث تعريف هذا النوع من الجرائم نتيجة حداثتها وارتباطها بتكنولوجيا متطورة[1]، بالإضافة إلى تعدد المصطلحات التي تدل عليها.

والحقيقة أن بعض المفاهيم الجزائية تتشابه إلى درجة المزج بينها والخلط، فتستخدم بعض المفاهيم كمصطلحات مترادفة وهذا هو الوضع نفسه في نطاق جريمة تقنية المعلومات الحديثة، فترى فقهاء القانون الجنائي والتشريعات المختصة الجزائية في القانون المقارن لم يتفقوا على الوصف القانوني أو التسمية القانونية وكيفية التفرقة السليمة والصحيحة بين المصطلحات المختلفة التي استخدمت للدلالة على الظاهرة الجرمية الناشئة في بيئة اندماج تكنولوجيا المعلومات وتكنولوجيا الاتصالات، فالبعض يستخدم مصطلح الجريمة المعلوماتية والبعض يطلق مصطلح الغش المعلوماتي أو اصطلاح إساءة استخدام الحاسب الآلي أو اصطلاح احتيال الحاسب الآلي أو جرائم الحاسب الآلي أو الجريمة المرتبطة بالحاسب الآلي أو جرائم الهاكرز والاختراقات أو جرائم الإنترنت أو الجرائم الإلكترونية أو جرائم الفضاء السبراني والعديد من الاصطلاحات الأخرى التي لا يتسع المجال لحصرها.

وإننا نجد أن تلك المصطلحات تتعلق غالبا بالمرحلة الزمنية التي استخدم بها الاصطلاح وبالنسق الذي يعالج به الباحث الموضوع ومع تقديرنا لشيوع مصطلح جرائم المعلوماتية –والذي وفقا لدلالة الكلمة بوصفها ترجمة عن الفرنسية لمصطلح المعالجة الآلية للمعطيات في مطلع التسعينات لدى بعض الفقه العربي–، إلا إننا نوافق الرأي الفقهي الذي يرى أن هذا التعبير غير دقيق باعتبار المعلوماتية الآن فرع مستقل من بين فروع المعرفة وعلومها ويتصل بقواعد البيانات بوجه عام انشاؤها وإدارتها والحقوق والالتزامات المتصلة، وهو في النطاق القانوني يتعلق بالمعلومات القانونية كأن نقول المعلوماتية القانونية وعلى هذا المنوال تقاس بقية المعلومات المتخصصة[2].

وبرأينا أن اختيار الاصطلاح يتعين أن يزاوج بين البعدين التقني والقانوني، وبالنظر إلى نشأة وتطور تقنية المعلومات نجد أنها تشمل فرعين هما الحوسبة والاتصال جرى بحكم التطور تقاربهما واندماجهما، فأنتج هذا الاندماج مفهوما جديدا لتقنية المعلومات، لذلك لابد أن يكون الاصطلاح شاملا بدلالة قطبي التقنية، وأن يكون قادرا على أن يعبر بقدر الإمكان على حدود محله فيكون شاملا لما يعبر عنه، فلا يعبر مثلا عن الجزء ليبين الكل أو يكون على العكس مانع الحدود يطال ما لا ينطوي تحت نطاقه، لذا فقد آثرنا اختيار مصطلح جرائم التكنولوجيا الحديثة للدلالة على هذه الظاهرة الجرمية الناشئة في بيئة تقنية المعلومات بمفهومها الحديث الذي أبرزه اندماجها بتكنولوجيا الاتصالات.

ونود أن نشير إلى أننا سوف نستعمل في هذه الدراسة تعابير جرائم التكنولوجيا الحديثة وجرائم تقنية المعلومات الحديثة وجرائم تكنولوجيا المعلومات كمترادفات.

فتكنولوجيا المعلومات الحديثة إذن أو التقنية الحديثة هي التكنولوجيا التي أنتجها اندماج تكنولوجيا المعلومات وتكنولوجيا الاتصالات، وهذه التكنولوجيا الحديثة الناشئة عن هذا الاندماج تختلف عن تكنولوجيا المعلومات ما قبل الاندماج، لأن تقنية المعلومات الحديثة ما هي إلا ثمرة المزاوجة بين تكنولوجيا الاتصالات وتكنولوجيا المعلومات (الأجهزة، الوسائط التكنولوجية) الذي أدى إلى ميلاد علم جديد هو علم انتقال المعلوماتية عن بعد (télématique) وهو مصطلح مركب من المقطع الأول لكلمة

[1] Pierre Catala, Informatique et droit pénal, Ed. Cujas, Paris, p18.

[2] يونس عرب، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، منشورات اتحاد المصارف العربية، ط1، الأردن، 2001، ص211.

اتصال عن بعد (télécommunication) والمقطع الثاني من كلمة المعلوماتية (informatique) وهو يعني بذلك علم اتصال المعلوماتية عن بعد أو من مسافة أو بالأحرى موت المسافات[1].

ولتعريف الجريمة المتصلة بتكنولوجيا المعلومات الحديثة، يجب التدقيق في المصطلحات أولا، مصطلح الجريمة والتكنولوجيا الحديثة، فالجريمة هي انحراف في السلوك الإنساني، أي أنها سلوك غير مشروع لأنها تمثل اعتداء على حق أو مصلحة من الحقوق أو المصالح التي يحميها القانون، أما مصطلح التكنولوجيا فيرجع أصله إلى الكلمة اليونانية التي تتكون من مقطعين أساسيين هما (Techno) التي تعنى التشغيل الصناعي، والثاني (Logos) بمعنى العلم والمنهج لذا تكون بكلمة واحدة هي علم التشغيل الصناعي[2]، وعليه يمكن القول إن التكنولوجيا هي التطبيق الفعال لنتائج البحث العلمي والخبرات العلمية لتطوير الحياة العملية، فهي عملية دمج الأدوات والمعدات المبتكرة مع الأسس النظرية والعلمية بهدف تحسين الأداء البشري.

وبالتالي لا يجوز التدليل على جرائم إساءة استخدام وسائط هذه التكنولوجيا الحديثة باصطلاح يقتصر على تناول أحد أجنحتها دون الجناح الآخر أو باصطلاح بتجاهل المفهوم الحالي لهذه التكنولوجيا، فالمصطلح لا بد أن يتصف بالمرونة وبعد النظر بمعنى أنه لا بد أن يراعي المستقبل وما قد يفرزه لنا هذا التطور الهائل في الاختراعات الإلكترونية ووسائل الاتصال من أجهزة غريبة تظهر في كل يوم ولا يصدق العقل بإمكانية اكتشافها.

بناء على ما تقدم؛ ثمة مقبولية ومبررات لاستخدام اصطلاح جرائم التكنولوجيا الحديثة فهو اصطلاح نراه شاملا بدلالته التقنية الحديثة التي أنتجها اندماج تكنولوجيا المعلومات مع تكنولوجيا الاتصالات، وبالتالي هو اصطلاح قادر أن يطوي تحت جوانبه العديد من السلوكيات الضارة بالأفراد والجماعة.

وقد أظهرت جرائم التكنولوجيا الحديثة تحديا قويا أمام رجال القانون والفقه للإحاطة بجوانبها المختلفة، فالقانوني بحكم تكوينه وتخصصه هو غير متخصص في الحقل التقني، لكن التعامل مع هذه الظاهرة الجرمية المستحدثة الناتجة عن سوء استخدام تكنولوجيا المعلومات الحديثة، يفرض عليه الإطلال على عوالم هذه التكنولوجيا وسبر أغوارها والنهل منها بصبر وتدقيق لإيجاد ما يلزم لتحديد تعريف الجرائم التي تثيرها هذه الأخيرة وطبيعتها وموضوعها، فعلى الرغم من أن الجانب الفني والتقني لنظم التقنية الحديثة قد يبدو بعيدا عن لغة القانون إلا أنه ليس بالمقدور تحقيق إدراك عميق لجرائم التكنولوجيا الحديثة دون إدراك البعد الفني لهذه التكنولوجيا والتعرف على وسائلها.

وعليه اهتم فقهاء القانون الجنائي مع نهاية القرن الماضي بدراسة الجرائم المتصلة بتقنية المعلومات الحديثة باعتبارها ظاهرة عرضت نفسها على المجتمع لما تنطوي عليه من مجموعة من السمات الخاصة حيث كان ارتباطها بالحاسب الآلي مميزا لها عن غيرها من الجرائم الأخرى، ومنذ ذلك التاريخ ونظرا لحداثة الظاهرة نسبيا من ناحية، والتطور الذي يطرأ عليها وعلى وسائط التكنولوجيا من ناحية أخرى فقد تعددت التعريفات التي استخدمت للدلالة عليها واختلف الباحثون في تحديد طائفة الأفعال التي تدخل في إطار هذه الجرائم.

---

[1] محمد محمد الألفي، العوامل الفاعلة في انتشار جرائم الإرهاب عبر الإنترنت، المؤتمر الدولي الأول حول حماية أمن المعلومات والخصوصية في قانون الإنترنت، القاهرة، 02-04 يونيو 2008.

[2] غسان قاسم الأمين، إدارة التكنولوجيا، مفاهيم ومداخل تقنيات تطبيقات علمية، دار المناهج، ط1، عمان، 2006، ص22.

فتعرف الجريمة عموما في نطاق القانون الجنائي بأنها فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدبيرا احترازيا[1]، أما جرائم تكنولوجيا المعلومات الحديثة فقد تعددت تعريفاتها بتنوع التعبيرات التي استخدمت للدلالة عليها وهو تعدد رافق مسيرة نماء وتطور هذه التكنولوجيا، ويمكننا أن نرجع السبب الرئيسي لهذا التعدد في التعريفات إلى كون الإطار أو البيئة الخاصة لهذه الظاهرة الجرمية كانت ولا تزال في طور النماء والتطور.

وقد بذل المهتمون بدراسة نمط الإجرام المصاحب لانتشار وسائط تكنولوجيا المعلومات جهدا كبيرا من أجل التوصل إلى تعريف مناسب يتلاءم مع طبيعة هذه الظاهرة الجرمية إلا أن كثيرا من المحاولات باءت بالفشل، حتى قيل أن هذه الظاهرة الجرمية تقاوم التعريف[2]، وهذا راجع لتعذر إيجاد تعريف مجمع عليه لجرائم هذه التقنية، فقد صك الفقهاء والدراسون لها عددا ليس بالقليل من التعريفات التي تتمايز وتتباين تبعا لموضع العلم الذي تنتمي إليه، إضافة لمعيار التعريف ذاته فاختلفت بين أولئك الباحثين في الظاهرة الإجرامية الناشئة عن استخدام تكنولوجيا المعلومات من الزاوية الفنية وأولئك الباحثين في ذات الظاهرة من الزاوية القانونية وفي الطائفة الأخيرة تباينت التعريفات تبعا لموضوع الدراسة ذاته وتعددت حسب ما إذا كانت الدراسة متعلقة بالقانون الجنائي أم متصلة بالحياة الخاصة أم متعلقة بحقوق الملكية الفكرية.

وفي إطار تقصينا لغالبية التعريفات التي وضعت لهذه الظاهرة الجرمية المستحدثة، نجد أن هذه التعريفات تنقسم في أغلبها إلى الاتجاهات التالي، أولا؛ نجد طائفة من التعريفات تقوم على معيار واحد، وهذه تشمل تعريفات قائمة على معيار شخصي وتحديدا متطلب توفر المعرفة والدراية التقنية لدى شخص مرتكبها، ثانيا؛ طائفة التعريفات القائمة على تعدد المعايير، وتشمل التعريفات التي تبرز موضوع الجريمة وأنماطها وبعض العناصر المتصلة بآليات أو بيئة ارتكابها أو سمات مرتكبيها، وظهرت طائفة حاولت الجمع بين التعريفين السابقين.

الفرع الأول: الاتجاه المضيق لمفهوم جرائم التكنولوجيا الحديثة

نظرا لتباين وجهات النظر لمفهوم جرائم التكنولوجيا الحديثة ذهب أنصار الاتجاه المضيق لهذا المفهوم والذي يربط بقوة بين ارتكاب الجريمة وبين وجود قدر كاف من المعرفة لدى الفاعل والشركاء معه إلى حد الإتقان، ذلك أن هذا الاتجاه يؤمن بأن جرائم تقنية المعلومات الحديثة ذات صلة وطيدة بتقنية التكنولوجيا الحديثة إما من حيث الطبيعة أو من حيث وسائل ارتكابها أو حتى من حيث نتائجها، وهو أمر جعلهم يربطون بين الجريمة والقدرة التقنية لدى الفاعل، فلا يرون وقوع الجريمة إلا من شخص لديه ذلك الإلمام بتقنية التكنولوجيا الحديثة، وهم هنا يوردون تعريفا لجرائم التكنولوجيا الحديثة مفاده أنها كل سلوك غير مشروع يكون الإلمام بالتكنولوجيا الحديثة بقدر كبير لازما لارتكابه من ناحية، ولملاحقته من ناحية أخرى[3].

---

[1] محمود نجيب حسني، شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الاحترازي، دار النهضة العربية، القاهرة 1989، ص40.

[2] هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، مصر، 1992، ص29.

[3] سلامة محمد عبد الله أبو بكر، موسوعة جرائم المعلومات، منشأة المعارف، الإسكندرية، 2006، ص11.

من هذا الجانب نجد تعريف الأستاذ Thompson؛ إذ يرى وجوب توافر معرفة بتقنية التكنولوجيا الحديثة لدى فاعل هذا النوع من الجرائم[1]، كما أن منظمة التعاون الاقتصادي والتنمية عرفت هذا النوع من الجرائم بأنه كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها[2]، إزاء هذه التعريفات يمكن القول إن جرائم التكنولوجيا الحديثة قاصرة بوسيلة معنية لارتكابها وهي استخدام وسائل التكنولوجيا الحديثة، وهي ذلك النوع من الجرائم التي تتطلب إلماما خاصا بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها والتحقيق فيها ومقاضاة فاعليها[3]، وبنفس المعنى عرفت بأنها تلك الجرائم التي تقع على شبكة الإنترنت أو بواسطتها من قبل شخص ذو معرفة تقنية[4].

ويرى الأستاذ Masse؛ أن المقصود بجريمة تكنولوجيا المعلومات الحديثة يتمثل بالاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح، كما ذهب Donn B. Parker إلى القول بأنها أي فعل متعمد مرتبط بأي وجه بالحاسبات يتسبب في تكبد أو إمكانية تكبد مجني عليه لخسارة أو حصول أو إمكانية حصول مرتكبه على مكسب، ويستخدم للدلالة على الجريمة تعبير إساءة استخدام الحاسب[5].

ويعرف جانب من الفقه جريمة تكنولوجيا المعلومات الحديثة على أساس سمات شخصية لدى مرتكب الفعل، وهي تحديد سمة الدراية والمعرفة التقنية، ومن هذه التعريفات نجد تعريف وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث وتبنتها الوزارة في دليلها لعام 1989 فعرفتها بأنها أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها.

ويعرفها الأستاذ Steinschi alberg بأنها "أي فعل غير مشروع تكون المعرفة بتقنية الكمبيوتر أساسية لارتكابه والتحقيق فيه وملاحقته قضائيا"[6]، كما عرفت جرائم التكنولوجيا الحديثة بأنها تلك الجرائم العابرة للحدود التي تقع على شبكة الإنترنت أو بواسطتها من قبل شخص ذي دراية فائقة بها[7]، وفي معرض تقدير هذه التعريفات، يمكننا القول إن شرط المعرفة التقنية شرط شخصي متصل بالفاعل، غير أن هذه الجرائم كما سنرى في أمثلة عديدة يرتكب جزء كبير منها من قبل مجموعة تتوزع أدوارهم بين التخطيط والتنفيذ والتحريض والمساهمة، وقد لا تتوافر لدى بعضهم المعرفة بتقنية المعلومات، فيمكن القول إنه لم يعد مطلوبا

---

[1] David Thompson, Current Trends in Computer Crime, Computer Control Quarterly, MCB University Press, Bingley, United Kingdom, Vol. 1, n°01, 1991, p02.

[2] تهدف هذه المنظمة إلى تحقيق أعلى مستويات النمو الاقتصادي وهي تضم في عضويتها 29 دولة منذ عام 1978 وقد بدأت الاهتمام بجرائم التكنولوجيا الحديثة حيث وصفت مجموعة أدلة وقواعد إرشادية تتصل بتقنية المعلومات، وقد أصدرت هذه المنظمة تقريرا بعنوان الجريمة المرتبطة بالحاسوب وتحليل السياسة الجنائية القانونية الجزائية، وتضمن التقرير قائمة الحد الأدنى لأفعال سوء استخدام الحاسوب التي يجب على الدول أن تجرمها وتفرض لها عقوبات في قوانينها ومن أمثلتها، الاستخدام أو الدخول إلى نظام ومصادر الحاسب على نحو غير مصرح به وإنشاء غير مصرح به لتلك المعلومات أو نسخها أو التلاعب فيها أو إتلافها أو تخريبها.

[3] عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، دار الكتب والوثائق المصرية، 2007، ص40.

[4] محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الإنترنت، الأحكام الموضوعية والأحكام الإجرائية، منشورات الحلبي الحقوقية، بيروت، ط1 2011، ص31.

[5] Donn B. Parker, Combattre la criminalité informatique, Oros, Paris, 1985, p18.

[6] Donn B. Parker, Susan Nycum, S. Stephen Oüra, Computer abuse: final report, Stanford Research Institute, 1973, p517.

[7] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، 2006، ص30.

العلم والمعرفة العميقين ليتمكن شخص مثلا من إرسال آلاف رسائل البريد الإلكتروني دفعة واحدة إلى أحد المواقع لتعطيل عملها.

وطبقا للتعاريف الحديثة فإن جرائم تكنولوجيا المعلومات الحديثة تنحصر في الحالات التي تتطلب قدرا من المعرفة التقنية في ارتكابها، وهو إن تحقق في بعض الأحيان فإنه لا يتحقق في أغلبها، ثم ماهي حدود المعرفة، وما هو معيار وجودها للقول بقيام الجريمة، خاصة في ظل التطور الذي شهدته وسائل التقنية الحديثة من تبسيط وسائل المعالجة وتبادل المعطيات، وتحويل الأجهزة المعقدة فيما سبق إلى أجهزة تكاملية سهلة الاستخدام، حتى ممن لا يعرف شيئا عن علوم التقنية الحديثة.

وهناك من يعرفها بأنها أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات[1]، فمن التعريفات أيضا التي تجدر الإشارة إليها حسب أنصار هذا الاتجاه أنها كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات.

إن هذا التعريف هو من التعاريف التي توسع من مفهوم جرائم التكنولوجيا الحديثة ولا تحصرها بنوع معين من الجرائم، إذ تتباين أنواع وصور هذه الأخيرة يوما بعد يوم، بتزايد تطور التكنولوجيا وبتزايد عدد المستخدمين، فيمكن القول إن هذا التعريف جاء شاملا –إلى حد ما– لفروع جرائم التكنولوجيا الحديثة، ويمكن الاستعانة به لوضع تعريف أشمل وأكثر مواءمة لهذه الجرائم، وذلك أن جرائم تكنولوجيا المعلومات الحديثة هي كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات؛ سرقة تدميرا، أو تشويها، سواء طالت الأشخاص أو المؤسسات، الأموال أو الحياة الخاصة.

نرى مع هذا الاتجاه أن جرائم التكنولوجيا الحديثة لا يمكن أن توجد بمعزل عن تقنية المعلومات الحديثة سواء كانت منفردة أم ضمن شبكة اتصال معلوماتي محلية كانت أم عالمية، وأن تقنية تكنولوجيا المعلومات الحديثة هي جوهر السلوك الجرمي ومحوره، إلا أننا في المقابل لا نؤيد هذا الاندماج الكبير بين وقوع الجريمة ومدى براعة الفاعل أو إتقانه لتقنية تكنولوجيا المعلومات، ذلك أن الفاعل قد يرتكب جرائم التقنية دون أن تتوافر له تلك البراعة لاقتراف جريمته، وقد لا تتوافر لديه الحدود الدنيا من تلك البراعة، فلا ينكر أن العديد من جرائم التكنولوجيا الحديثة ترتكب بكبسة زر واحدة فقط، هذه الكبسة السحرية التي يمكن لأي شخص القيام بها طالما وجد بين يديه وسيلة من وسائل ووسائط التكنولوجيا.

من هنا يمكن القول إن تعريف جرائم التكنولوجيا الحديثة حسب أنصار هذا الرأي جاء مستوحى من المبدأ الرئيسي لكل جريمة، وهو ضرورة أن يكون العمل المرتكب غير مشروع ومخالف للقانون وأن يؤدي إلى إلحاق الضرر بالمجني عليه، مع الأخذ بعين الاعتبار الطبيعة الخاصة لجريمة تكنولوجيا المعلومات الحديثة مع الفاصل المشترك بين جميع الجرائم.

من خلال ما سبق نلاحظ أن هذه التعريفات لا تستند في الحقيقة إلى موضوع الجريمة بالمعنى القانوني، الذي يشكل محل الاعتداء، فركزت هذه التعريفات على أنماط السلوك الإجرامي وأبرزتها متصلة بالموضوع لا الموضوع ذاته، وهذا افتراض مسبق على شمول نصوص قانون العقوبات لأنماط السلوك الإجرامي في جرائم التكنولوجيا الحديثة، وهي مسألة لا تراعي الجدل الذي لم ينته بعد حول مدى انطباق قواعد التجريم التقليدية على هذه الأفعال، والذي حسم تقريبا لجهة عدم انطباق نصوص القوانين القائمة

[1] تعريف Artar Solarz، مشار إليه لدى هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، مجلة الأمن والقانون العدد 02، كلية الشرطة، دبي، 1999، ص31.

وذلك بسبب طبيعة القانون الجزائي المحكوم بمبدأ لا جريمة ولا عقوبة إلا بنص، وما يترتب عليه من نتائج قانونية، إذ أن محاولة البحث في مدى إمكانية تطبيق تلك النصوص ينبغي أن يكون في إطار ما يستلزمه هذا المبدأ والحاجة إلى نصوص خاصة تراعي العناصر المميزة لهذه الجرائم عن غيرها من الجرائم التي عرفها قانون العقوبات.

الفرع الثاني: الاتجاه الموسع لمفهوم جرائم التكنولوجيا الحديثة

يؤكد التعريف العام للجريمة عدم وجود مدلول أو فكرة ثابتة تقيدها بمعنى أو مسلك واحد، فتغيير الجريمة يختلف باختلاف وجهات النظر إليه[1]، وهو ما ينطبق على الجريمة محل دراستنا ويمكن أن يطلق عليها الجرائم المستحدثة أو الجريمة العالمية أيضا[2]، والتي غالبا ما تستخدم فيها شبكة الإنترنت كأداة لارتكابها أو تسهيل ارتكابها[3]، والتكنولوجيا الحديثة عمادها، فهي هدف الجريمة حينا ووسيلتها حينا آخر وهي البنية أحيانا أخرى[4].

فذهب أنصار هذا الاتجاه إلى التوسع في مفهوم جرائم التكنولوجيا الحديثة، فلا يقيم ربطا كبيرا بين ارتكاب الجريمة وتحقق نتيجتها وبين إلمام الفاعل أو الشركاء معه بتقنية الوسائل الإلكترونية، وهم لا يقيمون وزنا لمدى براعة الفاعل وإجادته التقنية أو خبرته ومقدرته، بل المهم والأهم عند هذه الطائفة تحقق وقوع الجريمة، ولذلك فهم يرون أنها كل فعل غير مشروع يتم بمساعدة الحاسب الآلي أو هي كل جريمة تتم في محيط الوسائل والوسائط الإلكترونية التي تعد الطرف الثاني في الاشتراك بالجرم، فهي الطرف الأساس لارتكاب الجريمة من حيث الدور المساعد والمساهم لتنفيذ الاعتداء لذلك فالتعاريف التي أطلقها الفقهاء على هذا النوع من الجرائم يمكن أن تشكل مدخلا لتكوين رؤية واضحة نسبيا لما يمكن أن تكون عليه جريمة تكنولوجيا المعلومات الحديثة من أنواع وتبنى هذا الاتجاه الألماني Ulrich Sieber، ويعتمد هذا التعريف على معيارين أساسيين أولهما وصف السلوك وثانيهما اتصال السلوك بالمعالجة الآلية للبيانات أو نقلها، كما يعرفها Thomas J. Smedinghoff، بأنها أي ضرب من النشاط الموجه أو المنطوي على استخدام نظام الحاسوب.

ويعرفها Jack Bolanga وRobert Lindquist؛ بأنها جريمة تستخدم الأجهزة الإلكترونية كوسيلة أو أداة لارتكابها أو يمثل إغراء بذلك، أو جريمة تكون هذه الوسائل بنفسها ضحيتها، وفي ذات الاتجاه يرى Michel وCredo أنها سوء استخدام الوسائل الإلكترونية كأداة لارتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، كما تمتد لتشمل الاعتداءات المادية سواء على الجهاز ذاته أو المعدات المتصلة به وكذلك الاستخدام غير المشروع لبطاقات الائتمان، انتهاك ماكينات الحاسب الآلية بما تتضمنه من شبكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية

---

[1] محمود نجيب حسني، شرح قانون العقوبات، القسم العام، المرجع السابق، ص58.

[2] إن الجريمة العالمية مصدرها القانون الجزائي العالمي، لأنها تتمثل في التصرفات المنافية للأخلاق والمنظومة على عدوان يقع على القيم الأساسية للبشرية في العالم المتمدن، كالحق في الحياة وسلامة الجسم، ويشترك في النص عليها كافة القوانين الجزائية المعاصرة. حسنين إبراهيم صالح عبيد، الوجيز في قانون العقوبات، القسم الخاص، جرائم الاعتداء على الأشخاص والأموال، دار النهضة العربية، القاهرة، 1994، ص125.

[3] David Wall, Crime and the Internet, Routledge, Abingdon, United Kingdom, 1st Ed., 2001 p168.

[4] يونس عرب، جرائم الكمبيوتر والإنترنت، دليل أمن المعلومات والخصوصة، ج1، اتحاد المصارف العربية، الأردن، ط1، 2002، ص206.

والمعنوية[1]، وقد ذهب آخرون إلى تعريفها بأنها كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن الاستخدام غير المشروع لتقنية المعلومات[2].

ومن بين التعريفات التي جاء بها مؤيدو هذا الرأي، التعريف الذي جاء على أنها تلك الجرائم التي لا تعرف الحدود الجغرافية والتي يتم ارتكابها بواسطة الوسائل الإلكترونية عن طريق شبكة الإنترنت، وبواسطة شخص على دراية فائقة بتقنية المعلومات الحديثة[3] من خلال هذا التعريف يتبين أن المصطلحات والتعبيرات الدالة على هذه الظواهر الإجرامية، يربط بينها الوسائل الإلكترونية التي تكون إما هدفا للجريمة أو وسيلة مساعدة لارتكابها.

ومن تعريفات جرائم تكنولوجيا المعلومات الحديثة أيضا أنها كل نشاط إجرامي يؤدي فيه نظام الحاسب الآلي أو الأجهزة الذكية دورا لإتمامه، على أن يكون هذا الدور على قدر من الأهمية ولا يختلف الأمر سواء كان الجهاز أداة لإتمام النشاط الإجرامي أم كان محلا له[4]، وهي أيضا تلك الجرائم العابرة للحدود والتي تقع على شبكة الإنترنت أو بواسطتها من قبل شخص على دراية فائقة بها[5]، إلا أنه من الأفضل عدم تحديد هذه الجرائم بأنها عابرة للحدود لأنها من الممكن أن تكون جرائم داخلية أو دولية أو ذات بعد دولي.

الفرع الثالث: الاتجاه الجامع

بالعودة إلى التعريفات السابقة وتواريخها نجد أنها تعود إلى حقب زمنية مختلفة من مراحل التطور الذي شهدته كل من تكنولوجيا المعلومات وتكنولوجيا الاتصالات، فهذه التعريفات رافقت ظاهرة التقنية منذ بدايات ما يعرف بثورة تقنية المعلومات ومن ثم أخذت بالتوالي مواكبة لتطور مفهوم التقنية، إذ نلاحظ أن التطور المستمر لكل من تكنولوجيا المعلومات وتكنولوجيا الاتصالات خلال السنوات التي صكت فيها غالبية التعاريف وعدم تبلور مفهوم واضح لماهية تكنولوجيا المعلومات الحديثة في مرحلة ما قبل الاندماج بين تكنولوجيا المعلومات وتكنولوجيا الاتصالات، أدى إلى تنوع وتباين التعبيرات والتعريفات التي استخدمت للدلالة على ظاهرة جرائم تكنولوجيا المعلومات الحديثة، وإلى عدم التوصل إلى نموذج واحد متفق عليه فيما يتعلق بالنشاط الإجرامي لهذه الجرائم ذلك أن الفقه والأنظمة القانونية في بلدان العالم قاطبة لم تتفق على صور محددة يندرج في إطارها ما يسمى بجرائم تكنولوجيا المعلومات الحديثة وما استتبع ذلك من تعذر إيجاد فهم مشترك لهذه الظاهرة الجرمية.

أمام ذلك كله وأمام عجز أي من الاتجاهات الفقهية السابقة عن وضع تعريف شامل محدد لجرائم تكنولوجيا المعلومات الحديثة، كان لا بد من التفكير بضرورة شمول التعريف المقصود لكافة العناصر سالفة الذكر، أو معظمها مما يمكن تفادي القدر الأكبر من تلك الانتقادات والملاحظات.

---

[1] هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، دار النهضة العربية، 1997، ص13.

[2] هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، المرجع السابق، ص34.

[3] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2004، ص13.

[4] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، ط1، 2005، ص32 و33.

[5] نبيلة هبة هروال، المرجع السابق، ص31.

ومن هنا عرف البعض جرائم تكنولوجيا المعلومات الحديثة بأنها أية جريمة تستخدم الوسائل الإلكترونية لارتكابها، أو تكون محلا لإغراء ارتكابها، وكل جريمة تكون هذه الوسائل أو تقنيتها ضحيتها، ومن ذلك أيضا أنها كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية، بذات المسعى كان تعريف مكتب المحاسب العام الأمريكي لجرائم التقنية بأنها الأفعال العمدية والمرتبطة بتصميم أو استخدام أو تشغيل النظام والذي تدخل هذه الأفعال في نطاقه[1].

من جهة أخرى أضفى M. Alterman وH. Bloch تعريف منظمة التعاون والتنمية الاقتصادية للغش المعلوماتي على جريمة تكنولوجيا المعلومات الحديثة، وذهبوا إلى القول بأنها كل سلوك غير مشروع أو يتعارض مع قواعد السلوك أو غير مرخص والذي يخص المعالجة الآلية للمعطيات أو انتقال المعطيات[2]، حيث أدخل واضعو هذا المفهوم الجانب المعنوي الأخلاقي[3].

ويرى الخبراء أن هذا التعريف غير عملي ويفضلون الطريقة الأنجلوسكسونية، أي طريقة الجرد والقائمة بحيث يضعون قائمة للأعمال غير المشروعة والتي تدخل في نطاق جرائم التكنولوجيا الحديثة، والحقيقة أن أي مشرع دائما يحدد المصالح المهمة في المجتمع ليقوم بحمايتها وذلك عن طريق تجريم الأفعال التي تهددها بالخطر، ومحل هذا الاعتداء هو المحل القانوني للجريمة وهو الذي يميز هذا النوع من الجرائم عن غيرها.

من هنا يرى أنصار هذا الاتجاه أن الاعتداءات الموجهة ضد الكيان المنطقي للمعلوماتية هي التي تشكل جرائم التكنولوجيا الحديثة، وأن الاعتداء ضد الكيان المادي لا يدخل في عداد هذا النوع من الجرائم، وتبريره في ذلك أن العناصر المادية يمكن أن تخضع للأحكام التقليدية للقانون الجنائي إذ أن سرقة شريط ممغنط أو أسطوانة أو حتى الكمبيوتر لا تندرج تحت طائلة الجريمة المتصلة بالتكنولوجيا الحديثة، لكن هذا الرأي منتقد لأن الغاية من التجريم هي حماية النظام المعلوماتي بكل مكوناته المادية أو المعنوية التي يمكن أن تشمل حتى منتجاته.

وتجدر الإشارة إلى أفضلية استعمال مصطلح حماية النظام المعلوماتي نفسه وحماية منتجات النظام (مستخرجاته)، لأن النظام لا يضم فقط الجزء المادي والبرامج بل المعلومات المخزنة في الذاكرة، وبمفهوم آخر يضم المحتوى، وفي المقابل منتجات النظام وهي المعلومات التي يمكن أن تحفظ أو تستعمل فيما بعد، وأن حماية النظام نفسه لا تطرح أية إشكالية أو صعوبة تتعلق بحق الملكية أو قابليتها للتملك بشرط الأخذ بفكرة أن النظام هو مجموع واقعي يتكون من مجموعة من العناصر الأساسية والتي تعتبر كوسيلة أو وسائل معالجة المعطيات، وهي عبارة عن أموال مادية قابلة كأي منقول مادي للتملك (كمبيوتر وتوابعه)، أما البرامج فهي أعمال ذهنية محمية بواسطة قانون حق المؤلف، ويكفي أن نعتبر أن اجتماع مختلف هذه العناصر كوحدة نظام المعالجة الآلية للبيانات هو نفسه قابل لأن يكون موضوع أو محل للتملك (كمجموع واقعي) مثل المحل التجاري.

---

[1] هشام محمد فريد رستم، جرائم الحاسوب كصورة من صور الجرائم الاقتصادية المستحدثة، مجلة الدراسات القانونية، العدد 17، جامعة أسيوط، مصر 1995، ص260.

[2] H. Alterman, A. Bloch, La fraude informatique, Gazette du Palais, 1988, p530.

[3] Pierre Catala, Op.Cit., p18.

إن تعدد التعريفات واختلافها يرجع إلى اختلاف وجهة نظر فقهاء القانون الجنائي على الوصف القانوني أو التسمية القانونية لهذه الجريمة، فهم لم يتفقوا حتى على المصطلح المستعمل، واختيارنا لمصطلح جرائم التكنولوجيا الحديثة لعله راجع لأن المصطلحات القانونية لا بد وأن تتصف بالمرونة وبعد النظر، بمعنى أنها يجب أن تراعي ما قد يفرزه المستقبل من تطور في مجال الاختراعات الإلكترونية، فمن كان يتصور ظهور مثل هذه الأدوات والوسائط التكنولوجية التي نشاهدها اليوم مثل أجهزة المحمول واللوحات الرقمية التي أصبحت تشبه إلى حد كبير إمكانات الكمبيوتر والاتصال المحلي والدولي وإرسال الرسائل الإلكترونية والصور والكتابات والتعليقات والولوج إلى شبكة الإنترنت...إلخ، فاستعمال مصطلح جرائم التكنولوجيا الحديثة من شأنه أن يدخل في مفهومها جرائم الحاسوب وغيرها من الجرائم والتي قد يسميها البعض بالجرائم المعلوماتية والغش المعلوماتي أو الاعتداء على معطيات الحاسب الآلي وجرائم الإنترنت...إلخ، وبالتالي كان فيه من التوسع ما ينطوي تحت جوانبه العديد من السلوكيات الضارة بالأفراد والجماعة، مما يجعل المشرع يعزز الحماية الجنائية، فلا يستطيع المجرم أن يتحايل ويحقق مآربه وأهدافه عن طريق استغلال التقدم العلمي وما قد يجلبه من إمكانيات لم تكن في ذهن المشرع وقت وضع النصوص القانونية.

أضف إلى ذلك أن مجلس أوروبا استعمل مصطلح الاتفاقية المتعلقة بالجريمة الإلكترونية المعروفة باتفاقية (بودابست) سنة 2001، وتحث هذه الاتفاقية الدول الأعضاء على ردع كل الأعمال الموجهة ضد سلامة وسرية نظم الكمبيوتر والشبكات وبيانات الكمبيوتر وكذلك ضد إساءة استخدام مثل هذه النظم والشبكات والبيانات، فمن خلال استقراء مواد اتفاقية بودابست[1]، يتضح أنها تشمل الدخول غير المشروع، التعامل غير المشروع في بيانات النظام وإساءة استخدام الأجهزة (مما يعني أن جرائم التكنولوجيا الحديثة أشمل من الجريمة الإلكترونية وكذا الجريمة المعلوماتية).

حتى وإن تعددت المصطلحات فإننا نؤيد الرأي الراجح باصطلاحها جرائم تكنولوجيا المعلومات الحديثة، لأن البرامج والمعلومات أثناء تواجدها في النظام أو أثناء معالجتها أو انتقالها ماهي إلا عبارة عن نبضات إلكترونية ولابد من التعامل معها بلغة الآلة، وبناء على ما تقدم، فإن أي تعريف سليم لجريمة تقنية المعلومات الحديثة لابد أن ينطلق من الإحاطة الكاملة والتحديد السليم لماهية تكنولوجيا المعلومات الحديثة، والتي تشكل إطار وبيئة هذه الجريمة.

ومن ناحية ثانية يجب أن يتلاءم هذا التعريف مع فكرة عالمية تكنولوجيا المعلومات والاتصالات الحديثة، بمعنى أن يكون التعريف مقبولا ومفهوما على المستوى العالمي.

ومن ناحية ثالثة يجب أن يراعي هذا التعريف أن جرائم تقنية المعلومات الحديثة ليست محصورة في نموذج أمن المعلومات ذو الأبعاد الثلاثة (سرية المعلومات سلامة المعلومات، وجود المعلومات)، فهذه الجرائم لها صور أخرى متعددة تختلف باختلاف الهدف المباشر في الجريمة، إذ أنها تنطوي على أنماط عديدة من السلوك الإجرامي، وبالتالي من الخطأ قصرها على أنها كل فعل عمدي يتوصل فيه الجاني بغير وجه حق إلى موقع أو نظام معلوماتي يتم الدخول إليه ويترتب على الفعل إلغاء، حذف، تدمير، إفشاء، إتلاف، تغيير، إعادة نشر البيانات أو المعلومات.

[1] المواد من 01 إلى 06 من الفصل الأول، القسم الأول من اتفاقية بودابست سنة 2001 المتعلقة بالجريمة الإلكترونية.

ومن ناحية أخرى يجب أن يوضح التعريف خصوصية جريمة تكنولوجيا المعلومات الحديثة فيبدو واضحا الدور الذي تقوم به وسيلة تقنية المعلومات الحديثة في ارتكاب الجريمة، أي أن تقوم هذه الوسيلة بدور في الجريمة على قدر من الأهمية، ولا يعني ذلك في تقديرنا أن يصل هذا الدور إلى الحد الذي لا يمكن أن تتم الجريمة بدونه بل يكفي أن تسهل في ارتكاب الجريمة، أي أن يكون لها دور في إتمامها على النحو الذي تمت به.

من هنا يمكن القول إن جرائم التكنولوجيا الحديثة هي تلك الجريمة التي يكون محلها المعطيات المعالجة بلغة الآلة أي المعلومات والبرامج، أو بمفهوم أوسع النظام المعلوماتي، إضافة إلى وسيلة ارتكابها الكمبيوتر أو أية وسيلة إلكترونية لأنه يمكن الدخول إلى النظام بدونه، وتخرج من هذه الطائفة تلك الجرائم المرتكبة بواسطة الوسائل الإلكترونية التي تستوعبها القواعد التقليدية، وما دام هذا النوع من الجرائم مستحدثا فهذا يدل على أن لديها أسبابا ومميزات تختلف عن تلك المعهودة في الجرائم التقليدية.

وتجدر الإشارة إلى أن الفقه القانوني العربي لم يقف موقف المنتظر أمام هذا الجدل الدائر في الفقه الدولي المقارن حول إيجاد تعريف شامل محدد لجرائم التكنولوجيا الحديثة، بل تعدى مفكرو ورجال القانون فيه الحد الطبيعي لهذا النظام الجديد المستحدث من الإجرام، بغية رصد محاوره الرئيسة ومحاولة لإيجاد التعريف الجامع المانع لهذا النوع من الجرائم، ولكن بقيت روح تلك المحاولات منقادة وراء الاتجاهات السابقة في التركيز فقط على بعض جوانب الجريمة دون غيرها فيما جاءت محاولات أخرى أكثر شمولية.

فقد ذهب البعض إلى تعريف جرائم تكنولوجيا المعلومات الحديثة معتمدا على خاصية توافر المعرفة التقنية للفاعل، فجاءوا بتعريفها: "أنها جرائم يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالوسائل الإلكترونية بعمل غير قانوني"[1]، وعرفها الدكتور محمد سامي الشوا بأنها كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات ويهدف إلى الاعتداء على الأموال المادية أو المعنوية، وعرفها الريان بقوله "إنها جرائم تحتاج إلى معرفة التقنية لمرتكبها"[2]، فيما عرفها غيره بأنها سلوك غير مشروع يعاقب عليه القانون؛ صادر عن إرادة محلها معطيات الحاسوب، أما الدكتورة هدى حامد قشقوش فقد عرفت جرائم تكنولوجيا المعلومات الحديثة بأنها: "كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات"[3] ونجد أن مشرع دولة الإمارات العربية المتحدة قد أو رد مجموعة من التعريفات تتمحور حول المعلوماتية والجرائم المتصلة بها تكتسي نوعا من الدقة، وذلك ضمن المادة الأولى من قانون مكافحة جرائم تقنية المعلومات (2006/02).

بناء على ما سبق نجد تقاربا كبيرا في التعريفات بين مصطلح المعلوماتية وتقنية المعلومات، والتي تعرف بأنها أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزنة بها ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكيا أو لا سلكيا في نظام أو شبكة[4]، ويقصد بالمعلوماتية علم معالجة البيانات والمعلومات للتخزين والاسترجاع.

---

[1] عبد الله عبد العزيز اليوسف، التقنية والجرائم المستحدثة، الظواهر الإجرامية المستحدثة وسبل مواجهتها، ندوة علمية، أكاديمية نايف للعلوم الأمنية الرياض، 1999.

[2] محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، الهيئة المصرية العامة للكتاب، القاهرة، 2003، ص18.

[3] هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992، ص15.

[4] جاء هذا التعريف ضمن نص المادة 02 من نص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

بربط مفهوم كل من مصطلح الجريمة والتكنولوجيا نجد أدق تعريف للجريمة المتصلة بتكنولوجيا المعلوماتية هو ما قدمه الدكتور مارتن؛ والذي اصطلح على هذا النوع من الجرائم مصطلح الجريمة ذات التقنية العالية، فعرفها بأنها الجريمة التي تغطي جميع الأفعال غير المشروعة للاهتمام بتكنولوجيا المعلومات والاتصالات من حيث الأجهزة والبرمجيات.

إنطلاقا من هذا التعريف، يتضح جليا أنه علينا أن نميز بين صورتين أساسيتين، الأولى عندما تكون المعلوماتية موضوعا للاعتداء، وتتفق هذه الحالة عندما تقع الجريمة على المكونات المادية للوسائل الإلكترونية من أجهزة ومعدات وكابلات وشبكات ربط وآلات طباعة...إلخ[1]، أما الثانية عندما تكون المعلوماتية أداة ووسيلة للاعتداء، وتتحقق هذه الحالة عندما يستخدم الجاني الكمبيوتر كوسيلة لتنفيذ جرائمه، سواء على الأشخاص أو على الأموال[2].

ونجد أن المشرع الجزائري قد تطرق إلى الصورة الأولى على سبيل المثال من خلال المواد 394 مكرر وما يليها من قانون العقوبات[3] مسميا إياها بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، في حين أن الصورة الثانية تضمنها القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[4]، ومنه فالصنف الثاني هو الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

وحسن ما فعل المشرع الجزائري في عنونة القانون رقم 09-04 بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فهو بذلك جمع الصورتين، أي الجرائم المعلوماتية أو السبرانية وكذا الجرائم المتصلة بتكنولوجيا المعلوماتية، مع العلم أن الجرائم المعلوماتية ماهي إلا صنف من الجرائم المتصلة بالتكنولوجيا الحديثة، فالأولى هي الوسيلة والمحل في آن واحد، في حين الصنف الثاني تكون المعلوماتية فيه مجرد وسيلة، وبالرجوع إلى المادة 02 من نفس القانون المذكور أعلاه نجد أن المشرع اصطلح على الجرائم المتصلة بالتكنولوجيا الحديثة عبارة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على أنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية، ويعاب على المشرع الجزائري أنه أورد تسمية فضفاضة وتتسع لأكثر من تأويل باستخدامه لمصطلحي الإعلام والاتصال، إذ كان عليه أن يضع مصطلحات أكثر دقة، أو أن ينص على مدلول المصطلحين ضمن نص المادة الثانية من القانون رقم 09-04، ونحن نرى أن المصطلحات المعرفة في نص المادة سالفة الذكر غير كافية لإعطاء التسمية الدقيقة والصحيحة فجاء في نص المادة تعريف ما يلي:

الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

---

[1] هشام محمد فريد رستم، جرائم الحاسوب كصورة من صور الجرائم للاقتصادية المستحدثة، المرجع السابق، ص25.

[2] عامر نزار فايز أبو علي، فيروسات الكمبيوتر، دار حنين للنشر والتوزيع، عمان، 1994، ص48.

[3] قانون رقم 16-02 مؤرخ في 19 يونيو 2016 المتضمن قانون العقوبات، ج.ر، العدد 37، مؤرخة في 22 يونيو 2016، الصادر بموجب الأمر رقم 66-156 مؤرخ في 08 يونيو 1966، ج.ر، العدد 49، مؤرخة في 11 يونيو 1966، المعدل والمتمم.

[4] قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430ه الموافق لـ 05 غشت 2009م، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر، العدد 47، مؤرخة في 16 غشت 2009.

منظومة معلوماتية: أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.

معطيات المعلوماتية: أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها.

مقدمو الخدمات: أي كيان عام أو خاص يقدم للمستعملين خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات، وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصالات المذكورة أو لمستعمليها.

المعطيات المتعلقة بحركة السير: أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة.

الاتصالات الإلكترونية: أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.

بالرجوع إلى ما سبق من التعريفات لا نجد تعريفا لمصطلح الإعلام ولا مصطلح الاتصال ولا حتى مصطلح المعلوماتية في نص القانون، بل نجد أن التعريف الوارد في الفقرة أ ينطبق تماما ومصطلح الجريمة المتصلة بتكنولوجيا المعلوماتية، فهي كل جريمة تهدف للمساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات الجزائري، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية، وعليه فإننا نرى أن المشرع الجزائري قد وفق إلى حد ما في وضع تعريف أدق لجرائم التكنولوجيا الحديثة، إلا أنه كان من الأفضل تغيير التسمية إلى الجرائم المتصلة بتكنولوجيا المعلومات الحديثة عوض الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

بدورنا نرى أن التعريف أيا كان لا بد أن يكون دالا عن مضمونه ويقاس نجاحه أو فشله بمدى شموله للأجزاء المعرفة، ولهذا فإن أي تعريف صحيح لجرائم تكنولوجيا المعلومات الحديثة يجب أن تقع فيه بواسطة الحاسب الآلي أو عليه، أو أية وسيلة إلكترونية أخرى تفي بالغرض، وأن تكون مقصودة، بالإضافة إلى ضرورة توافر حد أدنى من المعرفة التقنية للجاني أو الجناة، ولهذا فإن التعريف الذي نجده هنا هو أن جرائم تكنولوجيا المعلومات الحديثة هي كل جريمة مقصودة ترتكب بواسطة تقنية أنظمة المعلومات أو عليها تتوافر فيها معرفة التقنية لفاعلها[1].

نخلص إلى القول إن جرائم تكنولوجيا المعلومات الحديثة هي تعبير شامل يشير إلى كل نشاط إجرامي مرتبط باستخدام تقنية المعلومات الحديثة، ولا يختلف الأمر سواء كانت وسيلة تقنية المعلومات الحديثة أداة لإتمام النشاط الإجرامي أم كانت محلا له أو هدفا للاعتداء.

[1] أسامة أحمد المناعسة وآخرون، جرائم الحاسب الآلي والإنترنت، دراسة تحليلية مقارنة، دار وائل، عمان، ط1، 2001، ص80.

المطلب الثاني: نشأة وتطور جرائم التكنولوجيا الحديثة

لما كان التطور هو سنة الحياة في الكون، وقاعدة أزلية وفطرة الله التي خلق الناس عليها، وبتباين المخترعات والمكتشفات التي تظهر كل يوم وفقا لما أفرزه التقدم العلمي والتقني في شتى نواحي الحياة كان الحاسوب هو إحدى هذه الصور وكانت الشبكة العنكبوتية هي إحدى صور الاستخدامات العامة والضرورية لمثل هذه التقنيات الحديثة وصورة حية من صور تقدم أجهزة الاتصال واستخدام تكنولوجيا المعلومات[1].

كما أنه بتقدم التكنولوجيا تطورت الجرائم المرتبطة بها، وأصبح استخدام التكنولوجيا الحديثة في ارتكاب الجرائم يشكل خطورة كبيرة، الأمر الذي مكن المجرمين من ارتكاب العديد من الجرائم كالتشهير، التهديد، الابتزاز، سرقة الأموال والمعلومات والتجسس...إلخ، من خلال تطور تدريجي لارتكاب تلك الجرائم وفقا لتطور التقنيات الحديثة.

الفرع الأول: مراحل تطور التكنولوجيا الحديثة والجرائم المتصلة بها

مر مفهوم جرائم التكنولوجيا بتطور تاريخي تبعا لتطور التقنية واستخداماتها، ذلك أن المجتمعات اعتمدت على الوسائل والوسائط التكنولوجية والتقنية اعتمادا رئيسيا في كافة مجالات الحياة، فكان لزاما أن يرافق التطور التكنولوجي التعدد في الجرائم المرتبطة بها تبعا لتطور التقنية واستخداماتها، وتعد بداية صناعة الحواسيب وإنطلاق ثورة الإلكترونيات مستقلة عن وسائل الاتصال التي وقعت في خمسينيات القرن الماضي، إذ اقتصر استخدام الحواسيب على المؤسسة العسكرية وفي مجالات ضيقة لدى المؤسسات الكبرى التابعة للدولة، كما بدأ الاستخدام التجاري للحواسيب في الخمسينات، وفي ذلك الوقت لم يكن في الأذهان تصور الخطر الناجم عن استخدامها، وإن وجد فلم يتعلق بالإجرام[2].

البند الأول: المرحلة الأولى (نهاية الخمسينات وبداية الستينات)

ظهر مصطلح تكنولوجيا المعلوماتية بظهور الحاسب الآلي وتطور إلى أن أصبح عالما قائما بذاته يدعى العالم الافتراضي وكان الهدف الأول من اختراع جهاز الكمبيوتر أو كما هو متعارف عليه جهاز الحاسوب لإجراء العمليات الحسابية وتخزينها، ويرجع تاريخ صناعة أول جهاز حاسوب في العالم إلى العام 1937 بجامعة هارفارد الأمريكية ليتم تطويره في عام 1946 بتمويل من قبل وزارة الدفاع الأمريكية والتي احتفظت بهذا الاختراع سرا، وكانت كامل أجزائه إلكترونية، إلا أنه كان يزن أكثر من ثلاثين طنا ويشغل مساحة كبيرة أيضا، ويقوم بحوالي 500 عملية جمع وحوالي 30 عملية ضرب في الثانية الواحدة، لكن صناعة حاسب إلكتروني التركيب بشكل كامل فتح باب التطوير والتطور.

وبدأت ظاهرة جرائم الحاسوب بالظهور في نهاية الخمسينات من القرن العشرين ولكن ضمن إطار مفهوم استخدام الحاسوب المؤسس على البعد الأخلاقي نتيجة انتشار الحواسيب وتعدد استخداماتها، ولعل أول جريمة معلوماتية كان ارتكابها في

---

[1] هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، المرجع السابق، ص09.

[2] علي جبار الحسناوي، جرائم الحاسوب والإنترنت، دار اليازوري العلمية للنشر والتوزيع، الأردن، 2009، ص17 و18.

الولايات المتحدة الأمريكية سنة 1958[1]، وكانت الأنشطة الإجرامية المتصلة بالحاسوب تصاغ وفق مدلول أخلاقي أكثر منه قانوني الأمر الذي أدى إلى عدم التمييز بين الأنشطة الإجرامية التي تستهدف ماديات الحاسوب وتلك التي تستهدف معطيات الحاسوب وحتى الرؤية القانونية تعاملت مع المكونات كممتلكات مادية منقولة لاعتداءات إجرامية لها نفس الدلالة للجرائم التقليدية.

وبدأ بروز مفهوم إساءة استخدام الكمبيوتر والعبث بالبيانات في مطلع الستينات وظهرت أولى المعالجات التي اقتصرت على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والتجسس المعلوماتي والاستخدام غير المشروع للبيانات المخزنة في نظم الكمبيوتر، وترافقت هذه النقاشات مع التساؤل عما إذا كانت هذه الجرائم مجرد شيء عابر أم ظاهرة إجرامية مستجدة، بل وأكثر من ذلك فقد ثار الجدل حول ما إذا كانت جرائما بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في بيئة أو مهنة الحوسبة وبقي التعامل معها أقرب إلى النطاق الأخلاقي منه إلى النطاق القانوني[2]، أما في البلاد الأوروبية فيرجع تاريخ أول جريمة معلوماتية إلى سنة 1968 في فنلندا وتعلقت بتقليد برامج الكمبيوتر[3].

ومع تزايد استخدام الحواسيب الشخصية في منتصف السبعينات، ظهر عدد من الدراسات المسحية والقانونية التي اهتمت بالجرائم المتصلة بها وعالجت عددا لا بأس به من قضايا الجرائم الفعلية وبدأ الحديث عن الجرائم المرتبطة بها بوصفها ظاهرة إجرامية لا مجرد سلوكيات مرفوضة ومنبوذة، إن هذا التطور الرهيب لم يكن نتاج تطور أجهزة الإعلام الآلي فحسب بل كان نتيجة لتطور الشبكات، وأهمها الإنترنت.

فالإنترنت تعتبر شبكة شبكات القرن الحادي والعشرين، ومحرك الحضارة الجديدة التي تقوم على فكرة الاتصال لا الانتقال، إذ تحددت نقطة الإنطلاق بإطلاق الاتحاد السوفييتي قمره الصناعي الأول سبوتنك في عام 1957، حينها شعرت الولايات المتحدة الأمريكية بخطورة هذه الخطوة العملاقة وأحست أنها تحتاج إلى إعادة تخطيط استراتيجيتها لضمان التفوق، وكان الرد متمثلا في إنشاء وكالة لمشروعات الأبحاث المتقدمة وعهدت إليها بمهمة تحقيق التفوق العلمي والتكنولوجي للقوات المسلحة في مواجهة الاتحاد السوفييتي.

وفي عام 1962 عهدت القوات الجوية الأمريكية لمؤسسة راند[4] بتنفيذ دراسة لتحقيق ضمان استمرار السيطرة على ترسانة الصواريخ والقاذفات إذا ما تعرضت الولايات المتحدة الأمريكية كلها أو جزء منها لهجوم نووي من جانب الاتحاد السوفييتي وكان الحل المقترح هو إنشاء شبكة اتصالات عسكرية للسيطرة والتحكم تعمل على أسس لامركزية وبأسلوب يحقق استمرار عمل الشبكة حتى ولو تعرضت بعض العقد الموجودة فيها إلى هجوم نووي، وبما يضمن إمكانية الرد على هذا الهجوم، وتعزيزا للاقتراح سالف الذكر قدم باحث الاتصالات الشهير بول بارن مقترحا لإنشاء شبكة اتصالات يتحقق من خلالها الاتصال عن طريق تقسيم رسالة إلى حزم متساوية، ثم إرسال نسخ متعددة من هذه الحزم في مسارات مختلفة بحيث يتم تجميع هذه الحزمة مرة أخرى في نقطة الاستقبال

---

[1] شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، أطروحة دكتوراه، كلية الحقوق، جامعة المنصورة، مصر، 2005، ص21.

[2] يونس عرب، جرائم الحاسوب، جرائم الكمبيوتر والإنترنت، إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات، مؤتمر الأمن العربي، أبو ظبي، 10-12 فبراير 2002.

[3] شيماء عبد الغني محمد عطا الله، المرجع السابق، ص21.

[4] مؤسسة راند هي مؤسسة حكومية أمريكية متخصصة في أنشطة البحوث والتطوير.

من أي من المسارات المكتملة، وبهذا لا يتأثر الاتصال عبر الشبكة بسقوطهم في مسار ما، إذ يستمر العمل عن طريق المسارات الأخرى وسميت هذه الطريقة بشبكة الحزم، فكانت هذه بداية فكرة الإنترنت وظهور الجرائم المرتبطة بها، وفي عام 1969 أنشئت الشبكة الأولى والتي سميت شبكة وكالة المشروعات المتقدمة، كل ما تحتويه هو أربعة حاسبات رئيسية موزعة بين جامعة كاليفورنيا في لوس أنجلس، معهد ستانفورد للأبحاث في شمال كاليفورنيا، جامعة كاليفورنيا في مدينة سانتا باربرا، وأخيرا جامعة يوتاه، متصلة بسرعة ربط تصل إلى 50 ألف نبضة في الثانية وكانت هذه بداية شبكة الإنترنت.

طور الباحث راي توم تيسون؛ أول برنامج للبريد الإلكتروني في عام 1972، كما شهد هذا العام أيضا تحويل وكالة المشروعات المتقدمة (ARPA) إلى وكالة الدفاع لمشروعات الأبحاث المتقدمة (DARPA: Defense Advanced Research Projects Agency)، وتطور استخدام بروتوكول للاتصالات سمي (NCP: Network Control Protocol) الذي يسمح باتصال أي حاسب يعمل وفق هذا البروتوكول، مما أدى إلى زيادة عدد الوحدات المتصلة بالشبكة إلى 23 حاسبا واستمرت سرعة شبكة الاتصال عند 50 ألف نبضة في الثانية، وفي عام 1973 طور فين سيرف؛ وهو الملقب بأب الإنترنت بروتوكولا سمي (TCP/IP) يسمح بتوصيل أجهزة الكمبيوتر التي تعمل بأنظمة عمل مختلفة وشبكات الكمبيوتر التي تعمل ببروتوكولات مختلفة ببعضها البعض، أما في عام 1974 استخدم فين سيرف؛ كلمة إنترنت (Internet) لأول مرة في ورقة قدمها إلى مؤتمر حول بروتوكولات التحكم في الاتصال (TCP).

وفي هذه الحقبة الزمنية دائما شهد عام 1976 تطورات هائلة غير مرتبطة بالإنترنت إلا أنها فتحت الباب على مصراعيه لحدوث طفرة فيها، ففي هذا العام قدمت شركة زيروكس عن طريق روبرت ميتكلف؛ بروتوكولات الإيثرنت Ethernet والذي قامت عليه معظم الشبكات الداخلية لأجهزة الكمبيوتر باستخدام الكابلات المحورية، إذ حقق هذا البروتوكول طفرة في إنشاء ما أطلق عليه الشبكات المحلية (LAN: Local Area Network) ونجحت تجارب الربط بين الولايات المتحدة الأمريكية وأوروبا باستخدام الأقمار الصناعية ونجحت شبكة SATNET، وفي هذا العام أيضا قررت وكالة الدفاع الأمريكية لمشروعات الأبحاث المتقدمة تبني بروتوكول (TCP/IP) على شبكتها (ARPA.NET) وأدى هذا لحدوث قفزة في عدد الحاسبات المتصلة بالشبكة لتصل إلى حوالي 111 حاسب واستخدمت لأول مرة الاتصالات اللاسلكية وشبكة الاتصالات عبر الأقمار الصناعية.

البند الثاني: المرحلة الثانية (الثمانينات)

في هذه الحقبة الزمنية، طفا على السطح مفهوم جديد لجرائم التكنولوجيا الحديثة ارتبط أساسا بعمليات اقتحام نظم الكمبيوتر عن بعد، وأنشطة نشر وزراعة الفيروسات الإلكترونية التي تقوم بعملية تدمير الملفات أو البرامج، وشاع في هذه الفترة اصطلاح الهاكرز المعبر عن مقتحمي النظم.

غير أن الحديث عن دوافع ارتكاب هذه الأفعال ظل في غالب الأحيان محصورا في الحديث عن رغبة المخترقين في تجاوز إجراءات أمن المعلومات وفي إظهار تفوقهم التقني، وانحصر الحديث عن مرتكبي هذه الأفعال حول صغار السن من المتفوقين الراغبين

في التحدي والمغامرة، ثم نشأت معه قواعد سلوكية لهيئات ومنظمات الهاكرز طالبو معها بوقف تشويه حقيقتهم وإصرارهم على أنهم يؤدون خدمة في التوعية لأهمية معايير أمن النظم والمعلومات.

لكن الحقيقة أن مغامري الأمس القريب أصبحوا عتاة إجرام فيما بعد، إلى حد إعادة النظر في تحديد سمات مرتكبي الجرائم وطوائفهم، وظهر المجرم المعلوماتي المتفوق المدفوع بأغراض إجرامية خطيرة، والقادر على ارتكاب أفعال تستهدف الاستيلاء على المال أو تستهدف التجسس أو الاستيلاء على البيانات السرية الاقتصادية والاجتماعية والسياسية والعسكرية[1].

وفي عام 1981 أنشئت الهيئة القومية للبحث العلمي (NSF: National Science Foundation) شبكة جديدة سميت (CSNET) لتربط بين الجامعات غير المشاركة في شبكة (ARPA NET) وذلك بسرعات وصلت حتى 56 ألف نبضة في الثانية وقدم فين سيرف؛ مقترحا لربط هذه الشبكة مع شبكة وزارة الدفاع (ARPA NET)، وكانت العناوين المستخدمة حتى هذا التاريخ في الرسائل التي يتم تبادلها تستخدم الأرقام حيث يتم إعطاء رقم محدد لكل مشترك أطلق عليه اصطلاح (IP Number) وكان على أي مشترك يرغب في التواصل مع مشترك آخر أن يحفظ هذا الرقم ويكتبه في بداية رسالته، إلا أن جامعة ويسكونسن؛ قدمت في عام 1983 خدمة إضافية هي خدمة اسم النطاق (DNS: Domaine Name Server) والذي يسمح باستخدام الأسماء إذ يكون أمام كل اسم الرقم الخاص به (IP Number)، ويتم التحويل بصورة أوتوماتيكية وبهذا فتح باب الاستخدام دون الحاجة لتذكر المشتركين.

وفي عام 1988 أفاق العالم على دودة موريس، هذه الحادثة هي إحدى أولى الهجمات الكبيرة والخطرة في بيئة الشبكات ترجع أحداث هذه الحادثة عندما تمكن طالب يبلغ من العمر 23 سنة يدعى روبرت موريس من إطلاق فيروس عرف آنذاك باسم دودة موريس عبر الإنترنت أدى إلى إصابة حوالي ستة آلاف جهاز يرتبط معها نحو60 ألف نظام عبر الإنترنت من ضمنها أجهزة العديد من المؤسسات والدوائر الحكومية، إثر هذه الحادثة تم تجريم روبيرت موريس وإدانته وتم الحكم عليه بالسجن لمدة 3 سنوات وبغرامة مالية قدرت بعشرة آلاف دولار أمريكي[2].

البند الثالث: المرحلة الثالثة (فترة التسعينات وبداية القرن الحالي)

شهدت تسعينات القرن الماضي وبداية القرن الحالي تناميا هائلا في حقل الجرائم المتصلة بالتكنولوجيا الحديثة، وتغيرا في نطاقها ومفهومها، والسبب الرئيسي في ذلك يرجع إلى ما أحدثته شبكة الإنترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكات المعلومات.

فظهرت أنماط جديدة وفريدة للجريمة، كأنشطة إنكار الخدمة، التي تقوم أساسا على فكرة تعطيل نظام تقني ومنعة من القيام بعمله المعتاد، وقد انتشر هذا النوع من الجرائم على مواقع الإنترنت التسويقية، الأمر الذي يسبب انقطاع الخدمة عنه لساعات إلى خسائر مادية تقدر بالملايين إن لم تكن بالملايير، ونشطت جرائم نشر الفيروسات عبر مواقع الإنترنت، لما تسهله من انتقالها إلى ملايين المستخدمين في العالم وفي الوقت ذاته، وظهرت أنشطة الرسائل والمواد الكتابية المنشورة على الإنترنت أو المرسلة عبر البريد

[1] يونس عرب، جرائم الحاسوب، جرائم الكمبيوتر والإنترنت، المرجع السابق.

[2] نبيلة هبة هروال، المرجع السابق، ص54.

الإلكتروني المنطوية على إثارة الأحقاد أو المساس بكرامة الأشخاص أو الترويج لمواد أو أفعال غير قانونية وغير مشروعة (جرائم المحتوى الضار)، في عام 1990 تطورت السرعة من (TI) إلى (TS) وهي سرعة تصل إلى 45 ميجابت / الثانية، كما ظهر لأول مرة أسلوب استخدام النصوص التفاعلية والذي يتيح للمستخدم الانتقال من جزء إلى آخر ثم العودة لذات المنطقة التي بدأ منها.

في عام 1992 ظهر مولد الشبكة العالمية (World Wide Web)، كما أنشأت جمعية الإنترنت العالمية (Internet Society) لتكون هي الجهة المسؤولة عن إدارة وتنظيم العمل على شبكة الإنترنت مما زاد من تنظيم هذه الشبكة وبالنتيجة زادت أعداد الأجهزة المتصلة لتتجاوز المليون جهاز، وفي عام 1993 قدم مارك أندرسون، وهو طالب بجامعة إلينوي أول واجهة تعامل بين الإنترنت والمستخدم تعتمد على التعامل الجرافيكي وسميت موزايك (Mosaic) وقام بعد ذلك بإنشاء شركة ناتسكيب (Netscape) التي تولت بناء متصفحات الإنترنت ليظهر بعد ذلك مصطلح العالم الافتراضي.

ففي عصرنا الذي يشهد تطورا سريعا، وكأنما العلوم والتكنولوجيا تتسابق في نهر جار، لا يكاد يتوقف تسابق كل قطرة فيه عن الأخرى، إذ أصبح كل اختراع واكتشاف في هذا المجال ينافس الآخر، وظهر الحاسوب الذي كان في بداية أمره لبعض الاستخدامات الشخصية وما لبثت أن ظهرت الشبكة العنكبوتية (الإنترنت) والتي كانت لها محدوديتها، أي أنها قاصرة على فئة معينة، فلم تكن آمنة في تصميمها وبنائها.

إلا أن دوام الحال من المحال، فقد أدى التطور التاريخي للإنترنت إلى زيادة عدد مستخدميه من جميع الفئات وهو بذلك فتح أبوابا مغلقة أمامهم ووسع حدودا أصبحت بلا حراسة مما ساهم في ظهور جرائم مستحدثة دقت ناقوس الخطر لتنبه المجتمعات عن مدى خطورتها، وظهر المجرم المدفوع بارتكاب الأفعال المجرمة في حقل التقنية كجرائم تكنولوجيا المعلومات الحديثة[1].

يتبين مما سبق ذكره أن جرائم تكنولوجيا المعلومات الحديثة لها جذور تاريخية ترجع إلى خمسينيات القرن الماضي، ولكن لم تكن معروفة كما هي عليه الآن، ولعل ذلك راجع إلى استخدام الوسائل الإلكترونية والانتشار الواسع لشبكات الإنترنت والتكنولوجيا الحديثة بالإضافة إلى وصول هذه التقنيات العالية إلى أشخاص على مستوى عال من الذكاء.

فجرائم التكنولوجيا الحديثة من الجرائم المستحدثة، تتنوع وتتضاعف يوما بعد يوم، والمستجد هو الكيانات المعنوية ذات القيمة المالية، ولولا هذه الطبيعة المستجدة في الأساس لما كنا أمام ظاهرة مستجدة برمتها، وكذلك المستجد هو دخول الكمبيوتر ومختلف الوسائل الإلكترونية والمتطورة عالم الإجرام، وقد عرفت الجزائر هذا النوع من الجرائم كغيرها من دول العالم ولكن ليس بنفس النسب والخطورة التي شهدتها الدول الغربية المتقدمة.

الفرع الثاني: تفاقم حجم الجرائم المتصلة بالتكنولوجيا الحديثة

هناك العديد من الأسباب والتي يمكن ذكرها على سبيل المثال لا الحصر كأسباب لتزايد حجم جرائم التكنولوجيا الحديثة.

البند الأول: أسباب تزايد حجم جرائم التكنولوجيا الحديثة

تميز القرن الواحد والعشرون باستخدام تقنية المعلومات على نطاق واسع، وعلى مدى السنوات القليلة الماضية توسعت

[1] جواهر بنت عبد العزيز آل سعود، الجرائم الإلكترونية ومكافحتها، مجلة الاتصالات والعالم الرقمي، العدد 209، جدة، 1428ھ، ص11.

الإنترنت أضعافا مضاعفة حاليا، فهناك حوالي 820 مليون شخص يستخدمون الإنترنت، ما يعادل زيادة قدرها 126% في الفترة الممتدة ما بين 2000 إلى 2015.

ولقد وفرت السهولة النسبية لاستخدام الإنترنت الحصول عليها على نحو متزايد بأسعار معقولة إضافة إلى الحصول على الوسائل الإلكترونية مع أجهزة المودم فائقة السرعة، كل هذا مكن الناس من الاتصال والتواصل وتكوين صداقات الجديدة، الترفيه التعلم، القيام بأعمال تجارية ودفع فواتير عبر الإنترنت...إلخ، بالإضافة إلى خلق شبكة ويب عالمية لما يسمى العالم الافتراضي أو الفضاء الإلكتروني والذي يعرف بأنه مكان لأجل غير مسمى حيث يتفاعل الأفراد والمجتمعات.

يتضح أن جرائم التكنولوجيا الحديثة أصبحت من أخطر الجرائم في الآونة الأخيرة، فقد أصبحت تهدد أمن واستقرار العالم أجمع بسبب خطورتها وتزايدها وانتشارها السريع، ولعل ذلك راجع أساسا إلى ارتفاع العائد المادي في الربح المتحصل عليه من الجاني من جرائم التكنولوجيا الحديثة وقلة المخاطر المتعرض لها إضافة إلى اتساع دائرة التعليم للوسائل الإلكترونية ومكوناتها وتعميم دراستها بالمدارس والجامعات وكذا القصور التشريعي لقمع الجناة، ما يقلل من درجة احتمالية ضبط هؤلاء الجناة وإيداعهم في المؤسسات العقابية لينالوا الجزاء[1]، وكان لتداخل الوسائل الإلكترونية في بيئة الأعمال التجارية والمعاملات في القطاع العام والخاص دور كذلك في زيادة مخاطر هذا النوع من الجرائم، كما أن عدم الاستقرار السياسي في العالم يضاعف احتمالات الاعتداء على أجهزة الحاسب الآلي والأجهزة الذكية ونظم الاتصالات، خاصة في الدول المتقدمة التي تعتمد كليا على التقنيات العالية، كما أن احتمالات القرصنة وسرقة المعلومات الشخصية والاعتداء على الحريات الخاصة من خلال شبكة الإنترنت كله من شأنه أن يساهم في تفاقم هذه الجرائم.

البند الثاني: حجم مستخدمي شبكة الإنترنت والجرائم المتصلة بها

لقد انتقل الناس من العالم الواقعي إلى العالم الافتراضي، وكذلك انتقلت الجريمة، ولنا أن نتصور حجم التفاعلات التي تتم في العالم الافتراضي سواء كانت شخصية، مؤسسية، أو في مجال الأعمال أو الخدمات أو الثقافة...إلخ، فعلى سبيل المثال على موقع التواصل الاجتماعي فيسبوك، نجد من المعجبين بصورة أو مقطع فيديو ما يفوق 5 مليون شخص، ومتوسط عدد الأصدقاء على نفس الحساب 130 صديق، وعدد المشتركين 850 مليون منهم 21% في آسيا و488 مليون يستخدمون فيسبوك الجوال و23% من المشتركين يتفقدون حساباتهم أكثر من 05 مرات في اليوم، وهناك أكثر من مليون موقع متصل مع فيسبوك، وتوضع أكثر من 250 مليون صورة يوميا، وفي عام 2013 تم تشغيل 210000 مقطع موسيقي من المشتركين منهم 43% ذكور و57% من الإناث.

ووفقا لمكتب إحصاءات العدل فإن معدل جرائم العنف انخفض بنسبة 10% سنة 2001، واستمر في الانخفاض منذ عام 1994، كما سجلت جرائم الإيذاء العنيف والممتلكات أدنى مستوى لها معدلات الجريمة منذ استخدام المسح الوطني لضحايا الجريمة في عام 1973، من ناحية أخرى، فإن عدد ضحايا جرائم التكنولوجيا الحديثة في ارتفاع نظرا لزيادة عدد مستخدمي الإنترنت، كما تجدر الإشارة إلى تزايد عدد الذين يعانون من خسارة مالية، أو المهددين أو المطاردين فهي مشكلة تستحق الدراسة

[1] ضياء يحي السادات، مبادئ استخدام الحاسب الآلي والإنترنت، وجهود مكافحة الجرائم الناشئة عنهما، منشأة المعارف، ط1، 2012، ص94.

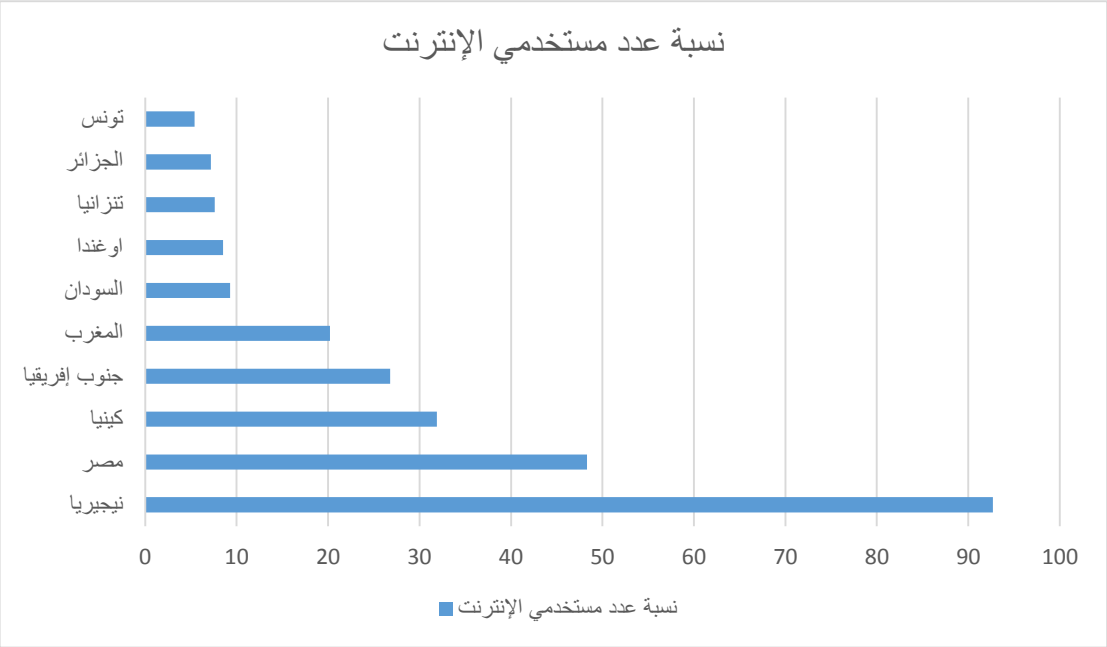
ويمكن دراسة نمط جرائم التكنولوجيا الحديثة من خلال وجهات نظر مختلفة، بما في ذلك وجهة نظر المجرم أو وجهة نظر الضحية إذ تمثل جرائم التكنولوجيا الحديثة المجال الجديد من الأبحاث في مجال علم الجريمة.

وقد أشار الاتحاد الدولي للاتصالات وإحصائيات عدد السكان الذين يستخدمون الإنترنت من أي جهاز –بما فيها الهواتف النقالة– إلى مايلي:

جدول يوضح عدد مستخدمي الإنترنت سنة 2016:

الدولة	عدد المستخدمين	النسبة المئوية بالنسبة للسكان	الدولة	عدد المستخدمين	النسبة المئوية بالنسبة للسكان
المملكة المتحدة	180.996.52	%85	فلسطين	997.561.1	%44.37
اليابان	316.063.102	%0.80	العراق	997.561.1	%25.37
أمريكا	822.542.243	%0.79	تونس	215.873.3	%0.36
الإمارات	963.880.3	%0.78	مصر	178.518.21	%74.26
البحرين	44.649	%0.55	ليبيا	6.049.04	%0.14
السعودية	28.550.10	%0.41	اليمن	247.549.2	%85.10
الكويت	763.972	%25.38			

وفيما يلي رسم بياني يوضح عدد مستخدمين الإنترنت بالدول الإفريقية سنة 2017.



وقد أظهرت البيانات السابقة أن عدد مستخدمي الإنترنت في العالم في تزايد مستمر، وبصفة خاصة الدول الإفريقية ويرجع ذلك إلى عدة أسباب أهمها الانتشار والتوسع في التعليم التكنولوجي وانتشار استخدام الحاسبات والهواتف الذكية واللوحات الرقمية المزودة بإمكانية الاتصال بشبكة الإنترنت والسماح لشركات الهاتف المحمول بالعمل كمزودين لخدمات الإنترنت، إضافة إلى الشغف في استخدام شبكات التواصل الاجتماعي.

وتعتبر دولة الجزائر من الدول التي قامت باقتناء تجهيزات وأنظمة معلوماتية متقدمة ومعقدة لحماية بنيتها التحتية الإلكترونية من جرائم التكنولوجيا الحديثة، ولكن لا تزال الفرق المختصة في الأمن المعلوماتي في مختلف القطاعات الأمنية تحصي الآلاف من هذا النوع من الجرائم، قد تنجح في فك شفرات بعضها وإحباطها قبل حدوثها وتفشل في صد الكثير منها، وسجلت نموا مستمرا في نسبة عدد مستخدمي الإنترنت، فسجلت برسم 2010 أكثر من 04 ملايين مستخدم لها، وكلما زاد عدد المستخدمين لها وتشعبت شبكة الإنترنت الوطنية كلما تطورت عصابات جرائم التكنولوجيا الحديثة فيها وأصبحت أكثر خطورة وتأثيرا على الفضاء الافتراضي.

وفي ظل الحديث المتزايد عن اعتماد نمط الحكومة الإلكترونية في إدارة الدولة، هذا ما يجعل كل البيانات الفردية للمواطنين وكذلك كل المعلومات المتعلقة بحياتهم ومعلوماتهم الخاصة في متناول هؤلاء المجرمين والقراصنة الإلكترونيين، إذ سجلت مصالح الدرك والشرطة الجزائريتين قرابة 2500 جريمة متصلة بالتكنولوجيا الحديثة خلال سنة 2017 بما فيها جرائم القرصنة والابتزاز والتحرش والتشهير الإلكتروني والاحتيال، وتشير أرقام المصالح الأمنية المكلفة بمكافحة الجرائم الإلكترونية إلى أن 80% من الجرائم المرتكبة تمت عن طريق موقع التواصل الاجتماعي فيسبوك، تعرض من خلالها عدد من الأشخاص إلى عمليات ابتزاز وتهديد بنشر صور أغلبها مفبركة وأخرى تتعلق بصور أو فيديوهات مخلة بالحياء أو وثائق ورسائل نصية.

وأضاف ذات المصدر أن حوالي 640 جريمة إلكترونية أغلبها جرائم ابتزاز لفتيات بصور حميمية التقطت لهن في لحظات عاطفية، وتضاف لهذه الأرقام حوالي 300 جريمة أخرى عالجها جهاز الدرك الوطني حسب ما صرح به رئيس مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية والحماية منها ومكافحتها التابعة للدرك الوطني.

وأكد مدير الشرطة القضائية، مراقب الشرطة عن المديرية العامة للأمن حسب ما نقل موقع هافيغنتون بوست عربي؛ أن نسبة الزيادة في الجريمة الإلكترونية في الجزائر فاقت 70% سنة 2015 بالمقارنة مع السنة التي قبلها، وحوالي 55% من الجرائم كانت تستهدف المجتمع والأسرة، وبحسب معلومات قدمها رئيس مصلحة الجريمة الإلكترونية بمديرية الشرطة القضائية في الجزائر العاصمة فقد تورط في غالبية الجرائم الإلكترونية المسجلة لعام 2018 حوالي 54 قاصرا في وقت أشارت تقارير جزائرية سابقة إلى أن شبكات توظف القصر للإيقاع بالضحايا باستعمال مختلف الأساليب، وكشف أمنيون مختصون إلى أن أكثر من 89% من الجرائم المرتكبة تمت عن طريق مواقع التواصل الاجتماعي فيسبوك وتويتر من خلال استعمال الابتزاز والتهديد بنشر الصور وأسرار شخصية أو التشهير وكشفت وكالة الأنباء الجزائرية على أن الجزائر عالجت أزيد من 11000 قضية تتعلق بالاستعمال السيئ للشبكة العنكبوتية (الإجرام السبراني) على المستوى الوطني منذ بداية شهر يناير من العام الجاري (2020)، حوالي 30% منها تتعلق بالابتزاز والتشهير حسبما أفاد به رئيس المصلحة المركزية لمكافحة الإجرام السبراني للدرك الوطني، إذ تم معالجة أزيد من 1140 قضية متعلقة بالجريمة الإلكترونية منها 136 قضية خاصة بالأطفال القصر.

البند الثالث: تقدير حجم الخسائر من جرائم التكنولوجيا الحديثة

يعاني حصر جرائم التكنولوجيا الحديثة بشكل كبير من مشكلة عدم الدقة، حيث يرتفع الفارق بين الحجم الحقيقي للجريمة وبين ما هو مسجل بالإحصائيات، وبالرغم من ذلك اهتمت بعض الكيانات المؤسسية سواء الحكومية أو الخاصة بمتابعة وحصر

عدد معتبر من جرائم التكنولوجيا الحديثة وأعداد الجرائم التي يتم ضبطها ودراسة نسبة الزيادة السريعة بأعداد الجريمة وحصر الخسائر الناجمة عنها، محاولة منهم لوضع الأطر والأساليب والمقترحات لمكافحة ومواجهة هذا النوع من الإجرام[1]، فقد زاد حجم الخسائر حول العالم، وهذا ما بينته دراسة ستانفورد الدولي (SRI) بالولايات المتحدة الأمريكية عام 1975 لحالات من جرائم التكنولوجيا الحديثة مؤكدة وغير مؤكدة أن معدل خسارة الجريمة الواحدة يبلغ 450 ألف دولار، وفي 1979 بلغت تقديرات المعهد لهذا المعدل حوالي 1685000 دولار.

كما أشارت شركة سيمانتك الأمريكية لحماية الشبكة الإلكترونية إلى أن المعدل السنوي للخسائر الناجمة عن جرائم التكنولوجيا الحديثة حول العالم قدر بحوالي 114 مليار دولار عام 2011 و أكثر من تريليون دولار أمريكي عام 2012 على أقل تقدير، وقد أصدرت الشركة تقريرا –يعد الأكبر من نوعه– بعنوان نورتون سايبر كرايم 2011 خلصت فيه إلى أن 431 مليون بالغ حول العالم كانوا ضحية للتهديدات الإلكترونية، بمعدل مليون ضحية يوميا و14 ضحية في الثانية.

كما صنف تقرير عام 2013 الخسائر إلى ستة تصنيفات، وهي خسائر الملكية الفكرية والجريمة الإلكترونية، وخسائر المعلومات المتعلقة بالعمل، وانقطاع الخدمة وتكاليف تأمين الشبكات ضد عمليات الاختراق، والضرر الذي يلحق بسمعة الشركة التي تتعرض للاختراق، وأن خسارة هذه الجرائم في الولايات المتحدة الأمريكية تقدر بين 24 و120 مليار دولار سنويا، وهو ما يقدر بنحو0.2% إلى 0.8% من الناتج المحلي الإجمالي، وفي هذا السياق أوضح المركز أنه من الصعب تقدير قيمة دقيقة من الخسائر السنوية الناتجة عن الهجمات الإلكترونية، لأن بعض الشركات لا تكشف عن تفاصيل خسائرها كما أن بعضها الآخر غير قادرة على تقدير الخسائر الناتجة عن الهجمات الإلكترونية التي تعرضت لها[2].

المطلب الثالث: خصائص جرائم التكنولوجيا الحديثة

تنبع خصائص أو سمات أية جريمة من خلال التعريف المعطى لها ومن خلال طبيعتها ووسيلة ارتكابها ونوعها، فالتعريف الذي أعطي لجريمة التكنولوجيا الحديثة أظهر أن هذه الجريمة جاءت نتيجة التطور التقني الذي شجع وساعد المجرمين وسهل عملهم وزاد من حجم جرائمهم من دون زيادة الجهد المبذول مع الجريمة التقليدية، وتتشابه جرائم التكنولوجيا الحديثة مع الجرائم التقليدية من حيث طرفي الجريمة (الجاني والمجني عليه)، فالجريمة هي سلوكيات إنسان غير مشروعة يسأل عنها ويتحمل العقاب لأجلها[3] وتختلف من حيث الأسلوب والوسيلة، ذلك بالإضافة إلى أنها جريمة بلا نهاية، فهي ذات حدود مفتوحة زمنيا ومكانيا صعبة الحصر والتعداد نظرا لازديادها وتنوع أساليبها مع ازدياد شبكة الإنترنت وازدياد التطور في الوسائل الإلكترونية والبرمجة، فالأسلوب أو الطريقة التي يتم من خلالها ارتكاب جرائم التكنولوجيا الحديثة يختلف تماما عن مجرى الجرائم التقليدية، إذ تميزت بوجود مميزات وخصائص تمتاز بها عن باقي الجرائم[4]، ويعتبر موضوع أو محل جرائم تكنولوجيا الحديثة أهم خاصية تتميز بها عن غيرها من الجرائم أين تكون

---

[1] هشام محمد فريد رستم، جرائم الفضاء الافتراضي، مجلة أكاديمية الشرطة، كلية الشرطة، دبي، 2013، ص93 و94.

[2] www.aleqt.com/2013/07/24/article-7727190.html

[3] محمود نجيب حسني، شرح قانون العقوبات، القسم العام، المرجع السابق، ص62.

[4] أكرم عبد الرزاق المشهداني، الجرائم التكنولوجية، دار الوفاق، بغداد، 2001، ص29.

المعلومات والبرامج محل الاعتداء، وهي عبارة عن نبضات إلكترونية، وعليه نكون أمام ظاهرة إجرامية مستحدثة ذات طبيعة خاصة.

فجرائم التكنولوجيا الحديثة إفراز ونتاج لتقنية المعلومات واتساع تطبيقها في المجتمع، مما أعطى لونا وطابعا قانونيا خاصا وميزها بمجموعة من الخصائص المختلفة عن الجرائم التقليدية لصعوبة إثباتها واكتشافها، وهذه الخصائص منها ما يتعلق بالشخص الذي يقدم على ارتكاب هذه الجريمة فميزته عن المجرم التقليدي، ومنها ما يتعلق بالجريمة في حد ذاتها لصعوبة اكتشافها واثباتها وهناك بعض الخصائص والسمات إذن تميز جرائم التكنولوجيا الحديثة عن غيرها من الجرائم التي سنحاول التطرق إليها على سبيل المثال وليس الحصر.

الفرع الأول: خصائص جرائم التكنولوجيا الحديثة من الناحية الوصفية

تتميز جرائم التكنولوجيا الحديثة من الناحية الشكلية بمجموعة من السمات والتي سيتم التطرق إليها فيما يتلو أدناه.

البند الأول: جريمة تنفذ عن بعد (عابرة للحدود)

أو كما يطلق عليها البعض جريمة ذات طبيعة متعدية للحدود[1]، ويمكن القول بعبارة أخرى أنها تخطت الحدود الجغرافية للدول، ويتطلب ذلك مهارة وذكاء من المجرم فيكفيه ارتكاب جريمته من خلال ضغطة زر من دون عناء أو مجهود، إذ يمكنه ارتكاب جريمة عن طريق وسيلة إلكترونية متصلة بشبكة الإنترنت موجودة في دولة معينة وتتحقق نتيجة هذا الفعل الإجرامي في دولة أخرى.

ويرجع ذلك إلى كون المجتمع المعلوماتي مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون جواز سفر أو مراقبة حرس حدود، وبالتالي لا تعترف بالحدود الجغرافية، فبعد ظهور الشبكات المعلوماتية لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، إذ تتمتع الحواسيب والأجهزة الإلكترونية في نقل كميات من المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الأميال، هذه الطبيعة تتميز بها جرائم التكنولوجيا الحديثة كونها جريمة عابرة للحدود، خلقت العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب تطبيقه[2]، بالإضافة إلى إشكاليات تتعلق بالملاحقة القضائية وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام[3]، فهي تربط بين دول لا تحدها حدود الطبيعة أو حدود السياسة، وتسمح لمستخدميها بالتنقل المعنوي أو الافتراضي بين الدول والقارات بدون تعقيدات أو صعوبات أو عوائق، فهي عالم ضخم متنوع متجدد خال من الحدود.

---

[1] محمد عبد الرحيم سلطان العلماء، جرائم الإنترنت والاحتساب عليها، المجلة العربية للدراسات الأمنية والتدريب، العدد 36، السنة 18، جامعة نايف العربية للعلوم الأمنية، الرياض، أكتوبر 2003، ص52.

[2] عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، الرياض، 2007.

[3] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، ط2، 2010، ص37.

والسبب يعود إلى تعدد الأماكن التي يمكن من خلالها ارتكاب الجريمة والتي يمكن أن تكون بين أكثر من دولة، هذا بالإضافة إلى خضوع القانون الجنائي لقاعدة هامة وهي إقليمية القانون الجنائي[1]، ومن حيث الزمان فإن التوقيت الزمني يختلف بين الدول أيضا[2].

وبالرجوع إلى الدور البالغ الأهمية الذي لعبه الحاسب الآلي ومختلف الأجهزة الإلكترونية الحديثة في العالم المعاصر، فقد أقدمت الدول المتقدمة صناعيا على إنتاج هذه الأجهزة وابتكار البرامج والمصنفات لتحقيق الربح المادي، لذا انتشرت هذه الأجهزة في أرجاء العالم ولهذا اتصفت برامج هذه الأخيرة بالعالمية، هذا من جانب، ومن جانب آخر نلاحظ أن شبكة الإنترنت قد ألغت أي حدود جغرافية بين الدول جاعلة من العالم قرية صغيرة[3].

وبالتالي يمكن لمرتكب الجريمة الذي يوجد في دولة ما من العالم ارتكاب جريمة بواسطة جهاز إلكتروني أو حاسب آلي دون أن يبرح مكانه[4]، بل وأكثر من ذلك يمكن ارتكاب الجريمة في قارة وأضرار هذه الجريمة في قارة أخرى، ولذلك فإن هذا النوع من الإجرام هو صورة صادقة من صور العولمة لإمكانية ارتكابها عن بعد.

هذا وقد لا يقتصر الضرر المترتب عن الجريمة على المجني عليه وحده، وإنما قد يتعداه إلى متضررين آخرين في دول عدة فتتعدد جنسياتهم وهذا ما يمكن ملاحظته من خلال نشر المواد ذات الخطر الديني، أو الأخلاقي أو الأمني أو السياسي أو التربوي أو الثقافي أو الاقتصادي، لذلك فإنه يجب إيجاد تعاون دولي لمكافحة هذه الجرائم عن طريق المعاهدات والاتفاقيات الدولية...إلخ[5].

ومثال على ذلك الاعتداء على City Bank في نيويورك من طرف Vladimir Levin وأعضاء من المافيا في روسيا، وقد خلق ذلك مشكلة كبيرة بالنسبة لمكتب التحقيقات الفدرالي، لأن المحققين كان عليهم فحص نظم البنوك في سبع دول مختلفة، وبناء عليه تم تنفيذ الايداع الإلكتروني للنقود، وكان تطبيق أوامر التفتيش والتتبع الزمني لهذا الحدث تحديا بالنسبة لمعظم المحققين المهرة وقد تم القبض على Levin وحكم عليه بالسجن 03 سنوات وإلزامه بدفع 240 ألف دولار لـ CityBank[6].

ومن القضايا التي لفتت النظر إلى البعد الدولي لجرائم تكنولوجيا المعلومات الحديثة، قضية عرفت باسم مرض نقص المناعة المكتسبة (الإيدز) عام 1989، وتتلخص وقائعها في قيام أحد الأشخاص بتوزيع عدد كبير من النسخة الخاصة بأحد البرامج الذي هدف في ظاهره إلى إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة، إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس حصان طروادة إذ كان يترتب على فتح البرنامج تعطيل جهاز الحاسوب وإعادة تشغيله فتظهر بعد ذلك عبارة على الشاشة

---

[1] محمود نجيب حسني، دروس في القانون الجنائي الدولي، دار النهضة العربية، القاهرة، 1960، ص72 و73.

[2] زينب أحمد عوين بديوي الشمري، عدم كفاية قواعد القانون الجنائي في مكافحة الجريمة المعلوماتية، مجلة كلية الحقوق، العدد 01، المجلد 13، جامعة النهرين، بغداد، 2011، ص05 و06.

[3] Rein Turn, Willis Howard Ware, Privacy and Security in Computer Systems, RAND Corporation, California, United States, 1975, p05.

[4] عبد الله عبد الكريم، جرائم المعلوماتية والإنترنت، الجرائم الإلكترونية، دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والإنترنت مع الاشارة إلى جهود مكافحتها محليا وعربيا ودوليا، منشورات الحلبي الحقوقية، بيروت، ط1، 2007، ص33.

[5] محمد عبيد الكعبي، المرجع السابق، ص37.

[6] Thomas A. Johnson, Forensic Computer Crime Investigation, CRC Press, Florida, United States, 2005, p05.

يقوم الفاعل من خلالها بطلب مبلغ مالي يرسل على عنوان معين حتى يتمكن المجني عليه من الحصول على مضاد للفيروس.

وفي الثالث من فبراير عام 1990 تم إلقاء القبض على المتهم بإنشاء وتوزيع هذا البرنامج المدعو جوزيف بوب في أوهايو بالولايات المتحدة الأمريكية وتقدمت المملكة المتحدة بطلب تسليمه لها ومحاكمته أمام القضاء الإنجليزي، وذلك أن إرسال هذا البرنامج قد تم من داخل المملكة المتحدة.

وبالفعل وافق القضاء الأمريكي على تسليم المتهم، وتم توجيه إحدى عشرة تهمة ابتزاز إليه وقعت معظمها في دول مختلفة، إلا أن إجراءات محاكمة المتهم لم تستمر بسبب حالته العقلية، ومهما كان الأمر فإن هذه القضية تعتبر المرة الأولى التي يقدم فيها شخص للمحاكمة بتهمة إعداد برنامج خبيث[1].

البند الثاني: خفاء (استتار) الجريمة

تتسم جرائم التكنولوجيا الحديثة بأنها خفية ومستترة في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، كما أن الجاني يتمتع بقدرات فنية تمكنه من اقتراف جريمته بدقة[2]، فجرائم التكنولوجيا الحديثة في أغلب صورها خفية لا يلاحظها المجني عليه ولا يدري حتى بوقوعها، والإمعان في حجب السلوك المكون له وإخفائه عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية التي تسجل البيانات عن طريقها في الكثير من الأحوال بحكم توافر المعرفة والخبرة في مجال الحاسبات غالبا لدى مرتكبيها[3].

حيث يستفيد المجرمون في مختلف الشبكات من تبادل الأفكار والمعارف والخبرات الإجرامية فيما بينهم، ويظهر لنا جليا في مختلف المواقع والمنتديات التي تضمن لهم الاتصال والتواصل فيما بينهم من أجل ارتكابهم لجرائمهم بعيدا عن أعين الأمن[4]، وتجدر الإشارة في هذا الصدد أن جرائم تكنولوجيا المعلومات الحديثة أسرع تطورا من التشريعات وذلك راجع إلى التطور التكنولوجي الهائل والمتسارع الذي تجسده شبكة الإنترنت.

البند الثالث: جريمة بلا عنف وبلا مقاومة

إن التطور التقني المتزايد يوما بعد يوم، وتأقلم الجاني مع استخدام هذه الوسائل ذات الطابع التقني أدى إلى سهولة ارتكاب جرائم التكنولوجيا الحديثة، أدى أيضا إلى سهولة تبادل الخبرات والأفكار بين الجناة حول العالم، وإلى سهولة ومرونة التخطيط والتنفيذ، فباعتبارها جريمة أقل عنفا في التنفيذ (اختلاف أسلوب ارتكاب جرائم التكنولوجيا الحديثة عن تلك التقليدية)، فإنها لا تتطلب بذل مجهود كبير، فهي تنفذ بأقل جهد ممكن مقارنة بالجرائم التقليدية، التي تتطلب نوعا من المجهود العضلي الذي قد يكون

---

[1] Bryan Clough and Paul Mungo, Approaching Zero: Data Crime and the Computer Underworld, Faber & Faber, London, United Kingdom, 1992, p136.

[2] محمد عبيد الكعبي، المرجع السابق، ص32.

[3] محمد عبيد الكعبي، المرجع نفسه، ص34.

[4] أيمن عبد الحفيظ عبد الحميد سليمان، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، مطابع الشرطة، مصر، 2005، ص26.

في صورة ممارسة العنف والإيذاء، كما هو الحال في جرائم السرقة مثلا، القتل أو الاختطاف، أو في صورة الخلع أو الكسر أو تقليد المفاتيح...إلخ[1].

إن جرائم التكنولوجيا الحديثة هي جرائم هادئة بطبيعتها لا تحتاج إلى العنف، بل كل ما تحتاج إليه القدرة على التعامل مع الوسائل الإلكترونية بمستوى تقني يوظف ارتكاب الأفعال غير المشروعة، وتحتاج كذلك إلى وجود شبكة المعلومات الدولية الإنترنت مع مجرم متمرس وخبير يرتكب هذه الجرائم دون سفك الدماء، وأحيانا تتم هذه الجرائم بتعاون أكثر من شخص فهو لابد من أن يكون الشخص الذي يرتكب هذه الأنواع من الجرائم إنسانا محترفا[2] يتمتع بقدر كبير من الذكاء، وهذه الخصوصية تميزه عن غيره من المجرمين التقليديين فالجاني إنسان عملي اجتماعي يمارس عمله في المجال المعلوماتي أو غيره من المجالات الأخرى يدخل شبكة الإنترنت بضغطة زر ويبدأ في اصطياد ضحاياه كمن يتلقى رسالة بريد إلكترونية تحمل في طياتها فيروس يفتك بالحاسب الآلي بمجرد الإطلاع عليها وما تؤديه من إتلاف للمعلومات والبرامج وسرقة الشيفرات والأرقام السرية لبطاقات الائتمان[3]، وبما أن الإنسان هو من يخترع ويكتشف فهو قادر على حماية نفسه بالعديد من الطرق، كالامتناع عن تشغيل أي مرفق برسالة إلكترونية إلا بعد الفحص والتأكد من خلوه من الفيروسات، وعليه يمكن الذهاب إلى القول إن الإجرام التكنولوجي الحديث هو إجرام الأذكياء بالمقارنة مع الإجرام التقليدي الذي يميل إلى العنف[4].

البند الرابع: صعوبات اكتشاف جرائم التكنولوجيا الحديثة

إن عدد الحالات التي اكتشفت فيها جرائم التكنولوجيا الحديثة هي حالات قليلة جدا إذا ما قورنت بالجرائم التقليدية وتتميز بصعوبة اكتشافها واذا اكتشفت فغالبا ما تكون بمحض الصدفة، وتعود أسباب صعوبة اكتشافها إلى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مادية، كقطرات الدم أو الزجاج المكسور مثلا كما في الجرائم التقليدية، كما وأن الجاني يمكن أن يتواجد في مكان بعيد نسبيا أو في دولة أخرى، بالإضافة إلى عدم ملاحظة المجني عليه هذه الجرائم أو عدم درايته حتى بوقوعها أحيانا، كما يؤثر إحجام المجني عليه عن الإبلاغ عن وقوعها في بعض الأحيان على صعوبة اكتشافها خاصة في تلك الجرائم التي تمس المؤسسات المالية والتجارية والبنوك حرصا من إدارة تلك المؤسسات، وخوفا منهم على سمعة مؤسساتهم ورغبة فيها في عدم زعزعة ثقة العملاء بها[5]، كما أن قدرة الجاني على إتلاف وتدمير أثر الإدانة في أقل من الثانية الواحدة الذي يطلق على هذا المصطلح الآثار أو الأدلة

---

[1] دياب موسى البدانية، دور الأجهزة الأمنية في مكافحة جرائم الإرهاب المعلوماتي، الدورة التدريبية المنعقدة بكلية التدريب، القنيطرة، المملكة المغربية 09 إلى 13 أفريل 2006.

[2] نهلا عبد القادر المومني، المرجع السابق، ص51.

[3] Michael Kunz, Patrick Wilson, Computer crime and computer fraud, Report Submitted to the Montgomery County Criminal Justice Coordinating Commission, State of Maryland, United States, 2004, pp12-13.

[4] محمد سامي الشوا، المرجع السابق، ص34.

[5] حسين بن سعيد بن سيف الغافري، مؤتمر الجوانب القانونية للمعلوماتية بين النظرية والتطبيق، كلية الحقوق، جامعة السلطان قابوس، مسقط، 13 و14 مارس 2011.

المعلوماتية الرقمية والتي تتيح للسلطة المختصة في حال وجود هذه الآثار رؤية أو كشف ملابسات الجريمة، إذ تغلب الصفة الإلكترونية على الدليل المتوفر التي تصعب من اكتشاف الجريمة هنا[1].

كما يدخل هناك سبب آخر يشارك في إبراز صعوبة إثبات جرائم التكنولوجيا الحديثة ويتمثل أساسا في غياب الدليل الرقمي، والذي يمكن فهمه بالقراءة، فأغلب البيانات تكون على شكل رموز مما لا يمكن للإنسان قراءتها وهذا ما يصعب الكشف عنها أو التعرف على مرتكبيها وذلك بسبب غياب الدليل[2].

فكل هذه الأسباب تدفع بالمجني عليه في جرائم التكنولوجيا الحديثة إلى الامتناع عن مساعدة السلطات المختصة في الكشف عن الجريمة، وحتى في حالة الإبلاغ فإن المجني عليه لا يتعاون مع جهات التحقيق خوفا مما يترتب عليه من دعاية مضرة وضياع ثقة المساهمين، فعادة ما يكون المجني عليه بنكا أو مؤسسة مالية أو مشروعا صناعيا ضخما يهمه المحافظة على ثقة عملائه وزبائنه، فيكون اهتمامهم منصبا كذلك حول عدم اهتزاز سمعته أكثر من اهتمامه بالكشف عن الجريمة ومرتكبيها، وعليه يفضل المجني عليه إرضاء عميله وينهي الأمر داخليا حتى لا يفقده.

البند الخامس: الآثار غير المرئية للجريمة

نظرا للطابع التقني للجريمة المتصلة بالتكنولوجيا الحديثة، وقدرة المجرم على الاستفادة من شبكة الاتصال عن بعد لتنفيذ جريمته فإن ارتكاب هذه الجريمة لا يتعد ثوان، ولا يترك وراءه أي أثر[3]، بالتالي عدم وجود أي أثر يمكن تتبعه لاقتفاء أثر الجاني واكتشاف الجريمة وإثباتها، وذلك لأن بيئة هذه الجرائم تكون عبارة عن البيانات والمعلومات التي تكون على شكل نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي، فيما يجعل محو الدليل وإتلافه أمرا سهلا للغاية[4].

فقد تمكن المواطن الأمريكي ستانلي مارك الذي يعمل أخصائيا للحسابات في بنك الباسيفيك الوطني من اكتشاف شفرة تحويل حسابات العملاء من البنك وغيره من البنوك التي تتعامل معه، فقام بإصدار أوامر إلكترونية لعدة فروع للبنك لتحويل مبالغ مالية لحسابه، ومرت شهور دون أن يكتشف أحد حقيقة ما حدث لولا أن المتهم نفسه قد اعترف بالواقعة وهو مخمور[5].

البند السادس: جريمة لا تتطلب اتصالا ماديا بين المجرمين والضحايا

هذه السمة لجرائم التكنولوجيا الحديثة تظهر غالبا من خلال جرائم المضايقة والملاحقة، والتي عادة ما تتم باستخدام البريد الإلكتروني أو مواقع الدردشة الآنية المختلفة، وذلك من خلال إرسال الجاني لرسائل تهديد أو مضايقة والاستفادة من القدرة على

---

[1] حسين بن سعيد بن سيف الغافري، مؤتمر الجوانب القانونية للمعلوماتية بين النظرية والتطبيق، المرجع السابق.

[2] خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط1، 2009، ص79.

[3] محمد علي العريان، المرجع السابق، ص53 و54.

[4] محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر والتوزيع، الأردن، 2010، ص166.

[5] محمد الشناوي، جرائم النصب المستحدثة، تقديم مأمون سلامة، دار الكتب القانونية، مصر، ط1، 2008، ص88.

إخفاء الهوية ومحو الآثار والأدلة التي ترشد إليه[1]، إذ أن لديه القدرة على تزويد الحاسب ببرامج متخصصة تستطيع إتلاف الدليل الرقمي وتدميره في زمن قياسي تعمل بأمره أو عند استخدامه من طرف أي شخص غيره[2] مما يخلف آثارا سلبية في نفسية الضحية.

الفرع الثاني: خصائص جرائم التكنولوجيا الحديثة من الناحية الإجرائية

بالإضافة إلى خصائص جرائم التكنولوجيا الحديثة من الناحية الشكلية يمكن الحديث عن خصائص أخرى تتعلق أساسا بخصائص من الناحية الإجرائية.

البند الأول: صعوبة الوصول إلى الدليل الرقمي

إن هذا النوع من الجرائم يتم في بيئة غير تقليدية، إذ أنها تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الوسائل الإلكترونية والإنترنت، مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن، ففي هكذا جرائم يتم الفعل الإجرامي دون علم المجني عليه كأن يتم إدخال فيروس إلى الجهاز عن طريق الاتصال بشبكة الإنترنت، ويظل الفيروس كامنا حتى لحظة معينة ثم يقوم بالنشاط وتدمير البرامج والمعلومات، فهذا المجني عليه لا يدري بالوقت الذي تم فيه إصابة جهازه بالفيروس، كما أن هذا الأخير يمكن أن يدمر نفسه في النهاية حتى لا يعرف نوعه، مما يجعل طمس الدليل ومحوه كليا من قبل الفاعل أمرا في غاية السهولة، فلا يوجد هنالك مسرحا للجريمة، أو بتعبير آخر يتضاءل دور مسرح الجريمة في الإفصاح عن الحقائق المؤدية للأدلة المطلوبة، وذلك لأن جرائم الإنترنت لا تخلق آثارا مادية، كما أن هناك فترة زمنية بين اكتشاف الجريمة ووقت ارتكابها، مما يمنح الوقت الكافي للجاني أو للأشخاص أن يتلفوا أو يعبثوا بالآثار المادية إن وجدت، فيمكن تدمير المعلومات التي يتم استخدامها كدليل في الإثبات في ثوان قليلة، كما قد يستخدم الجاني اسما مستعارا، أو يرتكب فعله من خلال إحدى مقاهي الإنترنت، كما أن لنقص الخبرة دورا في صعوبة الوصول إلى الدليل الرقمي في جرائم التكنولوجيا الحديثة من قبل المحققين[3].

هذا وأن الإلمام بالمعرفة التقنية للحاسب الآلي والأجهزة الإلكترونية الذكية غالبا ما يتيح للجاني طرقا يعيق بها عمل الشرطة أو السلطة المنوطة بالتحري للوصول إلى الدليل، ويتم ذلك عن طريق اتخاذ تدابير فنية واقية تزيد من صعوبة عملية التفتيش، مثل إضافة كلمة السر، أو دس تعليمات خفية بينها لتصبح كالرمز أو تشفير البيانات مما يستلزم الاستعانة بخبرة فنية عالية المستوى[4]. ولعل صعوبة إثبات هذا النوع من الجرائم تعود إلى صعوبة الاحتفاظ الفني لآثارها إن وجدت الحرفية الفنية العالية التي تتطلبها من أجل الكشف عنها وهذا ما يعرقل عمل المحقق الذي تعود على الجرائم التقليدية، واعتماد الخداع والمكر في ارتكابها والتضليل في التعرف على مرتكبيها، فهؤلاء يعتمدون على التخفي عبر دروب الإنترنت تحت قناع فني، كما يلعب البعد الزمني (اختلاف المواقيت

---

[1] John Arquilla, David Ronfeldt, Cyber crime Inquiry, Submissions - Australian Banking Association, 2007, p16.

[2] محمد عبد الرحيم سلطان العلماء، المرجع السابق، ص30.

[3] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص13. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، المرجع السابق، ص40.

[4] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص14 وما بعدها.

بين الدول) والمكاني (إمكانية تنفيذ الجريمة عن بعد)، دورا مهما في تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم[1].

فباعتبار جرائم التكنولوجيا الحديثة تقع في بيئة افتراضية، إذن؛ فإنها لا تترك أية آثار مادية محسوسة خلافا للجرائم التقليدية، فهذه الأخيرة يمكن إدراكها بالحواس كما هو الحال في المستندات المزورة والنقود والطوابع المزيفة، والأسلحة النارية، وما يمكن أن يخلفه الجناة من آثار مادية أخرى في مسرح الجريمة كالشعر والدماء وبصمات الأصابع وآثار الأقدام وما إلى ذلك، أما في جرائم التكنولوجيا الحديثة فمن السهل جدا التخلص من الأدلة الرقمية ومحوها، إذ يتم عادة في لمح البصر، وبمجرد لمسة خاطفة[2] فهي إذن جرائم غير مادية لا تترك آثارا خارجية أو مادية تدل عليها[3]، إنما يتمثل مظهر جرائم التكنولوجيا الحديثة في محو أو تغيير البيانات أو الأرقام أو إتلاف البرامج الموجودة بأنظمة الوسائل الإلكترونية[4].

كما أن قدرة الجاني على تدمير كل ما يعتبره دليلا ضده الذي يتم في أقل من ثانية[5] يصعب على السلطات المختصة من الوصول إلى الدليل، وبالتالي تنصله من مسؤولية هذا الفعل وإرجاعها إلى خطأ في نظام الحاسب الآلي أو الشبكة أو في الأجهزة وبالتالي فلجوء الجاني إلى ارتكاب تلك الجريمة الحديثة يدل على ثقته بنفسه وخبراته وعلمه وقناعاته بأنه من الصعب الوصول إليه ولذلك فإن سلطات التحقيق دائما تلجأ إلى الخبراء في هذا المجال في بدايات التحقيق، مثال ذلك؛ شهدت النمسا حالة استطاع فيها الخبراء إحباط مسعى الجاني لتدمير الأدلة على إدانته بطريقة آلية متطورة بعد قيام أحد مهربي الأسلحة بإدخال تعديلات على الأوامر العادية لنظام تشغيل حاسب صغير يستخدمه في تخزين عناوين عملائه والمتعاملين معه، بحيث يترتب على إدخال أمر إلى الحاسب من خلال لوحة مفاتيحه بالنسخ أو الطبع؛ محو وتدمير كافة البيانات ومع أن تعديل برمجة نظام تشغيل الحاسب الآلي كان قد أجري خصيصا من قبل الجاني للحيلولة دون نجاح أجهزة الملاحقة في الإجراءات المتوقعة للبحث عن الأدلة وضبطها، إلا أنه لم يفلح في تحقيق هذا الهدف نتيجة خبرة الخبراء والمختصين في معالجة البيانات بالجهاز المركزي لمكافحة الغش المعلوماتي بالنمسا بأن شيئا ما في نظام تشغيل حاسب الفاعل قد جرى تغييره، وقيامهم بناء على ذلك باستنساخ الأقراص الممغنطة[6].

هذا وأن البحث في ملفات الحاسب الآلي التي تقابله صعوبة غير عادية لاستطاعة الجاني تحريك الملفات من جهاز حاسب إلى آخر خلال واحد على الألف من الثانية واخفاؤها في مساحة ضئيلة جدا على ذلك الحاسب، أو يتم تخزينها في سيرفر يقع في دولة ذات اختصاص قانوني مختلف في تجريم جرائم التكنولوجيا الحديثة[7].

---

[1] نبيلة هبة هروال، المرجع السابق، ص40.

[2] جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002، ص113 وما بعدها.

[3] محمد الشنبري، التحقيق في جرائم الحاسب الآلي، دراسة قانونية ضمن أعمال مؤتمر القانون، الكمبيوتر والإنترنت، كلية الشريعة والإنترنت، جامعة الإمارات، الإمارات العربية المتحدة، مايو 2005.

[4] هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، المرجع السابق، ص41.

[5] فهد بن سيف بن راشد الحوسني، جرائم التجارة الإلكترونية ووسائل مواجهتها مع التطبيق على سلطنة عمان، أطروحة دكتوراه، كلية الدراسات العليا أكاديمية الشرطة، القاهرة، 2007، ص337.

[6] هشام محمد فريد رستم، جرائم الفضاء الافتراضي، المرجع السابق، ص93 و94.

[7] Thomas A. Johnson, Op.Cit., p05.

البند الثاني: صعوبة المعاينة والتفتيش وعدم الإبلاغ عن هذه الجرائم

التفتيش وما في حكمه في نطاق هذه البيئة ينظر إليه في كثير من الأحيان على أنه غير مجد لما يكتنفه من صعوبات أثناء تنفيذه، وبالذات عندما يتم في الفضاء الافتراضي (في بيئة الإنترنت) مقارنة بالجرائم التقليدية، وفيما يخص محل التفتيش وما في حكمه في البيئة المعلوماتية، فهو قد يرد على المكونات المادية للحاسب الآلي وملحقاته أو الأجهزة الإلكترونية، وهناك خلاف يذكر حول خضوعها للتفتيش والضبط طبقا لقواعد قانون الإجراءات الجزائية بما في ذلك البيانات المخزنة في أوعية أو وسائل مادية كالأشرطة الممغنطة والأقراص الصلبة والضوئية، وذلك تبعا للمكان أو الحيز الموجود فيه[1]، فيرد التفتيش على الجانب المنطقي للحاسوب، المتمثل في المعلومات والبيانات المعالجة إلكترونيا، وهي محل جدل كبير حول صلاحياتها لأن تكون موضوعا للتفتيش والضبط من عدمها.

البند الثالث: نقص الخبرة الفنية لدى المحققين

يشكل نقص الخبرات الفنية لدى المحققين عائقا أمام إثبات هذه الجرائم، وذلك لأن هذا النوع من الجرائم يتطلب خبرة فنية عالية وإلماما واسعا باستخدام الحاسوب، ونتيجة لهذا النقص في الخبرة فإن جهات التحقيق لا تبذل جهودا كبيرة لكشف هذه الجرائم وإثباتها على الجاني، فضلا عن هذا، فإن المحقق نفسه أحيانا يكون سببا في محو وإزالة الدليل، وذلك بسبب سوء تعامله مع تلك الأدلة بسبب نقص خبرته ومعرفته الفنية والتي تمكنه من استخراج الدليل بشكل سليم[2].

ولتفادي هذا النقص في الخبرة الفنية لا بد من ضرورة تخصيص وحدات أمنية متخصصة لديها الإلمام الكافي بمبادئ وتقنية الحاسب الآلي والأجهزة الإلكترونية وكيفية التعامل معها رصدا لحركة الهواة والمواقع المشبوهة والإباحية، الوجود في الدورات التدريبية التي تنظمها المعاهد الخاصة والشركات في مجال الحاسب الآلي لخلق علاقات طيبة مع المدربين والمتدربين في هذا المجال، ومتابعة المسجلين في جرائم التزوير والاحتيال، بالإضافة إلى ضرورة التواجد المستمر في مراكز الاتصالات المحلية والدولية لتفعيل الدور الوقائي في منع جرائم التكنولوجيا الحديثة وضرورة توفير المعلومات الأولية عن هذه الجرائم قبل وقوعها.

الفرع الثالث: بعض الخصائص الأخرى لجرائم التكنولوجيا الحديثة

بالإضافة إلى خصائص الجريمة من الناحية الوصفية الشكلية ومن الناحية الإجرائية، تتميز جرائم التكنولوجيا الحديثة بصفة عامة عن الجريمة التقليدية من عدة نواح، سواء كان هذا التميز في السمات العامة لها، أو بالنسبة للباعث على تنفيذها أو هدفها أو من حيث الوسيلة المستعملة في ارتكابها...إلخ.

أولا: وسيلة ارتكاب الجريمة، مع انتشار الإنترنت وتطور تكنولوجيا المعلومات، أصبح من الطبيعي أن يساء استخدام

---

[1] أسامة أحمد المناعسة وآخرون، جرائم الحاسب الآلي والإنترنت، دراسة تحليلية مقارنة، المرجع السابق، ص276 وما بعدها.

[2] ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2006، ص93 وما بعدها.

هذه الوسائل وارتكاب الجرائم، ويبدو ذلك جليا من خلال جرائم النصب والاحتيال التي يتعرض لها الأفراد والمؤسسات ويعد ذلك دليلا قويا لقدرة مرتكبها على الاختفاء، وعدم ترك أدلة تدينه بعد ارتكابها، وعليه يمكن القول إن العلاقة الوطيدة بين الجريمة ووسائل التكنولوجيا الحديثة نتج عنها ميلاد نوع مستحدث من الجرائم اصطلح على تسميته جرائم التكنولوجيا الحديثة –الموضوع محل الدراسة– كما أعطتها مجموعة من الخصائص والسمات المميزة عن الجرائم التقليدية، ومن هذه الخصائص ارتكاب جرائم التكنولوجيا الحديثة بواسطة الحاسوب، الأجهزة الإلكترونية الذكية والإنترنت...إلخ[1].

وما يميز جرائم التكنولوجيا الحديثة عن غيرها من الجرائم أنها تتم عن طريق مجموعة من الوسائل الإلكترونية كالحاسوب والأجهزة الذكية التي تتصل فيما بينها عبر شبكة المعلومات[2]، وتثور المشكلة –كما ذكرنا سالفا– عندما يطال الاعتداء على فن هذه الوسائل الإلكترونية، أي البيانات والبرامج المخزنة فيها وبالتالي فإن ارتكاب هذه الجريمة يكون في بيئة معلوماتية قوامها النظم المعلوماتية، إذ يتعين وجود كم هائل من المعلومات والبرامج والملفات المخزنة، والتي يتوجب فحصها ولها ارتباط بالجريمة، وفي بعض الأحيان يكون تتبع المعلومات داخل الجهاز كدليل تسعى الجهات الأمنية لملاحقته أمرا يتميز بالكثير من الصعوبات، تتمثل إما في طبيعة المعلومات أو في نقص الخبرة الفنية من قبل رجال الأمن في ملاحقتهم لتلك الأدلة التي يتطلب معها البحث استغراق فترة زمنية طويلة تؤثر بالسلب على طبيعة عمل المنشأة.

إذ تعد شبكات الإنترنت حلقة الوصل بين كافة الأهداف المشتركة لتلك الجرائم كالبنوك والشركات الصناعية وغيرها من الأهداف التي غالبا ما تكون الضحية لتلك الجرائم، وهو ما دعى معظم تلك الأهداف إلى نظم الأمان الإلكترونية في محاولة منها لحماية نفسها من تلك الجرائم أو على الأقل لتحد من خسائرها عند وقوعها ضحية لها.

ثانيا: الضحايا هم أشخاص طبيعية أو معنوية، من المتصور أن يقع ضحية لهذه الجرائم كل الأشخاص طالما كانوا يستعملون نظم الحاسوب في أنشطتهم الاقتصادية والاجتماعية وحتى السياسية؛ طبيعيين كانوا أو معنويين.

ثالثا: الإحجام عن جرائم التكنولوجيا الحديثة، الإبلاغ عن الجرائم هو فاتحة الإجراءات الجنائية، وهو الخطوة الأولى في تحركات الجهات المختصة للتعامل مع جرائم التكنولوجيا الحديثة بمختلف أشكالها لضبط مرتكبيها وتقديمهم للعدالة، فالبلاغ الجنائي هو إخطار السلطات المختصة عن وقوع الجريمة أو أنه توافرت دلائل وقرائن تفيد أنها على وشك الوقوع، ويختص عادة بتلقي البلاغات مأمور الضبط القضائي ومن بينهم العاملون بأجهزة الشرطة ومصالح الدرك الوطني[3].

وتجدر الإشارة إلى وجود عدد من المشكلات التي تتعلق بعزوف المجني عليهم في الجرائم المتعلقة بالتكنولوجيا الحديثة عن الإبلاغ عنها للجهات المختصة والتي ترجع أساسا إلى إحجام معظم الشركات والمؤسسات عن الإبلاغ عن الجرائم خوفا على سمعتها وكيانها والخوف من استغراق التحقيق والإثبات وقتا طويلا، مع احتمالية احتفاظ جهات التحقيق بالوسائل الإلكترونية مما يؤثر على

---

[1] سيتم التطرق لوسائل ارتكاب جرائم التكنولوجيا الحديثة في المبحث الثاني من الفصل الأول من الباب الأول في هذه الدراسة بالتفصيل.

[2] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2009، ص93.

[3] سعد أحمد محمود سلامة، التبليغ عن الجرائم، دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة الزقازيق، القاهرة، 2003، ص30.

حسن سير العمل بتلك الشركات والمؤسسات[1]، وقد يحدث الإحجام عن الإبلاغ عن جرائم التكنولوجيا الحديثة بسبب عدم إدراك المسؤولين عن الأنظمة الحاسوبية المعلوماتية بأن هذه الأفعال والهجمات معاقب عليها بموجب التشريعات والقوانين.

كما قد يكون الإحجام نتيجة جهل المجني عليهم كيفية التبليغ عن الجريمة[2]، أو إعتقاد بعض المجني عليهم بعدم قدرة الجهاز الأمني على التوصل للجناة في جرائم التكنولوجيا الحديثة، أو الخوف من الإساءة للسمعة والفضيحة، خاصة في تلك الجرائم المتعلقة بالجرائم الإباحية والتشهير بالسيدات أو في حالة الاعتداء الجنسي على الأطفال وعرض صور إباحية على مواقع الإنترنت فهناك من الأفراد من يخشون تحديد أنفسهم كضحية –خاصة النساء منهم– خوفا من النظر إليهم بوصمة العار بعد الإيذاء النفسي أو الجسدي الواقع عليهم[3]، أو خوف الموظف من الحرمان من خدمات عندما يتعرض لجريمة تكنولوجية حديثة ناتجة عن الاختراق أو زيارته لمواقع غير مسموح بزيارتها[4]، ولتفادي عدم الإبلاغ على هذا النوع من الجرائم[5] وجب مداومة الإعلان بوسائل الإعلام المختلفة عن أماكن تلك البلاغات في جرائم التكنولوجيا الحديثة، والتأكيد على خطورة عدم التبليغ عن هذه الجرائم.

رابعا: توافر العلم بالتقنية للجاني، تتميز جرائم التكنولوجيا الحديثة عن غيرها من الجرائم التقليدية الأخرى بتميز صفات مرتكبيها، فلا يمكن أن ترتكب هذه الجرائم إلا من طرف من لهم مهارة ومعرفة فنية في مجال الحاسب الآلي والأجهزة الإلكترونية الحديثة وكيفية تشغيلها وعملها، كما يمكن أن يرتكبها شخص ليس لديه مؤهل علمي إنما لديه ما يكفي من الإطلاع لارتكابها كأن يكون شخص يأخذ من التعامل مع الوسائل الإلكترونية هواية يمارسها[6] فتتناسب هذه الجريمة مع المعرفة التقنية تناسبا طرديا ويساهم في تعدد جنسيات الأشخاص والمنظمات المرتبطين بها، بل ويتزايد عدد الأشخاص المشتركين والمتضررين منها بشكل كبير كلما توافر العلم بوسائل التقنية الحديثة[7].

خامسا: صعوبة تحديد المسؤولية الجنائية، يظهر ذلك في حالة الجريمة على شبكة الإنترنت، كأن يدخل المستخدم على الموقع، فيجد به صورا إباحية مثلا، فهل يسأل عن هذه الجريمة عامل الاتصال أم المورد أم غيرهم من العاملين في مجال الإنترنت.

سادسا: الهدف من جرائم التكنولوجيا الحديثة، من المعروف أن معظم الجرائم المتصلة بالتكنولوجيا الحديثة يكون من ضمن أهدافها الأساسية الحصول على المعلومات الإلكترونية، التي تكون إما محفوظة على مختلف الأجهزة الإلكترونية أو أجهزة الحاسب

---

[1] وليد سمير فهيم المعداوى، دور الشرطة في حماية الحياة الخاصة من أخطار المعلوماتية، أطروحة دكتوراه، أكاديمية الشرطة، كلية الدراسات العليا، دبي 2011، ص313.

[2] Ian Walden, Computer Crimes and Digital Investigations, Oxford University Press, Oxford United Kingdom, 2007, p37.

[3] Basia Spalek, Crime Victims, Theory, Policy and Practice, Palgrave Macmillan, London United Kingdom, 2nd Ed., 2006, p10.

[4] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص68.

Jeffrey Ian Ross, John L. French, Criminal Investigations: Cybercrime, Chelsea House Pennsylvania, United States, 2010, p24.

[5] أحمد سعد محمد الحسيني، الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية، أطروحة دكتوراه، جامعة عين شمس، كلية الحقوق 2012، ص154.

[6] محمد حماد مرهج الهيتي، المرجع السابق، ص165.

[7] محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، 2005، ص36.

الآلي، وإما منقولة عبر شبكات الإنترنت، بالإضافة إلى جرائم أخرى يكون هدفها الاستيلاء على الأموال وأخرى تستهدف الأفراد أو جهات بعينها، وجرائم أخرى تكون أجهزة الكمبيوتر هدفا لها[1]، كما أن الاعتماد المتزايد على الحاسب الآلي في إدارة مختلف الأعمال، وشتى المجالات، ضاعف من الأضرار والخسائر التي تخلفها الاعتداءات على معطيات هذه الوسائل الإلكترونية وفي مقدمتها الحاسب الآلي، لاسيما إذا كانت تمثل قيمة مالية، وفي هذا الخصوص تشير الدراسات إلى أن الأضرار الناجمة عن جرائم التكنولوجيا الحديثة تفوق بكثير تلك الناجمة عن الجرائم التقليدية[2].

سابعا: القصور في القوانين الجنائية المتعلقة بجرائم التكنولوجيا الحديثة، أدى ذلك القصور إلى محاولة الفقه والقضاء إلى إخضاع جرائم التكنولوجيا الحديثة إلى نصوص قانون العقوبات، وحدث هذا خصوصا في فرنسا وأمريكا، فهذه الجرائم اعتبرتها من جرائم الصحافة باعتبار الشبكة من وسائل النشر، كما أن هناك عدة معوقات تمنع من توقيع العقاب على مرتكبي الجرائم المعلوماتية نذكر منها:

– قلة التشريعات التي تتطرق إلى الجرائم المتصلة بالتكنولوجيا حيث نجد أفعالا إجرامية لا ينطبق عليها أي نص قانوني في قانون العقوبات، إضافة إلى عدم تطور قانون العقوبات بنفس السرعة المذهلة التي تتطور بها التكنولوجيا وعدم مسايرته للتطورات التي يستخدمها الذهن البشري لتطويعها لأغراضه الإجرامية.

– جرائم التكنولوجيا الحديثة ذات بعد دولي فيمكن أن ترتكب هذه الجرائم داخل قطر دولة معينة وتقع النتيجة في دولة أخرى، ومنه تنتج إشكالية توقيع العقاب وإلى أي القوانين القضائية تخضع الجاني، وهو ما يعرف بصعوبة إلحاق العقوبة بالجاني المقيم بالخارج فهنا لابد من تدخل الإنتربول للقبض على الجاني وإخضاعه للعقاب.

– نقص الخبرة الكافية للمشرع والقضاء للتعامل مع الوسائل الإلكترونية التي تظهر أساسا في تطبيق العقوبات على الجناة.

المبحث الثاني: ارتكاب جرائم التكنولوجيا الحديثة

إن الجريمة بشكل عام لا تحتاج الذكاء والعلم اللذين أصبحت ترتبط بهما جرائم التكنولوجيا الحديثة، إذ يستلزم تنفيذ الجريمة إلماما كافيا بمهارات ومعارف فنية في مجال الأنظمة التقنية للإنترنت والكمبيوتر وكيفية التشغيل[3]، ولما كانت جرائم الكمبيوتر لا يصل إليها إلا المبرمج أو المستخدم المؤهل، فإن التطور المستمر وظهور الوسائل الإلكترونية الذكية، وسهولة التعامل مع الإنترنت وسعت من نطاق وحجم المتعاملين مع الإنترنت وهذه الوسائل[4].

وبالتالي يمكن القول إن مرتكبي جرائم التكنولوجيا الحديثة لا يصنفون ضمن فئة معينة، أو جنس معين، فقد يكون بالغا أو حدثا، فقيرا أو غنيا، رجلا أو امرأة، كما يمكن القول إن هدف أو غاية ارتكاب الجريمة تختلف من مجرم إلى آخر تبعا لسنه أو

---

[1] محمد محمد الألفي، جرائم الاعتداء على البطاقات الائتمانية كأحد الأنماط الإجرامية المستحدثة، ندوة مكافحة الجريمة عبر الإنترنت على المستوى العربي، شرم الشيخ، مصر، 20-24 أبريل 2008.

[2] محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، 2007، ص77.

[3] جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية القاهرة، 2002، ص10.

[4] مدحت عبد الحليم رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، ط1، 2000، ص11.

قدرة تعليمه، فقد تكون سياسية، أو إرهابية، مادية، أو لمجرد إثبات المهارة، أو تسخير قدراته التقنية لمصالح منظمات أو عصابات لجني المنافع، كما أن هناك العديد من الوسائل التي تستخدم في ارتكاب جرائم التكنولوجيا الحديثة، منها ما هو نفسي إذ يلجأ لخداع المجني عليه ليتمكن من اختراق النظم والوصول إلى غايته، ومنها ما هو برامج ووسائط تقنية تمكن الجاني من اختراق وسائل الحماية بالنظام.

المطلب الأول: أطراف جرائم التكنولوجيا الحديثة

إن الجرائم كما هو معلوم للجميع يوقعها مجرم يرتكب أفعالا ممنوعة بنفسه أو بواسطة أدوات جرمية مساعدة، إذ تقع تلك الأفعال على محل الجريمة الذي قد يكون شيئا وقد يكون كائنا حيا.

وقد ظهرت جرائم التكنولوجيا الحديثة نتيجة التطور الذي تجسد أساسا في انتشار التكنولوجيا ووسائلها التي تطورت بشكل مستمر، بالإضافة إلى البرامج المتقدمة وشبكات الاتصال التي قربت ملايين البشر بعضهم البعض وأتاحت فرصا جديدة للإطلاع على المعلومات وتبادلها، وحتى التفاوض وإبرام عقود مختلفة خاصة عبر شبكه الإنترنت، بل الأكثر من ذلك أتاحت تسليم المنتجات كالبرامج، المقاطع الموسيقية، الصحف الإلكترونية أو تقديم الخدمات مثل الاستشارات القانونية أو الطبية.

لكن ما دامت جرائم التكنولوجيا الحديثة ظاهرة اجتماعية والتي تعتبر من أكبر السلبيات التي خلفتها التكنولوجيا المتطورة فقد تركت هذه الجرائم في النفوس شعورا بعدم الثقة بخصوص التعامل والاستفادة من ثمار هذه الثورة الجديدة، فجرائم التكنولوجيا الحديثة إذن هي ظاهرة إجرامية مستجدة نسبيا تقرع في جنباتها أجراس الخطر لتنبه مجتمعات العصر الراهن بحجم المخاطر وهول الخسائر الناجمة عنها، تستهدف الاعتداء على المعطيات بدلالاتها التقنية الواسعة (البيانات، المعلومات، والبرامج بكافه أنواعها) فهي جريمة تقنية تنشأ في الخفاء يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية.

الفرع الأول: المجرم في جرائم التكنولوجيا الحديثة

نتناول في هذا البحث المجرم في جرائم التكنولوجيا الحديثة من حيث التعريف به ثم سماته ودوافعه وأخيرا أبرز أقسام المجرمين ولكن قبل ذلك لا بد من الإشارة إلى أنه ليس هنالك ما يمنع من أن يكون المجرم هنا شخصا طبيعيا أو معنويا كما أسلفنا الذكر مع الخلاف الدائر بين الفقه وبعض التشريعات في مدى إقرار المسؤولية الجنائية للشخص المعنوي، ويمكن تصور ارتكاب الجريمة المعلوماتية من قبل الشخص المعنوي كما في حالات قيام شركة أو مصرف أو مؤسسة بارتكاب جريمة الاحتيال المعلوماتي أو سرقة البيانات الإلكترونية أو ممارسة الإرهاب الإلكتروني وما شابه ذلك.

البند الأول: التعريف بالمجرم في جرائم التكنولوجيا الحديثة

من الناحية الجنائية تعني تسمية المجرم في جرائم التكنولوجيا الحديثة ذلك الشخص الذي يمتلك مهارات تقنية أو دراية بالتكتيك المستخدم في نظام الحاسوب الإلكتروني، أو الأجهزة الإلكترونية والقادر على استخدام هذا التكتيك لاختراق الكود السري

لتغيير المعلومات أو لتقليد البرامج، أو التحويل من الحسابات عن طريق استخدام الوسائل الإلكترونية نفسها[1].

أما الخبراء في التكنولوجيا الحديثة والإنترنت بل وحتى العديد من كتاب القانون في هذا المجال ذهبوا إلى القول إن المجرم في جرائم التكنولوجيا يظهر بإحدى الصورتين، الأولى هي الهاكرز HACKERS وهم من يتحدون إجراءات أمن النظم والشبكات دون أن تتوافر لديهم في الغالب دوافع حاقدة أو تخريبية، إنما ينطلقون من دوافع التحدي وإثبات المقدرة، أما الصورة الثانية فهي الكراكرز CRACKERS وهم ممن تعكس اعتداءاتهم ميولات إجرامية خطيرة، وهذا المعيار تعتمد عليه التشريعات الأمريكية في التمييز بين النوعين من المجرمين[2]، فيما يميل البعض[3] إلى تسمية المجرم هنا بالمجرم الإلكتروني الرقمي ويعرفه بأنه كل شخص لديه القدرة على تحويل لغته إلى لغة رقمية، وتخزينها واسترجاعها باستخدام الحاسوب الإلكتروني أو الرقمي وملحقاته ووسائل الاتصال الرقمية وذلك بأداء فعل أو امتناع عنه مخالفا لقواعد الضبط الاجتماعي مما يحدث اضطرابات في المجتمع الدولي أو المحلي.

ويمكن القول إن صورة المجرم في جرائم التكنولوجيا الحديثة باتت غير واضحة بين من يرى أن المجرم هنا ينتمي إلى طائفة المجرمين بطبيعتهم، أو ما يسمون المجرمين ذوي الياقات الزرقاء وبين من يرى أنهم ينتمون إلى طائفة الإجرام المكتسب أو ما يسمون بالمجرمين ذوي الياقات البيضاء[4].

وعلى العموم فإن تسمية الهاكرز تعود إلى ستينات القرن الماضي، أين أطلقت على الشخص الذي لديه قدرات متميزة في مجال الحاسوب مستغلا برامجه أقصى استغلال، وفي بداية السبعينيات تمكن شخصان من ولاية كاليفورنيا من فك رموز الشفرة الخاصة بالاتصالات الهاتفية وتمكنا من اختراق نظام الهواتف من دون دفع رسوم فواتير المكالمات، وفي مطلع الثمانينات تمت أول عملية اعتقال للهاكرز، إذ قامت الشرطة الفيدرالية في مدينة ملواكي بضبط مجموعة كبيرة من الهاكرز قاموا باختراق ستين موقعا في مختلف أنحاء الولايات المتحدة.

ثم صدر بعد ذلك قانون السيطرة على الجريمة المتكاملة والذي أتاح للشرطة الأمريكية القبض على منفذي عمليات الاحتيال المتعلقة بالبطاقات الائتمانية والكمبيوتر[5]، أما في أواخر الثمانينات فقد صدر قانونا جديدا في الولايات المتحدة عرف بقانون الاحتيال بالكمبيوتر وسوء الاستخدام، والذي زاد من سلطات الشرطة الفدرالية قياسا بالقانون الأول، غير أن هجمات الهاكرز باتت تتزايد مع تزايد المواقع الإلكترونية.

جدير بالذكر أن صورة الهاكرز لم تظهر بشكل واضح في مطلع ستينيات القرن الماضي، وذلك بسبب كبر حجم الحاسبات الآلية آنذاك فضلا عن وجود الحراسات عليها إضافة إلى وجودها في غرف ذات درجات حرارة معينة[6]، مما يحول بين هؤلاء المجرمين

---

[1] هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، المرجع السابق، ص32.

[2] أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، دراسة مقارنة، دار النهضة العربية، القاهرة، ط1، 2010، ص21.

[3] مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية، ماهيتها، مكافحتها، دراسة مقارنة، دار الكتب القانونية، القاهرة، 2005، ص16.

[4] مصطلح المجرمين ذوي الياقات البيضاء مصطلح متداول في ميدان علم الاجتماع دلالة على أولئك المجرمين الذين لا تظهر عليهم علامات الإجرام لتمتعهم بمناصب إدارية أو مكانه اجتماعيه حيت يرتكبون هذه الجرائم وهم جالسون في أماكنهم ومكاتبهم الراقية دون أن تتلوث أيديهم فعليا بها، ومن أشهر جرائم ذوي الياقات البيضاء جريمة غسيل الأموال وجرائم التزوير والاحتيال وتجاره الرقيق الأبيض.

[5] David J. Icove, Karl A. Seger, William Von Storch, Computer crime: a crimefighter's handbook, O'Reilly & Associates, Sebastopol, California, United States, 1995, p70.

[6] جون كيريللو، موسوعة الهاكرز (Hacks Attack Revealed)، ترجمة خالد العامري، دار الفاروق للنشر والتوزيع، 2008، ص12.

وبين الوصول إليها، ومع ذلك فإن دريبيس ريتشي وكين نومبسون يعدان من أوائل وأشهر الهاكرز آنذاك لتصميمهما عام 1969 برنامجا سمي اليونكس، والذي يعد الأسرع في ذلك الوقت، غير أن المدة الزمنية المنحصرة بين 1980 و1989 تعد الفترة الذهبية للهاكرز بسبب تصميم الحاسب الإلكتروني IBM وأصبح الحاسب صغير الحجم وسهل النقل، ويمكن استخدامه في أي مكان أو زمان، ولهذا بدأ الهاكرز في هذه الحقبة بالعمل الحقيقي على الاختراق والتخريب.

البند الثاني: سمات المجرم المعلوماتي في جرائم التكنولوجيا الحديثة

يتميز المجرم في جرائم التكنولوجيا الحديثة عن غيره من طائفة المجرمين التقليديين بعدد من السمات، فضلا عن كون الدوافع التي تدفعه إلى الجريمة متعددة ومتنوعة، ولعل أبرز هذه السمات والتي درج معظم الفقه الجنائي على ذكرها، فضلا عن بعض السمات التي أوردها الأستاذ باركر نتناولها في الآتي:

أولا: المجرم مجرم ذكي، جرائم التكنولوجيا الحديثة إجرام الأذكياء ولا يمكن أن يقال إن المجرم هنا ينتمي إلى طائفة المجرمين الأغبياء، فإذا كان من يسرق منزلا أو سيارة مجرم منخفض الذكاء في الكثير من الأحيان، فإن من يستعين بالكمبيوتر أو الأجهزة الإلكترونية الذكية من أجل سرقة مصرف أو شركة هو مجرم على درجة من الذكاء، بحيث يمكنه التغلب على كثير من المشكلات والعقبات الفنية التي تواجهه[1].

ثانيا: المجرم مجرم غير عنيف، يقال في العادة إن الإجرام في جرائم التكنولوجيا الحديثة هو إجرام غير عنيف مقارنة بالإجرام التقليدي الذي يميل فيه المجرم إلى العنف، فإذا كان من الممكن تصور قيام العنف في جرائم الاعتداء على الحاسب ماديات الحاسب أو الأجهزة الإلكترونية، فإن الإجرام التكنولوجي الحديث كإتلاف المعلومات لا يتطلب عنفا كونه من تقنيات التدمير الناعمة (soft sabotage) التي تتمثل في التلاعب بالمعلومات أو الكيانات المنطقية أو البيانات[2]، ومثل ذلك يقال أيضا بالنسبة لسرقة البيانات أو الاحتيال المعلوماتي، أو ما شابه من جرائم التكنولوجيا الحديثة التي يتمثل سلوك الجاني فيها بشكل معالجة فنية هادئة للمعطيات الإلكترونية التي تتم بهدوء وبروية ومن دون أي عنف.

ثالثا: المجرم مجرم متخصص، حيث أثبتت العديد من الدراسات في هذا المجال أن المجرمين في مجال التكنولوجيا الحديثة هم في الغالب لا يرتكبون سوى هذا النوع من الجرائم لتخصصهم فيه.

رابعا: المجرم مجرم محترف، يتطلب هذا النوع من الإجرام مهارة فنية عالية لا يستطيع الشخص المبتدئ القيام بها، إذ تتطلب هذه الجريمة قدرا من الدقة والتخصص لتجاوز العقبات الإلكترونية التي وضعها المتخصصون لحماية الأنظمة كما يحدث في البنوك مثلا، وهذا الاحتراف أو المهارة يكتسبها المجرم إما من الدراسة في مجال تكنولوجيا المعلومات أو عن طريق الخبرة العملية في هذا المجال أو التفاعل الاجتماعي مع الآخرين[3].

---

[1] رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، دار النهضة العربية، القاهرة، ط1، 2011 ص55. سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الإسكندرية، 2007، ص49.

[2] محمد سامي الشوا، المرجع السابق، ص49 و50.

[3] عادل يحي قربي، السياسة الجنائية في مواجهة الجريمة المعلوماتية، دار النهضة العربية، القاهرة، ط1، 2014، ص59.

خامسا: المجرم مجرم عائد إلى الإجرام، إذ يعمد مجرمو جرائم التكنولوجيا الحديثة في الغالب إلى العودة مرة أخرى إلى ارتكاب جرائمهم، إنطلاقا من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم ومن ثم كشف جرائمهم وتقديمهم إلى المحاكمة.

سادسا: المجرم متكيف اجتماعيا، يوصف المجرم التكنولوجي الحديث بأنه إنسان اجتماعي[1]، فهو لا يضع نفسه في حاله عداء سافر مع المجتمع الذي يحيط به[2]، بل هو متكيف اجتماعيا إنطلاقا من كونه إنسانا ذكيا[3]، وتطبيقا لذلك فإن الكثير من الجرائم في هذا الصدد ترتكب بدافع الكبرياء كالموظف المطرود من عمله، أو ترتكب بدافع الاحتيال أو اللهو أو لإظهار مدى ما يتمتع به المجرم من تفوق في مواجهة أنظمة المعلوماتية[4].

أما الأستاذ باركر فقد أورد عددا من السمات الخاصة بالمجرم في جرائم التكنولوجيا الحديثة، والتي يختلف فيها عن غيره من المجرمين[5] ويمكن إجمالها في مايلي:

- **المعرفة**، تعني هذه الخصيصة تعرف الجاني على كافة الظروف والملابسات المحيطة بجريمته التي يريد تنفيذها واحتمالات نجاحها أو فشلها.
- **الوسيلة**، أي الإمكانيات التي يحتاجها الفاعل لتنفيذ جريمته، وهي في الغالب تتجلى في جهاز الحاسب أو ما يقوم مقامه مع البرامج اللازمة لتنفيذ الجريمة في بعض الأحيان.
- **الباعث**، لا يختلف الباعث في جرائم التكنولوجيا الحديثة في الغالب عن الباعث في الجرائم التقليدية الأخرى، فيكون تارة الرغبة في الانتقام وتارة أخرى يكون تحقيق الربح المادي، وآخر في تحدي أنظمة حماية الحاسوب أو الإنترنت.
- **السلطة**، يقصد بالسلطة الميزة أو الحق الذي يمكن المجرم من ارتكاب جريمته، إذ أن الغالب من مجرمي جرائم التكنولوجيا الحديثة لديهم سلطة مباشرة، أو غير مباشرة في مواجهة المعلومات محل الجريمة، وهذه السلطة قد تتمثل في الشفرة –الرقم السري– التي تمكنه من فتح الملفات المخزونة ومن ثم نسخها أو تعديلها أو إتلافها أو سرقتها، كما قد تكون السلطة التي يتمتع بها الجاني غير حقيقية كشفرة الدخول الخاصة بشخص آخر.
- **المهارة**، تعد من أبرز خصائص المجرم التكنولوجي الحديث، لأن القيام بهذه الجرائم يتطلب نوعا من المهارة الفنية والتقنية التي يتمتع بها الفاعل، ولا فرق بين أن تكون هذه المهارة مكتسبة عن طريق الممارسة العملية أو عن طريق الدراسة والتحصيل العلمي أو عن طريق التفاعل مع الآخرين[6].

---

[1] سامي علي حامد عياد، المرجع السابق، ص50.

[2] غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت وجرائم الاحتيال المنظم باستعمال شبكة الإنترنت، دار الفكر والقانون المنصورة، 2013، ص04 و05.

[3] رامي متولي القاضي، المرجع السابق، ص55.

[4] محمد علي العريان، المرجع السابق، ص62.

[5] Donn B. Parker, Fighting Computer Crime: A New Framework for Protecting Information Wiley, Hoboken, New Jersey, United States, 1998, p94.

[6] وإن كان ذلك لا يعني –بتقديرنا – أن يكون مرتكب هذه الجريمة على قدر عال جدا من معلومات التحصيل العلمي أو الممارسة العملية في هذا المجال في جميع الأحوال إذ أثبتت الوقائع أن الصدفة كانت عاملا مهما في العديد من جرائم التكنولوجيا الحديثة.

البند الثالث: دوافع الإجرام في جرائم التكنولوجيا الحديثة

إذا كان قد تبين لنا مما سبق من عرض لأبرز سمات المجرم المعلوماتي والتي يتميز فيها عن المجرم التقليدي، فإن دوافع هذا النوع من الإجرام لا تكاد تختلف كثيرا عن الإجرام التقليدي من حيث المبدأ، مع الإشارة إلى أن هذه الدوافع لا تؤثر في التكييف القانوني للجريمة في ظل العديد من التشريعات الجنائية، إذ لا عبرة بالبواعث، ولكن تظل دراسة هذه الدوافع أمرا مهما من الناحية العلمية عله يفيدنا في تحديد أهم المعالجات التشريعية لجرائم التكنولوجيا الحديثة من حيث تشديد العقوبات في بعض الجرائم، وتنظيم أحكام العود وتشريع العقوبات الملائمة، وعلى العموم فإن أبرز هذه الدوافع تتجلى فيما يلي[1]:

أولا: السعي إلى تحقيق الأرباح المالية، أثبتت معظم الدراسات أن سعي المجرمين إلى تحقيق الربح يأتي في مقدمة الدوافع التي تقف وراء ارتكاب جرائم التكنولوجيا الحديثة[2]، حتى أن أبرز القطاعات المستهدفة من هذه الجرائم هي البنوك التي تعتمد على نظام التمويل الإلكتروني EFT، وشركات التأمين وكذلك حالات أخرى، ومن الجرائم في هذا المجال قضية R.v Thompson إذ تتلخص وقائعها في أن مبرمجا إنجليزيا يعمل في أحد البنوك في الكويت قد قام بالتلاعب في نظام الحاسب الآلي الخاص بالبنك فقام بإجراء خصومات من أرصدة العملاء ليودعها في حسابه الخاص، وبعد عودته إلى انجلترا قام بمخاطبة البنك طالبا منه تحويل الحساب الخاص به إلى عدة حسابات بنكية في انجلترا وقدم فيما بعد إلى المحاكمة وحكم عليه بعقوبة السجن، وفي عام 2007 توصلت دراسة إلى أن ثلث المصارف في سويسرا تقع ضحية جرائم التكنولوجيا الحديثة[3].

ثانيا: الأحقاد الشخصية والرغبة في الانتقام، من بين التصنيفات الفقهية لمجرمي جرائم التكنولوجيا الحديثة وجدنا فئة بارزة سميت ب الحاقدين[4]، ويبرز هذا الدافع في الغالب في الحالات التي يتم فيها إسناد مهمة إلكترونية إلى شخص معين داخل مؤسسة رسمية أو غير رسمية، فيتاح له من خلال هذه المهمة التعرف على محتويات الحاسبات لتلك المؤسسة بما تحتويه من أسرار عمل وأرقام بنكية سرية والمفاتيح السرية للحسابات Passeword، والمجرمين في هذه الحالة ينقسمون إلى قسمين أولهما المجرمين الذين يعملون في المؤسسة فيعمدون إلى اختراق أنظمتها الإلكترونية إما بسبب سوء التعامل معهم أو بسبب قلة أجورهم أو رواتبهم وما شابه، وثانيهما أولئك الذين يكونون خارج المؤسسة كالموظفين المطرودين من عملهم، والذين يعملون إلى الإساءة إلكترونيا إلى المؤسسات التي استغنت عن خدماتهم، فتتحول الثقة السابقة بمثل هكذا أشخاص إلى وبال على تلك المؤسسة في حالة طردهم أو الاستغناء عن خدماتهم لما يمتلكه هؤلاء من معرفة بأسرار النظام المعلوماتي للمنشأة التي كانوا يعملون بها.

---

[1] عمار عباس الحسيني، التجريم والعقاب في النظام التأديبي، قراءة معاصرة في النصوص الجنائية والتأديبية، منشورات الحلبي الحقوقية، بيروت، ط1 2015، ص17-20.

[2] Etienne Montero, "Premières considérations sur les questions de responsabilité liées aux paiements par WAP."Transferts électroniques de fonds. Académia Bruylant, 2001, pp163-186.

[3] Etienne Montero, Ibid., p165

[4] يونس عرب، جرائم الكمبيوتر والإنترنت، المرجع السابق.

ومع ذلك فهنالك حالات أخرى تبرز فيها طائفة الحاقدون غير حالات الموظفين في المؤسسات الرسمية وغير الرسمية ومنها مثلا قيام أحد الأشخاص لنشر صور تخص إحدى صديقاته التي هجرته بعد أن يدبلجها بأوضاع غير لائقة إباحية، ونشرها على بعض مواقع الإنترنت أو اختراق موقعها الإلكتروني الشخصي وما شابه.

ثالثا: الدوافع السياسية، شهدت السنوات المنصرمة وجود حرب سياسية إلكترونية بين العديد من الدول لاسيما في حالات الحرب والاختلافات السياسية كاختراق المواقع الإلكترونية للدولة الأخرى والتجسس عبر الإنترنت الذي بات من أبرز الوسائل المخابراتية، أو تدمير بعض المواقع الرسمية أو إيقافها عن العمل، ناهيك على أن بعض المجرمين هنا غير المنتمين إلى جهات سياسية أو حكومية قد يقومون وبدوافع سياسية ووطنية باختراق المواقع الإلكترونية لبلدان معادية لبلدانهم[1].

رابعا: تحدي وقهر النظام المعلوماتي، تدأب إدارات المواقع الإلكترونية على تأمين مواقعها بشكل محكم من خلال تعقيد الأرقام السرية وتغييرها باستمرار التشفير[2]، وهذا الأمر يحفز الكثير من المجرمين المحترفين على الدخول في تحد مع أنفسهم أولا ومع أنظمة تلك لمواقع ثانيا، من أجل قهر نظم الحماية تلك واختراقها، والغالب في هذه الفئة من المجرمين صفة عدم الخطورة الاجتماعية، إنما هم يلجؤون إلى هذه الأفعال بدافع التحدي وإثبات الذات والرغبة في تحدي أي نظام إلكتروني حديث[3].

خامسا: التسلية والولع بالأنظمة المعلوماتية، هذا الدافع قد يتداخل مع الدافع السابق وقد يكون صورة من صوره حيث يعمد بعض المجرمين في جرائم التكنولوجيا الحديثة ممن لديهم شغف وولع بالأنظمة المعلوماتية إلى محاولة إظهار تفوقهم ومستوى براعتهم التقنية وهم غالبا ما يكونون مدفوعين بدوافع التسلية ناهيك عن دوافع التحدي التي سبق إيرادها[4].

البند الرابع: أصناف مرتكبي جرائم التكنولوجيا الحديثة

تعددت تقسيمات الفقه لمرتكبي جرائم التكنولوجيا الحديثة ونشير هنا إلى أبرز تلك التقسيمات، وهي كالتالي:

أولا: تقسيم مرتكبي جرائم التكنولوجيا الحديثة من حيث السن والخبرة، لعل هذا التقسيم هو الأقدم بين تقسيمات المجرمين هنا وهو تقسيم ظهر مع أولى الكتابات القانونية في هذه المجال، ويذهب إلى تقسيمهم إلى هواة ومحترفين[5].

1- مرتكبي جرائم التكنولوجيا الحديثة الهواة: يطلق البعض على هذه الفئة أو الصنف تسمية المتلعثمين[6] فيما أطلق

---

[1] Teri Bidwell, Hack Proofing Your Identity in The Information Age, Syngress, 2002, p30.

[2] Louise Ellison, Yaman Akdeniz. "Cyber-stalking: the Regulation of Harassment on the Internet." Criminal Law Review, Sweet and Maxwell, London, United Kingdom, N°29, 1998 pp29-48.

[3] Louise Ellison, Ibid., pp144-145.

[4] محمد سامي الشوا، المرجع السابق، ص52 و53.

[5] David J. Icove, Karl A. Seger, William Von Storch, Op.Cit., p70.

[6] توم فوريستر، مجتمع التقنية العالية، قصة ثورة تقنية المعلومات، ترجمة محمد كامل عبد العزيز، مركز الكتب الأردني، عمان، ط1، 1989، ص407. جدير بالذكر أن لفظ التلعثم كناية عن صغر السن.

البعض الأخر عليه تسميه صغار نوابغ المعلوماتية[1]، وذهب آخرون إلى تسميتهم بالمجانين[2]، وسماهم آخرون بالشباب حديثي العهد بالمعلوماتية[3] أو الهواة[4] أو العابثين[5]، أو المخترقين[6] أما الاسم العلمي المتداول لهذه الطائفة من المجرمين فهو الهاكرز Hackers[7] وهو مصطلح أطلق في بادئ الأمر في ستينيات القرن الماضي على مجموعة من الطلبة الذين يدرسون في الجامعات الأمريكية، ممن يتميزون بقدرات عالية وكفاءة في إلمامهم بعلوم الحاسوب وتقنياته مع قدرتهم على اختراق شبكات الحاسوب بجهدهم الذاتي، وبدون الاستعانة بأية إرشادات أو تعليمات ومعظمهم من صغار السن.

ويهدف هذا النوع من المجرمين إلى الحصول على المعلومات بشتى الوسائل ويسخر قدراته في هذا المجال، وهم يقومون بأعمالهم هذه لمجرد إظهار أنهم قادرون على اقتحام المواقع الأمنية أحيانا، أو لمجرد ترك بصماتهم التي تثبت وصولهم إلى تلك المواقع أحيانا أخرى، وهم يدعون أن لا دوافع خبيثة وراء أفعالهم تلك، إنما الدوافع وراء تلك الأفعال التي يقومون بها تتمثل في الفضول وحب المعرفة والتعمق في عمل الأنظمة المعلوماتية[8]، وقد ذهب البعض[9] إلى اعتبار هذا النوع من المجرمين أبطالا شعبيين معاصرين يقدمون خدمة للتقنية الحديثة، فيما ذهب جانب أخر من الفقه إلى القول: "نستطيع أن نقرر أن هذا النمط من أفعال الغش والذي يرتكبه هؤلاء الشباب لا خوف منه على الإطلاق"[10].

ونرى أن القول الأخير محل نظر، إذ من غير المنطقي التسليم بعدم خطورة أي نمط من أنماط الجريمة مهما كان نوعها وأيا كان حجمها، لأن الإجرام يبقى ظاهرة تستحق الوقوف عندها ومعالجتها، وإذا كان هذا القول ينطبق على الإجرام التقليدي ذي

---

[1] محمد سامي الشوا، المرجع السابق، ص52-54، حيث عرفهم بأنهم الشباب البالغ المفتون بالمعلوماتية والحاسبات الآلية، وكثيرا ما لفتت النظر في الآونة الأخيرة عقب أفعال الانتهاك غير المسموح بها في العديد من ذاكرات الحاسبات الآلية، وذهب إلى التسمية ذاتها عبد الفتاح بيومي حجازي مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دراسة قانونية متعمقة في القانون المعلوماتي، دار الكتب القانونية، مصر، ط1، 2008 ص90. سامي علي حامد عياد، المرجع السابق، ص52. فريد منعم جبور، حماية المستهلك عبر الإنترنت ومكافحة الجريمة الإلكترونية، دراسة مقارنة منشورات الحلبي الحقوقية، بيروت، ط2، 2012، ص190.

[2] محمد محمود المكاوي، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية، المكتبة العصرية للنشر والتوزيع، المنصورة، 2010 ص45.

[3] محمد علي العريان، المرجع السابق، ص63.

[4] جلال محمد الزعبي وأسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان، ط1، 2010 ص74.

[5] محمد محمود المكاوي، المرجع السابق، ص45.

[6] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص51. ويشيرون إلى أن أحد أهم شركات حفظ أمن المعلومات قد صنفت هذه الفئة من المجرمين إلى ثلاثة نماذج هي: أولا المشردون وهم عادة ما يكونون من الأطفال، ثانيا؛ المستغلون أو ذوي القبعات السوداء وهم الذين يعملون من أجل الربح الشخصي أو التأثير في المواقف السياسية، وثالثا؛ ذوي القبعات البيضاء وهم الذين يعملون من أجل البحث.

[7] محمود أحمد عبابنة، المرجع السابق، ص40 و41.

[8] Donn B. Parker, Fighting Computer Crime: A New Framework for Protecting Information Op.Cit., pp144-146.

[9] توم فوريستر، المرجع السابق، ص401-407.

[10] محمد حماد مرهج الهيتي، المرجع السابق، ص53.

المخاطر البسيطة أو المحدودة في الغالب، فهو من باب أولى يكون واجب المراعاة في نمط الإجرام الإلكتروني لاسيما عند فئة الناشئين.

2- مجرمي التكنولوجيا الحديثة المحترفين: هذه الطائفة يطلق عليها (Crackers)، وأغلب مجرمي هذه الطائفة ممن تجاوزت أعمارهم 25 عاما ويتميزون بالتخصص العالي في مجال الوسائل الإلكترونية والمعرفة التقنية والذكاء، وجرائمهم تدل على خطورة إجرامية على عكس جرائم النوع الأول (الهاكرز)، وأغلب أفراد هذه الطائفة ممن يعملون في منشآت تستخدم الحاسب باستمرار، وهم بحكم وظيفتهم يتصلون بالوسائل الإلكترونية وفي مقدمتها الحاسب الآلي اتصالا وثيقا، الأمر الذي يجعلهم يطلعون بشكل دائم على محتويات الحاسب وأسرار العمل[1]، وكثيرا ما ينظر إلى مجرمي هذه الفئة بوصفهم مستخدمين مثاليين كما أنهم يتمتعون بثقة كبيرة في مجال عملهم وكثيرا ما يقومون بتغيير وظائفهم أثناء نشاطهم الحرفي[2].

جدير بالذكر أن هذه الطائفة من المجرمين البالغين تتميز بالخبرة والإدراك الواسع لمهارات الكمبيوتر والأجهزة الإلكترونية إضافة إلى التنظيم والتخطيط والخبرة، وأفراد هذا النوع من المجرمين تقسم إلى عدة طوائف، أبرزها طائفة مجرمي الاحتيال والتزوير وتتجه أغراضها إلى الكسب المادي والاستيلاء على أموال الآخرين، وكذلك طائفة التجسس الصناعي وهي التي توجه أنشطتها الإجرامية إلى اختراق نظم الكمبيوتر التابع للشركات الصناعية ومشاريع الأعمال، بقصد الاستيلاء على الأسرار الصناعية والتجارية وبصفة عامة فإن هذا النوع من المجرمين هم الأكثر خطورة[3].

ثانيا: تقسيم مجرمي التكنولوجيا الحديثة إلى مستخدمين ومبرمجين، ذهب البعض إلى تقسيم ثنائي -يقترب في مفهومه من التقسيم السالف- يعتمد على معيار المعرفة بنظم المعلوماتية، ونتناولها بإيجاز في الآتي[4]:

1- المجرمون المستخدمون: هذه الطائفة من المجرمين هم المستخدمين فقط ممن تتوافر لديهم المعلومات الكافية عن آلية عمل الوسائل الإلكترونية ومكوناتها ووظائفها الأساسية، ومعرفتهم ببعض البرامج التي يجري بها العمل، ولديهم أيضا معرفة بعمل الشبكة المعلوماتية، وهم يرتكبون جرائمهم دون أن تكون لهم علاقة بالنظم المعلوماتية، سوى الاستخدام فحسب، ومن أمثلتهم الموظفين في المؤسسات المالية كالبنوك، وهذه الفئة من المجرمين في تزايد واتساع وانتشار تبعا لتطور نظم تقنية الوسائل الإلكترونية وتعدد استخداماتها في مختلف المجالات.

2- مجرمون مبرمجون: نظرا للمستوى العالي الذي يتمتع به المبرمجون وقدرتهم على دخول واقتحام الأنظمة الحاسوبية بكل سهولة على الرغم من الاحتياطات الأمنية المتعددة فإن الخطورة واضحة هنا بصورة كبيرة، إذ غالبا ما تكون الجرائم المرتكبة من طرف هذه الفئة ضخمة وذات أهمية كبرى، ولعل ما يزيد من خطورة هذه الجرائم قلة العناصر القادرة على اكتشافها وهؤلاء المبرمجون قادرون على القيام بتعديل وتحويل ونسخ وإضافة أي معلومات على البرامج، بالإضافة إلى قدرتهم على إتلافها وتغيير محتواها لتحقيق أغراض مشروعة، كل ذلك يتم باستغلال المساحات الخالية بين أوامر برامج الحاسب الآلي مع الاستفادة من الأوامر الأخرى المحققة لأغراضهم.

---

[1] محمود أحمد عبابنة، المرجع السابق، ص42 و43.

[2] محمد سامي الشوا، المرجع السابق، ص55.

[3] محمد محمود المكاوي، المرجع السابق، ص47 و48.

[4] جلال محمد الزعبي وأسامة أحمد المناعسة، المرجع السابق، ص72-74.

ثالثا: تقسيم المجرمين من حيث أماكن عملهم، ذهب البعض[1] إلى تقسيم آخر للمجرمين من حيث أماكن عملهم نتناوله بإيجاز على النحو التالي:

1- المجرمون من داخل المؤسسة: هذه الفئة هي الأخطر وذلك لمعرفتها بنظام المؤسسة وتشغيل النظام والعبث به ومعرفة نقاط الضعف والقوة بذلك النظام، ويتزايد هذا النوع مع ازدياد ظاهرة تسريح الموظفين في قطاع تقنية المعلومات والإنترنت مما يؤدي إلى سعي هؤلاء إلى الانتقام من المؤسسة، ومن أمثلة ذلك قيام مدير لأنظمة الكمبيوتر كان يعمل في إحدى الشركات باختراق نظام الشركة وتغيير حسابات الزبائن وإزالة قواعد بيانات هامة، كل ذلك لأنه كان مستاء من تعامل الشركة معه، مما كبد الشركة التي كان يعمل بها خسائر فادحة أوصلتها إلى إعلان إفلاسها ومن ثم بيعها لاحقا، ومن الأمثلة الأخرى أن موظفا فصل من الشركة التي كان يعمل بها وقبل يومين من تركه للعمل، قام ببرمجة كمبيوتر في الشبكة زارعا نوعا من الفيروسات، وبعد مرور يومين حذفت معلومات هامة في الشركة.

2- المجرمون من خارج المؤسسة: وهم ثلاثة أصناف؛ مخترقو الشبكات، ناسخوا البرنامج وصانعوا الفيروسات.

أ- مخترقو الشبكات: هم الأشخاص الذين يخترقون شبكات الحاسوب مستعينين بما لديهم من قدرات متميزة ورغبات جامحة في الاختراق، وينقسمون إلى قسمين، الأول؛ هم المخترقون الذين يعملون في إطار منظم لتحقيق أهداف معينة، وغالبا ما تهدف هذه الفئة إلى الكسب غير المشروع من خلال اختراق حسابات البنوك أو الشركات التجارية، أما القسم الثاني؛ فهم المجرمون المعتمدون على قدراتهم لإشباع الفضول وإثبات الذات، وهؤلاء عندما يصلون إلى غايتهم فإنهم يتركون الشبكة دون العبث ببياناتها وملفاتها ولا يعودون لاختراقها ثانية إلا بعد تطوير طرق الحماية فيها مما يبعث فيهم روح التحدي الأخلاقي للاختراق[2].

ب- ناسخوا البرامج: يطلق على هؤلاء في الاصطلاح الإلكتروني الإعلامي تسمية القراصنة[3]، وهؤلاء هم نوع من الهاكرز المتخصصين بفك شفرات البرامج وليس تخريب الشبكة، وهم يقومون بخرق مقاييس الحماية التي تمنع من استنساخ البرامج فعادة عند شراء أي برنامج فإنه يتطلب رقم تسلسل (Serial Nimber) لإتمام عملية تثبيته في الجهاز الشخصي، ومن هنا يقوم هؤلاء بتشغيل برنامج يقوم بتجربة الملايين من الأرقام حتى يحصل على الرقم الصحيح ومن ثم استخدامه في تثبيت البرامج المنسوخة، ومن الطرق الأخرى لهذه الفئة خرق الصيغة المكتوبة للبرنامج بحيث يقوم بتغييرها[4]، ومجرمو هذه الطائفة يقعون بأحد الصورتين، الأولى هم من يقومون بهذه الأفعال بدوافع تحقيق غايات مادية وأرباح تجارية والثانية تقوم بهذه الأفعال بدوافع الاستخدامات الشخصية فحسب.

---

[1] مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية، المرجع السابق، ص24-27.

[2] David Wall, Op.Cit, pp59-73.

[3] Jos Dumortier, Patrick Van Eecke, Legal issues and the internet. Internet European Compared Law, Sous la dir, de Georges Chatillon, Bruxelles, Bruylant, Bruxelles, Belgique, 2000, p161.

[4] Peter N. Grabosky, Electronic Crime, Pearson Prentice Hall, New Jersey, United States, 2007 p13.

ج– صانعوا الفيروسات: يتمتع هؤلاء المجرمون بمهارات عالية في البرمجة، بحيث يستطيعون اختراق الأنظمة والقيام بعمليات حسابية لا تنتهي، ويستمر الحاسوب في التنفيذ والحساب حتى يستنفذ كل مصادره من الذاكرة الرئيسية والثانوية حتى ينهار النظام[1].

رابعا: تقسيم الأستاذ Parker لمجرمي التكنولوجيا الحديثة، ذهب الأستاذ باركر إلى تقسيم المجرمين إلى مجموعة من الأصناف، ولكن دون أن يعني ذلك أن كل مجرم يجب أن ينتمي إلى صنف محدد دون غيره، بل يمكن أن يكون المجرم الواحد مزيجا بين أكثر من طائفة[2]، ويمكن إجمال أهم هذه الأصناف فيما يلي:

1– طائفة يرتكبون جرائمهم بهدف التسلية واللهو وقضاء الوقت دون أن يكون في نياتهم الإضرار بالغير، وأبرز من يمثل هذه الطائفة هم صغار مجرمي التكنولوجيا الحديثة أي الأحداث.

2– طائفة تضم المجرمين الذين يقومون بكسر الحواجز الأمنية لغرض الدخول إلى أنظمة الوسائل الإلكترونية التي لم يصرح لهم بالدخول إليها، وكل ذلك يتم بغرض اكتساب الخبرة أو بدافع الفضول أو التحدي.

3– طائفة تهدف إلى إلحاق خسائر بالمجني عليهم دون أن يكون هدفها الحصول على مكاسب مادية، ومن أمثلة هؤلاء صانعي الفيروسات وموزعيها.

4– مجرمي هذه الطائفة هم الأكثر شيوعا بين مجرمي التكنولوجيا الحديثة، وهم يتمتعون بقدر معقول من الخبرة في هذا المجال، ويترتب على ارتكاب جرائمهم خسائر كبيرة تلحق بالمجني عليهم، يهدفون إلى إيجاد حلول لمشكلات مادية تواجههم دون أن يستطيعوا حلها بالوسائل الأخرى بما فيها اللجوء إلى الجريمة التقليدية، ويبررون أفعالهم بأن المجني عليه في جرائمهم –وهي في الغالب المؤسسات المالية– يستطيع تحمل الخسائر الناجمة عن أفعالهم.

5– يمكن القول إن المجرمين الذين ينتمون إلى هذه الطائفة يبغون من وراء نشاطهم الإجرامي تحقيق الربح المادي بطريقة غير مشروعة، وهم يعملون في الغالب بطريقة منظمة بحيث يمكن أن ينطبق على أفعالهم وصف الجريمة المنظمة[3]، إذ يقترب فاعل هذه الجريمة من المجرم التقليدي لاسيما بعد أن أصبحت جرائم التكنولوجيا الحديثة تجتذب اهتمام العديد من الجماعات الإجرامية المنظمة لما تدره من عائدات هائلة[4].

---

[1] Bruce Sterling, The Hacker Crackdown, Law And Disorder On The Electronic Frontier Bantam Books, New York, USA, 1992, pp35-36.

[2] Donn B. Parker, Fighting Computer Crime: A New Framework for Protecting Information Op.Cit., pp144-146.

[3] Peter Emeritus Grabosky, Peter Grabosky, Russell Gordon Smith, Gillian Dempsey Electronic Theft: Unlawful Acquisition in Cyberspace, Cambridge University Press, 2001 pp198-199.

[4] حسن طاهر داود، جرائم نظم المعلومات، مركز الدراسات والبحوث، أكاديمية نايف العربية للعوم الأمنية، الرياض، ط1، 2000، ص75 و76.

6– تضم هذه الطائفة الجماعات الإرهابية المتطرفة، مدفوعين بغايات سياسية أو دينية أو اجتماعية يرغبون في فرضها ويبدو نشاط مجرميها في تحقيق العنف ضد الأشخاص والممتلكات للفت الأنظار إليهم[1].

7 – طائفة المهملون الذين كثيرا ما يترتب على جرائمهم الواقعة بطريق الخطأ ولاسيما بصورة الإهمال أضرارا قد تؤدي في كثير من الأحيان إلى حد إزهاق الأرواح[2].

خامسا: التقسيم الثلاثي الإنجليزي لمجرمي التكنولوجيا الحديثة، ذهب بعض الأساتذة في إنجلترا إلى تقسيم مجرمي التكنولوجيا الحديثة إلى:

1– المخترقون أو المتطفلون: ذهب أصحاب هذا التقسيم إلى الجمع بين طائفتي الـ Hackers والـ Crackers تحت هذه الطائفة من مجرمي التكنولوجيا الحديثة، وذهبوا أيضا إلى أن طائفة الـ Hackers هم متطفلون يتحدون إجراءات أمن النظم والشبكات دون أن تتوافر لديهم دوافع حاقدة أو تخريبية إنما ينطلقون من دوافع التحدي وإثبات المقدرة، أما الـ Crackers فعلى العكس، إذ تتوافر لديهم دوافع إجرامية واعتداءاتهم تنبئ عن خطورة إجرامية ورغبة في إحداث التخريب[3].

2– المحترفون: أفراد هذه الطائفة يتميزون بالخبرة وسعة الإدراك للمهارات التقنية والتنظيم والتخطيط للأنشطة المركزية لهذا تعد هذه الطائفة الأخطر بين هؤلاء المجرمين، وتهدف اعتداءاتها إلى الكسب المادي لها أو للجهات التي كلفتها بارتكاب الجريمة وفي بعض الأحيان تهدف اعتداءاتهم إلى تحقيق أغراض سياسية والتعبير عن موقف فكري أو فلسفي، ويتميز أفراد هذه الطائفة بصفة التكتم على أفعالهم الإجرامية فلا يتبادلون الخبرات التقنية فيما بينهم بل يعمدون إلى تطويرها بشكل ذاتي، كما يتنوع مجرمو هذه الطائفة بحسب نوع الجريمة التي يمارسونها.

3– الحاقدون: أفراد هذه الطائفة يرتكبون أنشطتهم الإجرامية بدافع الثأر والانتقام، ولهذا فهم يقسمون إلى مجرمين على علاقة بالنظام وآخرين غرباء عن النظام، وقد يتطور إجرام هؤلاء إلى المستوى الدولي حيث تشن دولة حرب إلكترونية على دولة أخرى بدافع الانتقام لتعطيل أو تخريب أنظمتها الإلكترونية الخدمية في ظل ما يعرف اليوم بالحوكمة الإلكترونية.

4– المتسلل إلى نظم الاتصال الهاتفي: هو شخص يتسلل إلى شبكات التلفون أو أي نظام اتصال آخر مؤمن للتعرف على طبيعة عمله[4].

---

[1] مايكل سميث، الحرب بواسطة شبكات الاتصال، الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر حوارات إنسانية في القانون والسياسات والعمل الإنساني، 2002، ص88.

[2] حسن مظفر الرزو، الأمن المعلوماتي معالجة قانونية أولية، مجلة الأمن والقانون، العدد 01، السنة 12، أكاديمية الشرطة، دبي، نيسان 2004 ص200.

[3] محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والإنترنت، دراسة مقارنة، دار الفكر والقانون، المنصورة، 2013، ص14 و15. وأشار البعض إلى هذا التقسيم أيضا، وذهب إلى أن هؤلاء الأساتذة الثلاث قد أوردوا هذا التقسيم في مؤلفهم جرائم الكمبيوتر والإنترنت، الصادر عام 1995. أشار إليه أيمن عبد الله فكري، جرائم نظم المعلومات، دراسة مقارنة، دار الجامعة الجديدة للنشر، الإسكندرية، 2007، ص107-111. وفي حقيقة الأمر نرى أن التقسيم أعلاه لا يخرج عن كونه مشابها من حيث المبدأ للعديد من التقسيمات الواردة سلفا، ولكن كل ما في الأمر أن هذا التقسيم قد دمج بين بعض أصناف المجرمين المعلوماتيين طائفتي الـ Hackers والـ Crackers، فيما أبرز طوائفا أخرى لم تكن بارزة في التقسيمات الأخرى كطائفة الحاقدين وأدخل ضمنهم التقسيم الخاص بمجرمي التكنولوجيا الحديثة من حيث أماكن عملهم.

[4] جون كيريللو، المرجع السابق، ص122.

5- مخترقو الشبكات والنظم قليلو الخبرة: أو أطفال الاسكربتات وهم الأشخاص الذين يستخدمون ما توصل إليه الهاكرز من معلومات وبرامج لاستخدامها في الاختراق، وهم لا يستطيعون اكتشاف الثغرات بل يقومون فقط بتطبيقها.

الفرع الثاني: المجني عليه في جرائم التكنولوجيا الحديثة (الضحية)

تعتبر الجهات المتضررة من ارتكاب جرائم التكنولوجيا الحديثة من أهم عناصر البحث المطلوبة من المتخصصين والباحثين للوقوف على النسب الصحيحة والواقعية لارتكاب هذه الجرائم، وعليه اهتمت المجتمعات البدائية في العصور القديمة بالمجني عليه باعتباره المتضرر مباشرة من الجريمة، وتعاملت مع الجاني بقسوة في مختلف أنواع العقاب والتعذيب التي قد تصل إلى الحرق والتقطيع والإبادة وتعويض الضحية عما لحق به من أضرار، ثم أخذت نصرة الضحية والاهتمام به تتقلص تدريجيا في صور إجبار الجاني في دفع دية وتعويضات عينية لصالح المجني عليه، وبات الاهتمام يتزايد لمساعدة الجاني وحماية حقوقه، إلى أن نادى الفيلسوف الإنجليزي Jermy Bentham في القرن الثامن عشر بضرورة النظر إلى ضحايا الجريمة بعين الاعتبار والتعامل معهم على الأقل بالقدر الذي يعامل به الجاني[1]، وقد ظهرت فكرة الدفاع الاجتماعي وتبلور مفهومها في توفير الحماية الاجتماعية للمجتمع لحماية بعض فئاته من الانحراف في أواخر القرن التاسع عشر، وذلك لتقديم الرعاية الصحية والمعاملة الإنسانية والمساعدة النفسية والاجتماعية لكي يتمكنوا من تخطي الآثار النفسية والاجتماعية الناجمة عن الجريمة.

البند الأول: تعريف المجني عليه

لكل جريمة مجني عليه، وهو الشخص -الطبيعي أو المعنوي- صاحب المحل القانوني الذي تحميه القاعدة القانونية الجنائية ونظرا لاختلاف الزاوية التي ينظر من خلالها كل اتجاه من الفقهاء إلى ضحية الجريمة، فقد أدى ذلك إلى الاختلاف فيما بينهم حول صياغة تعريف محدد للمجني عليه، فقد عرفه البعض بأنه الطرف السلبي في الجريمة الذي يتحمل الضرر الناجم عنها ولا يمكن أن يكون سببا فيها[2] ويرى آخر أن المجني عليه هو كل من لحقه من الجريمة ضررا ماديا وأدبيا[3].

وقد عرفت الأمم المتحدة المجني عليهم طبقا لإعلان المبادئ الأساسية لتوفير العدالة لضحايا الجريمة الصادر في 01 ديسمبر 1985م بأنهم الأشخاص الذين لحق بهم ضرر أو خسارة أو إيذاء في أنفسهم أو ممتلكاتهم أو حقوقهم الإنسانية، كنتيجة لسلوك ناتج عن خرق قوانين الجزاء الوطنية، أو جرم ناتج عن خرق القانون الدولي، أو جرم ناتج عن خرق لحقوق الإنسان المعترف بها دوليا، أو جرم ناتج عن إساءة استعمال السلطة من قبل أشخاص ذوي سلطة سياسية أو اقتصادية، ويمكن أن يكون المجني عليه ضحية لإنسان أو مجموعات إنسانية أو هيئات اقتصادية أو سياسية أو جمعيات[4].

---

[1] محمد الأمين البشري، علم ضحايا الجريمة وتطبيقاته في الدول العربية، دار الحامد للنشر والتوزيع، عمان، 2005، ص68.

[2] سعود محمد موسى، شكوى المجني عليه، دراسة مقارنة، أطروحة دكتوراه، أكاديمية الشرطة، جامعة القاهرة، 1990، ص177.

[3] رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، دار الجيل، بيروت، 1985، ص120.

[4] سليمان سعيد عبيد المرشدي، دور الشرطة في حماية ضحايا الجريمة، دراسة مقارنة، أطروحة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة 2006، ص27.

وقد أوضح هذا التعريف أن الضحايا هم الأشخاص الذين أصيبوا بضرر فردي أو جماعي أو خسارة اقتصادية عن طريق أفعال أو حالات إهمال تشكل انتهاكا للقوانين الجنائية النافذة من قبل الجاني سواء كان معروفا أم مجهولا، تم القبض عليه أو لم يتم القبض عليه، أدين أو لم تتم إدانته، بصرف النظر عن العلاقة الأسرية التي قد تربط الضحية بمرتكب الجريمة ليشمل هذا المصطلح العائلة المباشرة للضحية، ومن يعولهم مباشرة، والأشخاص الذين أصيبوا بضرر جراء تدخلهم لمساعدة الضحايا في محنتهم أو وقف الإيذاء عنهم، وتنطلق الأحكام الواردة في هذا الإعلان على الجميع دون تمييز للون أو العرق أو الجنس أو الدين أو المركز الاجتماعي أو السياسي أو الثقافي أو السن، وهذا ما اعتمدته الأكاديمية القومية لمساعدة الضحايا إذ توسعت في التعريف عما عرفته الأمم المتحدة بشأن المبادئ الأساسية لعدالة ضحايا الجريمة وإساءة استخدام السلطة، من حيث أنها اتسعت في تعريف الضحايا لتشمل شخصا، أو الجماعات أو الكيانات، ليشمل الإيذاء البدني والنفسي والاقتصادي ويشمل ضحايا الغش أو المشاريع المالية، وحتى الحكومة، كما أن التعريف توسع في حقوق الضحايا ليشمل الشخص الذي عانى مباشرة أو تعرض لتهديد مادي أو معنوي أو كنتيجة لارتكاب جريمة سواء كانت الضحية فردا أم مؤسسة[1].

وبهذا المفهوم، يشكل ضحايا جرائم التكنولوجيا الحديثة قطاعات كبيرة ومتنوعة من الأفراد والمجتمعات والمؤسسات المالية والشركات التجارية، الأمر الذي يصعب معه تحديد ضحايا هذه الجرائم وتحديد مدى التضرر الذي أصاب كلا من الضحايا، ومما يضاعف تعقيدات ضحايا جرائم التكنولوجيا الحديثة صعوبة اكتشاف الجرائم والتعرف على الجناة أو الضحايا فيها بشكل دقيق وفي الوقت المناسب.

وفي مجال جرائم التكنولوجيا الحديثة دائما قد يكون سبب وقوع الجريمة ليس الجاني فقط، بل إنه في حالات كثيرة يكون للضحية دورا في وقوع الجريمة، بسبب جهله أو إهماله في أخذ الحيطة والحذر، أو عدم وضع الحماية اللازمة من برامج الحماية على الأجهزة للحفاظ على مستودع الأسرار سواء كانت شخصية أم معلومات خاصة بالعمل، مما يساعد الجاني في ارتكاب جريمته بسهولة ويسر كما يختلف الأمر عند قبول الفعل بواسطة تهديد ناعم، وعندما يتم إجبار الضحية دون رضاه، وفي معظم الأحوال يؤدى الرضا إلى إزالة أو نفي ركن من أركان الجريمة أو يبيح ما يعتبر فعلا جنائيا، وبالتالي لا يكون الشخص الجاني مذنبا، ولهذه القاعدة استثناءات، ويتعين على المشرعين تقدير مشروعية هذه الاستثناءات وفلسفة الرضا[2].

البند الثاني: التفاعل بين الشرطة والضحية

اهتم الجهاز الأمني اهتماما بالغا باكتشاف المجرمين في جرائم التكنولوجيا الحديثة والقبض عليهم ومحاكمتهم وحبسهم وإعادة تأهيلهم، لكنه وجه اهتماما أقل للضحايا، فكثيرا ما يؤذي الضحايا مثولهم أمام أجهزة العدالة الجنائية، مما يؤدي لزيادة الصدمة النفسية التي يتعرضون لها، فضلا عن شعورهم بالعجز والإحباط[3].

---

[1] محمد الأمين البشري، علم ضحايا الجريمة وتطبيقاته في الدول العربية، المرجع السابق، ص70 و71.

[2] Vera Bergelson, Victims' Rights and Victims' Wrongs: Comparative Liability in Criminal Law, Stanford University Press, California, United States, 2009, p15.

[3] ممدوح عبد الحميد عبد المطلب، دور الشرطة وضحايا الجريمة، مجلة كلية الدراسات العليا، العدد 13، أكاديمية الشرطة، الرياض، 2005، ص32 وما بعدها.

وفي هذا الإطار فقد نشر مكتب مساعدة ضحايا الجريمة بالولايات المتحدة الأمريكية في تقريره المعنون توجهات جديدة من الواقع حقوق وخدمات ضحايا الجريمة في القرن الحادي والعشرين، عددا من التوصيات التي يجب على رجال الشرطة اتباعها عند التعامل مع الضحية وهي كالآتي:

1- ضرورة إخطار الضحية شفهيا أو خطيا بحقوقه التي يكفلها له القانون، وأن تكون تلك المعلومات مناسبة للضحية من حيث اللغة والسن، وأن تحتوي تلك المعلومات على أسماء وأرقام الهواتف الخاصة ببرامج تقديم المساعدة للضحايا التي توفر خدمات الاستشارات والمعالجة والتأهيل، وذلك للاستفادة من آليات المجتمع لضمان حصول الضحايا على الخدمات المناسبة، كما يجب تقديم معلومات للضحية حول تعويضات ضحايا الجريمة، وكيفية التقديم للحصول عليها، مع الامتناع عن الحصول على أي مبالغ مالية من الضحية كتكاليف عمليات البحث عن الجاني أو الحصول على الأدلة اللازمة، بالإضافة إلى معلومات حول أمن وسلامة الضحية، وإحاطة الضحية بالعلم شفهيا بعملية التحقيق، مع اتخاذ إجراءات تسمح للضحايا باختيار شخص لمرافقتهم أثناء إجراءات التحقيق.

2- الإسراع في إرجاع الممتلكات التي يضبطها المحقق الجنائي (أجهزة حاسبات أو برامج أو أسطوانات مدمجة) مع إحاطة الضحايا حول كيفية استرجاع المضبوطات، مع قيام الجهاز الأمني بتخزين وحماية ممتلكات الضحية دون تقاضي أي رسوم، وهذا ما رسخته لجنة حقوق الإنسان بمنظمة الأمم المتحدة عقب صدور القرار رقم (1503) في عام 1946، بعد إنشائها، وذلك بتعزيز وتعميق وحماية حقوق الإنسان وحق الضحايا في استرداد حقوقهم والتعويض وإعادة التأهيل[1].

البند الثالث: حقوق ضحايا جرائم التكنولوجيا الحديثة

لضحايا جرائم التكنولوجيا الحديثة حقوقا حددتها القوانين الوطنية والمعاهدات الدولية، وهي حقوق قانونية وإنسانية، والتي يتمثل مجملها[2] في الاستجابة الفورية من قبل جهاز الشرطة والقضاء للبلاغ الذي يتقدم به الضحايا واتخاذ الإجراءات القانونية دون تأخير، حماية الضحايا وأسرهم وإزالة الضرر الذي يلحق بهم فورا، كفالة حق الضحايا في الوقوف على سير الإجراءات الجنائية والاستماع لرأيهم فيها، واحترام موقف المتضرر في الجريمة وتقدير حالته النفسية، والعمل على رفع معنوياته بالقدر الذي لا يؤثر سلبا في العدالة والسهر على حفظ الأسرار الشخصية للمتضرر من الجريمة وأسرته والجهات المتصلة به، تسهيل مهمة الضحية في حضور المحاكمات والإدلاء بشهادته ومعرفة نتائج التحقيقات والمحاكمات القضائية النهائية بالإضافة إلى حق إبلاغ الضحية بمواعيد الجلسات أو أي تعديل فيها وحق إخطاره بالقرار النهائي للمحكمة، وحق إبلاغه بقرار الإفراج المؤقت عن المتهم أو إخلاء سبيله من التهمة إضافة إلى حق المساعدة في التنقلات لمتابعة القضية التي رفعها وحق حمايته من ملاحقات وسائل الإعلام.

بناء على ما تم عرضه تجدر الإشارة إلى ضرورة تضمين مناهج على مساعدة ضحايا الجريمة، وبالأخص في مجال جرائم التكنولوجيا الحديثة وذلك لما يتعرضون له من إيذاء معنوي كبير.

---

[1] أحمد جاد منصور، الحماية القضائية لحقوق الإنسان، حرية التنقل والإقامة في القضاء الإداري المصري، دار الكتب، مصر، ط1، 1997، ص52.

[2] محمد الأمين البشري، علم ضحايا الجريمة وتطبيقاته في الدول العربية، المرجع السابق، ص156.

البند الرابع: دور الضحية في كبح الجريمة

في الأغلب الأعم من هذه الجرائم يكون دور الضحية ضئيلا وسلبيا إلى حد كبير إذ يفضل الكثير من المجني عليهم هنا إبقاء ما لحقهم من اعتداء سرا خوفا على سمعتهم أو سمعة تجارتهم، وحماية لمركزهم المالي وثقة العملاء بهم، فلا يرغبون بالكشف عن الاختراقات الحاصلة على أجهزتهم ونظم المعلومات لديهم حتى لا ينظر إلى تدابير الحماية لديهم على أنها ضعيفة غير فعالة فتسبب ضعف الثقة بالمؤسسة، وبالتالي عزوف العملاء عنها.

هنا يكون للصدفة في الكثير من الأحيان دورا أساسيا في كشف الجرائم وملاحقتها، وهذا الكلام صحيح إلى حد بعيد في بلادنا، أما في البلاد الغربية فالوعي أكبر، ولا يخشى أصحاب المؤسسات التي تم اختراقها الإعلان عن ذلك، بغية تحصيل حقوقهم، ومعاقبة المجرمين، وهو أمر يعود بالفائدة على الأجهزة القضائية، ومجموع المعتدى عليهم على حد سواء، فيما يتعلق بزيادة الخبرة وتحديد أطر الجريمة، وبالتالي وضع أفضل الحلول لمكافحتها مستقبلا.

البند الخامس: علاقة الجاني بالمجني عليه في جرائم التكنولوجيا الحديثة

يمكن القول إجمالا أن مسألة الجاني والمجني عليه هي عماد البحث الدائم في القانون الجنائي، على مستوى القاعدة الموضوعية والإجرائية على السواء، والقانون الجنائي في هذا الإطار يجعل من موضوع الجاني والمجني عليه مركز التقاء حركة المصالح الاجتماعية الاقتصادية التي يدور حولها موضوع الحماية الجنائية، على أن الأمر ليس على هذا القدر من العفوية، فيما يتعلق بتحديد منطق المسؤولية الجنائية عن الجرائم الناشئة عن استخدام الإنترنت، حيث أن المعادلة في هذا الإطار ليست كحالها في المنهج التقليدي، ذلك أن الإنترنت لم تجعل من التوصل إلى الجاني من المشكلات، بل تطور الحال فيما يبدو إلى المجني عليه الذي يعد تحديده من المشكلات الكبرى في هذا الإطار.

من هنا، فإن المجني عليه كثيرا ما يتجه إلى التقليل من شأن العدوان الواقع عليه، حيث يصور الأمر على كونه غير ذي أهمية، لاسيما إذا كان العدوان واقعا على مؤسسه تجارية أو اقتصادية تخشى إذا اعترفت به أن تفقد سمعتها التجارية أو الاقتصادية كما أن مسألة المبالغ التافهة في جرائم الاحتيال عبر الإنترنت تجعل موضع المجني عليه غير ذي أهمية بالمقارنة مع ما تم خسارته التي تتساوى في أحيان كثيرة ببعض الدنانير القليلة.

الفرع الثالث: المحل في جرائم تكنولوجيا المعلومات الحديثة (المعلومات)

البحث في موضوع جرائم تكنولوجيا المعلومات الحديثة يقود وبالتلازم إلى الحديث والبحث في مفهوم المعلومات كونها المحل الذي ينصب عليها هذا النمط من الجرائم، ونظرا لما للمعلومة اليوم من أهمية اقتصادية وسياسية واجتماعية كبيرة، حتى بات الحصول عليها ولحسن استخدامها من أبرز عوامل تقدم العديد من المؤسسات والبلدان، ومن ثم أضحى الحديث اليوم عن سلطة جديدة هي سلطة المعلومات.

البند الأول: المقصود من المعلومات

للوقوف على المقصود من المعلومات بوصفها محلا لجرائم تكنولوجيا المعلومات الحديثة نتناول بإيجاز تعريفها وتمييزها عن البيانات ومن ثم صورها.

أولا: تعريف المعلومات، مصطلح المعلومات في اللغة مأخوذة من الجذر اللغوي (علم) وعلم يعلم علما نقيض الجهل ويقال ما علمت بخبرك أي ما شعرت به[1]، وعلم بالشيء أي عرفه ويقال رجل علامة أي عالم وأعلم الفارس أي جعل له علامة[2].

ومصطلح المعلومات شائع منذ خمسينيات القرن الماضي وتم استعماله في مجالات متنوعة مما جعل له استخدامات مختلفة في الاستعمال الدارج، والمعلومات أصلها في اللغة اللاتينية دالة على شيء للإبلاغ والتوضيح أو النقل أو التوصيل، وعلى العموم فالمعلومات في أبسط تعريفاتها الاصطلاحية تعني المعطيات الأولية التي تتعلق بنشاط أو قطاع ما[3]، أو هي "المادة الأولية التي من خلالها أو بواسطتها يمكن إعداد الأفكار...، والمعلومات في ذاتها شيئا وليست فكرة"[4]، أما الأستاذ باركر؛ فقد عرفها بأنها مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل والاتصال أو التفسير والتأويل أو للمعالجة، سواء بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها أو نقلها بوسائل وأشكال مختلفة[5].

وإن كانت التفرقة لا تزال قائمة بين المعلومات والمعلوماتية، فالمصطلح الأخير يعود إلى الأستاذ Drefus Filip حينما استخدمه لتمييز المعالجة الآلية للمعلومات حيث عرفها بأنها: "علم المعالجة المنطقية للمعلومات التي تعد بمثابة دعامة المعارف الإنسانية والاتصالات في المجالات الفنية والاقتصادية، والاجتماعية، باستخدام معدات آلية"[6].

ثانيا: التمييز بين المعلومات والبيانات، تعرف البيانات بأنها تعبير عن مجموعة من الأرقام والكلمات والرموز أو الحقائق أو الإحصاءات الخام التي لا علاقة بين بعضها البعض ولم تخضع بعد للتفسير أو التجهيز للاستخدام والتي تخلو من المعنى الظاهر في أغلب الأحيان، أما المعلومات فهي المعنى الذي يستخلص من هذه البيانات[7].

ومع ذلك فإن البعض يرفض التمييز المشار إليه بالقول إن الذي يعنينا في هذا المقام هو حماية المعلومات بصفة عامة وطالما أن المعلومات هي المعنى المستخلص من البيانات فالحماية تشملهما معا، ومن ناحية أخرى قد لا تكون المعلومة مفهومة لدى متلقيها وهو ما يجعلها تخرج عن دائرة المعلومات طبقا لهذه التفرقة ورغم ذلك يكون الوصول إليها والتلاعب بها على قدر كبير من الخطورة فالذي يعنينا هو حماية المعلومات بغض النظر عن فهم محتواها، ولذلك فنحن نفضل تسمية المعلومات والبيانات في هذا المقام

---

[1] كتاب العين، الخليل بن أحمد الفراهيدي، تحقيق مهدي المخزومي، دار إحياء التراث العربي، بيروت، ط2، 2005، ص676.

[2] مختار الصحاح، محمد ابن أبي بكر ابن عبد القادر الرازي، مكتبة لبنان، لبنان، 1986، ص452.

[3] محمد علي العريان، المرجع السابق، ص36، وهو يشير إلى التفرقة بين المعلومة والفكرة، فالأخيرة يمكن اعتبارها مالا إذا كانت تشكل منهاجا أو أساسا لوضع مؤلف أو مصنف أو برنامج لحاسب آلي، أما المعلومة فهي ثمرة لمؤلف أو مصنف، إضافة إلى إمكانية تقويمها بوصفها مالا.

[4] سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الإنترنت، منشورات الحلبي الحقوقية، ط1، 2011، ص35.

[5] Donn B. Parker, Fighting Computer Crime: A New Framework for Protecting Information Op.Cit., pp27-28.

[6] محمود أحمد عبابنة، المرجع السابق، ص49.

[7] هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، المرجع السابق، ص26.

كمترادفين[1]، ولعل الانتقال إلى المعالجة التشريعية لمصطلحي البيانات والمعلومات، تشير إلى أن بعض التشريعات لم تفرق بين المصطلحين، بل واعتبرتهما مفهوما واحدا.

ثالثا: صور المعلومات، تصنف المعلومات بوصفها محلا لجرائم تكنولوجيا المعلومات الحديثة إلى المعلومات الاسمية المعلومات المتعلقة بالمصنفات الفكرية، المعلومات المباحة[2]، المعلومات السرية، المعلومات التجارية والصناعية والمعلومات العسكرية[3].

البند الثاني: عناصر المعلومات

بوصف المعلومات نتاج نشاط إنساني وجب أن يتوافر فيها كل من التحديد والابتكار والسرية والاستئثار من جهة أخرى.

أولا: عنصري التحديد والابتكار للمعلومات

1- عنصر التحديد للمعلومات: يعرف التحديد بأنه خاصية أساسية تفرض نفسها في كل شيء وبانعدامها تزول أية معلومات حقيقية، ولهذا أشار الأستاذ Catala إلى أن المعلومة -قبل كل شيء- هي تعبير وصياغة مخصصة من أجل تبليغ رسالة تبلغ أو يمكن تبليغها عن طريق علامات أو إشارات مختارة لكي تحمل الرسالة إلى الغير[4]، والمعلومات التي تفتقر إلى صفة التحديد لا يمكن أن تكون معلومة حقيقية، فالمعلومة بوصفها رسالة مخصصة للتبليغ يجب أن تكون محددة، لأن التبليغ الحقيقي يفترض التحديد، كما أن المعلومة المحددة هي التي يمكن حصرها في دائرة خاصة بها دون غيرها، بيد أن هذا التحديد يبدو أمرا ملحا في مجال الاعتداء على القيم لأن هذا التعدي يفترض دائما شيئا محددا وينبغي على هذا الشيء أن يكون بدوره محلا لحق محدد.

2- عنصر الابتكار للمعلومات: بمعنى أن تكون المعلومة غير شائعة بما يجعل من الوصول إليها سهلا ففي إطار براءة الاختراع ينبغي أن يكون الاختراع ذاته جديدا، والمعلومة غير المبتكرة هي معلومة شائعة ولا يمكن نسبتها إلى شخص محدد.

ثانيا: عنصري السرية والاستئثار للمعلومات، تشمل مايلي:

1- عنصر السرية للمعلومات: السرية صفة لازمة للمعلومة لأنها تحصر حركة الرسالة التي تحمل المعلومة في دائرة محددة من الأشخاص، لأن المعلومة غير السرية ستكون قابلة للتداول ومن ثم فإنها ستكون بمنأى عن أية حيازة، كما هو الحال بالنسبة إلى الرقم السري في البطاقات الائتمانية، ويقلل الطابع السري في الحالات المختلفة من استخدام المعلومات ويقصرها فقط على دائرة المؤتمنين عليها والذين يجدون أنفسهم في هذه الحالة منتفعين بحق الاستئثار عليها[5].

2- عنصر الاستئثار بالمعلومة: الاستئثار أمر ضروري لأنه في مجمل الجرائم التي تنطوي على اعتداء على القيم يستأثر الفاعل بسلطة تخص الغير وعلى نحو مطلق، والاستئثار في مجال المعلومات يمكن أن يرد على الولوج في المعلومة والمخصص لمجموعة

---

[1] نائلة عادل محمد فريد قورة، المرجع السابق، ص98.

[2] حنان ريحان مبارك المضحكي، الجرائم المعلوماتية، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2014، ص44 و45.

[3] محمد محمود المكاوي، المرجع السابق، ص55 و56. وهنالك تقسيم آخر للمعلومات وهو تقسيمها من حيث نوعيتها إلى معلومات شخصية ومعلومات اقتصادية أو مالية ومعلومات تجارية وصناعية ومعلومات عسكرية، وهنالك تقسيم آخر لها من حيث طبيعتها حيث تقسم إلى معلومات سرية وأخرى غير سرية. أيمن عبد الله فكري، المرجع السابق، ص29-33.

[4] سلامة محمد عبد الله أبو بكر، المرجع السابق، ص76. محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والإنترنت، المرجع السابق ص98.

[5] محمد سامي الشوا، المرجع السابق، ص157.

محددة من الأشخاص، لذا فإن الاستئثار ينظر إلى المعلومة بوصفها من قبيل الأسرار، ويمكن أن يرد الاستئثار أيضا بالنسبة لشخص بمفرده باعتباره صاحب سلطة التصرف في المعلومة، وعندئذ يكون الاستئثار لمؤلف المعلومة أو صاحبها.

المطلب الثاني: وسائل وتقنيات ارتكاب جرائم التكنولوجيا الحديثة

ولأن الأداة أو الوسيلة والتقنية التي ترتكب بواسطتها جرائم التكنولوجيا الحديثة عديدة ومتباينة، وجدنا من الضروري الوقوف على أهمها أين لعب الحاسوب، الإنترنت، الفيروسات أبرز الوسائل المعتمدة للجاني في اقترافه لجريمته، من خلال ماهيتها لما للإحاطة بها من أهمية واضحة في فهم الجوانب القانونية الخاصة بالجرائم المرتكبة بواسطتها.

الفرع الأول: الحاسب الآلي

لعب الحاسب الآلي دورا مهما منذ خمسينيات القران الماضي في ارتكاب جرائم التكنولوجيا الحديثة.

البند الأول: ماهية الحاسب الآلي ومكوناته

أولا: تعريف الحاسب الآلي، تستخدم كلمة الحاسب كمقابل للكلمة الإنجليزية computer، وتعني المنظم، وقد ابتكرها الفرنسي جاك بيري، وقد عرف القانون الأميركي الحاسب الآلي بأنه: "جهاز إلكتروني بصري كيميائي كهربائي أو جهاز إعداد معلومات ذو سرعة عالية، يؤدي وظائف منطقية حسابية أو تخزينية ويشتمل على أي تسهيل لتخزين المعلومات أو تسهيل اتصالات مباشرة مقترنة أو تعمل بالاقتران مع هذا الجهاز"[1].

ويعرف جانب من الخبراء الحاسب بأنه نظام معالجة كهربائي سريع ودقيق يستخدم في تداول البيانات ومصمم لتقبل وتخزين هذه البيانات ومعالجتها وإعطاء النتائج تبعا للبرنامج المخزن الذي يتألف بدوره من مجموعة أوامر موضحة خطوة خطوة وتستخدم كلمة نظام في دلالات عدة، وفي مجال الحوسبة تستخدم بعدة معان فوفق معناها الضيق تدل على إجراءات معينة في ماديات الحاسب مثل وحدة المعالجة المركزية (وحدة التحكم والحساب والمنطق)، أو للدلالة على برمجياته (نظام التشغيل)، وقد تستخدم بالمعنى الواسع للدلالة على الحاسب بأكمله كنظام معالجة ويراد بها في هذه الحالة مجموعة من الأجزاء المتكاملة التي تجمعها غاية مشتركة لتحقيق غرض أو مجموعة من الأغراض.

والحقيقة أن نظام الحاسب نظام متكامل يتكون من أنظمة جزئية، وهو بمجموعة أنظمته الجزئية يعتبر نظاما جزئيا في نظام أكبر منه للتحكم في مسألة معينة، كنظام التحكم بمرور الطائرات.

وعرف الحاسب الآلي أيضا بأنه: "جهاز إلكتروني يقوم باستقبال البيانات وتخزينها ومن ثم إجراء مجموعة من العمليات الحسابية والمنطقية عليها وفقا لسلسلة من التعليمات (البرامج) المختزنة في ذاكرته، ومن ثم يقوم بإخراج نتائج المعالجة على وحدات الإخراج المختلفة"[2]، فهو عبارة عن جهاز أو آلة مركبة تتكون من مجموعة من الأجهزة الإلكترونية التي تتضافر أعمالها في حل

---

[1] اسماعيل رضا، الوقاية من الجرائم الناشئة عن استخدام الحاسب الآلي، مجلة الاقتصاد الإسلامي، العدد 219، دبي، 1999، ص27.

[2] طارق عبد الله الشدي، آلية البناء الأمني لنظم المعلومات، دار الوطن للطباعة والنشر والإعلام، الرياض، 2000، ص03.

مشكلة معينة أو معالجة بيانات مطلوبة وفق برنامج، هو مجموعة من إرشادات وأوامر تعطى للحاسب ليقوم بعمليات المعالجة للمعلومات المدخلة فيه، ثم الحصول على النتائج المطلوبة[1].

ويعرف الحاسب بدلالة مكوناته بأنه مجموعة من الآلات الإلكترونية تقوم بمجموعة مترابطة ومتتالية من العمليات على مجموعة من البيانات الداخلة تتناولها بالمعالجة وفقا لمجموعة من التعليمات والأوامر الصادرة إليه، المنسقة تنسيقا منطقيا حسب خطة موضوعة مسبقا لحل مسألة معينة معرفة، بغرض الحصول على نتائج ومعلومات تفيد في تحقيق أغراض معينة، وتسمى التعليمات والأوامر جملا، ومجموعة الجمل هذه تسمى برنامجا، والشخص الذي يصمم البرنامج يسمى مبرمجا[2]، كما يعرف بأنه عبارة عن جهاز إلكتروني مصنوع من مكونات يتم ربطها وتوجيهها باستخدام أوامر خالصة لمعالجة وإدارة المعلومات بطريقة ما وذلك بتنفيذ ثلاث عمليات أساسية هي استقبال البيانات المدخلة (الحصول على الحقائق مجردة)، معالجة البيانات إلى معلومات (إجراء الحسابات والمقارنات ومعالجة المدخلات)، وإظهار المعلومات المخرجة (الحصول على النتائج)[3].

يظهر من هذه التعريف أن الحاسب الآلي ما هو ابتداء سوى آلة، لذا فلا مجال للحديث عن تركيب عقلي إلكتروني تلقائي قادر على الاختراع والابتكار كصورة قريبة للعقل البشري، فما الحاسب إلا آلة صامتة لا تؤدي أي عمل إلا بناء على مجموعة من الأوامر التي يزودها بها الفرد المختص، هذه الآلة تقوم بجملة عمليات حسابية ومنطقية، تشمل العمليات الحسابية الأربع المعروفة بالإضافة إلى اتخاذ قرارات منطقية استنادا إلى التعليمات المزودة بها، وفق ما يعرف ببرامج الحاسب الآلي، التي تزوده بطريقة تنفيذ الأوامر التي يتلقاها، كل ذلك بالاعتماد على الدوائر الكهربائية التي تضطلع بنقل الأوامر باختصارات تمثل اشارات كهربائية معينة يفهمها الحاسب الآلي.

بناء على ما تقدم يمكننا استخلاص تعريف لمفهوم الحاسب الآلي بأنه جهاز يحتوي على دوائر إلكترونية تديرها برامج حسابية ومنطقية لتشغيل البرامج المختلفة بتلقي الأوامر وإعطاء النتائج المطلوبة بسرعة خارقة وكفاءة عالية، إلا أننا نؤيد التعريف الذي أتت به موسوعة دلتا كمبيوتر في مؤلفها المعنون بالموسوعة الشاملة لمصطلحات الحاسب الإلكتروني وذلك لشموله جميع الوظائف التي يؤديها الحاسب في الحياة العملية، حيث عرفت الحاسب بأنه جهاز إلكتروني يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات إدخال بيانات أو إخراج معلومات وإجراء عمليات حسابية أو منطقية، وهو يقوم بالكتابة على أجهزة الإخراج أو التخزين، والبيانات يتم إدخالها بواسطة مشغل الحاسب عن طريق وحدات الإدخال مثل وحدة المعالجة المركزية التي تقوم بإجراء العمليات الحسابية وكذلك العمليات المنطقية، وبعد معالجة البيانات تتم كتابتها على أجهزة الإخراج مثل الطابعات أو وسائط التخزين المختلفة، وجميع العمليات التي يقوم بها الحاسب تتم في سرعة مذهلة تقترب في بعض الأحيان من سرعة الضوء.

ثانيا: مكونات الحاسب الآلي، يمكن تعريف نظام الحاسب بأنه: مجموعة من الأجهزة المترابطة والتي تعمل معا من خلال مجموعة من الأوامر والبيانات لتحقيق حل لمسألة معينة، أو أنه مجموعة من أجهزة إلكترونية تقوم بصورة أتوماتيكية باستقبال البيانات

---

[1] علي بن هادي البشري، الجهود القانونية للحد من جرائم الحاسب الآلي، الرياض، ط1، 1419هـ، ص11.

[2] محمد الفيومي، مقدمة الحاسبات، تشغيل الحاسبات الصغيرة، الحاسبات الإلكترونية وأنظمة المعلومات، المكتب الجامعي الحديث، الإسكندرية، 1998 ص07.

[3] زياد عبد الكريم القاضي، أساسيات علم الحاسوب، دار صفاء للنشر والتوزيع، عمان، 1997، ص13.

وخزنها ومعالجتها واستخراج النتائج تحت سيطرة تعليمات مخزنة فيها، ويتكون نظام الحاسب عموما من كيانين رئيسيين الكيان المادي؛ وهو مجموعة الأجهزة المادية التي يتكون منها الحاسب، أما الكيان المنطقي؛ فيتمثل بمجموعة من الأوامر أو التعليمات التي يضعها المبرمجون ليقوم الحاسب بالمهام المطلوب أداؤها، ويطلق على هذا الكيان لفظ البرمجيات، وهذه المعدات والبرمجيات لا قيمة لها دون وجود المستخدمين، وهم الأشخاص الذين يتعاملون معها تحقيقا لأهداف خاصة بهم تختلف من مستخدم لآخر.

1- الكيان المادي للحاسب: من حيث الأصل يؤدي الحاسب ثلاث عمليات رئيسية هي الإدخال، المعالجة والتخزين والإخراج، وتبعا لهذه العمليات تنقسم أجزاء الكيان المادي للحاسب إلى ثلاثة أقسام رئيسية، أما القسم الأول فيتمثل بأجهزة ووحدات نقل البيانات من خارج النظام إلى وحدة المعالجة والتخزين (الذاكرة) وتسمى أجهزة هذا القسم بأجهزة أو وحدات الإدخال، القسم الثاني يتمثل بأجهزة أو وحدات تنفيذ التعليمات والأوامر على البيانات لمعالجتها وخزنها، وهذه هي أجهزة المعالجة والتخزين وتسمى أيضا وحدة المعالجة المركزية، ويتمثل القسم الثالث في أجهزة إخراج وتسجيل النتائج من داخل نظام الحاسب إلى الوسط الخارجي الملائم وتسمى وحدات الإخراج.

ويجب أن يتضمن نظام الحاسب الآلي الكيانات المادية المذكورة للقيام بالعمليات الثلاثة الرئيسة، ولكن الحواسيب تختلف فيما بينها لا بوجود أو عدم وجود هذه الوحدات، بل بنوع الأجهزة المستخدمة لأداء عمليات الإدخال والمعالجة والإخراج.

أ- وحدات الإدخال: وتستعمل هذه الوحدات لإدخال المعلومات أو المعطيات أو البرامج المراد معالجتها من الوسط الموجودة عليه إلى ذاكرة الحاسب، وتكون وسائل الإدخال على أنواع[1]:

- وسائل تسمح بالاتصال المباشر بين الإنسان الوسط الخارجي وبين وحدة المعالجة المركزية، وتمثل لوحة المفاتيح[2] إحدى هذه الوسائل حيث يتم إدخال المعلومات من خلال المفاتيح مباشرة إلى وحدة المعالجة المركزية.

- وسائل تسمح بإدخال المعلومات بصورة غير مباشرة، ويتم بهذه الوسائل تهيئة المعلومات المراد إدخالها على وسائط معينة ومحددة بمعزل عن الحاسب أول الأمر، ثم تتم عملية الإدخال من خلال عملية وحدة إدخال ملائمة إلى وحدة المعالجة المركزية كما تشمل وحدات الإدخال كذلك الفأرة، كرة المسار، مشغلات الأقراص والماسح، بالإضافة إلى الأقراص المرنة والممغنطة والدسكات...إلخ.

---

[1] انتصار نوري الغريب، أمن الكمبيوتر والقانون، دار الراتب الجامعية، بيروت، ط1، 1994، ص16.

[2] تعتبر لوحة المفاتيح وحدة الإدخال الرئيسية في الحاسوب الأكثر انتشارا وهي تماثل الآلة الكاتبة من حيث توزيع الحروف وبعض لوحات المفاتيح تحتوي على أقل من ستين مفتاحا وبعضها الآخر يزيد على ذلك وهناك مفاتيح تؤدي وظائف خاصة مثل home وend وهي المفاتيح التي تسمح بالانتقال إلى أول الشاشة أو إلى آخرها، ومفاتيح pgup وpgdn والتي تسمح بالانتقال إلى صفحة أعلى وصفحة أسفل، ومفتاح prtse الذي يسمح بطباعة محتويات الشاشة، كما أن هناك مفاتيح الوظائف (functions keys) والتي تؤدي وظائف خاصة تتوقف على البرنامج التطبيقي المستخدم، وفي بعض لوحات المفاتيح تكون هناك أعداد إضافية (keypad) كما يوجد نوع من لوحات المفاتيح تسمى لوحة المفاتيح الحساسة للمس (touch sensitive keyboard) وهي لا تحتوي على مفاتيح متحركة ولكن عن طريق لمس مكان المفتاح فقط يتم توصيل إشارة كهربائية لإدخال الحرف المطلوب وهي تمتاز بعدم وجود فراغات وتستخدم مع العديد من أجهزة الحاسبات الصغيرة.

ب– وحدة المعالجة المركزية: تعتبر هذه الوحدة بمثابة العقل المفكر والمسيطر على عمل باقي الوحدات المكونة لجهاز الحاسب الآلي، وتقوم هذه الوحدة بمعالجة البيانات حسب التعليمات الواردة في البرنامج حيث يتم فيها جميع العمليات الحسابية أو المنطقية[1] وتتكون هذه الوحدة من وحدتين رئيسيتين:

– وحدة التحكم والسيطرة: وهي عبارة عن دوائر إلكترونية تتحكم في عمليات تنفيذ التعليمات وفي عمليات الإدخال والإخراج والتخزين والمعالجة داخل الحاسب[2].

– وحدة الحساب والمنطق: وهي الوحدة المسؤولة عن معالجة العمليات الحسابية والمنطقية، مثل المقارنات التي تسمح للحاسب بتقييم المواقف لتحويلها إلى الذاكرة أو اخراجها حسب الطلب إلى وسط مناسب للمستخدم[3].

– وحدة الذاكرة: وهي الوحدة التي تتم فيها عمليات تخزين المعلومات الواردة للجهاز أو تخزين النتائج الآتية من وحدة المعالجة المركزية، وهناك نوعان من وحدات الذاكرة **هما وحدة الذاكرة الرئيسية،** تقسم إلى قسمين، ذاكرة القراءة فقط والمعروفة اختصارا بـ (ROM)، ومن خصائص هذه الذاكرة الاحتفاظ بالبيانات والأوامر المخزنة حتى بعد انقطاع التيار الكهربائي، كما أنها لا تقبل تخزين أي بيانات بعد تصنيفها إلا بمعرفة الجهة الصانعة أو المتخصصين باستخدام أجهزة خاصة، وهذه الذاكرة تستخدم بصفة عامة لقراءة البيانات الموجودة بها فقط والذاكرة المؤقتة والمعروفة اختصارا بـ (RAM) وهذه الذاكرة تخزن فيها البيانات بصورة مؤقتة استعدادا لمعالجتها أو لتخزينها في وسائط التخزين الدائمة، أما النوع الثاني فيعرف **بوحدة الذاكرة المساعدة،** أين تعتبر هذه الوحدة وحدة ثانوية لتخزين المعلومات والبرامج إذا ما قيست بالوحدة الرئيسة، وتوجد على صور ثلاثة هي القرص الصلب، القرص المرن والأسطوانات.

ج– وحدات الإخراج: تؤدي مهمة إيصال الحاسب بالوسط الخارجي، فمهمتها هي عكس مهمة وحدات الإدخال التي كانت واسطة اتصال الوسط الخارجي بالحاسب والوسط الخارجي، في الحالتين يتمثل بالإنسان المستخدم للحاسب، فوحدات الإخراج تقوم بنقل النتائج المستخرجة من حل أو معالجة مسألة معينة من وحدة المعالجة المركزية إلى الخارج[4].

هذه بوجه عام هي المكونات المادية للحاسب تبعا لوظيفتها والغرض من استخدامها كجزء من نظام الحاسب العام، على أن يكون مفهوما أننا لم نتعرض لكل وسائط الربط بين الحواسيب وإدماج وسائل الاتصال بها، وكما ذكرنا فإنه لا بد لأي نظام من أنظمة الحواسيب أن يشتمل على هذه المكونات مع مراعاة اختلاف الوسائط المستخدمة في كل نظام للقيام بعمليات الحاسب الرئيسة، الإدخال، والمعالجة والخزن، الإخراج، ولا يتحقق نظام الحاسب من دون الكيان المنطقي، أو ما يشيع تسمياته بالبرمجيات التي أصبحت صناعة المال في حقل التقنية ومثلت أكثر مناطق الاهتمام القانوني بين مسائل تقنية المعلومات.

---

[1] محمود الزهد، محمد عثمان البشير، مقدمة في الحاسب الآلي، معهد الإدارة العامة، الرياض، 1985، ص10.

[2] محمد نزيه الدريني، مقدمة في أساسيات الحاسب الآلي، معهد الإدارة العامة، المملكة العربية السعودية، 1991، ص12.

[3] عوض منصور، مقدمة في علم الحاسب الإلكتروني وبرمجة بيسك، دار الأمل، عمان، 1991، ص04.

[4] انتصار نوري الغريب، المرجع السابق، ص17.

د- ملحقات الحاسب الآلي الرقمي الخارجية: هي الأدوات الخارجية التي ترتبط بالحاسب الآلي الرقمي من خلال أي من منافذه[1]، ويمكن تصنيفها إلى أدوات إدخال وأدوات إخراج وأدوات إدخال وإخراج.

-أدوات الإدخال: تتمثل أساسا في لوحة المفاتيح، الفأرة، الفأرة الضوئية[2]، كرة تتبع المسار التي تستخدم كبديل للفأرة الماسح الضوئي، لوحة اللمس، القلم الضوئي، آلة تصوير الفيديو الرقمية، آلة التصوير الرقمية، مكبر الصوت الصغير...إلخ[3].

-أدوات الإخراج: تظهر المعلومات من الحاسب بصريا أو سمعيا، وأدوات الإخراج البصري قد تعرض المعلومات كصور مؤقتة على الشاشة، أو كمخرجات مطبوعة، ومن أشهرها شاشة الحاسب التي تعتبر أداة الإخراج الأكثر شيوعا، فهي تنتج صورا مؤقتة من الحاسب تعرض على الشاشة، وهناك نوعان من الشاشات التي تستخدم مع الحواسيب الشخصية، منها العادية (CRT) والمسطحة (LCD) والطابعات (طابعة الليزر، الطابعات النافثة للحبر، الطابعات ذات المصفوفة النقطية...إلخ)، بالإضافة إلى وحدات الإخراج الصوتية التي تتمثل أساسا في مكبرات صوت، مضخمة، سماعات الرأس.

- أدوات الإدخال والإخراج: توجد أدوات تؤدي وظيفتي الإدخال والإخراج معا، أهمها المودم[4].

2- الكيان المنطقي للحاسب (البرمجيات): يتمثل الكيان المنطقي للحاسب في جزئه غير المادي وهو ما نسميه نحن وسائر الدراسات القانونية بالكيان المعنوي لانعدام صفته المادية، ويشيع تعبير البرامج أو البرمجيات[5] للدلالة على التعليمات والأوامر التي يضعها الإنسان المبرمج، لتوجيه الحاسب وتزويد أنظمته بآليات القيام بالمهام المتطلب منه أداؤها، فالحاسب بدون البرمجيات مجرد كتلة من السليكون والبلاستيك والمعدن فأجهزة الحاسب في وقتنا الحاضر سلعة أما البرمجيات فهي موضع الإثارة والمال، ومعدل تطورها يحدد في الحقيقة بشكل كبير آفاق تطور ثورة التقنية الحديثة برمتها[6].

وكثيرا ما يختلط في الحياة العملية بين اصطلاحي البرمجيات والبرنامج، فيطلق أحد التعبيرين ويقصد به الآخر، إلا أن اصطلاح برمجيات الحاسب اصطلاح أعم وأشمل من تعبير برنامج الحاسب، إذ يدخل في مفهوم برمجيات الحاسب أمورا أخرى غير البرنامج وإن كانت وثيقة الصلة به، مثل الوثائق والمستندات والمواد التي يطلق عليها المواد المساندة كالأقراص المرنة أو الأقراص المدمجة[7]، أما برنامج الحاسب فهو مجموعة من الأوامر والإرشادات التي تحدد لجهاز الحاسب العمليات التي يقوم بتنفيذها بتسلسل

---

[1] مصطفى محمد موسى، السيرة الذاتية للفيروسات الإلكترونية بين الوقاية والمكافحة والعلاج، دار الكتب القانونية، القاهرة، ط1، 2008، ص36.

[2] مصطفى محمد موسى، السيرة الذاتية للفيروسات الإلكترونية بين الوقاية والمكافحة والعلاج، المرجع نفسه، ص31.

[3] مصطفى محمد موسى، السيرة الذاتية للفيروسات الإلكترونية بين الوقاية والمكافحة والعلاج، المرجع نفسه، ص39.

[4] للاتصال بشبكة الإنترنت يلزم توافر جهاز حاسب مزود بمودم Modem (والذي هو عبارة عن وحدة ربط تستخدم في ارسال واستقبال البيانات عبر خطوط الهاتف وبما إن الحواسيب تتعامل مع الإشارات الرقمية digital signals بينما صممت خطوط الهاتف لتحمل الإشارات التناظرية analog signals رمي أصوات المستخدمين، فإن وظيفة المودم تحويل الإشارات العددية إلى إشارات تناظرية لنقلها عبر خطوط الهاتف) وبرمجيات الإنترنت وتسمى المتصفحات.

[5] وقد عرفت برامج الحاسب الآلي في القانون العربي النموذجي الموحد بأنها مصطلح للدلالة على جميع المكونات غير المادية لنظام الحاسب، ويشمل ذلك برامج النظام وهي البرامج اللازمة لتشغيل الحاسب وبرامج التطبيقات وهي البرامج التي تمكن من إنجاز المهام.

[6] توم فوريستر، المرجع السابق، ص224.

[7] فاروق علي الحفناوي، موسوعة قانون الكمبيوتر ونظم المعلومات، دار الكتاب الحديث، القاهرة، 2001، ص79.

وخطوات محددة، وتحمل هذه العمليات على وسيط[1] معين يمكن قراءته عن طريق الآلة وبعد ذلك يمكن للبرنامج عن طريق معالجة البيانات أن يؤدي وظائف معينة ويحقق النتائج المطلوبة منه.

تجدر الإشارة هنا أن الفقه انقسم في تعريفه لبرامج الحاسب الآلي إلى قسمين، أحدهما ضيق[2] يعتمد على التعليمات[3] التي توجه إلى الآلة فحسب ولم يذكر المستندات الملحقة ولهذا يظل التعريف ضمن التعريفات الضيقة للبرنامج[4]، والآخر واسع[5] وصف البرنامج وكذا المستندات الملحقة[6]، يتم التطرق فيه إلى التعليمات الموجهة إلى الآلة بالإضافة إلى الوصف التفصيلي للبرنامج.

فجرائم التكنولوجيا الحديثة تزداد خطورتها حينما تقع على برامج الحاسب الآلي وليس على المكونات المادية له، وذلك لقيمة ما تحتويه هذه البرامج من معلومات وبيانات جعلها تجلب انتباه واهتمام جميع الدول بتوفير الحماية القانونية اللازمة لها.

إن تجنب المشرع الجزائري وضع تعريف محدد لبرنامج الحاسب الآلي ربما هو الصواب، لأن وضع هذا الأخير في نصوص قانونية محددة يصعب معها وضع تعريف جامع مانع لها نظرا لتطوراتها المستمرة بالإضافة إلى تعديل في النصوص القانونية كل مرة لإدخال هذا المصنف المتجدد دوما، وهذا لا يعتبر قصورا أو فراغا تشريعيا.

ومن التعريفات سابقة الذكر لبرامج الحاسب الآلي، يمكن القول إنها مجموعة التعليمات والأوامر الموجهة من المستخدم إلى الحاسب الآلي التي تسمح له بتنفيذ مهمة معينة، وكذلك المستندات الملحقة التي تساعد على فهم وسهولة تطبيق هذه البرامج، كما تتمتع هذه البرامج بالحماية القانونية الدولية والوطنية، كما تعتبر المعطيات مجموعة معلومات يتم تنظيمها ومعالجتها داخل نظام المعالجة الآلية للمعطيات وتخزينها بغية استرجاعها عند طلبها، وكون المعطيات غير مادية لأنها عبارة عن نبضات إلكترونية داخل الحاسب لا يمكن لمسها نظرا إلى الأهمية البالغة للمعطيات، وما ينجر عنها من خسائر في حالة الاعتداء عليها، وجب على المشرع الجزائري حمايتها جنائيا، وذلك بإصداره عدة نصوص تضمنها قانون العقوبات الجزائري.

والجدير بالذكر أن البرمجيات تنقسم إلى نوعين: برمجيات النظم أو التشغيل وبرمجيات التطبيق أو البرمجيات التطبيقية.

أ- برمجيات النظم أو التشغيل: هي مجموعة من القواعد أو التعليمات التي تمثل النظام التشغيلي للحاسب، وتقوم هذه البرمجيات بوظيفة إجرائية حيث تسيطر على العمليات الأساسية للأداء الآلي داخل الحاسب[7]، فهي التي تمكن أجزاء الحاسب من

---

[1] يجب عدم الخلط بين برنامج الحاسب وبين الوسيط المادي الذي أفرغ عليه البرنامج (Material Object) وهو الوعاء الذي خزن أو حمل أو ثبت فيه البرنامج سواء كان الوعاء قرصا مرنا (Floppy Disk) أم قرصا مضغوطا (CD) أم شريطا ممغنطا أم رقيقة أو شريحة Chip أو ذاكرة الحاسب أيا كان نوعها أو أي وسيلة أخرى قد تخترع مستقبلا. فاروق علي الحفناوي، المرجع السابق، ص83.

[2] إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الائتمان، دار الجامعة الجديدة، الإسكندرية، 2007، ص100.

[3] رشا علي الدين أحمد علي تقي الدين، النظام القانوني لحماية البرمجيات، دار الجامعة الجديدة، مصر، 2007، ص16.

[4] روزا جعفر محمد الخامري، مشكلات الطبيعة القانونية لبرامج الحاسب الآلي، المكتب الجامعي الحديث، مصر، 2006، ص38.

[5] وصف البرنامج وهو التفسير والوصف الدقيق، وهو كل ما يساعد المستعمل على فهم البرنامج، وقد يتم ذلك كتابة أو في شكل محاضرات أو على أقراص ممغنطة، حيث تقدم شرحا مفصلا للعمليات التي تحدد تعليمات البرنامج.

[6] المستندات الملحقة: وهي مستندات لا دخل لها بالبرنامج ولا وصف هذه البرامج، بل هي مستندات موجهة لمستعمل البرنامج كدليل لإعداد البيانات وكيفية ومجال استخدام البرنامج وتطبيقه. محمود عبد الرحيم الديب، الحماية القانونية للملكية الفكرية في مجال الحاسب الآلي والإنترنت، دار الفكر الجامعي، القاهرة، 2008، ص23.

[7] انتصار نوري الغريب، المرجع السابق، ص35.

العمل معا، وبعض هذه البرمجيات يبنى داخل جهاز الحاسب، وبعضها يخزن على الأقراص المغنطة ويجب شراؤه بشكل منفصل ومن هذه البرمجيات لغات البرمجة[1] والمترجمات ونظم التشغيل.

ب– برمجيات التطبيق أو البرمجيات التطبيقية: وهي البرامج التي تبين للحاسب كيف يقوم بأعمال محددة للمستخدم فهي مصممة ومنتجة لتؤدي وظائف معينة تستجيب لاحتياجات العملاء ومتطلباتهم والبرامج التطبيقية لا تقع تحت حصر، ومن أمثلتها البرامج المستخدمة في البنوك والمؤسسات المالية لتؤدي وظائف معينة مثل مسك حسابات العملاء أو الربط بين فروع البنك[2].

ورغم وجود آلاف البرامج التطبيقية حسب حاجات المستخدمين، إلا أنها تقسم تبعا للمهام التي تؤديها إلى ثلاثة أنواع رئيسة، برامج معالجة الكلمات، وقاعدة المعطيات، وصفحات القيد التي تشبه إلى حد كبير صفحة دفتر الأستاذ في مجال المحاسبة وقد تطورت برمجيات التطبيق إلى إيجاد أنواع ثابتة منها للقيام بمهام رئيسة، لصفحات المحاسبة، وبرمجيات الفحص والتشفير...إلخ.

البند الثاني: التطور التاريخي للحاسوب

مرت مراحل تطور الحاسب الآلي بأجيال متعددة، حيث تذكر الأدبيات التاريخية أن أبرز الرواد الأوائل في مجال اكتشاف وتطوير الحاسوب هو Haward Aiken وكان أستاذ بجامعة هارفرد بإنجلترا عام 1944، إذ أدت الحرب العالمية الثانية إلى تطور واضح في مجال الحاسبات الإلكترونية واستخدامها في المجالات العسكرية، وقد كان الخطر الناجم عن العبث في استخدام الحواسيب محدودا آنذاك، وعلى العموم فيمكن تتبع مراحل تطور أجيال الحاسبات في الآتي[3]:

– الجيل الأول (1951–1959): حيث تم تطوير أول جهاز حاسوب للأغراض التجارية يدعى Universel وتم استخدام الصمامات المفرغة في صناعته، ومن خصائص حاسبات هذا الجيل أنها كبيرة الحجم وغالية الثمن وتولد حرارة عالية فضلا عن أن عمليات البرمجة تعد صعبة ومعقدة.

– الجيل الثاني (1959–1964): حاسبات هذا الجيل تميزت بظهور الترانسيستور، ويعد هذا تطورا هاما في الخزن مقارنة بالصمامات المستخدمة في الجيل الأول، مما زاد من سرعة تنفيذ العمليات الحسابية لحاسبات هذا الجيل مع انخفاض واضح في الحجم والكلفة مع استخدام لغات جديدة في البرمجة بدلا من لغة الآلة، كما شهد هذا الجيل تطورا في استخدام الأشرطة المغناطيسية كذاكرة مساعدة.

---

[1] البرمجة هي عملية كتابية أو وضع البرامج، ولغات البرمجة هي عبارة عن تدوين مجموعة خاصة من العلامات أو الرموز يعبر بها عن البرنامج، فلغات البرمجة هي لغات مصطنعة ولذلك فليس هناك حرية في التعبير كتلك التي تتميز بها اللغات الإنسانية، وهناك العديد من لغات البرمجة المستخدمة، ويتم تصميم كل منها لحل نوع خاص من المشكلات، ومن أهم لغات البرمجة المعروفة فورتران Fortran والكوبول Cobol والباسكال Pascal وسي C وجافا Java. محمد بلال الزعبي، أحمد الشرايعة، سهير عبد الله، خالدة الزعبي، الحاسوب والبرمجيات الجاهزة، المهارات الأساسية، عربي–إنجليزي، زمزم ناشرون وموزعون، عمان، ط2، 2011، ص35.

[2] فاروق علي الحفناوي، المرجع السابق، ص79.

[3] أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، الحماية الجنائية للحاسب الآلي، دراسة مقارنة، دار النهضة العربية، القاهرة، 2000 ص18 و19.

– **الجيل الثالث (1964–1970)**: شهد هذا الجيل ولادة الدوائر المتكاملة التي كان لها الأثر الكبير في تصغير حجم الحاسوب، كما زادت سرعة العمليات وانخفضت تكاليف الجهاز مع تحسين في أجهزة الإدخال والإخراج.

– **الجيل الرابع (1970–1981)**: امتاز هذا الجيل بتطوير الدوائر المتكاملة وازدادت سرعة العمليات بشكل أكبر كما تم تطوير رقائق صغيرة جدا من السيلكون تدعى المعالج الميكروي، كما تم في هذا الجيل إدخال تحسينات كبيرة على أجهزة الإدخال والإخراج.

– **الجيل الخامس (1981–1991)**: بدأ هذا الجيل بعقد مؤتمر دولي في طوكيو عام 1982 أين أعلن اليابانيون مشروع الجيل الخامس للحاسبات الإلكترونية، مع التطور الفائق للذكاء الاصطناعي وإنتاج حاسبات لها القدرة على الاستنتاج بصورة سريعة مع سرعة تصل إلى مليار عملية في الثانية باستخدام وسائل المعالجة المختلفة.

– **الجيل السادس (1992 حتى وقتنا الحاضر)**: أطلق مشروع هذا الجيل في شهر آذار 1992، ومن خصائص حاسبات هذا الجيل تقليد الدماغ البشري في محاولة لتقريب أسلوب معالجة المعلومات مع الأسلوب البشري، كما ظهر الحاسب المحمول الذي يمكن للمستخدم حمله في أي مكان في العالم والذي يعمل ببطارية شحن وله قدرة فائقة على الوصول بسهولة إلى شبكة الإنترنت فضلا عن إمكانية قيامه بعمليات واسعة من إدخال وإخراج البيانات ومعالجتها، ويمكن أن نضيف لحاسبات هذا الجيل الأجهزة الذكية ذات التقنية العالية التي تقوم العديد منها بمهام ووظائف الحاسب.

البند الثالث: أنواع أجهزة الحاسب الآلي

تتنوع صور أجهزة الحاسوب وتقسم إلى أصناف متعددة، لعل أبرزها:

أولا: من حيث وظيفتها وتركيبها، تقسم بدورها إلى الحاسوب القياسي، الحاسوب الرقمي والحاسوب الهجين[1].

ثانيا: من حيث أحجامها، تقسم إلى الحاسوب الكبير، الحاسوب المتوسط والحاسوب الصغير، وتجدر الإشارة إلى أن معظم الأفراد اليوم يميلون إلى استخدام هذا النوع من الحواسيب لصغر حجمها وانخفاض ثمنها.

البند الرابع: خصائص الحاسب الآلي وتطبيقاته

الحاسب الآلي بهذا المفهوم وتلك المكونات قادر على العمل وفق خصائص متعددة أهمها؛ السرعة في تنفيذ المهام بأسرع وقت ممكن[2]، الدقة؛ وتنصرف على جودة المهام وحسن تطبيق الجهاز لما يعطي من أوامر، ومدى قربها إلى هدف المستخدم وطلباته إضافة إلى قدرته عل تخزين الملايين من الإشارات الضوئية، ثم إمكانية استرجاعها وتحويلها إلى قوالب مفهومة، وهو ما يمكن المستخدم

---

[1] عمرو عيسى الفقي، الجرائم المعلوماتية، جرائم الحاسب الآلي والإنترنت في مصر والدول العربية، المكتب الجامعي الحديث، الإسكندرية، 2006 ص25. فضلا عن التقسيمات التقليدية المتقدمة فقد ذهب البعض إلى تقسيمها إلى حواسيب للأغراض العامة وحواسيب للأغراض الخاصة، والنوع الأول يقوم بتنفيذ مختلف العمليات التجارية والعلمية وغيرها، أما النوع الثاني فيقوم بتنفيذ عملية أو عمليات محدودة ذات هدف معين كتلك الحواسيب المستخدمة في الإنذار وما شابه، وهي غالبا ما تكون من الحواسيب الصغيرة أو المتوسطة. عماد محمد سلامة، الحماية القانونية لبرامج الحاسب الآلي ومشكلة قرصنة البرامج، دار وائل، عمان، 2005، ص30.

[2] محمد الفيومي، المرجع السابق، ص18. اسماعيل رضا، المرجع السابق، ص33.

من الوصول إلى مبتغاه بطريقة سهلة بمساعدة وسائل الاتصال الحديثة وخطوط الهاتف وظهور بيئة الإنترنت وبروتوكولاتها، فقد استطاع الحاسب الآلي أن يعطي مستخدمه قدرة على التواصل مع أي جهاز حاسب آخر ذي صلة بنظام اتصال موحد مع القدرة التفاعلية معه ومع محتوياته وعالم الإنترنت المتشعب المهام.

البند الخامس: علاقة الحاسب بجرائم التكنولوجيا الحديثة

لا يخفى على أحد مدى العلاقة الوثيقة بين استخدامات الحاسب الآلي وارتكاب جرائم التكنولوجيا الحديثة[1]، فنجد أن الحاسب الآلي يتميز بطاقة تخزينية كبيرة والسرعة العالية في كتابة البيانات المطلوبة وتحويلها إلى معلومات مع إمكانية استرجاعها وحذفها وتعديلها أكثر من مرة، وكل ذلك بفضل التقنية العالمية في الطريقة التي تسجل بها البيانات والبرامج المرتبطة بالحاسب الآلي.

من ناحية أخرى وفي إطار الجرائم المرتبطة بالحاسب الآلي نجد أنفسنا أمام مجرم محترف، على دراية بالتقنية الحديثة، قادرا على استخدام الحاسب الآلي ومعرفة ثغراته، وبعبارة أخرى فإن جرائم التكنولوجيا الحديثة يتطلب ارتكابها أن يتوافر لدى فاعلها معرفة بتقنية الحاسب[2]، وعليه يلعب الحاسب الآلي دورا مهما في جرائم التكنولوجيا الحديثة[3].

1-قد يكون الكمبيوتر هدفا أو موضوعا للجريمة[4]: ومن أوضح مظاهر اعتبار الكمبيوتر هدفا للجريمة في مجال التصرفات غير القانونية أن توجه الاعتداءات إلى معلوماته أو خدماته بقصد المساس بالسرية أو المساس بالسلامة والمحتوى، أو تعطيل القدرة والكفاءة للأنظمة للقيام بأعمالها، وهدف هذا النمط الإجرامي هو نظام الكمبيوتر وبشكل خاص المعلومات المخزنة داخله بهدف السيطرة على النظام دون أن يدفع الشخص مقابل الاستخدام، أو المساس بسلامة المعلومات وتعطيل القدرة لخدمات الكمبيوتر.

2- استخدام الحاسب الآلي كأداة لارتكاب الجريمة: في هذه الحالة لا يكون الحاسب محلا أو موضوعا للجريمة ولكن تقع الجريمة في هذه الحالة بواسطته أي أنه يستخدم كأداة لارتكابها[5]، ومن الناحية النظرية يمكن أن تقع بعض الجرائم بواسطة الحاسب مثل الجرائم التي تقع على الذمة المالية من سرقة ونصب وخيانة أمانة في عمليات السحب على الجوائز وانتهاك حرمة الحياة الخاصة[6].

يتبين أنه يمكن للحاسب الآلي أن يلعب الأدوار سالفة الذكر في آن واحد، ومثال ذلك أن يستخدم أحد مخترقي الكمبيوتر جهازه للتوصل دون تصريح إلى نظام مزود خدمات الإنترنت ومن ثم يستخدم الدخول غير القانوني لتوزيع برنامج مخزن في نظامه (أي نظام المخترق)، فهو قد ارتكب فعلا موجها نحو الكمبيوتر بوصفه هدفا (الدخول غير المصرح به) ثم استخدم الكمبيوتر لنشاط

---

[1] أسامة عبد الخالق الأنصاري، أثر تكنولوجيا المعلومات على مستقبل العلوم الشرطية، مؤتمر الشارقة الدولي لتأصيل العلوم الشرطية، مركز البحوث والدراسات بالشارقة، الإمارات، 1998، ص09 وما بعدها.

[2] David Thompson, Op.Cit., p02.

[3] محمد خليفة، المرجع السابق، ص25.

[4] إيهاب فوزي السقا، المرجع السابق، ص121.

[5] حسنين المحمدي بوادي، إرهاب الإنترنت، الخطر القادم، دار الفكر الجامعي، الإسكندرية، ط1، 2006، ص78.

[6] عفيفي كامل عفيفي وفتوح عبد الله الشاذلي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية بيروت ط1، 2003، ص23.

إجرامي تقليدي (عرض وتوزيع المصنفات المقرصنة)، واستخدم الكمبيوتر كبيئة للجريمة عندما قام بتوزيع برنامج مخزن في نظامه.

فالحاسب الآلي يلعب دورا رئيسا في ارتكاب العمل الإجرامي المعلوماتي، حيث يستطيع الجاني من خلاله الوصول إلى المعلومات والبيانات المراد الاعتداء عليها والقيام بقرصنتها أو استخدامها في مجالات أخرى، وفي المقابل يلعب دورا فعالا في اكتشاف الجريمة، فهو يستخدم الآن على نطاق واسع في التحقيق الإستدلالي لكافة الجرائم، عوضا عن جهات تنفيذ القانون التي تعتمد على النظم التقنية في إدارة المهام من خلال بناء قواعد البيانات ضمن جهاز إدارة العدالة والتطبيق القانوني.

الفرع الثاني: الوسائل الإلكترونية الذكية

اعتبرت الكثير من الدراسات أن استخدام الأجهزة الذكية والقدرة على التبادل الرقمي للمعلومات والخدمات، من أبرز الأسس المعرفية التي يقوم عليها مجتمع المعلومات، ولتوضيح هذا الدور الفعال للأجهزة في المجتمعات الحديثة والتي تتصف في الغالب –في الدول المتقدمة– بأنها مجتمعات المعلومات فإننا سوف ندرس في هذا الفرع ماهية الأجهزة الذكية وتكوينها والتقنيات الحديثة المضافة إليها والتي تعد أبرز ملحقاتها ووسيلة أداء الخدمات التي ينتفع بها مستخدمه، هذا إلى جانب إشارتنا إلى أبرز الجوانب الإيجابية والسلبية التي تعود على الفرد أو المجتمع نتيجة استخدام هذه الأجهزة.

تعتبر الأجهزة الإلكترونية الذكية أحد أشكال أدوات الاتصال، والذي يعتمد على الاتصال اللاسلكي عن طريق شبكة من أبراج البث الموزعة ضمن مساحة معينة، ومع تطورها؛ أصبحت أكثر من مجرد وسيلة اتصال صوتي بحيث أصبحت تستخدم كأجهزة كمبيوتر وتصفح الإنترنت، والأجهزة الجديدة يمكنها التصوير بنفس نقاء ووضوح الكاميرات الرقمية، وكذلك يمكن إرسال الرسائل القصيرة لأي مكان في العالم.

وتعرف الأجهزة الذكية بأنها وسيلة اتصال سمعية...، لنقل الكلام باستخدام التيار الكهربائي، كما تعرف بأنها أجهزة تفاعلية، تفهم ما يوجهه إليها مستخدميها من أوامر بسيطة، وتساعد على القيام بالأنشطة اليومية، كما أن لديها القدرة على الاتصال والمشاركة والتفاعل مع مستخدميها ومع الأجهزة الذكية الأخرى، وعلى الرغم من صغر حجمها، عادة تأتي بقدرة حسابية لعدد قليل من الجيجابايت، وأكثر الأجهزة الذكية استخداما هي الهواتف الذكية، والأجهزة اللوحية، والساعات الذكية والنظارات الذكية وغيرها من الأجهزة الإلكترونية الشخصية.

البند الأول: مكونات الأجهزة الإلكترونية الذكية

الأجهزة الذكية هي تلك الأجهزة التي تدار بواسطة أحد البرامج المعلوماتية، وبدون هذا البرنامج (الكيان المنطقي للنظام المعلوماتي للأجهزة الذكية) تصبح المكونات المادية لهذه الأجهزة والعدم سواء، فالتشابه واضح بين النظام المعلوماتي للأجهزة الذكية ونظام الحاسوب[1]، حتى أنه ظهرت بعض الأجهزة التي يصعب حاليا على وجه الدقة تصنيفها في إحدى الطائفتين (الحواسيب أم الهواتف) وهو ما نوضحه على النحو التالي:

[1] وتجدر الإشارة إلى أنه من الضروري التفرقة بين النظام المعلوماتي للحاسوب، وبين جهاز الحاسوب ذاته كمكونات صلبة والتي عرفت بأنها مجموعة متداخلة من الأجزاء لديها هدف مشترك من خلال أداء التعليمات المخزنة أو آلة حسابية إلكترونية ذات سرعة عالية ودقة كبيرة بمكنها قبول البيانات=

أولا: الأجزاء المادية، يتشابه التكوين المادي لمختلف الأجهزة الذكية أيا كان الجيل أو الطراز الذي تنتمي إليه، إذ تنقسم هذه الأجزاء إلى قسمين:

1- القسم الأول: الأجزاء الخارجية، والتي يمكن رؤيتها ومعاينتها بمجرد النظر للجهاز، ويرتبط مظهرها بطراز الجهاز والجيل الذي ينتمي إليه، ونوعية المستهلك للجهاز، وأبرز هذه الأجزاء الغطاء الخارجي وشاشة العرض (العدسة) الخاصة بالجهاز وهي عبارة عن طبقتين يتوسطهما مادة عضوية سائلة تأخذ شكل النقاط، ولوحة المفاتيح الخارجية، ويلحق بهذه الأجزاء السماعة الخارجية -السماعة العادية أو سماعة البلوتوث- والهوائي الذي يلحق ببعض الأجهزة لتقوية البث[1]، وهناك بطارية الطاقة، والشاحن اللازم لتزويد البطارية بالطاقة الكهربائية.

2- القسم الثاني: الأجزاء الداخلية، فأبرزها لوحة المعالجة الرئيسة ولوحة المفاتيح الداخلية للجهاز الذكي والسماعة والجرس وقاعدة سوكت الشحن، ويضاف إلى الأجهزة الذكية مكان خاص ببطاقة الذاكرة الإضافية وكاميرا للتصوير الفوتوغرافي والفيديو[2].

ثانيا: الأجزاء غير المادية للأجهزة الذكية، تتماثل الأجزاء المنطقية للأجهزة الذكية مع المكونات المنطقية لجهاز الحاسوب والتي يمكن التعبير عنها بأنها المعلومات المعالجة آليا سواء تمثلت في برامج تشغيل الأجهزة الذكية أو في برامج التطبيقات التي تخدم مستخدمه وتفعل خدماته سواء أعدت خصيصا من أجله أم كانت إحدى برامج تطبيقات الحاسوب القابلة للتشغيل بواسطة الأجهزة الذكية[3].

وبالتالي فإن ماهية وتعريف برامج الأجهزة الذكية لا تخرج عن المفهوم العام لبرامج الحاسوب والتي لم يستقر الفقه -القانوني أو المعلوماتي- على تعريف محدد بشأنها، إلا أنه لم يختلف الرأي حول طبيعتها فقد عرفت بأنها: "عمل ذهني يتمثل في مجموعة التعليمات والأوامر التي تستخدم في إدارة وتشغيل الأجهزة الذكية من أجل تنفيذ الأهداف المطلوبة من النظام"[4]، وتنقسم البرامج -بوجه عام- إلى نوعين؛ الأول يتمثل برامج الأساس المخصصة لتشغيل الوسائل الإلكترونية، أما النوع الثاني فيتمثل في البرامج التطبيقية على النحو السابق الإشارة إليه[5].

=وتخزينها ومعالجتها للحصول على النتائج المطلوبة. محمد أحمد فكيرين، أساسيات الحاسب الآلي، دار الراتب الجامعية، بيروت، 1993، ص07.

[1] هذا الهوائي الخارجي يتم توصيله في بعض أجهزة الهاتف المحمول والتي تحتوي علي مفتاح التوصيل بالهوائي الخارجي الذي يعمل على تقوية الشبكة في الأماكن التي تكون الشبكة بها ضعيفة.

[2] http://ngmelabdaa.own0.com/t138.topic

[3] معاذ سليمان راشد محمد الملا، المسؤولية الجنائية عن إساءة استعمال الهاتف المحمول، دارسة مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس القاهرة، 2013، ص22.

[4] ميرفت ربيع عبد العالي، عقد المشورة في مجال نظم المعلومات، أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة، 1998، ص16. محمود الربيعي، أحمد أحمد شعبان دسوقي، عبد العزيز إبراهيم الجبيري، علي ابن صالح الغامدي، المعجم الشامل لمصطلحات الحاسب الآلي والإنترنت، مكتبة العبيكان، 2001، ص391. محمد فهمي طلبة عبد المنعم يوسف بلال، محمد علي الشرقاوي، مصطفي رضا عبد الوهاب، الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، موسوعة دلتا كمبيوتر، القاهرة، 1991، ص417.

[5] طارق عفيفي صادق أحمد، الخطر محل التأمين من المسئولية المدنية في مجال المعلوماتية، أطروحة دكتوراه، كلية الحقوق، جامعة بني سويف، القاهرة 2010، ص26 وما بعدها.

أما عن المعلومات المعالجة آليا بواسطة أحد الأجهزة الذكية فهي تعد جزءا من مكوناتها، وهي مظهر من مظاهر الانتفاع بهذا الجهاز، ومن ذلك رسائل البريد الإلكتروني أو البريد النصي التي ترد أو ترسل من الجهاز الذكي والصور الرقمية ومقاطع الفيديو المخزنة على ذاكرة الجهاز، وبوجه عام تعتبر المعلومات كل ما يمكن استحداثه أو تسجيله أو بثه أو تخزينه بصيغة رقمية على الوسيط المادي (ذاكرة الحاسوب أو الأجهزة الذكية)، وبالتالي فإن قيمة هذه المعلومات يختلف بحسب نوعها وأهميتها لدى المستخدم.

البند الثاني: التقنيات والخدمات الإضافية بالأجهزة الذكية

تأتي الأهمية العملية والقانونية للأجهزة الذكية من خلال القدرات التقنية التي تمتلكها هذه الأجهزة والتي ساعدت على انتشارها بشكل ملحوظ في الآونة الأخيرة، والتي اكتسبتها نتيجة التطور المستمر في صناعتها والتي استفادت من الدراسات الحديثة في مجال المعلومات والاتصال، والتي نتج عنها ظهور بعض الأجهزة، وتأتي على رأس الخدمات المضافة للجهاز الذكي، خدمات الاتصال الصوتي وأحيانا خدمات المرئي والمتوفرة في الأجهزة الأكثر حداثة كأجيال الهاتف DCT، وخدمة مشاهدة التلفاز، ومتابعة أحوال الطقس، والتواصل عبر الرسائل النصية أو رسائل الوسائط المتعددة، والاتصال بشبكة الإنترنت[1]، إلا أننا سنحاول تناول الخدمات التي يكون لها دور في ارتكاب جرائم التكنولوجيا الحديثة كأن تكون أداة ارتكابها أو يكون مقصد الجاني حرمان المستخدم منها وذلك على النحو التالي:

1- خدمات الرسائل القصيرة الإضافية (SMS) وخدمات الوسائط المتعددة الإضافية (MMS)[2]، وخدمة (EMS)[3]، ويحصل المستخدم على الخدمتين الأخيرتين مقابل دفعه لرسم إضافي.

2- تقنية الكاميرا المدمجة، إذ نتج عن التطور في صناعة المنتجات الرقمية وربط الحاسوب المصغر أو إدماج برامجه بالعديد من الأجهزة ظهور الكثير من الأجهزة متعددة الخدمات، ومن ذلك الأجهزة الذكية التي أصبحت تحتوي على العديد من التقنيات المدمجة ومن ذلك الكاميرا الرقمية[4] التي تحظى باهتمام غالبية مستخدمي هذه الأجهزة.

ومن الحري بالقول إن الكثير من الإشكاليات القانونية المرتبطة باستخدام الأجهزة الذكية، وأبرزها الاعتداء على الحق في الخصوصية ترتبط بهذه التقنية (الكاميرا الرقمية) كتصوير الآخرين بدون إذن مسبق منهم، وتصوير المشاهد الإباحية بها أو تصوير

---

[1] سعد جاد الله الحيدر، النظام القانوني لعقد الاتصالات الحديثة، الهاتف النقال، دار الكتب القانونية، مصر، ط1، 2012، ص19.

[2] تتضمن خدمة الرسائل متعددة الوسائط (MMS) إرسال الرسائل النصية والمصورة، والملفات الصوتية، والمرئية (الفيديو) بمحتوى أكبر مقارنة بالرسائل العادية، يصل حجمه إلى 100 كيلوبايت في الرسالة الواحدة بينما لا يتعدى حجم الرسالة القصيرة العادية 140 بايت فقط.

[3] خدمة الرسائل المتطورة EMS، وهي خدمة تتيح إمكانية إرسال الرسوم البيانية الأساسية والنغمات إلى الهواتف الجوالة الأخرى المزودة بخدمة الرسائل المطورة إضافة إلى الرسائل النصية.

[4] والجدير بالذكر أن هذه الكاميرات لا تختلف عن آلات التصوير العادية من حيث المهام، إلا أنها تتميز بعدم حاجتها إلى عملية معالجة خارجية للصور الملتقطة بواسطتها كما في التصوير العادي (تحميض الفيلم الذي يحمل الصور الملتقطة)، إذ يتم تنزيل الصور الملتقطة بواسطة الكاميرا الرقمية على وسيط إلكتروني –قد يكون ذاكرة الهاتف أو ذاكرة إضافية– وغالبا ما يكون عبارة عن شريحة يطلق عليها المستشعر (Sensor)، تخزن عليه الصور على شكل أرقام (1-0)، وبالتالي فإنه يلزم لقراءة أو لإخراج هذه الصور اتصال الكاميرا بقارئ إلكتروني كشاشة مصغرة متصلة بالكاميرا ذاتها أو شاشة متصلة بجهاز الحاسوب أو الهاتف الجوال، وقد يكون هذا القارئ إحدى الطابعات.

http://lightfragrance.wordpress.com/2010/06/15/digicam

مشاهد الإيذاء المبهج الواقع على الآخرين، أو تصوير شخص ما في وضع غير لائق أخلاقيا أو اجتماعيا دون أن يدري مع نشر هذه الصور.

من الخدمات المميزة التي ساهمت في انتشار استخدام الأجهزة الذكية، تزويد هذه الأجهزة بالقدرة على الاتصال بشبكة الإنترنت، ومن أبرز أمثلة بروتوكولات اتصال مستخدم الأجهزة الذكية بشبكة الإنترنت، شبكة الوب WAP ونظام GPRS ونظام UMTS ونظام EDGE وكذلك نظام Wi-Fi، وتجدر الإشارة إلى أن إمكانيات وسرعة كل بروتوكول من هذه البروتوكولات تختلف عن الآخر من حيث سرعة الأداء والقدرة على التحميل[1]، والجدير بالذكر أن الاتجاه الحالي في نظم الاتصال يتجه إلى استغلال خدمات الاتصالات الصوتية عبر بروتوكول الإنترنت بمعني الانتقال من خدمات الأجهزة القديمة لبروتوكول الإنترنت التي تتعدد مزاياها سواء من حيث انخفاض تكلفة الاتصال أو جودة الاتصال[2].

البند الثالث: الجوانب الإيجابية والسلبية للأجهزة الذكية

يتضح من خلال العرض السابق لماهية الأجهزة الذكية ومكوناتها والتقنيات الملحقة بها مدى أهمية هذه الأجهزة في الحياة اليومية وإمكانية الاستفادة منها في العديد من أوجه الحياة وتتمتع هذه الأجهزة بجوانب إيجابية وأخرى سلبية نذكر منها ما يلي:

أولا: الجوانب الإيجابية

- الاستفادة من الأجهزة الذكية في ممارسة الأنشطة ذات الطابع التجاري وإدارة الأعمال –بوجه عام– حتى ظهر ما يسمى بالتجارة الإلكترونية عبر الجهاز الذكي، والتي تعد إحدى وسائل ترويج السلع نظرا لارتفاع أعداد مستخدمي هذا الجهاز[3] وأن الخدمات عبر الهاتف تحقق شخصية الخدمات والاهتمام بشخص العميل، إذ تتيح الهواتف الخلوية ربطا مباشرا بين الخدمة وبين شخص متلقيها، وهو ما يتيح شعورا مميزا لدى العميل بأنه محط اهتمام[4].
- ظهور ما يسمي بالبنوك الخلوية أو الصيرفة المنزلية، والتي من شأنها مساعدة عملاء البنك في الاستفادة من خدماته المصرفية عن بعد سواء كانوا موجودين في المنزل أو في أي مكان وفي أي وقت[5].
- يمكن الاستفادة من الأجهزة الذكية في مجال تقديم الخدمات الإخبارية سواء عبر خدمة الرسائل النصية أو عبر الإنترنت، هذا إلى جانب الاستعانة بالكاميرا الملحقة بها في توثيق الأحداث والصور، وقدرة بعض الأنواع من الأجهزة على استقبال

---

[1] يونس عرب، موسوعة القانون وتقنية المعلومات، المرجع السابق، ص04.

[2] http://www.itp.net/arabic/574255
http://www.aleqt.com/2010/12/26/article_483399.html

[3] بشير عباس العلاق، تكنولوجيا المعلومات والاتصالات وتطبيقاتها في مجال التجارة النقالة، المنظمة العربية للتنمية الإدارية، القاهرة، 2007 ص217-231.

[4] يونس عرب، الخصوصية وأمن المعلومات في الأعمال اللاسلكية بواسطة الهاتف الخلوي، منتدى العمل الإلكتروني بواسطة الهاتف الخلوي، اتحاد المصارف العربية، عمان، الأردن، 2001.

[5] عبد الرحيم الشحات البحطيطي، المخاطر المالية في نظم المدفوعات في التجارة الإلكترونية، كأحد التحديات التي تواجه النظم المصرفية، مجلة جامعة الملك عبد العزيز، الاقتصاد والإدارة، مجلد 21، العدد 02، السعودية، 1428هـ-2007م، ص50. رأفت رضوان، عالم التجارة الإلكترونية، المنظمة العربية للتنمية، القاهرة، 1999، ص77.

البث التلفزيوني والإذاعي، بل لقد وصل الأمر أن صارت خدمة الرسائل النصية تخدم حتى المجال القضائي أو القانوني بوجه عام فعلى سبيل المثال أطلقت لجان الفصل في منازعات الأوراق المالية بالمملكة العربية السعودية خدمة الرسائل النصية لمتابعة القضايا والتي تتيح إرسال التبليغات ومواعيد الجلسات إلى أطراف الدعاوى مباشرة على أرقام هواتفهم النقالة للمساعدة على إشعارهم وتذكيرهم بمواعيد دعاواهم المقامة لدى لجان الفصل في منازعات الأوراق المالية.

- كما يمكن لمستخدم الجهاز الذكي مراقبة منزله من على بعد، وتلقيه إنذارا من وجود حريق، كما يمكن الاستفادة منه في المراجعة الصحية، إذ تحتوي بطارية بعض الأجهزة على أجهزة استشعار من شأنها أن تنبه صاحبه حال حدوث تغيرات حيوية[1].
- تستخدم الأجهزة الذكية على قطاع واسع باعتبارها أداة للتسلية من خلال استخدامها في ممارسة الألعاب الإلكترونية خاصة عند الاتصال بمواقع التواصل الاجتماعي عبر الإنترنت[2].
- الاستفادة من الأجهزة الذكية في مجال التعليم والتدريب الإلكتروني.
- تعدت الاستفادة من الأجهزة الذكية مجرد الإبلاغ عن الجرائم –التقليدية منها أو المعلوماتية– إذ أصبح بمقدور ضحايا هذه الجرائم في العديد من الدول الاستفادة من خدمات التأهيل والدعم النفسي عبر الأجهزة الذكية.

ثانيا: الجوانب السلبية

- ظهور ظاهرة جديدة تسمي بإدمان الأجهزة الذكية[3].
- تؤثر نظم الاتصال اللاسلكية –كالهاتف المحمول– على عمل الكثير من الأجهزة الإلكترونية الدقيقة مثل الأجهزة الطبية وأجهزة الطائرات والملاحة الجوية من خلال التداخل بين إرسال الهاتف المحمول مع ذبذبات الأجهزة الإلكترونية المشار إليها الأمر الذي قد يسبب أخطارا على المرضى الخاضعين للرعاية الطبية تحت الأجهزة التي تتأثر بالموجات اللاسلكية أو كوارث للمسافرين بالطائرات، ويضاف إلى ما سبق ما أثبتته الدراسات من احتمالات إصابة مستخدم الهاتف المحمول

---

[1] معاذ سليمان راشد محمد الملا، المرجع السابق، ص42-44.

[2] شبكات التواصل الاجتماعي هي منظومة من الشبكات الإلكترونية التي تسمح للمشترك فيها –مستخدم أحد المواقع– بإنشاء صفحة ويب خاصة به يمكن ربطها بما يشاء من الصفحات الأخرى للمستخدمين إلكترونيا، وغالبا ما يكون تجمع الأفراد من خلال هذه الشبكات أساسه الاهتمام المشترك بأمر من الأمور العامة للمجتمع أو الاشتراك في إحدى الهوايات أو الإطلاع على ثقافات الآخرين، ومن الجدير بالذكر أن طبيعة الاتصال بين المستخدمين لكل شبكة من هذه الشبكات يختلف عن الاتصال والتواصل في المواقع الأخرى. وتصنف هذه المواقع ضمن مواقع الجيل الثاني للويب (ويب 2.0) وسميت اجتماعية لأنها أتت من مفهوم بناء مجتمعات، بهذه الطريقة يستطيع المستخدم التعرف على أشخاص لديهم اهتمامات مشتركة في تصفح الإنترنت والتعرف على المزيد من المواقع في المجالات التي تهمه، وأخيرا مشاركة هذه المواقع مع أصدقائه.

[3] أمجد أبو جدي، الإدمان على الهاتف النقال وعلاقته بالكشف عن الذات لدى عينة من طلبة الجامعتين الأردنية وعمان الأهلية، المجلة الأردنية في العلوم التربوية، المجلد 04، العدد 02، الأردن، حزيران 2008، ص141.

L. Torrecillas, "Mobile phone addiction in teenagers may cause severe psychological disorder." Medical studies, Vol. 14. n°03, 2007, pp11-13.

من أضرار صحية ناتجة عن الإشعاعات المنبعثة من هذه الأجهزة والتي تتراوح ما بين الإصابة بمرض السرطان، وبين مجرد شعور المستخدم باضطراب النوم أو الصداع ورؤية الكوابيس المزعجة[1].

- عدم مراعاة الذوق العام أو متطلبات الهدوء والطمأنينة في أماكن معينة مثل المساجد وقاعات المحاضرات وأثناء الاجتماعات والمناسبات الرسمية وغيرها.
- أصبح الجهاز الذكي يستخدم ليس فقد في مجال الإرهاب الإلكتروني وبث الفيروسات والتي يمكن أن تندرج في إطار النظرية العامة لجرائم التكنولوجيا الحديثة، بل استغله الإرهابيون لتنفيذ عمليات التفجير عن بعد، كما استغلته الكثير من جماعات المعارضة السياسية في عمليات التحريض السياسي.

البند الرابع: دور الأجهزة الذكية في ارتكاب جرائم التكنولوجيا الحديثة

ترتكب أفعال مؤثمة عبر تقنية الرسائل النصية المتاحة في الأجهزة الذكية وذلك من خلال كتابة الرسالة الإلكترونية غير المشروعة والمجرمة قانونا في ذاتها أحيانا، تنفيذ الجريمة من خلال استغلال التقنية الصوتية (المحادثة) الموجودة في الأجهزة الذكية وهذه الصورة الإجرامية المعروفة والأكثر انتشارا في الجرائم المتصلة بالأجهزة الذكية، ويسميها البعض جريمة الإزعاج الخلوي وجرمتها غالبية التشريعات، واستخدام ذاكرة الجهاز الذكي –أو الذاكرة الملحقة به– في تخزين المواد غير المشروعة، ارتكاب الجريمة الخلوية من خلال تقنية الكاميرا الرقمية المدمجة، بالإضافة إلى استعانة مجرم التكنولوجيا الحديثة بخدمات الإنترنت المتاحة للأجيال المتطورة من الأجهزة الذكية وخاصة عبر التطبيقات المتعلقة ببعض شبكات التواصل الاجتماعي –كفيسبوك وتويتر، وياهو...إلخ– في نشر أحد البرامج العدائية الضارة كبثه لأحد فيروسات الحاسوب أو الفيروسات المتعلقة بالأجهزة الذكية أو بث لأحد برامج التجسس.

الفرع الثالث: المايكروويف والبلوتوث

تتمثل أساسا فيما يلي:

البند الأول: المايكروويف (Microwave)

روابط المايكروويف تستخدم أسلوب الشبكات نقطة بنقطة، وهو الذي يغطي مسافات خط النظر، ويستخدم نطاق الترددات المرخصة، وتقنيات شبكات المدن المايكروويفية بطاقة عالية، تبث بإشارات ذات ترددات عالية جدا، إذ تعمل بصفتها اتصالات، بفعالية، نقطة بنقطة، والفائدة الجوهرية لاستخدام هذه الشبكات هي قلة التكلفة وسهولة انتشار هذه الموجات[2].

---

[1] أسعد فاضل منديل الجياشي، دراسة قانونية بالأضرار الناتجة عن أبراج الهاتف النقالة، مجلة الحقوق، السنة الثانية، العدد الثالث، العراق، 2010 ص141 وما بعدها.

[2] Gregory Kipper, Wireless Crime and Forensic Investigation, CRC Press, Florida, United States, 2007, p07.

البند الثاني: البلوتوث (Bluetooth)

تقنية جديدة تعتمد على نظم اتصال الراديو ذو الموجات القصيرة، لنقل البيانات في إطار المسافات القصيرة –وغالبا ما يكون في إطار يتراوح ما بين المتر والعشرة أمتار وأحيانا يصل إلى المائة متر دون الحاجة إلى استهلاك جهد كبير من الطاقة الكهربائية– سواء بين الوسائل الإلكترونية وبعضها أو بين أحد هذه الأجهزة وأحد الحواسيب الآلية أو بين هذه وبعضها، بمعنى أن هذه التقنية تمكن مستخدمي هذه الأجهزة من تبادل المعلومات والبيانات عبر موجات لاسلكية، دون الحاجة لأن تكون هذه الأجهزة في ترتيب معين –كأن تكون في ترتيب هندسي كصف واحد مثلا– إذ تكون هذه التقنية فعالة حتى ولو كانت هذه الأجهزة في غرف مختلفة طالما كانت هذه الغرف داخلة في نطاق البث[1]، وقد عرف البعض تقنية البلوتوث بأنها وسيلة ذات مواصفات عالمية تستخدم لربط كافة الأجهزة المحمولة مع بعضها البعض مثل الكمبيوتر والهاتف المحمول والكمبيوتر الجيبي والأجهزة السمعية والرقمية ليتمكن مستخدمو هذه الأجهزة من تبادل المعلومات ونقلها فيما بينهم عبر أجهزتهم.

وعرفها آخر بأنها منظومة لمجموعة من الأجهزة للاتصال فيما بينها بروابط لاسلكية قصيرة المدى وتستخدم في مختلف أجهزة الكومبيوتر المرتبطة بالشبكات المحلية وفي الأجهزة الذكية وغيرها من التقنيات اللاسلكية.

الفرع الرابع: الإنترنت

نقف في هذا الفرع على التعريف بتقنية الإنترنت وتطوره التاريخي واستخداماته كالآتي.

[1] ويرجع التطور التاريخي لتقنية البلوتوث Bluetooth لعام 1980 عندما بدأت تجارب ربط الأجهزة الإلكترونية بواسطة الاتصال اللاسلكي، للتغلب على عقبات الاتصال السلكي (الاستهلاك الإضافي للكهرباء، ورداءة الاتصال بين الأجهزة المربوطة سلكيا ببعض)، وقد كانت العقبة أمام تحقيق ذلك تكمن في غياب معايير أو أسس ثابتة ومتفق عليها من قبل جميع الشركات المنتجة للأجهزة الذكية وبالاعتماد على تقنية الأشعة تحت الحمراء (infrared) كحل أمثل لعمليات الاتصال والربط اللاسلكي، ولتحقيق ذلك قامت 30 شركة ومؤسسة تقريبا في شهر أغسطس من عام 1993 (منها HP IBM، Digital) بالعمل معا لتأسيس ما سمي بـ (IrDA: Infrared Data Association) بهدف استحداث ميثاق (بروتوكول) متفق عليه للاستخدام في عمليات نقل المعلومات اللاسلكية عبر تقنية الأشعة تحت الحمراء المشار إليها، وقد كان من المقدر لهذه التقنية الجديدة أن تصارع مع مشكلة صعبة وهي ضرورة الاتصال البصري بين الأجهزة المختلفة كشرط أساسي لإتمام عملية الربط، للأجل ذلك تم الاستعانة بشركة Ericsson لإيجاد طريقة ربط لاسلكي تحل محل الربط السلكي. كنتيجة للأبحاث توصلت كل من الشركات (Ericsson، Nokia، IBM، Toshiba Intel) إلى صياغة مجموعة من المواصفات (specifications) المتفق عليها، والتي استقت كما من المعرفة والمعلومات من الـ IRDA، انتهت هذه المواصفات إلى إيجاد وتأسيس ما يعرف بالبلوتوث. وكلمة بلوتوث (بالعربية السن الأزرق، Bluetooth in English, Blatand in Danish) أخذت من اسم ملك دنماركي (Harald Biatand) عاش في القرن العاشر للميلاد، اشتهر بمقدراته الفريدة على الاتصال مع الآخرين.

البند الأول: التعريف بالإنترنت

عرفت تقنية الإنترنت بالعديد من التسميات[1]، فقد سميت مثلا بالشبكة العنكبوتية الإلكترونية أو شبكة الشبكات[2] أو الفضاء السبراني الإلكتروني[3]، وجدير بالذكر أن مصطلح الإنترنت Internet هي مختصر لتعبير Interconnected network التي تعني الشبكة البينية، وهو اسم يدل على بنية شبكة الإنترنت باعتبارها شبكة ما بين الشبكات، ولهذا فمن الخطأ القول الشائع أن كلمة الإنترنت مكونة من المقطع Inter وهو مختصر International والتي تعني دولي[4] وكلمة Network والتي تعني شبكة وبذلك يصبح ترجمة عبارة الإنترنت (الشبكة الدولية للمعلومات)، وهو قول غير صحيح.

وعلى العموم يقصد بالإنترنت، شبكة مشاركة معلوماتية إلكترونية لوكالات حكومية وهيئات خاصة ومعاهد علمية وأفراد في كل دول العالم تقريبا عن طريق أجهزة الحاسب بمختلف أحجامها وأنواعها أو الأجهزة الذكية كالهاتف النقال، كما تعني بالمعنى الفني الدقيق، الترابط بين شبكات الحواسيب أو ما يقوم مقامها والمنتشرة في كل أنحاء العالم عن طريق الاتصال السلكي أو الاتصال اللاسلكي، وعلى العموم فقد أضحى الإنترنت بما يقدمه من خدمات أفضل وأوسع أداة للتواصل بين الأفراد والهيئات في العالم بغير التقيد بحدود المكان والزمان، وقد أضحت شبكة الإنترنت شبكة عالمية ضخمة تربط بين آلاف الشبكات المحلية (Lan) والواسعة (Wan)، وبهذا الصدد يجب عدم الخلط بين مفردتي الإنترنت والإنترانت، فالأخيرة يقصد بها نظام استخدام تكنولوجيا وبروتوكولات الإنترنت في وسط مغلق.

البند الثاني: شبكة الإنترنت والوب (WWW)

يظن الكثير من الناس بأن الإنترنت والوب شيء واحد، غير أن ذلك ليس صحيحا، لأن الإنترنت كما بينا هي عبارة عن شبكة تربط جميع شبكات الحاسوب المتصلة مع بعضها البعض، أما الوب (WWW)، فهو أحد تطبيقاتها فقط، أو إحدى الآليات التي تستعمل في الاتصال.

---

[1] يجب عدم الخلط بين الإنترنت Internet وبين الأنترانت Intranet التي تعني استخدام التكنولوجيا وبروتوكولات الإنترنت في وسط مغلق، ومثال ذلك الشركة التي تقيم شبكة الربط بين فروعها المختلفة باستخدام تقنية تصميم صفحات الإنترنت حيث يتم وضع لوائح العمل بالشركة أو أسعار بيع منتجاتها أو التطبيقات الخاصة بها، لكي يستفيد منها موظفو البيع أو أي بيانات أخرى تريد المنشأة إطلاع موظفيها عليها ولا يمكن لأي شخص خارجها الإطلاع على تلك الصفحات وكمثال على ذلك شركات الطيران.

[2] هذا المصطلح هو ذاته ما قضت به المحكمة الابتدائية لجنوب أوهايو في الولايات المتحدة الامريكية في حكمها الصادر في1997/2/3 في قضية "Compusrve وSan Ford Wallce"، وهو نفس المصطلح الذي أخذ به الأستاذ جورجيو بوفينز من جامعة بيركلي بالولايات المتحدة الأمريكية. Giorgio Bovenzi, Liabilities of System Operators on the Internet, Berkeley Technology Law Journal, Berkeley Law Admissions Office, University of California, Vol. 11, n°01, 1996 pp93-146.

[3] هو تعبير وصفه الروائي وليام جيبسون، ويقصد به العوالم الافتراضية التي تخلقها الشبكات المعلوماتية. أرنود روفر، الإنترنت، ترجمة منى ملحيس ونيبال إدلبي، الدار العربية للعلوم، ط2، ص149.

[4] عبد القادر عبد الله الفنتوخ، الإنترنت للمستخدم العربي، العبيكان للنشر، الرياض،2000، ص11.

فالإنترنت تحتوي على عدة تطبيقات ووسائل للتواصل، مثل البريد الإلكتروني E-mail والماسنجر Messenger والتي تستعمل في أفق الإنترنت، ولكنها ليست هي والإنترنت شيئا واحدا، فالإنترنت تشبه الطريق التي تكون بين المدن، في حين أن تلك التطبيقات المذكورة وعلى رأسها الوب، هي أنواع وسائل المواصلات التي تستخدم هذه البنية الأساسية، مثل السيارات أو الحافلات أو الدراجات النارية[1]، إذ يرتكز هذا النظام على بروتوكول (HTTP)[2]، أي بروتوكول نقل النصوص الترابطية، الذي يسمح بربط مواقع الوب الموصولة بالشبكة فيما بينها والتجول فيها، وهو لا يعمل إلا بواسطة برامج تصفح خاصة[3].

البند الثالث: المجتمع المعلوماتي (العالم الافتراضي)

أدى التطور التكنولوجي والاتصال بين الشبكات إلى خلق مساحة كبيرة من المعرفة، تحولت بحكم العوامل وتداخل الإنسان إلى ظهور مجتمع مبني على مفاهيم تكنولوجيا المعلومات، وبالتالي يمكن أن يعرف العالم الافتراضي أو المجتمع المعلوماتي بأنه المساحة الافتراضية التي خلقها التواصل العنكبوتي بين الشبكات والوسائل الإلكترونية المختلفة مع ما تحمله من برمجيات جعلت الآلة تنطق بمحتوياتها فتضع نفسها في خدمة الإنسان الذي لا ينفصل بدوره عن المجتمع، بل أنها عملت على إظهار الطاقات الإنسانية وهذا المجتمع تتوافر له كل مقومات الحياة، حيث انتقلت إليه رؤوس الأموال، والحركة العلمية والثقافية، وحتى مظاهر التسلية والترفيه[4].

وكانت نتيجة طبيعية لهذا التفاعل الاجتماعي أن تظهر سلبيات المجتمع وهي ظهور الجريمة وإضافة المعلوماتية إلى هذا المجتمع يمثل وضعا طبيعيا، بحسبان أن المعلومة هي موضوع هذا العالم الحديث فالآلة قامت بدور هام في استحداث قدرة جديدة جعلت من الممكن الحصول على المعلومة بشكل أكثر تحديدا، بالإضافة إلى خلق آلية محددة في التعامل الإنساني مع المعلومة فظهرت قواعد البيانات والقيمة الاستردادية للمعلومات، بالإضافة إلى ذلك فإن هذا المجتمع وما يتصف به بالفضائي قد خلق واقعا افتراضيا cyberspace أي المكان الخيالي أو الافتراضي[5]، والذي كان نتيجة الاتصال بين الحواسيب والشبكات والأنظمة الرقمية من مختلف أنحاء المعمورة، الأمر الذي أدى إلى إيجاد مجتمع لا يعرف الليل ولا النهار.

إن وجود مجتمع يختلف في نشأته وطبيعته عن المجتمعات الأخرى بعيدا عن كل ما تتصف به هذه المجتمعات ومقومات تكوينها ونشأتها، يكون حري بنا أن نتناوله بشيء من الدقة آخذين في الاعتبار أن النظرة من البداية حتى النهاية بالنسبة لهذا المجتمع تساوي شبكة الإنترنت، وهذا أهم ما يتصف به هذا العالم فإذا كانت بدايته منوطة بشبكة الإنترنت فإن نهايته مرتبطة أيضا بنهاية الإنترنت أو ما يحل محلها من تطورات مستقبلية.

---

[1] إيهاب ماهر السنباطي ميخائيل السنباطي، موسوعة الإطار القانوني للتجارة الإلكترونية، دار النهضة العربية، القاهرة، 2007، ص80.

[2] وهو اختصار لـ Hypertext Transfert Protocol. عبد الحسن الحسيني، القاموس الموسوعي في المعلومات والاتصالات والمعلوماتية القانونية مكتبة صادر، بيروت، 2004، ص408.

[3] طوني ميشال عيسى، التنظيم القانوني لشبكة الإنترنت، دراسة مقارنة في ضوء القوانين الوضعية والمواثيق الدولية، مكتبة صادر، بيروت، ط1، 2001 ص60.

[4] عمر محمد أبو بكر ابن يونس، المجتمع المعلوماتي والحكومة الإلكترونية، مقدمة إلى العالم الافتراضي، دار النهضة العربية، القاهرة، 2004، ص43.

[5] كان أول من استخدم كلمة الواقع الافتراضي cyberspace كاتب الخيال العلمي الأمريكي William GIBSON في روايته Neuromancer، التي تخيل فيها وجود شبكة كمبيوتر عالمية تسمى شبكة الماتريكس Matrix أو الشبكة الأم.

البند الرابع: الجهات المشرفة على الإنترنت

شبكة الإنترنت ليست ملكا لأحد، ومن حيث المبدأ لا توجد هيئة رسمية وحيدة –حكومية أو غير حكومية– للإشراف على الإنترنت، ذلك لأن البنية الأساسية تدار بإشراف جهات غير حكومية أخذت على عاتقها جعل الإنترنت مساحة حرة متاحة للجميع، أما الجهات التي تقوم بإدارة البنية الأساسية للإنترنت فهي الاتحاد الدولي للاتصالات ITU[1]، الذي يشرف على منظومات الاتصالات العالمية، ومنظمة ICANN[2]، وهي تشرف على أسماء المواقع وعناوينها (أسماء النطاقات).

لكي يتم تبادل ونقل البيانات والمعلومات عبر الإنترنت، يجب أن يكون لكل حاسوب أو نظام موصول بالشبكة عنوان خاص به وهو IP Address، يسمح بالتعرف عليه وتعيين مركزه، كما هي الحاجة لمعرفة عنوان المرسل والمرسل إليه في البريد العادي، ويطلق على عنوان الإنترنت IP Address تسمية عنوان البريد الإلكتروني، إذا كان يتعلق ببريد إلكتروني، ويسمي اسم النطاق إذا كان يختص بعنونة مواقع الوب.

البند الخامس: استخدامات وخدمات الإنترنت

هنالك خدمات واستخدامات متنوعة ومتعددة وربما لا يمكن حصرها لاسيما مع التطور السريع في هذه الشبكة وما يجري عليها من تحديثات تقنية وابتكار لبرامج خدمية يوما بعد يوم، ولعل من أبرز هذه الاستخدامات[3] التعليم عن بعد، الحصول على الخدمات الطبية، خدمة نقل الملفات وخدمة إنشاء المواقع الإلكترونية.

مع المزايا والخدمات للإنترنت والتي تقدم ذكرها، إلا أن هذه الشبكة شأنها شأن العديد من التقنيات الحديثة لا تخلو من العديد من العيوب والمساوئ[4]، لعل أبرزها يتمثل في إتاحة الإطلاع على المواقع الإباحية والإدمان على زيارة مواقع الإنترنت، تأثيراتها النفسية السلبية في فئة الشباب والمراهقين، كما باتت العديد من الأسرار الشخصية عرضة للانتهاك والإفشاء بل والافتضاح عن طريق برامج وتقنيات التجسس على المواقع أو الحواسيب الشخصية، كما يؤثر أيضا الإفراط في استخدام الإنترنت في فئة الأطفال من حيث تربيتهم على معلومات وأفكار افتراضية خيالية بعيدة عن التنشئة الصحيحة في ظل العالم الحقيقي واللهو عن الواجبات والفروض الدينية وأبرزها فرض الصلاة، خلق فجوة نفسية واجتماعية بين جيل تقليدي يؤثر الحفاظ على القيم الاجتماعية ولا يهتم بثقافة الإنترنت وجيل آخر من الشباب والمراهقين يعتمد اعتمادا شبه كلي على ثقافة الإنترنت، كما يؤدي استخدامات الإنترنت في جرائم خطيرة كجرائم الإرهاب وغسيل الأموال والسرقة والاحتيال وغيرها من الجرائم في صورتها المعلوماتية.

---

[1] وهو اختصار لـ International Telecommunication Union. عبد الحسن الحسيني، المرجع السابق، ص456.

[2] وهو اختصار لـ Internet Corporation For Assigned Name And Numbers. عبد الحسن الحسيني، المرجع السابق ص414.

[3] أحمد شحاتة بيومي، الجرائم الماسة بالحياء عبر وسائل الاتصال المستحدثة، أطروحة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة، 2009 ص71.

[4] وليد سمير فهيم المعداوى، المرجع السابق، ص119.

الفرع الخامس: البرامج الفيروسية

تعرف الفيروسات بأنها برنامج مكتوب بإحدى لغات البرمجة بطريقة خاصة، قادر على تكرار نسخ نفسه وله قدرة على التحكم بالبرامج الأخرى[1]، أو هو عبارة عن برنامج للحاسب الآلي يهدف إلى إحداث ضرر في نظام الحاسوب الإلكتروني وله القدرة على ربط نفسه بالبرامج الأخرى، وله القدرة على التكاثر، إذ أنه يتولد ذاتيا ويقوم بالانتشار داخل برامج الحاسوب ومواقع مختلفة من الذاكرة[2].

كما تستطيع البرامج الفيروسية تعديل البرامج غير المرتبطة بها بواسطة إدخال هيكل برمجته داخل البرامج الأخرى المستهدفة ويقوم بتنفيذ وتعديل عدد من البرامج ومنع إجراء أي تعديلات إضافية على هذه البرامج من الغير، وإدراك التعديلات التي أجريت على برنامج ما، ونستطيع القول إنه إذا لم يكن لبرنامج الفيروس هذا التأثير والقدرة فهو ليس فيروسا وإنما شيئا آخرا[3].

ومن الجدير بالذكر أن البعض يعتقد أن الملفات المحمية من الكتابة عليها لا يصيبها الفيروس، في حين أن للفيروسات إمكانية تغيير خاصية الملفات التي تم تحديدها على أنها للقراءة فقط ومن ثم الدخول إلى هذه الملفات، كما أن برنامج الفيروس يبحث دائما عن الملفات التنفيذية، فعن طريق تنفيذ هذه البرامج يستطيع الفيروس الانتشار، كما يصيب الفيروس البرامج التي لا تنفذ مباشرة عن طريق المستخدم والتي تحوي شفرة الفيروس، أما الملفات غير التنفيذية فهي لا يصيبها الفيروس الإلكتروني على الإطلاق مثل الملفات الرسومية والملفات النصية ذات الامتداد وغيرها[4].

وكان أول من فكر في فيروس الحاسوب هو جون فانيومان عام 1949 عندما طرح الفكرة الأساسية في تصميم الفيروس الإلكتروني في مقال نشر له تحت عنوان نظرية التيد الأوتوماتيكي ومفاده أن جهاز الحاسوب يمكن أن يدمر نفسه، ولم يلق هذا المقال في حينه أهمية لقلة انتشار الحواسيب[5].

وبعد انتشار الحاسبات، تبنى بعد ذلك مجموعة من العلماء نظرية جون فانيومان وطوروا أبحاثهم في هذا الاتجاه، مما أدى إلى بداية ظهور الفيروسات واستخدامها، وقد ظهرت أول نسخة من برنامج الفيروسات سنة 1959، على هيئة كود غريب يظهر في حواسيب بعض الشركات بعد عدة ساعات من العمل، ولا شك أن ظهور الشبكات سواء المحلية أم الدولية ساعد على سرعة انتشار برامج الفيروسات، محدثة أضرارا بالغة ببرامج الوسائل الإلكترونية[6].

البند الأول: خصائص الفيروسات

تمتاز الفيروسات بمجموعة من الخصائص التي تؤمن لها القيام بدورها التخريبي والمعطل ومن بين هذه الخصائص القدرة

---

[1] خالد أبو الفتوح فضالة، مدخلك إلى فيروسات الحاسب، مرض التكنولوجيا الحديثة، دار الكتب العلمية، القاهرة، ط3، 2000، ص39.

[2] عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، منشأة المعارف، الإسكندرية، ط1، 2009، ص505.

[3] مصطفى محمد موسى، السيرة الذاتية للفيروسات الإلكترونية بين الوقاية والمكافحة والعلاج، المرجع السابق، ص54.

[4] مصطفى محمد موسى، السيرة الذاتية للفيروسات الإلكترونية بين الوقاية والمكافحة والعلاج، المرجع نفسه، ص56 و57.

[5] نهلا عبد القادر المومني، المرجع السابق، ص126.

[6] أيمن عبد الحفيظ عبد الحميد سليمان، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، المرجع السابق، ص58.

على العدوى، فينتقل الفيروس من جهاز إلى آخر بسرعة كبيرة، يساعده في ذلك وجود وسائل اتصالات حديثة تربط شبكات الحاسب الآلي[1]، والملاحظ أن للفيروسات قدرة كبيرة على التخفي والخداع عن طريق الارتباط ببرامج أخرى للتمويه، كما يتمتع الفيروس بقدرة فائقة على الدخول إلى النظام والتسلل إليه واختراق كل سبل الحماية، وتجدر الإشارة إلى أن الهدف الأساسي للفيروسات هو تخريب وتعطيل البرامج، وأهم مظاهرها إبطاء جهاز التشغيل[2].

يستخدم الفيروس بشكل عام للغرض التخريبي بهدف عدواني للإطلاع على إمكانية الغير المنافس وإضعافها وتكبيده خسائر مالية ضخمة في القطاع السياسي أو العسكري أو الاقتصادي، فلا شك أن التطور العلمي والتقني أديا إلى الاعتماد على أنظمة الوسائل الإلكترونية في كافة المجالات والأنشطة، الأمر الذي يدفع بمرتكبي جرائم التكنولوجيا الحديثة إلى تدمير هذه الأنظمة مما يستوجب الوقاية منها باتباع أساليب الحماية الفنية.

كما قد يستخدم الفيروس لغرض حمائي، وذلك عن طريق حماية النسخ الأصلية للبرنامج من النسخ غير الشرعية، حيث ينشط الفيروس بمجرد النسخ وذلك من أجل حماية هذه البرامج، وقد يسلم البرنامج مع الفيروس ليقوم الأخير بتدمير البرنامج وذاكرة الحاسب إذا لم يف العميل بالتزاماته وإذا ما وفى فيقوم المنتج بإبطال مفعول الفيروس[3].

البند الثاني: أنواع الفيروسات

هنالك أنواع عديدة من الفيروسات الإلكترونية[4]، قسمت إلى فيروسات عامة العدوى وأخرى محدودة العدوى، وفيروسات التحميل وفيروسات النظام، وفيروسات مهاجمة لبرامج التشغيل وفيروسات مهاجمة لنظام التشغيل، وفي القرن الحادي والعشرين ظهرت تقسيمات أخرى؛ وهي فيروسات قطاع التشغيل وفيروسات الملفات وفيروسات خفية وفيروسات متحولة وغيرها[5]، وفيروسات المكان المستهدف داخل الكومبيوتر وتقسم إلى فيروسات قطاع الإقلاع[6]، وفيروسات الميكرو، وفيروسات الملفات[7]، وهناك فيروسات حسب المنشأ وتقسم إلى فيروسات ذات منشأ شخصي وهي التي يقوم بإنشائها محترف في برمجة وسائل التكنولوجيا الحديثة بهدف التخريب أو اللهو، وفيروسات ذات منشأ مؤسساتي تنتج من قبل المؤسسات للتجسس على أفراد معينين أو استخدامها في الدراسات الاستخباراتية[8]، وفيروسات ذات منشأ برمجي وهي الفيروسات التي تكون نتيجة خطأ برمجي أو خطأ أثناء العمل، وفيروسات حسب

---

[1] عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، الإسكندرية، ط1، 2006، ص94.

[2] محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، مصر، 2003، ص29.

[3] أمجد حسان، الفيروسات إرهابا تهدد نظام المعلومات، ملتقى الإرهاب في العصر الرقمي، المركز الجامعي بشار، 2008/06/20، مقال منشور على الموقع الإلكتروني: www.kfse.edu.sa

[4] خالد ممدوح إبراهيم، فن التحقيق الجنائي في البرامج الإلكترونية، المرجع السابق، ص127.

[5] خالد أبو الفتوح فضالة، المرجع السابق، ص151.

[6] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، أمن المعلومات الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2005، ص51. محمد محمود المكاوي المرجع السابق، ص51.

[7] محمد بن عبد الله القاسم، عبد الرحمن بن عبد العزيز الحمدان، أساسيات أمن المعلومات، مكتبة الملك فهد الوطنية، الرياض، ط2، 2008، ص28.

[8] نادية أمين محمد علي، الفيروسات وطرق الوقاية منها كوسيلة لأمن المعلومات، المؤتمر الدولي لأمن المعلومات، محافظة مسقط، عمان، 18–20 ديسمبر 2005، ص05 و06.

التأثير، فيروسات حميدة لا تأثير لها على أداء الأجهزة، ويكون عملها بفتح ثغرة في الجهاز للتنصت عليه، وفيروسات تقوم بتخريب مكونات الجهاز المادية أو الصلبة[1] وهو التغير الحاصل في برنامج التحميل الموجود في الذاكرة الدائمة والذي يمثل التعديلات في المكونات الصلبة[2].

أما عن كيفية حصول العدوى بالفيروس فله طرق عديدة منها وصول الفيروس بشكل رسالة إلكترونية آمنة ويقوم الفيروس بعد فتحها بأعمال مدمرة مثل نسخ وتعديل الملفات[3]، كما يتنقل الفيروس من حاسب إلى آخر من خلال الملفات المصابة أو عن طريق الملفات التنفيذية التي تحتوي شفرة برنامج فيروسي[4]، أو من خلال شبكات الاتصال[5]، أو عن طريق استخدام قرص مدمج مصاب بالفيروس حيث ينتقل الفيروس بمجرد تشغيل القرص المدمج...إلخ[6].

أولا: تعريف الديدان الإلكترونية، تعرف الديدان الإلكترونية بأنها برامج صغيرة قائمة بذاتها وغير معتمدة على غيرها من البرامج، صنعت للقيام بأعمال تدميرية أو لسرقة البيانات الخاصة لبعض المستخدمين أثناء تصفحهم على شبكة الإنترنت أو إلحاق الضرر بهم أو بالمتصلين معهم[7]، وتتميز الديدان بسرعة الانتشار وصعوبة التخلص منها وقدرتها الفائقة على التلون والتناسخ والمراوغة[8]، وعلى إعادة توليد نفسها، فهي تلوث كل جهاز متصل بالشبكة حيث تنتقل من ملف إلى آخر ومن جهاز إلى آخر عبر الشبكة[9]، وهي لا تعتمد على غيرها من البرامج لإصابة الوسائل الإلكترونية إلا أن لكل دودة آلية عمل، فبعضها يقوم بالتناسخ داخل الجهاز إلى أعداد هائلة، والبعض الآخر يتخصص بالبريد الإلكتروني حيث ترسل الدودة نفسها إلى جميع العناوين الموجودة في جهاز المستخدم، أو بالعمل على إرسال رسائل قذرة إلى بعض الموجودين في دفتر عناوين الجهاز باسم مالك البريد الإلكتروني مما يسبب له حرجا بالغا[10].

وتجدر الإشارة إلى أن الديدان الإلكترونية قام بصناعتها صانعو برامج الفيروس، إلا أنها تختلف عن الفيروسات في طريقة انتشارها وكذلك سرعة انتشارها، أما عن طريقة الانتشار تقوم الديدان بنشر نفسها من جهاز إلى آخر من خلال شبكة الإنترنت

---

[1] مصطفى محمد موسى، السيرة الذاتية للفيروسات الإلكترونية بين الوقاية والمكافحة والعلاج، المرجع السابق، ص61.

[2] خالد أبو الفتوح فضالة، المرجع السابق، ص74. ممدوح محمد الجنبيهي، الشركات الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2008، ص54.

[3] عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا، دراسة مقارنة، دار النهضة العربية، القاهرة، 2010، ص265.

[4] عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونية، شبكة الإنترنت وشبكة الهواتف النقالة وعبر الوسائط التقليدية والآلية والمطبوعات، دراسة قانونية مقارنة، دار الثقافة للنشر والتوزيع، عمان، ط1، 2015، ص132.

[5] عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، المرجع السابق، ص507.

[6] أيمن عبد الحفيظ عبد الحميد سليمان، استراتيجية مكافحة جرائم استخدام الحاسب الآلي، دراسة مقارنة، أطروحة دكتوراه، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، 2003، ص293.

[7] إن إنتاج أول دودة إلكترونية كان عام 1982 لاستخدامها في أعمال مفيدة من قبل شركة (Xerox carp)، للقيام بالعمليات التي تحتاج إلى التشغيل المتكرر على الحاسبات الرقمية الإلكترونية لأكثر من مرة، فتقوم الديدان بمسح الملفات الرقمية المؤقتة التي تنتهي الحاجة منها، ولكن تغير سلوك هذه الديدان وبدأت بتدمير الملفات الموجودة في الجهاز، مما دعى الشركة إلى إنتاج برنامج مضاد للفيروس للتخلص من هذه الديدان. مصطفى محمد موسى، الجهاز الإلكتروني لمكافحة الجريمة، دار الكتب القانونية، القاهرة، 2006، ص73 و74.

[8] ممدوح محمد الجنبيهي، المرجع السابق، ص61.

[9] حسن طاهر داود، الحاسب وأمن المعلومات، معهد الإدارة العامة، الرياض، 2000، ص77 و78.

[10] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، أمن المعلومات الإلكترونية، المرجع السابق، ص61.

فهي تحاول أن تصيب أكبر عدد من الأجهزة الإلكترونية[1]، عكس الفيروسات الإلكترونية التي تحتاج إلى تدخل المستخدم لنقلها من جهاز رقمي إلى آخر سواء كان هذا النقل مقصودا أم غير مقصود، فهي تصيبه عند التخزين عليه من قرص مرن مصاب بالفيروس كما يمكن أن يصاب عن طريق الإنترنت عند استقبال رسالة إلكترونية عليه مثلا.

أما عن سرعة كل منها تمتاز الديدان عن الفيروس بأن انتشارها سريع بسرعة انتشار الإنترنت[2]، ومن أمثلة تلك الديدان التي تنتشر بسرعة انتشار النار في الهشيم ما عرفت باسم تاناتوس، وكان ظهورها عام 2002 التي خلفت وراءها آثار تدميرية هائلة[3]، أما الفيروسات فإن سرعة انتشارها تساوي سرعة نقل أو تبادل المعلومات[4].

ثانيا: حصان طروادة، يعرف بأنه برنامج له القدرة على الاختفاء في البرنامج الأصلي للمستخدم وينشط عند تشغيل البرنامج الأصلي، أو هو جزء من الكود يضاف إلى البرمجيات ولا يخدم الوظائف العادية التي صنعت لأجلها هذه البرمجيات[5] ويؤدي حصان طروادة دورا تخريبيا للنظام، وتكمن خطورة حصان طروادة في عدم علم النظام المعلوماتي بوجوده حتى تحين اللحظة التي يؤدي فيها دوره التخريبي[6]، إذ يتم إدخاله إلى البرامج أثناء تصميمها أو تصنيعها من خلال إدخال دوائر سرية بشكل مباشر إلى الرقائق التي يتكون منها البرنامج الأصلي[7]، كما ويتم إدخال حصان طروادة من خلال إدخال تعليمات لغة المصدر في وقت لاحق، أو عن طريق إدخال التعليمات في لغة الآلة، وجاءت تسمية حصان طروادة من الحصان الخشبي الذي استخدمه الجنود الإغريق للدخول إلى حصن طروادة، وهذا التشبيه جاء للتدليل على خطورة البرنامج وقدرته على الخداع والمفاجئة والتضليل[8]، إذ يظهر على أنه برنامج صحيح ومفيد يؤدي الأعمال المخصص له ومن ثم يقوم بالأعمال التدميرية[9].

ويستخدم حصان طروادة في عمليات الاختراق، كاختراق البريد الإلكتروني، والاستيلاء على الأرقام السرية، وعمليات التجسس على الحسابات المالية، وبطاقات الائتمان والتنصت على المحادثات الخاصة والتجسس على خصوصيات الأفراد من خلال

---

[1] خالد بن محمد الطويل، التعامل مع الاعتداءات الإلكترونية من الناحية الأمنية، مركز المعلومات الوطني، وزارة الداخلية، ورشة العمل الثالثة (أحكام في المعلوماتية) الذي نظمه مشروع الخطة الوطنية لتقنية المعلومات، الرياض، 1423/10/19هـ. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، المرجع السابق، ص161.

[2] مصطفى محمد موسى، السيرة الذاتية للفيروسات الإلكترونية بين الوقاية والمكافحة والعلاج، المرجع السابق، ص76-78.

[3] ممدوح محمد الجنبيهي، المرجع السابق، ص61.

[4] مصطفى محمد موسى، التحري في جرائم مجتمع المعلومات والمجتمع الافتراضي، دار النهضة العربية، القاهرة، 2011، ص77.

[5] سليم عبد الله الجبوري، المرجع السابق، ص328.

[6] حسن طاهر داود، الحاسب وأمن المعلومات، المرجع السابق، ص76.

[7] حسن طاهر داود، جرائم نظم المعلومات، المرجع نفسه، ص134.

[8] عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا، دراسة مقارنة، المرجع السابق، ص242 وما بعدها.

[9] أحمد محمود مصطفى، المرجع السابق، ص234.

زرع حصان طروادة في حاسب الضحية[1]، ويستخدم في اختراق المواقع الأمنية للدول ومثال ذلك اختراق الحاسب الإلكتروني الخاص بوزارة الدفاع الأمريكية (البنتاجون)[2].

وهناك برامج تتشابه إلى حد ما مع حصان طروادة أهمها برنامج يطلق عليه اسم القنبلة الموقوتة، ويشتركان في أن كل منهما يعمل على تدمير المعلومات كما أن لهما نفس طريقة البرمجة، أما الفرق بينهما فهو في التصميم، حيث تصمم هذه القنابل بأداة مدمجة تتحرك بوقت معين، وتختلف أيضا عن حصان طروادة في كونها تكتشف من قبل برامج المقاومة للبرامج الضارة[3]، أما عن كيفية العدوى بحصان طروادة، فيكون عن طريق البريد الإلكتروني حيث يرسل وحيدا أو مع برامج أو ملفات ويقوم المستخدم باستقباله وتشغيله، أو ينتقل عند تحميل برامج من مصادر غير موثوقة، أو عند الاتصال بالشبكات سواء كانت داخلية أو شبكة إنترنت أو من خلال كتابة كوده على الجهاز نفسه فيتم تحميله بدقائق قليلة[4].

ولحصان طروادة أشكالا متنوعة والتي كانت محل اختلاف بين فقهاء القانون الجنائي، وذلك بخصوص القنابل الإلكترونية حيث اعتبرها البعض برنامجا متطفلا ضارا مستقلا بذاته، وذهب البعض إلى اعتبارها شبيهة ببرنامج حصان طروادة[5]، وذهب البعض الآخر إلى القول إن القنابل الإلكترونية ما هي إلا شكل من أشكال حصان طروادة[6].

فبالنسبة للقنبلة المنطقية هي عبارة عن جزء من رمز والذي يتم إدخاله عمدا إلى نظام برمجي ليقوم بأداء مدمر عند اجتماع شروط محددة، ومثاله عمل المبرمج على اخفاء جزء من الشيفرة لتبدأ بحذف الملفات تلقائيا إذا ما تم الاستغناء عن خدماته[7]، ونذكر من ذلك قيام أحد العاملين في إدارة المياه والطاقة في لوس أنجلوس الأمريكية بوضع قنبلة متطفلة في نظام الحاسب الآلي أدت إلى تخريب هذا النظام عدة مرات[8]، أما القنبلة الزمنية هي عبارة عن كود يتم زرعه في برنامج محدد ويتم برمجته للقيام بهجوم في موعد معين محدد سلفا وهذه المدة قد تطول أو تقصر حسب رغبة مصمم البرنامج[9]، ومثال على القنبلة الزمنية قنبلة مايكل أنجلو، التي سميت كذلك لنشاطها في يوم عيد ميلاد الفنان مايكل أنجلو في السادس من مارس، فتقوم بإتلاف قطاع بدء التشغيل على القرص

---

[1] يوسف حسن يوسف، الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، القاهرة، ط1، 2011، ص104.

[2] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي دراسة قانونية متعمقة في القانون المعلوماتي، المرجع السابق ص94.

[3] مصطفى محمد موسى، الجهاز الإلكتروني لمكافحة الجريمة، المرجع السابق، ص64.

[4] يوسف حسن يوسف، المرجع السابق، ص111.

[5] مصطفى محمد موسى، السيرة الذاتية للفيروسات الإلكترونية بين الوقاية والمكافحة والعلاج، المرجع السابق، ص64.

[6] أيمن عبد الحفيظ عبد الحميد سليمان، استراتيجية مكافحة جرائم استخدام الحاسب الآلي، دراسة مقارنة، المرجع السابق، ص303.

[7] عادل عزام سقف الحيط، المرجع السابق، ص133.

[8] عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا، دراسة مقارنة، المرجع السابق، ص253. ومن الأمثلة على هذا النوع من القنابل المعلوماتية ما حصل في ولاية لوس أنجلس الأمريكية عندما تمكن أحد الأشخاص من وضع قنبلة منطقية في نظام المعلومات الخاص بإدارة المياه والطاقة، مما أدى إلى تخريب النظام عدة مرات. محمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنت، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع الأردن، ط4، 2011، ص240.

[9] أيمن عبد الحفيظ عبد الحميد سليمان، استراتيجية مكافحة جرائم استخدام الحاسب الآلي، دراسة مقارنة، المرجع السابق، ص305.

كما تتلف جدول تجزئة القرص الصلب، وتوجد القنابل الزمنية على الخصوص في إسرائيل والولايات المتحدة[1]، ومثال على استخدام القنابل الزمنية كذلك ما قام به خبير الحاسبات الفرنسي بزرع قنبلة زمنية في حاسب المنشأ الذي يعمل فيه والذي انفجر بعد مرور ستة أشهر من فصله بدافع الانتقام[2].

الفرع السادس: برامج التجسس والقرصنة

لعل أهم برامج التجسس والقرصنة يمكن إجمالها فيما يلي:

البند الأول: البريد الإلكتروني غير المرغوب فيه

يعرف البريد الإلكتروني غير المرغوب فيه بأنه عبارة عن رسائل إلكترونية دعائية أو ترويجية يتم ارسالها عبر البريد الإلكتروني (E-Mail)، ويعود ظهور جرائم البريد الإلكتروني إلى عام 1998، وكان ذلك مرافقا لازدهار التجارة الإلكترونية عبر البريد الإلكتروني حيث تقوم الشركات التجارية في محاولة لجذب الزبائن عن طريق الدعاية لمنتجاتها على شبكة الإنترنت، وازدادت هذه الدعاية حتى أصبحت كابوسا على مستخدمي الإنترنت، وبما أن لكل خدمة حسنة سلبيات ترافقها؛ فإن سلبيات البريد الإلكتروني تتمثل بالرسائل غير المرغوب فيها، وهي تشبه رسائل الفاكس غير المرغوب فيها كما تشبه المعاكسات الهاتفية، ورسائل البريد الإلكتروني هي إما دعائية أو ترويجية للشركات، حيث تقوم هذه الشركات باستغلال البريد الإلكتروني للترويج لبضائعها، أو يتمثل في تضخيم البريد الإلكتروني من خلال إرسال عدد هائل من الرسائل المكررة والتي تؤدي إلى عدم انتظام سير النظام التقني المعلوماتي من خلال مواقع النقاش أو مواقع الوب المختلفة[3]، أو إرسال فيروسات تستهدف تخريب الأجهزة الإلكترونية التي تمثل أخطر التهديدات الممارسة ضد شبكة المعلومات والتي تؤدي إلى تلف وتدمير البيانات[4]، أو رسائل تحتوي على صور مخلة بالحياء العام، إذ يتم إرسال صور عارية للأشخاص عن طريق البريد الإلكتروني وهو ما قام به مواطن إماراتي بإرسال هذه الصور لكل مشترك يبدأ بريده الإلكتروني بـ (XXZ)[5]، أو تزوير الرسائل الإلكترونية حيث يقوم بعض الأشخاص بإرسال رسائل بأسماء أشخاص آخرين عن طريق البريد الإلكتروني لا يخرج بعضها عن نطاق التسلية، والبعض الآخر يتسم بالخطورة ويترتب عليها أضرارا بالغة[6].

البند الثاني: برامج التجسس

تعرف بأنها كل برنامج يحصل سرا على معلومات عن المستخدم عن طريق الربط بالإنترنت، خاصة بدعاوى دعائية

---

[1] عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، المرجع السابق، ص508.

[2] محمد سامي الشوا، المرجع السابق، ص171.

[3] خالد ممدوح ابراهيم، التقاضي الإلكتروني، الدعوى الإلكترونية وإجراءاتها أمام المحاكم، دار الفكر الجامعي، الإسكندرية، 2008، ص372-374.

[4] محمد محمود المكاوي، المرجع السابق، ص136.

[5] عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، ط1، 2009، ص154.

[6] نائلة عادل محمد فريد قورة، المرجع السابق، ص45.

وإعلانية، تتخذ شكل برامج مجانية أو برامج مشاركة يمكن تنزيلها من الإنترنت[1]، أو هي برامج تثبت خفية على الأجهزة للتجسس على المستخدمين أو السيطرة جزئيا على أجهزة الأفراد دون علم المستخدم، يقوم بجمع مختلف المعلومات الشخصية مثل تصفح الإنترنت، المواقع التي تم زيارتها كما وتعمل على تغيير إعدادات الكمبيوتر لتجعله أكثر عرضة للإصابة بمزيد من الفيروسات.

ويكون التجسس من برامج خارجية مبنية على أساس العميل والخادم، إذ يعمل برنامج الخادم داخل النظام للهدف حتى يتمكن الهاكر من الاتصال عن طريقه لتبدأ عملية التجسس، وقد ظهرت برامج كثيرة للتجسس على أنظمة ويندوز ولينكس[2] من خلال فتح منفذ في الجهاز المستهدف، ثم استقبال الأوامر من خلال هذا المنفذ، ومن ثم تنفيذ هذه الأوامر[3] لإتمام أعمال التجسس بالدخول إلى حواسيب أجهزة الدولة، أو للتجسس على بطاقات الائتمان وأرقام الحسابات وسرقة مختلف البيانات[4].

أما عن طريقة زرع برامج التجسس في جهاز الضحية فيكون عند زيارة المواقع المجهولة، أو من خلال البريد الإلكتروني، أو من خلال برامج المحادثة الشهيرة[5]، ومثال على ذلك برنامج التجسس (ICQ)[6] الشهير للتجسس، حيث ينتقل إلى جهاز الضحية من خلال الطلب منه أن يضع بياناته على الخادم الخاص بالبرنامج وعند الانتهاء من ملء البيانات يعطي للمستخدم رقما خاصا به مثل رقم التليفون والذي يكون وسيلة للاتصال بالخادم يتيح هذا الرقم لباقي مستخدمي الإنترنت ملاحظة وجود المستخدم على الشبكة بمجرد دخوله[7].

---

[1] ذيب بن عايض القحطاني، أمن المعلومات، مدينة الملك عبد العزيز للعلوم والتقنية، الرياض، 2015، ص222.

[2] www.bolsadesantiago.com.

[3] نهلا عبد القادر المومني، المرجع السابق، ص218.

[4] www.bolsadesantiago.com.

[5] نهلا عبد القادر المومني، المرجع السابق، ص219.

[6] وهو برنامج محادثة للتجسس من صنع إسرائيل.

[7] أيمن عبد الحفيظ عبد الحميد سليمان، استراتيجية مكافحة جرائم استخدام الحاسب الآلي، دراسة مقارنة، المرجع السابق، ص316.

الفصل الثاني: أهم الجرائم المرتكبة باستخدام وسائل التكنولوجيا الحديثة

أصبحت الجريمة في عصرنا الحاضر ترتكب بأساليب علمية متطورة ابتداء من مرحلتي التخطيط والإعداد مرورا بمرحلة التنفيذ وصولا إلى مرحلة التضليل والتمويه للهرب من وجه العدالة[1]، فباتت أفعالها تتسم بالتداخل والتشابك والاستفحال، وتعقد الأحداث الإجرامية إلى درجة أضحى معها النشاط الجرمي يتضمن أحداثا وأنشطة جرمية لم يكن المجرم نفسه يتوقعها كما لم تكن في حسبانه عند تخطيطه لجريمته.

وقد أصبح متاحا أمام المجرم أن يستعمل أدوات كثيرة تساعده في ارتكاب جرائمه التقليدية عينها وغيرها من الجرائم المستحدثة التي ما كان المجتمع يعرفها قبل الوصول إلى المستوى العالي من التكنولوجيا الذي أضحى عليه اليوم، من هنا تعددت جرائم التكنولوجيا الحديثة وتصنيفاتها، فقد أوجد مشروع الاتفاقية الأوروبية تقسيما جديدا نسبيا، تضمن أربع طوائف رئيسية لجرائم التكنولوجيا الحديثة، وهي الجرائم التي تستهدف العناصر السرية والسلامة (الدخول غير القانوني، الاعتراض غير القانوني، تدمير المعطيات، اعتراض النظم، إساءة استخدام الأجهزة)، والجرائم المرتبطة بالكمبيوتر (التزوير والاحتيال)، الجرائم المرتبطة بالمحتوى (الجرائم المتعلقة بالإباحية والأخلاقية)، إضافة الجرائم المرتبطة بالإخلال بحق المؤلف والحقوق المجاورة، قرصنة البرمجيات.

كما أن الأستاذ Ulrich Sieber صنف هذا النوع من الجرائم إلى ثلاث طوائف رئيسية، الأولى تحت عنوان جرائم الحاسب الآلي الاقتصادي (الاحتيال المعلوماتي، التجسس المعلوماتي، الإتلاف المعلوماتي، الدخول غير المصرح به إلى نظام الحاسب الآلي)، الثانية؛ جرائم الاعتداء على حرمة الحياة الخاصة، أما الثالثة؛ الجرائم التي تهدد المصالح القومية والسلامة الشخصية للأفراد[2].

صنفت منظمة التعاون الاقتصادي والتنمية جرائم التكنولوجيا الحديثة إلى الطوائف التالية: الأولى استغلال وقرصنة برامج الحاسب الآلي تجاريا، والثانية الدخول أو الاعتراض غير المصرح به لنظام الحاسب الآلي، والاستعمال غير المصرح به لنظام الحاسب الآلي، والثالثة تعديل أو محو معلومات موجودة بالفعل على نحو غير مشروع لتحويل الأموال أو الممتلكات التي تمثلها هذه المعلومات[3] وفي هذا الإطار وضع مشروع القانون النموذجي لجرائم الكمبيوتر والإنترنت عام 1998 تصنيفا من قبل فريق بحثي أكاديمي والمسمى (Model State Computer Crimes Code)، وفي نطاقه تم تقسيم هذه الجرائم إلى الجرائم الواقعة على الأشخاص والجرائم الواقعة على الأموال عدا السرقة، وجرائم السرقة والاحتيال، وجرائم التزوير، وجرائم المقامرة والجرائم ضد الآداب، عدا الجرائم الجنسية، والجرائم ضد المصالح الحكومية، ويلاحظ أن التقسيم يقوم على فكرة الغرض النهائي أو المحل النهائي الذي يستهدفه الاعتداء، كما أن البعض صنف جرائم التكنولوجيا الحديثة تبعا لنوع المعطيات ومحل الجريمة، أو تبعا لدورهما في الجريمة.

---

[1] محمد محمد عنب، استخدام التكنولوجيا الحديثة في الإثبات الجنائي، مطبعة السلام الحديثة، الاسماعيلية، 2007، ص56.

[2] Ulrich Sieber, The International Handbook on Computer Crime: Computer-related Economic Crime and the Infringements of Privacy, Wiley, 1986, pp03-06.

[3] الموقع الرسمي لمنظمة التعاون الاقتصادي والتنمية، وقد صدر هذا التصنيف سنة 1986 من قبل لجنة شكلت لدراسة الجريمة المعلوماتية، وقد صدر التقرير بعنوان جرائم الحاسب الآلي (تحليل للأنظمة القانونية المختلفة) www.oecd.com.

إلا أن هذه التصنيفات كلها إما صنفت جرائم الحاسوب، أو جرائم الحاسوب والإنترنت، ولم تلحظ تصنيفا مختصا بجرائم التكنولوجيا الحديثة، وعليه سنحاول دراسة هذا الفصل في المبحثين التاليين:

المبحث الأول: جرائم التكنولوجيا الحديثة المتعلقة بتقنية الاتصالات الحديثة

المبحث الثاني: جرائم التكنولوجيا الحديثة ذات الصبغة المالية

المبحث الأول: جرائم التكنولوجيا الحديثة المتعلقة بتقنية الاتصالات الحديثة

إن وجود وسائل اتصالات جديدة مستحدثة قائمة على الاتصالات البعدية مع القدرة على إجراء الاتصالات بين نهايات طرفية لا محدودة، ووجود القدرة على الاتصال بهوية مصطنعة كل ذلك ترك بيد الجناة مبررات تدفعهم أكثر فأكثر نحو عالم الإجرام والشر خصوصا مع القدرة التقنية العالية على إيقاع الفعل وإخفاء الهوية الحقيقية للفاعل إلى حد ما، فقد مهدت شبكة الاتصالات العالمية الإنترنت الطريق أمام إجرام من نوع جديد يقع لذات الغايات التقليدية ولكن هنا بأسلوب أكثر خفة وأعظم أثر، وعلى نحو يصعب معه إدراك الفعل وتحديد الفاعل، وامتد الإجرام باستغلال الاتصالات المعلوماتية إلى حد الاعتداء على القاصرين بشتى صنوف الإجرام والتهويل.

فبعد أن وقفنا في الفصل السابق على المقصود من جرائم التكنولوجيا الحديثة وخصائصها والمقصود من مرتكبها وتصنيفاته ومن ثم ماهية المعلومات ثم التطرق إلى مفهوم الوسائل الإلكترونية والإنترنت، نتناول في هذا الفصل الجرائم المتعلقة بتقنية الاتصالات الحديثة، أي الجرائم الواقعة على المعطيات أو المكونات المعنوية والمنطقية للوسائل الإلكترونية (البيانات والبرامج والمعلومات) والإنترنت وذلك بسرقتها أو إتلافها أو إعاقتها عن عملها، أو تعديلها أو تحريفها أي تزويرها، أو الاستخدام غير المصرح به لها، ومن هنا فإن أبرز الجرائم التي نتناولها في هذا الفصل هي السرقة المعلوماتية والإتلاف المعلوماتي وإعاقة النظام المعلوماتي والتزوير المعلوماتي والاستخدام غير المصرح به للنظام المعلوماتي وجريمة خيانة الأمانة في المجال المعلوماتي والجرائم الواقعة على البيانات الشخصية المخزنة معلوماتيا.

ولكن قبل أن نتناول هذه الجرائم المستحدثة نشير إلى أن الأفعال المادية التي لا تقع على المكونات المنطقية للأجهزة الإلكترونية والإنترنت، كإتلاف أجهزة الكومبيوتر أو سرقتها أو تعطيل مكوناتها المادية عن العمل، أو تزوير أوراق ووثائق ملكيتها وما شابه ذلك من صور الجرائم التقليدية التي تخضع للنصوص التقليدية في قوانين العقوبات لانتفاء محل الجريمة المعلوماتية وهو المعلومات أو البيانات أو البرامج. ولذا ولما أدخلته تقنية الاتصالات من تطور على مفهوم الجريمة ووسائلها نعالج تاليا أهم صور الجرائم المتعلقة بتقنية الاتصالات الحديثة.

المطلب الأول: جرائم الاعتداء على الحياة الخاصة للأفراد

عرف العالم مع بدايات النصف الثاني في القرن الماضي تطورا مذهلا في المجال العلمي والتقني والتكنولوجي والرقمي لاسيما في مجال تكنولوجيات الإعلام والاتصال وذلك بسبب ظهور الإنترنت والمواقع الإلكترونية ووسائل أخرى حديثة ومتطورة، وعليه فالتكنولوجيا والتطور العلمي والتقني مهما كان نوعه يمكن أن يكون سلاح ذو حدين، الأمر الذي دفع بالمشرعين لتنظيم هذه

المجالات بما يخدم حقوق الإنسان بمختلف أنواعها لا الاعتداء عليها، وتأطير كل طرق استخداماتها، لاسيما استخدام الإنترنت كأحدث وسيلة في مجال الاتصال والتواصل ونخص بالذكر مواقع الإنترنت أو مواقع التواصل الاجتماعي والتصدي لما ينتج عنها من مساس بالحقوق الخاصة للأفراد[1].

وعليه فإن تطوير الحواسيب الرقمية والأجهزة الذكية وتكنولوجيا الشبكات، وبشكل خاص الخدمات على مواقع الإنترنت أتاح نقل النشاط الاجتماعي والتجاري والسياسي والثقافي والاقتصادي من العالم المادي إلى العالم الافتراضي أي البيئة الإلكترونية ويوما بعد يوم تتكامل الشبكات العالمية للمعلومات مع مختلف أنشطة الحياة، وبنفس الوقت فإن التطور الثقافي في توظيف التقنية رافقه توجه واسع بشأن حماية خصوصية الأفراد.

ففي العالم الرقمي وعالم شبكات المعلومات العالمية، يترك المستخدم آثار ودلالات كثيرة تتصل به بشكل سجلات رقمية حول الموقع الذي زاره والوقت الذي قضاه على الشبكة، والأمور التي بحث عنها والمواد التي قام بتنزيلها والوسائل التي أرسلها والخدمات والبضائع التي قام بطلبها وشرائها أو التي قام بعرضها والدعاية لتسويقها، وهي سجلات تتضمن تفاصيل دقيقه عن شخصية وحياة وهوايات وميول المستخدم الشخصية على الشبكة وهي سجلات مؤتمتة ذات محتوى شخصي يتصل بالفرد، إذ ينتج عن التصفح والتجول عبر الإنترنت أن الفرد يترك لدى الموقع المزار كمية واسعة من المعلومات الشخصية على الرغم من أن جزءا من هذه المعلومات فقط لازم لإتاحة الربط بالإنترنت والتصفح، وبمجرد الدخول إلى صفحة الموقع فإن معلومات معينة تتوفر عن الزبون وهي ما يعرف بمعلومات رأس الصفحة، وهي التي يزودها الكمبيوتر المستخدم للكمبيوتر الخادم الذي يستضيف مواقع الإنترنت وهذه المعلومات قد يكون في استخدامها أثرا سلبيا على عدة مستويات وأهمها على مستوى حقوق صاحبها بصفة خاصة وحقوق الإنسان عموما رغم الإيجابيات المتعددة التي يمكن إحصاؤها من جراء التعامل بالآليات والتقنيات التكنولوجية المتطورة.

في ظل هذا كله لم تكن الحياة الخاصة للأفراد عبر تقنية نظم المعلومات بعيدة عن فرص التمتع بمزايا عصر العولمة التقنية وثورة الاتصالات ونظم المعلومات، بل أصبحت الحياة الخاصة بكافة مفرداتها جزءا من هذا النظام، مع ما يحمله في طياته تجاهها من حسنات عديدة أو مساوئ يأتي الحديث عنها لاحقا، فبعد أن كانت مؤسسات الدولة والشركات الخاصة ذات الاتصال الوثيق بالفرد ومؤسسات الخدمات ومكاتب المهنيين الذين يقدمون خدماتهم بتكرار للفرد داخل المجتمع، كالمحامين والصيادلة والأطباء ومؤسسات الضمان الاجتماعي تعمل بمنظومات تقليدية قوامها الورق والأخبار، ووسائلها النقل المادي والمناولة المباشرة فقد هجرت تلك المؤسسات سجلاتها التقليدية الورقية منها وغيرها، وأصبحت تستخدم الوسائل الإلكترونية، أهمها، الحاسب الآلي وأنظمته وبرامجه وسيلة لتثبيت ومعالجة وتخزين بيانات العملاء والزبائن والمراجعين الشخصية منها والمهنية والإحصائية.

فإذا ما تصورنا هذا الكم الهائل من البيانات والمعلومات الشخصية الموجودة على هذه الوسائل الإلكترونية كجهاز الحاسب الآلي، وتصورنا إمكانية الربط الإلكتروني بين الأجهزة الحاوية للمحتوى التقني من تلك المعلومات والبيانات حول العالم، وضمن منظومة شبكة الإنترنت، أو شبكات تقنية نظم المعلومات الداخلية الأخرى، كان لنا أن نتصور إلى أي حد أصبحت فيه حياة

[1] نوارة حسين، آليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة إلكترونيا، الملتقى الوطني حول آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 29 مارس 2017.

الناس الخاصة عرضة لمخاطر السلوك التقني السلبي الذي يستهدفها، ومن ذلك تحديدا الإطلاع والإفشاء والتعديل وغيرها الكثير الكثير الذي يتطور ويظهر مع كل تقدم في مجال تقنيات نظم الاتصالات والمعلومات، وبالتالي أصبحت تقنية نظم المعلومات تعطي للأفراد المنحرفين ذوي النزعات الجرمية سببا لارتكاب جرائم قد لا يمكن حصرها.

وفي الوقت الذي لا ننكر فيه مزايا تقنية أنظمة المعلومات على الحياة الخاصة تسهيلا لحياة الناس وتوسيعا لقدرات وميزات الاستفادة من المكان والزمان، فإننا لا نخفي تخوفا يشاطرنا به أغلب المطلعين على الحجم الهائل من المواد الإلكترونية المتعلقة بحياة الناس والمخزنة ضمن شبكات اتصالات مفتوحة، هذه المخاوف تجد أساسها في عدة أمور نذكر منها، السعة التخزينية الضخمة للوسائل الإلكترونية في كل ما يتعلق بالحياة الخاصة للناس ثم السعة اللامتناهية لشبكة الربط المعلوماتي العالمية (الإنترنت)، وتحقق الربط البعدي لجهازي حاسب آلي أو أكثر عبر العالم ثم قدرة العقل على اختراق نظم الاتصالات بطريقة أو بأخرى، والوصول إلى مكان وجود البيانات والمعلومات ذات العلاقة بالحياة الخاصة للأفراد حيثما وجدت، ومنه إيقاع الضرر بها بصور وأشكال تبد ومختلفة على القوالب التجريمية التقليدية المعروفة.

وقبل الحديث عن مظاهر الإجرام المتعلقة بالحياة الخاصة للأفراد، سنبحث تاليا مفهوم الحق بالحياة الخاصة، ثم مفهوم السر الخاص المستحق للحماية الجزائية في عالم البيئة الرقمية.

الفرع الأول: مفهوم الحق بالحياة الخاصة في عالم البيئة الرقمية

حق الشخص في الحياة قاعدة من قواعد الشريعة الإسلامية، وحقه في خصوصية حياته أساسها، فحرمت كل أشكال المساس بها أو الاعتداء عليها، فجعلت حمايتها من الواجبات والامتناع عن إيذائها من المفروضات، كما عنت المواثيق والدساتير في مختلف دول العالم ومنذ نشأة المجتمع المستحدث والدولة بسلطاتها الثلاث بحرمة الحياة الخاصة، فحيث يترك الفرد للدولة ملكه وسلطة تسيير الشؤون العامة، تكفل الدولة بالتبادل ترك مساحات مناسبة للفرد داخل المجتمع ليحيا حياته الخاصة، دون تدخل من أي كان، وهي أيضا تضمن لهذه الحياة الخاصة الحماية الجزائية اللازمة في مقابل أية اعتداءات تستهدفها والتي منها استخدامات تقنيات المعلومات والاتصالات لإيقاع الضرر بالأفراد والاعتداء عليهم بأشخاصهم وأموالهم.

البند الأول: تعريف الحياة الخاصة

لم يرد للحياة الخاصة تعريفا جامعا ومانعا لا في الفقه ولا في القضاء ولا في التشريع، ومرد ذلك هو صعوبة وضع تعريف موحد للمصطلح، لذلك تعد محاولة إيجاد تعريف للحياة الخاصة أمرا بالغ الصعوبة حيث يترتب على وضع هذا التعريف تحديد العناصر المشكلة له، فضلا عن أنها فكرة مرنة وغير محددة، وتختلف باختلاف الزمان والمكان والأشخاص، كما أنه يصعب وضع تعريف محدد للحياة الخاصة ذلك أن التعريف لا يكون إلا لفكرة ثابتة ومحددة، أما الحياة الخاصة فهي فكرة مرنة ومتغيرة ونسبية وعلى الرغم من عدم تحديد مدلولها والإلمام بمعناها إلا أن ذلك لا يمنع أنها تتمتع بالحماية القانونية الكاملة في العديد من التشريعات حتى تظل في منأى عن تدخل الغير وعن العلانية، بل أن القضاء قد استقر على ضرورة أن تحاط الحياة الخاصة بسياج وحائط يحميها من تدخل الغير وإطلاعه عليها.

تكمن الصعوبة في تحديد تعريف للخصوصية في ارتباطها بالانتماءات الدينية والعادات والقيم في المحيط الذي يعيش فيه الشخص[1]، فنجد أنه في التشريعات والقوانين الدولية لا يذكر فيها تعريفا معينا للخصوصية، وإنما تكتفي بوضع نصوص تكفل حماية هذا الحق وتعدد صور الاعتداء عليه.

وفي إطار تعريف الحق في الحياة الخاصة نذكر على سبيل المثال تعريف المحامي يونس عرب الذي قال بأن الحياة الخاصة للإنسان تشمل الحق في العيش مع ذاته وأسرته في هدوء وسكينة، والحق في السرية المهنية، وسرية المراسلات والمحادثات، حرمة المساكن، وحرية الإعتقاد والفكر، المسألة العاطفية والعائلية، والروحية والمالية...إلخ، وهي من المظاهر الاجتماعية الضرورية لكل إنسان وجزء لا يتجزأ من الوجود الإنساني تجب حمايته بكل قوة من التعسف والاعتداء أيا كان الشخص المعتدي وبغض النظر عن المعتدى عليه أو الوسيلة المستعملة في الاعتداء.

إن الحياة الخاصة للفرد تتحدد حسب المجتمع الذي ينتمي إليه ذلك الفرد أي حسب أخلاق وثقافة وعادات المجتمع لذلك تعتبر الحياة الخاصة فكرة نسبية محكومة ومقيدة بحكم قيم وقواعد السلوك والقانون الأخلاقي لكل مجتمع، لذلك تكون حتى صور الاعتداءات التي تقع على الحق في الحياة الخاصة مقيدة ومتوقفة على نفس العناصر، بل وبالنسبة للاعتداءات التي تقع على نفس الحقوق على الشبكة العنكبوتية أو على مواقع الإنترنت، أو بالوسائل التكنولوجية المتطورة تبقى أيضا متوقفة على درجة هذا التقدم، لذلك لا نستطيع مقارنة صور الاعتداء على الحياة الخاصة في الجزائر بتلك التي يتعرض لها الأفراد في الولايات المتحدة الأمريكية فأبعاد الخصوصية وعناصرها في المجتمعات العربية مختلفة إلى حد بعيد عن تلك المعروفة في المجتمعات الغربية.

ومن حيث تعريف الحياة الخاصة فلا نميز بين تلك المنتهكة بوسائل الاعتداء المادية التقليدية وتلك التي يتم انتهاكها بوسائل الاعتداء الإلكترونية أي باستخدام الوسيط الإلكتروني، لأن الاختلاف يمس صور الاعتداء لا الحق المعتدى عليه، ومن جهة أخرى، ارتبط مفهوم الخصوصية –في العديد من الكتابات والبحوث– بمصطلح حماية البيانات ومعالجتها مما جعلها تضبط في إطار حماية البيانات الخاصة، نذكر على سبيل المثال التعريف الذي صدر عن وزارة الداخلية السعودية حيث عرفت البيانات الشخصية في مذكرتها للمبادئ الأساسية لأمن المعلومات وخصوصيتها كالتالي بأنها كل ما يتعلق بالحياة الخاصة للإنسان كهويته وجنسيته واتجاهاته وميوله ومعتقداته وتعاملاته المالية والبنكية، فهي معلومات ترتبط بشخص معرف أو قابل للتعريف، وعرف مكتب خبراء البيت الأبيض للعلوم والتقنية نفس المصطلح بأن حق الفرد في الخصوصية هي حقه على الاختيار الشخصي فيما يريد مقاسمته مع الآخرين من أفكار وعواطف والحقائق المتعلقة بحياته الشخصية.

وما يمكن ذكره كتعريف للحق في الخصوصية حسب مجتمعنا العربي الإسلامي ما يلي: "إن الحق في الحياة الخاصة هي حق الشخص في أن يحترم الغير كل ما يعد من خصوصياته مادية كانت أو معنوية أو ما تعلقت بحريته، على أن يتحدد ذلك بمعيار الشخص العادي ووفقا للعادات والتقاليد والنظام القانوني القائم في المجتمع ومبادئ الشريعة الإسلامية"[2].

---

[1] عادل بسيوني، تاريخ القانون المصري، مصر الإسلامية، مكتبة نهضة الشرق، القاهرة، 1985، ص96.

[2] جعفر محمود المغربي وحسين شاكر عساف، المسؤولية المدنية عن الاعتداء على الحق في الصورة بواسطة الهاتف المحمول، دار الثقافة والنشر والتوزيع عمان، 2010، ص33.

البند الثاني: أهم عناصر الحق في حرمة الحياة الخاصة

أولا: حرمة المسكن، تمثل حرمة المسكن عنصرا أساسيا من عناصر الحق في حرمة الحياة الخاصة في التشريعات المختلفة وقد كفل الدستور الجزائري[1] حرمة المنزل وحظر تفتيشه إلا وفق القانون، ويقصد بالمسكن كل مكان مغلق معد للسكن يملكه أحد الأشخاص بغض النظر عن مدة إقامته فيه ولا يجوز للغير الدخول إليه إلا بإذن صاحبه، فهو مستودع لأسراره ويستمد حرمته من حرمة صاحبه سواء كان يقيم به إقامة دائمة أو مؤقتة وتمتد حرمة المسكن لتشمل كافة ملحقاته، كما تتمتع عيادة الطبيب ومكتب المحامي بحرمة مستمدة أيضا من شخص مالكها نظرا لاتصال ذلك بحياة مالكها الخاصة[2].

ثانيا: الحق في حرمة المراسلات والمحادثات، يقصد بالمراسلات كافة الرسائل المكتوبة سواء تلك المرسلة بطريق البريد أو بواسطة شخص يقوم بنقل تلك الرسائل وينصرف معنى المراسلات أيضا إلى البرقيات[3]، وتعد الرسائل ترجمة مادية لرأي خاص أو لأفكار شخصية، ولا يجوز لغير أطراف الرسالة معرفتها، وإذا قام أحد الأشخاص بالإطلاع عليها فإنه يعد منتهكا لحرمة الحياة الخاصة وسبب ذلك أن هذه الرسالة قد تتضمن أسرارا وأمورا تتعلق بخصوصيات طرفي الرسالة فلا يجوز الإطلاع عليها[4]، وللرسائل حرمة من لحظة إرسالها من المرسل حتى لحظة وصولها إلى المرسل إليه، وإذا كانت مغلقة وما زالت في الطريق لم تصل إلى المرسل إليه فلا يجوز فضها ومعرفة محتواها ومن يفض هذه الرسالة ويطلع على محتواها يعد مرتكبا لجريمة الاعتداء على حرمة المراسلات.

ثالثا: الحق في حرمة الحياة العائلية، إن حرمة حياة الشخص العائلية تعد عنصرا أساسيا وهاما من عناصر الحق في حرمة الحياة الخاصة، ولقد أجمع الفقه القانوني والمحاكم على تأكيد حق الإنسان في حماية أسراره العائلية، وعلة ذلك هو أن حياة الإنسان العائلية هي جزء هام من حياته بشكل عام، فالأسرار العائلية هي في غاية الأهمية للشخص ويحتاج إلى إحاطتها بالكتمان وحفظها بعيدة عن معرفة الناس، ولا يصح بأي حال من الأحوال أن تكون علاقات الشخص وحياته العائلية مجالا للنشر، وإذا تم ذلك فهو يشكل انتهاكا لحرمة الحياة الخاصة بالاعتداء على حياة الإنسان العائلية[5]، وقد حرمت التشريعات المختلفة ذلك الانتهاك حفاظا منها على حرمة الحياة العائلية للإنسان لأنها تحمل بين جنباتها أسرارا تمس الأخلاق والشرف والعلاقات الأسرية والاجتماعية وهي أسرار ذات أهمية كبيرة للإنسان داخل المجتمع، وهو الأمر الذي دعا بالمشرعين إلى إحاطتها بالحماية ووضع عقوبات لأي تجاوزات على حق الإنسان في حماية أسراره العائلية وحماية حرمة حياته العائلية[6].

---

[1] قانون رقم 16-01 مؤرخ في 26 جمادى الأولى 1437ھ الموافق لـ 06 مارس 2016م، يتضمن التعديل الدستوري، ج.ر، العدد 14، مؤرخة في 07 مارس 2016.

[2] محمد الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة في مواجهة الصحافة، دار النهضة العربية، القاهرة، ط1، 2001، ص06 و07.

[3] أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار الطباعة الحديثة، القاهرة، 1993، ص578.

[4] محمد الشهاوي، المرجع السابق، ص17.

[5] محمود عبد الرحمن محمد، نطاق الحق في الحياة الخاصة أو الخصوصية، دراسة مقارنة، دار النهضة العربية، القاهرة، 1994، ص181. ممدوح بحر حماية الحياة الخاصة في القانون الجنائي، مكتبة دار الثقافة، عمان، ط1، 1996، ص30.

[6] محمد الشهاوي، المرجع السابق، ص25.

رابعا: الحق في حرمة الحياة الصحية، تعد الحالة الصحية للإنسان وتاريخه المرضي والأمراض التي عانى أو يعاني منها وأسبابها وجميع ما يتعلق بحالته الصحية والأدوية التي يتناولها أو العلاجات التي يخضع لها عنصرا من عناصر الحق في الحياة الخاصة وسبب ذلك أن الحالة الصحية والرعاية الطبية التي تقدم له تعد من الأمور الخاصة التي يرغب الشخص عادة في عدم كشفها لأحد وبالتالي فقد جرم المشرعون أي إفشاء لهذه الأسرار المتعلقة بالحالة الصحية للشخص[1].

خامسا: الحق في حرمة صورة الإنسان، للإنسان الحق في منع التقاط صور له دون الحصول على موافقته وكذلك نشرها، فالصورة هي أحد عناصر الحياة الخاصة للإنسان، وللإنسان الحق في حرمة صورته وعدم التقاطها أو نشرها بغير إذنه والاعتداء على صورة الإنسان يعد انتهاكا لحرمة حياته الخاصة[2].

سادسا: الحق في حرمة الحياة المهنية وأسرارها، اتجهت التشريعات المقارنة إلى حماية الأسرار المهنية ويعتبر الإخلال بواجب كتمان وحفظ الأسرار المهنية جريمة تعرض مرتكبها للعقاب، ويقصد بإفشاء الأسرار المهنية الكشف عن واقعة لها صفة السر صادر ممن علم بها بمقتضى مهنته مع توافر القصد الجنائي[3].

البند الثالث: مفهوم السر الخاص

يعتبر السر الخاص جوهر الحياة الخاصة ونطاق الحق بالحياة الخاصة فلم ينشأ هذا الحق أصلا إلا لحرص الفرد على أن تبقى حياته بكافة تفصيلاتها الخاصة سرا على غيره، لا ينتهكها ولا يعلم بها غيره إلا ضمن إذن أو موافقة منه، وبالتالي فإن السر الخاص كما يرى بعض الفقه واقعة أو صيغة ينحصر العلم بها بعدد محدد من الناس إذا كانت فيه مصلحة يعترف بها القانون لشخص أو لأكثر في أن يظل العلم بها محصورا في ذلك النطاق، ومن هنا يمكن استظهار ملامح السر الخاص عموما في أن يشكل السر واقعة أو حدث، أن يكون صاحبه حريصا على ألا يعلم بها غيره، وأن تلقى تلك الواقعة أو ذلك الحدث حماية القانون.

وأمام هذا فإن الوقائع والأحداث التي نمر فيها كأفراد، لا يمكن الجزم بأنها تقع تحت طائلة الأسرار بشكل مطلق، وبالتالي فإن مسألة حمايتها وفقا لذلك تبقى أمرا غير ثابت، فإذا استبعدنا مبدأ أولئك الذين لا يعيرون حياتهم الخاصة أدنى مراتب الخصوصية ويتغنون بالانفتاح بكافة شؤونهم، يبقى لدينا من يحرصون –ولو بنسب متفاوتة من القول– على حماية سرية حياتهم وتفصيلاتها من وجهة نظرهم، ورغم ذلك لا يمكن الإقرار بالحماية المطلقة، فقد تنطوي أسرارهم على إساءة للغير، وقد تنطوي على جرائم، ثم قد يكون من يعلم بها واقعا تحت إلزام القانون بعدم الكتمان، فإذا تعارض حق الحياة الخاصة مع واجب الإبلاغ، كان الامتناع عن الإبلاغ رغم أنه يشكل انتهاكا لسر خاص مجرما، لأن حماية الصالح العام أولى من حماية الصالح الخاص.

---

[1] محمود عبد الرحمن محمد، المرجع السابق، ص182.

[2] مدحت عبد الحليم رمضان، جرائم الاعتداء على الأشخاص والإنترنت، المرجع السابق، ص111-114. Jared Strauss and Kenneth S. Rogerson, Policies for online privacy in the United States and the European Union Telematics and Informatics, Elsevier, Amsterdam, Netherlands, Vol. 19, n°02, 2002 pp173-192.

[3] محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، النظرية العامة للجريمة، دار النهضة العربية، القاهرة، 1982، ص75. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، المرجع السابق، ص10 وما بعدها.

ومثال ذلك الطبيب المعالج الذي يكفل قانونه حماية الحياة الخاصة لمرضاه، إلا أنه يقع تحت إلزام القانون، عندما يكتشف أثناء العلاج أن الجرح الذي أصاب مريضه هو نتيجة جرم ما، أو أن مريضه يتعاطى المخدرات مثلا ونحو ذلك، مما يشكل معه كتمان السر جرما معاقبا عليه، وبالتالي يخرج مثل هذا السر من نطاق الحماية بموجب أحكام القانون[1].

وفي ظل هذا يمكن لنا أن نوازن ضمن الحياة الخاصة بين ما يكفل القانون حمايته وسريته فيشكل إفشاؤه جرما، وبين ما لا يدخل ضمن نطاق الأسرار فلا تقع به الجريمة المبحوث عنها هنا، وبهذا المعنى يرتبط السر بالحياة الخاصة ويشكل محورها الرئيس ومن هنا يظهر تمسك الأفراد بالحق بالحياة الخاصة، فهم يحرصون كل الحرص على أن تبقى مفردات حياتهم حبيسة علمهم هم وحدهم دون سواهم، أو على الأكثر علم بعض الأشخاص وهم الأكثر قربا لهم، ولا أهمية بعد ذلك لطبيعة هذا السر، فقد يكون متعلقا بشؤون الفرد الصحية لكونه يعاني من مرض ما، أو متعلق بشؤونه المالية، أو يكون متعلق بشخصه كمعلومات عن أوصافه الشخصية ومكان عمله أو سكنه أو مكان تنقله، أو متعلق بشؤونه واهتماماته الدينية والسياسية وأفكاره وفلسفاته الفكرية والاجتماعية والإنسانية، المهم من ذلك كله أن يقع السر ضمن حماية القانون، وأن يكون ذو صلة بالفرد يؤثر فيه إظهاره للعامة ماديا أو معنويا، وأن يظهر حرص الفرد على إبقائه طي الكتمان[2].

ثم لا أهمية بعد ذلك لمكان حفظ السر أو طريقة ذلك، فقد يكون محفوظا على مختلف الوسائل الإلكترونية كجهاز الحاسب الآلي الخاص بالفرد نفسه، سواء ذلك الموجود في منزله أو مكان عمله، وسواء كان ذلك الحاسب الآلي منفردا أم موصولا مع غيره ضمن شبكة داخلية أو خارجية، مفتوحة أو مغلقة، ويبقى أن نعلم أن السلوك الجرمي المشكل لصور الجريمة الواقعة على السر يتعلق بتقنية المعلومات، ولا بد من أن تكون وسيلة الفاعل في ارتكاب الجريمة وسيلة إلكترونية، وبالتالي لا نبحث هنا في صور الحصول على الأسرار ذات العلاقة بالحياة الخاصة بتلك الوسائل التقليدية.

البند الرابع: تكريس مبدأ الحماية القانونية للحياة الخاصة ضد الاعتداءات الإلكترونية

تعتبر الحياة الخاصة أو ما يطلق عليها الحق في الخصوصية أقدم الحقوق التي أقرتها المجتمعات للأفراد لأنها مرتبطة ارتباطا وثيقا بحرية الفرد وحقوقه الأساسية الخاصة كما سبقت الإشارة إليه، حيث أقرت لها كل التشريعات الحماية القانونية من كل أشكال الاعتداء التي يمكن أن يتعرض لها الفرد، وقد تطور هذا الحق وامتد نطاقه ليشمل حماية كل عناصر الحياة الخاصة للشخص من كافة أوجه الاعتداء والتدخل في حياته أيا كان مظهرها أو طبيعتها، التي تمتد إلى حمايته من أشكال الاعتداء الإلكتروني الذي يقع بموجب الوسائل الحديثة الرقمية والإلكترونية وعبر شبكة الإنترنت وبالخصوص في إطار المواقع الإلكترونية أو أسماء النطاق[3].

فبسبب التطور التقني والتكنولوجي الذي شهده هذا العصر أصبحت الحماية القانونية للحق في الحياة الخاصة المنصوص عليها في النصوص القانونية التقليدية لاسيما قوانين العقوبات مقصرة بسبب كون التحديات التي تواجهها من نوع جديد في عصر المعلوماتية الرقمي وفي عصر العولمة والعصرنة، وذلك لعدم قدرة وكفاية الوسائل والآليات التي قررتها للحماية ضد الأنواع الجديدة

---

[1] أسامة أحمد المناعسة وآخرون، جرائم الحاسب الآلي والإنترنت، دراسة تحليلية مقارنة، المرجع السابق، ص216.

[2] أسامة أحمد المناعسة وآخرون، جرائم الحاسب الآلي والإنترنت، دراسة تحليلية مقارنة، المرجع نفسه، ص217.

[3] جعفر محمود المغربي وحسين شاكر عساف، المرجع السابق، ص33.

للاعتداء لاسيما بسبب صعوبة تحديد هوية المعتدي على المواقع الإلكترونية بالإضافة إلى أن نطاق الاعتداء هو الوسيط الإلكتروني الذي تتم فيه كل أركان الجريمة وهو عالم افتراضي وغير ملموس، غير أنه أمام استفحال ظاهرة الاعتداءات الإلكترونية على الحق في الخصوصية والجريمة الإلكترونية عموما، تم تكريس حمايتها تشريعيا أولا، ودوليا ثانيا.

أولا: التكريس التشريعي للحق في الحياة الخاصة، من حيث المبدأ، الحماية القانونية للحقوق المرتبطة بالحياة الخاصة أو للخصوصية مبدأ دستوري أقرته معظم الدساتير والتشريعات العالمية ومنهم الدستور الجزائري الذي كرس حماية حق الإنسان في حياته الخاصة في دستور 1996 في المادة 40 منه التي تقابلها المادة 39 في تعديل سنة 2016، التي تنص على أنه: "تضمن الدولة عدم انتهاك حرمة المسكن، فلا تفتيش إلا بمقتضى القانون، وفي إطار احترامه، ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة"، ويضيف على أنه: "لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه، ويحميهما القانون، سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة".

وقد كرس المشرع هذا الحق في المادة 303 مكرر ق.ع التي نصت على ما يلي: "يعاقب بالحبس من ستة أشهر إلى سنوات كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأي تقنية كانت وذلك:

1- بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، بغير إذن صاحبها أو رضاه.

2- بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه...".

كما وردت لهذه النصوص الدستورية بعض النصوص الخاصة المجسدة للمبدأ العام من خلال التطرق بصفة خاصة إلى حماية الحق في الحياة الخاصة، ومن بينها ما ورد في القانون العضوي رقم 12-05[1] المتعلق بالصحافة في المادة 02: "يمارس نشاط الإعلام بحرية في إطار أحكام هذا القانون العضوي والتشريع والتنظيم المعمول بهما وفي ظل احترام:

- الدستور وقوانين الجمهورية.
- الدين الإسلامي وباقي الأديان.
- الهوية الوطنية والقيم الثقافية للمجتمع...
- حق المواطن في إعلام كامل وموضوعي.
- سرية التحقيق القضائي.
- كرامة الإنسان والحريات الفردية والجماعية".

وهنا حماية للحياة الخاصة من تجاوزات الصحافة التي تبرر كل تصرفاتها التي تلحق الضرر بالغير على أساس مبدأ حرية الإعلام.

كما نص القانون رقم 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في المادة 04 منه على أنه: "يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 03... للوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب أو الجرائم الماسة بأمن الدولة، في حالة توافر معلومات عن احتمال اعتداء على منظومة معلوماتية...

[1] قانون رقم 12-05 مؤرخ في 18 صفر 1433ھ الموافق لـ 12 يناير 2012م يتعلق بالإعلام، ج.ر، العدد 02، مؤرخة في 2012/01/15.

وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات، بالنسبة للمساس بالحياة الخاصة للغير"، وهو نص في غاية الأهمية بالنسبة لمبدأ الحق في الحياة الخاصة لما يحمله من ضمانات للأفراد على وجه العموم، لكن مؤخرا، حاول المشرع الجزائري أن يتماشى مع ما هو معمول به في مجال محاربة جرائم التكنولوجيا الحديثة وذلك باستحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية بموجب القانون رقم 16-02 المتضمن تعديل قانون العقوبات، خاصة بسبب التزايد اللامتناهي للاعتداءات على الأنظمة المعلوماتية بتطور آليات الاتصال وظهور المواقع الإلكترونية والإنترنت، حيث يتضمن هذا التعديل الأخير في الفصل الثالث من الباب الثاني من الكتاب الثالث قسم سابع عنوانه المساس بأنظمة المعالجة الآلية للمعطيات، ويشمل المواد من 394 مكرر إلى 394 مكرر7.

ثانيا: التكريس الدولي للحق في الحياة الخاصة، لقد دفع التطور المذهل لوسائل الاعتداء على الحياة الخاصة للإنسان العديد من المفكرين وعلماء القانون والناشطين في مجال حقوق الإنسان إلى البحث جدية عن السبل الكفيلة لحماية الحياة الخاصة للإنسان بصفة عامة، لذلك تضافرت الجهود الدولية والإقليمية لحماية الخصوصية، فتضمنه الإعلان العالمي لحقوق الإنسان وأولاه أهمية خاصة، إذ نص في المادة 12 منه على أنه: "لا يجوز تعرض أحد لتدخل تعسفي في حياته الخاصة أو شؤون أسرته أو مسكنه أو مراسلاته... ولكل شخص الحق في أن يحميه القانون من مثل ذلك التدخل".

وأكد العهد الدولي الخاص بالحقوق المدنية والسياسية على حماية هذا الحق في المادة 17 منه: "لا يجوز تعريض أي شخص على نحو تعسفي أو غير قانوني للتدخل في خصوصياته، أو شؤون أسرته أو بيته أو مراسلاته، ومن حق كل شخص أن يحميه القانون من مثل ذلك التدخل"، كما أصدرت الجمعية العامة للأمم المتحدة القرار رقم 22-00 لسنة 1966 يتعلق بالاتفاقية الدولية للحقوق المدنية والسياسية وقد نصت هذه الاتفاقية في المادة 17 منها على أنه: "لا يجوز التدخل بشكل تعسفي أو غير قانوني في المسائل الخاصة بأي شخص أو عائلته أو بمسكنه أو بمراسلاته، كما لا يجوز التعرض بشكل غير قانوني لما يمس شرفه وسمعته، لكل شخص الحق في حماية القانون ضد مثل هذا التدخل أو التعرض".

وكان لمجلس أوروبا دوراكبيرا في عقد الاتفاقية الأوربية لحقوق الإنسان والحريات العامة لعام 1950، حيث أوجبت المادة 08 من هذه الاتفاقية على حماية الحياة الخاصة بالنص على حماية الأفراد من التدخل والاعتداء على حياتهم الخاصة وحياة أسرهم كما قررت المادة 10 من هذه الاتفاقية على وجوب حماية حق الوصول ونقل المعلومات، بالإضافة إلى ذلك فقد كان للاتحاد الأوروبي دوراكبيرا في حماية الحق في الخصوصية، حيث صدر عن الاتحاد عدة تعليمات بهذا الشأن منها التعليمات المتعلقة بحماية الأفراد من أنشطة خزن ونقل البيانات، التعليمات المتعلقة بحماية الأفراد من أثر التطور التقني لمعالجة البيانات، كما صدر التوجيه الأوربي عن البرلمان الأوربي تحت رقم 85 في سنة 2002 والمتعلق بالمعالجة الآلية للبيانات وحماية الحياة الخاصة[1].

[1] نوارة حسين، المرجع السابق، ص10 وما بعدها.

الفرع الثاني: نطاق اعتداء جرائم التكنولوجيا الحديثة على الحياة الخاصة

من المسائل البالغة الأهمية التي يجدر بنا التطرق اليها هي تحديد نوع الاعتداءات التي يمكن أن تمس بالحياة الخاصة والتي تتم عبر الوسيط الإلكتروني، والتي تتماشى مع طبيعة البيئة الإلكترونية حيث تساعد وتسهل على الجاني إتيان الفعل واكتمال أركان الجريمة، وكذلك القانون الواجب تطبيقه على الجريمة وأيضا نظام المسؤولية الذي يتم ردع الفعل على أساسه، نظرا لعدم وجود قانون خاص بجرائم التكنولوجيا الحديثة.

وبالرجوع إلى القانون الجزائري فيما يخص نطاق الحق في الحياة الخاصة المنتهكة عبر مواقع الإنترنت، أو حتى من الاعتداءات الإلكترونية الأخرى والتي تتم بموجب الوسائل الإلكترونية والرقمية، فلا نجد لها أثرا، فالمشرع من حيث النص لم يواكب التطورات في مجال المعلوماتية أو في المجال الرقمي الإلكتروني، واكتفى بإقرار المبدأ في حماية الخصوصية في شكله العام دون التعرض للوسيلة المعتمدة في تحقيق الاعتداء، فالحماية هنا قائمة مهما كانت أشكال الاعتداء؛ لأن الاعتداء في هذه الحالة يكون بوجود الخطأ والضرر الذي يلحق أحد جوانب الحياة الخاصة.

وعموما لا يوجد أي دستور عربي ينظم مظاهر حماية خصوصية المعلومات أو البيانات الشخصية أو مسائل معالجتها الإلكترونية على نحو ما هو منصوص عليه في دساتير الدول الأجنبية، مع خلوها من المبادئ التي قد تحد على الأقل من انتهاكات هذا الحق، لأن التجربة حاليا جديدة ومحتشمة، باستثناء النصوص التي تكفل الحق في حماية الحياة الخاصة كمبدأ عام والتي تخضع لنوع من التطويع لتكون قابلة التطبيق على جرائم التكنولوجيا الحديثة، لأن هذه الأخيرة في أصلها مثل الجريمة التقليدية وتختلف عنها في كونها مرتكبة عبر الوسيط الإلكتروني.

لقد صنع التقدم العلمي والتكنولوجي والتقني، الإلكتروني والرقمي طفرة في مجال وسائل الإعلام والاتصال والتواصل بحيث أصبح العالم قرية صغيرة محدودة المعالم، مما أثر على ذلك تأثيرا كبيرا على تطور الحق في الحياة الخاصة بسبب البحث عن وسائل وآليات جديدة لمواجهة الأخطار التي تهدد هذا الحق، ومن خلال سن قوانين جديدة قادرة على تنظيم هذا الحق الذي يتم تداوله عبر الوسائل الحديثة للاتصال والتواصل وحمايته بصفة فعالة أمام التحديات التي يفرضها واقع العصر الحديث[1].

البند الأول: أشكال وصور اعتداء جرائم التكنولوجيا الحديثة على الحياة الخاصة

إن المخاطر التي تهدد الحياة الخاصة كثيرة ومتعددة أفرزتها مختلف التطورات التي حدثت بظهور شبكة الإنترنت والتي توسعت من خلالها صور التواصل في المجتمع لاسيما في المواقع الإلكترونية بين الأفراد هذا من جهة، ومن جهة أخرى بسبب توسع نشاط تدخل الدولة في جمع البيانات عن الأفراد وتخزينها من خلال استغلال الأنظمة المعلوماتية المستحدثة[2]، وتجدر الإشارة إلى أن

---

[1] عندما يستخدم الأفراد مواقع الإنترنت يتوقعون قدرا من الخفية في نشاطهم أكثر مما هو في العالم المادي الواقعي، لكن في الحقيقة يمكن ملاحظة وجودهم ومراقبتهم من قبل الآخرين، فالإنترنت عبر نظم الخوادم ونظم إدارة الشبكات تصنع قدرا كبيرا من المعلومات عند كل وقفة في فضاء الشبكة، وهذه البيانات قد يتم اصطيادها ومعرفتها من قبل صاحب العمل عند استخدامه للشبكة أو غيره من القراصنة، وقد تجمع من قبل المواقع المزارة نفسها، فإن جمع شتات معلومات وسلوكيات معينة قد يقدم أوضح صورة عن شخص لم يرد كشف أي من تفاصيل ما تضمنته.

[2] نهلا عبد القادر المومني، المرجع السابق، ص317.

المخاطر التي تهدد الحياة الخاصة في ظل تطور مجال المعلوماتية كثيرة ومتنوعة[1]، نذكر منها على سبيل المثال وليس الحصر ما يلي:

– الوصول إلى المعلومات بشكل غير شرعي كسرقة المعلومات أو الإطلاع عليها أو حذفها أو تعديلها وجعلها غير قابلة للاستخدام، بالإضافة إلى الحصول على المعلومات السرية للمؤسسات والبنوك والجهات الحكومية والأفراد وابتزازهم بواسطتها.

– التنصت على المكالمات الخاصة وتسجيلها لإذاعتها على المواقع بهدف الابتزاز.

– التقاط الصور الخاصة دون الحصول على موافقة صاحبها وعرضها على مواقع الابتزاز أو التشويه بالسمعة.

– التجسس على الأسرار الخاصة والتجسس على الاتصالات والمراسلات وسريتها عن طريق المراقبة الإلكترونية بالأقمار الصناعية والكاميرات الرقمية المحولة عن طريق الهواتف المحمولة وكشفها على المواقع الإلكترونية لتحقيق الربح السريع.

– نشر وإعلان والتلاعب في البيانات الشخصية أو محوها عن طريق أشخاص غير مرخص لهم بذلك في وسائل الإعلام والاتصال المختلفة دون موافقة صاحبها الصريحة أو الضمنية.

– جمع معلومات وبيانات عديدة تتعلق بالوضع المادي والصحي والعائلي والعادات الاجتماعية للأفراد، عبر شبكات الاتصال بطرق التجسس والقرصنة الإلكترونية وتخزينها ومعالجتها ونقلها بسهولة كبيرة، مما يشكل انتهاكاً لخصوصية الأفراد ورغبتهم بعدم معرفتها من قبل الغير واستغلالها بطرق غير شرعية.

– انتحال الشخصيات عبر شبكة الإنترنت للقيام بعمليات النصب والاحتيال، وغالبا ما يكون الضحية من مستخدمي الإنترنت، وعادة ما تؤدي جريمة انتحال الشخصية إلى الاستيلاء على الأرصدة البنكية أو السحب من البطاقات الائتمانية وسرقة الحسابات المصرفية أو الإساءة إلى سمعة الضحية.

– جمع البيانات الشخصية وإعادة استغلالها بأساليب تمس الحياة الخاصة كصورة جديدة للاعتداء[2].

البند الثاني: الاستثناءات التي ترد على الحق في حماية الحياة الخاصة

يتضمن الحق في الحياة الخاصة عناصر كثيرة منها الحق في الاسم الكامل، الصورة، المعلومات الشخصية السرية، البيانات الخاصة...إلخ، وهي محمية من كل الاعتداءات بغض النظر إلى نوعها –حتى إن كانت على دعامة إلكترونية في مواقع الإنترنت– وهذا كقاعدة عامة، إلا أنه ورد عليها استثناء يتعلق بالحق في الإعلام، حيث يباح نشر صورة شخص معين، أو تقديم معلومات معينة وإن كانت خاصة بتبرير تحقيق مبدأ الحق في الإعلام عن كل الوقائع والجرائم التي تقع في المجتمع، وهو مبرر يقع ضد الحق في رفض الشخص أو الاعتراض عن نشر صورته أو ذكر اسمه أو تقديم أسراره عبر وسائل الإعلام بكل أشكالها لاسيما المواقع الإلكترونية.

---

[1] جعفر محمود المغربي وحسين شاكر عساف، المرجع السابق، ص41 و42.

[2] المقصود بجمع البيانات: أن استخدام الحواسيب أو الأجهزة الذكية في ميدان جمع ومعالجة البيانات الشخصية المتصلة بالحياة الخاصة للأفراد خلف آثارا إيجابية عريضة، لا يستطيع أحد إنكارها خاصة في مجال تنظيم الدولة لشؤون الأفراد الاقتصادية والاجتماعية والعلمية وغيرها، وهذا ما أوجد في الحقيقة ما يعرف ببنوك المعلومات التي قد تكون مقصورة على بيانات ومعلومات تتصل بقطاع معين، كبنوك المعلومات القانونية مثلا، أو قد تكون شاملة لمختلف الشؤون والقطاعات، وقد تكون مهيأة للاستخدام على المستوى الوطني العام كمراكز وبنوك المعلومات الوطنية أو المستخدمة على نحو خاص كمراكز وبنوك معلومات البنوك، وقد تكون كذلك مهيأة للاستخدام الإقليمي أو الدولي كمراكز وبنوك معلومات الشرطة...إلخ.

المطلب الثاني: جرائم التكنولوجيا الحديثة الماسة بالشرف والاعتبار

إن حق الإنسان في شرفه واعتباره من الحقوق اللصيقة بالشخصية القانونية والمتفرعة عنها أيا كانت المكانة الاجتماعية التي يحتلها في المجتمع، وبالتالي لا يوجد شخص معدوم الشرف والاعتبار كلية منذ أن اعترفت القوانين الحديثة لكل فرد بشخصيته القانونية، لذا أسبغ المشرع الحماية الجنائية على هذا الحق ونص على تجريم الاعتداء عليه.

ويثور في معرض الحديث عن جرائم الاعتداء على شرف الإنسان واعتباره موضوع ظهور وانتشار وسائل تقنية المعلومات الحديثة، حيث أنه في إطار مجتمع المعلومات الإلكترونية وجد العابثون غرضهم في ذم وقدح وتحقير الأشخاص بصور متنوعة تتنوع بتنوع الغرض من استخدام الوسيط الإلكتروني والطريقة التي يستخدم بها، مما أدى إلى التساؤل حول مدى انطباق النصوص التقليدية المتعلقة بجرائم التكنولوجيا الحديثة على مثل هذه الأفعال المرتكبة عبر تقنية المعلومات الحديثة من خلال مجالات استخدامها المختلفة.

ولعل أهم صور الجرائم الماسة بشرف الإنسان واعتباره، جريمة القذف والسبب، التشهير والمضايقة، ويقصد بالشرف والاعتبار من الناحية الموضوعية المكانة التي يحتلها كل شخص في المجتمع وما يتفرع عنها من حق في أن يعامل على النحو الذي يتفق مع هذه المكانة، أي أن يعطى الثقة والاحترام اللذان تقتضيهما هذه المكانة الاجتماعية، أما من الناحية الشخصية فيقصد بالشرف والاعتبار شعور كل شخص بكرامته وإحساسه بأنه يستحق معاملة واحتراما متفقين مع هذا الشعور من طرف أفراد المجتمع والحقيقة أن المدلولان غير متطابقان، فقد يبالغ الشخص في الشعور بكرامته أو يقدرها بأقل من قيمتها، وفي الحالتين يمس الفعل بالشرف والاعتبار في إحدى وجهتيه دون الأخرى، فإذا بالغ الشخص في الشعور بكرامته فإنه يؤذيه نفسيا فعل لا يمس في الحقيقة مكانته الاجتماعية، وإذا قدرها بأقل من قيمتها فقد يمس الفعل بمكانته الاجتماعية دون أن يؤذي إحساسه[1].

وعلى العموم فقد باتت الجرائم الماسة بالشرف والاعتبار المرتكبة عن طريق الإنترنت من أكثر جرائم التكنولوجيا الحديثة التي يمكن لمسها بسهولة على هذه الشبكة وصفحاتها، فلا يكاد يفلت منها شخصية عامة سياسية أو علمية أو عشائرية أو اقتصادية، بل في تقديرنا يصعب تنظيم إحصائية لما يحتويه الإنترنت من هذا الضرب من الجرائم التي تعدتها حتى إلى تلك الشخصيات غير العامة، بدوافع الحقد والحياء والغيرة والتباغض، لاسيما مع استخدام الأسماء الكاذبة أو الوهمية أو المستعارة للكاتبين (الجناة القائمين بالقذف أو السب)، ولهذا سنحاول تناول أهم الجرائم الماسة بالشرف والاعتبار.

الفرع الأول: القذف والسب في جرائم التكنولوجيا الحديثة

تعد جرائم القذف والسب المتصلة بالتكنولوجيا الحديثة من أبرز الجرائم التي تقع على شرف الإنسان واعتباره، وللوقوف على هذه الأخيرة نتناول التعريف بها وأركانها.

البند الأول: جريمة القذف المتصلة بالتكنولوجيا الحديثة

أولا: التعريف بجريمة القذف المتصلة بالتكنولوجيا الحديثة، القذف لغة، الرمي البعيد، ولاعتبار البعد فيه قيل منزل

[1] محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، المرجع السابق، ص496 و497.

قذف وقذيف وبلدة قذوف بعيدة، قال الله تعالى: "أن اقذفيه في التابوت فاقذفيه في اليم..."[1]، وقوله تعالى: "بل نقذف بالحق على الباطل..."[2]، وقوله تعالى: "... ويقذفون من كل جانب"[3]، واستعير القذف للشتم والعيب، كما استعير للرمي[4]، والقذف هو الرمي بالحجارة، وقذف المحصنة أي رماها[5]، وهو أيضا الرمي بالسهم والكلام والحصى.

أما في الاصطلاح التشريعي، فلم نجد تعريفا تشريعيا للقذف بصورته المعلوماتية مما يحتم الرجوع إلى تعريفات القذف بصورته التقليدية، ففي قانون العقوبات الجزائري عرف المشرع القذف في نص المادة 296 ق.ع بقولها:"يعد قذفا كل ادعاء بواقعة من شأنها المساس بشرف واعتبار الأشخاص، أو الهيئات المدعى عليها بها أو إسنادها إليهم..."، وتضيف نفس المادة في شطرها الثاني "يعاقب على نشر هذا الادعاء أو ذلك الإسناد مباشرة أو بطريق إعادة النشر حتى ولو تم ذلك على وجه التشكيك أو إذا قصد به شخص أو هيئة دون ذكر الاسم ولكن كان من الممكن تحديدهما من عبارات الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الإعلانات موضوع الجريمة".

فيما نصت المادة 144 مكرر و146 ق.ع على أن القذف الموجه إلى رئيس الجمهورية أو الهيئات العمومية قد يكون بأية آلية لبث الصوت أو صورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى.

ويمكننا تعريف جريمة القذف المتصلة بالتكنولوجيا الحديثة بأنها إسناد واقعة معينة إلى الغير بإحدى وسائل التكنولوجيا الحديثة من شأنها لو كانت صادقة، لأوجبت عقاب من أسندت إليه أو احتقاره عند أهل وطنه، والتعريف المذكور هو ترديد للتعريف التشريعي المذكور آنفا مع إدخال عنصر التكنولوجيا الحديثة وسيلة لإسناد أفعال القذف.

على العموم نرى أن القذف يمكن أن يقع وجاهي مكتوب أو مسموع أو مرئي، حيث تتضمن العديد من الخدمات التكنولوجية الحديثة وعن طريق الإنترنت برامجا ووسائطا للتواصل الاجتماعي تتيح الحوار المباشر المرئي والمكتوب والمسموع، ومن ثم فلا يستبعد أن يتم إسناد واقعة ما تمثل قذفا في مواجهة الطرف الآخر بإحدى هذه الطرق، وكذا الفرض في حال وقوع هذه الجريمة بطريق غير وجاهي كمن ينشر كتابات أو مقطع صوتية أو مرئية (فيديويا) يتضمن واقعة تمثل قذفا.

ثانيا: أركان جريمة القذف المتصلة بالتكنولوجيا الحديثة، يمكن إجمال هذه الأركان فيما يلي:

1- الركن المادي: يتكون الركن المادي لجريمة القذف سواء بصورته التقليدية أم المتصلة بالتكنولوجيا الحديثة من خمسة عناصر، أولها فعل الإسناد وثانيها موضوع الإسناد وثالثها طبيعة الواقعة ورابعها الشخص المقذوف وخامسها العلانية.

أ- فعل الإسناد، يراد بالإسناد نسبة واقعة إلى الغير بأية طريقة من طرق العلانية، فجميع الوسائل[6] الصالحة للتعبير عن

---

[1] سورة طه، الآية 39.

[2] سورة الأنبياء، الآية 18.

[3] سورة الصافات، الآية 08.

[4] المفردات في غريب القرآن، أبو القاسم الحسين بن محمد المعروف بالراغب الأصفهاني، المتوفى عام 502ھ، تحقيق صفوان عدنان الداودي، دار القلم بيروت، 2009، ص522.

[5] محمد ابن أبي بكر ابن عبد القادر الرازي، المرجع السابق، ص123.

[6] عبارة جميع الوسائل... الواردة في التعريف المذكور لفعل الإسناد تستوعب الوسائل الإلكترونية، مما يجعل النص شاملا للقذف المتصل بجرائم التكنولوجيا الحديثة في تقديرنا.

الأفكار والمعاني، تصلح وسائلا لإسناد الواقعة إلى الغير[1]، ويتحقق إسناد القذف بأية صيغة، سواء كانت تشكيكيه أو توكيدية متى كان من شأنها أن تلقي في أذهان الجمهور عقيدة في صحة الأمور المسندة إلى المجني عليه ولوكان ذلك بصورة وقتية ويصح أن يكون إسناد القذف شفويا أو مكتوبا[2]، سواء بخط اليد أو مطبوعا أو رسما كاريكاتوريا بل وحتى لوكان شفرة برموز معينة، كما يمكن أن يحصل بطريق الإشارة أو الإيماء متى كانت نسبة واقعة تتضمن قذفا[3]، ويعد قاذفا من يستخدم عبارات المديح إذا قصد الفاعل منها أمرا شائنا، كما يمكن أن يكون إسناد القذف صريحا أو ضمنيا كالاستعارة أو التورية، والحقيقة أن صور الإسناد المتقدمة وإن كانت تتعلق بالقذف في صورته التقليدية، إلا إننا لا نجد مانعا يحول دون انطباقها على القذف في صورته المتصلة بالتكنولوجيا الحديثة.

ب- موضوع الإسناد، فضلا عن العنصر المتقدم الذي يتضمن إسناد أمر شائن إلى الغير، يشترط أن يكون هذا الأمر محددا ومعينا وبهذا يتميز القذف عن السب في أن تحديد الواقعة يجعلها أقرب إلى التصديق، كما أن تأثيرها في شرف المجني عليه سيكون أشد وطأة، أما لو خلا الإسناد من تحديد واقعة معينة فعند ذلك يكون سبا، وليس قذفا كمن يسند إلى غيره أنه لص أو محتال أو زان أو مختلس، وعلى العموم فلا يعني اشتراط تحديد الواقعة أن تكون محددة في جميع تفصيلاتها وظروفها، فالقانون يكتفي بالتحديد النسبي[4] وعلى القاضي أن يسترشد بجميع الظروف التي أحاطت بالفعل ليحدد ما إذا أراد المتهم واقعة محددة أم لا، ولعل أهم ما يسترشد به القاضي في هذا التقدير هو الرجوع إلى العلاقة بين المجني عليه والجاني فضلا عن الدلالة العرفية لألفاظ الجاني[5].

ج- طبيعة الواقعة، لكي تكون الواقعة مما ينطبق عليها وصف القذف، يجب أن يكون من شأنها عقاب من تنسب إليه أو تؤدي إلى احتقاره عند أهل وطنه، أي أن موضوع الإسناد يتضمن فعلا يعده القانون جريمة، فيعاقب عليه جنائيا سواء شكل ذلك جناية أم جنحة أم مخالفة ولا يشمل ذلك ما يستوجب العقاب التأديبي، كما يتحقق القذف إذا كان من شأن الواقعة المسندة أن توجب احتقار المجني عليه عند أهل وطنه.

د- الشخص المقذوف، إن تعيين الواقعة في جريمة القذف يتطلب من جهة أخرى تحديد الشخص المقذوف أي المجني عليه وهو مستفاد من قول المشرع: "القذف هو إسناد واقعة إلى الغير"، ولكن ذلك لا يعني تحديد الشخص بالاسم، إنما يكفي أن يوجه الحديث بطريقة يسهل معها معرفة الشخص المقصود كذكر كنيته أو الأحرف الأولى من اسمه وإلا فلا تقوم جريمة القذف[6].

---

[1] سالم روضان الموسوي، جرائم القذف والسب عبر القنوات الفضائية، دراسة مقارنة معززة بتطبيقات قضائية، منشورات الحلبي الحقوقية، بيروت، 2012 ص23.

[2] وهي الصيغة الغالبة في القذف المتصل بجرائم التكنولوجيا الحديثة.

[3] ماهر عبد شويش الدرة، شرح قانون العقوبات، القسم الخاص، المكتبة القانونية، بغداد، 1997، ص447 و448.

[4] علي عبود جعفر، جرائم تكنولوجيا المعلومات الواقعة على الأشخاص وضد الحكومة، دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية بيروت، 2012، ص332.

[5] محمود نجيب حسني، شرح قانون العقوبات، القسم العام، المرجع السابق، ص519. أحمد شوقي عمر أبو خطوة، شرح الأحكام العامة لقانون العقوبات دار النهضة العربية، 2007، ص241.

[6] فخري عبد الرزاق الحديثي، شرح قانون العقوبات، القسم الخاص، مطبعة الزمان، بغداد، 1996، ص254 و255. سالم روضان الموسوي، المرجع السابق، ص29-31.

هـ- العلانية، يتطلب القانون أن تأتي أفعال القذف بإحدى وسائل العلانية، ومن الوسائل التي أوردها القانون لتحقق أفعال العلانية مجموعة الأعمال أو الإشارات أو الحركات إذا حصلت في طريق عام أو في محفل عام أو مكان مباح أو معرض لأنظار الجمهور أو إذا حصلت بحيث يستطيع رؤيتها من كان في مثل ذلك المكان أو إذا نقلت إليه بطريقة من الطرق الآلية والصحافة والمطبوعات الأخرى وغيرها من وسائل الدعاية والنشر، بالإضافة إلى الكتابة والرسوم والصور والشارات والأفلام ونحوها إذا عرضت في مكان عام مما ذكر، أو إذا وزعت أو بيعت إلى أكثر من شخص أو عرضت للبيع في أي مكان، ومن الواضح أن عمومية نص القانون وتعدد وسائل العلانية التي أوردها المشرع جاءت على سبيل المثال وليس الحصر لقوله تعد وسائلا للعلانية...، فضلا عن أن عبارة أو إذا نقلت إليه بطريقة من الطرق الآلية تستوعب الوسائل الحديثة التي باتت وسائطا للقذف بصورته المعلوماتية.

2- الركن المعنوي: القذف في جميع حالاته جريمة عمدية تتطلب القصد الجنائي بعنصريه العلم الإرادة، فيجب أن يعلم الجاني أن الواقعة التي يسندها إلى المجني عليه توجب عقابه أو احتقاره عند أهل وطنه، والعلم هنا يجب أن يكون علما فعليا وليس علما مفترضا، أما عن عنصر الإرادة، فيفترض أن تكون إرادة الجاني قد اتجهت إلى العبارات التي تتضمن وقائع القذف أو إلى تسجيلها كتابة أو إلى إتيان الإيماء الذي يتضمن القذف، فإذا ثبت أنه كان مكرها على ذلك فلا يتوافر القصد الجنائي لديه، وكذلك الحال في نفي القصد في حالة ما إذا كانت تلك العبارات قد صدرت نتيجة ثورة آنية أو نتيجة انزلاق اللسان أو نتيجة الجهل باللغة أو ورود عبارات سابقة أو لاحقة تنفي المعنى المستخلص من عبارات القذف[1].

تناول المشرع الجزائري عقوبة القذف الموجه للأشخاص الطبيعية، وتعاقب المادة 01/298 على القذف الموجه للأفراد بالحبس من شهرين إلى 06 أشهر وبغرامة مالية من 25 ألف إلى 100 ألف دينار جزائري أو بإحدى هاتين العقوبتين.

البند الثاني: السب في جرائم التكنولوجيا الحديثة

من جرائم التكنولوجيا الحديثة الواقعة على الشرف والاعتبار، جريمة السب ونقف على التعريف بها ومن ثم أركانها.

أولا: التعريف بجريمة السب المتصلة بالتكنولوجيا الحديثة، لم نجد تعريفا لجريمة السب المتصلة بالتكنولوجيا الحديثة ومع ذلك فإن مفهوم الأخيرة مستخلص من تعريفها التقليدي الذي سنأتي على ذكره، وما الاختلاف إلا بوسيلة ارتكاب الجريمة التي تتطلب صورتها المعلوماتية أي أن تكون قد وقعت عن طريق تقنية الوسائل الإلكترونية والإنترنت، مع أن عمومية النصوص والتعريفات التقليدية تسمح باستيعاب تلك الصورة المعلوماتية.

فالسب لغة، هو الشتم[2]، قال تعالى: "ولا تسبوا الذين يدعون من دون الله فيسبوا الله عدوا بغير علم..."[3].

والسب الكثير سباب[4]، والسب في بعض التشريعات يطلق عليه القدح.

---

[1] محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، المرجع السابق، ص563-567.

[2] أبو القاسم الحسين بن محمد المعروف بالراغب الأصفهاني، المرجع السابق، ص293.

[3] سورة الأنعام، الآية 108.

[4] كتاب العين، المرجع السابق، ص744.

وعرفه البعض بأنه خدش شرف الشخص واعتباره[1] عمدا دون أن يتضمن ذلك إسناد واقعة معينة، وتتفق جريمتا السب والقذف في أن كلاهما يمس شرف المجني عليه واعتباره في صورة إسناد ما يشينه، ومن ثم فإن تشابها بينهما في الركن المادي إلى جانب تماثلهما في محل الاعتداء، إلا أن اختلافهما في أن موضوع الإسناد في القذف واقعة محددة في حين أن موضوعه في السب حكم عام يتضمن بأي وجه من الوجوه خدشا للشرف والاعتبار[2].

وهذا الفارق يجعل من القذف أشد خطورة من السب، إذ أن الناس يميلون إلى تصديق نسبة الواقعة المحددة، لمظنة أن ثمة أدلة تؤيدها أكثر مما يصدقون حكما عاما يرونه تعبيرا عن محض كراهية أو حقد، وهذا الفرق يفسر شدة عقوبة القذف قياسا إلى السب، فضلا عن توافر ظروف مشددة وأسباب إباحة لا محل لها في الثانية، ومع ذلك فإن الصلة الوثيقة بين جريمتي القذف والسب تتجلى بوضوح في أن كل قذف يتضمن سبا، فمن ينسب إلى غيره واقعة إنما يضع الأساس الذي يمكن أن يستخلص منه حكم عام ينسبه إلى ذلك المجني عليه، ولو أن الجاني نسب إلى المجني عليه هذا الحكم فافترض الوقائع التي تدعمه دون أن يصرح بها لما ارتكب غير مجرد سب، ومن ثم يمكن القول بأن جريمة السب هي الجريمة الأساس من بين جرائم الاعتداء على الشرف والاعتبار فهي أبسطها أركانا، وسائر هذه الجرائم تفترضها ثم تزيد إليها المزيد من العناصر[3].

وعرفه نص المادة 297 ق.ع على أنه: "يعد سبا كل تعبير مشين، أو عبارة تتضمن تحقيرا، أو قدحا لا ينطوي على إسناد أية واقعة".

ثانيا: أركان جريمة السب المتصلة بالتكنولوجيا الحديثة، يمكن إجمالها أساسا فيما يلي:

1- الركن المادي: يتجلى الركن المادي لجريمة السب المعلوماتي في صدور نشاط إجرامي معلوماتي من شأنه خدش شرف واعتبار المجني عليه، يتمثل هذا النشاط في إسناد واقعة معينة إلى المجني عليه، شريطة ألا تتضمن واقعة محددة لأنها عند ذلك ستكون جريمة قذف، ومن أمثلة عبارات السب أن يوجه الجاني إلى غيره عبارات (يا كلب)، أو (يا سارق)..إلخ[4]، والنشاط الإجرامي في جريمة السب قد يكون كتابيا أو شفاهيا وإن كانت الصورة الغالبة في جريمة السب هنا أن يكون الإسناد قد جاء بصورة مكتوبة على شبكة الإنترنت إما على أحد المواقع الإلكترونية أو في إحدى صفحات التواصل الاجتماعي كبرامج فيسبوك وتويتر وغيرها دون أن يمنع ذلك من أن تأتي هذه الجريمة في صيغة معلوماتية قولية شفاهية وما أكثر هذه الصورة اليوم، ومن جهة أخرى يمكن أن يأتي هذا النشاط الإجرامي في صورة رسوم كاريكاتورية وما شابه منشورة على شبكة الإنترنت، ونشر عبارات السب بصورة معلوماتية من شأنه أن يحقق العلانية التي تطلبها المشرع في تطبيق النص الخاص بهذه الجريمة.

---

[1] حنان ريحان مبارك المضحكي، المرجع السابق، ص317.

[2] أحمد شوقي عمر أبو خطوة، المرجع السابق، ص289.

[3] محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، المرجع السابق، ص506 و507.

[4] وقضى بأن توجيه عبارات مثل لص أو نصاب أو مزور أو هاتك للأعراض أو سكير أو فاسق، تعد من قبيل السب، ومع ذلك فلا يمكن استبعاد صدور مثل هذه العبارات في صورة معلوماتية إلكترونية مما يجعلها من قبيل السب المعلوماتي.

مع ملاحظة أن عبارات السب يجب أن تكون موجهة إلى شخص معين ومحدد، لأن مناط الشرف والاعتبار المعتدى عليه في هذه الجريمة يتطلب تحديدا لشخص المجني عليه، من دون أن يعني ذلك أن يكون التحديد تفصيليا وبشكل دقيق، وإنما يمكن لمجموعة من الناس أن تتعرف عليه، ولعل المختص في تحديد ذلك هو قاضي الموضوع.

2- الركن المعنوي: جريمة السب جريمة شأنها شأن جريمة القذف جريمة عمدية، يتخذ الركن المعنوي فيها صورة القصد الجنائي العام بعنصريه العلم والإرادة، فعنصر العلم يتحقق بثبوت علم المتهم بمعنى الألفاظ التي صدرت عنه مع إدراكه لما يتضمنه هذا اللفظ من خدش للشرف والاعتبار، أما عن عنصر الإرادة فيعني وجوب توافر إرادة النطق أو الكتابة أو تسجيل عبارة السب ومن ثم ينتفي القصد إذا كان الجاني مكرها على إتيان النشاط المذكور وكذلك لو كان صغيرا أو سكرانا أو مخدرا بشكل غير عمدي ومن جهة أخرى يجب أن تتوافر لدى الجاني نية إعلان تلك العبارات التي صدرت.

وتجدر الإشارة أن المشرع الجزائري تناول جريمة السب في المادة 297 بقولها: "يعد سبا... إسناد أية واقعة"، وأقر لها العقوبات في المادتين 298 و298 مكرر، والمادة 299 ق.ع.

الفرع الثاني: التشهير والمضايقة في جرائم التكنولوجيا الحديثة

تعد جريمتا التشهير والمضايقة صورا من صور جرائم التكنولوجيا الحديثة.

البند الأول: جريمة التشهير المتصلة بالتكنولوجيا الحديثة

سنحاول التطرق إلى جريمة التشهير المتصلة بالتكنولوجيا الحديثة عبر شبكات التواصل الاجتماعي كنموذج.

أولا: تعريف التشهير، قال ابن فارس: الشين والهاء والراء أصل صحيح يدل على وضوح في الأمر، والشهرة وضوح الأمر[1]، تقول: شهرت الأمر من باب قطع وشهرة أيضا (فاشتهر) و(اشتهرته) أيضا (فاشتهر) و(شهرته) أيضا (تشهيرا) ولفلان فضيلة (اشتهرها) الناس، وتأتي الشهرة بمعني التشنيع؛ ظهور الشيء في شنعة حتى يشهره الناس، ومن التعاريف التي ذكرها بعض المعاصرين للتشهير: "هو إذاعة السوء عن شخص أو جهة"[2]، ويمكن القول بأنه نشر ما يسيء إلى الشخص سواء الحقيقي أو المعنوي بغرض فضحه والانتقاص منه.

من الطبيعي أن يكون لكل جريمة دوافع وأسباب، ومن أهم أسبابها الخلاف والخصومة بين المستخدم –غالبا ما تكون شبكات التواصل الاجتماعي– وبين المشهر به، وقد يكون سبب التشهير التعصب والجهل، وقد يكون سببه التنافس بين أفراد أو جهات تجارية وغير تجارية، ومن أهداف التشهير أيضا التي يتم استخدامها من قبل مستخدمي شبكات التواصل الاجتماعي هو الابتزاز، وإن كان الابتزاز جريمة مستقلة لكنها عادة يتبعها جريمة التشهير، حيث أن المبتز يحاول الحصول على مبتغاه من خلال الجريمة الأولى.

---

[1] معجم مقاييس اللغة، أحمد ابن فارس بن زكريا أبو الحسين، المتوفي عام 395ه، تحقيق وضبط عبد السلام محمد هارون، دار الفكر 1399ه-1979م.

[2] محمد ابن عبد العزيز الخضيري، أحكام التشهير، مجلة البيان، المنتدى الإسلامي، العدد 70، ص18.

ثانيا: أركان جريمة التشهير المتصلة بالتكنولوجيا الحديثة، جاء نظام مكافحة جرائم التكنولوجيا الحديثة بتجريم التشهير من قبل مستخدمي شبكات التواصل الاجتماعي سواء كان المشهر به من المستخدمين لبرامج شبكات التواصل الاجتماعي أو لم يكن منهم، إذ العبرة هي بمكان الجناية وبالمسئولية الجنائية التي تلحق الجاني في برامج هذه الشبكات.

1- الركن المادي: في الركن المادي لجريمة التشهير المتصل بالتكنولوجيا الحديثة من قبل أحد مستخدمي شبكات التواصل الاجتماعية لابد من توفر ثلاثة أمور:

- السلوك الإجرامي: وهو ما يصدر من الجاني إيجابا أو سلبا على المصلحة المحمية، والجاني في جريمة التشهير يقوم بهذا السلوك كتابة أو تصويرا أو نشرا عن طريق برامج التواصل الاجتماعي، والتي تعتبر مكانا خصبا للانتشار على نطاق واسع[1].

- النتيجة الإجرامية: وهي ما يترتب على الفعل من أضرار وآثار -غالبا تكون معنوية- معتبرة في التجريم والعقاب، إذ أن نشر ما يسيء إلى الشخص من سب وشتم أو قذف كل ذلك ضرر يعاقب عليه ويعتبر ركنا من أركان الجريمة.

- العلاقة السببية: هي الصلة ما بين فعل التشهير في برامج شبكات التواصل الاجتماعي وما نتج عنه من نتيجة سواء كانت مادية محسوسة أو معنوية.

ومن صور الركن المادي لجريمة التشهير من طرف مستخدمي شبكات التواصل الاجتماعي النشر الكتابي أو إعادته عن المشهر به، وذلك عبر النشر والكتابة سواء كانت صدقا أم افتراء عليه أو تشويها لصورته، وانتهاكا لكرامته عن طريق السب والقذف والفضيحة، أو التشهير بنشر الصور أو الفيديو سواء كانت حقيقية أم مركبة، ويكون التشهير كذلك بإنشاء حساب جديد وباسم وهمي، والتشهير من خلاله حينما يريد الجاني التخفي وعدم معرفة شخصيته ليقوم بالتشهير والنشر بلا قيد أو رادع، وقد يدخل ضمن هذه الجريمة جريمة أخرى وهي انتحال الشخصية حينما تتم تسمية الحساب باسم شخص معروف وإلحاق الضرر به وبالمشهر به أيضا. كما يكون التشهير عن طريق الوسم (هاشتاق "Hashtag"): ويعتبر من أخطر أنواع التشهير وأكثره شيوعا حيث لا يقتصر انتشار التشهير عند متابعي المستخدم الجاني، بل يتعداه لكل من يطلع على هذا الوسم، بل وأدعى إلى سرعة التداول والانتشار بشكل سريع وخطير.

2- الركن المعنوي: وهو القصد الجنائي العام (العلم والإرادة)، وهو مهم في تحقق الجرائم عموما، وتزيد هذه الأهمية في جريمة التشهير، حيث أنها المؤشر الرئيس في تحديد المسؤولية الجنائية.

وقد استقر القضاء على أن القصد الجنائي في جرائم القذف والسب والإهانة يتحقق متى كانت الألفاظ الموجهة إلى المجني عليه شائنة بذاتها[2]، ولا يمكن إثبات جريمة التشهير إلا بطريق الإستدلال والاستنتاج من الأفعال التي أتاها المتهم ومن الظروف والقرائن المحيطة بأفعاله، أما إذا تخلف العلم أو الإرادة فلا مسئولية جنائية كما ذكرنا سابقا.

---

[1] محمد محمد الألفي، جرائم النشر الإلكتروني، مركز تطوير الأداء والتنمية، مصر، 2009، ص83.

[2] محمد محمد الألفي، جرائم النشر الإلكتروني، المرجع نفسه، ص85.

البند الثاني: المضايقة في جرائم التكنولوجيا الحديثة

أولا: مفهوم المضايقة في جرائم التكنولوجيا الحديثة، هناك العديد من الأفعال التي لا تدخل في مفهوم الإيذاء أو الضرب أو الجرح لعدم وقوعها على الجسد المادي المقصود بها فلا تطاله بشكل مباشر ولا تحدث ضغطا عليه، إلا أنها قد تسبب للضحية الكدر والضيق والمعاناة والإزعاج أو الخوف أو المرض أو الجنون وأحيانا قد تكون السبب في وقوع جرائم أخرى كالقتل والاغتصاب، وهذه الأفعال قد تكون بتهديد الضحية أو بترصده[1]، كالتسكع على مقربة منه بقصد إزعاجه، أو مراقبته وتعقبه في كل الأمكنة التي يتواجد فيها أو منعه أو إعاقته من الوصول إلى مكان إقامته أو عمله أو أي مكان آخر يتردد إليه، أو موالاته بإرسال الخطابات والاتصالات الهاتفية غير المرغوب فيها والطرود سواء تضمنت تهديدا أم لم تتضمن، أو التصرف بأية طريقة تسبب لشخص أخر خوفا على سلامته.

ويدلل غالبية الفقه الإنجليزي والتشريعات الأجنبية على نمط السلوك الذي يتضمن الأفعال سابقة الذكر باصطلاح (Stalking Crime) والفقه الفرنسي باصطلاح (Les atteintes à la tranquillité des personnes) أو (harcèlement) وتعني ترجمتها للعربية (المضايقة) وهو مصطلح لم يتداول في الفقه العربي، واصطلاح (Stalking) هو اصطلاح حديث في القاموس الأجنبي[2] يمكن اعتباره وصفا لسلوك معين يقع بأشكال عديدة أكثر من كونها طائفة قانونية[3].

ويعرف اصطلاح المضايقة في هذا السياق بأنه سلوك تطفل غير مرغوب فيه ومتكرر يسبب للضحية المخاوف والأذى العاطفي أو الجسدي، فهو ظاهرة معقدة ذات سلسلة من البواعث المتضمنة الحقد أو الغيرة أو الغيظ أو الهوس أو حب ممارسة السيطرة على الآخرين[4]، وهذا السلوك قد يأخذ أشكالا عديدة تتضمن الملاحقة أو إبقاء الضحية تحت المراقبة، الاتصالات المتكررة والمزعجة، ترك شيء عدواني للضحية أو إلحاق الضرر بممتلكاته، وقد يستمر لفترة معتبرة من الزمن، وبالرغم من أن سلوك المضايقة في أغلب الأحيان يفتقر إلى العنف الجسدي إلا أنه يترك أثرا نفسيا بارزا على الضحية قد يتضمن قلقا أو اضطرابات في النوم أو التفكير بالانتحار أو الانهيار العصبي أو الاختلال العقلي والجنون[5].

---

[1] يعرف الفقهاء سلوك الترصد بأنه ملاحقة بشكل تطفلي للهدف أي الشخص المستهدف، كالبقاء مدة طويلة أمام منزله والقيام بالمراقبة المستمرة له والتسكع أو الظهور بشكل غير متوقع وغير مرحب به في المجال الخاص للضحية.

Ann W. Burgess, Timothy Baker, Deborah Greening, Carol R. Hartman, Allen G. Burgess John E. Douglas, Richard Halloran, Stalking Behaviors Within Domestic Violence, Journal of Family Violence, Springer, Berlin, Germany, Vol. 12, n°04, 1997, pp389–403. Paul Bocij Cyberstalking: Harassment in the Internet Age and how to Protect Your Family, Greenwood Publishing Group, Connecticut, United States, 2004, p04.

[2] The Oxford English Dictionary, example first cited in 1984.

[3] Celia Wells, Stalking, The Criminal Law Response, Criminal Law Review, London, England 1997, p463.

[4] Paul E. Mullen, Michele Pathé, Rosemary Purcell, Stalkers, Their Victims, Cambridge University Press, 2000, p157.

[5] Emma Ogilvie, Stalking: Legislative, Policing and Prosecution Patterns in Australia Australian Institute of Criminology, 2000, p19.

كما تعني جريمة المضايقة في النصوص القانونية التي تعرضت لها: "ارتكاب سلوك متكرر مع نية تسبيب أذى نفسي للضحية أو إثارة خشيته أو خوفه على سلامته أو سلامة غيره"[1]، فهذه النصوص لم تقتصر على سلوك التهديد فقط بل شملت كل سلوك قد يسبب لشخص معاناة ألم نفسي وعاطفي[2]، ولا تشترط غالبية التشريعات أن يتكرر حدوث الفعل الذي ينطبق عليه وصف المضايقة أو الملاحقة كي يعتبر مرتكبه مقترفا لجريمة مضايقة.

كان لظهور تكنولوجيا المعلومات الحديثة وانتشار وسائطها، وكذا التقدم العلمي أثرا مهما بالنسبة لأفعال المضايقة، بدأ الناس يدركونه مع بداية انتشار الهواتف واستعمالها من قبل المتصلين الذين يستخدمون لغة بذيئة، فاحشة...إلخ، والاتصالات المتكررة والمجهولة أو تلك التي تتضمن تهديدا[3]، فلم يقتصر دور تكنولوجيا المعلومات الحديثة على تزويد المجرمين بحزمة واسعة من الطرق الجديدة لارتكاب أفعال المضايقة فحسب وإنما ساعدت بتخطي الصعوبات التقليدية التي كانت تحول دون تحقيق ارتكاب العديد من أفعال المضايقة التي لا يستطيع الفاعل القيام بها وجها لوجه[4]، وهكذا برزت ظاهرة إجرامية جديدة أصطلح عليها الفقه جريمة المضايقة عبر وسائل تقنية المعلومات الحديثة.

وعرفت جريمة المضايقة المتصلة بالتكنولوجيا الحديثة بأنها نمط السلوك الذي يوجه إلى شخص معين عبر استخدام وسائل تقنية المعلومات الحديثة بنية إزعاجه، أو مضايقته، أو الضغط عليه أو تهديده أو تخويفه، وبمعنى آخر بنية التسبب له بأذى نفسي وعاطفي وأحيانا بأذى جسدي.

كما يعرفها بعض الفقهاء بأنها إرهاب عاطفي عبر استخدام وسائل تقنية المعلومات الحديثة لغرس الخوف من الأذى أو الموت في شخص ما، فهي شكل لاعتداء نفسي أو فكري، بحيث يقوم الجاني مرارا وتكرارا، وبدوافع مباشرة أو غير مباشرة يمكن إرجاعها إلى المجال العاطفي، وبشكل عام في مجال أفعال جريمة المضايقة تؤخذ بالاعتبار الميزات أو مجموعة الخصائص التالية: الخبث سبق الإصرار والترصد، الشدة، التكرار، الثأر، الغرض غير الشرعي، استهداف شخص بعينه[5].

ثانيا: أركان جريمة المضايقة المتصلة بالتكنولوجيا الحديثة، لا تختلف جريمة المضايقة في جرائم التكنولوجيا الحديثة عن أية جريمة أخرى تقليدية مقررة عن طريق قانون الجزاء من حيث أنها تتطلب لتحققها الأركان المتفق على ضرورة تحققها في أية

---

[1] Jonathan Clough, Principles of Cybercrime, Cambridge University Press, Cambridge, United Kingdom, 2nd Ed., 2015, p369.

[2] Naomi Harlin Goodno, Cyberstalking, a new crime: Evaluating the effectiveness of current state and federal laws, Missouri Law Review, n°72, 2007, p125.

[3] Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace, ABC-CLIO, California United States, 2010, p92.

[4] Raymond Wacks, Privacy in cyberspace: personal information, free speech and the Internet Privacy and Loyalty, Oxford, 1997, p93.

على سبيل المثال أظهرت دراسة أجريت في إحدى الكليات حول تعرض الفتيات لحوادث مضايقة، أن 40 بالمئة من أصل 696 حالة مضايقة تتضمن المضايقة عبر وسائل تكنولوجيا المعلومات الحديثة.

Bonnie S. Fisher, Francis T. Cullen, Michael G. Turner, Being Pursued, Stalking Victimization in a National Study of College Women, Criminology & Public Policy, Wiley Online Library 2006, p257.

[5] J. Laughren, Cyberstalking awareness and education - Sexuality research and social policy Journal of NSRC, Vol. 04, n°02, 2007, p27.

جريمة أخرى للتواجد على أرض الواقع، فبالإضافة إلى ضرورة توافر الركن الشرعي[1]، فإنه لا بد من وجود ركن مادي ملموس يعبر عن إرادة الفاعل بشكل جلي يمكن إثباته، ومن ثم لا بد أيضا من ركن معنوي يعبر عن إرادة مجرم تقنية المعلومات الحديثة.

ثالثا: صور المضايقة في جرائم التكنولوجيا الحديثة، بناء على ما تقدم نرى بأن جريمة المضايقة عبر وسائل تقنية المعلومات الحديثة تتخذ الصور التالية:

1- المضايقة عبر البريد الإلكتروني: يعرف البريد الإلكتروني بأنه: نظام للتراسل باستخدام شبكات الحاسبات، وتقوم فكرة البريد الإلكتروني على تبادل الرسائل الإلكترونية، والملفات والرسوم والصور، والصوتيات والبرامج...إلخ، وبالرغم من الفوائد الهائلة التي تقدمها هذه الخدمة إلا أنها من الممكن أن تتحول إلى قنبلة مدمرة تهدد الناس ومصالحهم فيما لو أسيء استخدامها ويشكل البريد الإلكتروني غير المرغوب فيه ذو المحتوى المثير للكراهية أو المتضمن موادا مسيئة وفاحشة أو تهديدا، واحدة من الأشكال الأكثر شيوعا للمضايقة عبر البريد الإلكتروني[2].

كما قد يتخذ سلوك المضايقة في جرائم التكنولوجيا الحديثة عبر البريد الإلكتروني مظهر التخريب، كقصف البريد الإلكتروني بإرسال الفيروسات التي تصيب ملفات الشخص المستهدف[3]، أو إرسال مئات أو آلاف الرسائل الإلكترونية غير المرغوب فيها، أي ما يعرف برسائل الخردة الإلكترونية، ما يؤدي إلى تدمير هذا البريد سواء كان العنوان البريدي لشخص أو شركة[4].

2- المضايقة بالتخاطب عبر الإنترنت (Chat)، ومنتديات المناقشة والمجموعات الإخبارية وصفحات الوب: يعرف التخاطب عبر الإنترنت بأنه خدمة التحدث بين المستخدمين من خلال الأجهزة المتصلة بشبكة الإنترنت بالكتابة، ومن الممكن أن تتم بالصوت والصورة.

وقد أصبح التخاطب المباشر أكثر شعبية بين مستخدمي الإنترنت مع ظهور أدوات حديثة، أين باتت غرف الدردشة والمجموعات الإخبارية من أكثر أنظمة التحادث شيوعا وشهرة في مجال التخاطب عبر الإنترنت ووسيلة مهمة تمكن مرتكبي جريمة المضايقة الإلكترونية من تحديد ومتابعة ضحاياهم والتشهير بهم وتهديدهم.

---

[1] يرى كثير من الشراح القانونيين عدم التسليم باعتبار الركن الشرعي (نص التجريم) ركنا في الجريمة، واستندوا في تأييد رأيهم هذا على الحجج التالية:
أولا: أن نص التجريم يصنع الجريمة، ومن غير المقبول من الناحية المنطقية القول إن الصانع أو المنشئ جزء وركن فيما صنع أو أنشأ.
ثانيا: لوكان نص التجريم ركنا في الجريمة، لترتب على إلغاء المقنن له أن تزول الجريمة بصفتها كائنا قانونيا، والواقع بخلاف ذلك إذ تظل الجريمة قائمة بكل مقوماتها بصفتها واقعة تاريخية ومنتجة لآثارها القانونية، حيث تعد سابقة بحق المجرم إذا ارتكب بعدها جريمة أخرى.
ثالثا: لوكان نص التجريم ركنا في الجريمة، لترتب على هذا استلزام إحاطة قصد الجاني في الجرائم العمدية بهذا الركن شأنه في ذلك شأن سائر أركان الجريمة ومقوماتها، وهذا لا يتسق مع مبدأ افتراض العلم بالنص المجرم وعدم الاعتداد بالجهل به. عبد الفتاح مصطفى الصيفي، قانون العقوبات، النظرية العامة دار الهدى للمطبوعات، مصر، 1998، ص153.

[2] Katie Dean, The Epidemic of Cyberstalking, WIRED Magazine (www.wired.com), 2000 visit: https://www.wired.com/2000/05/the-epidemic-of-cyberstalking/.

[3] حسن سعيد عبد اللطيف، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية، القاهرة، ط1، 1999، ص231 وما بعدها.

[4] Emma Ogilvie, Cyberstalking, Trends and issues in crime and criminal justice series, no. 166. Australian Institute of Criminology, Canberra, 2000, p166. McGraw D. K., Sexual harassment in cyberspace: The problem of unwelcome email. Rutgers Computer and Technology Law Journal, n°21, 1995, pp491–518.

وعندما يدخل الشخص إلى غرفة محادثة يظهر اسمه على الشاشة وينضم إلى قائمة أسماء الآخرين في المجموعة، بحيث تتخذ المضايقة الإلكترونية في مثل هذه الحالات البعد العلني والعام بدلا من البعد الخاص، فعندما يقوم شخص بإرسال رسالة إلى مجموعة محادثة إخبارية عامة، فإن هذه الرسالة يصبح متاح للجميع رؤيتها والاحتفاظ بنسخة منها، بالإضافة إلى هذا فإن اسم الشخص وبريده الإلكتروني ومعلومات حول مزود الخدمة متاحة بسهولة كجزء من الرسالة نفسها، وهذه الرسائل العلنية عبر مجموعات المحادثة يمكن الدخول إليها عبر أي شخص وفي أي وقت وحتى بعد مرور سنوات على كتابتها.

3- المضايقة عبر استهداف الأجهزة الخاصة بالضحية: في هذا النوع من المضايقة يقوم مرتكب الجريمة باستهداف الوسائل الإلكترونية الخاصة بالضحية كشكل من أشكال التخويف أو الإرعاب أو لهدف المراقبة، فالمجرم الذي يملك قدرة وكفاءة تقنية يستطيع أن يتحكم بالدخول إلى هذه الوسائل لجمع معلومات، لحذف أو تعديل بيانات أو ليمارس سيطرته عليها.

المطلب الثالث: الجرائم الجنسية الإباحية والواقعة على الآداب العامة عن طريق وسائل تقنية المعلومات الحديثة

لا شك أن عالمية نطاق وسائط تقنية المعلومات الحديثة أدى إلى تحولها إلى مساحة مفتوحة لممارسة جميع أنواع الإجرام الممكنة والمحتملة من جرائم جنسية وإفساد الأخلاق والتعرض للآداب العامة[1] التي هي في الأساس جرائم تقليدية موجودة بالفعل إلا أن وسائط تقنية المعلومات الحديثة سهلت عملية ارتكابها وخلقت منها شكلا جديدا ومتنوعا[2]، فانتشرت الأخطار الناجمة عن نشر وعرض المواد الخلاعية من كتابات ورسومات وصور وأفلام ورموز مخلة بالآداب العامة[3]، إضافة إلى التحريض على الفجور عبر المواقع والقوائم البريدية الإباحية وارتيادها والشراء منها والاشتراك فيها أو إنشائها.

وعليه لابد من القول ابتداء إلى أن هنالك عددا من الجرائم ذات البعد الأخلاقي والتي عاقب عليها المشرع في العديد من البلدان، ومع ما لها من بعد أخلاقي وجنسي إلا أنها في الحقيقة جرائم لا تقوم على أفعال الاتصال الجنسي الجسدي المادي بين طرفين أو أكثر، إنما هي جرائم تتناول حالات الفساد والإفساد الاجتماعي والترويج لها، كما في جرائم إنشاء المواقع ونشر الصور الإباحية والتعامل بها وترويجها وإرسالها، وسواء كانت موجهة إلى جمهور الأفراد بشكل عام أو موجهة إلى فئة القاصرين، فضلا عن أفعال التحريض المعلوماتي على الجرائم الجنسية الإباحية.

على الرغم من هذا الإجرام المستحدث يطال ضرره المتعاملين بوسائط تقنية المعلومات الحديثة بصرف النظر عن أعمارهم أو جنسهم، إلا أن واقع هذه الظاهرة الجرمية وغالبية الدراسات والجهود الدولية في هذا المجال أظهرت مدى الحاجة لحماية القاصرين

---

[1] والمقصود بالآداب العامة هو ما تعارف عليه الناس من خروج على الاحتشام مما تجرح رؤيته أو سماعه شعور الجمهور، كالصور والأفلام وغير ذلك، أيا كانت درجة الفحش الذي تمثله أو تنطوي عليه. محمد محرم محمد علي، خالد كدفور المهيري، قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة فقها وقضاء، دار الفتح للطباعة والنشر، أبو ظبي، ط2، 1999، ص930.

[2] أورين كير، نطاق الجريمة الافتراضية، ترجمة عمر محمد أبوبكر بن يونس، دار النهضة العربية، القاهرة، 2004، ص29.

[3] وهذه المواقع الإلكترونية الإباحية بغالبيتها تريد تحقيق الكثير من المكاسب المادية عن طريق زيادة مرتاديها، فإنها تشترط دفع مبالغ مالية مقابل الحصول على خدماتها المتمثلة في عرض وتحميل الأفلام الإباحية، لذا فإنها تحاول عمل ذلك عن طريق إعطاء مرتادي تلك المواقع العديد من الصور الجنسية بلا مقابل مادي، لتحاول جذب من يرتاد تلك المواقع إليها.

بشكل خاص من أن يكونوا عرضة لهذه المواد الإباحية، أو من أن يكونوا محلا لها مما يشكل أذى ماديا ومعنويا لهم، والملاحظ أن المشرع الجزائري لم يتدخل –شأنه شأن معظم التشريعات العربية– في معالجة جرائم العرض وإفساد الأخلاق في مواجهة تقنية المعلومات الحديثة، وإن كان قد جرم في القسم السادس من قانون العقوبات التعرض للأخلاق والآداب العامة بصورها التقليدية.

الفرع الأول: إنشاء المواد الإباحية أو نشرها أو ترويجها أو إرسالها أو التعامل بها عن طريق وسائل التكنولوجيا الحديثة

تقدم القول إن الجرائم الماسة بالجانب الأخلاقي للإنسان لا تقتصر على جوانب الاتصال أو الاعتداء الجسدي في صورته الجنسية التقليدية فحسب، بل قد تقع في أحوال عديدة تتجلى في نشر الصور والأفلام والرسوم الإباحية والتعامل بها وتخزينها ونشرها وإرسالها، والغريب والمريب في الأمر أن عدد هذه المواقع الإلكترونية بات اليوم بالآلاف وأن الدخول إليها بات سهلا جدا ومغريا بشكل ملفت للانتباه، وأن العديد من هذه المواقع هدفها تجاريا والآخر هدفها اجتماعيا تخريبيا، وكشفت العديد من الدراسات أن هنالك إقبالا كبيرا على ارتياد مثل هذه المواقع الإلكترونية، اليوم أصبح عدد مقاطع الفيديو والصور الإباحية المنشورة على الإنترنت يقدر بالملايين، والمشكلة التي تعاني منها البلدان الغربية أن نشر وتداول هذه المواد الإباحية يتم تبريره في الغالب بدواعي الحرية الشخصية والحق في حرية التعبير أما مشكلة أغلب البلدان العربية تتجلى في أن هذه المواقع الإباحية متاحة للجميع، والحقيقة أن الآثار المدمرة لهذه المواقع الإباحية باتت واضحة من خلال ارتفاع جرائم الاغتصاب ولاسيما تلك الواقعة على الأطفال.

وقد تناول المشرع الجزائري هذا النوع من الإجرام في القسم السادس من الفصل الثاني من الباب الثاني من قانون العقوبات تحت عنوان انتهاك الآداب فجاءت المادة 333 بقولها: "يعاقب بالحبس من شهرين إلى سنتين وبغرامة مالية من 500 دج إلى 2000 دج كل من ارتكب فعلا علانيا مخلا من أفعال الشذوذ الجنسي ارتكب ضد شخص من نفس الجنس تكون العقوبة بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 20000 دج إلى100000 دج".

وفيما يتعلق بالجرائم المتصلة بالكتابات أو الرسومات أو الصور أو الأفلام أو الرموز المخلة بالآداب العامة، فجاء في هذا الصدد نص المادة 333 مكرر بقولها: "يعاقب بالحبس من شهرين إلى سنتين وبغرامة من 000 20 إلى 000 100 دينار كل من صنع أو حاز أو استورد أو سعى في استيراد من أجل التجارة أو وزع أو أجر أو لصق أو أقام معرضا أو عرض أو شرع في العرض للجمهور أو باع أو شرع في البيع أو وزع أو شرع في التوزيع كل مطبوع أو محرر أو رسم أو إعلان أو صور أو لوحات زيتية أو صور فوتوغرافية أو أصل الصورة أو قالبها أو أنتج أي شيء مخل بالحياء".

تقوم هذه الجرائم كغيرها من جرائم التكنولوجيا الحديثة على مجموعة من الأركان تتمثل أساسا فيما يلي:

أولا: الركن المادي، يتطلب الركن المادي في هذه الجرائم تحقق السلوك أو النشاط الإجرامي المنصوص عليه في التشريعات المتقدمة، أي استخدام الشبكة المعلوماتية أو وسائل تقنية المعلومات في إنتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية، ما لم يكن ذلك لأغراض علمية فنية مصرح بها، أو لأغراض رسمية لم يجزها القانون، ومن صور السلوك الإجرامي الأخرى، إنتاج أو إعداد أو تهيئة أو إرسال أو الخزن بقصد الاستغلال أو التوزيع أو العرض على الغير عن طريق الشبكة المعلوماتية

أو إحدى وسائل تقنية المعلومات، ما من شأنه المساس بالآداب العامة، وبتقديرنا فإن هذه الجرائم من جرائم الخطر (جرائم السلوك) التي لا تتطلب تحقق نتيجتها الضارة، فهي تقوم بمجرد تحقق السلوك الإجرامي المنصوص عليه قانونا.

ثانيا: الركن المعنوي، لا تقوم هذه الجرائم على تحقق النشاط الإجرامي فحسب بل لابد من تحقق القصد الجنائي الذي يقوم على عنصري العلم والإرادة، أما لو وقعت هذه الجرائم أو أحدها بشكل خاطئ غير مقصود أو وقع هذا النشاط لأغراض علمية فنية مسموح بها قانونا، فلا تقوم الجريمة عند ذلك، ومن المفيد الإشارة إلى أن صور هذه الجرائم تقوم ولكن دون أن تترتب المسؤولية الجنائية لفاعلها في حال لو ارتكبت تحت وطأة أحد موانع المسؤولية الجنائية كالإكراه، الضرورة، صغر السن، الجنون، أو السكر والتخدير غير العمدي.

الفرع الثاني: التحريض على ارتكاب الجرائم الجنسية والإباحية المتصلة بالتكنولوجيا الحديثة

نصت معظم التشريعات الجنائية التقليدية على جرائم التحريض بوجه عام، فيما ذهبت التشريعات المتخصصة بجرائم التكنولوجيا الحديثة إلى تجريم التحريض على الجرائم الإباحية والجنسية المتصلة بالتكنولوجيا الحديثة، وتناول مفهوم التحريض على هذا النوع من الجرائم وبيان أركانها.

البند الأول: مفهوم التحريض المعلوماتي لارتكاب الجرائم الجنسية والإباحية

ابتداء لابد من القول إن التحريض هنا يحتمل صورتان، أولهما التحريض على ارتكاب الجرائم الجنسية معلوماتيا، أي أن التحريض هنا يأتي في صورة معلوماتية بواسطة وسائل تقنية نظم المعلومات بغية حمل الغير على ارتكاب جرائم جنسية معلوماتية أو تقليدية واقعية مادية، وثانيهما التحريض المعلوماتي على ارتكاب الجرائم الجنسية المعلوماتية فحسب، أي من خلال إنشاء ونشر مواقع وصور إباحية والتشجيع على التعامل بها وترويجها معلوماتيا.

وعلى العموم فإن التحريض لغة هو الحث على الشيء، وحرضه أي حثه[1]، وقد قال تعالى: "...وحرض المؤمنين عسى الله أن يكف بأس الذين كفروا..."[2]، وقوله تعالى: "يا أيها النبي حرض المؤمنين على القتال..."[3].

والتحريض في مفهومه البسيط عندنا هو دفع الغير–بأحد وسائل التكنولوجيا الحديثة– إلى ارتكاب جريمة تقليدية أو متصلة بالتكنولوجيا الحديثة، أو هو خلق فكرة الجريمة في ذهن الغير بعد أن كان الذهن خاليا منها أو مترددا إزاءها، أو هو حمل الغير معلوماتيا على ارتكاب جريمة ما، أو هو الإيحاء المعلوماتي للغير بالجريمة أو دعوته إليها،...إلخ، وبهذا المعنى يختلف التحريض عن الاتفاق الجنائي في أن إرادة المحرض تعلو على إرادة من يقوم بتحريضه لأن الأول هو صاحب فكرة الجريمة وهو من يقوم بخلق التصميم عليها لدى الغير، فيما نجد أن الاتفاق تتساوى فيه إرادة المتفقين.

---

[1] المنجد في اللغة، المطبعة الكاثوليكية، لويس معلوف، المجلد 01، بيروت، ص126.

[2] سورة النساء، الآية 84.

[3] سورة الأنفال، الآية 65.

وللتحريض صورتان، الأولى يكون فيها تحريضا فرديا ويسمى بالتحريض الخاص، وفيه تتوجه أفعال الحث والحمل وخلق فكرة الجريمة إلى شخص معين أو أشخاص معينين، وليس هنالك وسيلة محددة لكي يقع هذا النوع من التحريض بها، أما الصورة الثانية فيكون فيها التحريض عاما (التحريض الجماعي) وفيه تكون أفعاله موجهة إلى الجمهور، بمعنى أنه لا يوجه إلى أشخاص معينين بذاتهم، فهم غير معلومين أو محددين للمحرض، والحقيقة أن هذا النوع من التحريض لا يقع في تقديرنا إلا بإحدى طرق العلانية التي ينص عليها القانون ولعله الأقرب إلى التحريض – محل دراستنا- الذي غالبا ما تتوجه فيه وسائل التحريض إلى عدد غير معين أو محدد من الأفراد.

وبهذا الخصوص ذهب عدد من التشريعات المتخصصة بجرائم التكنولوجيا الحديثة إلى تجريم أفعال التحريض المعلوماتي على ارتكاب الجرائم الجنسية والإباحية، ومنها المشرع الجزائري الذي ذهب إلى القول في المادة 347 ق.ع: "يعاقب بالحبس من ستة أشهر إلى سنتين وبغرامة من 20000 دج إلى 000 100 دج كل من قام علنا بإغراء أشخاص من أي من الجنسين بقصد تحريضهم على الفسق وذلك بالإشارة والأقوال أو الكتابات أو بأية وسيلة أخرى".

البند الثاني: أركان جريمة التحريض الجنسي المتصلة بالتكنولوجيا الحديثة

أولا: الركن المادي، من الواضح أن التحريض في صورته المتصلة بالتكنولوجيا الحديثة يعد من جرائم الخطر، أي تلك التي لا تشترط حصول نتيجة لقيامها، وقد يقع السلوك هنا باستخدام أية وسيلة من وسائل ارتكاب جرائم التكنولوجيا الحديثة وأبرزها شبكة الإنترنت، سواء تم ذلك عن طريق نشر الصور الإباحية أو مقاطع الفيديو أو نشر قصص جنسية إباحية يراد منها تشجيع الغير على القيام بممارسة الجنس أو حثهم على المشاركة في هذه الأنشطة الإباحية المعلوماتية، ولا يشترط أن يكون هذا التحريض موجها إلى فئة معينة فيما خلت النصوص التي عالجت موضوع التحريض المعلوماتي الموجه إلى القاصرين والتي سنأتي على بحثها لاحقا.

ثانيا: الركن المعنوي، لا يكفي لقيام جريمة التحريض في هذا النوع من الجرائم أن يقوم الفاعل بالسلوك أو النشاط الإجرامي، بل لابد من توافر الركن المعنوي الذي يتطلب هنا قصدا جنائيا عاما بعنصريه العلم والإرادة، أي أن يعلم الفاعل أن نشاطه سيؤثر في نفسية الشخص المخاطب (المحرض) وأن من شأن الوسائل التحريضية التي يقوم بها الفاعل أن تحمل الغير على ارتكاب الجريمة، وأن تتجه كذلك إرادة الجاني إلى خلق فكرة الجريمة لدى المخاطب (المحرض)، ونرى أن التحريض على ارتكاب الجرائم الإباحية والجنسية المتصلة بالتكنولوجيا الحديثة يتطلب في كثير من الأحيان قصدا جنائيا خاصا يتمثل في حث الغير على ارتكاب أفعال الفجور أو الدعارة أو في مساعدته على ذلك على وفق ما نصت عليه العديد من التشريعات.

البند الثالث: صور التعرض للآداب وإفساد الأخلاق والحض على الفجور عبر وسائل تقنية المعلومات الحديثة

إن انتشار الجرائم الماسة بالأخلاق والآداب العامة والحض على الفجور والدعارة عن طريق وسائط تقنية المعلومات الحديثة يؤدي بتلك الوسائط إلى اعتبارها جزءا من هذه الجريمة سواء كانت وسيلة لارتكابها أو محلا للجريمة ذاتها، وذلك لما تحفل به هذه

الوسائط من خدمات يساء استخدامها للتعرض للآداب وإفساد الأخلاق والحض على الفجور، وجميع هذه الصور ترتكب عن طريق تقنية المعلومات الحديثة من خلال المبادلات الإلكترونية الكتابية أو الصوتية أو الفيديوية سنحاول التطرق بإيجاز إلى أهمها.

أولا: البريد الإلكتروني (Electronique mail)، كما أشرنا سابقا فإن البريد الإلكتروني يعتبر نظاما للتراسل باستخدام مختلف الوسائل الإلكترونية من حواسيب وأجهزة ذكية يشترط امتلاكها خاصية الاتصال بالإنترنت، يوفر إمكانية التواصل بملايين البشر حول العالم كبديل للبريد التقليدي ويمكن من خلاله كتابة الرسائل وتضمينها الصور والفيديو، أو إرسال واستقبال الرسائل الصوتية أو السمع بصرية من أي مستخدم لشبكة الإنترنت، ويقع التعرض للآداب وإفساد الأخلاق والحض على الفجور عبر البريد الإلكتروني بما يوزع على الناس من الكتابات أو الرسوم أو الصور أو الأفلام والشارات والتصاوير على اختلافها وغير ذلك من الأشياء المخلة بالحياء، بحيث يتم النشر والإذاعة عبر البريد الإلكتروني من خلال إرسال الرسالة المتضمنة المواد المسيئة أو التي تشكل تحريضا على الفجور إلى أكثر من شخص، بأن يتم تداول الرسالة بين أكثر من مستخدم لشبكة الإنترنت سواء عن طريق الإرسال المباشر إليهم أو غير المباشر.

ثانيا: شبكة الوب العالمية (World wide web)، لكل مستخدم لشبكة الإنترنت أن ينشئ له موقع (site)[1] على شبكة الوب العالمية، تتضمن معلومات يمكن إعادة تخزينها والتي يمكن لأي مستخدم آخر في جميع أنحاء العالم استقبال هذه المعلومات من خلال نظم الاستقبال، الأمر الذي جعل شبكة الوب تحفل بالمواقع التي تدعو بشكل سافر وصريح للرذيلة والبغاء وتقدم خدماتها للجمهور بمقابل أو بدون مقابل، بل وتقوم تلك المواقع بالتعريف عن نشاطها والدعاية لها بإرسال آلاف الرسائل الإلكترونية لمستخدمي الشبكة، وفي ظل عالمية هذه الشبكة وانتشارها أصبح بإمكان أي فرد الولوج لتلك المواقع والإطلاع على ما تتضمنه من مواد مخلة بالآداب، بل والتواصل عبر هذه المواقع والانضمام لعضويتها، حتى وإن كانت قوانين دولته قد تمنع تلك المواقع أو تجرمها[2].

ثالثا: مجموعات الأخبار (News groups)، كما تقدم معنا في هذه الدراسة، بأن مجموعات الأخبار عبارة عن مناطق مناقشات عامة عبر شبكة الإنترنت، يمكن من خلالها التحدث حول أي موضوع، مع إمكانية تبادل مختلف الصور والمعلومات، ويتم ذلك من خلال نظام News groups أو نظام UseNet وكلاهما عبارة عن مجموعات أخبار، لكن يختلف أحدهما عن الأخر من ناحية إقامة المسؤولية الجنائية حول مراقبة وتوزيع الوثائق[3]، ونجد أن صور التعرض للآداب وإفساد الأخلاق

---

[1] كلمة site (موقع) تعني عقلا إلكترونيا ذو سعة كبيرة، يرتبط مباشرة بمجموعة من شبكات الإنترنت، وذلك لتخزين واستقبال وتوزيع المعلومات ويتطلب بناء موقع على الإنترنت أو صفحة رئيسية (home page) خادم ويب ومحتوى معلوماتي.

[2] هناك تقرير نشرته شبكة (CNN) الإخبارية في موقعها الإلكتروني، بينت فيه أن سهولة الوصول للملفات الإباحية أضحت بنفس سهولة الوصول لملفات الموسيقى، وبالتالي فإن تحميل الملفات الإباحية يتم بنفس السهولة التي تتم عند تحميل ملفات الموسيقى، نشر التقرير في 2003/03/15 تحت عنوان: سهولة الوصول للملفات الإباحية في الموقع الإلكتروني: www.cnn.com

[3] ففي مجموعات أخبار New Group لا تثار مشكلات خاصة من ناحية المسؤولية الجنائية، ولا ينطبق عليها نظام المسؤولية المطبقة في مواد وسائل الإعلام المرئية والمسموعة، والتي تعني بأن شخصا يمارس صحافة ويقوم بمراقبة وتوزيع هذه الوثائق، حيث أن هذا النظام يستخدم بواسطة الإنترنت ويتم بواسطة إدارة المعلومات ومراقبة توزيعها، أما نظام UseNet فهو عبارة عن أحد الأنظمة التي تقدم خدمة بالإنترنت ويقوم بواسطتها المستخدم عن طريق استخدام نظام اوتوماتيكي يبث رسالة أو عدد من الرسائل إلى مجموعة من المستخدمين أو المشتركين، وبالتالي يمكن إقامة المسؤولية الجنائية=

والحض على الفجور تمارس من خلال مجموعات الأخبار عبر ما يتبادله المتعاملين بهذه المجموعات من الأشياء المخلة بالحياء.

رابعا: غرف المحادثات والدردشة Chat Rooms، مر معنا فيما سبق بأن غرف المحادثة عبارة عن ساحات معروفة في الفضاء الافتراضي تتيح لمستخدميها الاشتراك في محادثات بين بعضهم البعض، فالتخاطب عبر هذه الغرف يتم بأن يكتب المستخدم رسالة حيث يمكن للآخرين رؤية ما يكتب الذين يكتبون رسائل بدورهم، ويتم التعرض للآداب وإفساد الأخلاق والحض على الفجور وغالبا ما تكون من خلال الكتابة.

الفرع الثالث: جرائم التكنولوجيا الحديثة الجنسية المتعلقة بالقاصرين

امتدت نوازع الشر ومظاهر الإجرام الإلكتروني لتطال فئة عمرية تحظى أصلا بالحماية والرعاية الخاصة سواء كان على المستوى الاجتماعي أو القانوني، نظرا لحداثة السن وقلة الخبرة، وهذه الفئة هي فئة القاصرين في المجتمع، ويندرج ضمن مفهوم القاصر من وجهة نظر القانون كل من لم يصل سن البلوغ، ذكورا أو إناثا، وفقا لأحكام القانون الوطني، على أن تراعى الفروقات بتحديد سن البلوغ لدى بعض التشريعات المقارنة.

فمع اتساع نطاق بيئة الإنترنت، وتنوع الأنشطة والمهارات المتعلقة بها، ودخول فئات عمرية حديثة مجالات واسعة لتقنية نظم المعلومات، سعيا للاستفادة من خدمات هذه التقنية، واعتمادهم عليها، وغياب وعي الأهل والبيئة المحيطة، وقلة المراقبة، فقد أصبح القاصرون موضوع اعتداءات متكررة، أخذت بالاتساع بإتباع تقنية نظم المعلومات واستخداماتهم المختلفة لها، كما أصبح استهداف القاصرين عبر الإنترنت يتزايد مع مرور الزمان، دون رادع أو زاجر حقيقي، وهو يأخذ على العموم مظاهر الاستغلال الجنسي بمختلف صوره وأشكاله[1]، من خلال توفر تقنية الإنترنت ومواقع مشبوهة والتي تلعب دورا رئيسيا في اتساع نسبة استغلال القصر جنسيا عبر الإنترنت.

البند الأول: صور الاعتداءات على القصر

قد لا يكون بالإمكان رصد كافة صور الاعتداءات الجرمية الواقعة على القاصرين هنا، ومع ذلك سنتولى بحث المحور الأكثر انتشارا من تلك الاعتداءات وهو الاستغلال الجنسي للقاصرين عبر شبكة الإنترنت، هذا المحور الذي تتفرع عنه العديد من صور الاعتداءات المرتبطة به، والتي تنسجم فيما بينها في أن الضحية فيها هو القاصر ذكرا كان أو أنثى، نبحثها فيما يلي:

أولا: تحريض القاصرين على الأعمال الجنسية، هناك مواقع على شبكة الإنترنت متاحة للكافة، متخصصة بالجنس ذات بوابات ونوافذ مغرية للقاصرين، يتم الوصول إليها مباشرة عبر إدخال العنوان الإلكتروني في شريط العناوين، يبدأ الموقع بعرض

=للأشخاص الذين يقومون بإدارة هذا النظام إذا ما ثبت أنهم قد أخذوا موقع أحد المجموعات غير المشروع (أي رسائل ومعلومات يعاقب عليها القانون) وعلى العكس من ذلك، فقد أصدر مجلس الدولة الفرنسي حكم في عام 1991 يذهب فيما يبدو إلى استبعاد UseNet من تطبيق القوانين الخاصة بالصحافة المرئية والمسموعة، والتي تنطبق على تبادل المعلومات أو الرسائل ما بين المستخدمين للشبكات التلفزيونية. أحمد حسام طه تمام، المرجع السابق، ص327.

[1] وفقا لمجلة إنترنت فيلتر فإن دخل تجارة الجنس عبر الإنترنت بلغ 97.06 مليار دولار عام 2012 بلغت فيها نسبة استغلال الأطفال ثلاثة مليارات دولار من نفس الفترة.

مواده تلقائيا، والخطير أن معظم هكذا مواقع هي مواقع مجانية، يمكن الدخول إليها بمطلق السهولة، ودون تكلفة مادية تذكر، وتجدر الإشارة إلى نقطة أخرى أكثر خطورة إذ تتيح تقنية تلك المواقع الدخول إليها عبر مواقع أخرى يصدف أن المتصفح يعمل عليها وذلك أثناء أو عبر الاشتراك باتصال مع مواقع أخرى، حيث لا يجد القاصر نفسه إلا وهو داخل موقع للإباحة الجنسية، ويصدف أن يدخل القاصر إلى موقع ما يتعلق بمواد الإباحة الجنسية، ويجد نفسه فريسة سهلة لمروجي هذه التجارة، تعرض تلك المواقع فرصا للاتصال الجنسي، وتمهد له وتعرض مساعدات بترتيب لقاءات وهمية مع الطرف الآخر، وذلك للقيام بعمل جنسي معين، وفق منظومة وصور ومقاطع فيديو تصف الحال، بهدف إغواء القاصرين على أعمال جنسية معينة، أو تحريضهم للقيام بها، سواء بصورة منفردة أو بصورة جماعية، وغالبا ما تدفع تلك المواقع القاصرين دخول مواقعها من خلال الوعد بجائزة، أو مسابقة مغرية ونحو ذلك.

وقد جرم المشرع الجزائري هذا الفعل حسب ما تضمنته المادة 342 ق.ع: "كل من حرض قاصرا لم يكمل الثامنة عشرة (18) سنة على الفسق أو فساد الأخلاق أو تشجيعه عليه أو تسهيله له ولو بصفة عرضية، يعاقب بالحبس من خمس (05) سنوات إلى عشر (10) سنوات وبغرامة من 20000 دج إلى 100000 دج.

ويعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات المقررة للجريمة التامة".

ثانيا: إنتاج صور فاضحة للقاصرين، تتنوع صور الإنتاج بحد ذاتها مستخدمة تقنية الإنترنت والحاسب الآلي والأجهزة الإلكترونية الذكية، وتضع هذه التقنية بين يدي الفاعل منظومة غير محددة لسبل إنتاج صور جنسية فاضحة للقاصرين ذكورا أو إناثا، بعضها قد يكون حقيقيا حصل عليه الفاعل بطرق غير مشروعة، يروجها كما هي، وأخرى وهي الأكثر والأعم، صور ومقاطع غير حقيقية، تدخل منظومة تقنيات الدبلاج والتحوير ونحو ذلك، ثم يعاد استغلال المنتج في الجريمة واستغلال القاصرين بها.

والحقيقة أن استغلال القاصرين هنا يكون بأحد الأمرين، إما أن يكون القاصر هو مادة الإنتاج الجنسي، سواء تمثل ذلك بالصور الفوتوغرافية، أو مقاطع الفيديو، ثم إعادة ترويجها، أو أن يكون القاصر هو هدف الاستغلال السابق ومادته، في آن واحد فمخرجات الإنتاج صورا كانت أو مقاطع فيديو توجه هنا إلى القصر، وهو ما تناوله المشرع الجزائري في المادة 333 مكرر 1 ق.ع.

ثالثا: استغلال الأطفال القاصرين جنسيا، لابد ابتداء أن تتوافر حالة فاضحة لأحد القاصرين ذكرا كان أم أنثى بين يدي الفاعل، فالشرط هنا أن تكون المادة الفاضحة ذات علاقة بالقاصر، من حيث اعتباره موضوعا لها، فهو محور بنائها، مما يظهر لنا تعاظم الاستغلال غير المشروع للقاصرين عبر تقنية نظم المعلومات، واعتبارهم وسيلة الاعتداء وموضوعه في آن معا.

ولعل أهم صور استغلال القصر جنسيا عبر تقنية المعلومات الحديثة[1] تتجلى في توزيع، بيع وتداول، نشر، وبث الصور الفاضحة عبر منظومة الإنترنت، ويستوي هنا أن يحصل الفاعل على الصور الفاضحة للقاصرين لمنفعته الخاصة بغية استغلالها الشخصي، أو لمنفعة الغير، أو لاستغلال الغير الخاص، أو حتى لغايات استثمارية، المهم ألا نقف في مفهومنا لاستغلال القاصرين جنسيا عند حد النمط المادي للاستغلال، فهو وإن كان أحد صور الاستغلال، إلا أنه لا يشمل كافة الصور، خصوصا مع دخول

[1] عرفت الاتفاقية الأوروبية حول جرائم الإنترنت في 2001 صور الأطفال الفاضحة بأنها المواد التي توضع بالتصوير المرئي أحد القاصرين منشغلا بارتكاب فعل أو سلوك جنسي فاضح.

تقنية نظم المعلومات وتطور وسائل الاتصالات التقنية المتعلقة بانسياب المعلومات والمواد المسجلة إلكترونيا، واتساع نطاق توزيعها عبر العالم.

وقد عالج قانون العقوبات الجزائري هذا السلوك في المادة 333 مكرر 1 التي تنص على أنه: "يعاقب بالحبس من (05) سنوات إلى عشر(10) سنوات وبغرامة من 500000 دج إلى 1000000دج، كل من صور قاصرا لم يكمل 18 سنة بأي وسيلة كانت وهو يمارس أنشطة جنسية بصفة مبينة، حقيقية أو غير حقيقية، أو صور الأعضاء الجنسية للقاصر لأغراض جنسية أساسا، أو قام بإنتاج أو توزيع أو نشر أو ترويج أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد إباحية متعلقة بالقصر...".

رابعا: أعمال الدعارة والترويج لها، لا يقتصر استغلال القاصرين جنسيا عبر شبكة الإنترنت على حالات إنتاج صور إباحية خاصة بهم، ونشرها أو بثها أو تداولها عبر الشبكة، وإنما قد يتخذ الاستغلال صور ارتكاب القصر لأعمال الدعارة، وإظهار ذلك من خلال صور أو أفلام مصورة تظهرهم بحالات القيام بأعمال جنسية مختلفة، سواء مع بعضهم البعض أو مع بالغين، ليس هذا فحسب؛ بل قد تتخذ أعمال الدعارة هنا استهداف القاصرين بأفلام وصور جنسية للبالغين، تمرر عبر وسيلة اتصال معينة، أو عبر تقنية شبكة الإنترنت للقاصرين، بحيث يضمن علمهم بها، سواء برغبتهم، أو رغما عنهم، من خلال مواقع متخصصة أو عبر اختراقات منظمة مسبقا في حال دخول القاصرين عبر مواقع أخرى معينة قد لا تكون موثوقة، أو عبر اختراق البريد الإلكتروني الخاص بأحد القاصرين، وإرسال ملفات ذات محتوى جنسي له، وقد بحث قانون العقوبات الجزائري هذه المسألة وأورد لها نصا تجريميا في المادة 344.

البند الثاني: أركان هذه الجرائم

أولا: الركن المادي، يتمثل الركن المادي لهذه الجرائم الجنسية والإباحية الواقعة على فئة القاصرين في أفعال تسجيل أو نقل صورة قاصر إذا كان لهذه الصورة طبيعة جنسية، وكذلك صنع أو نقل أو عرض بأي وسيلة كانت أية مادة إباحية تتعلق بالقاصرين أو رسالة لها طبيعة جنسية أو إرسال أو نشر عن طريق نظام معلومات أو الشبكة المعلوماتية قصدا، كل ما هو مسموع أو مرئي يتضمن أعمالا إباحية يشارك فيها أو تتعلق بالاستغلال الجنسي وما شابه، وبعبارة أخرى يكون النشاط الإجرامي لهذا النوع من الجرائم في كل الأفعال الجنسية والإباحية غير المشروعة الموجهة إلى القاصر أو من هو في حكمه، ونرى أن هذه الجرائم في صورها لا تتطلب نتيجة إجرامية شأنها في ذلك شأن الجرائم الجنسية والإباحية الأخرى الموجهة إلى غير القاصرين فهي جرائم تقوم بمجرد السلوك، جرائم خطر وليست جرائم ضرر.

ثانيا: الركن المعنوي، تعد هذه الطائفة من الجرائم، جرائم عمدية ومن ثم فلابد من توافرها على القصد الجنائي العام بعنصريه العلم والإرادة أي أن يكون الجاني عالما بأنه يقوم بنشاط إجرامي موجه إلى القاصرين بحيث يعلم أن نشاطه يشكل جريمة وأن يوجه هذا النشاط إلى هذه الفئة كما يجب أن تتجه إرادته إلى هذه الأفعال ومن ثم فلا تنطبق نصوص التجريم المتقدمة إذا توجهت تلك الأفعال إلى غير فئة القاصرين وإن كانت ستشكل جريمة أخرى تنطوي تحت نصوص تجريمية أخرى، كما لا تنطبق هذه النصوص إذا كان الفاعل مكرها أو صغيرا أو مجنونا وما شابه.

البند الثالث: الجهود الدولية لمكافحة الظاهرة

أمام هذا كله ولتعاظم الظاهرة وعظم خطورتها فقد تظافرت الجهود الدولية للحد من ظاهرة الاعتداء على القصر جنسيا واستهدافهم بمختلف الأنشطة الموضحة سابقا، ومن أبرز الجهود الدولية في هذا الإطار، ما خرج به منتدى الشرق الأوسط وشمال إفريقيا حول أمن الأطفال عند استخدام الإنترنت، المنعقد في مصر في الفترة 25-30 يونيو2005، وقد ركزت الاتفاقية على التنبيه إلى أن المقصود من الاعتداءات المستهدفة للقاصرين جنسيا هي تلك التي تتخذ منهم مادة لها، فالفاعل يعمد إلى إنتاج مادته الجنسية الفاضحة من القاصرين أنفسهم، ولا ينصرف المعنى إلى حالات ترويج صور أو مقاطعة الأفلام المنتجة من قبل الكبار على القاصرين، وفي هذا التحديد تضييقا لنطاق الجريمة، وإن كان القصر هم هدف الحماية وأساسها، فإن هذه الحماية يجب ألا تقف عند حد يمكن معه استمرار الاعتداءات على القاصرين دون رادع فعال، إلى حد القضاء على تلك المظاهر الجرمية.

وعليه فلا بد من أن يطال التجريم كافة أشكال وصور الاعتداءات المستهدفة للقاصرين، سواء كانت المواد الجنسية الإباحية منتجة منهم، أي باعتبارهم موضوع الفعل الفاضح، أو كانوا هم هدفها أم المخاطبون بها.

وعلى المستوى العربي كانت الاتفاقية العربية لمكافحة جرائم تقنية نظم المعلومات والتي أوردت في المادة 12 منها ما يؤكد ملاحقة المجرمين التقنيين حماية للقاصرين من أي استغلال جنسي عبر الإنترنت، وإن كان النص يبحث في الجرائم الإباحية إلا أن اهتمام النص التجريمي بالقاصرين جاء من حيث التشديد في العقاب كلما كان المجني عليه في الأفعال الموصوفة بالنص قاصرين.

المطلب الرابع: جرائم نظم الاتصالات

مهدت نظم الاتصالات البعدية المحصورة منها وتلك المفتوحة عالميا لظهور مساحات أكبر لجرائم التكنولوجيا الحديثة سواء من حيث وسيلة الارتكاب أو من حيث طبيعة وشكل الجريمة، مما أظهر للواقع أنواعا جديدة من الجريمة التقنية تقوم أساسا على الاستفادة من تكنولوجيا الاتصالات التقنية.

الفرع الأول: جريمة اختراق نظم الاتصالات بطريقة غير مشروعة

تعتبر هذه الصورة المستحدثة من الجرائم ذات الصلة الوثيقة بنظم المعلومات، إذ يشكل اختراق تلك النظم التقنية محور السلوك الجرمي، والركن المادي فيها، وهي بصفتها تلك؛ لا تتعلق بنظم الاتصالات المتاحة، والتي تفتقر إلى نظم الحماية الإلكترونية ذلك أن علة التجريم هنا هي في الاختراق ذاته، هذا الاختراق القائم على الدخول عنوة وبغير رضا صاحب النظام إلى هذا النظام بغض النظر بعد ذلك عن هدف أو قصد ودافع الفاعل، ولا تتوافر هذه العلة حيث لا وجود لنظم الحماية وأمن الشبكات ولا أهمية بعد ذلك لمدى قوة نظم الحماية أو ضعفها، ولا إلى الوسيلة التي استخدمها الفاعل في تحقيق الاختراق، ثم لا أهمية لطبيعة نظم المعلومات، ومدى أهمية المعلومات والبيانات لصاحب النظام أو لغيره ولطبيعتها.

ويظهر السلوك الجرمي بظهور الركن المادي القائم على إتيان الفاعل لسلوك تقني، ذو بعد فني محله نظم المعلومات المحمية ويتحقق اختراق نظم الحماية فيها دخولا إلى النظام، سواء تحقق الدخول الكلي أو اقتصر على مجرد دخول جزئي، ثم إمكان التجول فيه بكل حرية دون أدنى حق للفاعل في إجراء ذلك[1].

البند الأول: الدخول أو البقاء في النظام

نص المشرع الجزائري على هذه الجريمة في المادة 394 مكرر بقوله: "يعاقب بالحبس من 03 أشهر... كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك..."، يمكن القول وإنطلاقا من نص المادة أنه ولقيام هاته الجريمة لابد من اشتمالها على ركنين ألا وهما المادي والمعنوي وهو ما سيتضح كما يلي:

أولا: الركن المادي، الواضح من صياغة هذا النص أنه تضمن صورتين للركن المادي لهذه الجريمة، فهناك الصورة البسيطة لفعل الدخول أو البقاء غير المشروع، وهناك الصورة المشددة للعقاب على فعل الدخول أو البقاء غير المشروع، وتتجلى الصورة البسيطة لجريمة الدخول إلى النظام أو البقاء فيه فيما يلي:

1 - **فعل الدخول:** وفقا للتصور المعنوي لفكرة الدخول فإنه يتحقق بأي صورة من صور التعدي، أي يستوي أن يكون التعدي مباشرا أو غير مباشر، وبما أن المشرع لم يحدد وسيلة الدخول إلى النظام، فإنه يمكن الدخول بأية وسيلة كانت، وذلك عن طريق كلمة السر الحقيقية متى كان الجاني غير مخول في استخدامها، أو باستخدام برنامج أو شفرة خاصة، أو عن طريق استخدام الرقم الكودي لشخص آخر أو الدخول من خلال شخص مسموح له بالدخول[2].

ويتحقق الدخول غير المشروع كذلك متى كان مخالفا لإرادة صاحب النظام، أو من له حق السيطرة عليه، كتلك الأنظمة المتعلقة بأسرار الدولة أو دفاعاتها أو التي تتضمن بيانات شخصية لا يجوز الإطلاع عليها[3]، كما يتحقق فعل الدخول إلى النظام، متى دخل الجاني إلى النظام كله أو جزء منه كالدخول إلى شبكة الاتصال أو البرنامج، وكذلك يتحقق الدخول غير المشروع متى كان مسموحا للجاني بدخول جزء معين في البرنامج، فيعد تجاوزه إلى جزء آخر غير مسموح له بالدخول فيه، ويخرج من نطاق الدخول غير المشروع، الدخول إلى برنامج منعزل عن نظام المعلومات الذي حظر عليه الدخول فيه، كما لا تتوافر الجريمة إن اقتصر دور الجاني على مجرد قراءة الشاشة دون الولوج إلى داخل النظام، إذ بهذه الأفعال لا تقوم جريمة الدخول غير المشروع للنظام المعلوماتي[4].

2 - **فعل البقاء:** يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على

---

[1] أحمد خليفة الملط، الجرائم المعلوماتية، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، ط2، 2006، ص190. منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص39 وما بعدها.

[2] عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الثاني، الحماية الجنائية لنظام التجارة الإلكترونية، دار الفكر الجامعي الإسكندرية، 2002، ص28 و29.

[3] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية، بيروت، 1999، ص123.

[4] عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الثاني، الحماية الجنائية لنظام التجارة الإلكترونية، المرجع السابق، ص30.

هذا النظام[1]، ويتحقق الركن المادي في جريمة البقاء في النظام كذلك إذا اتخذ صورة البقاء داخل النظام.

ومما لا شك فيه أن البقاء داخل نظام الكمبيوتر بعد دخوله عن طريق الخطأ، لا يختلف عن الدخول غير المصرح به من حيث وجوب التجريم، فاتجاه إرادة الفاعل إلى البقاء داخل هذا النظام على الرغم من معرفته أنه غير مصرح له بالدخول، لا يختلف في جوهره عن الدخول غير المصرح به إلى نظام الكمبيوتر أو الأجهزة الذكية، فالنتيجة الإجرامية في الحالتين واحدة وهي الوصول إلى نظام غير مصرح للدخول إليه، فالمصلحة التي يحميها القانون هي حماية هذا النظام في الحالتين.

وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معا وذلك في الفرض الذي لا يكون فيه الجاني له الحق في الدخول إلى النظام ويدخل إليه فعلا ضد إرادة من له حق السيطرة عليه، ثم يبقى داخل النظام بعد ذلك، ويتحقق في هذا الفرض الاجتماع المادي لجريمتي الدخول والبقاء غير المشروع في النظام[2].

في هذا الصدد يذهب رأي راجح من الفقه إلى أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي يبدأ فيها الجاني التجول داخل النظام، أو يستمر في التجول داخله بعد انتهاء الوقت المحدد، أي منذ علم الجاني أنه ليس له حق الدخول، فإذا دخل وظل ساكنا تظل الجريمة جريمة دخول إلى النظام، أما إذا بدأ في التجول فإن جريمة البقاء داخل النظام تبدأ من تلك اللحظة لأنه يتجول في نظام يعلم مسبقا أن مبدأ دخوله واستمراره فيه غير مشروع، ومنذ تلك اللحظة تبدأ جريمة البقاء داخل النظام.

وتعتبر هذه الجريمة جريمة سلوك مجرد أي أنها تبدأ وتنتهي بانتهاء السلوك المكون لها، وهو الدخول أو البقاء دون أن يتطلب المشرع في نموذجها القانوني حسب نصوص التجريم أي نتيجة إجرامية.

ثانيا: الركن المعنوي، تعتبر جريمة الدخول أو البقاء من الجرائم العمدية يكفي فيها القصد العام، فيكفي لتوافر هاته الجريمة أن يعلم الجاني أنه قد دخل إلى نظام ليس له حق الدخول فيه، أو تعمد البقاء فيه رغم انتهاء مدة حقه في البقاء فيه ولو كان الدخول مشروعا، أما إذا انتفى علمه فإنها لا تتوافر الجريمة، كأن يجهل وجود حظر الدخول، أو كان يعتقد خطأ أنه مسموح له الدخول فيه.

وتظهر الصورة المشددة لجريمة الدخول إلى النظام أو البقاء فيه من خلال استقراء نص المادة 394 مكرر ق.ع، التي نجد أنها قد نصت على ظرفين تشدد بهما عقوبة الدخول، أو البقاء داخل النظام، ويتمثل هذان الظرفان في حالة ما إذا نتج عن الدخول أو البقاء غير المشروع محو أو تعديل البيانات التي يحتويها النظام، أو عدم قدرة النظام على تأدية وظيفته، ويكفي لتوافر هذا الظرف المشدد أن تكون هناك علاقة سببية بين الدخول أو البقاء غير المشروع وبين النتيجة التي تحققت، وهي محو النظام، أو عدم قدرته على أداء وظيفته، أو تعديل البيانات، وهو ما سيتم التطرق إليه بالتفصيل لاحقا في هذه الدراسة.

البند الثاني: جريمة الاعتداء القصدي على النظام

لم يتعرض المشرع الجزائري لهذه الجريمة، بل اكتفى بالنص على جريمة الاعتداء على المعطيات فقط، ولذلك فإنه لتحقق هذه الجريمة يستلزم توافر الركن المادي والركن المعنوي.

---

[1] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص133.

[2] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص133.

أولا: الركن المادي، يتمثل الركن المادي إما في فعل توقيف أو تعطيل نظام المعالجة الآلية للمعطيات عن أداء نشاطه وإما في فعل إفساد نشاط أو وظائف هذا النظام، ولا يشترط أن يقع فعل التعطيل أو فعل الإفساد على كل عناصر النظام، بل يكفي أن يؤثر على أحد هذه العناصر فقط سواء المادية أو المعنوية[1].

1 – **التعطيل أو التوقيف**: تعتبر عملية إعاقة سير عمل نظام المعالجة الآلية للمعطيات بأنها فعل يتسبب في تباطؤ أو ارتباك عمل نظام المعالجة، ومن ثم ينتج عن ذلك تغيير في حالة عمل النظام، وهذا الارتباك الناجم عن الإعاقة تتأثر به أجهزة الكمبيوتر والبرامج على السواء[2].

2 – **الإفساد أو التعييب**: ويقصد بالإفساد أو التعييب كل فعل وإن كان لا يعطل نظام معالجة البيانات لكنه يجعل هذا النظام غير قادر على الاستعمال السليم، وذلك بأن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها.

وتتنوع وسائل التعييب أو الإفساد كاستخدام القنبلة المعلوماتية، بحيث يدخل من خلالها مجموعة من المعطيات التي تتكاثر داخل هذا النظام بحيث تجعله غير صالح للاستعمال، أو استخدام فيروس يجعل مخرجات النظام غير تلك التي كان يجب عليه أن يخرجها.

ثانيا: الركن المعنوي، جريمة الاعتداء القصدي على نظام المعالجة الآلية للمعطيات جريمة عمدية، بحيث يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصريه العلم والإرادة، على اعتبار أن تتجه إرادة الجاني إلى فعل الإفساد مع علمه بأن نشاطه الجرمي من شأنه أن يوصله إلى تلك النتيجة، فإذا قام شخص يتعامل مع النظام بصورة مشروعة بإعاقة أو إفساد النظام نتيجة لخطأ في التشغيل أو التعامل مع البيانات ينتفي القصد الجنائي لديه، ولا يسأل عن هذه الجريمة.

البند الثالث: جريمة الاعتداء القصدي على المعطيات

يتضح من خلال النص المادة 394 مكرر 1 ق.ع أنه حتى تقوم الجريمة لابد من توافر ركنيها المادي والمعنوي.

أولا: الركن المادي، ينحصر النشاط الإجرامي في هذه الجريمة في أفعال الإدخال والمحو والتعديل ويكفي توافر إحداها لقيام الجريمة، فلا يشترط اجتماعها معا حتى يتوافر النشاط الإجرامي فيها، ومن ثم يقام الركن المادي في الجريمة، لكن القاسم المشترك في هذه الأفعال جميعا هو انطوائها على التلاعب في المعطيات التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة غير صحيحة، أو محو أو تعديل آخر قائمة.

ومن هنا يمكن القول إن النشاط الإجرامي لهذه الجريمة إنما ينصب على المعطيات أي المعلومات المعالجة آليا والتي أصبحت رموزا وإشارات وليست المعلومات في ذاتها باعتبارها أحد عناصر المعرفة، كما أن محل هذا النشاط الإجرامي يقتصر على المعطيات الموجودة داخل النظام والتي تشكل جزءا منه، وبناء عليه فالجريمة لا تتحقق إذا وقع النشاط الإجرامي على المعطيات خارج النظام

---

[1] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص139.

[2] ومن أمثلة التخريب أو التعطيل الواقع على أنظمة المعالجة الآلية للمعطيات قضية موريس وهي أحد أول الهجمات الكبيرة والخطرة في بيئة الشبكات التي سبق الحديث عنها آنفا في هذه الدراسة. يونس عرب، جرائم الحاسوب، جرائم الكمبيوتر والإنترنت، المرجع السابق.

سواء قبل دخولها أم بعد خروجها، أما المعلومات غير المعالجة التي لم تدخل إلى النظام فهي خارج نطاق الحماية المشمولة بهذا النص وإن كان يجوز حمايتها وفقا لنصوص جنائية أخرى[1].

ولعل المقصود من الأفعال المكونة لهذه الجرائم:

1- **فعل الإدخال**: ويقصد بذلك إدخال بيانات في نظام المعالجة لم تكن موجودة من قبل، وقد يتم إدخال هذه البيانات بقصد التشويش على صحة البيانات القائمة.

2- **فعل المحو**: ويقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة، والموجودة داخل النظام، أو تحطيم تلك الدعامة، أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة[2].

3- **فعل التعديل**: ويقصد به تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى.

ثانيا: الركن المعنوي، تتحقق هذه الجريمة بمجرد توافر النية الجرمية بكافة عناصرها (العلم والإرادة)، وبالتالي يكفي أن يعلم الجاني أنه يقوم بأحد الأفعال السابقة الذكر (الإدخال، المحو، التعديل)، ومع إرادته في القيام بهذا الفعل تقوم الجريمة وبالتالي لا يشترط لقيامها توافر نية الإضرار بالشخص مالك البرنامج أو صاحب النظام، وإن كان الضرر قد يتحقق في الواقع نتيجة النشاط الإجرامي إلا أنه ليس عنصرا في الجريمة.

الفرع الثاني: جريمة الحيلولة بين صاحب النظام الإلكتروني ونظامه

وفي هذه الصورة المستحدثة لجرائم التكنولوجيا الحديثة يتوصل الفاعل من خلال معرفته بتقنية نظم المعلومات وباستخدام الأجهزة التقنية وقنوات الاتصال إلى منع صاحب النظام من استخدام نظامه أو الدخول إليه أو الاستفادة منه، ويظهر من هذا النموذج الجديد للجريمة احتوائه على فرضين كل منهما يشكل جريمة قائمة بحد ذاتها وهما:

أولا: منع صاحب النظام من الدخول إلى نظامه، فقد يعمد الفاعل إلى استخدام أجهزة الرصد البعدية فيحصل على شيفرات دخول أو كلمات السر الخاصة بصاحب النظام أثناء تشغيل النظام، من قبل صاحبه، أو بأية طريقة أخرى تقنية كانت أم عادية، ثم يعمل على تغيير وتبديل تلك الشيفرات وكلمات السر فلا يعود النظام يتقبل كلمات السر المعلومة لصاحبه، وقد يعمد الفاعل لتحقيق ذات الغاية بتعديل نظم التشغيل أو تقنيات التعرف على الهوية، وقد يعمد الفاعل باستخدام شبكات الاتصالات وتقنيات نظم المعلومات على إدخال برامج أو تقنيات لتحقيق ذات الهدف.

ثانيا: منع صاحب النظام من استخدام نظامه، هنا يعمد الفاعل ليس إلى منع صاحب النظام من الدخول إلى نظامه المعلوماتي بل إلى منعه من استخدامه والحصول على منفعته، فصاحب النظام قادر على الدخول إلى نظامه، إلا أنه هنا عاجز عن تحقيق المنفعة التي من أجلها وجد هذا النظام لديه، مثال ذلك من يقطع سير الاتصالات أو يغير مسارها أو يعدل في أنظمة تغذية النظام بأوامر التشغيل وأداء المهام[3]، وقد عاقبت مختلف القوانين الجزائية المقارنة على هذا السلوك.

---

[1] عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الثاني، الحماية الجنائية لنظام التجارة الإلكترونية، المرجع السابق، ص43.

[2] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، 2007، ص49.

[3] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص58.

الفرع الثالث: جريمة إساءة استخدام وسائل الاتصالات

إن تقنيات نظم الاتصالات مع ما وفرته من إمكانيات هائلة سهلت على البشرية تواصلها، وعظمت من محاور التعايش والاستفادة أكثر فأكثر من تقنيات نظم المعلومات وخدمات هذه التقنية، مع ذلك كله فقد تستخدم تلك التقنيات في غير مرادها فتكون وسيلة لإلحاق الضرر والأذى بالناس وبأموالهم وممتلكاتهم، وربما بحياتهم الخاصة أيضا، وهو ما سيتم معالجته من خلال بيان صور وأساليب استخدام وسائل تقنية نظم الاتصالات بصورة سيئة، إذ تتعدد صور الركن المادي في جريمة إساءة استخدام وسائل الاتصالات، وتتنوع بتطور نظم تقنية المعلومات بصورة مضطردة ومتسارعة، ونتناول أهم هذه الصور على النحو الآتي:

أولا: توجيه رسائل تهديد بوسيلة اتصال، إذ عالجت مختلف التشريعات جوانب جرائم التهديد وبحثت في شتى صورها.

ثانيا: توجيه رسائل إهانة أو رسائل منافية للآداب العامة، ليس من السهل ضبط فكرة الإهانة أو النظام العام أو الآداب العامة لتحقق الجريمة ذلك أن هذه الأفكار فضفاضة تختلف باختلاف الزمان والمكان، فما يعتبر من النظام العام اليوم لم يكن كذلك مثلا قبل عشرين عاما والعكس، وربما كانت فكرة الآداب العامة أكثر تعديلا وتطورا من هذا كله، أما مسألة الإهانة فإنها أكثر ارتباطا بالشخص المجني عليه من ارتباطها بالزمان والمكان، فجنس المجني عليه ومكانته الاجتماعية ونحو ذلك من ركائز يعتمد عليها لاستظهار مدى وصول الرسائل إلى حد وصفها بأنها رسائل إهانة.

ثالثا: نقل خبر مختلف بقصد إثارة الفزع، بات مفهوما أن وسيلة النقل هي إحدى وسائل الاتصال التقنية على اختلافها.

نلاحظ أنه في التشريعات المقارنة يدخل في جرائم إساءة استخدام وسائل تقنية نظم الاتصالات سلوكيات أخرى كثيرة منها استخدام شبكات تقنية الاتصالات في شراء وبيع واستيراد وتوزيع وعرض وإتاحة سائر البرامج الكافية لإيقاع جريمة تقنية معينة أو قادرة على فك رموز وكلمات مرور تقنية، وعلى العموم كل ما من شأنه تسهيل ارتكاب جريمة من جرائم التكنولوجيا الحديثة.

الفرع الرابع: إساءة استخدام المواقع الإلكترونية

هناك مواقع إلكترونية في شتى مجالات الحياة، فهناك المواقع التي تهتم بالجوانب الاجتماعية والتواصل الاجتماعي وأخرى ذات علاقة بالشؤون الإخبارية وتناقل أحوال العالم وغيرها متخصصة في الترفيه والألعاب والتسلية وجميعها تنطلق من مواقع إلكترونية متاحة للكافة، فمقابل هذا الاستغلال الإيجابي للمواقع الإلكترونية وجد الاستغلال غير المشروع بأبشع صورة تبتكر وسائله الأيدي الآثمة، وتتفنن في تحقيق أهدافه العقول الشريرة خدمة لأصحابها لتحقيق نفع مادي أو معنوي، أو حتى بعدم تحقيق أي نفع يذكر.

وقد عززت معظم التشريعات القانونية التقليدية بطبيعة الحال وتلك المتخصصة بالجريمة المرتكبة في العالم الافتراضي ما يورد نصوصا ذات علاقة بتجريم أشكال وصور السلوك غير المشروع المنصب على الاستغلال غير الصحيح للمواقع الإلكترونية، ونحن إذ نبدي اهتماما بالأمر نرصد العديد من السلوكيات التي تحتاج إلى تدخل تشريعي بالنظر إلى مدى خطورتها على الأفراد والمجتمع على حد سواء، نذكر منها في هذا المقام إنشاء موقع إلكتروني على الشبكة الإلكترونية المفتوحة واستعمال هذا الموقع للترويج للاتجار بالبشر، أو الاتجار بالأعضاء البشرية، أو التوسط أو تسهيل القيام بذلك، إنشاء موقع إلكتروني على الشبكة الإلكترونية المفتوحة واستعمال هذا الموقع في الاتجار بالأسلحة بمفهومها العام، أو لبيان وشرح وتوضيح طرق صناعتها وصناعة المتفجرات، أو طرق

استعمالها وتنفيذ هجوم بواسطتها، وعلى العموم كل ما من شأنه رفع مستويات الاستعمال الخطر للأسلحة بين الأفراد بما يوفر الموقع من معلومات وبيانات وطرقا للاستعمال والتعامل مع الأسلحة، وإنشاء موقع إلكتروني على الشبكة الإلكترونية واستعمال ذلك الموقع في الترويج للمخدرات أو المؤثرات العقلية أو المستحضرات والعقاقير الطبية ويشمل ذلك بيان آليات وطرق تصنيعها وزراعتها وإنتاجها وأساليب توزيعها، بالإضافة إلى إنشاء موقع إلكتروني واستعماله لأية غايات أخرى مخالفة للقانون أو دون الحصول على إذن أو تصريح قانوني حيث توجب التشريعات المعنية الحصول على ذلك الإذن أو التصريح.

وعلى العموم فإن الاستخدام الأمثل لتقنية نظم المعلومات والاتصالات الحديثة يقود كذلك إلى الحديث عن الاستعمال الأمثل لكل ما يتعلق بتقنية نظم المعلومات والاتصالات من أدوات ووسائل، فلا يجوز إساءة استعمالها، كما لا يجوز التجاوز على حدود الإذن لاستعمالها، أو استعمالها في غير الأغراض الموجودة من أجلها.

الفرع الخامس: جرائم الاعتداء على المواقع الإلكترونية الحكومية

تتعرض المواقع الإلكترونية الحكومية لاعتداءات إلكترونية بقصد تدميرها، تشويهها، أوشلها عن العمل، فيقوم المهاجمون بتحقيق أهدافهم عن طريق شن هجمات إلكترونية تهدف إلى إغلاق المواقع الحيوية الحكومية على الشبكات المعلوماتية أو الاستيلاء على محتوياتها أو السيطرة عليها والتحكم فيها، وتتعدد أساليب وطرق الاعتداء على المواقع، ومن أهم تلك الأساليب والطرق مايلي:

أولا: تدمير المواقع، يقصد به الدخول غير المشروع إلى نقطة ارتباط أساسية أو فرعية متصلة بشبكة إلكترونية من خلال نظام آلي أو مجموعة نظم مترابطة شبكية بهدف تخريب نقطة الاتصال أو النظام، ومن الوسائل المستخدمة لتدمير المواقع ضخ مئات الآلاف من الرسائل الإلكترونية إلى الموقع المستهدف للتأثير على السعة التخزينية للموقع، فتشكل هذه الكمية الهائلة من الرسائل الإلكترونية ضغطا يؤدي في النهاية إلى تفجير الموقع العامل على الشبكة وتشتيت البيانات والمعلومات المخزنة في الموقع[1]، ولعل من أخطر وسائل تدمير المواقع وأشدها ضررا استخدام ما يعرف بالفيروس الذي سبق وأن عرضنا له بشيء من التفصيل عند دراسة وسائل وتقنيات ارتكاب جرائم التكنولوجيا الحديثة.

ثانيا: تشويه المواقع، تقتصر الأضرار التي تتسبب بها عمليات تشويه المواقع الإلكترونية الحكومية على الإضرار بسمعة الجهة الحكومية المالكة للموقع، إذ يتم تغيير الصفحة الرئيسية فقط من الموقع بصفحة أخرى من تصميم المخترق، وتتضمن هذه الصفحة الجديدة أحيانا رسالة ترغب الجهة التي قامت بعملية التشويه إيصالها، وعادة ما تتضمن هذه الرسالة اعتراضا على الحالة السياسية ونظام الحكم القائم.

ويتبع المخترقون عدة أساليب في عمليات تشويه المواقع الإلكترونية، تختلف من موقع إلى آخر، بناء على نوع نظام التشغيل ومزود الوب الذي يعتمد عليه الموقع، منها الحصول على ملف الشفرة الخاصة بأحد المشرفين على الشبكة أو من يملكون حق تعديل محتويات الموقع، حيث يتم فك تشفيرها وإرسالها في مختلف المزودات أو عبر استغلال الثغرات الأمنية في مزودات الوب، وأنظمة التشغيل، حيث لا يخلو أي نظام تشغيل أو مزود ويب من ثغرات أمنية تعرضه لخطر الاختراق، ويعمل المطورون بشكل مستمر على

[1] عبد الرحمن بن عبد الله السند، وسائل الإرهاب الإلكتروني حكمها في الإسلام وطرق مكافحتها، السجل العلمي لمؤتمر موقف الإسلام من الإرهاب جامعة الإمام محمد بن سعود الإسلامية، الرياض، 2004، ص16 و17.

سد هذه الثغرات كلما اكتشفت إلى أن يجد القيمون على تصميم النظام الحل المناسب لها، وغالبا ما تبقى أغلب الثغرات التي يكتشفها المخترقون متاحة لفترة طويلة حتى يتم اكتشافها، حيث أنهم لا يعلنون عنها بسرعة ليتمكنوا من استغلالها فترة أطول.

ثالثا: حجب الخدمة، يقصد به جعل الوصول إلى الموقع الإلكتروني غير ممكن، أي قفل الموقع وتعطله عن العمل[1]، وتتم هذه العملية عن طريق توجيه جهة ما لحزم بيانات شبكية بصورة كثيفة جدا إلى مزودات المواقع بهدف إيقافها عن العمل، وتوجد عشرات الطرق التي يمكن إتباعها لدفع الحزم أو الطلبات الشبكية إلى مزودات معينة لإيقافها عن العمل سواء كانت مزودات ويب أو مزودات بريد إلكتروني أو أي مزود يمكنه أن يستقبل الحزم الشبكية[2].

المطلب الخامس: جرائم التجسس وإنشاء المواقع الإرهابية

مع ارتباط الغالبية العظمى من الدول بشبكة المعلومات العالمية وازدياد اعتمادها على نظم المعلومات الإلكترونية، اتخذت الجرائم المرتكبة عن طريق تقنية المعلومات الحديثة أبعادا جديدة وازدادت الخطورة على أمن الدول، من خلال استخدام الأنظمة الإلكترونية والشبكات المعلوماتية لغرض الإخلال بالنظام العام وتعريض سلامة المجتمع وأمنه للخطر، فظهرت أفعال الاعتداء على نظم المعلومات الإلكترونية الحكومية بغية تعطيل أنشطتها واستهداف مصالحها والمنشآت التي ترتبط بها في كافة القطاعات المختلفة.

ولم يقف خطر الاستخدام الإجرامي لتقنية المعلومات الحديثة على أمن الحكومات والدول عند حد الاعتداءات، بل نمت وازدهرت في العصر الرقمي أفعال التجسس والتهديد والترويع وإثارة الفتنة ونشر الأفكار الإرهابية وتبادل معلومات التطرف والإرهاب عبر وسائل تقنية المعلومات الحديثة، واتخذت أبعادا جديدة وآفاقا أرحب مع تطور وسائل الاتصال والتواصل[3]، فبات التقاء الإرهابيين والمجرمين لتعلم طرق الإجرام والإرهاب[4]، وتبادل الآراء والأفكار والمعلومات سهلا عن طريق الشبكات الإلكترونية[5].

الفرع الأول: جريمة التجسس المتصلة بالتكنولوجيا الحديثة

إذا ما توافرت هذه التقنية بيد الجناة المنحرفين كنا أمام خطورة جرمية تظهر في قوالب جديدة منها جرائم التكنولوجيا الحديثة المتعلقة بأمن المعلومات، وعليه سنحاول البحث في أشد هذه الجرائم التقنية خطورة على أمن المعلومات وأمن الأفراد ألا وهي جريمة التجسس الإلكتروني.

---

[1] Susan W. Brenner, Op.Cit., p68.

[2] خلاصة ورشة عمل أجرتها منظمة CERT للتعامل مع هجمات حجب الخدمة، منشورة على الموقع الإلكتروني:
www.cert.org/erports/dsit-workshop.pdf

[3] حسين بن سعيد بن سيف الغافري، الجاسوسية الرقمية، مقال منشور على الموقع الإلكتروني: www.omanlegal.net

[4] عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، المؤتمر الدولي الأول حول حماية أمن المعلومات والخصوصية في قانون الإنترنت، القاهرة، 02-04 يونيو 2008، ص15.
Philipp Brunst, Cyberterrorism: The Use of the Internet for Terrorist Purposes, Council of Europe Publishing, 2007, p09. Francois Debrix, Tabloid Terror: War, Culture, and Geopolitics Routledge, 2007, p22.

[5] عبد الرحمن بن عبد الله السند، المرجع السابق، ص07. علي عدنان الفيل، الإجرام الإلكتروني، دراسة مقارنة، منشورات زين الحقوقية، لبنان، ط1 2011، ص80.

يعرف سلوك التجسس بأنه فعل إيجابي قوامه الكشف واستظهار الحقائق المخفية، ولكنه كشف واستظهار غير مشروع إن كان بوسائله أو بغايته أو بأحدهما، وهو لذلك فعل يقره المشرع ويفرد لمرتكبه العقوبة الجزائية الرادعة دون تهاون، انسجاما مع روح التشريع، وإدراكا لعظم خطورة هذا السلوك، ويتمثل محل هذا السلوك، في المعلومات التقنية المعالجة آليا بأحد طرق ووسائل المعالجة المعلوماتية، أيا كان نوعها شريطة أن تتسم بطابع السرية، هذا الطابع الذي يحيلها من مجرد معلومات تقنية عادية متاحة للكافة إلى معلومات يحرص صاحبها سواء كان فردا عاديا أم كيانا معنويا على عدم إطلاع الغير عليها، أو إبقائها في إطار ضيق من الإطلاع.

وللإحاطة بكافة عناصر وصور السلوك في الواقع العملي فإننا سنتحدث عن محورين أساسين هما أسرار ووثائق الدولة الأسرار والوثائق الخاصة، إذ اهتمت الدولة ومنذ الأزل بجانب مهم وحساس من وثائقها الرسمية، خصوصا تلك المعلومات المتعلقة بكيانها ونشاطاتها ومخططاتها وإمكانياتها، بالإضافة إلى كل ما يتعلق بقوتها وتعداد جيشها وتسليحهم ونحو ذلك، وجعلت هذه المعلومات والوثائق بحرز آمن ضد تلاعب الأشخاص، وقد تزايدت الحاجة لضمان الحماية الفعالة لتلك الأسرار مع تسارع نمو قطاع الإلكترونيات والاتصالات وتقنية نظم المعلومات، واعتماد الدولة أكثر فأكثر على تقنية نظم المعلومات في معالجة أسرارها ووثائقها لا بل أصبحت هذه التقنية هي أداة معالجة المعلومات والبيانات الوطنية على العموم حفظا، تخزينا، معالجة وتعاملا، والتي من ضمنها تلك المعلومات والبيانات والأسرار الحساسة والمهمة وذات الأبعاد الأمنية.

إلى جانب مساهمة هذه التقنية الجديدة في تطور وسائل معالجة المعلومات والبيانات العادية منها والسرية ساهمت أيضا في تنوع وسائل الاعتداء على تلك السرية إلى جانب الأفراد والمؤسسات الخاصة، فلا يمكن القول إن السر أو الوثيقة حصر على الدولة بل إن هذا المفهوم وكما سيأتي لاحقا يتعلق بطبيعة المعلومة والوثيقة لا بصاحبها، وهو أمر يقف فيه الفرد والدولة على قدم المساواة في ظل نطاق التجريم والعقوبة، وقد تقع الجريمة في كل تلك الفروض باستخدام تقنية المعلومات، فتقع الجريمة المبحوث عنها حصرا هنا، وهم –الجناة– إذ يفعلون ذلك إنما يرتكبون الجريمة بوسائل إلكترونية، فكانت الجريمة إذن وعلى هذا الوصف الجديد المستحدث جريمة تجسس إلكتروني[1].

وعليه فلم يعد مصطلح التجسس قاصرا على أسرار ووثائق الدولة التقليدي ونقصد بذلك تلك الوثائق والمعلومات والأوراق المحفوظة على دعائم مادية، بل امتد ليشمل في نطاقه كل وثيقة أو سر محفوظ بطرق تقنية يحرص صاحبه على إبقائه كذلك، إضافة إلى شمول الجريمة بالوصف الجديد وهو التجسس الإلكتروني كلما ارتكبت الجريمة بوسائل وأدوات تقنية نظم المعلومات.

البند الأول: مفهوم السر في جريمة التجسس

نتناول في هذا الموضوع حماية الأسرار والوثائق سواء تلك المتعلقة بالدولة وأمنها أو تلك المتعلقة بالمؤسسات والقطاعات الخاصة، فمن المعلوم أن جريمة التجسس تعتبر إحدى الجرائم التي تطال أمن الدولة، وفي ظل هذا يفهم السر باعتباره المحور الأول في

[1] لوحظ أن ازدياد حجم الربط بالإنترنت وضعف أنظمة الحماية المعلوماتية تعتبر ظروفا تزيد من مخاطر التجسس الإلكتروني، وقد سجلت العديد من أعمال التجسس التي لم تسلم منها الدول رغم أنظمة الحماية العديدة.

هذه الجريمة، فهو بالضرورة معلومة أو وثيقة لها علاقة بالدولة تحرص على بقائها سرا[1]، في حين ينصرف المحور الثاني من ذات المفهوم إلى السر كمفهوم مرتبط بنشاطات القطاع الخاص وعلاقته بالمجتمع والأفراد فيه والعلاقات الخاصة الناشئة عن ذلك كله.

أولا: أسرار ووثائق الدولة، لتحقيق هذه الحماية ابتداء لا بد من أمرين أساسين يتعلق الأول بوجود أسرار أو وثائق تخص إحدى مؤسسات الدولة أو إحدى هيئاتها، وأن تكون هذه الأسرار ذات علاقة بأمن الدولة[2]، وأن تكون هذه المعلومات على درجة من السرية ومن شأن إفشائها إلحاق ضرر بأمن الدولة الداخلي أو الخارجي دون بيان لحجم أو طبيعة هذا الضرر.

ففي ظل هذين الأمرين يفهم السر محور الحماية ونطاق الجريمة، لكن السر بهذا المفهوم لا يتمتع بدرجة واحدة من الحماية فقد صنف قانون حماية أسرار ووثائق الدولة الأسرار، وأفرد حماية معينة لكل صنف منها، فجعلها ثلاثة أصناف وجعل لها ثلاث مستويات للحماية وهي:

1-الأسرار والوثائق المصنفة بدرجة "سري": ومنها خطط وتفصيلات العمليات الحربية، والمعلومات والوثائق ذات العلاقة بالأمن الداخلي...إلخ[3].

2-الأسرار والوثائق المحمية بدرجة "سري للغاية": ومنها الوثائق والمعلومات المتعلقة بإحدى مؤسسات الدولة أو هيئاتها العامة والتي يؤدي إفشاؤها إلى إلحاق الضرر بالدولة، أو إلى تحقيق منفعة دولة أخرى[4].

3-الأسرار والوثائق المصنفة بدرجة محدودة: وهي الوثائق والمعلومات التي يؤدي إفشاؤها إلى إيقاع الدولة بحرج دولي، أو يمكن أن يؤدي ذلك إلى صعوبات اقتصادية أو مالية.

ثانيا: أسرار ووثائق القطاع الخاص، أصبح اعتماد القطاع الخاص على تقنيات نظم المعلومات أمرا لا مفر منه، بل على الأرجح أصبح أمرا لازما، فلم تعد قطاعات الصناعة والتجارة والتسويق والخدمات والمهن قادرة على العمل بعيدا عن نظم المعلومات تلك النظم التي أصبحت تحوي كافة المعلومات والبيانات المتعلقة بالعمل، والتي كانت سابقا حبيسة الأدراج والملفات، بل أبعد من ذلك، فقد دخلت نظم المعلومات وشبكات الاتصال والمعلومات المحلية والعالمية المجال، فأصبحت المعلومات والبيانات عرضة أكثر فأكثر للاختراق والإطلاع والإنشاء، على أنه ولأهمية البحث في حماية أسرار ووثائق الدولة فإننا سنخصص المساحة الأكبر تاليا لذلك، على أنه تم البحث في حماية الأسرار والوثائق الخاصة سواء تعلقت بالقطاع الخاص أو ما تعلق منها بالحياة الخاصة للأفراد عند تناولنا جرائم الاعتداء على الحياة الخاصة للأفراد ضمن هذه الدراسة.

البند الثاني: الركن المادي للجريمة

يمكن تصور السلوك المادي لهذه الجريمة بإحدى الصورتين، أما الصورة الأولى فتتمثل في الحصول مباشرة على الدعامة

---

[1] مغبغب نعيم، حماية برامج الكمبيوتر، الأساليب والثغرات، منشورات الحلبي الحقوقية، بيروت، 2006، ص229.

[2] أسامة أحمد المناعسة، الوسيط في شرح قانون محكمة أمن الدولة، دار وائل للنشر، عمان، ط1، 2006، ص225 و226.

[3] أسامة أحمد المناعسة، الوسيط في شرح قانون محكمة أمن الدولة، المرجع نفسه، ص229.

[4] أسامة أحمد المناعسة، الوسيط في شرح قانون محكمة أمن الدولة، المرجع نفسه، ص229. وقد اعتبر برنامج ECHELON أكبر منظومة للتجسس الإلكتروني، وهو برنامج قادر على اختراق نظم المعلومات والتجسس على الاتصالات الخلوية والبريد الإلكتروني.

الإلكترونية (كسواقة فلاش مثلا) المخزنة للأسرار أو المعلومات والوثائق المعلوماتية، وتتمثل الصورة الثانية في الدخول بصورة إلكترونية إلى أنظمة تخزينها باستخدام تقنيات نظم المعلومات والاتصالات لتحقيق الولوج المباشر أو عن بعد للنظام أو للجهاز الحاوي لمكمن السر الإلكتروني، وذلك تمهيدا لارتكاب الجريمة التي سنرى صورها فيما يأتي.

وقد عالج قانون العقوبات الجزائري مختلف صور الجريمة ولكن بشكلها التقليدي المنصب على فعل مادي ملموس يعتمد على ماديات محسوسة محتوية للأسرار والوثائق والمعلومات بصورة تقليدية، وهو أمر يخرج عن نطاق التجسس الإلكتروني، ودورنا هنا أن نبحث في الركن المادي لجريمة مستحدثة جاءت انعكاسا لتطورات النظم المعلوماتية وتطور الفكر الإجرامي معها، ومحاولة لبيان مقدرة النصوص التقليدية على ضبط هذه السلوكيات الجديدة وتحقيق الفاعلية العقابية.

ويتخذ السلوك الجرمي المكون للركن المادي في الجريمة محل دراستنا المحور الفني التقني المباشر، وهو القائم على الدخول غير المشروع لأنظمة المعالجة الآلية للمعلومات والبيانات الإلكترونية والحصول على تلك البيانات والمعلومات والوثائق السرية، أو المحور الفني التقني غير المباشر، وهو القائم على التقاط النبضات الكهرومغناطيسية الحاملة للمعلومات والبيانات المعالجة إلكترونية وذلك بواسطة أجهزة خاصة تستخدم لتلك الغاية.

البند الثالث: الركن المعنوي لجريمة التجسس المتصلة بالتكنولوجيا الحديثة

كان الاشتراط ليتحقق التجريم ضرورة وجود القصد الخاص لدى الفاعل، فلا يكفي القصد العام، أما القصد الخاص هنا فيتمثل بقصد الفاعل إيقاع ضرر بالدولة والإساءة لها[1]، أو قصد الإضرار بالأفراد أو بالكيانات المعنوية الخاصة، ولذلك ينظر إلى انصراف نية الفاعل إلى إلحاق الضرر بالدولة وأجهزتها وشخصياتها، وإلى إلحاق الضرر بالأفراد والكيانات المعنوية الخاصة، ومن هنا كان لا بد من جعل الضرر ومقداره سببا في تشديد العقاب، هذا وفقا للقواعد العامة للتجريم، وهو أمر صحيح، فلا بد وفقا لذلك من أن يكون إتيان الفعل من الفاعل بقصد، فإن وقع الفعل بإهمال أو نحو ذلك من صور السلوكيات غير المقصودة لم تكتمل أركان وعناصر التجريم ولم يكن عندها الفعل مجرما.

الفرع الثاني: جريمة الإرهاب المتصلة بالتكنولوجيا الحديثة

مع انتشار تقنية نظم الاتصالات المعلوماتية، وانتشار وسائلها وشيوع شبكة الإنترنت، وإمكان استخدامها من الكافة في كل زمان وأي مكان، ومع تطور أنظمة الوسائل الإلكترونية، فقد تطور الإجرام الإرهابي، سواء من حيث طبيعة السلو، فأخذ منحى معنويا اعتمد على التقنية أكثر منه على الفعل المادي، أو من حيث الأهداف فإن كانت سابقا مادية بحتة، فقد أضيف إليها حديثا أهدافا معنوية، ازدادت وتنوعت مع ازدياد وتنوع الاستخدامات التقنية لنظم المعلومات، أدى ذلك إلى ظهور مصطلح جديد هو مصطلح الإرهاب الإلكتروني يستفيد الفاعل والمساهمون معه من تقنيات عالية النفاذ لتحقيق ذات أهدافهم، أما خطورة الإرهاب الإلكتروني فتتعاظم عند تصورنا لأحد أمرين أو كليهما معا وهما؛ مدى اتساع اعتماد المجتمعات على تقنية أنظمة المعلومات، سواء

[1] مغبغب نعيم، المرجع السابق، ص235.

في نطاق الدولة الواحدة أو نطاق إقليمي أو عالمي، وكذا ضآلة إن لم يكن انعدام البيئة التشريعية اللازمة لمكافحة الجريمة المستحدثة بشكل عام، والتي منها على وجه التخصيص جرائم الإرهاب المتصلة بالتكنولوجيا الحديثة.

البند الأول: تعريف الإرهاب في جرائم التكنولوجيا الحديثة

الإرهاب في جرائم التكنولوجيا الحديثة كمفهوم مستحدث لا يزال يكتنفه بعض الغموض، ذلك أنه يعتمد على تقنية أنظمة المعلومات من حيث وسيلة ارتكابه، ومن حيث دور الفاعل فيه وطبيعة سلوكه، وهو أيضا ووفقا لذلك يوقع نتائج تطال أمن المعلومات وتقنية أنظمة المعلومات بالإضافة إلى ما يتسبب به من أضرار واسعة الانتشار، عظيمة الأثر على المجتمع وأفراده.

أما المحور الرئيسي في جريمة الإرهاب الإلكتروني فهو كما نعتقد يكمن في مدي تسبب الفعل بإيقاع الرعب لدى الناس من عدمه، فحتى تكتمل الجريمة هنا لا بد أن يؤدي الفعل إلى إيقاع الرعب لدى الناس بل ويكفي أن يكون ذلك محل احتمال مهما كان الاحتمال ضئيلا، إذ أن تحقق الرعب مرتبط بتحقق الفعل إلى درجة ما، وهو أمر أكده المفهوم المتعارف عليه للإرهاب في جرائم التكنولوجيا الحديثة إذا لم يرتبط الإرهاب بإيقاع الفعل بل التقت مجالاته، بحيث أمكن القول بقيام جريمة إرهاب إلكتروني حتى في حالات بقاء الفعل المقصود في طور التهديد بإيقاعه، وهو أمر متصور الوقوع كثيرا في نطاق الإرهاب الإلكتروني، إذ غالبا ما يقتصر الفعل عمليا على التهديد بالقيام بأعمال عنف موجهة ضد المجتمع دون القيام بها فعلا.

البند الثاني: الركن المادي في جرائم الإرهاب المتصلة بالتكنولوجيا الحديثة

يتوفر الركن المادي في جرائم الإرهاب الإلكتروني، بتحقق إمكانية إيقاع الفعل باستخدام تقنية أنظمة المعلومات، وفي كل حالة يرتبط فيها النشاط موضوع الفعل بنطاق إلكتروني يعتمد عليه شريطة تحقق استخدام قدر كاف من العنف التهديدي، والحقيقة أن استخدام العنف كمفهوم تقليدي في ظل سلوك إلكتروني معنوي يأتيه الفاعل يبقى خارج نطاق البحث وإن أمكن تصور مفهوم مستحدث للعنف المقصود بالنص، بالإضافة إلى أن يكون من شأن استخدام هذا العنف أو التهديد به إيقاع الرعب بين الناس أو تعريض حياتهم للخطر، على أن يتبع تنفيذا لعمل فردي أو جماعي.

وفي ظل هذه المحددات يمكن تصور الإرهاب إلى حيز الوجود كجرائم مستحدثة مستوجبة العقاب ومن ذلك:

1- استخدام أو التهديد باستخدام العنف بهدف تعريض أمن المجتمع للخطر، أو الإخلال بالنظام العام فيه، ولا يشترط هنا تحقيق الضرر أو الإخلال، بل يكفي احتمال وقوعه.

2- استخدام العنف أو التهديد بهدف تعطيل أحكام الدستور والقوانين أو بهدف الإضرار بالموارد الوطنية وتعريضها للخطر، من خلال استخدام تقنية أنظمة المعلومات[1].

3- استخدام العنف أو التهديد باستخدامه بهدف تعطيل الاتصالات أو أنظمة الوسائل الإلكترونية كاختراق شبكات تقنية أنظمة المعلومات أو التشويش عليها، وهي في النص التقليدي ظرفا مشددا، ونحن هنا نراها جريمة إرهاب متصلة

[1] أسامة أحمد المناعسة، الوسيط في شرح قانون محكمة أمن الدولة، المرجع السابق، ص86.

بالتكنولوجيا الحديثة قائمة بحد ذاتها لا بد أن ترتبط بالعنف أو التهديد باستخدامه، لا أن تكون أثرا فقط وظرفا لتشديد العقوبة.

ويبقى أن نشير إلى أن أي عمل إلكتروني أو التهديد به قادرا على تعريض أمن المجتمع وسلامته للخطر، أو قادرا على الإخلال بالنظام العام سواء كان عملا فرديا أو جماعيا، يمكن أن يقع ضمن نطاق التجريم.

البند الثالث: الركن المعنوي في جرائم الإرهاب المتصلة بالتكنولوجيا الحديثة

إذا كانت الجريمة المقصودة بشكل عام تقوم على الركن المعنوي القائم على عنصري العلم والإرادة، فإن الإرهاب الإلكتروني لا يكفي فيه القصد العام، إذ لا يكفي علم الفاعل بالسلوك الجرمي الذي يرتكبه، وإرادة ارتكاب هذا السلوك لقيام الجريمة، بل لا بد من ثبوت القصد الخاص، الذي يتمثل في الغرض الإرهابي، فلا بد من أن يتوافر في نية الفاعل وهو يقدم على استخدام تقنية نظم المعلومات، أن يوقع أو يهدد بإيقاع أحد الأغراض المعلنة في نص التجريم التقليدي أو المستحدث، لما سيقدم عليه من فعل إلكتروني، فإن لم يتوافر ذلك لم تقم الجريمة.

المبحث الثاني: جرائم التكنولوجيا الحديثة ذات الصبغة المالية

أسهمت ثورة تقنية نظم المعلومات وتطور التكنولوجيا الحديثة وبلا شك في إجبار فقهاء القانون على تعديل نظرية الجريمة بشكل عام وعلى الأخص لجهة السلوك وطبيعته، ولم تكن جرائم الأموال التقليدية بمنأى عن ذلك، فقد مكنت تقنية نظم المعلومات وبما وفرته بيد الجناة من وسائل إلكترونية من إيجاد قوالب تجريمية مستحدثة جديدة تظهر بشكل واضح لجهة السلوك، الأمر الذي حتم تطور نظرية الجريمة وبما يتوافق مع ذلك.

المطلب الأول: السرقة والتزوير في جرائم التكنولوجيا الحديثة

أثرت تكنولوجيا المعلومات الحديثة التي اجتاحت ميادين الحياة كافة في أساليب ارتكاب الجرائم، فلم تعد ترتكب بذات الأشكال التقليدية المعروفة، ففي جريمة السرقة مثلا لم يعد مطلوبا من السارق أن يحمل السلاح أو يقتحم المنازل في سبيل تحقيق هدفه، بل يكفيه بضع ضغطات على لوحة المفاتيح لكي يقوم بتحويل مبالغ طائلة إلى حسابه الشخصي وهو جالس في منزله كما هو الحال بالنسبة لجريمة التزوير.

يتطلب تحديد ماهية السرقة والتزوير في جرائم التكنولوجيا الحديثة بيان مفهومها، فالاعتداء فيها منصب على الكيان المنطقي كالمعلومات والبرامج، والتي تغدو من القيم الاقتصادية المتداولة في العالم بعد أن توسع مفهومها في ظل الثورة المعلوماتية وبذلك فقد توسع مفهوم هذا النوع من الجرائم ليشمل ما أفرزته التطورات التكنولوجية من قيم جديدة، واستنادا على ما تقدم سنحاول التعرض لكل من جرائم السرقة والتزوير المتصلة بالتكنولوجيا الحديثة من خلال تعريفها وبيان أركانها.

الفرع الأول: السرقة في جرائم التكنولوجيا الحديثة

يمكننا دراسة هذه الجريمة من خلال التعريف بها وبيان أركانها.

البند الأول: تعريف جريمة السرقة المتصلة بالتكنولوجيا الحديثة

سبق وأوضحنا أن المعلومات غدت قيمة مالية قابلة للتملك والاستغلال، وتجب معاملتها معاملة المال، نظرا إلى ما لها من قيمة اقتصادية كبيرة، فتتهافت المؤسسات المختلفة والأفراد والدول للحصول عليها لتسريع عملية التقدم في كافة المجالات، وفي مقابل هؤلاء توجد طائفة أخرى تسعى إلى الاستغلال غير المشروع لهذه المعلومات وبشتى الوسائل ومنها السرقة، وهي إحدى أكثر هذه الوسائل انتشارا في مجال الاعتداء على المعلومات، ويطلق عليها البعض بجريمة قرصنة المعلومات[1]، والتي تعرف بأنها نسخ البرامج بصورة غير شرعية أو الحصول على معلومات مخزنة في ذاكرة الحاسب أو الأجهزة الذكية دون وجه حق[2].

والسرقة هنا تتميز عن السرقة التقليدية في أنها ترد على محل معنوي متمثل بالمعلومات والبرامج وعناصر أخرى، يصعب في كثير من الأحيان تصنيفها وتحديدها إذا كانت من العناصر المادية للمعلوماتية أم أنها من عناصرها المعنوية، ومن ثم فإن سرقة المعلومات غالبا ما تكون من خلال سرقة الوسيط الذي يتضمنها، لكن الوصول إلى المعلومات والإطلاع عليها قد لا يتحقق بسرقة الوسيط المادي الذي يحتويها دائما، فقد يتم بمجرد قراءتها من على شاشة الحاسب الآلي أو الأجهزة الإلكترونية الذكية أو نسخها على قرص ممغنط[3]. من هنا نتجرأ ونعرف جريمة السرقة في جرائم التكنولوجيا الحديثة بأنها الاستيلاء على المعلومات المعالجة آليا عن طريق الالتقاط الذهني باستخدام حاستي السمع والبصر أو الالتقاط الإلكتروني باستخدام وسائل تكنولوجية، أو فسخ أو نقل هذه المعلومات.

البند الثاني: أركان جريمة السرقة المتصلة التكنولوجيا الحديثة

مما هو معلوم أن أركان جريمة السرقة التقليدية تتمثل أساسا في الركن المادي وركن المحل والركن المعنوي[4]، وهنا سنتناول مدى إمكانية تحقيق هذه الأركان بالنسبة إلى جريمة السرقة المتصلة بالتكنولوجيا الحديثة، واضعين في الاعتبار الطبيعة الخاصة لها.

أولا: الركن المادي، (الاختلاس في جريمة السرقة المتصلة بالتكنولوجيا الحديثة)

إن فعل الاختلاس المكون للركن المادي للسرقة هنا يتكون من عنصرين هما، العنصر الموضوعي (المادي) الذي يتمثل في الاستيلاء والحيازة على نحو يؤدي لإخراج الشيء من حيازة المجني عليه وإدخاله في حيازة أخرى، والعنصر المعنوي المتمثل في عدم

---

[1] نهلا عبد القادر المومني، المرجع السابق، ص99.

[2] هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، المرجع السابق، ص106.

[3] نائلة عادل محمد فريد قورة، المرجع السابق، ص118.

[4] علي عبد القادر القهوجي، قانون العقوبات، القسم الخاص، جرائم الاعتداء على المصلحة العامة وعلى الإنسان والمال، منشورات الحلبي الحقوقية بيروت ط1، 2002، ص684.

رضا المالك أو الحائز، وفق هذا المفهوم التقليدي لفعل الاختلاس؛ عرف البعض[1] الاختلاس في البيئة الرقمية بأنه الاستيلاء على المعلومات والبيانات دون علم وإرادة صاحبها الشرعي.

1- العنصر المادي: إن الطبيعة المعنوية لوسائل التكنولوجيا الحديثة أثارت خلافات في الفقه حول مدى إمكانية ورود فعل الاختلاس على المعلومات المعالجة آليا فانقسم إلى اتجاهين، الأول يرى عدم إمكان ورود الاختلاس على تقنيات المعلومات الحديثة، والثاني يذهب إلى إمكانية وروده عليها.

2- العنصر المعنوي: (عدم رضا المالك)، يعد عدم رضا المالك عن فعل اختلاس الجاني في جريمة السرقة المتصلة بالتكنولوجيا الحديثة عنصرا مفترضا[2].

ثانيا: ركن محل الاختلاس المعلوماتي، يجب أن يكون محل الاختلاس وفق المفهوم التقليدي لجريمة السرقة مالا منقولا وأن يكون مملوكا لغير الجاني، تبعا إلى ذلك فإن محل السرقة في جرائم التكنولوجيا الحديثة هو مال معلوماتي مملوك لغير الجاني[3] والمعروف أن جريمة السرقة المتصلة بالتكنولوجيا الحديثة إنما تنصب على المعلومات المعالجة آليا.

ثالثا: الركن المعنوي للسرقة في جرائم التكنولوجيا الحديثة، يتطلب الركن المعنوي لجريمة السرقة في ضوء القواعد العامة[4] قصدا عاما ويتمثل في انصراف إرادة الجاني إلى اختلاس مال منقول مع علمه بأنه مملوك لغيره، وهو ما يتجسد في عنصري العلم والإرادة، وإن كان البعض[5] يرى أنه لا يكتفي بالقصد العام لقيام جريمة السرقة هنا، بل لابد من توافر القصد الخاص، ألا هو نية تملك المال المختلس من قبل الجاني والظهور عليه بمظهر المالك، أما بالنسبة إلى الركن المعنوي في جريمة السرقة المتصلة بالتكنولوجيا الحديثة فيبدو أن القصد العام لهذه الجريمة يتحقق باتجاه إرادة الجاني إلى الاستيلاء على المعلومات المعالجة آليا، مع علمه بأنها ليست ملكا له وأنه يرتكب فعل الاستيلاء دون إرادة صاحبها أي بمعنى أن القصد العام متحقق في جريمة السرقة، وبتعبير آخر، يجب أن تقوم لدى الجاني الرغبة في الاستيلاء على المال ومباشرة السلطات التي يحق للمالك أن يباشرها على ماله، إلا أنه من الصعب القول بتحقق القصد الخاص في جريمة السرقة المتصلة بالتكنولوجيا الحديثة، ذلك لأن الجاني قد يطلع على المعلومات من خلال قراءتها على شاشة الوسائل الإلكترونية الحديثة أو سماعها من خلال مكبرات الصوت أو عن طريق وحدات طرفية أو غيرها، فالجاني هنا لم يقصد حرمان المالك منها بصفة دائمة أو مؤقتة، بل شاركه بالانتفاع بها حين اطلع عليها[6].

وعليه نؤيد اتجاه الفقه الذي ذهب إلى صعوبة تحقق القصد الجنائي الخاص في جريمة السرقة المتصلة بالتكنولوجيا الحديثة كون المعلومات ذات كيان معنوي وقابلة للتعدد، أي تتحول المعلومة الواحدة إلى عدد غير منتهي من نفس المعلومة عن طريق

---

[1] أيمن عبد الله فكري، المرجع السابق، ص402.

[2] أحمد خليفة الملط، المرجع السابق، ص262.

[3] هلالي عبد الله أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001، دار النهضة العربية القاهرة، ط1، 2003، ص151.

[4] حميد السعدي، شرح قانون العقوبات الجديد، جرائم الاعتداء على الأموال، الجزء الثاني، مطبعة المعارف، بغداد، ط2، 1976، ص163 وما بعدها.

[5] حميد السعدي، المرجع نفسه، ص163 وما بعدها.

[6] سليم عبد الله الجبوري، المرجع السابق، ص350. صباح رمضان ياسين صالح، السياسة الجنائية في مواجهة الجرائم المعلوماتية، دراسة تحليلية، أطروحة دكتوراه، سكول القانون والإدارة، جامعة كوية، إقليم كردستان، العراق، 2013، ص58.

النسخ، ومن ثم لا يمكن القول بتحقق اختلاس المعلومة مع بقاء أصلها في حيازة المالك أي دون تحول الحيازة من المالك إلى الجاني.

من خلال ما سبق، تجدر الإشارة إلى أن العقبة الأساسية أمام تطبيق نصوص قوانين العقوبات التقليدية على جريمة السرقة المتصلة بالتكنولوجيا الحديثة تتمثل أساسا في أن هذه النصوص قد صيغت في وقت كان يعتد فيه بالأشياء المادية، وصيغت لحمايتها من صور الاعتداء المألوفة وقتها، الأمر الذي تصعب معه مواجهة أفعال التعدي التي تقع في الوقت الحالي على عناصر ومكونات الوسائل الإلكترونية.

وعلى هذا الأساس سار المشرع الجزائري على نهج المشرع الفرنسي[1] في مواجهة الجرائم المتصلة بالتكنولوجيا الحديثة من خلال إدخال تعديل على قانون العقوبات الجزائري، حيث فرض حماية جنائية خاصة على أنظمة المعالجة الآلية للمعلومات أو البيانات في المواد من 394 مكرر إلى 394 مكرر 8، لكنه مع ذلك لم يبسط هذه الحماية الجنائية على المعلومات من السرقة.

من جهة أخرى تتعدد صور السرقة في جرائم التكنولوجيا الحديثة وتتطور مع تطور تقنياتها ووسائل ارتكابها، فيصعب ضبطها، إلا إننا نستطيع رصد صورة نموذجية شائعة تصلح تطبيقا عمليا للسرقة التقنية وهي جريمة تحويل الأرصدة البنكية، هذا الواقع الجديد لم يكن بعيدا عن المخاطر، فسرعان ما طالت يد الإجرام هذه البيئة، فظهر للوجود هذا النموذج المستحدث من السرقة التقنية، ليشكل اعتداء على نظام البنك المالي، وخرقا لآليات عمل البنوك الإلكترونية، فيقوم الفاعل هنا بتحويل مبالغ مالية إلكترونية من حسابات إلى أخرى، ويفتح حسابات وهمية للحصول على منافع مالية طائلة، ويستولي على أموال الآخرين بصورة غير مشروعة، ومن الممكن أن يحدث السلوك الجرمي محل البحث من داخل المؤسسة المالية نفسها أو من خارجها بالاستعانة بشبكة الاتصالات ونظم تقنية المعلومات، فيدخل الفاعل إلى نظام إدارة ومعالجة المال المعلوماتي داخل تلك المؤسسة، ويستعين بخبراته وبرامج خاصة، ويعمد إلى التلاعب في قاعدة البيانات المالية للعملاء فلا أهمية بعد ذلك لكون الدخول إلى نظام المعالجة الإلكترونية للبيانات المالية في المؤسسة كان بطريقة مشروعة أو بطريقة غير مشروعة[2].

الفرع الثاني: تزوير المحررات في جرائم التكنولوجيا الحديثة

تشهد جريمة تزوير المحررات المتصلة بالتكنولوجيا الحديثة بوصفها إحدى صور الغش المعلوماتي تزايدا ملحوظا، وذلك تماشيا مع حلول الدعامات المعلوماتية محل المحررات التقليدية في جميع المجالات نظرا إلى ما تمتاز به من سعة تخزينية وحسن تبويب المعلومات المخزنة وسرعة استرجاعها، الأمر الذي دفع البعض[3] إلى القول إن جريمة تزوير المحررات هنا هي من أخطر جرائم الغش المعلوماتي.

وإن كانت القوانين الجزائية قد حرصت على النص على تجريم التزوير في المحررات بأنواعها المختلفة إيمانا منها بأنها تهدد الثقة التي يمنحها الأفراد لها في اكتساب الحقوق أو تحمل الالتزامات، إلا أن هذه النصوص صيغت لمواجهة الاعتداءات التي ترد على الأموال المادية أو المحررات المعرضة للتلف المادي، ومن ثم فإنها تعجز عن مواجهة الاعتداءات التي تستهدف القيم المعنوية أو المحررات

---

[1] زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، 2011، ص86.

[2] توفر التقنية الحديثة وسائل وأجهزة وتقنيات تمكن الفاعل من اختراق نظم الاتصالات والوسائل الإلكترونية الأخرى حتى مع توافر نظم الحماية.

[3] سليم عبد الله الجبوري، المرجع السابق، ص359. حسني عبد السميع إبراهيم، الجرائم المستحدثة عن طريق الإنترنت، دراسة مقارنة بين الشريعة والقانون، دار النهضة العربية، القاهرة، 2001، ص445.

المعلوماتية الناشئة عن الثورة المعلوماتية التي يشهدها العالم، فجريمة تزوير المحررات لم تعد حبيسة البيئة المادية كما كانت في السابق وأصبحت تقع في البيئة المعلوماتية أيضا وعلى نطاق أوسع، إذ تكاد لا تخلو جرائم التكنولوجيا الحديثة من التزوير المعلوماتي بشكل أو بآخر[1]، الأمر الذي يقتضي تدخل المشرع لمواجهة أنماط السلوك الإجرامي لهذه الجريمة في بيئتها الجديدة.

البند الأول: تعريف جريمة تزوير المحررات المتصلة بالتكنولوجيا الحديثة

يعرف التزوير في جرائم التكنولوجيا الحديثة بأنه تغيير الحقيقة بأي وسيلة كانت، سواء كان ذلك في محرر أو دعامة أو سند طالما أن هذه الدعامة لها أثر في إنشاء حق أو من شأنها إحداث نتائج قانونية معينة[2]، كما يعرف بأنه تغيير في حقيقة المستند المعالج إلكترونيا بقصد إحداث ضرر بالطرق المحددة قانونا[3]، ويعرف أيضا بأنه تغيير الحقيقة في المستندات المعالجة آليا والمستندات المعلوماتية وذلك بنية استعمالها[4]، ويلاحظ من هذا التعريف الأخير أخذه للمفهوم التقليدي لجريمة التزوير مع توسيع نطاقه ليستغرق التغير الحاصل في حقيقة المحررات المتصلة بالتكنولوجيا الحديثة، كما يعرف كذلك بأنه أي تغيير للحقيقة يرد على مخرجات الوسائل الإلكترونية سواء تمثلت في ورقة مكتوبة أو مرسومة عن طريق الرسم، ويستوي في المحرر المعلوماتي أن يكون باللغة العربية أو أي لغة أخرى لها دلالتها، كذلك قد تتمثل في مخرجات غير ورقية بشرط أن تكون محفوظة على دعامة كبرنامج منسوخ على أسطوانة بشرط أن يكون المحرر المعلوماتي ذا أثر في إثبات حق أو أثر قانوني[5].

انطلاقا مما سبق يمكن استخلاص تعريف للتزوير في جرائم التكنولوجيا الحديثة من المادة 07 لاتفاقية بودابست المتعلقة بالجرائم المعلوماتية لسنة 2001 بأنه: إدخال بيانات إلى الحاسب الآلي أو تبديلها أو محوها أو تدميرها، فتنتج عنها بيانات غير أصلية، بقصد استخدامها أو الاعتماد عليها في أغراض قانونية، كما لو كانت أصلية، بغض النظر عما إذا كانت هذه البيانات مقروءة ومفهومة بشكل مباشر من عدمه.

البند الثاني: أركان جريمة تزوير المحررات المتصلة بالتكنولوجيا الحديثة

تقوم جريمة تزوير المحررات التقليدية على ثلاثة أركان هي الركن المادي المتمثل في تغيير الحقيقة في محرر بإحدى الطرق المحددة قانونا، وركن الضرر، والركن المعنوي المتمثل في القصد الجنائي الخاص، وهي ذاتها أركان جريمة تزوير المحررات المتصلة بالتكنولوجيا الحديثة، ومن المتفق عليه أنه لا توجد إشكالية فيما يتعلق بالركن المعنوي وركن الضرر، بيد أنها تظهر بوضوح في الركن المادي بسبب اختلاف طبيعة المحرر المعلوماتي عن المحرر الورقي الأمر الذي قد يحول دون تطبيق النص الجنائي الخاص لجريمة التزوير التقليدية على

---

[1] صباح رمضان ياسين صالح، المرجع السابق، ص75. منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها المرجع السابق، ص90.

[2] أحمد حسام طه تمام، المرجع السابق، ص407.

[3] هدى حامد قشقوش، السياسة الجنائية لمواجهة الجريمة المعلوماتية، دار النهضة العربية، القاهرة، 2012، ص47.

[4] عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر والإنترنت، منشأة المعارف، 2010، ص159.

[5] أيمن عبد الحفيظ عبد الحميد سليمان، استراتيجية مكافحة جرائم استخدام الحاسب الآلي، دراسة مقارنة، المرجع السابق، ص86.

التلاعب بالبيانات والمعلومات[1]، ومن هذا المنطلق سوف نقصر دراستنا هنا على أحد عناصر الركن المادي لجريمة التزوير المتصلة بالتكنولوجيا الحديثة، وهو المحرر المعلوماتي دون ركن الضرر والركن المعنوي اللذان لا يثيران أية إشكالات قانونية.

أولا: مفهوم المحرر المعلوماتي، تزداد أهمية المحرر المعلوماتي يوما بعد يوم حيث أصبح يحل محل المحرر التقليدي في كثير من المجالات، فهو يماثل المحرر الورقي في أوجه الاستعمال، كما أنه قد يماثله في نظر العديد من التشريعات من حيث القوة القانونية المقررة له، إضافة إلى أن للمحرر المعلوماتي الكثير من المزايا التي تكفل له انتشارا واسعا وتزايدا في الاستعمال[2]، الأمر الذي دفع البعض[3] إلى التنبؤ بأن مراكز المعلومات في المستقبل سوف تصبح عبارة عن مستودعات لا ورقية للمعلومات، وأن انحسار المحررات الورقية سيمتد ليشمل صفوف الفكر وتطبيقاته المتنوعة في مجالات الحياة المختلفة.

ويعرف المحرر المعلوماتي[4] بأنه حروف وكلمات ذات دلالات معينة تنتظم في عبارات ورموز وصور تعبر عن معنى محدد على وسط إلكتروني، إذ يتم إدخال الكتابة إلى ذاكرة الحاسب الآلي –غالبا باستخدام لوحة المفاتيح– لتتم بعد ذلك معالجته إلكترونيا ثم تخزينه، وذلك لإمكان استرجاعه عند الحاجة إليه باللجوء إلى وحدات التخزين الإلكتروني المعروفة كالأشرطة الممغنطة والأقراص المرنة والأقراص الصلبة وغيرها[5]، أو هو كل دعامة مادية مهيأة لاستقبال المعلومات والتي يتم تسجيل المعطيات عليها من خلال تطبيق إجراءات المعالجة المعلوماتية، أو بعبارة أخرى الدعامة المادية التي تم تحويل المعطيات المسجلة عليها إلى لغة الآلة[6]، كما يعرف أيضا أنه كل جسم منفصل أو يمكن فصله عن نظام المعالجة الآلية للمعلومات وقد سجلت عليه معلومات معينة سواء كان معدا للاستخدام بواسطة نظام المعالجة الآلية للمعلومات أم مشتقا من هذا النوع[7].

ويجب أن يتضمن المحرر تعبيرا ذو قيمة قانونية عن معاني وأفكار إنسانية مترابطة، ويقصد بذلك أن ما يشمله المحرر يمثل أداة للتفاهم وتبادل الأفكار، وهذا ما يؤكد الدور الاجتماعي للمحرر باعتباره وسيلة المعاملات القانونية، بمعنى أن يترتب على التلاعب به وقوع ضرر كشرط للعقاب مثلما هو مقرر في تزوير المحررات الورقية، مع ضرورة اتصاف المحرر بالصفة الإلكترونية.

بناء على ما سبق نجد أن الفقه اختلف حول مدى اعتبار تغيير الحقيقة المنصب على المعلومات المخزنة بطريقة إلكترونية سواء على شريط ممغنط أو قرص من أقراص الحاسب الآلي أو أي شريحة رقاقية أخرى من قبيل تغيير الحقيقة في محرر، وبالتالي إمكانية تطبيق النصوص التقليدية لجريمة تزوير المحررات عليها.

وعليه، فقد انقسم الفقه إلى اتجاهين، الأول يرى شمول فكرة المحرر للمحرر الإلكتروني والورقي مع إمكان تطبيق النصوص التقليدية للتزوير على تغيير الحقيقة فيه، أما الاتجاه الآخر فيرى أن فكرة المحرر لا تشمل المحرر المعلوماتي ومن ثم لا إمكانية لتطبيق

---

[1] سليم عبد الله الجبوري، المرجع السابق، ص360. صباح رمضان ياسين صالح، المرجع السابق، ص82 و83.

[2] أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني، دراسة مقارنة، دار النهضة العربية، القاهرة، 2006، ص06.

[3] هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص17.

[4] يسميه البعض الوثيقة المعلوماتية، والبعض الآخر يسميه المستند الإلكتروني. أحمد حسام طه تمام، المرجع السابق، ص417. أشرف توفيق شمس الدين المرجع السابق، ص08 وما بعدها.

[5] صباح رمضان ياسين صالح، المرجع السابق، ص84.

[6] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص139.

[7] أحمد حسام طه تمام، المرجع السابق، ص422.

نصوص التزوير التقليدية عليه –وهو ما نؤيده– مستندين في ذلك إلى العديد من الحجج يمكن إجمالها فيما يلي:

- أن مفهوم المحرر الذي جرمت أغلب التشريعات المساس به يرتبط على وجه اللزوم بالأوراق، كما لا تتصف الكلمات والرموز المثبتة على المحرر المعلوماتي بالبقاء النسبي حتى تكون حجة على المتعاملين به لمدة طويلة نسبيا[1].
- أن المعلومات المخزنة في ذاكرة الوسائل الإلكترونية لا تعد محررا مكتوبا كونها ليست مقروءة ولا يمكن للمعنى الذي تحمله أن ينتقل عن طريق العين المجردة، من ثم فإنها تفتقر إلى صفة المحرر الذي يكون قابلا للإدراك بمجرد الإطلاع عليه دون الحاجة إلى الاستعانة بأجهزة خاصة للقراءة كالحاسب الآلي مثلا[2].
- ربط المشرع بين مفهوم التوقيع كونه أحد عناصر الكتابة على المحرر ووجوب اعتماده على حركة اليد، فقد حدد صور التوقيع بالإمضاء أو بصمة الإبهام أو الختم الشخصي، وهو ما لا يتوافر في مفهوم التوقيع الإلكتروني[3]، الذي يتمثل في رقم أو شفرة لا علاقة لها باسم أو لقب الشخص أو ملامح بصمته[4].

كما أن جريمة التزوير بمفهومها التقليدي تشترط الكتابة وهو شرط غير متحقق في الوعاء المعلوماتي الذي يحوي المعلومات المعالجة آليا أيا كان نوع هذا الوعاء، مما يعني أن التغيير فيها لا يحقق جريمة التزوير[5]، كما أن جريمة التزوير هنا تبين عموما إمكانية استعمال الوثيقة المزورة كوسيلة إثبات لكن التسجيلات المعلوماتية لا تصلح لذلك[6].

لأجل مواجهة الجرائم المستحدثة ولمعالجة القصور في النصوص العقابية التقليدية وبهدف مد مظلة الحماية الجنائية للمعلوماتية من هذه الجرائم وبخاصة جريمة تزوير المحررات المتصلة بالتكنولوجيا الحديثة، نظرا إلى خطورتها وانتشارها بعد استخدام الأجهزة الآلية وبنطاق واسع في تسيير أمور المجتمع المهمة، عمد المشرع في العديد من الدول إلى استحداث نصوص تجريمية أو إدخال تعديلات على النصوص القائمة.

في هذا الصدد عالج المشرع الجزائري جريمة التزوير في قانون العقوبات، وشأنه شأن سائر التشريعات الأخرى اكتفى ببيان طرق التزوير المادية والمعنوية للمحررات الرسمية في المواد 214 و215 و216، ومن خلال استقرائنا لهذه النصوص نصل إلى عدم إمكان تطبيقها على تغيير الحقيقة المنصبة على المحررات المعلوماتية، كما أن المشرع الجزائري وإن سار على نهج المشرع الفرنسي بأن قام بإجراء تعديل على قانون العقوبات بهدف حماية النظام المعلوماتي ككل متكامل (الكيان المادي والكيان المعنوي)، إلا أنه لم يتعرض إلى جميع الجرائم التي تطرق لها المشرع الفرنسي ومنها جريمة تزوير المستندات (المحررات المعلوماتية) والتي هي على قدر كبير من الأهمية، ومن ثم فإن المشرع الجزائري لم يوفق في الإحاطة الشاملة بكل جرائم التكنولوجيا الحديثة، لذا نلتمس انتباه المشرع

---

[1] أيمن عبد الله فكري، المرجع السابق، ص272 و273.

[2] نهلا عبد القادر المومني، المرجع السابق، ص149.

[3] يعرف التوقيع الإلكتروني بأنه حروف أو أرقام أو رموز أو إشارات لها طابع متفرد تسمح بتحديد شخص صاحب التوقيع وتميزه عن غيره، وله عدة صور منها؛ التوقيع الكودي أو السري والتوقيع البيومتري والتوقيع بالقلم الإلكتروني والتوقيع الرقمي...إلخ. عادل رمضان الأبيوكي، التوقيع الإلكتروني في التشريعات الخليجية، دراسة مقارنة، المكتب الجامعي الحديث، الإسكندرية، ط1، 2009، ص15 وما بعدها.

[4] صباح رمضان ياسين صالح، المرجع السابق، ص86.

[5] أيمن عبد الله فكري، المرجع السابق، ص273.

[6] عفيفي كامل عفيفي وفتوح عبد الله الشاذلي، المرجع السابق، ص226. حسني عبد السميع إبراهيم، المرجع السابق، ص460.

الجزائري إلى النص على جريمة تزوير المحررات سواء من خلال تعديل النصوص القائمة أسوة بنظيره الفرنسي أو استحداث أخرى جديدة[1].

المطلب الثاني: النصب وإساءة الائتمان في جرائم التكنولوجيا الحديثة

سنحاول دراسة هذا المطلب من خلال التطرق إلى جرائم الاحتيال، إساءة الائتمان كل جريمة على حدى.

الفرع الأول: النصب في جرائم التكنولوجيا الحديثة

تعد جريمة النصب (الاحتيال)[2] إحدى جرائم الاعتداء على حق الملكية، حيث تتمثل في الاستيلاء على الحيازة الكاملة لمال الغير بوسيلة يشوبها الخداع تسفر عن تسليم ذلك المال[3].

وأدى التطور العلمي والتقني في العصر الحالي إلى خروج جريمة النصب من إطارها التقليدي واتخاذها بعدا تقنيا في المجال المعلوماتي، تختلف عن صورتها التقليدية من حيث محل السلوك الإجرامي والطرق والوسائل الاحتيالية المستخدمة فيها، فلم تعد جريمة تستهدف البسطاء فقط وإنما باتت تستهدف الأذكياء أيضا[4]، ولدراسة هذه الجريمة، سوف نتعرض لتعريفها ثم نتناول أركانها.

البند الأول: تعريف النصب في إطار جرائم التكنولوجيا الحديثة

يشير وصف النصب المعلوماتي إلى صورة مستحدثة للاحتيال تقوم على إساءة استخدام الوسائل الإلكترونية والتلاعب في نظم المعالجة الآلية للمعلومات بغية الحصول بغير وجه حق على أموال أو أصول أو خدمات، وهي بهذه الصورة تتميز عن النصب التقليدي بعدة سمات، أهمها التعقيد الناجم عن استخدام المفاتيح والشفرات والوسائل الإلكترونية في ارتكابها ومحلها ذو الطبيعة المعنوية المتمثل في المعلومات وكذلك إمكانية ارتكابها عن بعد[5].

ويعرف النصب في البيئة الرقمية، بصفة عامة، بأنه سلوك خداعي مرتبط بالوسائل الإلكترونية يهدف شخص بواسطتها إلى كسب فائدة ومصلحة مالية[6]، أو أنه حث الوسائل الإلكترونية على تغيير بعض الحقائق بأي أسلوب كان بهدف الحصول على ربح غير مشروع على حساب شخص آخر، فوظيفة الوسائل الإلكترونية تكمن في مساعدة الجاني على إتمام فعل النصب[7]، كما

---

[1] خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، أساليب وثغرات، دار الهدى، عين مليلة، الجزائر، 2017، ص142-145.

[2] اختلفت التشريعات الجنائية العربية فيما بينها في تسميتها لجريمة الاحتيال، البعض منها ذهب إلى تسميتها بجريمة النصب كالتشريع الجزائري والمصري والليبي والكويتي والبحريني والمغربي، أما البعض الآخر فقد استخدم تعبير جريمة الاحتيال كالتشريع الأردني والسوري والعراقي والعماني والقطري واللبناني.

[3] حسن صادق المرصفاوي، المرصفاوي في قانون العقوبات، القسم الخاص، منشأة المعارف، الإسكندرية، 1987، ص379. هشام محمد فريد رستم، جرائم الحاسوب كصورة من صور الجرائم للاقتصادية المستحدثة، المرجع السابق، ص268.

[4] أيمن عبد الحفيظ عبد الحميد سليمان، استراتيجية مكافحة جرائم استخدام الحاسب الآلي، دراسة مقارنة، المرجع السابق، ص22.

[5] هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، المرجع السابق، ص45 و46.

[6] ناظم محمد نوري الشمري، عبد الفتاح زهير، الصيرفة الإلكترونية، الأدوات والتطبيقات ومعيقات التوسع، دار وائل للنشر، عمان، ط1، 2008 ص197.

[7] Hugo Cornwall, Data Theft, Computer Fraud, Industrial Espionage and Information Crime Mandarin, 1990, p67.

يعرف أيضا بأنه الخداع أو الغش المعلوماتي الذي يقوم على التلاعب في نظم المعالجة الآلية للمعلومات بهدف الحصول دون وجه حق على خدمات أو أموال أو أصول معينة[1].

بينما عرف البعض[2] النصب المعلوماتي بأنه التلاعب بالبرامج أو البيانات بالتغيير فيها بما يترتب عليه إيهام المجني عليه بصحتها والتسليم بها، وفي سبيل تفادي قصور التعريفات السابقة عن بيان جميع العناصر التي تميز النصب المعلوماتي عن صورته التقليدية عرفه البعض الآخر[3] بأنه التلاعب العمدي بمعلومات وبيانات تمثل قيما مالية يختزنها نظام الحاسب الآلي، أو الإدخال غير المصرح به لمعلومات وبيانات صحيحة، أو التلاعب في الأوامر والتعليمات التي تحكم عملية البرمجة، أو أية وسيلة أخرى من شأنها التأثير في الوسائل الإلكترونية حتى تقوم بعملياتها بناء على هذه البيانات أو الأوامر أو التعليمات، لأجل الحصول على ربح غير مشروع وإلحاق ضرر بالغير.

مما تقدم، يتبين لنا أن النصب في جرائم التكنولوجيا الحديثة يتماثل مع النصب التقليدي فيها يتعلق باستخدام وسائل خداع للاستيلاء على أموال المجني عليه، ويختلف معه كونه ينطوي على استخدام الجاني للوسائل التقنية الإلكترونية في خداع وإيهام المجني عليه ودفعه إلى تسليم أمواله المتمثلة في القيم المعلوماتية.

البند الثاني: أركان جريمة النصب المتصلة بالتكنولوجيا الحديثة

يعد النصب المعلوماتي من الأنشطة الجرمية المستحدثة، فهي جريمة تقع على معلومات داخل نظم المعالجة الآلية عن طريق التلاعب فيها بالاستعانة بالوسائل التقنية الحديثة، إذ تبين لنا أنه يتطلب لقيامها تحقق ركنيها المادي والمعنوي[4]، وهنا سنحاول بيان مدى إمكانية تحقق هذين الركنين في إطار المعلوماتية لهذه الجريمة كما يأتي:

أولا: الركن المادي لجريمة النصب المعلوماتي، يتألف الركن المادي لجريمة النصب المتصل بالتكنولوجيا الحديثة من ثلاثة عناصر هي السلوك الإجرامي، النتيجة الجرمية والعلاقة السببية، وتثير هذه العناصر في مجال الاحتيال المعلوماتي الكثير من الخلاف والجدل، كونها جريمة على درجة من التعقيد سواء كان ذلك من حيث طبيعة المحل الذي ترد عليه أو من حيث الوسائل التي ترتكب من خلالها، التي تتنوع[5]، لكنها تتفق في انطوائها على التلاعب بالبيانات والمعلومات التي يحتوي عليها النظام المعلوماتي من أجل تحقيق ربح مادي غير مشروع حاول جانب من الفقه تحديدها، والتي تتحدد أساسا في التلاعب في مرحلة إدخال البيانات[6]

---

[1] محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، القاهرة، 2001، ص79.

[2] هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، المرجع السابق، ص132.

[3] نائلة عادل محمد فريد قورة، المرجع السابق، ص444.

[4] ماهر عبد شويش الدرة، المرجع السابق، ص338 و339.

[5] هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، المرجع السابق، ص57 وما بعدها. أحمد محمود مصطفى، المرجع السابق، ص274 و275.

[6] نائلة عادل محمد فريد قورة، المرجع السابق، ص454-458.

التلاعب في مرحلة إخراج البيانات[1]، التلاعب في البرامج[2]، التلاعب في المكونات المادية[3]، التلاعب في البيانات التي يتم تحويلها عن بعد، التلاعب في محيط الصرف الآلي وكذا استعمال شفرة غير صحيحة للدخول إلى النظام مدفوع الأجر.

ثانيا: الركن المعنوي في جريمة النصب المعلوماتي، جريمة النصب المتصلة بالتكنولوجيا الحديثة جريمة عمدية، يتطلب قيامها توافر القصد الجنائي الذي يتمثل في القصد الجنائي العام، أي انصراف علم الجاني إلى ما يقوم به من تلاعب في المعلومات الموجودة في نظام المعلومات الآلي أو إدخال معلومات إلى هذا النظام، وهو فعل غير مشروع من شأنه أن يوقع الوسائل الإلكترونية في الغلط، كما يجب أن ينصرف علم الجاني إلى أن ما يتسلمه من مال مملوك للغير، ويستوي في ذلك أن يكون عالما أنه مملوكا للمجني عليه أو لشخص آخر غيره، وأن تتجه إرادته إلى إيقاع الوسائل الإلكترونية في الغلط بهدف سلب المال المملوك للغير[4].

أما فيما يتعلق بالقصد الجنائي الخاص في جريمة النصب المعلوماتي (أي نية عن تملك المعلومات فيصعب القول بتحققها ذلك أن استيلاء الجاني على المعلومات محل الاحتيال لا يترتب عليه حرمان المجني عليه منها، بل تظل في حيازته وتحت سيطرته خاصة في حالة حصول الجاني على المعلومات أو الإطلاع عليها.

تجدر الإشارة في هذا المقام أن المشرع الجزائري لم يتطرق في التعديل الذي أجراه على قانون العقوبات إلى جريمة النصب المعلوماتي، وبذلك يكون قد أحال معالجتها إلى النص الخاص بجريمة النصب (الاحتيال) التقليدية، إذ تنص المادة 372على أنه: "كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو براء من التزامات أو بالحصول على أي منها أو شرع في ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها...".

ويستخلص من هذا النص أن ليس كل شيء مادي ومنقول يصلح أن يكون محلا لجريمة النصب المتصلة بالتكنولوجيا الحديثة بل يجب أن يكون ضمن التعداد الذي ذكره المشرع في هذه المادة، غير أن لفظ المنقول ورد في النص دون تحديد طبيعته أو تقييده من قبل المشرع مما يعطي المجال لتفسير النص على نحو يشمل المعلومات ذات الطبيعة المعنوية، غير أن تطبيق هذا النص قد يواجه العديد من الصعوبات منها التسليم، وعلى فرض إمكانية وقوعه فإنه لن ينتج عنه حرمان المجني عليه من المعلومات، وهو إن كان يتفق مع طبيعة المعلومات فإنه لا يتفق مع طبيعة النشاط الإجرامي لجريمة النصب المتصلة بالتكنولوجيا الحديثة.

الفرع الثاني: جريمة إساءة الائتمان المتصلة بالتكنولوجيا الحديثة (خيانة الأمانة)

إن انتشار العبث بالائتمان الخاص غدا أمرا يهدد العلاقات الخاصة ويقضي على روح التعامل بين الناس في ثقة واطمئنان

---

[1] محمد قدري حسن عبد الرحمن، جرائم الاحتيال الإلكتروني، مجلة الفكر الشرطي، المجلد 20، العدد 89، مركز بحوث الشرطة، الإمارات العربية المتحدة أكتوبر 2011، ص69.

[2] محمد محمد شتا، المرجع السابق، ص83-85. Donn B. Parker, Fighting Computer Crime: A New Framework for Protecting Information, Op.Cit., p94.

[3] نائلة عادل محمد فريد قورة، المرجع السابق، ص465.

[4] عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة، 2009، ص385.

وحماية هذا الائتمان أصبحت مصلحة جوهرية مما اقتضى ضرورة تدخل المشرع الجنائي لإسباغ الحماية على هذه المصلحة، كما أن جريمة خيانة الأمانة المعلوماتية لا يمكن فهمها بعيدة على القواعد التقليدية في جريمة خيانة الأمانة[1]، والتي تعد من جرائم الاعتداء على الأموال وهي بذلك تتفق مع جريمة السرقة وجريمة الاحتيال أو النصب[2] من حيث كون محل الجريمة مالا منقولا مملوكا لغير الجاني.

غير أن وجه الاختلاف بين جريمة خيانة الأمانة والسرقة يكمن في أن التسليم في جريمة خيانة الأمانة يعد شرطا لتحققها فالمال محل الجريمة يجب أن يكون في حيازة الجاني ابتداء، لكن حيازته تكون حيازة ناقصة، أي يده عليها يد مؤقتة بناء على عقد من عقود الأمانة، ثم تنصرف إرادة الجاني إلى تحويل حيازته للمال إلى حيازة كاملة، وذلك بالاستيلاء عليه أو تبديده والظهور عليه بمظهر المالك، بينما التسليم في جريمة السرقة يكون نافيا لقيام الجريمة[3]، وتتميز جريمة خيانة الأمانة عن جريمة النصب هنا، أن تسليم المال في جريمة الاحتيال وإن كان برضا المجني عليه، إلا أنه يحصل نتيجة استخدام وسائل احتيالية، أي نتيجة غش، بينما التسليم في جريمة خيانة الأمانة حصل برضا المالك أو الحائز وغير مشوب بغلط أو تدليس، كما وأن التسليم في جريمة النصب يكون بنية نقل الحيازة الكاملة للمال، وذلك بخلافها في جريمة خيانة الأمانة، حيث يكون لمجرد نقل الحيازة الناقصة أو المؤقتة[4].

البند الأول: تعريف جريمة إساءة الائتمان المتصلة بالتكنولوجيا الحديثة

لم يتعرض المشرع الجزائري لجريمة خيانة الأمانة المتصلة بالتكنولوجيا الحديثة، كما لم يشر في قانون العقوبات إلى وقوع خيانة الأمانة على المعلومات، غير أن ذلك لا يعني عدم إمكان قيامها في نطاق التكنولوجيا الحديثة، وفي ظل هذا النقص التشريعي وعدم وجود تعريف فقهي لجريمة خيانة الأمانة المتصلة بالتكنولوجيا الحديثة، فإننا نتفق مع تعريف لهذه الجريمة مستمد من تعريف كبار الفقهاء لجريمة خيانة الأمانة التقليدية عله يضيف شيئا في هذا المقام بأنه: كل تصرف أو استعمال أو استغلال وما في حكمها لمعلومات أو برامج مملوكة للغير سلمت إلى الجاني على سبيل الأمانة أضرارا بمالكها أو حائزها مع توافر القصد الجنائي.

فبالرجوع إلى قانون العقوبات الجزائري نجد خلوه من أي نص خاص بجريمة خيانة الأمانة المتصلة بالتكنولوجيا الحديثة وعالج جريمة خيانة الأمانة التقليدية في المادة 376 ق.ع والتي تنص على أنه: "كل من اختلس أو بدد بسوء نية أوراقا تجارية أو نقودا أو بضائع أو أوراقا مالية أو مخالصات أو أية محررات أخرى تتضمن أو تثبت التزاما أو إبراء لم تكن قد سلمت إليه إلا على سبيل الإجارة أو الوديعة أو الوكالة أو الرهن أو عارية الاستعمال أو لأداء عمل بأجر أو بغير أجر بشرط ردها وتقديمها أو لاستعمالها..."، وفي ظل عدم إمكان تطبيق هذا النص على المعلومات فإن المشرع الجزائري مدعو كغيره من المشرعين إلى تعديله أو إصدار نصوص جديدة توفر الحماية الجنائية للمعلومات من جريمة خيانة الأمانة المتصلة بالتكنولوجيا الحديثة.

---

[1] يطلق عليها بعض التشريعات جريمة إساءة الائتمان.

[2] جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، المرجع السابق، ص123. علي عبد القادر القهوجي، قانون العقوبات القسم الخاص، جرائم الاعتداء على المصلحة العامة وعلى الإنسان والمال، المرجع السابق، ص827.

[3] ماهر عبد شويش الدرة، المرجع السابق، ص317.

[4] جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، المرجع السابق، ص123.

البند الثاني: أركان جريمة إساءة الائتمان المتصلة بالتكنولوجيا الحديثة

أولا: الركن المادي في الجريمة المستحدثة، يختلف الركن المادي في جريمة إساءة الائتمان التقليدية عنه في الجريمة المستحدثة، هذا الاختلاف يبرز من حيث الأسلوب والوسيلة والنتائج والمحل ولهذا وجب تطوير النص الجزائي التقليدي ليستوعب المفهوم الجديد المستحدث لمحل الجريمة والسلوك المادي فيها بكل ما يشمله من عناصر، دون إخلال بأركان الجريمة التقليدية الأساسية من حيث سبب التسليم وغايته، مع بحث في طبيعة السلوك الذي أصبح يأخذ طابعا معنويا هو الآخر من كافة جوانبه، سواء من حيث الأسلوب أو الأداة أو النتيجة.

وعليه يمكن تصور إساءة الائتمان الإلكتروني ضمن عقود الائتمان[1] الواردة حصرا بالنص التقليدي تقوم في مجملها على التسليم، هذا التسليم الذي ينتظر به المالك تنفيذ مهمة معينة على عاتق المستلم بعد فراغ غاية التسليم وفقا لسببه، على أنه من الضرورة إدراك الطبيعة الجديدة للتسليم، فلم يعد المطلوب التسليم المادي أو المبادلة اليدوية أو بواسطة ثالث لتنفيذ مضمون العقد بل أصبح يكتفي بالتسليم المعنوي القائم على سلوكيات معنوية، فتسليم برنامج تقني للقيام بخدمات ما يكون مثلا بتسليم الشخص مفتاح العمل أو التشغيل أو كلمة المرور ونحو ذلك، وتسليم برنامج تطبيقي يمكن أن يكون عن طريق تقنية نظم الاتصال المعلوماتي وعبر شبكة الإنترنت مثلا، والخلاصة أن كافة عقود الائتمان الواردة حصرا بنص التجريم تصلح أن تكون قاعدة لجريمة إساءة الائتمان التقنية مع تفاوت في مدى انتشار ذلك في الواقع العملي.

ثانيا: الركن المعنوي، يجمع الفقه على أن جرم إساءة الائتمان مثله مثل السرقة والنصب يحتاج لتمامه قصدا خاصا، فلا يكفي في جرائم إساءة الائتمان لتحقق الركن المعنوي العلم والإرادة العنصرين العامين، بل لا بد من ثبوت القصد الخاص[2] إلى جانب ذلك، والذي يتمثل في نية التملك والظهور من قبل الفاعل بمظهر المالك على الشيء محل الجريمة.

وهنا اجتمع الفقه على تطلب القصد الخاص في إساءة الائتمان، إلا أنه اختلف في ثبوته ضمنا في كل صور السلوك الجرمي، فمنهم من يرى أن القصد الخاص مطلوب فقط في صور الاستعمال والظهور مظهر المالك والتصرف باعتبار ذلك أساس نية التملك وهي جوهر القصد الخاص، ولا يطلبون القصد الخاص (نية التملك) في غير ذلك من صور السلوك كما في الإتلاف والتبديد[3].

في حين يرى آخرون أن القصد الخاص (نية التملك) مطلوب في كافة صور الركن المادي في جريمة إساءة الائتمان، باعتبار أنه في التبديد والإتلاف وإلحاق الضرر لا يعمد الفاعل إلى ذلك إلا بعد أن يكتسب في نفسه حق الاستثمار بالمال، فتكون نية التملك الحدث الأسبق لفعل الإتلاف والتبديد، فكانت إذن مطلوبة في كل صور الركن المادي، وهو توجه نراه ونقره نحن أيضا، مع بيان أنه وفي أحوال الإتلاف والتبديد فإن القصد الخاص يكون بصورة حرمان صاحب المال منه نهائيا[4].

---

[1] أنظر المواد من القانون المدني الباحثة في عقود الائتمان.

[2] أحمد خليفة الملط، المرجع السابق، ص408.

[3] عفيفي كامل عفيفي وفتوح عبد الله الشاذلي، المرجع السابق، ص199.

[4] عفيفي كامل عفيفي وفتوح عبد الله الشاذلي، المرجع نفسه، ص199.

المطلب الثالث: المساس بالملكية الفكرية في جرائم التكنولوجيا الحديثة

اتسعت مجالات الاعتداء على حقوق الملكية الفكرية والأدبية لتشمل أشكال التعبير المبتكرة التي أظهرها التطور التكنولوجي، فشملت برامج تشغيل نظم معلومات الوسائل الإلكترونية[1]، وقاعدة بيانات الحاسوب الإلكترونية بعد أن كانت محمية باعتبارها داخلة ضمن حقوق الملكية الصناعية (براءات الاختراع)، وأصبحت الآن من قبيل المصنفات الداخلة ضمن حقوق الملكية الأدبية والفكرية.

إن الاعتداء على حق الملكية الفكرية يتمثل في أفعال تنتهك هذا الحق بدون إذن، وله عدة صور، كتزوير العلامات التجارية والصناعية، استنساخ المصنفات بصفة غير شرعية عن طريق الإضافة أو الحذف، إعادة طبع المؤلفات دون إذن صاحبها الاقتباسات والترجمات غير المشروعة...إلخ، كل هذه الأفعال تشكل اعتداء على الملكية الفكرية، ولعل أهمها وأكثرها شيوعا هي التقليد والقرصنة سواء تعلق الأمر بمجال الملكية الصناعية، العلامات، البراءات، الرسوم والنماذج الصناعية وأسماء النطاقات التي ينظر إليها كأحد المسائل المتعين إخضاعها لنظام الأسماء والعلامات التجارية بسبب ما أثارته من منازعات جراء تشابهها بالعلامات والأسماء التجارية وتطابقها في حالات عديدة، أو لقيامها بذات المهمة تقريبا في البيئة الرقمية، أو بمجال الملكية الأدبية الفنية، حق المؤلف والحقوق المجاورة نظرا للآثار السلبية التي يخلفها هذا الاعتداء ليس فقط على الفرد وإنما على كيان المجتمع ونظامه الاقتصادي.

الفرع الأول: جرم التقليد عبر شبكة الإنترنت

نظرا لأهمية حقوق المؤلف الأدبية والمالية، فإن القانون لم يكتف بتقرير الجزاءات المدنية لحمايتها، وإنما أقر بعض الجزاءات على تلك التي تقع على من يعتدي على حق المؤلف، وسببه يرجع إلى أن المؤلف قد يتعرض لاعتداءات خطيرة على حقوقه الأدبية والمالية توجب فرضية مثل هذه الجزاءات الجزائية على مرتكبيها كعامل ردع يدفع بالغير إلى الابتعاد عن انتهاك حقوق المؤلف والجنحة التي ينص عليها القانون في هذه الحالة تسمى جنحة التقليد، وتتكون من عنصر مادي وآخر معنوي وعلاقة سببية بينهما وهي من الأمور التي تقع على البرمجيات وقواعد المعلومات، والتي اعتبرت مصنفات أدبية تحمي بموجب قوانين حق المؤلف مع إمكانية وجود اتجاه حديث وتحديدا في أمريكا وأوروبا يعيد طرح نجاح حمايتها عبر آلية حماية براءات الاختراع.

البند الأول: الإطار القانوني لجرم التقليد

جرمت القوانين على اختلافها الفعل الذي يعد تقليدا للمصنف الفكري، فالتقليد معاقب عليه ولا يجوز لأحد الاعتداء على حقوق المؤلف والقيام بتقليد المصنفات أو نشرها دون موافقته، لأن ذلك فيه مساس بشخصيته الفكرية، ويمثل انتهاكا لحقوقه الأدبية، وقد أضاف المشرع الجزائري صورا أخرى جديدة تتناسب مع التطور الحاصل في مجال المعلوماتية وشبكات الاتصالات وقد

[1] مأمون التلهوني، حماية حقوق الملكية الفكرية وإنفاذها في الأردن، ندوة الوب الوطنية عن الملكية الفكرية للصحفيين تنظمها المنظمة العالمية للملكية الفكرية (الويبو) بالتعاون مع دائرة المكتبة الوطنية / وزارة الصناعة والتجارة ومركز الملك عبد الله الثاني للملكية الفكرية، عمان، 06 نيسان 2004 ص01.

عاقب مرتكبي هذه الصور لأن فيها اعتداء على حقوق المؤلف الأدبية.

فالدستور بصفته القانون الأساسي يقر الحماية لحقوق المؤلف، وجاءت نصوصه عامة وشاملة تاركا التفاصيل لقانون حق المؤلف، الذي يساير التطورات العلمية والتقنية، خاصة مع ظهور مصنفات جديدة تتمثل في برامج الوسائل الإلكترونية كالحاسب الآلي، فتضمن الدستور الجزائري أحكاما متعلقة بالملكية الفكرية، خاصة في المادة 44 منه التي تنص على أن حرية الإبداع الفكري والفني والعلمي مضمونة للمواطن، وحقوق المؤلف يحميها القانون.

إنطلاقا من أن قواعد البيانات هي مجموعة الملفات التي تحتوي معلومات للمعالجة، فإن مصنفات قواعد البيانات لا تعدو أن تكون برامج حاسوب معدة خصيصا لهذا الغرض باعتبارها تأخذ شكل هيكلة وتصميم داخليين مرتبطين بالجهاز الإلكتروني الذي يقوم بتشغيلها –من حاسوب أو غيره– وهي على هذه الصورة غير قابلة للتعامل معها من طرف الإنسان إلا بواسطة البرمجيات المعدة خصيصا لها.

واستدراكا للنقص الموجود في الأمر رقم 97-10، أصدر المشرع الجزائري الأمر رقم 03-05[1] المتعلق بحقوق المؤلف والحقوق المجاورة، الذي لم ينص صراحة على اعتبار برامج الوسائل الإلكترونية من بين المصنفات المحمية، إلا أن هذا لا يمنع من استخلاص اتجاهه إلى ذلك بصورة ضمنية[2]، كما استبعد صراحة برامج الحاسب الآلي من نطاق الاختراعات بموجب المادة 07 من الأمر رقم 03-07 المتعلق ببراءة الاختراع واتجه إلى حمايتها وفق قانون حق المؤلف بموجب المادة 04 من الأمر رقم 03-05[3] أين أقر الحماية القانونية للمصنفات الفكرية التي من بينها برامج الحاسب الآلي، وفي مجال حماية المصنفات لا يمكن أن تنصب هذه الحماية على شيء مستقبلي أو على مجرد أفكار، بل لا بد أن يفرغ المصنف في صورة مادية يبرز فيها إلى الوجود ويكون معدا للنشر لا أن يكون مظهر التعبير عن الفكرة قد بلغ الغاية من الوضع المستقر، فلا تكون أصول المصنف المكتوب مثلا مجرد مشروع لا يزال قيد التنقيح والتبديل، بل يجب أن تكون هذه الأصول قد أخذت وضعها النهائي وأصبحت معدة للطبع والنشر، ولا يهم بعد ذلك نوع المصنف ولا طريقة التعبير عنه لأن طرق التعبير عن المصنفات تتعدد بحسب نوعها[4] وهو ما أشارت إليه المادة 03 من الأمر رقم 03-05[5]، من هذا المنطلق نجد أن المشرع الجزائري قد فرض الحماية القانونية للمصنفات الأدبية والفنية ومنها برامج الحاسب الآلي التي تفرغ في صورة معينة.

---

[1] أمر رقم 03-05 مؤرخ في 19 جمادى الأولى 1424ﻫ الموافق لـ 19 يوليو 2003م، يتعلق بحقوق المؤلف والحقوق المجاورة، معدل للأمر رقم 97-10، ج.ر، العدد 44، مؤرخة في 2003/07/23.

[2] عبد الهادي بن زيطة، حماية برامج الحاسوب في التشريع الجزائري وفقا لأحكام قانون المؤلف الجديد رقم 03-05، دار الخلدونية للنشر والتوزيع الجزائر، ط1، 2007، ص34.

[3] تنص المادة 04 من الأمر رقم 03-05 على أنه: "تعتبر على الخصوص كمصنفات أدبية أو فنية محمية ما يأتي: المصنفات الأدبية المكتوبة مثل المحاولات الأدبية، والبحوث العلمية والتقنية، والروايات والقصص والقصائد الشعرية وبرامج الحاسوب".

[4] عبد الهادي بن زيطة، المرجع السابق، ص38 و39.

[5] المادة 03 من الأمر رقم 03-05: "تمنح الحماية مهما يكن نوع المصنف ونمط تعبيره ودرجة استحقاقه ووجهته بمجرد إيداع المصنف، سواء كان مثبتا أم لا بأي دعامة تسمح بإبلاغه إلى الجمهور".

البند الثاني: تعريف جريمة التقليد

يمكن تعريف جريمة التقليد[1] بأنها كل اعتداء مباشر أو غير مباشر على حقوق التأليف في مصنفات الغير واجبة الحماية[2] كما عرف فقهاء القانون التقليد بأنه صنع شيء جديد أخف قيمة من الشيء القديم ومشابه له، وذلك بقصد المنفعة الناتجة عن الفرق الحاصل ما بين الشيئين المشار إليهما، وعلى أي حال، فإن ذلك يعني أن كل من يعتدي على حق من حقوق المؤلف الأدبية يعتبر مرتكبا لجريمة التقليد، وجريمة تقليد المصنفات الأدبية والفنية لا تختلف عن غيرها من الجرائم المنصوص عليها في قانون العقوبات والتي تستلزم لتوافرها ركنا ماديا وآخر معنويا.

البند الثالث: أركان جريمة التقليد

أولا: الركن المادي، هو الفعل المادي[3] الخارجي الذي ينص القانون على تجريمه، سواء كان هذا الفعل إيجابيا أم سلبيا وهو ضروري لقيام الجريمة وتنعدم بعدمه، ويترتب على ذلك عدم اعتبار ما يدور في الأذهان من أفكار ورغبات وتطلعات من قبيل الركن المادي طالما لم تتخذ سبيلها إلى الحيز الخارجي بمظهر ملموس، وتطلب الركن المادي شرط لازم في جميع صور الجريمة، فإن كان تاما وترتبت عليه نتيجة كانت الجريمة تامة، وإذا أوقف عند حد أو لم تتحقق النتيجة المقصودة أو في طور المحاولة كانت الجريمة غير تامة[4]، ويتمثل النشاط الإجرامي في جريمة التقليد بقيام الجاني بأحد أفعال النسخ للبرنامج المحمي، وتتحقق النتيجة الإجرامية بمجرد الانتهاء من أي فعل منها، بالإضافة إلى ذلك لا بد من توافر العلاقة السببية بين النشاط الإجرامي وتلك النتيجة الإجرامية[5].

وبالنسبة لمحل الجريمة فإنه يشترط لقيام هذه الأخيرة أن ينصب النشاط الإجرامي للجاني على برامج الإلكترونية أيا كان نوعها؛ تشغيلية، تطبيقية، برامج ألعاب أو غيرها من البرامج، وسواء كانت مهيأة للتداول والبث بالطرق المادية التقليدية المعتادة أو بالطرق المستحدثة، وفي جميع الأحوال لا بد أن تكون مملوكة للغير سواء كان هذا الغير شخصا طبيعيا أو شخصا معنويا.

ويشكل النسخ الفعل الأكثر شيوعا في جريمة التقليد والذي يقوم عليه الركن المادي، والاستنساخ هو إمكانية استغلال الشيء المحمي في شكله الأصلي، أو المعدل بفضل تثبيته المادي على أية دعامة وبكل وسيلة تسمح بعرضه، والحصول على نسخ أو أكثر منه، وعليه فلا يجوز لأي شخص ممارسة هذا الحق إلا بعد الحصول على إذن كتابي من صاحبه، يسمح بموجبه نسخ العدد الذي يراه مناسبا للترويج دون المساس بحقوق صاحبه، فالنسخة الخاصة والشخصية مشروعة، إذ يقتصر الناسخ على عدد محدود من النسخ بحيث لا يشكل ضررا ملموسا بصاحبه، وذلك لاستعماله لأغراض شخصية كالبحث أو الدراسة ويفترض في هذا

---

[1] ديالا عيسى ونسه، حماية حقوق التأليف على شبكة الإنترنت، دراسة مقارنة، المنشورات الحقوقية صادر، 2002، ص140.

[2] Xavier Linant de Bellefonds, Alain Hollande, Droit de l'informatique et de la télématique Delmas, 1990, p102. Claude Colombet, Propriété littéraire et artistique et droits voisins, Dalloz, Paris, 9ème Ed. 1999, p194.

[3] محمود محمود مصطفى، شرح قانون العقوبات، القسم العام، قانون العقوبات ومجال تطبيقه، أسباب الإباحة، الركن المادي للجريمة، الركن المعنوي الأهلية الجنائية، العقوبة، مطبعة جامعة القاهرة، القاهرة، 1983، ص265 وما بعدها.

[4] سمير عالية، شرح قانون العقوبات، المؤسسة الجامعية للدراسات، بيروت، 1998، ص200.

[5] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المرجع السابق، ص08.

الاستعمال انعدام نية الربح، لا يكتسي طابعا تجاريا، أما النسخ التجاري أو غير المشروع هو الذي يتم بدون رخصة صاحبه وعلمه حيث أن استنساخ نسخة واحدة يكفي لتحقيق جنحة التقليد.

ثانيا: الركن المعنوي، لابد من توافر الركن المعنوي لإتمام جريمة التقليد، ويتمثل الركن المعنوي بتوافر القصد الجنائي لدى الفاعل وهو سوء القصد أو الخطأ[1]، هذا وقد أجمع القضاء الفرنسي على أن جريمة التقليد تتطلب أحد الأمرين؛ العمد، أو الإهمال الشديد، ويلحق الإهمال الشديد بصورة عامة بالعمد، وهو ارتكاب التقليد بعلم صاحبه ورضاه، ويفترض سوء النية أو الإهمال الشديد في المقلد بمجرد ارتكاب الفعل المادي للتقليد، أي أن حسن النية لا يفترض لدى المتهم وإنما يقع على المتهم عبء الإثبات فإذا استطاع المتهم إثبات حسن نيته يعفى من المسؤولية الجزائية لانعدام الركن المعنوي، ولكن هذا لا يعني إعفاءه من المسؤولية المدنية أيضا بل يبقى مسؤولا عن الأضرار التي ألحقها بالمؤلف نتيجة لانتهاكه حقوق المؤلف الأدبية والمالية.

وفي المصنفات المشتركة إذا قام الشريك بنشر المصنف دون إذن وموافقة باقي الشركاء، هناك من يرى أنه لا يسأل جنائيا عن جريمة التقليد، ولكنه يسأل مسؤولية مدنية لتجاوزه في استعمال حقه[2]، أما الناشر إذا قام بنشر المصنف بناء على طلب بعض الشركاء في تأليف المصنف دون موافقة البعض الآخر ومعارضتهم، فيسأل مسؤولية جنائية على اعتدائه على حق المؤلفين المعارضين ومسؤولية مدنية أيضا عما أصابهم من أضرار.

الفرع الثاني: قرصنة العناوين الإلكترونية عبر شبكة الإنترنت

ظهر موضوع قرصنة العلامات التجارية عبر شبكة الإنترنت من اندماج المعلوماتية بشبكة الاتصالات الحديثة، وهو العنوان الإلكتروني، وذلك بعد انتقال المعاملات من أرض الواقع إلى شبكة الإنترنت وظهور ما يسمى بالتجارة الإلكترونية، مما أدى إلى مسارعة المشروعات الكبيرة والصغيرة إلى امتلاك موقع على شبكة الإنترنت لعرض منتجاتها وخدماتها.

وإزاء هذه الأهمية التي تمثلها هذه المواقع الإلكترونية، كان لا بد من وجود وسيلة للوصول إليها عبر الفضاء الرحب، وتم الوصول إلى وسيلة جديدة تسمى العنوان الإلكتروني، ولسهولة الوصول إلى المواقع على الشبكة، حرصت المشروعات أن تختار عناوين إلكترونية تحمل اسمها أو علامتها التجارية، حتى تميز الموقع الخاص بها عن المواقع الأخرى التي تمثلها شركة منافسة، وبسبب هذا الدور الجديد أصبح العنوان الإلكتروني هدفا للكثير من الأشخاص والمشروعات التي سارعت إلى تسجيل عناوين إلكترونية دون أن تمتلك أي حق أو مصلحة مشروعة، معتدية بذلك على حقوق شركات أخرى، وقد شكل هذا الواقع الجديد نوعا من القرصنة أو السطو على حقوق الآخرين عبر شبكة الإنترنت.

البند الأول: تعريف القرصنة الإلكترونية

يقصد بالقرصنة الإلكترونية أو السطو الإلكتروني أن يقوم شخص أو مشروع لا يمتلك أي حق على علامة تجارية بتسجيل هذه العلامة في صورة عنوان إلكتروني عبر شبكة الإنترنت، وذلك بقصد الإضرار بمالك هذه العلامة أو بقصد إعادة بيع العنوان

---

[1] محمود محمود مصطفى، شرح قانون العقوبات، القسم العام، المرجع السابق، ص416 وما بعدها.

[2] أبو اليزيد علي المتيت، حقوق المؤلف الأدبية، مكتبة النهضة العربية، القاهرة، 1989، ص156.

الإلكتروني إلى هذا المالك مرة أخرى بثمن مغال فيه، ومن ثم نكون أمام قرصنة إلكترونية سواء كان قصد القرصان من تسجيل العنوان الإلكتروني إعادة بيعه للمالك الأصلي أو لأحد منافسيه[1]، أو القصد منه منع المالك من تسجيل هذا العنوان.

وقد تنبه القضاء في أوروبا والولايات المتحدة الأمريكية منذ العام 1996 إلى خطورة هذه القرصنة، على غراره في الجزائر فأصدر العديد من الأحكام التي تدينها بكل صورها، واستند القضاء في أحكامه إلى العديد من الأسس القانونية، ومن هذه الأسس قواعد قانون العلامات التجارية وأحكامه وقانون حماية الملكية الفكرية، والقواعد التي تضمنتها القوانين الخاصة التي سنت بصورة خاصة لمعالجة هذه الظاهرة، وتزداد القرصنة أو السطو الإلكتروني بالنسبة للعناوين الإلكترونية العامة مثل التي تنتهي ب (com.) أو (net.) أكثر من العناوين الوطنية، فهذه العناوين تعد مجالا خصبا يجذب الأشخاص والمشروعات، مما يساعد على الاعتداء على العلامات التجارية[2].

البند الثاني: ماهية العنوان الإلكتروني

تنقسم العناوين الإلكترونية إلى عناوين إلكترونية دولية أو عامة لا تنتمي إلى دولة معينة، وعناوين إلكترونية وطنية تنتهي بحرفين من حروف كل دولة، ومن أمثلة تلك العناوين الدولية التي تنتهي بالمقطع com.، net.، org.، ومن أمثلة العناوين الوطنية العناوين الإلكترونية الجزائرية dz.، المصريةeg. والفرنسيةfr..

أولا: تعريف العنوان الإلكتروني، اختلفت التعريفات وأثارت جدلا بنظر الفقه أو حكم القضاء وهي على الشكل التالي:

1- **التعريفات التي تستند إلى الطبيعة الفنية للعنوان الإلكتروني**: عرف العنوان الإلكتروني بأنه مجرد تحويل أو نقل مجموعة من الأرقام في صورة حروف تشكل مصطلحا يتماشى واسم المشروع أو المنظمة، والحروف المستخدمة في هذا العنوان هي الحروف اللاتينية دون الفرنسية، واستنادا لذلك عرفه البعض بأنه ترجمة لأرقام تتم عن طريق حروف معينة تسمح بدوران المعلومات عبر شبكة الإنترنت، وقد تم استبدال الحروف اللاتينية لصعوبة التعامل بها بحروف بسيطة، على أن تترجم هذه الحروف إلى أرقام عند وصولها إلى الخادم أو الـ server، فيعرف الموقع المطلوب، ويترتب على ذلك أنه بمجرد كتابة المستهلك أو المستخدم لبعض الحروف التي تشتق من اسم شركة أو منظمة أو جامعة أو من علامتها التجارية، يصل إلى موقعها مباشرة، هذه الوسيلة الجديدة هي العنوان الإلكتروني، وإعمالا لهذه الطريقة يستطيع المستهلك أن يصل إلى موقع شركة Microsoft بكتابة العنوان الإلكتروني www.microsoft.com مجموعة من الأرقام قد لا تعي ذاكرته بعضها.

2- **التعريفات التي تستند إلى تكوين العنوان الإلكتروني**: استند جانب من الفقه في تعريفه للعنوان الإلكتروني إلى مكونات هذا العنوان، ويتألف الموقع عبر الإنترنت من جزأين، جزء ثابت وجزء متغير، ويتمثل الجزء الثابت دائما في المقطع ويشير هذا الجزء إلى برتوكول المستخدم، أما الجزء المتغير فهو الذي يلي هذا الجزء الثابت، وهو الذي يميز المشروع عن غيره من المشروعات

---

[1] Cédric Manara, A propos du caractère des noms de domaine, Droit du Commerce Electronique, Dalloz, n°08, 2000, p02.

[2] Larrffeu J., Protection d'une Marque Renommee Contre le Cyberpritage, Expertises, 1999 p260.

وهو الذي يطلق عليه العنوان الإلكتروني، وينقسم هذا الجزء إلى قسمين، الأول هو العنوان الإلكتروني من الدرجة الأولى (TLD)[1] ويمثله المقطع Com. وOrg. وNet.، والثاني هو العنوان الإلكتروني من الدرجة الثانية (SLD)[2]، ويمثله الحروف الأولى من اسم المشروع أو المنظمة أو حروف كل الاسم.

3- التعريفات التي تنتمي إلى وظيفة العنوان الإلكتروني: قال مؤيدوا هذا الجانب من الفقه أنه بدائل العنوان البريدي المحدد لتعرف شخص بعينه عبر شبكة المعلومات[3]، وقالوا أيضا أن العنوان الإلكتروني ليس سوى وسيلة تمكن مستخدمي الإنترنت من الوصول إلى المواقع عبر الشبكة[4]، فهو مثلا مجرد عنوان يعهد لصاحبه بحق استخدام المصطلح الذي سجله عبر شبكة الإنترنت أو عنوان لموقع معين[5].

المطلب الرابع: جرائم غسيل الأموال والبطاقات المالية المتصلة بالتكنولوجيا الحديثة

تعتبر سلوكيات غسيل الأموال وإساءة استعمال البطاقات المالية بكافة أشكالها جرائما ذات خطورة عظيمة، فهي تبنى على ملفات جرائم ارتكبت أصلا، تحصلت فيها أموال قذرة أو مشبوهة، ثم هي من جانب آخر تدخل هذه المتحصلات المالية في أنشطة إجرامية أخرى، كتمويل الإرهاب والعمليات غير المشروعة، مما أمكن وصف جريمة غسيل الأموال بأنها جريمة تبنى على مخلفات جريمة سابقة أو جرائم سابقة، ثم تقع هي كحلقة لسلسلة الإجرام، إذ تعتبر هذه الجريمة تمويلا أو تمهيدا لجرائم أخرى تبدي خطورة جرمية عظيمة تحتاج لضبط وملاحقة.

دفعت هذه الخطورة مع ما يصاحبها من أضرار طائلة على الاقتصاد وأمن الدولة وعلى الصعيدين المحلي والدولي بالجهود الدولية والوطنية تبعا لذلك نحو سن التشريعات والقوانين والأنظمة والتعليمات الكفيلة بضبط هذه الجرائم وتحديد أصول التحقيق فيها، وملاحقة الجناة ثم أسس وأصول التعامل مع متحصلاتها من أموال غير مشروعة وتشكيل توافق مع طبيعة هذه الجرائم خصوصا بشكلها الإلكتروني.

الفرع الأول: جرائم غسيل الأموال المتصلة بالتكنولوجيا الحديثة

---

[1] يقصد به (Top Level Domaine Name).

[2] يقصد به (Second Level Domain).

[3] محمد حسام محمود لطفي، المشكلات القانونية في مجال المعلوماتية، خواطر وتأملات، مؤتمر تحديات حماية الملكية الفكرية من منظور عربي ودولي، تحت رعاية الجمعية المصرية لحماية الملكية الصناعية، والجمعية الدولية لحماية الملكية الصناعية، القاهرة، 21-23 أكتوبر 1997.

[4] Cecelia Bucki, Le Conflit entre Marque et Nom de Domaine, Revue du droit de la propriété intellectuelle, de l'information et de la concurrence, Genève, 2000, p09.

[5] Francis Baillet, Internet: le droit du cybercommerce: le guide pratique et juridique. Ed. Strategies, Connecticut, United States, 2001, p26.

والبعض قال بحرية مستخدم الإنترنت في اختيار اسمه الإلكتروني، إذ يجوز له أن يستخدم اسمه الحقيقي، كما يجوز له أن يستخدم اسما مستعارا، إلا أن هذه الحرية تقف عند عدم المساس بحق الغير في اسمه، فالاسم هو حق لصيق بشخصية صاحبه وهو حق يكفل القانون حمايته من الاعتداء. صابر عبد العزيز سلامة، العقد الإلكتروني، دار النهضة العربية، القاهرة، ط2، 2007، ص46.

سهلت التكنولوجيا الحديثة من عمليات تزييف العملات وغسيل الأموال الناتجة عن الأنشطة الجرمية[1]، وهي جرائم غالبا ما تحدث في دول أخرى غير الدول التي تم جمعها فيها، وجرائم غسيل الأموال عبارة عن الجرائم التي يتم من خلالها إضفاء الشرعية على الأموال التي تم جمعها من خلال الأنشطة الجرمية الخفية والعمليات المشبوهة لتبدو في صورة استثمارات تجارية مشروعة، فيتم فصل تلك الأموال عن مصدرها الحقيقي المتسخ حتى يتم إعادة استخدامها بحرية وبمعزل عن الخوف من الملاحقة القانونية لاحقا[2].

تعد ظاهرة غسيل الأموال ظاهرة عالمية إنطلقت منذ بداية ثمانينات القرن العشرين في البلدان الغربية، ثم انتشرت في مختلف بلدان العالم التي يمكن للمجرم فيها أن يخفي آثار الأموال القذرة ذات المصدر غير المشروع، ما يشكل عرقلة لعمليات التنمية الاقتصادية والاجتماعية والثقافية، بالإضافة إلى تعرض حقوق وحريات الإنسان وكذا السلم والاستقرار الدوليين إلى الخطر[3]،وقد يتم ذلك عن طريق إيداع تلك الأموال في المصارف أو شراء العقارات أو المقتنيات باهظة الثمن أو غير ذلك من الأنشطة التجارية المعروفة بعيدا عن مصدر الحصول عليها زيادة في التمويه، واستغلالا للنقص في التنسيق بين الدول وأجهزة الملاحقة المختلفة[4].

وتعتبر التكنولوجيا الحديثة سواء منها ما يتعلق بالمصارف وعملياتها المالية أو ما يتعلق بوسائل الاتصال السريعة أو غير ذلك، من أكثر الوسائل المساعدة على تسهيل ارتكاب مثل ذلك النوع من الإجرام[5]، وتتضمن عمليات غسل الأموال عدة مراحل تبدأ أولا بمرحلة التوظيف، وهي المرحلة التي يقصد بها توظيف الأموال الملوثة أو الناتجة من مصدر غير مشروع في الاقتصاد الرسمي دون النظر إلى تحقيق الأرباح، وذلك بهدف إظهار تلك الأموال على أنها متحصلة من أنشطة اقتصادية مشروعة تمهيدا لاستثمارها أو إيداعها بالمؤسسات المالية، ونقلها أو تداولها من خلال تلك المؤسسات[6]، ثم تنتقل ثانية إلى مرحلة التغطية التي يقصد بها إجراء عمليات مصرفية عديدة ومعقدة على الودائع بهدف الفصل بين الأموال ومصدرها الجديد المصطنع، ويتم تدعيم تلك العمليات المصرفية بالمستندات المثبتة لها[7]، وغالبا ما تتم عمليات التغطية في أماكن متعددة بعيدة عن الأماكن الأصلية التي تولدت فيها الأموال

---

[1] وتجدر الإشارة إلى أن تعبير غسيل الأموال ظهر لأول مرة في الولايات المتحدة الأميركية في القرن العشرين، عندما اشترى أحد رجال الأعمال من التابعين لعصابات المافيا مغسلة عامة، وجعل جميع تعاملاتها من خلال القطع النقدية الصغيرة، بحيث يضاف في نهاية اليوم الواحد إلى أرباحها جزء من أموال تجارة المخدرات التي تقوم بها المافيا بالأموال النقدية من الفئات الكبيرة حتى لا يرتاب أحد في أمر المبالغ المالية الكبيرة التي كان يجمعها.

[2] محمد محمد عنب، المرجع السابق، ص63.

[3] محمد حافظ الرهوان، عمليات غسل الأموال، مفهومها وخطورتها واستراتيجية مكافحتها، مجلة الأمن والقانون، العدد 02، السنة 10، أكاديمية الشرطة دبي، يوليو 2002، ص127.

[4] عبد الله الصعيدي، دراسة في حجم الاقتصاد الخفي، مجلة الفكر الشرطي، المجلد 09، العدد 01، شرطة الشارقة، دولة الإمارات العربية المتحدة ص203 وما يليها.

[5] محمد عبد اللطيف فرج، تجريم عمليات غسيل الأموال في مصر والأنظمة المقارنة، مجلة مركز بحوث الشرطة، العدد 13، القاهرة، يناير 1998 ص243.

[6] حمدي عبد العظيم، غسيل الأموال في مصر وفي العالم، الجريمة البيضاء، أبعادها، آثارها وكيفية معالجتها، الدار الجامعية، الإسكندرية، ط3، 2007 ص41.

[7] صفوت عبد السلام عوض الله، الآثار الاقتصادية لعمليات غسيل الأموال ودور البنوك في مكافحة هذه العمليات، مجلة كلية التدريب والتنمية، العدد 02، كانون الثاني 2000، ص192.

غير المشروعة وبهذا يضمن مرتكبوا جريمة غسل الأموال الملوثة بقاء تلك الأموال في أمان لصعوبة تتبعها من قبل الجهات الأمنية والرقابة المختصة[1].

ويلي ذلك كله مرحلة الاندماج والتي يتم فيها إعادة ضخ الأموال التي تم غسلها مرة أخرى في الاقتصاد كأموال عادية مشروعة مستمدة من المصدر المصطنع الذي تم خلقه في مرحلة التغطية، وبهذه الطريقة يصعب الفصل بين تلك الأموال والأموال المشروعة، فيختلط النوعان، وتندمج الأموال الملوثة في الاقتصاد الرسمي للدولة، كأنها متحصلة من نشاط اقتصادي مشروع[2] وصولا إلى مرحلة إعادة التوطين، أين يتم في هذه الأخيرة إعادة الأموال التي تم غسلها إلى بلد المصدر الأصلي الذي تم الحصول عليها فيه بشكل يجعلها تبدو وكأنها اكتسبت بطريقة مشروعة فيصعب على أجهزة الرقابة والأمن والتحقيق اكتشاف حقيقتها[3]، لاسيما باستخدام الوسائل التكنولوجية الحديثة، ومنها التحويلات البرقية والبنوك الخاصة ومؤسسات التحويل الفوري للأموال وسوق المزادات العلنية[4].

وتعتبر بطاقات الائتمان من أفضل السبل المعتمدة لدى مجرمي غسل الأموال وأنسبها لمساعدتهم على تنفيذ عمليتي التغطية والاندماج، فيتم ضخ الأموال في الأنظمة المصرفية في العالم[5].

ويؤكد بعضهم على أن عمليات غسل الأموال كانت السبب في نشوء وانتشار جرائم خطيرة مستحدثة مثل تزوير البطاقات الائتمانية، والتحويل الإلكتروني غير المشروع للنقود[6]، في حين يؤكد بعض آخر على أن تزوير بطاقات الائتمان يعتبر فرصة ذهبية لغاسلي الأموال وتجار المخدرات والأعضاء البشرية والدعارة وبيع الأطفال[7]، ومن ذلك ما حدث في الولايات المتحدة الأميركية عندما استطاع مجرمي غسل الأموال من تركيب وتكوين ماكينة للصرف الآلي مصطنعة، استطاعوا عن طريقها أن يكتشفوا ويعرفوا الأرقام السرية للعملاء المستخدمين لتلك الماكينة، ثم قاموا بتزوير بطاقات مماثلة من حيث الخصائص لبطاقات هؤلاء العملاء واستخدامها في عمليات السحب والإيداع عن طريق ماكينات الصرف الحقيقية، فتم من خلال ذلك غسل العديد من الأموال القذرة بهذه الطريقة، إلى أن تم اكتشاف تلك العملية بعد ذلك[8].

كما أمسى مجرمو غسل الأموال يستخدمون الشبكة الدولية للمعلومات عن طريق المقامرة والنشاطات المصرفية، سواء منها المقترنة بعمليات المقامرة أو المستقلة بذاتها لما توفره تلك النشاطات للمجرم من تحويل سريع للنقود بالمقارنة مع الاستخدام التقليدي للنقود الورقية[9]، لاسيما مع وجود ما يسمى بتقنية الموندكس (Mondex) التي يمكن معها تشفير عمليات تحويل الأموال

---

[1] صفوت عبد السلام عوض الله، المرجع السابق، ص63.

[2] خالد حمد محمد الحمادي، غسل الأموال في ضوء الإجرام المنظم، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة، 2002، ص100.

[3] صفوت عبد السلام عوض الله، المرجع السابق، ص63.

[4] محمد عبد اللطيف فرج، المرجع السابق، ص249.

[5] صفوت عبد السلام عوض الله، المرجع السابق، ص63.

[6] محمد حافظ الرهوان، المرجع السابق، ص144.

[7] حمدي عبد العظيم، المرجع السابق، ص96.

[8] هدى حامد قشقوش، جريمة غسيل الأموال في نطاق التعاون الدولي، دار النهضة العربية، القاهرة، 2001، ص58.

[9] عبد الفتاح بيومي حجازي، جرائم غسل الأموال بين الوسائط الإلكترونية ونصوص التشريع، دار الفكر الجامعي، الإسكندرية، 2005، ص18.

عبر الإنترنت عبر جهاز المودم (Modem) أو عبر أحد مواقع الإنترنت، بحيث تصعب معرفة أي تتبع لمضمون العملية بل يستحيل ذلك[1].

البند الأول: الركن المادي في جرائم غسيل الأموال المتصلة بالتكنولوجيا الحديثة

بالنظر إلى المفهوم الذي اختاره المشرع للسلوك الجرمي في جرائم غسيل الأموال نلاحظ أنه حصر السلوك بصورته الإيجابية فلا تقع جريمة غسيل الأموال بسلوك سلبي، أي أن محل السلوك دائما ما يكون مالا متحصلا من جريمة، وأن محل السلوك إما اكتساب مستقل للمال أو تصرف بهذا المال غير المشروع، كما نلاحظ أن السلوك قد يكون منصبا على المال كحفظ المال أو إيداعه أو استبداله، أو يكون منصبا على مصدره ومثال ذلك إخفاء أو تمويه مصدر ذلك المال.

ولفهم الطبيعة الخاصة لجرائم غسيل الأموال وللسلوك الجرمي المشكّل للركن المادي فيها، نبين تاليا المراحل التي يمر بها السلوك الجرمي، وصولا إلى ظهور جريمة غسيل الأموال حيز الواقع، واستحقاق فاعليها العقاب، إذ يمر السلوك الجرمي في جرائم غسيل الأموال بمراحل أساسية ثلاثة هي سلوك الادخال، سلوك التغطية وسلوك الدمج، وتظهر تفاصيل الركن المادي لجرائم غسيل الأموال من خلال هذه المراحل الثلاث، ففي البداية يلجأ الجاني إلى مرحلة الإدخال وهي عملية تحريك المتحصلات من جريمة ما من مكان إلى آخر لنفي الشبهة عن مصدر هذا المال، هذا التحريك يأخذ أشكالا وطرقا مختلفة، منها الطرق التقليدية الاعتيادية التي تتمثل بوضع النقود أو الأصول المادية الأخرى ضمن حقائب وعبور الحدود بها، وقد أفرد القانون عقوبات معينة لكل من يخالف هذا الالتزام، فأعطى لدائرة الجمارك صلاحيات حجز الأموال، أو التحفظ عليها عند كل شك أو شبهة بها، أو تقديم بيانات مغلوطة أو غير صحيحة لها.

في المقابل قد يلجأ الجاني بغية تحريك المال إلى أعمال التهريب سواء داخل الدولة أو لخارجها، وقد يلجأ إلى طرق أخرى لتحريك المال المتحصل من جريمته وذلك باستخدام طرق إلكترونية أكثر تعقيدا، إذ لم تعد الطرق التقليدية لنقل وتحويل الأموال عبر الدول مطروحة، نظرا لعظم المخاطر على الطريق ولتشديد الدول في واجبات الإفصاح والتفريغ، فكان أن تحول الجناة إلى طرق أكثر أمنا بنظرهم، لتحويل الأموال ونقلها عبر الدول، ولا أكثر ملاءمة لذلك من الطرق الإلكترونية التي تأخذ من التحويلات البنكية والإيداع في المؤسسات المالية شكلا مختلفا لها، كما قد يلجأ الجناة إلى التعامل مع شركات الصرافة لنقل الأموال بكميات ضخمة من بلد إلى آخر، سواء بعلم ذلك الصيرفي أو دونه، وقد يلجأ الجناة أيضا إلى شراء الأصول وإعادة شحنها، ثم تسليمها، لتحقيق النقل الآمن للمال، بالإضافة إلى وضع النقد ضمن أدوات أخرى قابلة للتداول، ثم إعادتها إلى شكلها النقدي عند وصولها بلد المقصد، فإذا تمت عملية التحويل أو النقل، انتقل الجناة إلى المرحلة الثانية من مراحل السلوك الإجرامي في جرائم غسيل الأموال الأكثر تعقيدا وهي مرحلة التغطية.

---

[1] ويؤكد الخبراء أنه يمكن للمصارف الصغيرة من خلال استخدام تقنية المونداكس (Mondex) أن تستفيد من التراخيص التي تمنحها إياها المصارف الكبيرة بإصدار بطاقات الائتمان لكي تسهل عمليات تحويل المبالغ المالية من بطاقة إلى أخرى باستخدام الهاتف. عبد الفتاح بيومي حجازي، جرائم غسل الأموال بين الوسائط الإلكترونية ونصوص التشريع، المرجع السابق، ص39.

أما مرحلة التغطية فهي جوهر السلوك الجرمي ومحوره، وتهدف إلى إيجاد غطاء قانوني للمال، وإلى إخفاء مصدره الحقيقي غير المشروع بإيجاد مصدر قانوني، وهي تقوم على فصل العوائد النقدية والمتحصلات عن أصولها، وذلك باستخدام طرق ومعادلات وأدوات مالية معقدة تجعل من أمر التدقيق والكشف في المستقبل أمرا صعبا، إن لم يكن مستحيلا، ومن ذلك، مزج النقد بنقد آخر ذي أصول قانونية سليمة، أو تعمد إنشاء الشركات على اختلاف الغايات لاستعمالها كطرق وهمية كافية لتغطية مصادر النقد المتحصل من موضوع جريمة غسيل الأموال، وإظهاره على أنه عائد من طرق قانونية شرعية.

فإذا نجت مرحلة التغطية واستطاع الجناة إيجاد قالب قانوني وهمي أحيانا وشرعي أحيانا أخرى انتقلت العملية إلى مرحلتها الأخيرة وهي مرحلة الدمج، أين يبدأ الجناة باصطناع الأصول، وخلق المبررات والأسباب للإجابة على السؤال الذي يطرحه المحققون وهو من أين جاءتك هذه الأموال كلها؟ وهم إذ يقصدون ذلك، تراهم يضخمون المدفوعات ويقللون المدخلات، ويوجدون منافذ دخل وهمية، تبرر وجود المال بين أيديهم، وهم يستثمرون دخلا وهميا بقطاعات ذات مداخيل كثيرة، كأسواق المال والأسهم، وقطاع العقارات وتطويرها، فإذا تمت هذه المراحل كان للجناة بعدها أن يوفروا المصدر الشرعي الوهمي لكم هائل من الأموال المحصلة لديهم محل جريمة غسيل الأموال، وكان هذا الجزء من المال ذا صيغة قانونية كافية ومنطقية وذا سبب مشروع يصعب تبيان زيفه.

وضمن هذا الإطار، يمكن لنا أن نستوعب صور الركن المادي في جرائم غسيل الأموال، التي يصعب حصرها، فاكتساب الأموال هو المرحلة الأولى في الجريمة القائمة على ارتكاب جريمة تنتج عنها متحصلات، سواء كانت نقدية أم عينية أو حتى حق له قيمة مادية في التعامل، ثم لدينا الحيازة والتصرف والنقل والإدارة والحفظ والاستبدال والإيداع والاستثمار لهذه المتحصلات، وهي عناصر المرحلة الثالثة المعروفة بمرحلة الدمج، ولا يخرج سلوك التمويه والإخفاء لطبيعة ومصدر المتحصلات وحقيقتها ومكانها عن كونه إحدى تصرفات وسلوكيات المرحلة الثانية لغسيل الأموال المعروفة باسم التغطية.

على أن يدخل النقل والتلاعب في الحركة أو التحويل ضمن المرحلة الأولى وهي مرحلة التحويل، ومع ذلك فإن كلا من هذه التصرفات يشكل صورة من صور الركن المادي لجريمة غسيل الأموال يستحق فاعله العقاب، وعليه فإن كل تصرف ذو أثر يدخل ضمن أي مرحلة من مراحل العملية الهادفة إلى غسيل الأموال يستوجب العقاب باعتباره عملية غسيل الأموال.

البند الثاني: الركن المعنوي في جرائم غسيل الأموال المتصلة بالتكنولوجيا الحديثة

يقوم الركن المعنوي في جرائم غسيل الأموال على القصد العام المبني على عنصري العلم والإرادة، العلم بالسلوك الجرمي المعاقب عليه هو علم مفترض بطبيعته مبني على وجود القاعدة التجريمية، إذ لا يعذر أحد بجهله بالقانون، ثم إرادة ارتكاب ذلك السلوك بصفته تلك، رغم العلم بأنه مجرم.

الفرع الثاني: جرائم البطاقات المالية المتصلة بالتكنولوجيا الحديثة

صاحب ثورة تقنية نظم المعلومات الابتعاد تدريجيا عن استخدام النقود التقليدية والاتجاه أكثر نحو استخدام المال المعلوماتي في انجاز الأعمال والمعاملات التجارية، حيث ظهر ما يسمى بالنقد الإلكتروني، وعليه توسع استخدام البطاقات المالية كبطاقات الائتمان، بطاقات الصراف الآلي، أو البطاقات الذكية بمختلف صورها وحسب مجال تخصصها، وعلى الرغم من المزايا التقنية والأمنية

العالية التي تحققها هذه البطاقات، إلا أن جانب الشر لدى البعض عمل على اختراقها وإساءة استخدامها، حيث تم الاعتداء عليها بصورة ألحقت الضرر بالآخرين وفوتت الغاية من هذا الابتكار.

البند الأول: الطبيعة القانونية للبطاقات المالية

تتعدد العلاقات القانونية في مجال استخدام البطاقات المالية، فنجد أن البطاقات الائتمانية هي الصورة الأكثر انتشارا وتداولا من بين البطاقات المالية عموما، من ذلك؛ فإن البحث هنا سيتناول البطاقات الائتمانية على وجه الخصوص مع التطرق إلى النماذج الأخرى من البطاقات المالية عند اللزوم، وفي ذلك نجد أن التعامل بالبطاقات الائتمانية يوجب وجود مجموعة من العلاقات القانونية تتمثل بوجود علاقة بين مصدر البطاقة وحاملها[1]، وعلاقة بين مصدر البطاقة والتاجر[2]، وعلاقة أخرى بين التاجر وحامل البطاقة[3]، من هنا نجد أن بطاقات الائتمان تتميز بخصوصية قانونية من حيث تحديد الطبيعة القانونية التي تلعب دورا كبيرا وفعالا في تحديد الوصف القانوني للأعمال التي تمثل إساءة في استخدام هذه البطاقات.

---

[1] تقوم مجموعة من الالتزامات القانونية بين مصدر البطاقة وحاملها، ومن أهم التزامات مصدر البطاقة؛ تسليم البطاقة إلى المنتفع بها والتزامه بدفع ديون العميل الناشئة عن استخدام البطاقة والإفصاح عن المحاذير المترتبة عن البطاقة وكشف حساب العميل، بالمقابل يلتزم العميل بتقديم البيانات المطلوبة بشكل صحيح ودفع رسوم استخراج البطاقة والوفاء بقيمة المشتريات للبنك والمحافظة على البطاقة، ولذلك يرى اتجاه من الفقه أن طبيعة العلاقة بين حامل البطاقة والبنك هي علاقة فرض لكون العميل يقوم بشراء احتياجاته ويقوم البنك بالوفاء على أن يتولى العميل السداد في مرحلة لاحقة، وفي ذلك أنظر ثناء أحمد محمد المغربي، الوجهة القانونية لبطاقات الائتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2003. ويرى جانب من الفقه أن هذه العلاقة لا تعد أن تكون حوالة دين ومن هذا الاتجاه الصديق محمد الأمين الضرير، بطاقة الائتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2003. إلا أن أي من هذه الاتجاهات لم يخل من النقد، ذلك أن فكرة القرض تقوم على العلاقة الثنائية بين المقرض والمقترض مع تحديد قيمة القرض ونسبة الفائدة إليه وعليه السداد، بالإضافة إلى أن الائتمان أوسع مدلولا من القرض وأن العلاقة بين المقرض والمقترض تنتهي بانتهاء القرض مع المقترض وتحتاج إلى اتفاق جديد لقرض جديد وهو ما ينطبق على استخدام بطاقة الائتمان، وفي ذلك نتفق مع الدكتور عصام حنفي موسى الذي يعتبره عقد فتح حساب يتعهد بموجبه مصدر البطاقة بأن يضع تحت تصرف حامل البطاقة أدوات ائتمان بحدود مبلغ معين لمدة معينة أو غير معينة لقاء عمولة يدفعها الطرف الآخر، وبالتالي يتضمن مثل هذا العقد وعدا بالقرض يتمتع بموجبه العميل بمهلة للوفاء، مع المحافظة على خصوصية استخدام هذه البطاقة المتمثلة بالتزام مصدر البطاقة بالوفاء بقيمة المشتريات مع تزويد العميل بأدوات الائتمان مع غياب نية المضاربة عن هذه المعاملة.

[2] تفرض البطاقة الائتمانية التزامات متبادلة بين مصدر البطاقة والتاجر، يلتزم من خلالها مصدر البطاقة بإصدارها وتزويد التاجر بأدوات استخدامها والتزامه بالوفاء للتاجر وحماية البطاقة من التزوير، ومقابل ذلك يلتزم التاجر بقبول البطاقة مع عملية البيع والشراء والتحقق من صلاحية البطاقة وسلامتها ووضع العمولة لمصدر البطاقة، ومثل هذه العلاقة التبادلية كيفها البعض بأنها كفالة (ومن هذا الاتجاه الدكتور وسعد محمد سعد، المسائل القانونية التي تثيرها العلاقة الناشئة عن استخدام بطاقة الائتمان بين الجهة مصدرة البطاقة والتاجر، مجلة مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2003، مدللا على رأيه بأن مصدر البطاقة ملتزم بذاته بدفع قيمة المشتريات مما يخلق التزاما بمواجهة التاجر وكذلك اقتطاع مصدر البطاقة نسبة من قيمة المشتريات)، في حين يرى اتجاه آخر أن هذه الوكالة هي وكالة بالعمولة بحيث تقوم الجهة مصدرة البطاقة بتحصيل حقوق التاجر لقاء عمولة معينة، وفي هذا الاتجاه نتفق مع ما ذهبت إليه الباحثة فداء الحمود باعتبار أن التزام الجهة المصدرة بمواجهة التاجر هو من قبيل التعهد الشخصي غير القابل للرجوع فيه من قبل الجهة المصدرة وهذا التعهد لا علاقة له بوضع الحامل وملاءمته المالية، ذلك أنه التزام مستقل حلقي على عاتق الجهة المصدرة في مواجهة التاجر.

[3] أما عن العلاقة القانونية التي تربط التاجر بحامل البطاقة فهي علاقة تفرض التزاما على حامل البطاقة وتواجه التوقيع على فواتير الشراء وأن يستخدم البطاقة بشكل أصولي مقابل التزام التاجر ببيع السلع بسعرها النقدي وتسليم البضاعة، وبصرف النظر عن آلية دفع ثمن المشتريات فإن العقد الذي يربط=

وفي إطار البحث عن الطبيعة القانونية لهذه البطاقة نجد أنها تقوم على عملية مصرفية ذات طبيعة خاصة[1] تخرج عن الأنظمة التقليدية، وذلك لحداثة هذا النظام وطبيعة الروابط القانونية التي تتم بين أطراف البطاقة (التاجر وحامل البطاقة، مصدر البطاقة والتاجر، وحامل البطاقة ومصدرها)، والتي تحقق الغاية القانونية والفنية من استخدامها المتمثل بتمكين حامل البطاقة من الحصول على السلع والمشتريات لقاء مهلة للوفاء تدفع إلى شخص ثالث هو مصدر البطاقة، والذي يتولى بدوره دفع الثمن معجلا للبائع لقاء عمولة يحصل عليها من التاجر وحامل البطاقة.

ومن ذلك نجد أن العلاقة القانونية التي تحكم أطراف هذه العلاقة تقوم على منح حامل البطاقة مهلة للوفاء، وبذلك تكون هذه البطاقة أداة ائتمان، وبذات الوقت نجد أن التاجر يحصل ثمن بضاعته مباشرة بصورة غير نقدية، مما يجعل هذه البطاقة أداة وفاء وكذلك نجد أن هذه البطاقة والتي تحوي مجموعة من البيانات المخزنة تقنيا يتعذر قراءتها بشكل مباشر، وإنما تقرأ باستخدام أدوات خاصة إلكترونية مربوطة بطرفيات وحواسيب، تعمل على قراءة المادة المخزنة على الشريط الممغنط الملصق على البطاقة، والذي يحوي البيانات الخاصة بحامل البطاقة ورقم الحساب وغيرها من البيانات البنكية والفنية والتي تمكن التاجر وحاملها من إبرام عقود البيع وسائر العقود الأخرى بموجبها.

وبعيدا عن الخلافات الفقهية نرى أن أغلب الفقه يتجه إلى نظرية اشتراط مصلحة الغير في تحديد الطبيعة القانونية لهذه البطاقات[2]، والتي تقوم على علاقة ثلاثية يتولى أحد المتعاقدين (المشترط) إبرام عقد مع الطرف الثاني (المتعهد) لتحقيق مصلحة لطرف ثالث (المستفيد) مع توفر مصلحة للطرف الأول، وعليه فإن استخدام بطاقة الائتمان في ظل وجود هذه النظرية يعطي حامل البطاقة (المستفيد) الحق بشراء احتياجاته من السلع والخدمات، وأن يتولى الدفع من خلال البطاقة ويفرض على التاجر (المتعهد) التزام قبول الوفاء بهذه الطريقة، بالمقابل يملك مصدر البطاقة (المشترط) حق مطالبة المتعهد بتنفيذ مضمون العقد المبرم لصالح المستفيد (حامل البطاقة)[3]، ولعل هذا التكييف هو الأكثر توافقا مع الطبيعة القانونية لبطاقات الائتمان.

البند الثاني: إساءة استخدام البطاقات المالية

بعد أن يتم تصميم البطاقة وطرحها للتداول بتسليمها إلى العميل، فإن الاعتداء عليها أو إساءة استخدامها قد يصدر من العميل أو من الغير، الأمر الذي يستوجب بحث صور الاعتداء التي تصدر عن كل منهما، إذ أن إساءة استخدام البطاقة من قبل العميل تأتي بعد أن يتم تسليم البطاقة للعميل بموجب عقد مبرم مع مصدرها يحدد للعميل سقفا معينا للتعامل، وعلى أن يتم استخدامها في فترة الصلاحية المحددة لها.

=حامل البطاقة بالتاجر هو عقد بيع. للمزيد حول التكييف القانوني للعلاقات الناشئة عن استخدام بطاقة الائتمان راجع الحمود فداء يحيى، النظام القانوني لبطاقة الائتمان، دار الثقافة للنشر والتوزيع، عمان، 1999. وموسى عصام حنفي موسى، الطبيعة القانونية لبطاقات الائتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2003. وسعد محمد سعد، المرجع السابق.

[1] كميت طالب البغدادي، الاستخدام غير المشروع لبطاقات الائتمان، دار الثقافة للنشر والتوزيع، عمان، 2009، ص134 وما بعدها.

[2] سعد محمد سعد، المرجع السابق، ص816.

[3] يؤخذ على هذه النظرية أن للمتعهد (التاجر) حق التمسك قبل المنتفع (الحامل) بالدفوع التي تنشأ عن العقد، كون التاجر لا يملك الرجوع على حامل البطاقة لأخذ مستحقاته في حالة عجز البنك عن الوفاء. كميت طالب البغدادي، المرجع السابق، ص130.

فإذا ما خالف العميل هذه الالتزامات فإنه يعد تصرفا غير مشروع يستدعي إقامة المسؤولية القانونية، الأمر الذي يستوجب بحث كل منهما على حدى وذلك على النحو التالي:

أولا: استخدام البطاقة أو السحب عليها على الرغم من عدم وجود رصيد أو عدم كفايته، وفي ذلك نجد أن البطاقات المالية ووفق الغايات المخصصة لها تستخدم لغايات الشراء المباشر، كما يمكن استخدامها أيضا كبطاقة سحب نقدي، وتتصور هذه الحالة عندما يقوم العميل بتقديم البطاقة إلى البائع وهو يعلم أنه قد استنفذ حدود الائتمان الممنوح له، أو أن مجمل مبيعاته تتجاوز حدود هذا السقف، وبحسن نية يقوم التاجر بتسجيل عملية البيع وإعداد فواتير الخصم لتقديمها للجهة الإلكترونية لعمليات الصراف الآلي[1]، وذلك أن هذا الجهاز مربوط بطرفيات توصل العميل بالبنك، يقارن العمليات التي تمت على الرصيد زيادة أو نقصا، وبالتالي يعتبر شراء العميل للبضائع والوفاء بموجب البطاقة عمل مستند للعقد المبرم بين مصدر البطاقة وحاملها، وهذا العقد هو الذي يحدد طبيعة التزام كل منهما والأثر المترتب عن مخالفة كل من المتعاقدين لالتزاماته بالعقد.

وبما أن جريمة السرقة تستوجب انتفاء الجواز الشرعي لمثل هذا التصرف، فإن تجاوز مثل هذا العقد يرتب التزامات عقدية وأي مخالفة لهذا العقد ترتب المسؤولية العقدية، وعليه وبما أن التعامل يتم من خلال الصراف الآلي المبرمج بإجابة طلب العميل وفق ما هو مبرمج بموجبه، الأمر الذي يجعل هذا الجهاز مجردا من الإرادة، وبالتالي ما هو مبرمج بموجبه، وهو ما يجعل هذا الجهاز مجردا من الإرادة، وبالتالي، ينفذ هذا الجهاز الأوامر المقترنة من العميل ومن البنك مالك هذا الجهاز، الأمر الذي يجعل هذا التسليم تسليما إراديا لجزء من موجودات البنك التي وضعت تحت إمرة حامل البطاقة.

ثانيا: استعمال البطاقة بعد إلغائها أو انتهاء مدة صلاحيتها، في العادة تعمل بطاقات الائتمان والبطاقات المالية لمدة محدودة، يستوجب على العميل إبرام عقد تجديد لها إذا ما رغب في الاستمرار باستيفاء المنفعة المتحققة منها، وفي بعض الأحيان ووفق شروط العقد، قد يعمد مصدر البطاقة إلى إنهاء التعامل بها بإلغائها، وعند ذلك فإن استمرار العميل باستخدام هذه البطاقة يكون في الغالب أمرا غير ممكن، كون مصدر البطاقة يوجه أمرا لجهاز الحاسوب بعدم قبول هذه البطاقة لكن من المتصور ولعطل في البرنامج أو لتأخر أحد الموظفين من إصدار أمر للحاسوب بوقف التعامل بها، قد يعمد العميل إلى استخدام البطاقة، الأمر الذي يستوجب ترتيب مسألة قانونية تبحث كلا من الصورتين على حدى.

1- استخدام البطاقة بعد انتهاء مدة صلاحيتها: من المتعارف عليه أن للبطاقات الائتمانية مدة صلاحية معينة غالبا ما تكون سنة واحدة، يستوجب على العميل ردها للبنك بانتهاء تلك السنة لإعادة برمجتها واستخدامها برقم جديد، خاصة إذا ما علمنا أن بعض العقود المتعلقة بمنح العميل ائتمانا ماليا تنص صراحة على وجه البطاقة بشكل بارز بإعادتها عند انتهاء مدتها المحددة وفي حالة امتناع العميل عن رد البطاقة لمصدرها يرى جانب من الفقه أن العميل يكون قد ارتكب جرما جزائيا[2]، في حين يرى اتجاه آخر[3] أن مثل هذا الفعل لا يشكل جرما مدللا على رأيه عدم توفر كافة أركان جريمة إساءة الائتمان التي تستوجب توافر العناصر التالية؛ أن يكون محل الجريمة مالا منقولا، أن يكون المال مملوكا للغير وأن يتم تسليم هذا المال للغير بموجب أحد عقود الأمانة.

---

[1] محمد سامي الشوا، المرجع السابق، ص109.

[2] محمد سامي الشوا، المرجع نفسه، ص114.

[3] عماد علي الخليل، الحماية الجزائية لبطاقات الوفاء، دراسة تحليلية مقارنة، دار وائل، عمان، ط1، 2000، ص105.

ويرى أصحاب هذا الاتجاه أن تسليم البطاقة للغير يكون بموجب عقد بيع بحيث يظهر حائز البطاقة بصفة المالك، مما يرتب انتفاء الركن الثاني والثالث المشار إليهما، وبالتالي لا يمثل كتم البطاقة جريمة يعاقب عليها القانون، وفي ذلك نرى خلاف ما ذهب إليه أصحاب هذا الرأي، فإن كنا نسلم بأن عقد البيع لا يعد من عقود الأمانة، إلا أن تسليم البطاقة للعميل لا يستند إلى عقد البيع، فمجرد دفع رسم البطاقة لا يشكل ثمنا لها وبالتالي لا تقع تحت طائفة البيوع مدعمين رأينا بالحجج التالية؛ لو كان العميل مالكا للبطاقة فإنه لا يحتاج إلى إعادة تجديدها وإنما سيتم إعادة تفعيلها ذاتها تلقائيا، والعميل يملك حق التصرف فيها ببيعها أو رهنها أو هبتها كواحدة من حقوق الملكية، وهو ما لا يتوافر باستخدام البطاقة المالية، وإن إن كان مجرد دفع رسم البطاقة والذي يقل كثيرا عن كلفتها لا يشكل ثمنا لها.

فالغاية الأساسية إذن من منح العميل البطاقة يكون لغايات تسهيل معاملاتها البنكية وكخدمة تشجيعية له، ولذلك نرى توفر كامل أركان وعناصر جريمة إساءة الائتمان[1]، وما يحدث عمليا في الوقت الحاضر هو تطوير للأجهزة بحيث تقوم بسحب البطاقة بعد انتهاء مدة صلاحيتها إذا كرر استخدامها رغم رفضها.

2- استعمال البطاقة بعد أن تم إلغاؤها من قبل البنك: قد يلجأ البنك في بعض الحالات ولإجراءات إحترازية أو أمنية إلى إلغاء البطاقة أو وقف العمل بها وطلب استردادها، ويترتب على مثل هذا القرار قطع العلاقة الائتمانية التي تربط البنك بالعميل وبالتالي إذا ما لجأ العميل إلى استخدام البطاقة رغم ذلك فإنه يكون متصرفا بمال الغير، الأمر الذي دفع البعض للمناداة بملاحقة العميل بجريمة الاحتيال لتوافر أركانها العامة والخاصة والتي قوامها:

- محل الجريمة مالا منقولا أو غير منقول، والذي يمثل المال المودع لدى البنك أو البضاعة التي تم تسليمها من قبل التاجر.

- الركن المادي والذي يشمل مثلا الاحتيال المتمثل بالأساليب الاحتيالية وقوامها الكذب المجرد من قبل العميل بأنه حائز على ائتمان بنكي بموجب البطاقة، واستخدام وسائل خارجية بإبراز البطاقة الصادرة عن أحد البنوك، والتي توهم التاجر بحيازته لائتمان مالي وهذا ما قضت به محكمة النقض الفرنسية وجاء بأحد أحكامها بأن هذا السلوك يعد من قبيل الطرق الاحتيالية التي تهدف إلى الإقناع بوجود دين وهمي من أجل الحصول على مبالغ نقدية من البنك التي يتم الاستيلاء عليها[2]، وذلك أن إبراز البطاقة للتاجر لا تعد بحال من الأحوال لجوء إلى استخدام وسيلة احتيالية، فهو في الواقع العملي حصل على هذه البطاقة بموجب عقد مبرم مع البنك (مصدرها) وإذا ما استغل العميل البطاقة بصورة تخالف العقد فإن ذلك يقيم بمواجهته المسؤولية العقدية.

ثالثا: إساءة استخدام البطاقة من قبل الغير، يمتاز العمل باستخدام البطاقة بالطابع الشخصي بحيث تخول الشخص الذي صدرت باسمه فقط استخدام هذه البطاقة، لكن الواقع العملي شهد صور استخدام مثل هذه البطاقة من قبل الغير، ويخرج عن نطاق هذا البحث الاعتداء على جسم البطاقة كأخذها عنوة من مالكها أو العثور عليها أو كتمها وغير ذلك، ولكون محل هذه الأفعال مالا منقولا (جسم البطاقة) فإن مثل هذه التصرفات تعتبر جرائما يعاقب عليها القانون، سواء بجرم السرقة أو إساءة الائتمان

---

[1] زكي أمين حسونة، جرائم الكمبيوتر الأخرى في مجال التكتيك المعلوماتي، المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25-28 أكتوبر 1993، ص482.

[2] (Tribunal Correctionnel de Paris, Banque, 16 Octobre 1974, 1975, 7344, Obsmurin.) وارد في كتاب محمد سامي الشوا، المرجع السابق ص115. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، المرجع السابق، ص108 وما بعدها.

ولغايات هذه الدراسة فإن البحث يقتصر على الجرائم المرتكبة باستخدام البطاقة، سواء كانت البطاقة المستخدمة مزورة أم مقلدة أم كان استخدام البطاقة من قبل الغير بصورة غير مشروعة.

1- تزوير الغير للبطاقة الائتمانية واستعمالها، تمتاز البطاقة الائتمانية كغيرها من البطاقات النقدية، بتقنية فنية عالية ونظام أمني عالي المستوى يحول دون تزويرها أو تقليدها، إلا أن التطور التقني الذي أنتج البطاقة قابله تطورا مماثلا ومكن الغير من إيجاد بطاقة مطابقة للبطاقة الأصلية، وهو ما يدعي تقليد البطاقة، أو على الأقل إمكانية تسمح بتقليد التوقيع الإلكتروني والرقم السري للبطاقة، وهو ما يدعي بالتزوير، وتزوير البطاقة أو تقليدها يستوجب إدخال البيانات على جهاز الحاسوب، وبما أن المنتج الأخير هو البطاقة سواء مقلدة بكاملها أو مزورة بمحتوياتها فإن مثل هذا التصرف يعتبر تصرفا غير مشروع.

وعن مدى تجريم مثل هذه التصرفات، لا بد من ثبوت تزوير البطاقة ابتداء حتى يتم الحديث عن استعمالها باعتبارها بطاقة مزورة، ولانتفاء جرم التزوير من وجهة نظرنا عن البطاقات الائتمانية فإنه يتعذر الحديث عن جرم استخدامها كمحرر مزور.

2- استعمال البطاقة من قبل الغير بصورة غير مشروعة، إن الطبيعة الخاصة للبطاقة الائتمانية تفرض على حاملها المحافظة عليها والمحافظة على الرقم السري الخاص بها، بصور تمنع الغير من استخدامها لكن الواقع العملي شهد العديد من الحالات التي تعرضت بها البطاقة للسرقة، أو تم فقدان البطاقة وعثر عليها شخص ما وقام باستخدامها إذ أن أيا من الصورتين السابقتين يدل على أن من قام باستخدام البطاقة هو شخص غير مخول باستخدامها، الأمر الذي يقيم المسؤولية القانونية بمواجهته، وهو الأمر الذي يستوجب على هذا القانون تحمل عبء التكييف القانوني لمثل هذا التصرف، وبحدود هذا التصرف نرى أن محل الاعتداء عبارة عن بيانات ومعلومات إلكترونية لا تمثل مالا منقولا، وبما أن محل جريمة السرقة مالا منقولا مملوكا للغير، فإن مجرد الاعتداء والحصول على هذه البيانات لا يشكل بوجهة نظرنا جريمة السرقة لانتفاء محلها.

الباب الثاني: آليات مكافحة جرائم التكنولوجيا الحديثة

نتيجة لثورة تكنولوجيا المعلومات الحديثة، بات متطلبا من الأجهزة الجنائية الإجرائية في ممارستها لحق المجتمع في الذود عن كيانه ضد الإجرام أن تتعامل مع أشكال غير محسوسة[1]، واتضح لنا أن جرائم التكنولوجيا الحديثة ترتكب في فضاء افتراضي مفرغ سواء ارتكبت عبر شبكة الإنترنت أم في داخل نطاق ذات المؤسسة التي يتم الاعتداء عليها، أو ارتكاب الجريمة من خلالها، وتعرضنا فيما سبق إلى المشكلات الموضوعية التي تثيرها هذه الجرائم في تطبيق القواعد التقليدية لقانون العقوبات الذي صيغت جل نصوصه ونظمه الأساسية لتواجه سلوكا ماديا يرتكب في عالم مادي ملموس، وما يميز هذه الجرائم هو أنها ترتكب في مسرح إلكتروني أو مجال مفرغ يختلف كليا عن المسرح التقليدي الذي ترتكب فيه الجريمة التقليدية التي يتم الإستدلال عليها وضبطها وإثباتها بالوسائل التقليدية، فهي إجراءات صيغت لضبط وإثبات جرائم ترتكب في عالم ملموس ماديا يلعب فيه السلوك المادي الدور الأكبر والأهم، وهنا يثور التساؤل حول مدى صلاحية هذه الإجراءات لضبط وإثبات جريمة ارتكبت في عالم افتراضي غير ملموس.

أما إذا ارتكبت الجريمة عبر الشبكة العنكبوتية الدولية (الإنترنت)، تزداد العقبات القانونية صعوبة فلا نكون أمام مشكلات إجرائية تخص ضبط الجريمة وإثباتها فحسب، بل نجد أنفسنا أمام مشكلة أكثر تعقيدا تتمثل في تحديد الاختصاص القضائي المرتبط بتحديد القانون الواجب التطبيق على هذه الجريمة، فقواعد الاختصاص القضائي التقليدية صيغت لكي تحدد الاختصاص المتعلق بجرائم قابلة للتحديد المكاني للجريمة، وهي قواعد ترتكز على مبدأ الإقليمية، وهو ما يرتبط بسيادة الدولة على إقليمها[2].

فلا يكون الخروج عليه بقبول اختصاص قضائي أجنبي إلا في حالات استثنائية يجب النص عليها صراحة، وهنا تثور أمامنا مدى امكانية الاعتماد على هذه القواعد لتحديد الاختصاص القضائي لجريمة ترتكب في مجال تنعدم فيه الحدود الجغرافية، وكثيرا ما يكون مرتكبيها في بلاد مختلفة ومن جنسيات متعددة، وغالبا ما يتعلق السلوك الإجرامي بأكثر من دولة؛ الدولة التي ارتكب فيها السلوك، والدولة التي تم فيها القبض على الجاني وتلك التي حدثت فيها النتيجة الإجرامية وهو ما يتطلب منا التطرق إلى مشكلات ضبط الجريمة وإثباتها، ثم عن مشكلات الاختصاص والأهم من ذلك تحديد المكان في حالة الجرائم المستمرة.

تقتضي مواجهة هذه الظاهرة المستحدثة والمعقدة من الإجرام إذن تحقيق عدة أمور، منها ضرورة إعداد كوادر أمنية وقضائية للبحث والتحقيق والمحاكمة في هذا النوع من الجرائم، كذلك تطوير التشريعات الجنائية الحالية سواء الموضوعية أو الإجرائية بإدخال نصوص التجريم والعقاب والنصوص الإجرائية اللازمة لمواجهة هذا الإجرام المستحدث، فضلا عن ذلك فإن التعاون الدولي في مجال الأمن والتحقيق وتسليم المجرمين وتنفيذ الأحكام يعد ضرورة لا مفر منها.

وعليه تم تقسيم هذا الباب إلى الفصلين التاليين:

الفصل الأول: الأحكام الموضوعية لمكافحة جرائم التكنولوجيا الحديثة

الفصل الثاني: الأحكام الإجرائية لمكافحة جرائم التكنولوجيا الحديثة.

---

[1] Edward M. Wise, Computer Crimes and other Crimes against Information Technology in the United States, Revue Internationale de Droit Pénal, Paris, v.64, 1993, pp645-669.

[2] جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، المرجع السابق، ص115.

الفصل الأول: الأحكام الموضوعية لمكافحة جرائم التكنولوجيا الحديثة

دفعت جرائم التكنولوجيا الحديثة بالكثير من التشريعات إلى التدخل من أجل حماية المصالح المتضررة منها، ومن هنا طفت إلى السطح عدة إشكاليات قانونية حول قدرة النص الجنائي التقليدي على الإحاطة بهذه المفاهيم والسلوكيات، وهو ما خلق عدة صعوبات وتحديات أرقت المشرع وكانت السبب في جدل فقهي واسع، هنا حاولت العديد من التشريعات إنقاذ القانون الجنائي وتحديثه، إلا أن هذا التدخل لم يكن على قدم المساواة، حيث نجد أن بعض التشريعات كانت سباقة في وضع سياسة جنائية موضوعية وإجرائية للحد من هذه الجرائم بينما اكتفت تشريعات أخرى بجانب معين من الحماية ومنها من تخلف عن الركب.

إن وضع نصوص قانونية جنائية لمواجهة جرائم التكنولوجيا الحديثة كان وليد جدل فقهي حول مدى قابلية النصوص الجنائية التقليدية لتشمل على هذا النوع من القيم الجديدة، وحقيقة الأمر أن الاتجاه الفقهي القائل بإمكانية ذلك لم يكتب له النجاح، لأن تبني هذه الأفكار سيؤدي إلى تشويه المبادئ المستقرة التي تقوم عليها تلك الجرائم، الأمر الذي سيؤدي بدوره لا محالة إلى وجود ثغرات قانونية، وهو ما جعل الفكر القانوني يستقر ويقتنع بضرورة وضع نصوص قانونية خاصة بهذه الجرائم.

وبما أنه لا يمكن مواجهة جرائم التكنولوجيا الحديثة[1] بدون توفير حماية كافية للمجال والنطاق الذي تتواجد فيه المعلومات فقد حاول المشرع الجزائري مكافحة الجرائم الماسة بالأنظمة والبرامج المعلوماتية أو كما سماه بأنظمة المعالجة الآلية للمعطيات ومن ثمة حماية المعلومات المتواجدة في هذه الأنظمة.

لقد أصبحت جرائم التكنولوجيا الحديثة أكثر قوة بفضل التقنية الحديثة أو قد تكون محلا للاعتداء وهو الأمر الذي استلزم تدخل المشرع الجزائري من أجل التصدي لمثل هذه الظواهر ومعاقبة مرتكبيها إنطلاقا من مبدأ الشرعية وفقا لأحكام المادة الأولى من قانون العقوبات الجزائري التي تنص على أنه لا جريمة ولا عقوبة أو تدابير أمن بغير قانون، وتبعا لذلك جرم بعض صور جرائم تكنولوجيا المعلومات الحديثة وعاقب مرتكبيها، وتناولها تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات من المواد 394 مكرر إلى المادة 394 مكرر 7 من نفس القانون مسايرة للتطورات التكنولوجية وعدم استفحال وتيرة النمو المتسارع في استخدام النظم المعلوماتية، فضلا عن العولمة والتبعية التكنولوجية، بالإضافة إلى استحداث القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

من خلال هذه التعديلات نجد أن المشرع الجزائري قد ركز على الاعتداءات الماسة بالأنظمة المعلوماتية وأغفل الاعتداءات الماسة بمنتجات الإعلام الآلي والمتمثلة في التزوير المعلوماتي[2]، وعليه تم تقسيم هذا الفصل إلى المبحثين التاليين:

المبحث الأول: آفاق مكافحة جرائم التكنولوجيا الحديثة

المبحث الثاني: دور الأجهزة الأمنية في مكافحة جرائم التكنولوجيا الحديثة

---

[1] أسامة أحمد المناعسة وآخرون، جرائم الحاسب الآلي والإنترنت، دراسة تحليلية مقارنة، المرجع السابق، ص70 وما بعدها. شول بن شهرة، الحماية الجنائية للتجارة الإلكترونية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2011-2012، ص87.

[2] محمود أحمد عبابنة، المرجع السابق، ص12.

المبحث الأول: آفاق مكافحة جرائم التكنولوجيا الحديثة

لا يمكن لأي بلد في هذا العصر أن يعيش معزولا عن التطورات التقنية المتسارعة والآثار الناجمة عنها، وفي ظل الترابط الوثيق بين أجزاء العالم عبر تقنيات المعلومات والاتصالات والتطبيقات، بات من الضروري لكل بلد حماية أفراده ومؤسساته ومقدراته وحضارته من آثار هذا الانفتاح، ومع إدراك الجميع اليوم للفوائد الجمة لتقنية المعلومات، فإن المخاطر الكامنة في تغلغل هذه التقنية تتطلب من المجتمع والدولة جميعا الحيلولة دون حصول تلك المخاطر بشتى أنواعها، ومن أهم ما يجب توفيره في هذا الصدد الأحكام والأنظمة واللوائح المنظمة لسلوك الأفراد والمؤسسات حيال التعامل مع تقنية المعلومات، مهما كان نوع التعامل وأيا كانت مقاصده دون تقييد لحرية المجتمع عن الاستثمار البناء لتلك التقنية.

ولهذا ظهرت الحاجة الملحة لإيقاظ النصوص التقليدية التي أكل عليها الدهر وشرب ولم تعرف ما وصل اليه العالم الآن سواء كان ذلك بتعديل هذه النصوص وإضافة المولود الجديد بين ثنايا القانون الجنائي، أو خلق تشريع عقابي خاص به يحتوي على الجانبين، المبادئ العامة التي تجرم الأفعال والقسم الإجرامي الذي يزيل –فيما لو تم وضعه– هالة الغموض المحيطة بالجانب الإجرائي المحيطة بجرائم التكنولوجيا الحديثة، بالإضافة إلى التعاون بين الدول للسيطرة على هذه الظاهرة الإجرامية، من خلال إبرام الاتفاقيات الخاصة بتسليم المجرمين أو امتداد إجراءات التفتيش إلى دولة أو أكثر بهدف الكشف عن الجريمة، أو عقد المؤتمرات أو اصدار القرارات التي تجرم بموجبها الأفعال الإجرامية التي تقع بواسطة التكنولوجيا الحديثة[1].

إذ دأبت المجتمعات والدول عبر حقب زمنية مختلفة في سن تشريعات وقوانين من أجل مواجهة كل من تسول له نفسه خرق الآداب العامة بأعمال غير مشروعة، ومن ذلك الجرائم المرتكبة عبر الإنترنت أو بواسطتها، فبالرغم من قلتها إلا أنها تعتبر محاولات هامة وملموسة في هذا المجال وتتمثل هذه الجهود على المستوى الدولي في الجهود التي تبذلها مختلف الهيئات والمنظمات العالمية، بالإضافة إلى المنظمات الإقليمية والتي تعتبر كإطار دولي يوازي عالمية هذه الجرائم، وتعتبر الجهود الدولية داعمة للجهود التي تبذلها مختلف الدول في تشريعاتها الداخلية، فهي بمثابة قوانين استرشاديه تأخذ بها الدول التي اتخذت سبيل تطوير قوانين العقوبات كما هناك دول ارتأت أفرادها بقوانين خاصة.

المطلب الأول: الجهود المبذولة على المستوى الخارجي

تشكل جرائم التكنولوجيا الحديثة تهديدا خطيرا لأمن المجتمعات، ويعتبر الفراغ أو القصور التشريعي أحد أهم التحديات الرئيسية في مجال مكافحة هذه الجرائم، إذ أن مبدأ الشرعية الجنائية يفرض عدم جواز التجريم والعقاب دون نص، الأمر الذي يحول دون مجازاة مرتكبي الفعل الضار أو الخطر على أمن المجتمع المعلوماتي، طالما أن المشرع الجنائي لم يقم بسن التشريعات اللازمة لإدخال هذا الفعل ضمن دائرة التجريم والعقاب، وسنركز في هذا المطلب على دراسة أبرز الجهود التشريعية الدولية والإقليمية لحماية سرية المعلومات الإلكترونية ومكافحة الجرائم الماسة بها باعتبارها موضوع هذا البحث.

---

[1] جعفر عبد السلام، دور التنظيم الدولي في مكافحة الجريمة، مؤتمر الوقاية من الجريمة في عصر العولمة، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، دبي، 06-08 مايو 2001، ص12 وما بعدها.

الفرع الأول: الجهود الدولية لمواجهة جرائم التكنولوجيا الحديثة

أدى اكتساب جرائم التكنولوجيا الحديثة الطابع العالمي باعتبارها من الجرائم العابرة للحدود بأعضاء المجتمع الدولي إلى التصدي لها، سواء من خلال أطر الاتفاقية الخاصة بحماية برامج الحاسب الآلي، أم من خلال جهود الأمم المتحدة لمواجهة الإجرام التكنولوجي الحديث، فالبرمجيات هي الكيان المعنوي للوسائل الإلكترونية ومن دونها لا يكون ثمة أي فائدة للمكونات المادية.

إنطلاقا من أهمية البرمجيات، جاءت الدعوة عالمية إلى حماية حقوق هؤلاء المبرمجين بوصفهم مبدعين لعمل فكري، وبالفعل أصبح الحديث عن حماية حقوق الملكية الفكرية منذ سبعينيات القرن الماضي هو الشغل الشاغل لدعاة حماية هذه الحقوق، وهذه الدعوة لن يكون لها أثر ما لم تتعلق بالحماية القانونية على الصعيد الدولي، التي ستؤثر جديا على التشريعات الداخلية للدول، وقد لاقت هذه الدعوة صداها لدى ممثلي الدول في مفاوضات اتفاقيات تحرير التجارة العالمية فضمت أجندة عمل هذه المفاوضات لأول مرة حماية حقوق الملكية الفكرية وعلى الأخص حماية البرامج، وثار الصراع بين الدول الصناعية الكبرى المالكة لتكنولوجيا البرمجيات التي قدمت وعودا بتسهيل نقل هذه التكنولوجيا إلى الدول النامية مقابل ترسيخ مبادئ احترام هذه الحقوق أين انتهت المفاوضات بتوقيع الدول على اتفاقيات تحرير التجارة العالمية التي حوت بين طياتها اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية[1].

البند الأول: دوافع الحماية الدولية

هنالك عدة دوافع أدت إلى حماية البرامج والبيانات نذكر منها ما يلي:

أولا: الدوافع الشخصية، تفضي حماية برامج الحاسب الآلي والأجهزة الإلكترونية الذكية إلى حماية المعلومات المودعة فيها والتي قد يتضمن شيوعها ونشرها تعرضا لأسرار الحياة الخاصة، فلا شك أن هذه البرامج قد تنطوي على معلومات تم جمعها وحفظها فيها، وحماية هذه الأخيرة تحول دون تفاقم أخطار استعمال الوسائل الإلكترونية ضد الحياة الخاصة للمواطن.

ولكون بعض البرامج تقوم على تغيير بعض البيانات التي تم تخزينها، وإحداث غش فيها أو إتلاف برنامج أو التجسس على ما تحتويه برامج أخرى من معلومات أو ما إلى ذلك من وقائع إجرامية؛ فقد قامت دول النظم القانونية الغربية بوجه خاص بإحداث تعديلات تشريعية فيها بغية حماية الحياة الخاصة للأفراد[2]، وذلك اعتبارا من السبعينيات والثمانينيات لمواجهة الأشكال الجديدة للإجرام وتأكيد حماية حقوق الملكية الأدبية التي يتمتع بها الأفراد والحيلولة دون الاعتداء عليها باستغلال التيسيرات التي تقدمها تكنولوجيا المعلومات، خاصة مع تعدد الأساليب التي يستخدمها مجرمو تكنولوجيا المعلومات الحديثة.

ثانيا: الدوافع الفنية، يعد تصميم وتصنيع البرمجيات مجالا خلاقا للمبرمجين يمكنهم الإبداع فيه، ولكن هذا الإبداع قد يكلف الملايين من الدولارات، لذاك يحاول المبرمجون إحاطة البرمجيات بالحماية، فلو لم تتوافر للمبرمج الأطر القانونية والتشريعية التي تكفل له حماية برنامجه فإنه سوف يتوقف عن الإبداع والابتكار، ولتوقفت معه التكنولوجيا وتقنياتها عن التطور.

---

[1] رشا علي الدين أحمد علي تقي الدين، المرجع السابق، ص04.

[2] محمد محمد شتا، المرجع السابق، ص18.

وعلى هذا الأساس، نجد المبرمج يضع العديد من التقنيات التكنولوجية لحماية برنامجه من النسخ والتقليد وغيرها من صور الاعتداءات، إلا أن قراصنة البرمجيات في الآونة الأخيرة أصبحوا على قدر كبير من المعرفة البرمجية، ما جعلهم يتغلبون على الأنظمة الفنية التي يضعها المبرمج لحماية برنامجه، ولم تعد الأساليب التي تتبعها شركات البرمجيات كافية لمحاربة القرصنة.

ومن هنا، ندرك البواعث الفنية التي تدعو إلى حماية البرمجيات التي تتمثل فيما يلي:

– **قصور الوسائل المتاحة:** يمكن للمبرمج وضع رقم كودي معين أو شيفرة لمنع نسخ برنامجه مرة أخرى[1]، ولكن الواقع العملي أثبت أن ذلك لم يمنع قراصنة البرمجيات من نسخه عدة مرات[2]. ورغم أن هذه الطريقة كنوع من طرق الحماية لم تعد فعالة بقدر كاف إلا أنه لا يمكن أن نهملها من حيث التطوير والاهتمام؛ فهي وسيلة وقائية[3].

– **التشجيع على الابتكار:** إن حماية برامج الوسائل الإلكترونية تشجع على الابتكار وولوج عالم تأليف البرامج التي تساعد على تقدم الأمم علميا وتكنولوجيا، ذلك أن المبرمج المبتكر سينال مقابلا عادلا لجهده، فيحيا حياة كريمة، تدفعه إلى الإمعان في التعمق في الابتكار، وإلا فما حاجة أي شخص إلى الابتكار إذا كان مآل عمله إلى الاستغلال المجاني للجمهور[4]، كذلك إن حجم الاستثمارات والميزانيات المنفقة على إنتاج الأموال المعلوماتية المعنوية كبير جدا، ويمس كثيرا من مصالح الشركات والبنوك[5].

– **حماية البرامج تقلل من خطر القرصنة الدولية:** لا شك أن عدم شمول برامج الحاسب الآلي والأجهزة الإلكترونية الذكية بالحماية الجنائية، سيفضي إلى تفاقم مشكلة القرصنة الدولية لهذه البرامج، وارتكاب كافة الجرائم المتصلة بها، لاسيما أن هذه الجرائم تتسم بصعوبة الكشف عنها وصعوبة إثباتها لتميز مرتكبي هذه الجرائم بمهارات ومعارف فنية خاصة[6].

ثالثا: الدوافع الاقتصادية، تعد صناعة برامج الوسائل الإلكترونية الذكية حاليا قوة عظيمة في اقتصاد الدول وستؤثر موضوعات حماية الملكية الفكرية على مستقبل صناعتها، فإذا لم تكن هناك حماية مناسبة متوافرة لحقوق المؤلف، فإن صناعة البرامج قد تتوقف أو على الأقل تخضع لتغيرات كبيرة[7]، وهكذا، فإن حماية البرامج هنا هي حماية لأهداف التنمية الاقتصادية ذاتها[8].

رابعا: التشجيع على الاستثمار، بالنظر إلى ضخامة الاستثمارات المادية والبشرية المستخدمة لإعداد وإنجاز هذه البرامج برزت ضرورة فرض حماية قانونية للبرامج[9]، فكثيرا ما تتعرض الشركات والبنوك لقرصنة برامجها عن طريق عمليات النسخ غير المشروع للبرامج، واستخدامها دون شرائها من مصدرها الأصلي أو من الجهات المخولة ببيعها رسميا.

---

[1] محمد حماد مرهج الهيتي، المرجع السابق، ص154.

[2] رشا علي الدين أحمد علي تقي الدين، المرجع السابق، ص75.

[3] رشا علي الدين أحمد علي تقي الدين، المرجع نفسه، ص76.

[4] محمد محمد شتا، المرجع السابق، ص20.

[5] هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، المرجع السابق، ص70.

[6] محمد محمد شتا، المرجع السابق، ص21 و22.

[7] برنار أ. جالر، الملكية الفكرية وبرامج الحاسبات، حق المؤلف وبراءات الاختراع من وجهات النظر الفنية والقانونية، ترجمة محمد حسام محمود لطفي الجمعية المصرية لنشر المعرفة والثقافة العالمية، مصر، ط1، 1998، ص21.

[8] محمد محمد شتا، المرجع السابق، ص23.

[9] فاروق علي الحفناوي، المرجع السابق، ص108.

خامسا: الدوافع القانونية لحماية البرمجيات: بسبب إعراض معظم دول العالم –وخاصة في عالمنا العربي–، عن سن القوانين المضادة لقرصنة البرمجيات عجزت النصوص التشريعية التقليدية عن وضع حماية فعالة لها، وذلك برغم أن لعمليات القرصنة وجها سلبيا وهو أنها تحول دون ترويج المبرمجين العرب لمنتجاتهم محليا لكونها ستدخل في سوق القرصنة مباشرة دون أن تعود عليهم ولو بجزء يسير من الجهود والأموال والوقت التي بذلت خلال عمليات الإنتاج[1]، فتوفير حماية قانونية يؤدي إلى تشريع صناعة البرامج وفسح المجال الرحب للمنافسة المشروعة من جهة، ومن جهة أخرى، غلق الأبواب المفتوحة أمام القرصنة الدولية في هذا المجال[2].

البند الثاني: أهم الاتفاقيات الدولية للتصدي لجرائم التكنولوجيا الحديثة

تعد البرمجيات مجالا مهما من مجالات حماية الملكية الفكرية التي اهتم النظام العالمي الجديد بحمايتها، وظهرت معها الحاجة الملحة إلى حماية البرامج وإيجاد نظام قانوني متكامل لحمايتها على الصعيد الدولي[3].

أولا: اتفاقية برن لحماية المصنفات الأدبية والفنية، بدأ الإطار التشريعي الحديث لقوانين الملكية الفكرية بصفة عامة في القرن التاسع عشر عندما اشتدت الحركة الدولية التي تطالب بحماية حقوق الملكية الفكرية ما تمخض عنه عقد معاهدة برن[4] بسويسرا في 09 سبتمبر 1886 والمكملة بباريس في 04 ماي 1896[5].

وبموجب المرسوم الرئاسي رقم 97-341[6] انضمت الجزائر بتحفظ إلى اتفاقية برن لحماية المصنفات الأدبية والفنية، وتعتبر هذه الاتفاقية حجر الأساس في مجال الحماية الدولية لحق المؤلف ولقد وقعت على هذه الاتفاقية 120 دولة[7]، وقدمت هذه الاتفاقية مستوى عالميا من الحماية الخاصة بحقوق المؤلف، ويتوجب على أعضاء الاتفاقية توفير الحد الأدنى لحماية حقوق المؤلف لفترة زمنية هي مدة حياة المؤلف إضافة إلى خمسين سنة أخرى للأعمال التي تم النشر عنها لأول مرة في دولة عضو وللأعمال المنشورة أو غير المنشورة للأشخاص الذين ينتمون أو يقيمون في دولة عضو بالاتفاقية.

وتحدد المادة 02 من اتفاقية برن المصنف المحمي بأنه كل إنتاج في المجال الأدبي والعلمي والفني أيا كانت طريقة أو شكل التعبير عنه، من خلال استقراء نص هذه المادة يتبين أنها جاءت مرنة فهي لم تحدد المصنفات المحمية، بل تركت المجال واسعا، كما لم تحدد الطريقة التي يتم بها التعبير عن هذا المصنف المحمي، كما حددت نفس المادة أن الحماية القانونية لا تنطبق على الأخبار اليومية أو الوقائع المختلفة التي تتصف بكونها مجرد معلومات صحفية[8].

---

[1] محمد محمد شتا، المرجع السابق، ص26.

[2] روزا جعفر محمد الخامري، المرجع السابق، ص49.

[3] رشا علي الدين أحمد علي تقي الدين، المرجع السابق، ص92.

[4] رشا مصطفى أبو الغيط، تطور الحماية القانونية للكيانات المنطقية، دار الفكر الجامعي، الإسكندرية، ط1، 2006، ص100.

[5] شحاتة غريب شلقامي، الملكية الفكرية في القوانين العربية، دراسة لحقوق المؤلف والحقوق المجاورة ولخصوصية حماية برامج الحاسب الآلي، دار الجامعة الجديدة، مصر، 2008، ص19.

[6] مرسوم رئاسي رقم 97-341 مؤرخ في 13 سبتمبر 1997، المتضمن انضمام الجزائر بتحفظ إلى اتفاقية برن لحماية المصنفات الأدبية والفنية، ج.ر العدد 61، مؤرخة في 1997/09/14.

[7] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص200.

[8] رشا مصطفى أبو الغيط، المرجع السابق، ص100.

أما بالنسبة إلى الحقوق المالية وحق استغلال المصنف من قبل مؤلفه فقد أكدت عليه المادة 06، ثم جاء نص المادة 09 مقررا لمؤلفي المصنفات الأدبية والفنية حقا استشاريا في التصريح بعمل نسخ من مصنفاتهم بأي طريقة أو أي شكل كان بالإضافة إلى ما ورد بنص المادة 08 في منح المؤلفين حقا استئثاريا في ترجمة مصنفاتهم أو التصريح بذلك طوال مدة الحماية، كذلك ورد نص المادة 11 بتقرير حق التمثيل والأداء العلني ونقل التمثيل أو الأداء إلى الجمهور[1]، وتنظم المادة 15 لمؤلفي المصنفات الأدبية والفنية إقامة الدعاوى ومقاضاة من يعتدي على حقوقهم أما المادة 16 من الاتفاقية فتنص على أن جميع نسخ المصنف غير المشروعة تكون محلا للمصادرة في دول الاتحاد التي يتمتع فيها المصنف الأصلي بالحماية القانونية، وتطبق نفس الأحكام على النسخ الواردة من دولة لا يتمتع فيها المصنف بالحماية القانونية.

كذلك وردت في المادة 33 من هذا الملحق بشأن حق البلدان النامية في تقييد حق الاستنساخ وحق التشريعات الوطنية في منح التراخيص غير الاستئثارية وغير القابلة للتحويل في ضوء الضوابط الواردة بهذه المادة أيضا، التي يحكمها بصفة أساسية تلبية الاحتياجات العامة للجمهور أو التعليم المدرسي والجامعي.

نتيجة لما سبق بيانه، يتضح أن اتفاقية برن هي أول اتفاقية عالمية وضعت المبادئ العامة لحقوق الملكية الفكرية، بالإضافة إلى كثرة عدد الدول المشتركة فيها، وكذا اهتمامها بالقواعد الموضوعية، كما تعتمدها كل الاتفاقيات اللاحقة لها كمرجع، ولكنها من جانب آخر لم تتطرق إلى حماية البرمجيات بصورة مباشرة.

ثانيا: اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية، أسفرت جولة الأورجواي[2] لمنظمة التجارة العالمية عن اتفاق تريبس (TRIPS)[3] المتعلق بحماية حقوق الملكية الفكرية، وحددت فترة انتقالية للدول النامية هي 10 سنوات منذ دخول اتفاق منظمة التجارة العالمية حيز التنفيذ، معنى ذلك أن اتفاقية حقوق الملكية الفكرية أصبحت واقعا في عام 2005 وهو ما يعني تغييرا في شكل حماية الملكية الفكرية[4]، وهي بذلك تكون قد نقلت الحماية من المستوى المحلي إلى المستوى الدولي، مما يجعل الحماية موحدة[5].

تم التوقيع على تلك الاتفاقية من قبل الدول الأعضاء عام 1994 وقد عالج موقعو الاتفاقية العامة تعريفات التجارة –الجات– وحقوق الملكية الفكرية بتوقيع اتفاق الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية، فربطوا في ذلك بين المعايير الدولية والمعايير المحلية، وتتضمن تلك الاتفاقية العديد من الإجراءات المهمة والفعالة لردع الاعتداءات على حقوق الملكية الفكرية كما أنها ومن جهة أخرى تفرض على الدول اتخاذ العديد من التدابير المهمة لمعالجة الوضع، ومن تلك التدابير على سبيل المثال لا الحصر إعطاء الحق للسلطات في إصدار الأوامر بشن حملات مفاجئة لضبط أدلة ارتكاب الجريمة التي عادة ما يكون سهلا التخلص

---

[1] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص201.

[2] جولة أورجواي هي الجولة قبل الأخيرة في سلسلة الجولات التفاوضية التي عقدت بين ممثلي دول العالم التي بدأت جولاتها منذ عام 1948 بهدف تحرير التجارة وتنميتها، وقد سميت بهذا الاسم نسبة إلى البلد الذي بدأت فيه منذ 20 سبتمبر 1986. فاروق علي الحفناوي، المرجع السابق، ص37.

[3] TRIPS اختصار لعبارة The agreement on Trade-Related aspects of Intellectual Property Rights

[4] شحاتة غريب شلقامي، المرجع السابق، ص18.

[5] عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، المرجع السابق، ص77.

منها لو لم تكن هناك سرعة في محاولة ضبطها، كذلك التحفظ على أدوات ارتكاب الجرائم فضلا عن فرض عقوبات جنائية رادعة، وفي حالة تراخي الدولة العضو في اتخاذ مثل تلك الإجراءات وجهل في تطبيق قوانينها الوطنية، فإن المنظمة العالمية تعلن أن تلك الدولة لا تقوم بما عليها من واجبات في تطبيق الشروط والإجراءات المنصوص عليها في المعاهدة، وبالتالي تكون عرضة لأن تتخذ ضدها العديد من الإجراءات العقابية من باقي الدول الأعضاء[1].

كما تجدر الإشارة إلى أن الاتفاقية ضمت نصوصا موضوعية صيغت صياغة أكثر مرونة مما ورد في عدد من الاتفاقيات الدولية التي أحالت إليها اتفاقية تريبس[2]، وأهم ما تضمنته أنها أعطت موضوع الملكية الفكرية بشكل عام بعدا عالميا مهما، وربطت موضوعات الملكية الفكرية بآليات دولية محددة قد لا تستطيع دول كثيرة الفكاك منها، ولابد أن لهذه الاتفاقية تأثيرات مهمة على اقتصاديات كثير من الدول، ومنها الدول العربية أو على تشريعاتها الوطنية، ومن بين الموضوعات التي تناولتها هذه الاتفاقية تناولا صريحا موضوع الحماية القانونية للبرمجيات، وأهم ما جاء في هذه الاتفاقية ما يلي:

– سحبت الاتفاقية الحماية القانونية المقررة في اتفاقية برن نسخة باريس 1971 بشكل صريح إلى برامج الكمبيوتر سواء في صورة برنامج المصدر[3] أو برنامج الهدف[4] واعتباره مصنفا أدبيا بموجب المادة 1/10، والمعروف أن اتفاقية برن هي أهم اتفاقية دولية تتناول حماية المصنفات الأدبية والفنية[5]، والذي يهمنا من تقسيمات البرامج إلى لغة المصدر أو لغة الهدف هو أن الحماية القانونية تنصرف إلى البرنامج بمفهومه الواسع سواء كان بلغة مصدر أم بلغة هدف.

– نصت الاتفاقية في المادة 2/09 على امتداد الحماية المنصوص عليها في اتفاقية برن إلى التعبير عن الأفكار دون الأفكار المجردة، كما لا تمتد الحماية إلى أساليب وطرق إجراء العمليات ولا إلى المفاهيم والنظريات الرياضية نفسها.

ومعنى ذلك أن الأفكار المجردة يجوز لأي شخص أن يتقنها ويتداولها دون أن تصبح فعلته مخالفة للقانون طالما تناولها بأسلوب مبتكر وأضفى عليها طابعه الشخصي، وبمعنى أدق أن الفكرة إذا أفرغت وتجسدت في وسيلة من وسائل التعبير مصحوبة بقدر من الإبداع أصبحت الطريقة أو الصورة التي تم التعبير بها عن هذه الفكرة محلا للحماية، ومع ذلك يجوز لأي شخص أن يتناول نفس الفكرة بصورة أو طريقة أخرى من طرق التعبير عن الأفكار أو حتى بذات الطريقة ولكن بشكل آخر ينم عن ابتكار وتفرد، فوجود برنامج لمعالجة الكلمات فكرة يجوز لأي شخص في أي وقت أن يتناولها وينتج برنامجا يعالج الكلمات طالما تضمن

---

[1] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص201 و202.

[2] رشا علي الدين أحمد علي تقي الدين، المرجع السابق، ص174.

[3] برنامج المصدر: هو عبارة عن مجموعة من الأوامر والتعليمات التي يتم تحريرها بلغة منخفضة المستوى أو عالية المستوى، وهي لا تخاطب الآلة إلا بعد تعديلها إلى لغتها، أي يترجمها إلى لغتها بواسطة مترجم أو مفسر، وهي برامج خاصة بذلك تكون ضمت لغات البرمجة المستخدمة في كتابة برنامج المصدر. روزا جعفر محمد الخامري، المرجع السابق، ص46.

[4] برنامج الهدف: عكس مفهوم برنامج المصدر تماما، إذ تدركه الآلة وتستطيع التعامل معه وتشغيله، وبين برنامج المصدر والآلة توجد برامج ذات غرض تحويلي (برامج الترجمة) بموجبها يتحول برنامج المصدر إلى برنامج آلة.

أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، مصر، 2008، ص56.

[5] فاروق علي الحفناوي، المرجع السابق، ص113.

برنامجه الجديد طريقة مبتكرة غير منقولة من البرامج التي سبقته ولا يستطيع أول منتج لبرنامج معالجة الكلمات أن يدعي أنه مالك لحقوق الطبع على هذه الفكرة[1].

كما أن هناك حماية عامة، وتشمل هذه الحماية من ناحية أن هناك التزاما على عاتق الدول الأعضاء في اتفاقية أوجه التجارة المتصلة بحقوق الملكية الفكرية على ضمان اشتمال قوانينها مجموعة إجراءات لإنفاذ حقوق الملكية المنصوص عليها في هذا الجزء من الاتفاقية، وذلك بهدف تسهيل اتخاذ تدابير فعالة ضد أي تعد على حقوق الملكية الفكرية التي تغطيها الاتفاقية وكذلك اتخاذ إجراءات سريعة وذلك لمنع التعديات الحالة وردع التعديات الأخرى.

– مدت الاتفاقية الحماية القانونية إلى عمليات تجميع أو توليف البيانات أو أي مواد أخرى سواء كانت على وسيط مقروء للآلة أم أي وسيط آخر طالما انطوت على إيداع فكري سواء بسبب طريقة اختيارها أم تنظيمها، إلا أن هذه الحماية لا تمتد إلى البيانات نفسها، وذلك مع عدم الإخلال بأي حقوق مقررة تخص هذه البيانات أو المواد، ونصت المادة 11 من الاتفاقية على أنه بالنسبة إلى برامج الكمبيوتر والمصنفات السينمائية، فإن على الدول الأعضاء منح المؤلف وخلفائه الحق في تأجير أو منع تأجير أعمالهم الأصلية المتمتعة بحقوق الطبع أو النسخ المنتجة عنها تأجيرا تجاريا للجمهور، كما جاء في المادة 12 من نفس الاتفاقية على حكم مهم يتعلق بحساب مدة الحماية (على أساس آخر غير مدة حياة الشخص الطبيعي)، فنصت على أن مدة الحماية (فيما عدا أعمال التصوير الفوتوغرافي والفن التطبيقي) يجب ألا تقل عن 50 سنة تبدأ من تاريخ انتهاء السنة التي تم نشر العمل بها نشرا مرخصا، فإذا لم يكن النشر قد تم خلال هذه المدة فإن مدة الحماية (50 سنة) تحسب من تاريخ نهاية السنة التي تم فيها العمل[2].

– تلتزم البلدان الأعضاء بتنفيذ أحكام الاتفاقية، ويجوز لها دون إلزام أن تضمن قوانينها بما يتيح حماية أوسع من الحماية التي تطلبها اتفاقية تريبس تكريسا للمادة الأولى من هذه الأخيرة، وللبلدان الأعضاء حرية تحديد الطريقة الملائمة لتنفيذ أحكام هذه الاتفاقية في إطار أنظمتها القانونية حسب ما جاءت به المادة 05، ثم أضافت المادة 42 ضرورة توافر إجراءات قضائية مدنية إلى جانب إجراءات إدارية أخرى، وفي هذا الإطار تلتزم البلدان الأعضاء في الاتفاقية بمراعاة أحكام المواد من 01 إلى 21 من معاهدة برن وملحقاتها، مع مراعاة أن هذه الحماية تسري فقط على الإنتاج وليس على مجرد الأفكار أو الإجراءات أو أساليب العمل أو المفاهيم الرياضية.

وفي مجال الحماية المدنية، يجور للبلدان الأعضاء في اتفاقية تريبس أن تخول السلطات القضائية صلاحية الأمر باسترداد الأرباح أو دفع التعويضات المقررة سلفا أو هما معا، وذلك في جميع الأحوال بما في ذلك حالة ما إذا كان المعتدي لا يعلم بأنه قام بالتعدي، وكذلك يمكن التصرف في الأدوات التي تشكل تعديا وذلك على التفصيل الوارد في المادة 46 من الاتفاقية مع إمكانية الحصول على المعلومات الواردة في المادة 47 أيضا واتخاذ التدابير المؤقتة في القسم الثالث من الاتفاقية في مادتها 50، وفي المادة 61 من نفس الاتفاقية تمت إجراءات جنائية في حالة انتحال حقوق المؤلف على نطاق تجاري وغيرها من الجرائم[3].

فجميع أحكام اتفاقية تريبس تتوحد في هدف واحد وهو تحرير التجارة العالمية مع الأخذ بعين الاعتبار ضرورة توفير

---

[1] فاروق علي الحفناوي، المرجع السابق، ص137.

[2] فاروق علي الحفناوي، المرجع نفسه، ص114.

[3] محمد علي العريان، المرجع السابق، ص167.

إجراءات وتدابير لإنقاذ حقوق الملكية الفكرية دون أن تقف عائقا أمام التجارة الدولية المشروعة، والعمل على تشجيع الحماية الفاعلة في مجال حقوق الملكية الفكرية بجميع أنواعها، ولم يكن الطريق معبدا أمام تحقيق هذين الأمرين الأساسيين، حيث كان واجبا الموازنة بين هذين الأمرين بعناية ووعي بعد سنوات عديدة من التفاوض (من سبتمبر 1986 إلى أفريل 1994)، وقد بلغ عدد الدول الأعضاء في منظمة التجارة العالمية قرابة 150 دولة من بينها 11 دولة عربية، وهذه الدول بالتبعية أعضاء في اتفاقية تريبس ويدل هذا على سعي الدول بجميع إيديولوجياتها وتوجهاتها السياسية للانضمام إلى النظام العالمي الجديد.

نلاحظ وجود علاقة تكاملية بين اتفاقية تريبس وغيرها من الاتفاقيات الدولية الأخرى المبرمة في تاريخ سابق عليها فهذه الاتفاقية لم تلغ أحكام الاتفاقيات الدولية السابق إبرامها بل احتوت وطورت أحكام هذه الاتفاقيات، وعلى هذا الأساس، اهتمت هذه الاتفاقية في جانب كبير منها بوضع القواعد الإجرائية أكثر من اهتمامها بالقواعد الموضوعية، بل إنها أحالت القواعد الموضوعية التي أقرتها الاتفاقيات الدولية الرئيسية المبرمة من قبل في شأن حقوق الملكية الفكرية وأسبغت الحماية الدولية على البرامج بوصفها مصنفات أدبية تخضع لقواعد الحماية المقررة لحق المؤلف، ولهذا أحالت الاتفاقية في هذا الشأن إلى اتفاقية برن باعتبارها من أهم الاتفاقيات في هذا المجال[1].

فقد أصبحت اتفاقية تريبس اليوم بمثابة القانون الدولي الذي ينظم كافة الجوانب المتعلقة بالملكية الفكرية، الذي تستقي منه كافة الدول أحكام وقواعد قوانينها بشأن الملكية الفكرية باعتبار كافة دول العالم خاصة الدول الأعضاء في منظمة التجارة العالمية أو الدول الراغبة في الانضمام إلى المنظمة ملزمة بصياغة نصوص قانونية تتماشى مع قواعد هذه الاتفاقية، وبالرغم من أن اتفاقية برن هي الإطار القانوني الدولي الذي ينظم ويحمي حقوق المؤلف إلا أنها لم تتضمن إجراءات قضائية أو عقابية كافية كتلك التي قررتها اتفاقية تريبس بل اكتفت بالنص فقط على إجراء قضائي مدني وحيد وهو حجز ومصادرة النسخ غير المشروعة، كما نصت على وسائل حماية قانونية أوسع من تلك التي تناولتها اتفاقية برن.

ثالثا: المنظمة العالمية للملكية الفكرية WIPO، ظهرت الحاجة إلى توفير الحماية الدولية للملكية الفكرية عندما امتنع عدد من المخترعين الأجانب من المشاركة في المعرض الدولي للمخترعات في فيينا عام 1873 خشية أن تتعرض أفكارهم للنهب والاستغلال التجاري في بلدان أخرى، فجاءت اتفاقية باريس 1883 لتحمي براءات الاختراع والعلامات التجارية إضافة إلى الرسوم والنماذج الصناعية، وبدأت بتوقيع 14 دولة وتوالت بعدها الاتفاقيات في المجالات المختلفة، فظهرت الحاجة إلى قيام جهة مسؤولة عن تنفيذ هذه الاتفاقيات لتطوير نظام دولي متوازن وميسر بشأن الملكية الفكرية؛ نظام يكافئ الإبداع ويحفز الابتكار ويساهم في التنمية الاقتصادية، ولعل هذه الجهة تمثلت في المنظمة العالمية للملكية الفكرية.

تأسست المنظمة العالمية للملكية الفكرية WIPO بموجب اتفاقية ستوكهولم ويقع مقرها في مدينة جنيف السويسرية هذه المنظمة هي منظمة دولية حكومية، وتعد إحدى الوكالات الستة عشرة المتخصصة التابعة لمنظمة الأمم المتحدة، إذ أصبحت إحدى تلك الوكالات المتخصصة عام 1974 ثم توسعت في دورها وذلك بدخولها في اتفاق تعاون مع منظمة التجارة العالمية عام 1996[2].

---

[1] رشا علي الدين أحمد علي تقي الدين، المرجع السابق، ص187.

[2] عبد الله عبد الكريم، الحماية القانونية لحقوق الملكية الفكرية على شبكة الإنترنت، دراسة في الأطر القانونية للحماية مع شرح النظام القانوني للملكية الفكرية في التشريعات المصرية والأردنية والأوروبية والأمريكية ومعاهدتي الإنترنت، دار الجامعة الجديدة، مصر، 2008، ص252.

وقد صادقت الجزائر على الاتفاقية العالمية المتعلقة بإنشاء المنظمة العالمية للملكية الفكرية بموجب الأمر رقم 75-02 المؤرخ في 1975/01/09، تهدف إلى تقديم المساعدة من أجل ضمان حماية حقوق المبدعين وأصحاب الملكية الفكرية في جميع أنحاء العالم[1]، وهي ترى في هذا الدور اعترافا بالمبدعين والمخترعين ومكافأة لهم على إبداعاتهم، تعتبر هذه الحماية حافزا يشجع على الإبداع والتميز ويدفع بعجلة التجارة الدولية إلى الأمام بتوفيرها مناخا مستقرا من أجل تبادل منتجات الملكية الفكرية، كما تعمل على تحديث وتفعيل إدارة الاتحادات المؤسسة في مجالات حماية الملكية الصناعية والملكية الأدبية والأعمال الفنية مع الاحترام الكامل لاستقلال كل اتحاد منها، لهذا تم مراجعة وتعديل اتفاقية برن على فترات دورية لمواجهة التطور في مجال الملكية الفكرية، مع ذلك ومع وجود الحاجة إلى إيجاد قواعد دولية جديدة في مجال حقوق المؤلف أخذت كل من المنظمة العالمية للتجارة الدولية وكذلك المنظمة العالمية لحماية حقوق الملكية الفكرية في دراستها وتحليلها والعمل على تكوينها، حيث أسفرت عن وجود اتفاقيات جديدة.

أما عن وظائف المنظمة، فلقد حددت المادة 04 من هذه الاتفاقية وظائف المنظمة بالنقاط التالية:

– العمل على دعم اتخاذ الإجراءات التي تهدف إلى تيسير الحماية الفعالة للملكية الفكرية في جميع أنحاء العالم وإلى تنسيق التشريعات الوطنية في هذا المجال.

– تقوم بالمهام الإدارية لاتحاد باريس وللاتحادات الخاصة فيما يتعلق بذلك الاتحاد واتحاد برن.

– يجوز لها أن تقبل المهام الإدارية الناشئة عن تنفيذ أي اتفاق دولي آخر يهدف إلى دعم حماية الملكية الفكرية أو المشاركة في مثل هذه المهام.

– تشجيع إبرام الاتفاقيات الدولية التي تهدف إلى تدعيم حماية الملكية الفكرية.

– تعرض تعاونها على الدول التي تطلب المساعدة القانونية الفنية في مجال الملكية الفكرية.

– تجمع المعلومات الخاصة بحماية الملكية الفكرية وتنشرها وتجري الدراسات في هذا المجال وتشجعها وتنشر نتائج تلك الدراسات[2].

– توفر الخدمات التي تيسر الحماية الدولية للملكية الفكرية وتنهض بأعباء التسجيل في هذا المجال، كما تنشر البيانات بالتسجيلات، حيثما كان ذلك ملائما.

– تتخذ كل إجراء ملائم آخر.

هذا باختصار عن أهداف منظمة WIPO ووظائفها، أما الذي يعنينا في هذه الدراسة فهو البرمجيات باعتبارها من المصنفات الأدبية والفنية التي مما لا شك في أنها تنبئ عن إبداع فكري لمصمميها وبعد ما تزايدت الحاجة إلى وجوب إيجاد نصوص قانونية خاصة لحماية البرامج شكلت المنظمة العالمية للملكية الفكرية مجموعة عمل تضم عددا من الخبراء تهدف إلى حماية برامج الحاسب الآلي، إلا أن التطور القانوني السائد في تلك الفترة جزم بعدم اعتبارها من قبيل الاختراعات، وهو ما أكدته الاتفاقية الأوروبية لبراءات الاختراع المبرمة في ميونيخ في 05 أكتوبر 1973، ونتيجة لاستمرار لجان الخبراء في دراسة الأسلوب المناسب

[1] فاروق علي الحفناوي، المرجع السابق، ص75.

[2] محمود أحمد عبابنة، المرجع السابق، ص160.

لحماية برامج الحاسب الآلي ومسائلها الفنية وعبر الاجتماعات المتكررة وآخرها الذي تم في عام 1985 والتعاون ما بين WIPO واليونسكو في جنيف، ساد الاتجاه لدى أغلب الدول الصناعية ودول العالم الثالث إلى الميل إلى خضوع هذه البرمجيات لقوانين حماية حق المؤلف، ومنذ ذلك العام وحتى الآن عدلت معظم الدول تشريعاتها الخاصة بحق المؤلف حيث أضافت برامج الحاسب الآلي والأجهزة الإلكترونية الذكية إلى المصنفات الأدبية المحمية وفقا للقانون.

تقوم المنظمة العالمية للملكية الفكرية بالإشراف على نحو 23 اتفاقية دولية خاضعة لحقوق الملكية الفكرية، ومتى وقعت إحدى الدول على هذه المعاهدات، فإن ذلك يعني أنها أصبحت ملزمة بتطبيقها على أراضيها، وللمعاهدات في الدول قوة تنفيذية تفوق القوانين الداخلية فعند التقاضي بينه وبين التشريع الداخلي ترجح المعاهدة في التطبيق والتنفيذ وهنا تكمن أهميتها أيضا ويتحقق التناسق في مستويات الحماية عبر الدول، ولم تكتف المنظمة بالمفاهيم التقليدية لحقوق الملكية الفكرية الواجب حمايتها بل واكبت التطورات التي تحدث على الصعيد التكنولوجي وأخذتها بعين الاعتبار[1]، ومع ظهور شبكة الإنترنت وثورة المعلومات وانتشار الملكية الفكرية للإلكترونيات أصبحت المنظمة تهتم بوضع قواعد ومعايير جديدة كي تساير كل ذلك.

وعند تأسيس منظمة التجارة العالمية ودخولها حيز التنفيذ في الأول من جانفي 1995 نجد أن كلا المنظمتين نجحت في تحقيق نوع من التعاون والعمل المشترك بينهما، وذلك من خلال توحيد الأهداف التي تنشدها كل منهما وهي حماية حقوق الملكية الفكرية بكافة جوانبها في العالم أجمع ومساعدة بلدان العالم على النمو والتقدم من خلال هذه الحماية، وكان ذلك من خلال عمليات متتابعة من التوعية والتدريب وتقديم المساعدات الفنية، ودخل الاتفاق المبرم بين المنظمتين حيز التنفيذ في 01 جانفي 1996، وينص على التعاون بين المنظمتين في تنفيذ اتفاق الجوانب التجارية لحقوق الملكية الفكرية، وكان من نتائج هذا الاتفاق ما قامت به المنظمتان في عام 2000 من مبادرة مشتركة لمساعدة البلدان النامية في الوفاء بالتزاماتها المترتبة على اتفاق الجوانب التجارية لحقوق الملكية الفكرية أو ما يعرف باسم برنامج المنظمة العالمية للملكية الفكرية للتعاون الإنمائي[2]، وفي 14 جويلية 2001 بدأت المنظمتان مبادرة مشتركة جديدة لمساعدة الدول الأقل نموا للاستفادة القصوى من المنافع التي تعود عليها من جراء حماية حقوق الملكية الفكرية ومساعدتها على الوفاء بالتزاماتها المترتبة على اتفاق الجوانب التجارية لحقوق الملكية الفكرية في سنة 2006 وذلك من خلال برامج المساعدة الفنية[3].

---

[1] عبد الله عبد الكريم، جرائم المعلوماتية والإنترنت، الجرائم الإلكترونية، دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والإنترنت مع الاشارة إلى جهود مكافحتها محليا وعربيا ودوليا، المرجع السابق، ص252.

[2] برامج المنظمة العالمية للملكية الفكرية للتعاون الإنمائي هي العبارة الشائعة في منظمة الأمم المتحدة، ويقصد بها مساعدة البلدان النامية، والهدف الرئيسي المنشود من برنامج التعاون الإنمائي هو الإسهام بوجه خاص في عملية التنمية داخل البلدان النامية في مجال الملكية الفكرية.

[3] المساعدة الفنية المقصودة في هذه المبادرة المشتركة التي أعلنتها المنظمتان تتضمن التعاون في مراجعة التشريعات والتدريب من قبل الاختصاصيين، وإعادة بناء المؤسسات وتحديث أنظمة الملكية الفكرية والحرص على تنفيذ كل ذلك تنفيذا سليما. عبد الله عبد الكريم، جرائم المعلوماتية والإنترنت، الجرائم الإلكترونية، دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والإنترنت مع الاشارة إلى جهود مكافحتها محليا وعربيا ودوليا، المرجع السابق ص259.

وقد صدر عن المنظمة العالمية للملكية الفكرية معاهدتين سميتا بمعاهدتي الإنترنت[1] إذ سنكتفي بدراسة معاهدة الإنترنت الأولى لأنها تنصب على حماية برامج الحاسب الآلي، وبموجب المادة الأولى، فإن هذه المعاهدة تعتبر اتفاقا خاصا بالمعنى الذي تحدده المادة 20 من اتفاقية برن لحماية المصنفات الأدبية والفنية بالنسبة إلى الأطراف المتعاقدة من بلدان الاتحاد المنشأ بموجب تلك الاتفاقية، وليس لهذه المعاهدة أي صلة بمعاهدات أخرى خلاف اتفاقية برن، ولا تخل بأي حق أو التزام من الحقوق والالتزامات المترتبة على أي معاهدات أخرى.

إن القواعد الاتفاقية بالنظر إلى مضمونها تارة، وتأثرا بمبدأ نسبية أثر هذه الاتفاقيات تارة أخرى وقفت عاجزة في غالب الأحيان عن إيجاد حلول موحدة ومعايير وقائية تتفق عليها دول العالم جميعا، مما أحدث نوعا من التباين التشريعي على الصعيد الداخلي لدول العالم، وهذا يرجع إلى عدة أمور منها أن قواعد القانون الدولي الاتفاقي تضع قواعد اتفاقية تمثل الحد الأدنى للحماية ويعني هذا أن لكل دولة عضو في اتفاقية ما أن تضع أحكام قواعد حماية تفوق ما أقرته الاتفاقية.

ونجد كذلك العديد من دول العالم ما زالت خارج حدود القانون الدولي الاتفاقي نظرا إلى عدم انضمامها إلى الاتفاقيات الدولية، كما أن هذه الاتفاقيات في الغالب تميل إلى وضع الأطر العامة للحماية دون الدخول في الأمور التفصيلية كتحديد القانون الواجب التطبيق، أو وضع التعاريف القانونية كتحديد صفة المؤلف في مجال حماية حق المؤلف مثلا، مما يستوجب العودة إلى التشريعات الداخلية لتحديد مثل هذه الأمور، وتتباين هذه التشريعات الداخلية في فلسفتها التشريعية مما ينعكس على حكم وقواعد التشريعات الوطنية ويخلق هذا بالطبع نوعا من التباين بين أحكام هذه التشريعات[2].

لهذا، يمكن القول إنه لنجاح هذه الاتفاقيات في القيام بدورها لا بد أن تكون هذه الاتفاقيات مقبولة في كافة النظم القانونية حتى لا تصطدم بشدة مع القوانين الخاصة بكل دولة، إضافة إلى وجوب الانضمام والمصادقة على هذه الاتفاقيات، لضمان فاعلية قواعدها الدولية، وعلى هذا الأساس وجب تكاتف الجهود الدولية، وذلك من خلال الانضمام إلى هذه الاتفاقيات ومحاولة تجسيدها على مستوى التشريعات الداخلية لكل دولة.

البند الثالث: جهود الأمم المتحدة لمواجهة جرائم التكنولوجيا الحديثة

لقد نظمت الأمم المتحدة عدة مؤتمرات دولية، محاولة منها لتقديم توصيات توضح من خلالها المخاطر الناجمة عن استخدام التكنولوجيا الحديثة، وتبين الإجراءات التي يجب على الدول الأخذ بها قصد مواجهة هذه الجرائم.

أولا: جهود منظمة الأمم المتحدة في ميدان حماية الحياة الخاصة، توجهت جهود منظمة الأمم المتحدة في ميدان حماية الحياة الخاصة في مواجهة التقدم التقني وحماية الأفراد وحرياتهم من خطر التعدي عليها وذلك في المؤتمر الدولي الأول لحقوق الإنسان الخاص بأثر التقدم التكنولوجي على حقوق الإنسان الذي تبنت الجمعية العامة توصياته، وأبرز ما جاء فيها أن الحاسبات

---

[1] معاهدة الإنترنت الأولى وتسمى أيضا معاهدة الويبو بشأن حق المؤلف، كما اعتمدها المؤتمر الدبلوماسي للمنظمة العالمية للملكية الفكرية في 1996/12/20، ومعاهدة الإنترنت الثانية بشأن الأداء والتسجيل الصوتي 1996.

[2] رشا علي الدين أحمد علي تقي الدين، المرجع السابق، ص05 و06.

الإلكترونية تمثل أكبر تهديد للحياة الخاصة والحرية الشخصية إذ أنها تعد من أدوات المراقبة وأجهزة التطفل الحديثة خاصة إذا تم تخزين البيانات الشخصية عليها وتحليلها مما يكشف عن أنماط التعامل والعلاقات[1].

كما أكد مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين الذي تم انعقاده في مدينة ميلانو بإيطاليا سنة 1985 على وجوب تطبيق التطورات الجديدة في مجال العلم والتكنولوجيا في كل مكان لصالح الجمهور، وبالتالي منع الجريمة على نحو فعال وأكد أيضا على وجوب اتخاذ تدابير ملائمة ضد حالات إعادة الاستعمال الممثلة للتكنولوجيا لما قد تولده من أشكال جديدة من الجريمة، وأشار إلى مسألة الخصوصية التي يمكن أن تخترق عن طريق الإطلاع على البيانات الشخصية المخزنة داخل نظام الحاسب الآلي التي تشكل انتهاكا لحقوق الإنسان، واعتداء على حرمة حياته الخاصة، وأكد المؤتمر على وجوب اعتماد ضمانات ملائمة لصون السرية، وإقرار نظم تكفل وصول الأفراد إلى هذه البيانات لتصحيح الأخطاء فيها، كذلك أكد المؤتمر عبر قواعده التوجيهية على ضرورة تشجيع التشريعات الحديثة التي تجرم وتتناول جرائم التكنولوجيا الحديثة باعتبارها نمطا من أنماط الجريمة المنظمة كغسيل الأموال والاحتيال المنظم...إلخ[2].

ثانيا: مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين، ناشد في قراره المتعلق بالجرائم ذات الصلة بالتكنولوجيا الحديثة الدول الأعضاء إلى تكثيف جهودها كي تكافح بمزيد من الفعالية عمليات إساءة استعمال وسائل التكنولوجيا التي تستدعي تطبيق جزاءات جنائية على الصعيد الوطني بما في ذلك النظر إذا دعت الضرورة إلى تحديث القوانين والإجراءات الجنائية واتخاذ التدابير اللازمة من أجل ضمان أن الجزاءات والقوانين الراهنة بشأن سلطات التحقيق وقبول الأدلة في الإجراءات القضائية تنطبق على هذه الجرائم وإدخال تغييرات مناسبة عليها إذا دعت الضرورة إلى ذلك[3]، بالإضافة إلى النص على جرائم وجزاءات وإجراءات تتعلق بالتحقيق والأدلة حيث تدعو الضرورة إلى ذلك للتصدي لهذا الشكل الجديد والمعقد من أشكال النشاط الإجرامي في حالة عدم وجود قوانين تنطبق على نحو ملائم.

كما دعى المؤتمر إلى مضاعفة الأنشطة التي تبذلها الدول الأعضاء على الصعيد الدولي من أجل مكافحة الجرائم المتصلة بالتكنولوجيا الحديثة بما في ذلك دخولها حسب الاقتضاء أطرافا في المعاهدات المتعلقة بتسليم المجرمين، وتبادل المساعدة في المسائل الجنائية وأن تتخذ خطوات محددة حسب الاقتضاء من أجل تحقيق هذا الهدف وذلك بالإضافة إلى توصيات أخرى.

وقد يكون ملائما كخطوة تعزيز مسار التعاون الفعال وتكملة ما اتخذه مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين في هذا الشأن من قرارات أن يسفر بحث مؤتمرات الأمم المتحدة لموضوع الجرائم ذات الصلة بالتكنولوجيا الحديثة عن فتح آفاق جديدة للتعاون الدولي في هذا المضمار لاسيما فيما يتعلق بوضع أو تطوير معايير دولية لأمن المعالجة الآلية للبيانات، واتخاذ تدابير ملائمة لحل مشكلات الاختصاص القضائي التي تثيرها الجرائم المتصلة بتقنية المعلومات العابرة للحدود مع كفالة الحماية في الوقت نفسه لحقوق الأفراد وحرياتهم وسيادة الدول.

---

[1] علي جبار الحسناوي، المرجع السابق، ص149.

[2] محمود أحمد عبابنة، المرجع السابق، ص157 و158.

[3] نهلا عبد القادر المومني، المرجع السابق، ص52.

ثالثا: المؤتمر التاسع لمنع الجريمة ومعاملة المجرمين، انعقد هذا المؤتمر برعاية الأمم المتحدة في القاهرة عام 1995 وأكدت توصياته على وجوب حماية الإنسان في حياته الخاصة وفي ملكيته الفكرية من تزايد مخاطر التكنولوجيا، ووجوب التنسيق والتعاون بين أفراد المجتمع الدولي لاتخاذ الإجراءات المناسبة للحد منها، وفي عام 2000 عقدت الأمم المتحدة مؤتمرها العاشر لمنع الجريمة ومعاملة المجرمين في بودابست وأكدت على وجوب العمل الجاد للحد من هذه الجرائم المتزايدة والمستحدثة، واتخاذ تدابير للحد من أعمال القرصنة[1].

وعليه، فالأمم المتحدة تبذل مجهودات جبارة من خلال المؤتمرات الدولية التي تنظمها كمحاولة منها للتصدي لجرائم التكنولوجيا الحديثة، مؤكدة على وجوب تعزيز التعاون بين الدول في الجوانب القانونية سواء كانت موضوعية أم إجرائية، من أجل الحد من انتشار الجريمة وتعاظم مخاطرها.

الفرع الثاني: الجهود الإقليمية لمكافحة جرائم التكنولوجيا الحديثة

نستعرض في هذا الفرع أبرز الجهود التشريعية الإقليمية على المستوى الأوروبي لانطوائها على جهود هامة في مجال حماية المعلومات، والتي شكلت نموذجا للكثير من دول العالم في هذا المجال، ثم ننتقل لنلقي الضوء على الجزء الذي يهمنا كمنطقة عربية واستعراض أبرز الجهود على المستوى العربي في هذا المجال أيضا، للوقوف على مدى كفايتها وفاعليتها.

البند الأول: على المستوى الأوروبي

كان للدول الأوروبية والغربية منها تحديدا السبق في مجال التشريعات الخاصة بالجرائم المتصلة بالتكنولوجيا الحديثة وحماية البيانات والمعلومات المعالجة آليا، وذلك بحكم كونها أحد منابع ثورة المعلومات التي إنطلقت إلى باقي دول العالم، وأولى الدول التي غاصت في بحور تقنيات المعلومات والاعتماد عليها بشكل كبير، وأولى الدول التي انكوت بنار تلك التقنية، وأمام مخاطر وتحديات تلك التقنية الحديثة، كان لزاما على تلك الدول أن تتخذ من التشريعات درعا واقيا لها ولمؤسساتها وأفرادها لصد تلك المخاطر، ومن أبرز تلك الجهود التشريعية ما يأتي:

أولا: الدليل الإرشادي لحماية الخصوصية ونقل البيانات الخاصة الصادر عن منظمة التعاون الاقتصادي والتنمية

تم إعداد هذا الدليل في عام 1980، وقد تضمن مجموعة من القواعد التي تشكل ضمانات للمعلومات والبيانات الشخصية المعالجة إلكترونيا في كل مرحلة من مراحل الجمع والتخزين والمعالجة والنشر، وتتلخص هذه المبادئ في مشروعية جمع البيانات، وتحديد الهدف من جمعها واستخدامها للغرض الذي جمعت من أجله، وتوفير وسائل حماية أمن المعلومات وضمان سريتها، ويختص نطاق هذه القواعد بالبيانات والمعلومات المتعلقة بالأشخاص الطبيعيين فقط في القطاعين الحكومي والخاص، وتشمل تلك البيانات المعالجة آليا أو المعدة يدويا[2].

---

[1] علي جبار الحسناوي، المرجع السابق، ص148.

[2] يونس عرب، قراءة في الاتجاهات التشريعية للجرائم الإلكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان، ورقة عمل مقدمة بورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، هيئة تنظيم الاتصالات، مسقط، سلطنة عمان، 02-04 أبريل 2006، ص26 و27.

ثانيا: اتفاقية المجلس الأوروبي بشأن حماية الأفراد في مواجهة المعالجة الآلية للبيانات الشخصية، لقد أبرمت هذه الاتفاقية في 1981/01/28 بمدينة ستراسبورغ بفرنسا وأصبحت نافذة بتاريخ 1985/10/01، وهي اتفاقية ملزمة للدول المصدقة عليها، وتتضمن المبادئ التي تمثل الحد الأدنى للخصوصية المتعين على الدول الأطراف تضمينها في التدابير التشريعية والقوانين التي تضعها، وهذه المبادئ تتقارب لحد كبير مع مبادئ منظمة التعاون الاقتصادي والتنمية، والمبادئ التي تضمنها قرار الجمعية العامة للأمم المتحدة 95/45 لسنة 1990 بشأن مبادئ توجيهية لتنظيم ملفات البيانات الشخصية المعدة بالحاسبات الإلكترونية السالف بيانها.

ويضاف إلى الجهود السابقة على المستوى الأوربي إصدار الاتحاد الأوروبي مجموعة من التعليمات المتعلقة بخصوص حماية بيانات الأفراد مثل تعليمات 1976/04/08 المتعلقة بحماية الأفراد من أنشطة التقييم الآلي للبيانات، وتعليمات 1979/05/08 المتعلقة بحماية الأفراد في مواجهة التطور التقني لمعالجة البيانات، وتعليمات 1982/03/09 بذات الموضوع.

ثالثا: اتفاقية المجلس الأوروبي بشأن مكافحة الجرائم المعلوماتية، سبق وأن تناولنا أحكام هذه الاتفاقية في مواقع سابقة من هذا البحث، إلا أنه كان لزاما أن نتعرض إليها ولو بشكل موجز في معرض الحديث عن الجهود التشريعية الإقليمية لحماية سرية المعلومات الإلكترونية ومكافحة الجرائم الماسة بها باعتبارها أبرز تلك الجهود وأكثرها ارتباطا بالجريمة المتصلة بالتكنولوجيا الحديثة.

أقدمت الدول الأعضاء في المجلس الأوروبي والدول الأخرى الموقعة على هذه الاتفاقية على هذه الخطوة وفقا لما جاء في ديباجة هذه الاتفاقية إدراكا منها بالحاجة لإيجاد سياسة جنائية مشتركة، تهدف إلى حماية المجتمع من جرائم الفضاء المعلوماتي واعترافا منهم بالحاجة للتعاون المتبادل بين الدول والقطاع الصناعي الخاص إيمانا منهم بأن المكافحة الفعالة لهذا النوع من الجرائم تستلزم مزيدا من التعاون الدولي السريع والفعال في المسائل الجنائية[1].

جسدت اتفاقية بودابست لمكافحة الجرائم المتصلة بالتكنولوجيا الحديثة الجهود التي بذلها المجلس الأوروبي للتصدي لهذا النوع من الجرائم التي شكلت تحديا خطيرا وتهديدا حقيقيا لمصالح الدول والأفراد والمؤسسات، وقد ضمت هذه الاتفاقية معظم الدول الأوروبية بالإضافة إلى كندا، واليابان، وجنوب إفريقيا والولايات المتحدة وطرحت للتوقيع في بودابست في 23 نوفمبر 2001 ودخلت حيز التنفيذ في الأول من يوليو 2004 ويمكن لأية دولة في العالم الانضمام للاتفاقية إذا ما رغبت بذلك[2].

وتتألف هذه الاتفاقية من 48 مادة وتغطي الاتفاقية مجموعة كبيرة من الجرائم الجنائية، على النحو الآتي:

- الجرائم ضد سرية وسلامة وإتاحة البيانات والنظم؛ وتشمل جرائم الولوج غير القانوني، جرائم الاعتراض غير القانوني الاعتداء على سلامة البيانات، الاعتداء على سلامة النظام، إساءة استخدام أجهزة الحاسب.
- الجرائم المتصلة بالتكنولوجيا الحديثة وتشمل التزوير المعلوماتي، والغش المعلوماتي.
- الجرائم المتصلة بالمحتوى، وهي الجرائم المتصلة بالمواد الإباحية الطفولية عبر النظم المعلوماتية.
- الجرائم المتصلة بالانتهاكات الخاصة بحقوق الملكية الفكرية والحقوق المجاورة لها.

---

[1] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/default_en.asp

[2] كريستينا سكولمان، عن جرائم الإنترنت، طبيعتها وخصائصها، برنامج تعزيز حكم القانون في بعض الدول العربية مشروع تحديث النيابات العامة، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، ا 19 و20 يونيو 2007، ص40.

- الشروع والاشتراك في جرائم تكنولوجيا المعلومات الحديثة.

وأوجبت هذه الاتفاقية أيضا تقرير مسئولية الأشخاص المعنوية.

ولم تقتصر اتفاقية بودابست على جوانب الحماية الجنائية الموضوعية فحسب، بل شملت كذلك الجوانب الإجرائية وتشمل: نطاق تطبيق الإجراءات الجنائية وشروطها وضماناتها، التحفظ العاجل على البيانات المعلوماتية المخزنة، الأمر بإنتاج أو تقديم بيانات معلوماتية، تفتيش وضبط البيانات المعلوماتية المخزنة والاختصاص القضائي، فيما نظمت موضوع التعاون الدولي وهو أحد الأهداف الأساسية للاتفاقية، ويشمل؛ المبادئ العامة المتعلقة بالتعاون الدولي والمبادئ المتعلقة بتسليم المجرمين، المساعدة القضائية المتبادلة والإجراءات المتعلقة بالمساعدة المتبادلة في حالة عدم وجود اتفاقيات دولية واجبة التطبيق.

وعلى النحو المتقدم تكون اتفاقية بودابست نموذجا وركيزة أساسية، في مجال مكافحة الجرائم المتصلة بالتكنولوجيا الحديثة تسترشد بها باقي دول العالم في صياغة تشريعاتها الوطنية أو لإبرام اتفاقيات ثنائية أو إقليمية أو دولية.

البند الثاني: على المستوى العربي

وفقا لتقرير مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية الذي عقد في مدينة سلفادور بالبرازيل في الفترة من 12 إلى 19 أبريل 2010، تعد الدول النامية بما فيها الدول العربية من أكثر الدول عرضة لمخاطر جرائم التكنولوجيا الحديثة، مما يجعلها بحاجة إلى وضع آليات تشريعية محددة لمكافحة تلك الجرائم، وقد عملت الدول العربية من خلال جامعة الدول العربية على توحيد جهودها التشريعية في سبيل مكافحة الجريمة بشكل عام وجرائم التكنولوجيا الحديثة بما فيها الجرائم الماسة بسرية المعلومات الإلكترونية بشكل خاص وهي جهود حميدة، وفيما يلي نستعرض أبرز تلك الجهود.

أولا: القانون الجزائي العربي الموحد الاسترشادي، اعتمد مجلس وزراء العدل العرب بتاريخ 19 نوفمبر 1996 القانون الجزائي العربي الموحد كقانون نموذجي وذلك بالقرار رقم 229-د12[1]، وقد جرم هذا القانون الاعتداء على حقوق الأشخاص الناتج عن الجذاذات والمعالجات المعلوماتية، وذلك بالمواد من 461 إلى 464، حيث جرمت جمع المعلومات الاسمية أو معالجتها آليا، أو استعمالها بالمخالفة لأحكام القانون، أو المساس بسلامة وسرية معلومات الأشخاص.

وبمطالعة المادتين 463 و464، نلاحظ أنها تناولت صورتين من صور الجرائم الماسة بسرية المعلومات الإلكترونية، وتناولت المادة 462 جريمة الاعتراض غير القانوني للبيانات والمعلومات الشخصية للأفراد الطبيعيين فقط، حيث تنص تلك المادة على أنه "يعاقب بالحبس مدة لا تزيد على سنة وبالغرامة كل من حصل على معلومات اسمية خاصة بالغير، أثناء تسجيلها أو ترتيبها أو إرسالها بأية وسيلة من وسائل المعالجة التي من شأن إفشائها المساس بسمعة المعني بالأمر أو بحياته الشخصية، مما يمكن إطلاع الغير ممن لا تسمح له صفته الإطلاع على تلك المعلومات دون إذن المعني بالأمر".

في حين تناولت الفقرة الأولى من المادة 464 جريمة الدخول غير المصرح به أو البقاء داخل نظام المعالجة الآلية حيث تنص على أنه "يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين كل من دخل بطريق الغش إلى كامل أو جزء من نظام المعالجة الآلية للمعلومات، أو بقي فيه، وتضاعف العقوبات إذا نتج عن ذلك إما محو المعلومات التي يحتوي عليها النظام أو تعديلها...".

[1] www.arableagueonline.org

ثانيا: قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات، جاء هذا القانون كخطوة متقدمة في مجال العمل العربي المشترك لمكافحة الجرائم المتصلة بالتكنولوجيا الحديثة، حيث تم اعتماده من قبل كل من مجلس وزراء العدل العرب في دورته التاسعة عشرة بالقرار رقم 495-د19 في 2003/10/08، ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم 417-د2004/21[1]، ويتألف هذا القانون من 27 مادة، تشمل صور الجرائم المتصلة بالتكنولوجيا الحديثة المختلفة بما فيها جرائم الدخول غير المصرح به أو البقاء داخل النظام المعلوماتي، والاعتراض أو الالتقاط غير القانوني للمعلومات والبيانات بالإضافة إلى عدة صور أخرى مثل إعاقة النظام وإتلاف البيانات والمعلومات والاحتيال والتزوير وغيرها.

وقد تم إعداد هذا القانون ليكون بمثابة نموذج أو دليل تسترشد به كل دولة عضو بالجامعة العربية عند سنها تشريعا وطنيا خاصا بمكافحة الجرائم المتصلة بالتكنولوجيا الحديثة.

ويعد ذلك مثالا هاما على التعاون الإقليمي والدولي لمكافحة هذه الجرائم، كونه يشكل نوعا من المساعدة للدول التي تفتقر إلى الخبرات والكفاءات في هذا المجال لتطوير بنيتها التشريعية، فضلا عما يشكله من فرصة لتبادل الأفكار في هذا المجال فالصورة الإجرامية التي قد تظهر في دولة ما قد لا تظهر في ذات الوقت في دولة أخرى، وبهذا تكون مثل هذه القوانين فرصة لسد الثغرات التي قد ينفذ من خلالها الإجرام التكنولوجي الحديث، لذا نرى أنه ونظرا لقيام الدول العربية بإبرام اتفاقية خاصة بمكافحة جرائم تقنية المعلومات الحديثة في عام 2010 والتي سنتناولها فيما يلي، فإنه يتعين إعادة طرح هذا القانون النموذجي للمناقشة من قبل الجهات المختصة بالجامعة العربية مثل مجلسي وزراء العدل والداخلية العرب، لإعادة النظر فيه وإجراء التعديلات اللازمة عليه في ضوء تلك الاتفاقية، ونقترح أن يكون هذا القانون النموذجي حاضرا بشكل دوري على طاولة اجتماعات المختصين بالدول العربية لمراجعته بشكل مستمر وإدخال التعديلات اللازمة عليه بما يجعله نموذجا متطورا بقدر التطور السريع الذي تتسم به هذه الجرائم.

ثالثا: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، أبرمت هذه الاتفاقية بتاريخ 2010/12/21 ووقعت عليها سبع عشرة دولة عربية[2]، وقد عبرت المادة الأولى منها عن الهدف الذي تنشده وهو تعزيز التعاون فيما بين الدول العربية لمكافحة جرائم تقنية المعلومات الحديثة التي تهدد أمنها ومصالحها وسلامة مجتمعاتها، وذلك بتبني سياسة جنائية مشتركة تهدف إلى حماية أمن المجتمع العربي وأفراده ومصالحهم ضد تهديدات جرائم تقنية المعلومات، وقد جاءت هذه الاتفاقية بعد مطالبات عديدة من قبل المختصين في أكثر من مناسبة بإصدار مثل هذه الاتفاقية، حيث تضمن إعلان القاهرة لمكافحة الجريمة الإلكترونية الصادر عن المؤتمر الإقليمي الأول حول الجريمة الإلكترونية المنعقد في القاهرة بتاريخ 26 و27 نوفمبر 2007، بالإضافة إلى دعوة الدول العربية إلى الإسراع في إقرار تشريعات لمكافحة الجرائم المتصلة بالتكنولوجيا الحديثة، وتشجيع دول المنطقة العربية للاسترشاد باتفاقية بودابست عند إعداد القوانين الموضوعية والإجرائية الخاصة بمكافحة هذه الجرائم[3].

وتتألف هذه الاتفاقية من 43 مادة، شملت الجوانب الموضوعية والإجرائية الخاصة بالجرائم المعلوماتية، ومظاهر التعاون بين الدول الأعضاء، حيث تضمن الفصل الثاني صور الأفعال التي جرمتها الاتفاقية وهي: الدخول غير المشروع، الاعتراض غير المشروع

[1] www.arableagueonline.org
[2] www.arableagueonline.org
[3] www.arabipcenter.com/pulic/cybercrimelaws

الاعتداء على سلامة البيانات، إساءة استخدام وسائل تقنية المعلومات، التزوير، الاحتيال، الجرائم المرتبطة بالإباحية كالمقامرة والاستغلال الجنسي، الاعتداء على حرمة الحياة الخاصة، الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات، الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات، الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة، الاستخدام غير المشروع لأدوات الدفع الإلكترونية، وتناولت أحكام الشروع والاشتراك في ارتكاب الجرائم السابقة، والمسؤولية الجنائية للأشخاص الطبيعية والمعنوية، وقد تم تخصيص الفصل الثالث من الاتفاقية إلى الأحكام الإجرائية التي تتمثل أساسا في نطاق تطبيق الأحكام الإجرائية التحفظ العاجل على البيانات المخزنة في تقنية المعلومات، التحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين، أمر تسليم المعلومات، تفتيش المعلومات المخزنة، ضبط المعلومات المخزنة، الجمع الفوري لمعلومات تتبع المستخدمين، واعتراض معلومات المحتوى، في حين خصص الفصل الرابع للتعاون القانوني والقضائي المتمثل في تسليم المجرمين، المساعدة المتبادلة، المعلومات العرضية المتلقاة، الإجراءات المتعلقة بطلبات التعاون والمساعدة المتبادلة وحالات رفض المساعدة، الحفظ العاجل للمعلومات المخزنة على أنظمة المعلومات، الكشف العاجل لمعلومات تتبع المستخدمين المحفوظة، التعاون والمساعدة الثنائية المتعلقة بالوصول إلى معلومات تقنية المعلومات المخزنة، الوصول إلى معلومات تقنية المعلومات عبر الحدود، التعاون والمساعدة الثنائية بخصوص الجمع الفوري لمعلومات تتبع المستخدمين، التعاون والمساعدة الثنائية فيما يخص المعلومات المتعلقة بالمحتوى.

وبنظرة عامة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، يلاحظ أنها شملت كافة المسائل اللازمة لمكافحة جرائم التكنولوجيا الحديثة بشكل عام، من حيث الصور الإجرامية، ومجالات التعاون القانوني والقضائي التي تتناسب وطبيعة الجرائم المعلوماتية من سرعة في جمع الأدلة وملاحقة المجرمين، وهو ما يكسبها قيمة وفاعلية في مجال مكافحة تلك الجرائم، ومن زاوية أخرى فإن هذه الاتفاقية تعد بمثابة حافز للدول التي مازالت تعاني فراغا أو قصورا تشريعيا يستوجب أن يعالج، تنفيذا لالتزامها بهذه الاتفاقية نظرا لإلزامية نصوصها لكافة الدول الموقعة عليها

بالإضافة إلى ما تقدم يلاحظ تأثر هذه الاتفاقية، بنظيرتها الأوربية –اتفاقية بودابست الخاصة بالجرائم المعلوماتية 2001– بل تكاد تتطابق معها في معظم نصوصها، لذا نقترح أنه طالما تلك الاتفاقية تحمل ذات المبادئ المقبولة لدى الدول العربية، نحث على قيام الدول العربية بالانضمام إلى تلك الاتفاقية لما في ذلك من فائدة كبيرة لها خاصة على صعيد مجالات التعاون الدولي، من تسليم وملاحقة المجرمين وجمع الأدلة وغيرها، بما يمكن للدول العربية من التصدي للكم الهائل من الهجمات الإلكترونية أو المعلوماتية.

الفرع الثالث: أهم المؤسسات الدولية لمكافحة جرائم التكنولوجيا الحديثة

بالرغم من التطرق إلى الإطار القانوني المتمثل في الاتفاقيات المبرمة لمواجهة الإجرام التكنولوجي الحديث، وكذا عقد المؤتمرات وما يصدر عنها من توصيات إلا أن هذه الجهود تبقى غير كافية، ما يتطلب جهودا أخرى تقوم بمحاولة الكشف عن جرائم التكنولوجيا الحديثة ومتابعة المجرمين بالإضافة إلى طرق أخرى تسهم في الحد من ارتكاب هذه الجرائم.

البند الأول: مركز الشكاوى الخاص بجرائم التكنولوجيا الحديثة

يعتبر هذا المركز من أهم الأطر المؤسسية لمكافحة الجرائم المتصلة بالتكنولوجيا الحديثة، فالنظام المعروف باسم (IC3) هو

كناية عن نظام تبليغ وإحالة لشكاوى الناس في الولايات المتحدة الأمريكية والعالم أجمع ضد الجرائم المرتبطة بالإنترنت، يتلقى المركز المشار إليه استمارة الشكاوى مرسلة على الإنترنت وبواسطة فريق من الموظفين والمحللين والجمهور ووكالات فرض تطبيق القوانين الأمريكية والدولية التي تحقق في الجرائم المتصلة بالتكنولوجيا الحديثة[1].

أولا: هيكلية المركز، نشأ مركز الشكاوى الخاصة بالجرائم المعلوماتية كمفهوم سنة 1998 بإدراك ملائم بأن الجريمة بدأت تدخل الإنترنت، لأن الأعمال التجارية والمالية كانت قد بدأت تتم عبر الإنترنت وأن مكتب التحقيقات الفدرالي أراد أن يكون قادرا على تعقب هذه النشاطات وعلى تطوير تقنيات تحقيق خاصة بجرائم التكنولوجيا الحديثة، ولم يكن هناك آنذاك أي مكان يمكن للناس التبليغ فيه عن هذه الجرائم وأراد مكتب التحقيقات الفدرالي التمييز بين الجرائم المتصلة بالإنترنت والنشاطات الإجرامية الأخرى التي تبلغ عنها عادة الشرطة، المحلية ومكتب التحقيقات الفدرالي والوكالات الأخرى التي تطبق القوانين الفدرالية وهيئة التجارة الفدرالية والمكتب الأمريكي للتفتيش وهو الشعبة التي تطبق القوانين المتعلقة بمصلحة البريد الأمريكية وغيرها من الوكالات.

وقد تم تأسيس أول مكتب للمركز سنة 1999 في مورغانتون بولاية واست فيرجينيا وسمي مركز شكاوى الاحتيال عبر الإنترنت، وكان المكتب عبارة عن شراكة بين مكتب التحقيقات الفدرالي والمركز القومي لجرائم موظفي المكاتب، وهذا الأخير مؤسسة لا تبغي الربح وهي متعاقدة مع وزارة العدل الأمريكية مهمتها الأساسية تحسين قدرات موظفي أجهزة تطبيق القانون على صعيد الولاية، والصعيد المحلي على اكتشاف جرائم المعلوماتية أو الجرائم الاقتصادية ومعالجة أمرها[2].

وقد أصبح هناك اليوم في مركز الشكاوى القائم بفيرمونت بفيرجينيا موظفين فدراليين ومحللين من القطاع الأكاديمي وقطاع صناعة الكمبيوتر وخدمات الإنترنت يتلقون الشكاوى المتعلقة بجرائم الإنترنت من الجمهور، ثم يقومون بالبحث في الشكاوى وإعداد ملفها وإحالتها إلى وكالات تطبيق القانون الفدرالية والمحلية والتابعة للولايات وإلى أجهزة تطبيق القانون الدولية أو الوكالات التنظيمية وفرق العمل التي تشارك فيها عدة وكالات للقيام بالتحقيق فيها، وبإمكان الناس من كافة أنحاء العالم تقديم شكاوى بواسطة موقع مركز الشكاوى الخاصة بالجرائم على الإنترنت[3]، ويطلب الموقع اسم الشخص وعنوانه البريدي ورقم هاتفه، إضافة إلى اسم وعنوان ورقم الهاتف والعنوان الإلكتروني إذا كانت متوفرة للشخص أو المنظمة المشتبه بقيامه بنشاط إجرامي علاوة على تفاصيل تتعلق بكيفية وقوع الجريمة حسب إعتقاد مقدم الشكوى ووقت وسبب إعتقاده بوقوعها، بالإضافة إلى أي معلومات أخرى تدعم الشكوى[4].

ثانيا: نطاق أعمال مركز الشكاوى الخاص بالجرائم المعلوماتية في العالم، يهدف المركز أساسا إلى أخذ شكوى المواطن الفرد التي قد تتعلق بجريمة تنجم عنها أضرار مادية في حدود معينة، ويساعد أحيانا وكالات تطبيق القانون من خلال إجراء

---

[1] عبد الله عبد الكريم، جرائم المعلوماتية والإنترنت، الجرائم الإلكترونية، دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والإنترنت مع الاشارة إلى جهود مكافحتها محليا وعربيا ودوليا، المرجع السابق، ص115.

[2] أمير فرج يوسف، المرجع السابق، ص114.

[3] www.ic3.gov

[4] عبد الله عبد الكريم، جرائم المعلوماتية والإنترنت، الجرائم الإلكترونية، دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والإنترنت مع الاشارة إلى جهود مكافحتها محليا وعربيا ودوليا، المرجع السابق، ص117.

أبحاث وإعداد ملف القضية الأولي، وقد وجد محققو المركز خلال السنتين والنصف الأوليين من عمر المشروع وعلى الرغم من جهود إعداد القضايا وإحالتها بسرعة إلى وكالات تطبيق القوانين، أن فرق العمل الخاصة بمكافحة الجرائم المتصلة بالتكنولوجيا الحديثة لم تكن جميعها مجهزة لمتابعة هذه الجرائم أو التحقيق فيها بسرعة، وقد لا تملك بعض فرق العمل هذه القدرة على القيام بعمليات سرية أو قد لا تملك التجهيزات اللازمة لاقتفاء الآثار الرقمية للأدلة الجرمية التي يحولها إليها مركز الشكاوى، لذلك أصبح من المهم جدا بالنسبة إلى هذا المركز أن يطور ويتعقب آثار الجرائم ثم يتوصل إلى إعداد ملف القضية الأولي[1].

في هذا الصدد، انضم محققون ومحللون يعمل الكثير منهم على قضايا جرائم التكنولوجيا الحديثة لجمع المعلومات لإعداد ملفات قضايا قانونية ذات شأن وبمساعدة وكالات تطبيق القانون في جميع أنحاء العالم على اكتشاف هذا النوع من الجرائم ومحاربتها وذلك بالتوصل إلى معرفة المصدر الذي تنبثق منه الجريمة، ومن يقف وراءها، وطريقة محاربتها[2]، كما يعمل مركز الشكاوى الخاص بجرائم الإنترنت أيضا مع منظمات دولية مثل هيئة الجرائم الاقتصادية والمالية في نيجيريا، حيث توجد مستويات عالية من الجرائم الاقتصادية والمالية كتبييض الأموال والاحتيال بقبض أموال مسبقة لمشاريع وهمية، أو ما يسمى احتيال 419 مما كانت له عواقب سلبية شديدة على ذلك البلد.

وتجمع هذه الجريمة التي أطلق عليها هذا الاسم لخرقها الفقرة 419 من مدونة القوانين الجنائية النيجيرية، ما بين جرم انتحال الشخصية وتشكيلة متنوعة من مؤامرات قبض الأموال مسبقا لمشاريع وهمية، فالضحية المحتملة تتلقى رسالة إلكترونية أو فاكس من أشخاص يدعون أنهم موظفون حكوميون نيجيريون أو أجانب يطلبون فيها المساعدة في إيداع مبالغ طائلة من المال في حسابات في مصارف خارجية، عارضين حصة من الأموال مقابل ذلك، ويعتمد المخطط على إقناع الضحية الراغبة في التعاون بإرسال مبلغ من المال إلى كاتب الرسالة على دفعات لأسباب متنوعة، وقد أدى خطر هذه الجرائم في نيجيريا إلى تأسيس لجنة الجرائم الاقتصادية والمالية هناك، وخلال السنة ونصف قام مركز الشكاوى الخاص بجرائم الإنترنت بعدة عمليات صودرت فيها بضائع وتم إلقاء القبض على أشخاص في إفريقيا الغربية نتيجة لهذا التحالف بين المركز ولجنة الجرائم الاقتصادية والمالية ونتيجة لتحالفات أخرى[3].

ويعمل مركز الشكاوى عن كثب أيضا مع المنظمة الكندية المسماة بالإبلاغ عن الجرائم الاقتصادية على خط الإنترنت ويدير هذه المنظمة المركز القومي للجرائم المكتبية في كندا وتدعمها شرطة الخيالة الملكية الكندية ووكالات أخرى، وتنطوي منظمة الإبلاغ عن الجرائم على شراكة متكاملة بين وكالات تطبيق القوانين الدولية والفدرالية والإقليمية من جهة، وبين المسؤولين عن وضع وتطبيق أنظمة العمل والمنظمات التجارية الخاصة التي لها مصلحة تحقيقية مشروعة في تلقي شكاوى الجرائم الاقتصادية من جهة أخرى، وهناك أيضا مجموعة متنامية من الوكالات الدولية المنخرطة لمحاربة الجرائم لامتصلة بالتكنولوجيا الحديثة.

ويعمل مركز الشكاوى الخاص بالجرائم المتصلة بالتكنولوجيا الحديثة مع مسؤولين عن تطبيق القانون في بلدان عديدة بينها

---

[1] أمير فرج يوسف، المرجع السابق، ص118.

[2] عبد الله عبد الكريم، جرائم المعلوماتية والإنترنت، الجرائم الإلكترونية، دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والإنترنت مع الاشارة إلى جهود مكافحتها محليا وعربيا ودوليا، المرجع السابق، ص119.

[3] أمير فرج يوسف، المرجع السابق، ص121 و122.

أستراليا والمملكة المتحدة، كما يحضر ممثلو مركز الشكاوى أيضا اجتماعات دورية للمجموعة الفرعية حول جرائم التكنولوجيا المتقدمة التابعة لمجموعة الثماني (كندا، فرنسا، ألمانيا، إيطاليا، اليابان، روسيا، المملكة المتحدة، الولايات المتحدة)، ويعمل قسم من هذه المجموعة الفرعية على محاربة هذه الجرائم وتعزيز التحقيقات بشأنها.

ومشروع الشكاوى الخاص بجرائم الإنترنت (IC3)، ووحدة مبادرات جرائم الإنترنت ودمج مواردها هما بمثابة عمل متطور ومتقدم باستمرار، وأثناء هذا التقدم يراجع موظفو ومحللو مركز الشكاوى ما أثبت نجاحه وما ثبت فشله من إجراءات، ويسعون باستمرار لتأمين مساعدة الخبراء والمصادر التي تزودهم بمعلومات استخباراتية ليصبحوا أكثر فطنة بخصوص هذا النوع من الجرائم ولكي يتعلموا كيف يمكنهم محاربتها بصورة أكثر فعالية، فهذه هي مهمة مركز الشكاوى الدائمة التي لا تتغير.

فبالرغم من عالمية هذا المركز والخدمات التي يقدمها، إلا أن تطبيقاته على أرض الواقع تبقى صعبة للغاية، وهذا راجع إلى الطبيعة الخاصة بجرائم التكنولوجيا الحديثة التي يتم فيها الاعتداء على معطيات وبيانات غير ملموسة من خلال وسائل التكنولوجيا وشبكة الإنترنت مما يصعب معه تحديد مرتكبها وفي حالة القبض عليه فأي قانون يكون واجب التطبيق باعتبارها جريمة عابرة للقارات، وما يزيد الأمر تعقيدا عدم التبليغ عنها من طرف الشخص المتضرر.

البند الثاني: الاتحاد الدولي للملكية الفكرية

يعد الاتحاد الدولي للملكية الفكرية من الهيئات الدولية التي تعنى بأمور الملكية الفكرية وجرائم التكنولوجيا الحديثة ومقرها في الجامعة الأمريكية بواشنطن، وهو عبارة عن جهة خاصة تشكلت في عام 1984 في الولايات المتحدة الأمريكية، ويتكون من اتحاد الناشرين الأمريكيين واتحاد تبادل البرامج الرقمية، اتحاد تسويق الأفلام الأمريكية واتحاد الصور المتحركة واتحاد تجارة البرامج واتحاد ناشري الموسيقى الوطنية واتحاد صناعة التسجيل في أمريكا وموقعه على شبكة الإنترنت[1]، ويدخل في اهتمامات الاتحاد ما يلي:

– نشر دراسات وإحصائيات منتظمة تتعلق بحجم خسائر الدول من جراء أعمال القرصنة وخاصة تلك المتعلقة بالبرامج.

– مناقشة الأحكام المتصلة بحماية حقوق الملكية الفكرية وفقا لاتفاقية تريبس وبيان نقاط الضعف فيها، كعدم إمكانية التفتيش في قيمة الخصم وانخفاض قيمة التعويضات التي يفرضها القانون وعدم إمكانية إلقاء الحجز على الآلات المستخدمة في الاعتداء (القرصنة) وعدم عقاب المستخدم النهائي لبرامج الحاسب الآلي التي تمت قرصنتها[2].

يتركز اهتمام الاتحاد على القرصنة باعتبارها عائقا أمام التجارة التي يمكن مواجهتها من خلال اتخاذ قرار الإجراءات الفورية ضد القطاع الأكبر من القراصنة التجاريين وفرض عقوبات رادعة وتطبيق الالتزامات المفروضة وفقا لأحكام اتفاقية تريبس ووضع أساس متكامل من خلال إتاحة الإجراءات المدنية والإدارية والجنائية لتنفيذ القانون بصورة فعالة ضد أشكال القرصنة.

وتعتبر جامعة ستانفورد في الولايات المتحدة الأمريكية من المؤسسات العلمية الرائدة على مستوى العالمفي هذا الصدد وتضم الجامعة معهدا متخصصا في مجال إحصائيات الإجرام ورصده ونشر العديد من الإحصائيات على مستوى العالم استعان بها

[1] http://www.iipa.com

[2] محمود أحمد عبابنة، المرجع السابق، ص175.

الدارسون في مجال القانون الجنائي، وفي الآونة الأخيرة تزايد اهتمام المعهد بجرائم التقنية العالية ونشر العديد من الدراسات والإحصائيات التي تبين نسبة الإجرام التكنولوجي الحديث وأصنافه.

وقد قامت الجامعة أيضا بعقد العديد من المؤتمرات الدولية بهذا الخصوص وأبرزها المؤتمر الذي عقد في 06 و07 ديسمبر 1999 بمشاركة العديد من الهيئات والمنظمات الدولية والممثلين القانونيين للولايات، وفي هذا المؤتمر تم تقديم اقتراح لاتفاقية دولية لتعزيز الحماية من الإرهاب وجرائم التكنولوجيا الحديثة، وقدم هذا الاقتراح باجتماع معهد هوفر والاتحاد البحثي حول أمن المعلومات وسياستها ومركز الأمن والتعاون الدولي وجامعة ستانفورد، وتم اقتراح هذه الاتفاقية قياسا على اتفاقية المجلس الأوروبي ولكنها تختلف عنها في أنها تخص الولايات المتحدة الأمريكية فيما بينها.

وفي معرض بيان المؤتمرين لمدى حاجتهم إلى مثل هذه الاتفاقية متعددة الأطراف أشاروا إلى أن جرائم تقنية المعلومات من الجرائم العالمية، وبالتالي تحتاج إلى رد فعل عالمي لمواجهتها، كما أن مرتكبي هذه الجرائم استغلوا ضعف القوانين وهشاشة التدابير المتخذة في الولايات المتحدة الأمريكية وكشفوا لها أن مخاطر هذه الجرائم تفوق قدرتهم الفردية والثنائية لمواجهتها كما أشاروا إلى وجوب تكاتف الولايات المتحدة الأمريكية وتعاونها في مجال التحقيق وتسليم المجرمين تمهيدا لمقاضاتهم في ولاياتهم[1].

وعليه ومن خلال تتبع الجهود التي يبذلها الاتحاد الدولي للملكية الفكرية على المستويين الداخلي والخارجي، فإنه لا يستطيع أحد إنكار أهمية الدور الذي يلعبه من خلال الدراسات الجنائية والإحصائيات التي يقدمها وكذا بيان الجوانب الإجرائية اللازم اتخاذها للحد من القرصنة، بالإضافة إلى المجهودات التي تقوم بها جامعة ستانفورد في مجال اهتمامها بالإجرام التكنولوجي الحديث.

البند الثالث: اتحاد الشركات والكيانات الاقتصادية في مجال حماية أمنها الإلكتروني

تعد الكيانات الاقتصادية من أهم الأهداف المحتملة لأي عمليات إجرامية تتم عبر الوسائل التكنولوجية، وغالبا ما يكون الهدف من ارتكاب تلك الجرائم هو البحث عن أموال تلك الشركات الضخمة أو عما تخفيه من معلومات تريد الشركات الأخرى الحصول عليها في محاولة منها للتغلب على ما تعانيه من نقص في المعلومات الإلكترونية التي تساعدها على النهوض تكنولوجيا وتصبح في عداد الشركات الاقتصادية الكبرى بما يعود عليها بفوائد ضخمة، وعليه فغالبا ما تكون هذه الشركات هي الهدف الذي يلهث وراءه مرتكبوا جرائم التكنولوجيا الحديثة، كما قد يكون الهدف من الجرائم التي تتعرض لها تلك الشركات الاقتصادية الضخمة هو الحصول على معلومات هامة عنها للقيام بابتزازها والحصول منها على مبالغ مالية في مقابل عدم نشر ما تم الاستيلاء عليه من معلومات في الغالب يكون نشرها ضارا بالشركة ضررا بالغا، وعليه فإن الكثير من الكيانات الاقتصادية الهامة في العالم تتحد مع بعضها البعض في محاولة منها للقيام ببناء حائط صد إلكتروني مضاد لما قد تتعرض له من هجمات ومحاولات اختراق وقرصنة متعددة في ارتكاب الإجرام المتصلة بالتكنولوجيا الحديثة، ومكاسب تلك الكيانات الاقتصادية عظيمة من تعاونها مع بعضها البعض في هذا الأمر ومنها أن التعاون الذي يتم بينها وبين الكيانات الاقتصادية الأخرى يوفر لها قدرا كبيرا من الأموال فيما لو كانت ستقوم ببناء هذا الحائط المضاد بمفردها، فعندها كانت ستتحمل بمفردها ما تكلف من أموال دون أي مساعدة من أي جهة خارجية[2]، إضافة

[1] محمود أحمد عبابنة، المرجع السابق، ص176 و177.

[2] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص198.

إلى أن هذا الاتحاد يكون ائتلافا قويا في مواجهة تلك الهجمات على تلك الكيانات وبالتالي يجعلها أقوى عند مواجهة تلك الاختراقات وصدها وتعقب مرتكبيها.

كما أن تعاون تلك الشركات وعدم تحمل أي منها للتكاليف بمفردها يجعلها تستطيع القيام ببناء حائط منيع في مواجهة مرتكبي جرائم التكنولوجيا الحديثة، وبالتالي يصعب كثيرا من فرص اختراقه والنفاذ إلى تلك الشركات[1]، وعليه نجد أن تعاون الكيانات الاقتصادية الكبرى في مجال مكافحة هذه الجرائم يساعد كثيرا على حمايتها ويحافظ عليها من أي محاولات ابتزاز قد تتعرض لها إذا ما استطاع أي شخص النفاذ إلى معلوماتها والحصول عليها فعندئذ سيكون عليها أن تدفع له الكثير من الأموال لمنعه من نشر معلوماتها السرية التي قد تستفيد منها الشركات المنافسة لها في الأسواق العالمية أو التي قد تضر بالشركة ضررا بليغا إذا ما تم نشر تلك المعلومات[2].

البند الرابع: منظمة الشرطة الجنائية الدولية (إنتربول)[3]

يأخذ التعاون الدولي[4] لمكافحة الجريمة المتصلة بالتكنولوجيا الحديثة عدة صور كتوقيع الاتفاقيات الدولية وتنظيم المؤتمرات الدولية بالإضافة إلى تبادل المساعدة الشرطية والأمنية، حيث قطع التعاون الشرطي الدولي شوطا طويلا سواء على مستوى التعاون الثنائي أم على مستوى التعاون متعدد الأطراف، إقليميا وعالميا، وكان من أبرز العلامات على طريق هذا التعاون إنشاء منظمة الشرطة الجنائية الدولية إنتربول في 1923/09/07 ومقرها الحالي يوجد بليون في فرنسا[5]، وتعد من أهم المنظمات الناشطة في مجال مكافحة الجريمة نظرا إلى ما تقدمه من إمكانية تعقب وضبط مرتكبي الجرائم على اختلاف أنواعها أينما وجدوا وتسليمهم إلى الهيئات المختصة بغية محاكمتهم وتوقيع العقوبة المناسبة عليهم، وتضم حاليا 190 بلد عضو فيها، ويعمل لديها موظفون من جنسيات مختلفة وتباشر مهامها بأربع لغات رسمية (الإنجليزية، الفرنسية، الإسبانية، العربية).

كما ظهرت العديد من صور وأشكال ووسائل التعاون بين أجهزة الشرطة، وبرز من بين هذه الصور والوسائل بعض النماذج الهامة يذكر منها التعليم والتدريب الشرطي المتخصص والمعاونات الفنية، وتبادل المراجع والخبرات والبحوث، وربط شبكات الاتصال والمعلومات أين يجري الاتصال بين أجهزة العدالة الجنائية الوطنية بصفة عامة وأجهزة الشرطة بصفة خاصة وبين مثيلاتها في الدول الأخرى، وقد حاولت منظمة الإنتربول تيسير الاتصال بين هذه الأجهزة الشرطية عن طريق إنشاء شبكة اتصالات خاصة

---

[1] جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات، رؤية جديدة للجريمة الحديثة، دار البداية، الأردن، ط1، 2007، ص238.

[2] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص199.

[3] كان لفظ إنتربول في البداية عنوان المنظمة ومع تداول استخدامه أصبح اسمها الرسمي.

[4] التعاون الدولي هو تبادل العون والمساعدة وتضافر الجهود المشتركة بين طرفين دوليين أو أكثر لتحقيق نفع أو خدمة أو مصلحة مشتركة في مجال التصدي لمخاطر وتهديدات الإجرام وما يرتبط به من مجالات أخري؛ كمجال العدالة الجنائية، مجال الأمن، أو لتخطيط مشكلات الحدود والسيادة التي قد تعترض الجهود الوطنية لملاحقة المجرمين وتعقب مصادر التهديد سواء كانت هذه المساعدة المتبادلة قضائية أم تشريعية أم شرطية، موضوعية أم إجرائية. علاء الدين شحاتة، التعاون الدولي لمكافحة الجريمة، دراسة للاستراتيجية الوطنية للتعاون الدولي لمكافحة المخدرات، إيتراك للطباعة والنشر والتوزيع، مصر، ط1 2000، ص18.

[5] موقع المديرية العامة للأمن الوطني الإلكتروني، www.algeriepolice.dz

بالإضافة إلى التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف ومدها بالمعلومات المتوفرة لديها على إقليمها خاصة فيما تعلق منها بالجرائم المتصلة بالتكنولوجيا الحديثة المتشعبة في عدة دول[1].

وقد مرت جهود المنظمة في هذا المجال بالعديد من المراحل، إلى أن تم إنشاء عدة مراكز اتصالات إقليمية في عديد من المدن مثل طوكيو، نيوزيلندا، نيروبي وأذربيجان...إلخ، لتسهيل مرور الرسائل، ويضاف إلى ذلك مكتب إقليمي فرعي في بانكوك وبالنظر إلى تنوع أنظمة الدول المختلفة، فقد كان هناك خياران لأنظمة الاتصال داخل هذه الشبكة، أولهما هو نموذج يخصص للدول المركزية وتجرى الاتصالات العالمية للشرطة فيها من خلال الجمعية العامة واللجنة التنفيذية بواسطة السكرتارية العامة، والثاني للدول اللامركزية وتجري الاتصالات فيه مباشرة بين أجهزة الشرطة في الدول المختلفة[2].

وعلى غرار هذه المنظمة، أنشأ المجلس الأوربي في لوكسمبورج عام 1991 شرطة أوربية لتكون همزة وصل بين أجهزة الشرطة الوطنية في الدول المنظمة ولملاحقة الجناة في الجرائم العابرة للحدود ومنها بطبيعة الحال جرائم التكنولوجيا الحديثة وتعد صورة التعاون الأمني من أهم الصور في مجال مكافحة جرائم التكنولوجيا الحديثة، لاسيما أن أجهزة العدالة الجزائية ليست بنفس المستوى والجاهزية في جميع الدول وإنما هناك تفاوت فيما بينها، فبعض الدول متقدمة تقنيا وتكنولوجيا ولها صيت كبير في مواجهة هذه الجرائم تشريعيا وفنيا، والبعض الآخر يفتقد ذلك[3].

مما سبق، يتبين أن المنظمات والمراكز الدولية الخاصة بتتبع الجرائم المعلوماتية والكشف عنها وإلقاء القبض على مرتكبيها لها دور فعال في التصدي لهذه الجرائم، لكن يبقى دورها قاصرا عن تتبع كل الجرائم وهذا راجع إلى إحجام المجني عليهم عن التبليغ من جهة، والطابع العالمي لهذه الجرائم من جهة أخرى مما يستدعي تعاونا دوليا لتحقيق قانون جنائي موضوعي وإجرائي للحد من هذه الجرائم العابرة للقارات، وقد انضمت الجزائر إلى المنظمة الدولية للشرطة الجنائية (إنتربول) أثناء انعقاد الجمعية العامة للإنتربول في فنلندا خلال شهر أوت 1963، بمشاركة 53 بلدا.

المطلب الثاني: الجهود المبذولة على المستوى الداخلي

تحاول جهود دولية وأخرى إقليمية التصدي للجرائم المتصلة بالتكنولوجيا الحديثة حيث تسعى كل الدول جاهدة لمواكبة هذه الاتفاقيات الدولية وذلك بسن تشريعات جديدة تتلاءم والتطورات التكنولوجية الحاصلة، بالإضافة إلى الدور الذي يلعبه الإطار المؤسساتي في هذا المجال.

وعلى الرغم من هذه الجهود، إلا أنها تبقى غير كافية، مما يستدعي تعزيز التعاون بين الدول في جميع المجالات، وهذا لا يكون إلا بالانضمام إلى الاتفاقيات الدولية الخاصة بحماية حقوق الملكية الفكرية أو إبرام اتفاقية دولية تتضمن أهم المبادئ التي جاءت بها اتفاقية بودابست.

---

[1] علاء الدين شحاتة، المرجع السابق، ص111.

[2] Malcolm Anderson, Policing the World: Interpol and the Politics of International Police Co-operation, Clarendon Press, Oxford, United Kingdom, 1989, pp168-185.

[3] حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الإنترنت، مقال منشور على الموقع الإلكتروني: www.arablaws.com

بالإضافة إلى ذلك لابد أن يكون هناك توافق بين السياسة الجنائية الدولية والسياسة الجنائية الوطنية عن طريق التدخل التشريعي قصد تعديل النصوص القانونية أو تحديثها على نحو يتماشى مع المقتضيات العربية والدولية والمستجدات التي تعرفها الجريمة المتصلة بالتكنولوجيا الحديثة، حتى يسهل تتبع المجرمين في أي دولة والقبض عليهم أملا في القضاء على هذه الجرائم والحد من انتشارها.

لذلك فإن المجتمع الدولي أضحى اليوم في حاجة ماسة إلى تعزيز جميع سبل التعاون الدولي على كافة المستويات المحلية الإقليمية والدولية وفي جميع المجالات القانونية وكذا المؤسساتية لمواجهة فعالة وناجحة ضد الإجرام المتصل بالتكنولوجيا الحديثة.

الفرع الأول: أهم القوانين الخاصة للتصدي لجرائم التكنولوجيا الحديثة

حرص المشرع الجزائري على مواكبة التطور التكنولوجي الذي يشهده العالم وذلك من خلال عديد النصوص التي تطرقت للمعلوماتية سواء من جانب التنظيم أو من جانب الحماية والتجريم، وفيما يلي أهم النصوص الواردة في هذا الصدد.

أولا: في الدستور الجزائري، كفل الدستور الجزائري حماية الحقوق الأساسية والحريات الفردية، على أن تضمن الدولة عدم انتهاك حرمة الإنسان، وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات والإجراءات الجنائية وقوانين خاصة أخرى تحظر كل مساس بهذه الحقوق، ومن أهم المبادئ الدستورية العامة ما جاء في المادة 38 "الحريات الأساسية وحقوق الإنسان والمواطن مضمونة..."، إضافة إلى ما تضمنته المادة 44 بقولها: "حرية الابتكار الفكري والفني والعلمي مضمونة للمواطن، حقوق المؤلف يحميها القانون، لا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا بمقتضى أمر قضائي، الحريات الأكاديمية وحرية البحث العلمي مضمونة وتمارس في إطار القانون، تعمل الدولة على ترقية البحث العلمي وتثمينه خدمة للتنمية المستدامة للأمة"، وما جاء في نص المادة 46 "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة، لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية. ويعاقب القانون على انتهاك هذا الحكم، حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه"، بالإضافة إلى العديد من المواد التي جاءت لحماية الحريات الأساسية كتلك المتعلقة بضمان عدم انتهاك حرمة المسكن.

ثانيا: في القانون المدني[1]، نصت المادة 323 مكرر 1 من القانون المدني على أنه: "يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها، وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها"، فقد أسس المشرع من خلال هذا النص مبدأ التعادل الوظيفي، بين الكتابة في الشكل الإلكتروني والكتابة على الدعامة الورقية كما قد اعترفت المادة سالفة الذكر بالكتابة الإلكترونية في إثبات التصرفات والعقود من جهة وجعلتها معادلة في حجيتها للوثيقة المخطوطة على دعامة ورقية، أي لها نفس الأثر والفعالية في حجيتها وصحتها.

ثالثا: في قانون العقوبات، تدارك المشرع الجزائري خلال السنوات الأخيرة ولو نسبيا الفراغ القانوني في مجال الإجرام

[1] قانون رقم 05-10 مؤرخ في 13 جمادى الأولى 1426ھ الموافق لـ 20 يونيو 2005م، المعدل والمتمم للأمر رقم 75-58 مؤرخ في 20 رمضان 1395ھ الموافق لـ 26 سبتمبر 1975م، يتضمن القانون المدني، ج.ر، العدد 44، مؤرخة في 26 يونيو 2005.

المتصل بالتكنولوجيا الحديثة بموجب تعديل قانون العقوبات، والذي بموجبه جرم المشرع بعض الأفعال المتصلة بجرائم التكنولوجيا الحديثة، فبالرجوع إلى النصوص التقليدية لقانون العقوبات نلاحظ أن ظهور المعلوماتية وتطبيقاتها المتعددة أدى إلى ظهور مشاكل قانونية جديدة، أو ما يسمى بأزمة القانون الجنائي في مواجهة واقع المعلوماتية، فرض حلها البحث في الأوضاع القانونية القائمة ومدى ملائمتها لمواجهة هذه المشاكل، فالقانون الجنائي له مبادئه وأصوله وعلى رأسها مبدأ الشرعية والذي يتفرع عنه مبدأي التفسير الضيق وحصر القياس في مجال التجريم[1].

رابعا: قوانين الملكية الفكرية، نظرا للاعتداءات التي تتعرض لها مختلف المنتجات الفكرية عبر الإنترنت ارتأينا البحث في مدى إمكانية الحماية من خلال نصوص قانون الملكية الفكرية، وسنفصل في ذلك من خلال نقطتين أساسيتين:

1- من خلال قوانين الملكية الصناعية: تطرق المشرع الجزائري إلى تنظيم أحكام العلامات التجارية من خلال عدة قوانين آخرها الأمر رقم 03-06 والمتعلق بالعلامات[2].

نعلم أن كل برنامج يحمل اسما خاصا به، لذلك فقد عمد أصحاب البرامج إلى تسجيل هذا الاسم كعلامة تجارية للبرنامج ولما كانت هذه الحماية قاصرة على الاسم دون المحتوى فقد لجأ أصحاب البرامج إلى وضع الاسم مقترنا به، غير أن الحماية بأحكام العلامات التجارية قد تكون فعالة بالنسبة للنسخ البسيط، لكن الأمر ليس كذلك بالنسبة للنسخ المعقد.

كما نظم المشرع الجزائري أحكاما في الأمر رقم 03-07 المتعلق ببراءات الاختراع[3]، فقد عرفت المادة 02 من نفس الأمر الاختراع بأنه فكرة لمخترع تسمح عمليا بإيجاد حل لمشكل محدد في مجال التقنية، وبشأن الشروط التي يجب توافرها في الاختراع المتمثلة أساسا في شرط الابتكار، شرط الجدة، والقابلية للتطبيق الصناعي، إضافة إلى المشروعية؛ يتحصل المخترع في حال توافر هذه الشروط على براءة الاختراع وهي الوثيقة التي تمنحها الدولة للمخترع فتخول له حق استغلال اختراعه والتمتع بالحماية القانونية المقررة لهذا الغرض وذلك لمدة محدودة وبشروط معينة، تمنح هذه الشهادة في الجزائر من طرف المعهد الجزائري لحماية الملكية الصناعية.

وتجدر الإشارة هنا أن التشريعات المعاصرة بصفة عامة تستبعد البرامج المعلوماتية من مجال الحماية بواسطة براءات الاختراع لأحد السببين؛ إما تجرد البرامج من أي طابع صناعي، وإما صعوبة البحث في مدى جدة البرنامج لتقدير مدى استحقاق البرنامج للبراءة فليس من الهين توافر شرط الجدة في البرمجيات، كما أنه ليس من الهين إثبات توافر هذا الشرط، إذ يجب أن يكون لدى الجهة التي تقوم بفحص طلبات البراءة قدرا معقولا من الدراية لتقرر ما إذا كان قد سبق تقديم اختراعات مشابهة للاختراع المقدم الطلب بشأنه أم لا، لأن الأمر يتطلب أن تكون هذه الجهة على درجة عالية من الكفاءة والتمييز في المجالات التي تتولى بحثه.

---

[1] فشار عطاء الله، المرجع السابق، ص465.

[2] تجسدت هذه القوانين في الأمر رقم 66-57 مؤرخ في 1966/03/19، المتعلق بعلامات المصنع والعلامات التجارية، المعدل والمتمم بالأمر رقم 67-233 مؤرخ في 1967/10/19، المتضمن أحكام العلامات التجارية، والمعدل بالأمر رقم 03-06 مؤرخ في 19 جويلية 2003 المتعلق بالعلامات، ج.ر، العدد 44، مؤرخة في 23 جويلية 2003. وتعرف العلامات التجارية على أنها كل ما يتخذ من تسميات أو رموز أو أشكال توضع على البضائع التي يبيعها التاجر أو يصنعها المنتج أو يقوم بإصلاحها أو تجهيزها أو ختمها لتمييزها عن بقية المبيعات أو المصنوعات أو الخدمات، ويشترط في العلامة أن تكون مميزة وجديدة وغير مخالفة للنظام العام.

[3] أمر رقم 03-07 مؤرخ في 19 جمادى الأولى عام 1424ه الموافق لـ 19 يوليو 2003م، يتعلق ببراءات الاختراع، ج.ر، العدد 44، مؤرخة في 2003/07/23.

إضافة إلى التحفظ العملي لمنتجي برامج الحاسب على استعمال قوانين براءة الاختراع، ويتمثل هذا التحفظ في الإجراءات المعقدة للحصول على براءة الاختراع والتكلفة العالية والمدة الطويلة التي يستغرقها هذا التسجيل، فعمر البرنامج قصير نسبيا لا يتعدى الثلاث سنوات، بينما قد تمتد إجراءات تسجيل البراءة مثل ذلك أو أكثر، وعليه يمكن للغير الوصول إلى سر البرنامج واستغلاله قبل صدور البراءة، كما تجدر الإشارة إلى أن المشرع الجزائري قد استبعد البرامج المعلوماتية صراحة من مجال الحماية بواسطة براءات الاختراع وذلك طبقا للمادة 07 من الأمر رقم 03-07 المتضمن براءة الاختراع التي نصت على أنه: "لا تعد من قبيل الاختراعات في مفهوم هذا الأمر برامج الحاسوب".

2- من خلال قوانين الملكية الأدبية والفنية: شهد النصف الأخير من القرن العشرين تطورا ملحوظا في مجال الاتصال رافقه تطورا في وسائل نقل الإنتاج الفكري على اختلاف صوره من علوم وفنون وآداب، مما أوجد مصنفات جديدة جديرة بحماية حق المؤلف كانت محل اهتمام ودراسة من قبل المختصين في مجال الملكية الفكرية، وقد كان من أهم هذه المصنفات؛ المصنفات الخاصة ببرامج الحاسبات الإلكترونية، وقواعد البيانات التي كانت طبيعتها التقنية تختلف عن المصنفات التقليدية، الأمر الذي يتطلب متابعتها باستمرار ووضع قواعد قانونية محددة وثابتة لحمايتها[1].

اتجه المشرع الجزائري إلى الاعتراف صراحة بوصف المصنف المحمي لمصنفات الإعلام الآلي بموجب الأمر رقم 03-05 والذي يتبين من خلال استقرائنا له ما يلي:

أ- أن المشرع وسع قائمة المؤلفات المحمية حيث أدمج تطبيقات الإعلام الآلي ضمن المصنفات الأصلية، والتي عبر عنها بمصنفات قواعد البيانات وبرامج الإعلام الآلي، التي تمكن من القيام بنشاط علمي أو أي نشاط من نوع أخر أو الحصول على نتيجة خاصة من المعلومات التي تقرأ بآلة وتترجم باندفاعات إلكترونية، أما قواعد البيانات فهي عبارة عن مجموعة المصنفات والأساليب والقواعد، كما يمكن أن تشمل الوثائق المتعلقة بسير المعطيات وقد أشارت المادة 05 إلى قواعد البيانات بنصها: "تعتبر أيضا مصنفات محمية الأعمال الآتية؛ أعمال الترجمة والإقتباس والتوزيعات الموسيقية والمراجعات التحريرية... ".

ب- أن الحماية تحدد من 25 سنة إلى 50 سنة بعد وفاة المبدع، تماشيا مع اتفاقية برن التي حددت المدة الدنيا للحماية بـ 50 سنة، وبالتالي هذه المدة تشمل حتى المصنفات المعلوماتية[2].

ج- تشديد العقوبات الناجمة عن المساس بحقوق المؤلفين لاسيما مؤلفي المصنفات المعلوماتية، إذ أن تجريم الاعتداءات على الملكية الفكرية أخرجت بموجب الأمر رقم 03-05 من مظلة قانون العقوبات وأصبح لها تجريما خاصا، أين أقر لها عقوبتي الحبس والغرامة[3].

اتضح مما سبق أن المشرع الجزائري سواء بدافع توفير الحماية الجزائية للمعلوماتية أو بدوافع خارجية قد واكب إلى حد ما

---

[1] عمر مشهور حديثة الجازي، المبادئ الأساسية لقانون حق المؤلف، ندوة حق المؤلف في الأردن بين النظرية والتطبيق، كلية الحقوق، الجامعة الأردنية 12 كانون الثاني 2004، ص04.

[2] عبد القادر دوحة، محمد بن حاج الطاهر، مدى مواكبة المشرع الجزائري لتطور الجريمة الإلكتروني، الملتقى الوطني الأول، النظام القانوني للمجتمع الإلكتروني، معهد العلوم القانونية والإدارية، المركز الجامعي خميس مليانة، 11/10/09 مارس 2008.

[3] أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة للنشر، الجزائر، ط2، 2007، ص78 و79.

التطورات الحاصلة في المجال المعلوماتي بأن أخضع المعلوماتية لقانون الملكية الفكرية، موسعا بذلك من سلطة القاضي لتقرير العقوبة وذلك ضمانا وحماية لحق المؤلف ومالك الحقوق المجاورة.

خامسا: في قانون الإجراءات الجزائية الجزائري[1]، بالنسبة لمتابعة جرائم التكنولوجيا الحديثة فإنها تتم بمجموعة من الإجراءات مثلها مثل الجريمة التقليدية، كالتفتيش، المعاينة، استجواب المتهم، الضبط، التسرب، الشهادة والخبرة، غير أن المشرع الجزائري نص على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم المتصلة بالتكنولوجيا الحديثة في المادة 37 ق.إ.ج.

كما نص على التفتيش في المادة 47 من نفس القانون حيث اعتبر أن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه في القواعد الإجرائية العامة من حيث الشروط الشكلية والموضوعية، فالتفتيش وإن كان إجراء من إجراءات التحقيق قد أحاطه المشرع بقواعد صارمة، ونص على التوقيف للنظر في جريمة المساس بأنظمة المعالجة في المادة 51 وكذا على اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في المادة 65 مكرر 10، وطبقا لقانون الإجراءات الجزائية المعدل والمتمم في الفصل الرابع تحت عنوان اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، نصت المادة 65 مكرر5 على أنه في حالة ضرورة التحري أو التحقيق في مجموعة من الجرائم من ضمنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يجوز لوكيل الجمهورية المختص أن يأذن بالاعتراض ووضع ترتيبات تقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية في أماكن خاصة أو عامة أما بالنسبة لنصوص إجراءات التحقيق والمحاكمة تطبق عليها نفس الإجراءات.

سادسا: في قانون البريد والاتصالات الإلكترونية[2]، أنشئت بموجب هذا القانون سلطة ظبط مستقلة للبريد والاتصالات الإلكترونية تكلف بالقيام بضمان ضبط أسواق البريد والاتصالات الإلكترونية لحساب الدولة، فباستقراء القانون الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية نلاحظ مواكبة المشرع الجزائري إلى التطور التكنولوجي الذي شهدته التشريعات العالمية -إلى حد ما- فتطرق في المادة 10 منه إلى تحديد مفهوم كل من الاتصالات الإلكترونية، الأمن السبراني، الإنترنت والشبكات الإلكترونية المفتوحة للجمهور...إلخ، كما تضمنت المادة 97 و117 منه إلى ضرورة احترام شروط خصوصية البيانات والمعلومات التي تم ايصالها بواسطة شبكة الاتصالات الإلكترونية، شروط حماية الحياة الخاصة للمشتركين والبيانات ذات الطابع الشخصي المقتضيات التي تتطلبها ضرورة الحفاظ على النظام العام والدفاع الوطني والأمن العمومي، وحماية الأطفال خصوصا فيما يتعلق باستعمال خدمة الإنترنت.

كما ألزمت المادة 119 من نفس القانون متعاملي الاتصالات الإلكترونية باتخاذ التدابير التي من شأنها أن تضمن سرية المكالمات والمعلومات التي يحوزونها عن مشتركيهم، وألا يسمحوا بوضع أي ترتيبات بغرض اعتراض الاتصالات أو مراقبة المكالمات الهاتفية والوصلات والمحادثات والمبادلات الإلكترونية دون إذن مسبق من السلطة القضائية وفقا للتشريع المعمول به، ويجب عليهم أن يطلعوا أعوانهم على الالتزامات التي يخضعون لها وعلى العقوبات التي يتعرضون لها في حالة عدم احترامهم لهذه الأحكام.

---

[1] قانون رقم 19-10 مؤرخ في 14 ربيع الثاني 1441ه الموافق لـ 11 ديسمبر 2019م، يعدل ويتمم الأمر رقم 66-155 مؤرخ في 18 صفر 1386ه الموافق لـ 08 يونيو 1966م، يتضمن قانون الإجراءات الجزائية، ج.ر، العدد 78، مؤرخة في 18 ديسمبر 2019.

[2] قانون رقم 18-04 مؤرخ في 24 شعبان عام 1439ه الموافق لـ 10 مايو سنة 2018م، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية ج.ر، العدد 27، مؤرخة في 27 شعبان عام 1439ه الموافق لـ 13 مايو سنة 2018م.

وفي مجال الجرائم المتصلة بالتكنولوجيا الحديثة فقد جاء القانون بأحكام جزائية في المواد 164 وما يليها التي تضمنت في مجملها عقوبة الحبس والغرامة أو كليهما على كل شخص ينتهك سرية المراسلات المرسلة عن طريق الاتصالات الإلكترونية أو يفشي مضمونها أو ينشرها أو يستعملها دون ترخيص من صاحبها أو يخبر بوجودها، أو يفتحها، أو يحولها أو يخربها، أو يساعد في ارتكاب هذه الأفعال، كما تسري نفس العقوبات على كل متعامل للاتصالات الإلكترونية يحول بأي طريقة كانت المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الاتصالات الإلكترونية أو أمر أو ساعد في ارتكاب هذه الأفعال، ويمكن للجهة القضائية أيضا النطق بواحدة أو أكثر من العقوبات التكميلية المنصوص عليها في المادة 09 من قانون العقوبات.

سابعا: في قانون التأمينات الاجتماعية[1]، قد تطرق هذا القانون كذلك إلى تنظيم الجريمة المتصلة بالتكنولوجيا الحديثة من خلال هيئات الضمان الاجتماعي في نصوص قانونية عديدة تخص البطاقة الإلكترونية التي تسلم للمؤمن له اجتماعيا مجانا بسبب العلاج وهي صالحة في كل التراب الوطني، وكذا للجزاءات المقررة في حالة الاستعمال غير المشروع أو من يقوم عن طريق الغش بتعديل أو نسخ أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني المهني الصحي للبطاقة الإلكترونية حسب المادة 04 من نفس القانون.

ثامنا: في القانون الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين[2]، تم استحداث هذا القانون بهدف مسايرة التطور التكنولوجي على المستوى العالمي لاسيما في الجانب الاقتصادي، إضافة إلى تفعيل مشروع الحكومة الإلكترونية الذي تسعى الدولة إلى تجسيده في أقرب وقت.

يحدد هذا القانون من جهة مجمل الإجراءات الواجب اتخاذها في هذا الصدد والجهات المكلفة بذلك ومن جهة ثانية نص على مختلف التعريفات والأحكام المنظمة لعمليتي إنشاء واستغلال كل من التوقيع والتصديق الإلكترونيين، وتم تخصيص فصل للأحكام الجزائية في المواد من 66 إلى 75 مستحدثا بذلك جزاءات جديدة تتمثل في الإدلاء بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني موصوفة، الإخلال بالتزام إعلام السلطة الاقتصادية بالتوقف عن نشاط خدمات التصديق الإلكتروني في الآجال المحددة حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوفة خاصة بالغير، الإخلال عمدا بالتزام تحديد هوية طالب شهادة تصديق إلكتروني موصوفة، أداء خدمات التصديق الإلكتروني للجمهور دون ترخيص أو بعد سحب الترخيص، وكذا كشف معلومات سرية من قبل الشخص المكلف بالتدقيق اطلع عليها أثناء قيامه بالتدقيق واستعمال شهادة التصديق الإلكتروني الموصوفة لغير الأغراض التي منحت من أجلها، ومعاقبة الشخص المعنوي عن الجرائم سالفة الذكر.

تاسعا: في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، دفع القصور الذي عرفه قانون العقوبات المتضمن حماية جزائية نسبية لأنظمة المعلومات من خلال تجريم مختلف أنواع الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات بالمشرع الجزائري إلى سد الفراغ التشريعي الذي يعرفه مجال الجرائم المتعلقة بوسائل الإعلام والاتصال وخاصة الجرائم الناشئة عن

---

[1] قانون رقم 08-01 مؤرخ في 15 محرم عام 1429ھ الموافق لـ 23 يناير 2008، ج.ر، العدد 04، مؤرخة في 19 محرم عام 1249ھ الموافق لـ 27 يناير 2008م، يتمم القانون رقم 83-11 مؤرخ في 21 رمضان عام 1403ھ الموافق لـ 02 يوليو 1983م والمتعلق بالتأمينات الاجتماعية.

[2] قانون رقم 15-04 مؤرخ في 11 ربيع الثاني 1436ھ الموافق لـ 01 فبراير 2015م، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين ج.ر، العدد 06، مؤرخة في 20 ربيع الثاني عام 1436ھ الموافق لـ 10 فبراير 2015م.

الاستخدام غير المشروع لشبكة الإنترنت من خلال سن القانون رقم 09-04 سالف الذكر، وذلك بوضع هذا القانون من أجل تعزيز القواعد السابقة من خلال وضع إطار قانوني أكثر ملائمة مع خصوصية الجريمة المتصلة بتكنولوجيا المعلومات الحديثة.

كما تكمن أهمية هذا القانون في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها، من هنا أخذ المشرع بعين الاعتبار الصعوبات التي تثيرها المصطلحات القانونية المتعلقة بهذه المادة، لذلك تم اختيار عنوان القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حتى لا يكون النص مرتبطا بتقنيات تشهد تطورا مستمرا بقدر ما يرتبط بالأهداف والغايات التي ترمي إليها هذه التكنولوجيا، كما أن التركيز على مجالي الإعلام والاتصال بين مقاصد النص الذي يهدف إلى جعل المتعاملين في مجال الاتصالات السلكية واللاسلكية شركاء في مكافحة هذا الشكل من الإجرام والوقاية منه[1].

يحتوي القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على ستة فصول يمكن تلخيصها فيما يلي:

- الفصل الأول: نص على الأحكام العامة التي تبين الأهداف المتوخاة من القانون وتحدد مفهوم مصطلح التقنية الواردة وكذا مجال تطبيق أحكامها[2].
- الفصل الثاني: جسد في المادة 04 أحكاما خاصة بمراقبة الاتصالات الإلكترونية، وقد راعى في وضع هذه القواعد خطورة التهديدات المحتملة وأهمية المصالح المحمية، فنص القانون على أربعة حالات يسمح فيها للسلطات الأمنية بممارسة الرقابة على المراسلات والاتصالات الإلكترونية، منها الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب والجرائم التي تمس بأمن الدولة وكذلك في حال توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام، ولمقتضيات التحريات والتحقيقات القضائية، عندما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية وفي إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.
- الفصل الثالث: تضمن القواعد الإجرائية الخاصة بالتفتيش والحجز في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وذلك وفقا للمعايير العالمية المعمول بها في هذا الشأن مع مراعاة ما تضمنه قانون الإجراءات الجزائية من مبادئ عامة وعلى هذا الأساس يجوز للجهات القضائية وضباط الشرطة القضائية الدخول والتفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها، مع إمكانية اللجوء إلى مساعدة السلطات الأجنبية المختصة من أجل الحصول على المعطيات المبحوث عنها في منظومة معلوماتية تقع في بلد أجنبي، ويسمح القانون للمحققين باستنساخ المعطيات محل البحث في حال تبين جدوى المعلومات المخزنة في الكشف عن الجرائم أو مرتكبيها[3].
- الفصل الرابع: تطرق إلى التزامات المتعاملين في مجال الاتصالات الإلكترونية وذلك من خلال تحديد الالتزامات التي تقع

---

[1] الأزرق عبد الله، أحمد عمراني، نظام المعلومات في القانون الجزائري واقع وآفاق، المؤتمر السادس لجمعية المكتبات والمعلومات السعودية، البيئة المعلوماتية الأمنة، المفاهيم والتشريعات والتطبيقات، الرياض، 06 و07 أفريل 2010.

[2] المواد 01، 02 و03 من قانون رقم 09-04.

[3] فشار عطاء الله، المرجع السابق، ص35.

على عاتق المتعاملين في الاتصالات الإلكترونية لاسيما إلزامية حفظ المعطيات المتعلقة بحركة السير التي من شأنها المساعدة في الكشف عن الجرائم ومرتكبيها، كما أعطى هذا القانون لمقدمي الخدمات دورا إيجابيا ومساعدا للسلطات العمومية في مواجهة الجرائم وكشف مرتكبيها[1]، حيث ألزمهم بالتدخل الفوري بمجرد العلم بطريقة مباشرة أو غير مباشرة لسحب المحتويات التي بإمكانهم الإطلاع عليها والمخالفة للقانون، النظام العام، والآداب العامة، ولتخزينها وجعل الدخول إليها غير ممكن ووضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحتويها وإخطار المشتركين لديهم بوجودها.

- الفصل الخامس: أشار إلى الهيئة الوطنية للوقاية من الإجرام المتصل بتكنولوجيات الإعلام والاتصال ومكافحتها، إذ نص القانون على إنشاء هيئة وطنية ذات وظيفة تنسيقية في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في المادتين 13 و14، وقد تمت الإحالة على التنظيم فيما يخص تحديد كيفية تشكيل وتنظيم هذه الهيئة.
- كما نص الفصل السادس على التعاون والمساعدة القضائية الدولية، إذ تناول قواعد الاختصاص القضائي فهو فضلا عن قواعد الاختصاص العادية فقد تم توسيع اختصاص المحاكم الجزائية للنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال التي ترتكب من طرف الرعايا الأجانب عندما تكون المصالح الاستراتيجية للجزائر مستهدفة.

أما فيما يتعلق بالتعاون الدولي في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال فنجد أنه يقوم على مجموعة من المبادئ العامة، خاصة ما يتعلق منها بالمساعدة وتبادل المعلومات، حيث تم اعتماد مبدأ التعاون على أساس المعاملة بالمثل[2].

يعتبر القانون رقم 09-04 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها نطاقا شاملا في مجال مكافحة الجرائم المتصلة بالتكنولوجيا الحديثة، حيث جاء تجريمه للأفعال المخالفة للقانون والتي ترتكب عبر وسائل الاتصال والتواصل عاما وبالتالي فهو يطبق على كل التكنولوجيات الجديدة والقديمة بما فيها شبكة الإنترنت وعلى كل تقنية تظهر مستقبلا.

الفرع الثاني: أهم الهياكل الخاصة للتصدي لجرائم التكنولوجيا الحديثة

تتم عملية مراقبة وكشف ومعاقبة مرتكبي جرائم التكنولوجيا الحديثة عبر مجموعة من الهيئات الخاصة والمؤسسات.

البند الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

تضمن القانون رقم 09-04 القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ونص في مادته 13 منه: "تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم".

---

[1] المواد من 10 إلى 12 من قانون رقم 09-04.

[2] الأزرق عبد الله، أحمد عمراني، المرجع السابق.

وفي ذات القانون نصت المادة 14 منه على ما يلي: "تتولى الهيئة المذكورة في المادة 13 أعلاه، خصوصا المهام الآتية:

أ- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

ب- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية،

ج- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم".

وفي هذا الصدد صدر المرسوم الرئاسي رقم 19-172[1] الذي يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، والذي جاء في مضمونه ما يلي:

أولا: التعريف بالهيئة، عرف المرسوم الرئاسي الهيئة وفقا للمادة 02 على أنها مؤسسة عمومية ذات طابع إداري، تتمتع بالشخصية المعنوية والاستقلالية المالية توضع تحت سلطة وزارة الدفاع الوطني، ويحدد مقرها حسب ماجاء في نص المادة 03 بمدينة الجزائر، ويمكن نقله إلى أي مكان آخر من التراب الوطني بموجب قرار من وزير الدفاع الوطني.

ثانيا: تنظيم الهيئة وتشكيلها، قسم المشرع الجزائري الهيئة إلى قسمين:

1- مجلس التوجيه: بالرجوع إلى أحكام المادة 05، يترأس مجلس التوجيه وزير الدفاع الوطني أو ممثلا عنه.

أ- تشكيله، يتشكل من ممثلي وزارة الدفاع الوطني، الوزارة المكلفة بالداخلية، وزير العدل، والوزارة المكلفة بالاتصالات السلكية واللاسلكية.

ب- مهامه، يكلف مجلس التوجيه على الخصوص بما يلي:

- التداول حول الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- التداول حول مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.
- القيام دوريا بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال للتمكن من تحديد مضامين عمليات المراقبة الواجب القيام بها والأهداف المنشودة بدقة.
- اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- الموافقة على برنامج عمل الهيئة.
- إعداد نظامه الداخلي والمصادقة عليه أثناء أول اجتماع له.

---

[1] مرسوم رئاسي رقم 19-172 مؤرخ في 03 شوال عام 1440ه الموافق لـ 06 يونيو سنة 2019م، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج.ر، العدد 05، مؤرخة في 06 شوال عام 1440ه الموافق لـ 09 يونيو 2019م.

- دراسة التقرير السنوي لنشاطات الهيئة والمصادقة عليه.
- إبداء رأيه في كل مسألة تتصل بمهام الهيئة.
- تقديم كل اقتراح يتصل بمجال اختصاص الهيئة.
- المساهمة في ضبط المعايير القانونية في مجال اختصاصه.
- دراسة مشروع ميزانية الهيئة والموافقة عليه.

حسب المادة 07 من نفس القانون، يجتمع مجلس التوجيه في دورة عادية مرتين في السنة بناء على استدعاء من رئيسه ويمكنه أن يجتمع في دورة غير عادية كلما دعت الضرورة لذلك، بناء على استدعاء من رئيسه أو بطلب من أحد أعضائه أو من الدير العام للهيئة، وتحدد قواعد وكيفيات سير مجلس التوجيه بموجب قرار من وزير الدفاع الوطني.

2- **المديرية العامة:** يديرها مدير عام، وتنحصر مهامها فيما يلي:

- السهر على حسن سير الهيئة.
- إعداد مشروع ميزانية الهيئة.
- إعداد وتنفيذ برنامج عمل الهيئة.
- تنشيط وتنسيق ومتابعة ومراقبة أنشطة هياكل الهيئة.
- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- تبادل المعلومات مع مثيلاتها الأجنبية لغرض تجميع كل المعطيات المتعلقة بتحديد مكان مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرف عليهم.
- تحضير اجتماعات مجلس التوجيه.
- إعداد التقرير السنوي لنشاطات الهيئة.

وتتشكل المديرية العامة حسب ما جاءت به المادة 10 من مصالح مديرية الإدارة والوسائل ومصالح المديرية التقنية، التي تعد القلب النابض للمديرية العامة نتيجة للمهام الموكلة إليها، والمتمثلة أساسا في مهمة المراقبة الوقائية للاتصالات الإلكترونية في إطار الوقاية من الجرائم الموصوفة بالأفعال الإرهابية والتخريبية والاعتداء على أمن الدولة، بالإضافة إلى مساعدة السلطات القضائية ومصالح الشرطة القضائية بناء على طلبها، بما في ذلك في مجال الخبرات القضائية في إطار مكافحة الجريمة المتصلة بتكنولوجيات الإعلام والاتصال والجرائم التي تتطلب اللجوء إلى أساليب التحري الخاصة للهيئة، كما تتكفل بجمع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها وتتبعها بغرض استعمالها في الإجراءات القضائية، وتضع المديرية التقنية التجهيزات والوسائل والأجهزة التقنية الضرورية لتنفيذ مهامها على مستوى المنشآت القاعدية للمتعاملين ومقدمي الخدمات في مجال الاتصالات الملزمون بتقديم المساعدات الضرورية للمديرية التقنية من أجل تنفيذ مهامها على أكمل وجه.

البند الثاني: بعض الهيئات الأخرى الخاصة للتصدي لجرائم التكنولوجيا الحديثة

تتمثل أهم الهيئات الوطنية الخاصة للتصدي لجرائم التكنولوجيا الحديثة فيما يلي:

أولا: الهيئات القضائية الجزائية المتخصصة، تختص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقا للمواد 37، 40، و329 ق.إ.ج، تتمتع باختصاص إقليمي موسع، بحيث تنظر في القضايا المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة في الخارج حتى ولو كان مرتكبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني حسب المادة 15 من القانون رقم 09-04.

ثانيا: المديرية العامة للأمن الوطني، تتصدى هذه المديرية لجرائم التكنولوجيا الحديثة من عدة جوانب فلم تغفل عن الوقاية والتوعية، وهذا من خلال برمجتها لتنظيم دروس توعوية في مختلف الأطوار الدراسية وكذا المشاركة في الملتقيات والندوات الوطنية وجميع التظاهرات التي من شأنها توعية المواطن حول خطورة الجرائم المتصلة بالتكنولوجيا الحديثة، ودائما في إطار مكافحة جرائم التكنولوجيا الحديثة ونظرا للبعد الدولي الذي عادة ما يتخذه هذا النوع من الجرائم، أكدت عضويتها الفعالة في المنظمة الدولية للشرطة الجنائية إنتربول، هاته الأخيرة تتيح مجالات للتبادل المعلوماتي الدولي وتسهل الإجراءات القضائية المتعلقة بتسليم المجرمين وكذا مباشرة الإنابات القضائية الدولية ونشر أوامر القبض للمبحوث عنهم دوليا.

ثالثا: المعهد الوطني للأدلة الجنائية وعلم الإجرام، هو مؤسسة عمومية ذات طابع إداري تحت الوصاية المباشرة لوزير الدفاع الوطني مقرها بالجزائر العاصمة، مكلفة بالمهام التالية:

- إجراء الخبرات والفحوص العلمية في إطار التحريات الأولية والتحقيقات القضائية وهذا بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات والجنح.
- ضمان المساعدة العلمية أثناء القيام بالتحريات المعقدة باستخدام مناهج الشرطة العلمية.
- المشاركة في الدراسات والتحاليل المتعلقة بالوقاية والتقليل من كل أشكال الإجرام.
- تصميم وإنجاز بنوك المعطيات.
- المشاركة في تحديد سياسة جنائية مثلى لمكافحة الإجرام.
- المبادرة وإجراء بحوث متعلقة بالإجرام باللجوء إلى التكنولوجيات الدقيقة.
- العمل على ترقية البحوث التطبيقية وأساليب التحريات التي أثبتت فعاليتها في ميادين علم الإجرام والأدلة الجنائية على الصعيدين الوطني والدولي.
- المشاركة في كل الملتقيات والمحاضرات أو الندوات على الصعيدين الوطني والدولي الضرورية لتطوير مستوى مستخدمي المعهد.
- المساهمة في تنظيم دورات الإتقان والتكوين ما بعد التدرج في تخصص العلوم الجنائية.
- تصور وضمان متابعة الأبحاث الموكلة إلى الغير.
- اختصاصات متنوعة لهدف واحد ألا وهو كشف خيوط الجريمة.

لتأدية مهامه على أكمل وجه، فإن المعهد الوطني للأدلة الجنائية وعلم الإجرام يحتوي على العديد من الأقسام والمصالح المختصة أهمها مصلحة الإعلام الآلي؛ على مستوى هذه المصلحة يتم رصد ومراقبة وتتبع عمليات الاختراق والقرصنة المعلوماتية وكذا اكتشاف المعلومات المسروقة وتفكيك البرامج المعلوماتية، وعليه يعتبر المعهد الوطني للأدلة الجنائية وعلم الإجرام أهم قلاع مكافحة الجريمة وتتبعها على مستوى الجزائر[1].

المبحث الثاني: دور الأجهزة الأمنية في التصدي لجرائم التكنولوجيا الحديثة

تتمتع كل دولة بمساحة جغرافية محددة، وتنتهي هذه المساحة عند أطراف حدودها التي تميزها عن غيرها من الدول المجاورة وتباشر كل دولة أعمال السيادة على أراضيها، وتهتم بتأمين حدودها الجغرافية وفرض سيادتها الكاملة على إقليمها.

ومع ظهور التقنيات التكنولوجية الحديثة، والانتشار والتوسع في استخدام شبكة الإنترنت لما يسهم به في سرعة تداول المعلومات والمراسلات، وتنفيذ الكثير من الأغراض الحياتية والعملية والعلمية، زادت معدلات ارتكاب جرائم التكنولوجيا الحديثة وتجاوزت حدود الإقليم الواحد وعبرت الحدود الجغرافية للدول، وللجرائم المتصلة بالتكنولوجيا الحديثة أضرارا جسيمة وتكاليف باهظة ونتائج تنعكس بالسلب على برامج التنمية الاجتماعية والاقتصادية، وتسبب خسائر على الممتلكات والأموال العامة والخاصة وتعوق حركة الإنسان وحريته، وتؤثر في الثقة بين مختلف فئات الشعب والأجهزة الأمنية بسبب الأضرار التي تلحقها بكافة أفراد المجتمع.

ونظرا لطبيعة خصائص هذه الجرائم كان لزاما على الدولة وضع هذه الجرائم المستحدثة نصب عينها، وتكليف السلطة التنفيذية بالتصدي لها، فيعد جهاز الشرطة من أهم الركائز التي تقوم عليها الدولة في مواجهة ومكافحة تلك الجرائم، وذلك بتأهيل وتدريب وتطوير العنصر البشرى عماد جهاز الشرطة، مع تطوير أساليب التحقيق والاعتماد على العلم والتكنولوجيا والتطوير؛ من خلال التخطيط السليم لمنظومة التحقيق ومكافحة هذه الجرائم، مع الاعتماد على المنظومة الإعلامية في تنمية الوعي المجتمعي حيث يلعب الإعلام دورا أساسيا في التوعية بالمخاطر التي تصيب كافة شرائح المجتمع بسبب قدرة الوسائل الإعلامية على الوصول إلى شريحة واسعة من الناس، وقدرتها على نشر الأفكار والحقائق والمعلومات، فالإعلام ضرورة حضارية يسهم بآلياته المتعددة في تنظيم واستقرار الحياة الاجتماعية.

كما تعتمد الدولة أيضا على دور المنظمات والكيانات الدولية في تحجيم وضبط الجرائم المعلوماتية، من خلال بعض الاتفاقيات الدولية وقواعد تسليم المجرمين، وذلك لما تشهده الساحة العالمية من جرائم معلوماتية عابرة للحدود رغم الصعوبات والتحديات التي تواجهها.

المطلب الأول: مواجهة السلطة التنفيذية لجرائم التكنولوجيا الحديثة

يظل منع الجريمة وسيلة لتحقيق غايات الأمن وبث الطمأنينة في المجتمعات، ومن هذا المنطلق فلابد أن تحيطه الدولة برعاية خاصة، من خلال بتسخير الإمكانات البشرية والمادية الأفضل نوعا والأكبر عددا في كافة مؤسسات الدولة ذات الصلة بمكافحة جرائم التكنولوجيا الحديثة.

[1] http://djamakamel.over-blog.com/2014/11/54609acd-fdbb.html

وقد اضطلعت بعض الأجهزة الأمنية للقيام بدورها السامي في منع الجريمة –محل دراستنا– وضبط مرتكبيها بالتطوير ومواكبة التقدم التكنولوجي بما يحمله من إيجابيات وسلبيات، وذلك من خلال إنشاء واستحداث إدارات متخصصة في مجال مكافحة الجرائم المتصلة بالتكنولوجيا الحديثة تصديا لها طبقا للعمل بالقوانين الموضوعة لمنع هذه الجرائم.

وقد اتجهت بعض الدول مثل الولايات المتحدة، ألمانيا، بريطانيا والصين إلى ضرورة إعداد قوات خاصة لمواجهة العدوان الإلكتروني، لوضع رؤية أمنية شاملة عن جرائم التكنولوجيا الحديثة، وذلك بتحديد الجناة وأدوارهم[1]، فلا تعتمد هذه القوات على التدريبات المادية التي يتلقاها رجال الشرطة للوصول إلى هذه المرتبة هنا، إنما تعتمد على قوة تكوين البناء العلمي والتكنولوجي لأفرادها، والمهمة التي تكلف بها تلك القوات هي مكافحة جرائم تقنية المعلومات الحديثة، بحيث يمكنهم القيام بأنشطة مطاردة المحتالين ومخترقي الأنظمة المعلوماتية على كافة مستوياتهم.

الفرع الأول: الجهات الأمنية المنوط بها مواجهة جرائم التكنولوجيا الحديثة

تمثل الشرطة التجسيد الطبيعي لسلطة المجتمع اللازمة للدفاع عن نفسه ضد كل من تسول له نفسه العبث بالقوانين والتعدي على الأمن العام الذي يحميه المشرع بالقوانين المختلفة، ومن هذا المنطلق، ومع تطور الجريمة وانتشار الجرائم المتصلة بالتكنولوجيا الحديثة، كان لزاما على الجهاز الأمني استحداث إدارات لمكافحة هذه الأنواع المستحدثة من الجرائم، تنفيذا لمراحل مواجهة تلك التحديات التي أفرزتها العولمة وانتشار التكنولوجيا الحديثة والاعتماد عليها في شتى المجالات.

البند الأول: مراحل وأدوات مواجهة الأجهزة الأمنية لجرائم التكنولوجيا الحديثة

مواكبة للتطور التقني، ولمواجهة الصور المستحدثة من الإجرام الإلكتروني، يجب اعتماد الجهات الأمنية المعنية بالمكافحة سياسة التقدم العلمي والتكنولوجي في مراحل مواجهة هذه الجرائم.

أولا: مراحل مكافحة الأجهزة الأمنية لجرائم التكنولوجيا الحديثة، تتمثل أهم مراحل المكافحة فيما يلي:

1– مرحلة ما قبل وقوع الجريمة: تعتمد الجهات الشرطية المنوط بها مكافحة الجرائم المتصلة بالتكنولوجيا الحديثة في عملها على اتخاذ بعض الإجراءات للحد منها وهي كالتالي:

أ –الإجراءات الوقائية، تشمل الإجراءات الوقائية فيما يلي:

– إعداد بحوث فنية لدراسة مواءمة أساليب المكافحة مع التطور في أساليب ارتكاب الجرائم المتصلة بالتكنولوجيا الحديثة.

– وضع ودراسة الخطط الأمنية في مجال المعلوماتية، ووضع الاحتمالات والسيناريوهات اللازمة لتحجيم ذلك النوع من الجرائم.

– متابعة أحدث الجرائم المرتكبة في هذا المجال، محليا، إقليميا ودوليا، وإعداد البرامج اللازمة لمنع الجرائم المرتكبة باستخدام البرامج الخبيثة.

– متابعة التراخيص التي تصدر للشركات والمكاتب الخاصة التي تعمل في مجال نظم المعلومات والإنترنت.

[1] Johnny Nhan, Policing Cyberspace: A Structural and Cultural Analysis, LFB Scholarly Publishing LLC., 2010, p33.

– المرور على مقاهي الإنترنت ومتابعة العاملين بالمجال، والتأكد من حصرهم للمترددين وتسجيل بياناتهم.

– المرور على متاجر بيع المصنفات الفنية، والتأكد من عدم بيع مصنفات فنية مزورة، حفاظا على حقوق الملكية الفكرية.

– إبداء الرأي والمشورة والمساعدات الفنية سواء داخل الجهاز الأمني أو خارجه في ضبط جرائم التكنولوجيا الحديثة.

– بحث مدى ملاءمة التشريعات الجنائية لمواجهة هذه الجرائم، مع اقتراح التوصيات لعرضها على الأجهزة المختلفة.

– إعداد قاعدة بيانات بالجرائم المتصلة بالتكنولوجيا الحديثة التي تدخل في نطاق الإدارة والأحكام القضائية التي صدرت فيها، مع حفظ بيانات مرتكبي الجرائم مع تصنيفهم حسب درجات خطورتهم.

– التعاون الدولي مع كافة الأجهزة الأمنية المعنية.

– توعية مستخدمي شبكة الإنترنت من جميع فئات المجتمع بماهية جرائم التكنولوجيا الحديثة ومخاطرها وسمات مرتكبيها وخصائصها وأشهر الطرق لارتكابها وكيفية تجنبها والوقاية منها، وأهمية تطبيق ضوابط الأمن والحماية للحفاظ على أمان تعاملاتهم وخصوصيتهم.

ب– متابعة محتوى الإنترنت: أصبح من الضروري متابعة محتوى شبكة الإنترنت وما يتضمنه من معلومات، وذلك بعد اعتماد العناصر الإجرامية على التقنيات الحديثة وخاصة العناصر الإرهابية في ظل انتشار الإرهاب الإلكتروني، واعتماد التنظيمات الإرهابية على التقنيات الحديثة في تداول المعلومات فيما بينهم وإصدار التكليفات لعناصرها لتنفيذ العمليات الإرهابية.

وتعتبر عملية متابعة محتوى شبكة الإنترنت عملية في غاية الصعوبة، لما تحمله الشبكة من كم هائل من المعلومات والمواقع وأنه لا يوجد طريقة محددة في العالم لتنفيذ ذلك الإجراء، مع صعوبة المتابعة على مدار 24 ساعة، ولذلك كان من الضروري تنظيم هذه الأعمال وتوضيح الهدف منها مع بيان أهم الأنظمة الحديثة للمتابعة والتحليل، وذلك على النحو التالي:

– نظرية المتابعة على شبكة الإنترنت: ضرورة تحديد الوقت والشخص أو الموقع والسبب المراد المتابعة بشأنه، وأن يكون هناك فريق عمل محدد لهذه الأعمال لديهم الخبرة والقدرة على تنفيذها، وتحديد المطلوب من المتابعة تحديدا دقيقا، وتحليل المعلومات المطلوبة التي تحتاج لها المؤسسة الأمنية وتطوير الأدوات المستخدمة في هذه الأعمال من برامج وأجهزة.

ضرورة أن يشمل تكوين فريق العمل العناصر الآتية: فنيين تقنيين على دراية كاملة بالاتصال بشبكة الإنترنت وأخصائيين في تحليل المعلومات وتصنيفها وفنيين لصيانة أجهزة الحاسب الآلي المستخدمة في عملية المتابعة وشخص أو عدة أشخاص لديهم القدرة على التحدث والترجمة لعدة لغات، وذلك لتفسير وترجمة المعلومات المدونة بلغات أخرى على شبكة الإنترنت.

– أهداف المتابعة والتحليل: تحديد وتقييم والوصول لفكرة عامة عن آراء واتجاهات الأشخاص والرأي العام، والبحث السريع وتوقع التهديدات المحتملة، وتحديد التهديدات الأمنية المختلفة ومحاولة منعها قبل حدوثها.

– النماذج الحديثة للمتابعة والتحليل:

• **نموذج Digimind**: وهو برنامج متابعة ورصد وتصفية وتحليل محادثات وسائل التواصل المعروفة وغير المعروفة على الإنترنت حيث تجمع الإشارات من أكثر من 850 مليون مصدر في جميع أنحاء العالم، لمعرفة ماذا، متى، كيف، أين، من وراء الثرثرة، ويساعد هذا البرنامج من وضع هذه المعلومات في صورة لتصنيف الظواهر على الساحة المعلوماتية.

• **برنامج Google Alerts**: وهو أحد الأدوات على شبكة الإنترنت التي تعطي إنذارا معينا من خلال كلمات معينة، وهذه الخاصية يمكن استخدامها على مواقع: Google–Yahoo ولا يمكن استخدامها على موقع فيسبوك، وهي خدمة مجانية.

• **برنامج Google Truster Flagger**: وهو أحد الأدوات التي تمكن الشرطة من معرفة بعض المعلومات عن المواقع على موقع Google، لكن يشترط عقد اتفاقية مع إدارة شركة Google للاستفادة من هذه الخدمة.

• **أداة Tweetdeck.tweeter.com**: تساعد هذه الأداة على متابعة خاصية هاش تاج[1] وما يكتبه الأشخاص مباشرة في أي دولة في العالم على موقع التواصل Twitter.

وفي جميع الأحوال، يجب دعم الشرطة بشراء البرامج اللوجستية وتحديث البرامج المستخدمة لمتابعة محتوى الإنترنت من رسائل وصور للمستخدمين العاديين.

2- مرحلة بعد وقوع الجريمة: رغم قيام الجهاز الأمني بالدور الوقائي في مرحلة ما قبل وقوع الجريمة قد يستمر وجود الجرائم المتصلة بالتكنولوجيا الحديثة، ولمواجهة تلك الجرائم تضطلع إدارات البحث المعنية في كشفها بدورها في إجراءات التحقيق الجنائي لكشف الجناة وتقديمهم للعدالة، وتتمثل بداية العمل للجهاز الأمني في مرحلة بعد وقوع الجريمة في:

- تلقي البلاغات، سواء كان البلاغ من أفراد، شركات أو مؤسسات، وسواء كان بحضور المبلغ أو عن طريق البلاغ الإلكتروني أو تلقى معلومة من أحد المصادر السرية لإدارات البحث.

- مكافحة الجرائم التي تقع في مجالات نظم المعلومات وقواعد البيانات والإنترنت بالاشتراك مع الأجهزة المختصة سواء من داخل الجهاز الأمني أو خارجه وفقا للتعليمات والاتفاقيات المنظمة لذلك[2].

- إجراء التحريات اللازمة وأعمال الضبط في الجرائم بعد تحديد شخص المتهم، من خلال عمليات التتبع باستخدام البرامج الحديثة لتحديد وتتبع IP للأجهزة على شبكة الإنترنت[3].

- ضبط المتهمين وتقديمهم للعدالة وفقا للإطار القانوني، مع ضرورة عمل إدارة المكافحة، من خلال تطبيق المواد القانونية الواردة بالقوانين المختلفة بالدولة.

ثانيا: أهم الأدوات المستخدمة في مكافحة جرائم التكنولوجيا الحديثة، يستخدم العاملون في مجال التحقيق الجنائي والبحث في الجرائم المتصلة بالتكنولوجيا الحديثة مجموعة من الأدوات والمواقع والبرامج التي تساعدهم في عمليات البحث والمتابعة للجناة بهدف الوصول للحقيقة وتقديم الجناة للعدالة، ومن أهم الأدوات المستخدمة في ذلك مايلي:

أ-موقع Viewdns.info: يتميز هذا الموقع بأنه مدون عليه أغلب بيانات IP للمستخدمين على شبكة الإنترنت ويتم من خلال هذا الموقع تحديد أول شخص قام بالاتصال بشبكة الإنترنت مستخدما هذا الـ IP.

ب- موقع Stolencamerafinder.com: يتميز هذا الموقع بقدرته على تحديد الجهاز الذي تم استخدامه في عرض صور على شبكة الإنترنت، وتحديد ما إذا كان تم عرض هذه الصورة على مواقع أخرى أم لا، حتى في حالة تعديل أو

---

[1] الهاشتاق (Hashtag) هي أي كلمة تأتي بعد علامة (#) لحصر جميع المشاركات التي تتحدث عن موضوع معين، فعندما نريد عمل هاشتاق لكلمة التكنولوجيا مثلا، نقوم بإضافة (#) قبل الكلمة لتصبح هكذا (#التكنولوجيا)، فبعد عمل هاشتاق لكلمة التكنولوجيا يمكن النقر على زر إدخال (Enter) حتى تظهر لنا جميع المواقع التي تتحدث عن هذا الموضوع، أو بالأصح ستظهر لنا جميع المواضيع التي بها هاشتاق لهذه الكلمة.

[2] أيمن عبد الحفيظ عبد الحميد سليمان، استراتيجية مكافحة جرائم استخدام الحاسب الآلي، دراسة مقارنة، المرجع السابق، ص457.

[3] أيمن عبد الحفيظ عبد الحميد سليمان، استراتيجية مكافحة جرائم استخدام الحاسب الآلي، دراسة مقارنة، المرجع نفسه، ص454.

تغيير الصورة باستخدام برامج فوتوشوب مثلا، وذلك من خلال المعطيات الرقمية للصورة EXIF، سواء تم التقاط الصورة باستخدام كاميرا أو تليفون محمول، ويستخدم هذا الموقع في الجرائم المتصلة بالتكنولوجيا الحديثة الخاصة بنشر صور إباحية أو الصور الخاصة بجرائم الاستغلال الجنسي للأطفال، وجرائم التشهير...إلخ.

ج- موقع Trendsmap.com: يساعد هذا الموقع في تحديد خاصية الهاشتاج ومكانه على مختلف مواقع التواصل الاجتماعي.

كما يستخدم المحققون والفنيون في الفحص والمتابعة محركات البحث الأكثر شهرة على شبكة الإنترنت مثل Bing Yahoo, Google...إلخ، في البحث عن المعلومات البيضاء، ومحرك البحث Yasni للبحث عن الأشخاص و Ixquick Duckduckgo للبحث عن المعلومات، وتمتاز هذه المحركات بعدم تسجيلها لبيانات الباحث وهناك بعض المواقع التي تساعد في عملية البحث على شبكة الإنترنت، منها:

- **موقع Name Checkr**[1]: يساعد هذا الموقع على معرفة حساب معين، وإن كان قد تم استخدامه من شخص آخر أم لا، ويمكن الكشف والبحث عليه عن طريق الـ Email أو اسم Profil، لكن لا يستطيع إعطاء IP لصاحب الحساب.
- **موقع Qwant**: وهو محرك بحث أطلقته شركة فرنسية، بدأ تشغيله في فبراير 2013، يعمل على البحث في الشبكات الاجتماعية عن طريق تسجيل اسم الشخص المراد فحص حساباته وتتبعه.
- **موقع Way Back Machine**[2]: يوضح هذا النظام كافة البيانات المؤرشفة على شبكة الإنترنت مثل فيسبوك وتويتر وكافة الإصدارات المحفوظة على شبكة الإنترنت وأيضا موقع Archive.org للبحث عن كافة البيانات المؤرشفة في كافة المواقع.

إضافة إلى ضرورة إلمام المحقق الجنائي بكافة المواقع والتقنيات الضرورية والحديثة، وتطوير وزيادة قدراته العملية والفنية لتنفيذ وتحقيق الواجبات المنوطة به من الفحص والمتابعة والوصول للأدلة تحقيقا للعدالة.

البند الثاني: تأهيل الأجهزة الأمنية للتصدي لجرائم التكنولوجيا الحديثة

إن التحديات المستجدة لجهاز الأمن لمواجهة الآثار السلبية للمتغيرات المحلية والدولية جعلته يعمل جاهدا على تطوير نفسه وتحديث وسائله وأساليبه في التعامل مع الجرائم المتصلة بتكنولوجيا المعلومات الحديثة، وأن يقدر مسؤولياته الضخمة والجسيمة خاصة في المراحل المهمة التي تسعى الدولة فيها بخطى حثيثة للقفز إلى صفوف الدول المتقدمة لخلق بيئة إلكترونية أمنة ومستقرة ويأتي هذا من خلال الاعتماد على التطوير والتحديث والمتابعة والتخطيط السليم، مع الاهتمام بدور الإعلام في تنمية وتوعية الفكر لمواجهة جرائم التكنولوجيا الحديثة.

[1] https://www.namecheckr.com
[2] http://www.waybackmachine.com

أولا: دور الإعلام الأمني، أصبح الإعلام والاتصال من الأدوات المهمة التي تستخدم في البناء الاجتماعي والأمني من أجل مصلحة الفرد والمجتمع ككل، وقد ازدادت أهمية وسائل الاتصال الجماهيري في الوقت الراهن وأصبحت من أهم المصادر التي يستمد منها الفرد معلوماته ومعارفه عن العالم ومن حوله.

وتعتبر وسائل الاتصال قوة مؤثرة في العديد من أوجه النشاطات منها المجال الأمني، إذ تلعب وسائل الإعلام دورا مهما في توعية المجتمع بكل أطيافه بالمخاطر التي قد يتعرض لها، وهنا يبرز دور الإعلام الأمني لتنمية الوعي الأمني لدى الجمهور، فيقوم بنشر الأمن والطمأنينة بين أفراد المجتمع لمواجهة الجرائم المتصلة بالتكنولوجيا الحديثة.

1- مفهوم الإعلام الأمني: هو فن التعبير الذي يمارسه الجهاز الأمني بصوره الإيجابية المختلفة للتفهم والمشاركة مع المجتمع لتحقيق الأمن، وقد حدد مفهوم الإعلام الأمني بما يصدر عن أجهزة الأمن من مجلات ونشرات وبرامج وجميع الأنشطة الإعلامية التي تهدف إلى تحقيق الوعي الاجتماعي لتساعد على تدعيم المبادئ والقيم الإسلامية التي تشكل سدا منيعا ضد الجريمة[1]، والإعلام الأمني بمفرده لا يكفي لتحقيق الاستقرار والأمان للمجتمع، حيث إن تحقيق الأمن يقوم على التعاون المشترك بين الجهاز الأمني والجماهير.

2- وظائف الإعلام الأمني: يقوم الإعلام الأمني بعدد كبير من الوظائف بغية الوصول إلى تحقيق أهدافه، ومن أهم هذه الوظائف ما يلي:

- تشجيع الجمهور على التعاون مع الشرطة، وتنمية الشعور بالمسؤولية الاجتماعية لديهم، وخلق روح الارتباط بين جهاز الأمن وأفراد المجتمع[2].
- بث الطمأنينة في نفوس الجماهير، وخلق صور إيجابية لدى المواطنين عن جهاز الأمن ومهامه ووظائفه لتحقيق الصالح العام لأفراد المجتمع.
- التبصير بالإجراءات والتدابير الوقائية في مواجهة خطر جرائم التكنولوجيا الحديثة مع توعية الشعب بالإجراءات التي يجب اتخاذها لتقليل آثار تلك الجرائم[3].
- إعلام الجمهور بالخدمات الحكومية الرسمية التي يؤديها له الجهاز الأمني.
- نقل الحقائق، والتوعية بكل ما هو جديد في نطاق الجرائم المتصلة بالتكنولوجيا الحديثة لتحصينهم من الوقوع في براثن تلك الجرائم.
- قياس الرأي العام ومعرفة اتجاهاته والتسويق للسياسات والأنشطة الأمنية.

---

[1] إيمان عبد الرحمن أحمد محمود، دور الإذاعة في نشر التوعية الأمنية، الإذاعة السودانية نموذجا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2010 ص25.

[2] علي الباز، الإعلام والإعلام الأمني، مركز الإشعاع الفني، الإسكندرية، ط1، 2001، ص32.

[3] أشرف السعيد أحمد حافظ، الاتصال والتواصل بين الإعلام الأمني ووسائل الإعلام، مجلة كلية التدريب والتنمية، العدد 28، القاهرة، مارس 2013 ص174.

- المتابعة الدقيقة والمستمرة لكل ما نشر في وسائل الإعلام المختلفة داخليا وخارجيا، وذلك لدراسته وتحليله والاستفادة منه في وضع الاستراتيجية والخطط الأمنية.
- إبراز أهم التطورات في مختلف الأجهزة الأمنية من حيث مواكبة التقدم العلمي والتكنولوجي.
- إرشاد الجمهور للوسائل الإجرامية التي يستخدمها المجرمون للحذر منها، مما يؤدي إلى يقظة وحرص الأجهزة الأمنية وقيامها بدورها في تأمين المجتمع ضد الانحرافات التي يمر بها.

3- أهداف الإعلام الأمني: يستهدف الإعلام الأمني إثارة الوعي الجماهيري بالمشاكل والقضايا والأحداث الطارئة بالمجتمع مما يزيد عملية الإدراك لدى جميع أفراد المجتمع وتبصيرهم بكافة المعارف والخبرات والاتصال بالجوانب الأمنية المختلفة اتصالا ينفي أي نوع من الجهل أو عدم المعرفة، والابتعاد عن الحقائق والمحددات الأمنية لتحقيق أكبر قدر ممكن من الاتصال للوصول لاستقرار وأمان المجتمع.

مع تزايد الجرائم المتصلة بالتكنولوجيا في العصر الحديث، وتزايد التعاملات عبر الإنترنت استوجب على الإعلام الأمني وضع الخطط الاستراتيجية لتوعية الأفراد والشركات والمؤسسات بمخاطر الإنترنت وسبل الأمان والحماية، وطرق وأساليب الإبلاغ في حالة وقوع جرائم ضدهم وذلك بكافة وسائل الإعلام الممكنة[1]، إذ يسهم الإعلام الأمني في بناء الثقة والاحترام بين رجال الأمن من جهة، وجميع أفراد المجتمع من جهة أخرى، وترسيخ الإعتقاد لدى المواطنين بأن الجهاز الأمني مستعد لتقديم الخدمات الأمنية في الحاضر والمستقبل، ويجب على الإعلام الأمني أن يشمل المعلومات الكاملة والجديدة والمهمة التي تغطي كافة الأحداث الأمنية والقوانين المتعلقة بأمن المجتمع[2].

4- خطة الإعلام الأمني لتنمية الفكر الاستراتيجي لمواجهة الجرائم المعلوماتية: لإنجاح برامج الإعلام الأمني لتنمية الفكر الاستراتيجي لمواجهة الإجرام المعلوماتي لابد من وضع خطة مدروسة تقوم على خطوات علمية.

أ- تحديد أهداف الخطة الإعلامية، يجب تحديد الهدف الأساسي من الخطة الإعلامية وهو توعية وتثقيف مستخدمي وسائل ووسائط التكنولوجيا الحديثة بالمخاطر المحتمل التعرض لها من خلال استعمالها وطرق الحماية والتأمين الواجب اتخاذها لتجنب هذه المخاطر لتحجيم انتشار الجرائم المتصلة بها، وأيضا نشر الثقافة القانونية للحد من وقوع الهواة تحت طائلة القانون نتيجة جهلهم بما يرتكبونه من أفعال تجرم وفقا للقانون، كما يجب التوعية بأسلوب الجرائم التي ما زالت ترتكب دون الوصول لمرتكبيها.

ب- تحديد جماهير الخطة الإعلامية: لضمان نجاح الخطة الإعلامية للتوعية من مخاطر المعلوماتية، يجب تحديد الجماهير المستقبلة لرسالة الجهاز الإعلامي الأمني مثل فئات الشباب، وطلبة المدارس والجامعات والعاملون في مجال تكنولوجيا المعلومات والاتصالات خاصة في المنظمات الاقتصادية وأولياء الأطفال في المدارس، وقد تذاع الرسالة عبر وسائل الإعلام المرئي وأحيانا يجب

---

[1] حمود عبد الله عوض الخضير، دور الإعلام في تحقيق الوعي الأمني لدى الرأي العام بالتطبيق على دولة الكويت، أطروحة دكتوراه، كلية الدراسات العليا أكاديمية الشرطة، 2007، ص77.

[2] وليد سمير فهيم المعداوى، المرجع السابق، ص419.

أن تكون عبر الصحف أو الإذاعة، وأحيانا تكون عبر شبكات الإنترنت وأخيرا قد تكون في جميع وسائل الإعلام حسب أهمية هذه الرسالة للوصول لكافة فئات الشعب.

ج- تحديد مضمون الرسالة: قد يختلف مضمون الرسالة من حالة لأخرى حسب الهدف منها، وفي كل الحالات يجب أن يكون مضمون الرسالة سهلا وبسيطا وباللغة المتعارف عليها في الدولة، تحقيقا لهدف تنمية الفكر لمواجهة جرائم التكنولوجيا الحديثة[1].

رغم نجاح خطط الإعلام الأمني في عدة قطاعات أمنية، إلا أنه في مجال مكافحة الجرائم المتصلة بالتكنولوجيا الحديثة لم يصل إلى المستوى المطلوب في توعية الأفراد تجاه هذه الجرائم، وقد يرجع سبب ذلك لنقص التعاون والتنسيق بين الإعلام الأمني وأجهزة الإعلام المختلفة.

ثانيا: التخطيط لمواجهة جرائم التكنولوجيا الحديثة، أقبل القرن الحادي والعشرون منذ سنوات قليلة، وتكاثرت معه تحديات متعددة في عالم سريع التغير، ومع ظهور العولمة كنتيجة منطقية لظروف الحياة المعاصرة وانتشار الإنترنت، فقد اكتسبت هذه الظاهرة أبعادا عديدة من عولمة للإعلام والثقافة والتجارة والإدارة وجميع مناحي الحياة.

ومن هذا المنطلق، أصبح العصر الحالي، عصرا جديدة في حياة الإنسان، عصر التقدم التكنولوجي وقد أصبحت الجريمة في ظل نظام العولمة مشكلة عالمية في تزايد مستمر وبأشكال جديدة[2]، لهذا يجب البحث عن وسائل حديثة لمكافحة جرائم تكنولوجيا المعلومات تتواءم مع مقتضيات العصر التكنولوجي، من خلال تأهيل وتدريب المختصين في المكافحة ليصبحوا أكثر كفاءة في أعمال التحقيق، من خلال تحول سريع في أسلوب العمل، وهو ما يفرض على الجهاز الشرطي الاعتماد على التخطيط الأمني لمواجهة الجرائم المتصلة بالتكنولوجيا الحديثة.

1- مفهوم التخطيط وخصائصه: تعتبر كلمة التخطيط من الكلمات ذات المعنى الواسع، فهو مصطلح شامل له منفعته فهو أسلوب تنظيمي يهدف إلى تحقيق التنمية في كافة أنشطة المجتمع خلال فترات زمنية محددة، عن طريق حصر الإمكانيات المادية والبشرية وجعلها قادرة على تحقيق الأهداف في ضوء الفلسفة العامة للمجتمع بواسطة الإعداد العلمي، ولذلك يعتبر التخطيط أحد العناصر الرئيسية في عملية الإدارة.

بات التخطيط الأمني ضرورة حتمية إذن، ينبغي لكل مجتمع العمل على تحقيقه وترجمته واقعيا، وتفعيله وفق القواعد العلمية المتعارف عليها في عالم التخطيط وعلم الاستراتيجيات، الأمر الذي يفرض على المسؤولين بالجهاز الشرطي في كل مجتمع الأخذ بأسباب العلم ونظرياته وتقنياته بما يحقق متطلبات الحاضر والتزاماته، وبما يتيح التنبؤ بالمستقبل[3] ويضمن مواجهة التحديات الأمنية لمكافحة الجرائم المتصلة بالتكنولوجيا الحديثة، ويتفق التخطيط الشرطي في خصائصه مع التخطيط العام في عدة مجالات تتمثل أساسا فيما يلي[4]:

---

[1] وليد سمير فهيم المعداوى، المرجع السابق، ص425.

[2] عادل حسن علي السيد، تحديات التخطيط الأمني لمواجهة العولمة، جامعة نايف العربية للعلوم الأمنية، الرياض، ط1، 2006، ص55.

[3] عادل حسن علي السيد، المرجع نفسه، ص85.

[4] علي إسماعيل مجاهد، التنبؤ كأساس للتخطيط الأمني، أطروحة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة، 2004، ص65.

- أن تكون أغراض الخطة وأهدافها محددة تحديدا واضحا ومباشرا.
- أن تكون الخطة مرنة، لإمكانية تعديلها لمواجهة المتغيرات التي يمكن أن تطرأ أثناء التنفيذ دون التأثير على النتائج.
- أن تكون الخطة محكمة وفي الإمكان تنفيذها.
- إعداد الخطة وفقا لمقاييس علمية، مع ضرورة الابتعاد عن المقاييس الشخصية.
- أن تكون الموارد المتاحة تسمح بتنفيذ الخطة.

وتتبلور أهمية التخطيط الشرطي في العمل على زيادة الكفاءة والفاعلية في منع وضبط الجريمة المتصلة بالتكنولوجيا الحديثة أساسا فيما يلي:

- يحدد الأهداف التي تسعى إليها الإدارة الأمنية بوضوح حتى لا تتعارض مع بعضها البعض[1]، حيث يرتبط التخطيط بالمستقبل فيساعد على معرفة المخاطر المستقبلية الكامنة.
- يحقق التخطيط الاستخدام الأمثل للموارد بمختلف أنواعها –سواء كانت بشرية، فنية، مالية، أو تكنولوجية، كما ونوعا– وبذلك يمكن الاستعداد لكل الظروف والاحتمالات التي يمكن أن تواجه العمل الشرطي أثناء مكافحة الجريمة المتصلة بالتكنولوجيا الحديثة.
- يسهل التخطيط عملية الرقابة لضمان مواءمة الأنشطة الفعلية للخطط الموضوعة مسبقا، والالتزام بتنفيذها في الوقت المحدد لها من خلال وضع المعايير وقياس مستوى الأداء لهذه المعايير للتعرف على الانحرافات التي حدثت أثناء التنفيذ وتصحيحها.
- يؤدي التخطيط إلى الاستغلال الأمثل للإمكانيات المتاحة من خلال عمليات ذهنية، فنية ومهنية، لإزالة كافة المعوقات التي يمكن أن تعترض العمل الأمني.
- ويتضح من ذلك أن نجاح التخطيط لمكافحة الجرائم المعلوماتية يعتمد على:
- التنسيق على مستوى عال تجاه إعداد الخطة وتنفيذها.
- تشكيل فريق بحثي متعاون لإجراء التفتيش والضبط بشكل فعال.
- جمع كافة المعلومات الدقيقة عن نظام الحاسب الآلي المراد تفتيشه.
- وضع خطة تنفيذ دقيقة ومفصلة ومرنة قابلة للتغيير والتعديل استنادا على المعلومات التي تم جمعها عن الجهاز –الحاسب الآلي مثلا– المراد تفتيشه [2].
- أن تكون الخطة مفهومة وواضحة، مما يساعد على تخطي صعوبات قد تواجه المحقق الجنائي.
- اهتمام ضابط الشرطة بإجراءات جمع الأدلة بداية من تلقي البلاغ حتى الضبط، فهو يعني تحديد الوسائل التي تبلغ بها الشرطة أغراضها وتحقيق أهدافها، وأهداف الشرطة في أي مجتمع واضحة، فهي التي تصون وترعى وتحمي الحريات والأملاك والسيطرة

[1] أكرم أنور كرارة، القيادة واتخاذ القرار الأمني، أكاديمية الشرطة، كلية الشرطة، ص95.

[2] وليد سمير فهيم المعداوى، المرجع السابق، ص399.

على الجريمة ومنعها قبل ارتكابها وما يتطلبه ذلك من توفير الأمن والشرطة بدورها كجهاز تنفيذي داخل المجتمع، يقع عليها العبء الأكبر في تحقيق الانضباط داخل المجتمع، فهي اليد التي تنفذ القانون، وهي التي تنظم السلوك، ويتطلب تحقيق هذه الأهداف تخطيطا منظما لكافة العمليات المستقبلية التي تقوم بها الشرطة، سواء ما تعلق منها بسياساتها العامة والإجراءات أم العمليات الإضافية المختلفة[1].

2- مراحل التخطيط الأمني: يقوم التخطيط على مجموعة من المراحل الأساسية تتمثل فيما يلي:

أ- مرحلة التفكير في خطة البحث في جرائم التكنولوجيا الحديثة: تعتمد المرحلة الأولى في وضع خطة البحث على جمع المعلومات الضرورية لتحقيق أهداف البحث الجنائي من خلال تقييم ذاتي وموضوعي دقيق[2]، مع مراعاة تحديد طبيعة المعلومات المطلوب البحث عنها بداية من تلقي البلاغ حتى معاينة مسرح الجريمة المعلوماتية، حصر مصادر المعلومات وكيفية الحصول عليها إضافة إلى حصر الإمكانيات المادية والبشرية المتاحة، وهو ما يعرف بالتقييم الذاتي، مع مراعاة الظروف الخارجية بالبحث الجنائي مثل مكان وجود الجهاز المستخدم في ارتكاب الجريمة المتصلة بالتكنولوجيا الحديثة، ويعقب ذلك مرحلة تصنيف تلك المعلومات وجدولتها لتحديد العلاقة بينها، وصولا لتحليلها وتفسيرها واستخلاص النتائج لمعرفة مدى أهميتها في إعداد ووضع خطة البحث.

ب- مرحلة إعداد خطة البحث في جرائم التكنولوجيا الحديثة: تعتمد هذه المرحلة على وضع افتراضات واحتمالات والتأكد من صلاحيتها اعتمادا على تحديد رجال البحث المتخصصين بالمهارات المهنية التقليدية والمهارات الفنية المتعلقة ببرامج ونظم الحاسبات الآلية والهواتف المحمولة والتقنيات الحديثة بشتى أنواعها وكيفية التعامل معها مثل خبراء المعمل الجنائي الإلكتروني، بالإضافة إلى تحديد الإمكانيات المادية اللازمة لمنع وضبط الجرائم المتصلة بالتكنولوجيا الحديثة، كتوفير البنية التحتية في الاتصالات عبر شبكة الإنترنت، وأجهزة الحاسب الآلي، والهاتف المحمول والبرامج والنظم الإلكترونية الرقمية، وكذا تحديد الإمكانيات الإلكترونية المطلوبة لخطة البحث واللازمة لمعالجة الأدلة، واكتشاف المعلومات التي يتضمنها الدليل الإلكتروني الرقمي وهي كالتالي:

- **الأجهزة**: يجب توفير أجهزة حاسوب حديثة باستمرار، وطابعات ملونة وأبيض وأسود وماسح ضوئي مجهزة بالإمكانيات الحديثة وبطاقات شبكة الإنترنت ووصلات خارجية للربط من أي شبكة، ومجموعة فارغة من أقراص مرنة ذات سعة عالية وحقيبة من أدوات التفكيك والمفكات.
- **أنظمة التشغيل**: ومنها: Win XP،Win7، Win8، Win10، IOS، Android .
- **البرمجيات**: منها برمجيات الضغط وفك الضغط، كـ: Zip،RAR، ARC وبرمجيات معالجة الصور وعرضها مثل: ACD SEE، وبرمجيات نسخ الأقراص المدمجة مثل: EASY CD CREATOR، وبرمجيات الاتصال بين أي من حواسب المعمل الجنائي والحاسبات المضبوطة عبر الـ PORTS، وبرامج التشفير وفك التشفير مثل: PGP، وبرامج إلغاء أو كشف كلمات المرور وبرامج كشف الأجزاء المخفية على الأقراص الصلبة والمدمجة وبرامج التنصت عبر الإنترنت واختراق المواقع وبرامج مكافحة البرامج الإلكترونية المتطفلة الضارة (الفيروسات) Norton, Kaspersky, McAfee، وبرامج فحص

[1] أكرم أنور كرارة، المرجع السابق، ص100.

[2] وليد سمير فهيم المعداوى، المرجع السابق، ص399.

ثغرات الشبكات ونقاط الضعف فيها، وبرامج حماية الشبكات والأنظمة من الاختراق FIREWALLS، وبرامج البحث الدقيق واستعادة الملفات المشطوبة، وبرامج البحث عبر الإنترنت وتحديد الخطط البديلة من خلال التنبؤ باحتمالات المستقبل، وذلك لاستخدامها في حالة الاحتياج و لمواجهة المواقف الطارئة والجريمة عند تنفيذ الخطة.

ج- مرحلة إقرار خطة البحث في جرائم التكنولوجيا الحديثة: تتطلب هذه المرحلة مجهودا ذهنيا عميقا قائما على تقييم السلبيات والإيجابيات المتوقعة لاتخاذ القرار السليم واختيار البديل الأفضل، تعتبر هذه المرحلة تنفيذا للخطة المقترحة في الوثيقة الآمرة والتي تشمل الهدف، المنفذين، قواعد وإجراءات البحث، الجدول الزمني المحددة للتنفيذ[1].

الفرع الثاني: وسائل الأمن السبراني

نظرا للتطور السريع والمتلاحق لثورة تكنولوجيا المعلومات والاتصالات، وزيادة اعتمادية الأفراد والمؤسسات والدول على استخدام الأجهزة الإلكترونية، ونظم وشبكات المعلومات والاتصالات في كافة مناحي الحياة المعاصرة، وتعذر الاستغناء عن هذه الاستخدامات التكنولوجية لارتباطها بالعديد من المصالح الخاصة والعامة وأمن واستقرار المجتمعات، باتت الحاجة ملحة إلى مزيد من الجهود على مختلف الأصعدة لمكافحة الاستخدام غير الآمن لإنجازات ثورة المعلومات والاتصالات وتجنب مخاطرها.

وقد يظهر أن مجرمي التكنولوجيا الحديثة لهم قدرة فائقة وأن نظام الحاسب الآلي مثلا له مساوئ، وليس هناك ما يمكن فعله سوى الخضوع لهذا التهديد، لكن الأمر ليس كذلك، بل هناك العديد من الاتجاهات لحماية نظم المعلومات من الاعتداءات كما هو احال في الجرائم التقليدية، وتكون مكافحة الجرائم المتصلة بالتكنولوجيا الحديثة أولا بالوقاية، ومنع الجرائم من خلال تحديد المخاطر واتخاذ كافة التدابير اللازمة لحماية النظم المعلوماتية لبسط الحماية للبيانات الشخصية والمعلومات الموجودة بالأنظمة المعلوماتية[2].

البند الأول: إجراءات الأمن السبراني

تتمثل إجراءات الأمن المعلوماتي عموما فيما يلي:

أولا: التأمين الطبيعي لنظم المعلوماتية، يعتبر الأمن الطبيعي أول خطوط الدفاع، وتكمن أهميته فيما يحميه من الأجهزة الإلكترونية والأنظمة المعلوماتية الذي يهدف إلى تأمين البنية التحتية لمراكز المعلومات من التهديدات والمخاطر، فمن الضروري حسن اختيار المكان المناسب لأجهزة الحاسب الآلي والأنظمة المعلوماتية للحماية من المخاطر والكوارث الطبيعية، حيث يجمع الأمن المادي الإمكانات المادية للحاسب الآلي (المبنى -غرفة الحاسب الآلي -الأسطوانات -الأشرطة -الطابعة...إلخ)[3]، توفير وسائل اكتشاف الحريق قبل وقوعه باستخدام كاشفات الدخان وكاشفات الحريق، استخدام نظم التحكم في الوصول لأماكن الحاسبات باعتبارها مناطق مؤمنة، بحيث لا يسمح بالدخول لهذه المناطق إلا للمصرح لهم فقط بالدخول والتواجد بها، إجراء الدعم الفني والصيانة

---

[1] وليد سمير فهيم المعداوى، المرجع السابق، ص400.

[2] David J. Icove, Karl A. Seger, William Von Storch, Op.Cit., p23.

[3] وليد سمير فهيم المعداوى، المرجع السابق، ص264 و265.

الدورية لأجهزة الحاسبات في مكان ملائم ضمن حدود المنطقة المؤمنة بهدف تجنب وصول غير المصرح له بالدخول.

إضافة إلى تأمين منطقة النظام المعلوماتي بتركيب أجهزة إنذار وأنظمة كشف الدخلاء التي تتوافق مع المعايير العالمية، مع التحكم في الدخول والخروج بوسائل تحديد الهوية وأنظمة التحكم بالدخول[1]، وتتعدد هذه الوسائل فمنها ما يستخدم بصمة الأصابع، ومنها ما يستخدم كلمة السر...إلخ، وكذا ضرورة حماية الأجهزة من انقطاع الطاقة الكهربائية والعيوب الكهربائية الأخرى مثل: زيادة أو نقصان قيمة الجهد أو التيار أو التردد مع استخدام أجهزة منع انقطاع التيار (UPS)، واستمرار فحص كفاءة البطاريات الخاصة للتأكد من قدرتها، مع ضرورة حماية الكابلات ومكونات البنية التحتية للنظام المعلوماتي من الأعطال والتلف[2].

ثانيا: تأمين القائمين على النظام المعلوماتي، يعد العنصر البشري أضعف حلقة ضمن سلسلة الأمن السبراني، ولإقامة وضع أمني فعال يتحتم ضمان وجود ضوابط مناسبة من أجل التخفيف من المخاطر البشرية التي تتمثل في السرقة أو الاحتيال أو سوء استعمال النظام المعلوماتي، ويجب أن يغطي برنامج التأمين الشخصي التهديدات بواسطة الأنماط المختلفة من الأفراد، حيث توجد وظائف في الهيكل التنظيمي للنظام الإداري المعلوماتي بأحقيات دخول بعض العاملين إلى مصادر معلومات على قدر كبير من الأهمية والسرية، مثل مدير الشبكات أو مدير قواعد البيانات أو مهندسي الصيانة الأمر الذي يوجب اتخاذ بعض الإجراءات الأمنية كحماية خاصة معهم منذ التحاقهم للعمل بالمؤسسة وبعد تقاعدهم[3].

بناء على ما سبق، تكمن أهم الإجراءات الواجب اتباعها لتحقيق أمن الأفراد فيما يلي:

– ضرورة أن يتضمن طلب التوظيف للعاملين في المجال المعلوماتي بطاقة الهوية الشخصية والشهادات الأكاديمية والمؤهلات المهنية في هذا المجال، وتحديد مسؤوليات التأمين في مرحلة التوظيف، وأن يتضمن عقد الوظيفة تلك المسؤوليات لضمان السرية وعدم الكشف عن معلومات المؤسسة، ومن الضروري أن يوقع العاملون على هذه المسؤوليات وعلى الإجراءات القانونية التي قد تتخذ ضده في حالة مخالفتها[4].

– ضرورة توفير وسائل لمراقبة العاملين بالنظام المعلوماتي أثناء تأدية عملهم، واقتصار حقوق المستخدمين في الوصول إلى المعلومات على تلك التي يحتاجون إليها من أجل الالتزام بمتطلباتهم الوظيفية، على أن يتم وضع المنطقة المغلقة للنظام المعلوماتي تحت المراقبة بأنظمة التسجيل بكاميرات الفيديو، الذي يبدأ التصوير عند بدء دخول العاملين لمنطقة العمل وإيقافها عند المغادرة، مع حفظ التسجيلات لمدة (30) يوما قبل حذفها، وفي حالة الاشتباه في أحد العاملين، يجب إحضار الملف الشخصي للموظف للحصول على البيانات الأساسية له.

– ضمان أن يكون الموردون أو المتعاقدون أو زوار النظام المعلوماتي مسجلين وفقا لبيانات تعريفية وحصولهم على شارات زوار محددة لأماكن الزيارة وأن يمتثلوا لسياسات الأمن، إضافة إلى تعليم العاملين بالنظام المعلوماتي أسس الأمن والسلامة، والكشف عن اللصوص، وتحديد العملاء والعاملين المشتبه فيهم.

---

[1] www.isecur1ty.org

[2] وليد سمير فهيم المعداوى، المرجع السابق، ص272.

[3] وليد سمير فهيم المعداوى، المرجع نفسه، ص274.

[4] وليد سمير فهيم المعداوى، المرجع نفسه، ص274.

ثالثا: التشفير، يعتبر التشفير المعلوماتي من أهم وسائل الحماية في مجال الأمن المعلوماتي وحماية البيانات المتبادلة والمعلومات عبر شبكة الإنترنت، فهو عملية تتمثل في تحويل المعلومات المقروءة إلى إشارات غير مفهومة[1]، فالتشفير هو الممارسات التقنية التي تؤمن التواصل بين جهتين في وجود جهة ثالثة، أي أننا لا نحتاج للتشفير إن كانت الجهتان المتواصلتان هما فقط وبشكل قطعي يحصلان على المعلومة، أما الحاجة الفعلية للتشفير فتنبثق من وجود إمكانية لجهة ثالثة أن تطلع على المعلومة المرسلة، فبعض مستخدمي شبكة الإنترنت يستطيعون –بواسطة برنامج خاص– تشفير معلوماتهم قبل نقلها عبر الشبكة على أن يتم فك رموزها ببرنامج مماثل عند استقبالها من جانب المرسل إليه، وهناك شبه إجماع بين الشركات المنتجة للنظم الأمنية حول التقنيات المستخدمة فيها، فجميع الأساليب المستخدمة للتأمين المعلوماتي تعتمد على تقنيات التشفير، بينما تختلف هذه الشركات فيما بينها في طريقة التنفيذ فقط وليس في المبادئ الأساسية، ومثال ذلك اتفاق شركتي ماستر كارد وفيزا كارد على تقنيات فنية مشتركة (التشفير) لحماية التسويق الذي يتم عبر شبكة الإنترنت باستعمال بطاقات الائتمان[2].

1– أنواع التشفير[3]: يمكن إجمال أنواع التشفير فيما يلي:

• **التشفير المتماثل**: هو عبارة عن استخدام مفتاح سري وحيد، وهذا المفتاح يستخدم في عملية تشفير الرسائل أو فك شفرتها، فالطرفان اللذان يودان تبادل رسائل مؤمنة يجب عليهما استخدام نفس المفتاح، كما يجب عليهما الاحتفاظ به، فيتبادلانه بطريقة تضمن عدم اطلاع طرف ثالث عليه.

• **التشفير غير المتماثل**: يستخدم هذا الأسلوب زوج من المفاتيح، يكون معلوما لأكثر من شخص ويتم تبادله بين الأطراف المختلفة، أما المفتاح الآخر فيظل سريا لا يعرفه سوي طرف واحد (صاحب المفتاح)، وإذا تم تشفير الرسالة بواسطة أحد المفتاحين، فإن فك شفرتها يحتاج إلى استخدام المفتاح الآخر، مثالا لذلك، استحدثت شركة (Apple) نظام التشغيل الخاص بها (iOS11) واستخدمت نظام التشفير لكافة بيانات مستخدمي منتجاتها توفيرا لأعلى قدر من الأمان الذي تستطيع توفيره لعملائها.

وعليه يجب أن يشمل التشفير عملية تخزين المعلومات، ولا يقتصر التشفير على نقل المعلومات فقط، خاصة في المؤسسات والشركات المالية، مع استحداث نظام المسؤولية المشتركة في المعلومات المخزنة، بحيث يكون أحد العاملين مطلعا على البيانات وآخر لديه مفتاح الدخول للبيانات المخزنة، وآخر لتحديد المعلومات التي يتم الإطلاع عليها، بحيث لا يكون هناك شخص بمفرده له حرية الإطلاع على المعلومات ونقلها أو التلاعب فيها، إذ أن كثيرا من جرائم التكنولوجيا الحديثة يتم ارتكابها بمعرفة العاملين بالمؤسسات.

---

[1] جميل عبد الباقي الصغير، الحاسب الآلي كوسيلة لإثبات الجرائم، ندوة المواجهة الأمنية للجريمة المعلوماتية، مركز بحوث الشرطة، أكاديمية الشرطة 2009، ص15.

[2] جميل عبد الباقي الصغير، الحاسب الآلي كوسيلة لإثبات الجرائم، ندوة المواجهة الأمنية للجريمة المعلوماتية، المرجع نفسه، ص15.

[3] حسن طاهر داود، جرائم نظم المعلومات، المرجع السابق، ص107.

2- ضوابط التشفير: بما أن التشفير منظومة حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات إلكترونيا، كان لابد له من وجود ضوابط وقواعد تتمثل فيما يلي[1]:

- إباحة تشفير البيانات والمعلومات التي يتم تدوينها أو التعامل فيها من خلال الوسائط الإلكترونية، مع ضرورة تحديد القواعد والضوابط الخاصة بتشفير المحررات والبيانات الإلكترونية، خاصة فيما يتعلق بتشفير التوقيع الإلكتروني، وبطاقات الائتمان وغيرها من البيانات التي يتم نقلها أو تخزينها.

- احترام سرية البيانات المشفرة، والاعتراف بحق أصحابها في الخصوصية وهذه البيانات المشفرة تعتبر خاصة بصاحبها ولا يجوز فض سريتها إلا بناء على تصريح كتابي منه، واستخدام التشفير كوسيلة قانونية لتحرير البيانات والمعلومات يكون من طرف الجهات المختصة.

وللتشفير أيضا خطورته، في منع اكتشاف الجرائم المتصلة بالتكنولوجيا الحديثة، وخاصة بالنسبة للإرهابيين ومروجي الصور ذات الطابع الإباحي، الأمر الذي يصعب من الإجراءات الشرطية والتحقيق الابتدائي لكشف الجرائم[2]، ونظرا لخطورة تقنية التشفير وضعت بعض الدول مثل هولندا مشروع قانون يضع عملية التشفير للحصول على ترخيص، مع الالتزام بإيداع مفاتيح الشفرات لدى مكتب متخصص ملتزم بالسرية، وعليه أن يقدم هذه المفاتيح لرجال البحث الجنائي الذين حصلوا على أمر بالضبط والتفتيش من سلطات التحقيق، وإن كان احتمال إفشاء مثل هذه المفاتيح قد يضعف من وسائل الحماية ضد جرائم التكنولوجيا الحديثة[3].

رابعا: تأمين الاتصال بشبكة الإنترنت، يعتبر أمن الاتصالات أمرا مهما جدا، ويشمل تأمين الاتصالات: البريد الإلكتروني، الفاكس، التليفون، الحاسب الآلي، البريد الصوتي...إلخ، وتزداد الأهمية لأمن الاتصالات في ارتباط الوسائل الإلكترونية بشبكة الإنترنت، مع ضرورة شمول أمن الاتصالات العديد من الطرق والوسائل لحماية النظام المعلوماتي[4].

ويعتبر تأمين الاتصال بشبكة الإنترنت من أهم مسؤوليات مديري الشبكات، سواء بالجهات الحكومية أو بالمؤسسات والشركات أو على المستوى الشخصي، وذلك من خلال مراعاة عدد من الاعتبارات المهمة، ندرجها فيما يلي:

- إعداد نظام تأمين للشبكة وإعطاء صلاحيات محددة لكل فرد يعمل على الشبكة[5]، مع تحديد مستوى صلاحيات كل فرد في الشبكة ومستوى الملفات التي يحق له الدخول عليها مع تحديد صلاحياته في الاستخدام من قراءة، قراءة وتعديل، قراءة وتعديل ومسح.

- ضرورة الاحتفاظ بنسخ احتياطية من جميع الملفات والتعاملات التي تتم على الشبكة بخزائن مؤمنة أو على (Hard Disc) مؤمن ضد السرقة، على أن يكون مكان الحفظ خارج المؤسسة التي تتم فيها التعاملات.

- ضرورة إعطاء اسم مستخدم وكلمة مرور لكل فرد في الشبكة، على أن تكون كلمة المرور لا يمكن تخمينها بسهولة

---

[1] فهد بن سيف بن راشد الحوسني، المرجع السابق، ص92 و93.

[2] جميل عبد الباقي الصغير، الحاسب الآلي كوسيلة لإثبات الجرائم، ندوة المواجهة الأمنية للجريمة المعلوماتية، المرجع السابق، ص16.

[3] جميل عبد الباقي الصغير، الحاسب الآلي كوسيلة لإثبات الجرائم، ندوة المواجهة الأمنية للجريمة المعلوماتية، المرجع نفسه، ص17.

[4] David J. Icove, Karl A. Seger, William Von Storch, Op.Cit., p23.

[5] ضياء يحي السادات، المرجع السابق، ص232.

ويفضل أن تكون كلمة السر معقدة تتكون من حروف وأرقام وعلامات خاصة متغيرة باستمرار، مثال ذلك؛ نظام أمن المعلومات والشبكات (Token code) باستخدام تقنية (RSA Secure ID) والذي تستخدمه شركة (Vanguard)، وهي واحدة من أكبر وأهم الشركات الاستثمارية في الولايات المتحدة الأمريكية، والتي يتعامل معها أكثر من 20 مليون عميل.

– يجب عدم التعامل مع الوسائل الإلكترونية مجهولة الهوية، والتي ترد عبر البريد الإلكتروني، فقد تكون محملة ببعض الملفات الضارة أو تكون محلا للنصب والخداع.

– عدم التعامل مع المواقع الإلكترونية وغرف المحادثة المشبوهة كتلك المتطرفة، الإباحية، الإرهابية...إلخ؛ لكونها أرضا خصبة لارتكاب جرائم التكنولوجيا الحديثة.

– تجاهل الرد على كافة أنواع الرسائل الإلكترونية التطفلية (Spam).

– ضرورة الاستعانة ببرامج التأمين اللازمة مثل الجدران النارية في الأجهزة الخادمة لحماية الشبكة.

– يجب تشفير الملفات ذات الأهمية البالغة، بحيث لا يطلع عليها إلا الأفراد المصرح لهم بذلك.

– ضرورة استخدام البرامج الأصلية التي تحظى بدعم فني مستمر من الشركة الأصلية المصممة لها وعدم استخدام برامج منسوخة[1].

– التدريب المستمر للأفراد العاملين في الشبكة، مع التوعية المستمرة بأهمية أمن المعلومات وأمن الشبكات والمستجدات من الجرائم المتصلة بالتكنولوجيا الحديثة.

– الحرص على عدم إصلاح أي جزء من المكونات المادية للشبكة خارج المؤسسة.

– عدم تحميل أي ملفات سواء كانت برامج، أفلام، ألعاب...إلخ؛ من مواقع إلكترونية مجهولة وغير مؤمنة.

البند الثاني: احتياطات أمنية عامة

نظرا لزيادة اعتمادية الأفراد والمؤسسات والدول على استخدام التقنيات الحديثة ونظم وشبكات المعلومات والاتصالات في كافة مناحي الحياة، بات من الضروري التوعية بسبل ووسائل الحماية لتجنب مخاطر الجرائم المتصلة بها، من خلال زيادة الوعي بين الضحايا المحتملين لهذه الجرائم، باتخاذ إجراءات تأمين التعامل مع شبكة الإنترنت، بجانب إجراءات الأمن المادي والشخصي وتأمين المعلومات[2].

بناء على ما سبق نلاحظ وجوب توافر بعض الاحتياطات التي يجب مراعاتها عند التعامل مع التقنيات التكنولوجية، وذلك على النحو التالي:

أولا: احتياطات أمنية للأفراد والشركات والمؤسسات، يمكن إجمالها أساسا فيما يلي:

– تجنب الدخول في حديث صوتي، أو تشغيل كاميرا الجهاز مع من لا تعرفهم لأنه يمكن فتح ثغرات أثناء الحديث لا تستطيع برامج الحماية إغلاقها.

---

[1] ضياء يحي السادات، المرجع السابق، ص234.

[2] David J. Icove, Karl A. Seger, William Von Storch, Op.Cit., p23.

– ضرورة حماية المعلومات الشخصية بعناية، وعدم إدخال رقم بطاقة الائتمان أو أية معلومات بنكية في حالة عدم الثقة في الموقع الطالب.

– عدم إرسال كلمة السر بالبريد الإلكتروني لأي شخص.

– عدم الاستجابة لأي طلبات غير معتادة تطلب منك أثناء المحادثة أو المراسلة الإلكترونية، والحذر في التعامل مع الرسائل الإلكترونية التي تعد بمكاسب مادية أو الالتحاق بوظائف.

– تجنب مشاركة الآخرين في وصلات الإنترنت، لإحكام الرقابة ودرء للمسؤولية[1].

– استخدام أكثر من محرك بحث في البحث عن المعلومات التي تريدها، وعدم الاعتماد على محرك بحث واحد، مع ضرورة استخدام برامج الحماية المضادة للفيروسات والملفات التلصصية والرسائل الخادعة، ومداومة تحديث تلك البرامج.

– غلق جميع الحسابات الخاصة بك، مثل E-mail, Messenger, Facebook قبل الخروج من شبكة الإنترنت وفي حالة فقد الاتصال أثناء المحادثة يجب إعادة الدخول للموقع مرة أخرى من خلال الأيقونة الخاصة بالبرنامج، وليس من خلال صفحة كتابة كلمة المرور مباشرة، وذلك لاحتمالية أن تكون صفحة مزيفة شبيهة بالصفحة الأصلية لسرقة البريد الإلكتروني.

– ضرورة وجود بريد إلكتروني بديل يرتبط بعنوان البريد الإلكتروني الأساسي، لمعرفة أي تعديلات قد تتم على البيانات الرئيسية بعنوان البريد الإلكتروني الأساسي مثل كلمة السر، ملف تعريف المستخدم...إلخ، وقت حدوث تلك التعديلات بما يتيح استخدام الإجراءات اللازمة لاستعادة الحسابات الأصلية بعد تغييرها.

– عدم الشراء من أي موقع إلكتروني باستخدام بطاقات الدفع الإلكتروني إلا بعد التأكد من السياسات الخاصة بالمحافظة على الخصوصية للمتعاملين معه.

– عدم الدخول على المواقع الإباحية وغرف الدردشة المشبوهة على شبكة الإنترنت.

ثانيا: احتياطات أمنية للعاملين في الجهاز الأمني، نظرا لانتشار الوسائل والوسائط المختلفة لنقل المعلومات، مع عدم الاهتمام والوعي بأمن المعلومات، استدعى الأمر وضع عدد من الضوابط الضرورية لأمن المعلومات الأمنية أثناء تداولها أو حفظها وهي كالتالي:

– عدم استخدام التطبيقات المختلفة وبكافة أنواعها كتلك الموجودة على الهواتف المحمولة الذكية في نقل أي بيانات أو معلومات تخص العمل الأمني.

– عدم تداول المعلومات الأمنية عبر البريد الإلكتروني الخاص بشبكة الإنترنت، أو عبر مواقع التواصل الاجتماعي، مع مراعاة عدم وضع الصور الشخصية للعاملين بالجهاز الأمني على تلك المواقع.

– عدم توصيل أجهزة حاسبات شخصية غير تابعة للجهاز الأمني للدخول على شبكة المعلومات الخاصة به، أو استخدامها للتعامل مع قواعد البيانات الخاصة بالجهة؛ لما يمثله ذلك من خطورة بالغة على أمن المعلومات واحتمالية إصابة الشبكة الخاصة به بالفيروسات.

---

[1] ضياء يحي السادات، المرجع السابق، ص23.

– عدم إنشاء بريد إلكتروني لأي من الجهات الأمنية إلا من طرف الجهة المحددة لتنفيذ ذلك عبر شبكة الإنترنت.

– حظر خروج أي شخص من قاعات الحاسب الآلي بوسائط إلكترونية متعددة محمل عليها أي بيانات متعلقة بالعمل الأمني، إلا في المأموريات الرسمية المصرح بخروجها.

– حسن التعامل مع أجهزة الحاسب الآلي ومراعاة الغلق الآمن لها، دون الغلق المفاجئ يدويا لما يسببه ذلك من تلف قواعد البيانات وأنظمة التشغيل المثبتة عليها.

– عدم تبادل وسائط التخزين دون عمل فحص مسبق لمنع انتشار الفيروسات.

– حظر الاستعانة بأي فنيين من خارج الجهاز الأمني وغير تابعين لأي من الشركات المتعاقد معها لإجراء عمليات الصيانة والإصلاح أو تعديل قواعد البيانات المتعلقة بالجهات الأمنية المختلفة.

المطلب الثاني: التعاون الدولي في مواجهة جرائم التكنولوجيا الحديثة

أدى التطور الهائل في عالم البرمجيات وتزايد الاعتماد على بنوك المعلومات والوسائل الإلكترونية في تنظيم نواحي الحياة كافة إلى وصول هذه التقنية في أيدي الخير والشر معا، ما أدى إلى استغلال البعض ممن يملكون المعرفة بالتقنية العالية لارتكاب الجرائم، سواء تلك الواقعة على تكنولوجيا المعلومات أو تلك التي ترتكب بواسطة المعلوماتية، وقد اكتسبت جرائم التكنولوجيا الحديثة طابعا دوليا ذلك لأنها عابرة للحدود، إلا أن هذا لا يعني اعتبارها من الجرائم الدولية التي ينظمها القانون الجنائي الدولي، فالركن الدولي فيها ليس ذات الركن المكون للجرائم الدولية، بل ركن آخر يتصل بالجرائم العالمية التي تعتبر في حقيقتها من الجرائم الداخلية التي يعاقب عليها قانون العقوبات ويرجع سر تسمية هذه الجرائم بالعالمية إلى مزاولة الإجرام فيها على مستوى عالمي عابر للدول.

وعن حجم ظاهرة الجريمة المتصلة بالتكنولوجيا الحديثة على الصعيد العالمي، فقد تنوعت صورها وتزايدت مخاطرها حتى باتت تشكل تهديدا للأمن القومي وللاقتصاد الدولي، ولذلك بات أمر التعاون الدولي في مجال مكافحة هذه الجرائم والوقاية منها أمرا لا مفر منه لعجز الدول فرادى عن ذلك، ولأن أثر هذه الجرائم أيضا لا يقتصر على النطاق الدولي بل يمتد إلى العالمية، قد تكون بلدان كثيرة متورطة في جريمة واحدة، لذا تشكل متابعة وحفظ سلسلة الأدلة تحديا كبيرا بل حتى الجرائم المحلية قد يكون لها بعدا دوليا، وربما تكون هناك حاجة إلى طلب المساعدة من جميع البلدان التي مرت الهجمة من خلالها، مما يستتبع التعاون بين البلدان في المجال القضائي وكذا التعاون في مجال تسليم المجرمين.

الفرع الأول: المساعدة القضائية الدولية

تعرف المساعدة القضائية الدولية بأنها كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم، وتتمتع المساعدة القضائية بأهمية كبيرة في مجال مكافحة الجرائم المتصلة بالتكنولوجيا الحديثة بشكل عام والماسة بسرية المعلومات الإلكترونية بشكل خاص، وتشكل جرائم الدخول غير القانوني والبقاء غير القانوني داخل النظام المعلوماتي والاعتراض غير القانوني للمعلومات الإلكترونية نموذجا لجرائم التكنولوجيا الحديثة عابرة الحدود، باعتبار أنها ترتكب في معظم حالاتها عن بعد وعبر الحدود، وسنتناول في هذا المطلب أهمية المساعدة القضائية المتبادلة ومجالاتها.

البند الأول: أهمية المساعدة القضائية المتبادلة

يتعدى أثر جرائم تقنية المعلومات الحديثة في غالب الأحيان حدود الدول، فقد يكون مرتكب الهجوم في بلد ما ويتم شن الهجوم في بلد آخر، وتقع الآثار المترتبة على ذلك في بلد ثالث، وقد يرتكب المجرم جميع مراحل جريمته في دولة لم تطأها قدماه أصلا من قبل، لذا تقتضي فعالية التحقيق والملاحقة القضائية تتبع أثر النشاط الإجرامي من خلال تقفي أثر قناة الاتصالات بالجهاز مصدر الهجوم والجهاز الضحية أو بأجهزة أخرى تعمل مع مقدمي خدمات الإنترنت في دول مختلفة ولتحديد مصدر الجريمة، غالبا ما يتعين على أجهزة التحقيق الاعتماد على السجلات التاريخية التي تبين متى، من أين ومن الذي أجرى التوصيلات المختلفة، وفي أحيان أخرى قد يتطلب إنفاذ القانون تتبع أثر التوصيل وقت إجرائه، وقد يصطدم المحققون أثناء ذلك بصعوبات قانونية تنجم عن مشاكل الحدود –وهو ما يحدث في أغلب الأحيان– وهنا تظهر أهمية المساعدة القانونية والقضائية المتبادلة بين سلطات التحقيق في الولايات القضائية في مختلف الدول.

كان التعاون القضائي والقانوني بين الدول محدودا لعدة أسباب أبرزها تعقيدات وبطء إجراءات تبادل المساعدة القضائية التقليدية وعدم فاعليتها، فقد يستغرق اتخاذ الإجراء شهورا، الأمر الذي لا يتناسب مع ضرورة توخي السرعة في التعامل مع الأدلة الرقمية غير الملموسة وسريعة الزوال، ومن زاوية أخرى قد يؤدي غياب المساعدة القانونية والقضائية المتبادلة أو بطئها، إلى أن يجري المحققون في إحدى الدول التي تسعى إلى الحصول على المعلومات في حواسيب موجودة في دولة أخرى عمليات بحث عابرة للحدود تكون هي الأخرى غير مرخص بها في النظم الحاسوبية، لذا فإنه لابد من اعتماد آليات للتعاون وتبادل المساعدة تتلاءم مع طبيعة الجرائم المتصلة بالتكنولوجيا الحديثة تمكن المحققين من الحصول على المعلومات بصورة عاجلة.

البند الثاني: مجالات المساعدة القضائية لمواجهة جرائم التكنولوجيا الحديثة

لا تزال العديد من الإجراءات الرسمية الواردة باتفاقات المساعدة القانونية المتبادلة القائمة تتسم بنوع من التعقيد والبطء وهو ما لا يتناسب مع الطبيعة السريعة للجرائم المتصلة بالتكنولوجيا الحديثة، لذا فإنه كان من اللازم استحداث وسائل أخرى للتعاون أكثر سرعة وفاعلية للتصدي لهذه الجرائم، سنحاول استعراض تلك المجالات في ضوء الاتفاقيات الخاصة بالجرائم المعلوماتية مثل اتفاقية بودابست[1] المتعلقة بالجريمة الإلكترونية 2001، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

تنص المادة 23 من اتفاقية بودابست المتعلقة بالجريمة الإلكترونية على أنه: "يجب على الأطراف أن تتعاون مع بعضها البعض وفقا لأحكام هذا الفصل، في تطبيق الأصول الدولية المتصلة بالتعاون الدولي في المواد الجنائية، والاتفاقيات المعتمدة على التشريعات المتماثلة أو النظيرة والقوانين المحلية، إلى أوسع نطاق ممكن لأغراض التنقيب والتحري أو الإجراءات الجنائية المتعلقة بالجرائم الجنائية المرتبطة بنظم وبيانات معلوماتية أو لجمع أدلة ذات شكل إلكتروني للجريمة الجنائية".

---

[1] تعد اتفاقية بودابست 2001 المتعلقة بالجريمة الإلكترونية نموذجا عالميا للاتفاقيات في مجال مكافحة جرائم التكنولوجيا الحديثة، حيث إن هذه الاتفاقية غير قاصرة على دول الاتحاد الأوروبي، فقد انضمت إليها كل من كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية، كما أنه يمكن لأية دولة في العالم الانضمام لها أيضا، وتعد هذه الاتفاقية من أول الاتفاقيات الدولية التي عرفت جرائم الإنترنت وتتضمن أحكام إجرامية محددة وأحكاما تتعلق بالتعاون الدولي. كريستينا سكولمان، المرجع السابق، ص40.

وقد بينت هذه المادة المذكرة التفسيرية لهذه الاتفاقية أين أقرت ثلاث مبادئ عامة تحكم التعاون الدولي وهي كالآتي[1]:

– يجب على جميع الأطراف التعاون مع بعضها البعض في أوسع نطاق ممكن، وهذا المبدأ يفرض التزاما على الدول الأطراف بأن يزيلوا ما استطاعوا من العقبات التي تحول وهذا التعاون في جمع الأدلة وتدفق المعلومات على المستوى الدولي، والالتزام هنا في تقديرنا هو التزام بتحقيق نتيجة وليس فقط ببذل عناية وإلا لن يؤتي هذا المبدأ ثماره.

– إن التعاون لابد أن ينفذ وفقا لأحكام هذا الفصل الخاص بمواجهة جرائم التكنولوجيا الحديثة عن طريق التعاون الدولي من هذه الاتفاقية، وتطبيقا للأصول الدولية المتصلة بالتعاون الدولي في المواد الجنائية والاتفاقيات المعتمدة على التشريعات المماثلة والقانون المحلي، وبمقتضى هذا المبدأ نجد أن المادة 23 لا تبطل شروط الوثائق الدولية المتعلقة بالمساعدة القضائية وتسليم المجرمين والاتفاقيات الأخرى النظيرة بين الدول الأطراف بالنسبة لهذه الوثائق، أو شروط القانون المحلي المتعلقة بالتعاون الدولي.

بالإضافة إلى مجالات التعاون الدولية التي تضمنتها اتفاقية التعاون القضائي الدولية والإقليمية على النحو السالف بيانه فقد تضمنت هذه الاتفاقية بعض صور مجالات التعاون القضائي والتي تتناسب مع طبيعة الجرائم المتصلة بالتكنولوجيا الحديثة يمكن إجمالها فيما يلي:

أولا: المساعدة القضائية المتبادلة في مجال الإجراءات العاجلة، وتشمل المجالات الآتية:

1– التحفظ العاجل على بيانات الحاسب المخزنة: تناولت هذا الإجراء المادة 29 من هذه الاتفاقية والتي تنص على أنه: "يجوز لأي طرف أن يطالب طرفا آخر أن يأمر أو بالأحرى أن يتحفظ على بيانات مخزنة بواسطة وسائل إلكترونية، يقع داخل إقليم ذلك الطرف الآخر والتي بشأنها ينوي الطرف الطالب تقديم طلب بالمساعدة المتبادلة من أجل البحث أو الدخول أو مصادرة أو تأمين أو كشف هذه البيانات...إلخ، وعند استلام الطلب من الطرف الآخر، يقوم الطرف المطلوب منه باتخاذ كافة الإجراءات الملائمة وذلك لسرعة التحفظ على البيانات المحددة وفقا للقانون الوطني لأغراض الاستجابة لا يلزم وجود ازدواجية في الجريمة كشرط لتوفير مثل هذا التحفظ...إلخ"[2].

والمساعدة المتبادلة في التحفظ العاجل على البيانات المخزنة في النظام المعلوماتي المنصوص عليه في المادة السابقة، هو أمر ضروري تستلزمه طبيعة الأدلة في جرائم التكنولوجيا الحديثة، وذلك لتفادي أي تغيير في هذه الأدلة أو نقلها أو إتلافها ومحو آثار الجريمة خلال المدة التي تستغرقها إجراءات طلب المساعدة المتبادلة للحصول على تلك البيانات بالطرق التقليدية، وعملية التحفظ هي إجراء ذو طبيعة وقتية للتدخل بطريقة أكثر سرعة من مجرد تنفيذ التماس أو طلب المساعدة المتبادلة التقليدي.

بالإضافة إلى ما يتميز به هذا الإجراء من سرعة، فإنه يعد أقل تدخلا، ولعل ذلك راجع إلى أنه إجراء لا يتطلب من سلطات الدولة الموجه إليها طلب المساعدة نزع البيانات من الجهة القائمة عليها والاستحواذ عليها، وإنما مضمون هذا الإجراء أن تقوم تلك السلطات باتخاذ الإجراءات التي تضمن أن الجهة التي بحوزتها المعلومات موضوع طلب المساعدة –غالبا ما تكون هذه الجهة هي مزود الخدمة أو شخص ثالث– لا تقوم بمحو هذه البيانات لحين صدور أمر بتحويلها إلى سلطات تنفيذ القانون في وقت

---

[1] هلالي عبد الله أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست، دار النهضة العربية، القاهرة، 2011 ص241-243.

[2] يقابلها المادة 37 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

لاحق، كما يتسم هذا الإجراء بأنه إجراء لا يمس بسرية المعلومات والبيانات محل الإجراء الوقتي موضوع الطلب، فلا يتم كشفها ولا فحصها من قبل سلطات تنفيذ القانون إلا في بعض الحالات ووفقا للشروط المقررة قانونا بما يكفل حق الشخص المعني بالمعلومات في الخصوصية بسرية.

جدير بالذكر أنه يوجد اتجاه نحو استبعاد تطبيق قاعدة التجريم المزدوج بالنسبة لكل الوسائل الإجرائية ما عدا الأكثر تطفلا أو تدخلا في الحياة الخاصة كالتفتيش والتنصت، والتحفظ على البيانات والمعلومات المخزنة إلكترونيا لا يعد من وجهة نظر واضعي الاتفاقية من قبيل التطفل أو التدخل في الحياة الخاصة، ويرون أن كل ما يفعله الحارس على البيانات أو القائم عليها هو المحافظة عليها بأن تبقى في حيازته بشكل قانوني وأن يحافظ عليها من المحو أو الإتلاف، وألا يتم الكشف عنها أو فحصها من قبل سلطات الدولة مقدمة الطلب إلا بعد تقديم طلب المساعدة وفقا للإجراءات الرسمية بغرض كشف سرية هذه البيانات والمعلومات.

وقد أعطى البند الرابع الدول الأطراف الحق في اشتراط أو التمسك بمبدأ التجريم المزدوج استثناء للرد على طلب المساعدة المتبادلة في هذا المجال، إلا أن نطاق هذا الاستثناء مقيد بالجرائم غير الواردة في المواد من 02 إلى 11 من هذه الاتفاقية، وهذه الجرائم هي الولوج غير القانوني، الاعتراض غير القانوني، الاعتداء على سلامة البيانات، الاعتداء على سلامة النظام وإساءة استخدام أجهزة الحاسب ومعداته، التزوير المعلومات، الغش المعلوماتي، الجرائم المتصلة بالمواد الإباحية، الجرائم الواقعة على الملكية الفكرية والحقوق المجاورة، الشروع والاشتراك، بالإضافة إلى تجميع الأدلة تحت شكل إلكتروني للجريمة الجنائية، أي أن هذا الاستثناء يمكن أن يطبق بالنسبة للحالات التي تكون فيها الجريمة مرتكبة باستخدام نظام معلوماتي أو بالنسبة للجرائم التي تكون فيها الجريمة لم ترتكب بواسطة نظام معلوماتي ولكن يمكن أن تكون محلا لجمع أدلة ذات شكل إلكتروني، فالجرائم الواردة بالمواد 02-11 يفترض أن تستوفي شرط التجريم المزدوج بطريقة آلية بين الطرفين[1].

2- الافشاء العاجل لسرية بيانات المرور المتحفظ عليها: يتكامل هذا المجال من التعاون مع المجال السابق، ففي غالب الأمر يظهر هذا المجال بمناسبة المجال السابق، فالمادة 30[2] من ذات الاتفاقية تنص على أنه: "في حالة ما إذا اكتشف الطرف المطلوب منه، أثناء تنفيذ الطلب المقدم إليه وفقا للمادة 29 من أجل التحفظ على خط سير بيانات تتعلق باتصال محدد، أن أحد مقدمي الخدمة في دولة أخرى مشتركا في نقل الاتصال يقوم الطرف المطلوب منه على الفور بالكشف عن القدر الكافي من خط سير البيانات لتمكن مقدم الخدمة من التعرف هذا المسار الذي سلكه الاتصال".

ما يحدث في هذه الحالة أنه عندما يقوم الطرف المقدم إليه الطلب بتنفيذ ما طلب منه بالتحفظ على بيانات المرور المتعلقة بنقل الاتصال بواسطة مزودي الخدمات من خلال تتبع مصدر الاتصال لتحديد هوية مرتكب الجريمة أو تجميع الأدلة، قد يكتشف أثناء ذلك أن بيانات المرور التي وجدت في إقليمه تشير إلى أن الاتصال قد تم إرساله من خلال مزود خدمات موجود في إقليم دولة ثالثة أو حتى في اقليم الدولة مقدمة الطلب، فإنه في هذه الحالة يجب على الدولة المقدم إليها الطلب أن تقوم بالكشف للدولة الطالبة عن القدر الكافي من البيانات من خط سير البيانات الذي يمكنه من التعرف على مزود الخدمة، والمسار الذي سلكه

[1] هلالي عبد الله أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست، المرجع السابق، ص276 و277.

[2] يقابلها المادة 38 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

الاتصال، وفي ذلك فائدة للدولة مقدمة الطلب حيث تتمكن من خلال هذه المساعدة معرفة الدولة التي تقدم إليها طلب المساعدة العاجلة بشأن التحفظ على البيانات والمعلومات المخزنة في النظام المعلوماتي وهكذا حتى يتم الوصول إلى المصدر الحقيقي للاتصال[1].

ثانيا: المساعدة القضائية المتبادلة في مجال سلطات التحقيق، وتشمل أهم المجالات الآتية:

1- المساعدة المتبادلة الخاصة بالولوج إلى البيانات المعلوماتية المخزنة: جاء في نص المادة 31[2] من الاتفاقية على أنه: "يجوز لأي طرف أن يطلب من طرف آخر القيام بالبحث في بيانات الكومبيوتر، أو الدخول عليها، أو مصادرتها، أو تأمينها أو الكشف عنها، تكون مخزنة بواسطة نظام كومبيوتر داخل إقليم الطرف المطلوب منه، بما في ذلك البيانات التي تم التحفظ عليها وفقا للمادة 29 يستجيب الطرف المطلوب منه الطلب من خلال تطبيق الوثائق والترتيبات والقوانين الدولية المشار إليها بالمادة 23، وطبقا للنصوص القانونية الأخرى ذات الصلة في هذا الباب..."، وتتشابه هذه المادة مع البند ج من الفقرة الثانية من المادة 18 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة والخاصة بتقديم المساعدة القانونية المتبادلة بالكامل بمقتضي قوانين الدولة متلقية الطلب ومعاهداتها واتفاقاتها وترتيباتها ذات الصلة بشأن تنفيذ عمليات التفتيش والضبط والتجميد، وبمقتضى المادة 31 سالفة الذكر يحق لإحدى الدول الأطراف في الاتفاقية بمناسبة تحقيقات تجريها في جريمة ما أن تطلب من دولة طرف أخرى يقع على إقليمها النظام المعلوماتي تفتيش هذا النظام والدخول إليه والتحفظ أو مصادرة البيانات المخزنة بداخله لمصلحة الدولة مقدمة الطلب، تماما كما هو الحال بالنسبة لعمليات التفتيش والضبط التي تجريها الدولة المقدم إليها الطلب على البيانات والمعلومات المخزنة إلكترونيا في النظم المعلوماتية الموجودة في إقليمها، وهو ما يفرض على الدول الأطراف أن تكون مؤهلة لتلبية تلك الطلبات من الناحية الفنية والتقنية، ووفقا للبند الثاني من هذه المادة فإنه يسري بشأن هذا الطلب الشروط المقررة في المعاهدات والاتفاقيات والتشريعات الوطنية المطبقة في هذا الخصوص.

2- الدخول عبر الحدود إلى البيانات المعلوماتية المخزنة بتصريح: يعد هذا المجال الذي تضمنته المادة 32[3] من اتفاقية بودابست من مجالات المساعدة القضائية المتبادلة الذي أفرزته طبيعة الجرائم المتصلة بالتكنولوجيا الحديثة التي تنص على أنه: "يجوز لأي طرف وبدون تفويض من أي طرف آخر،

أ- الدخول على بيانات كومبيوتر مخزنة متاحة علنا، وبغض النظر عن مكان تواجد البيانات جغرافيا،

ب- الدخول على، أو تلقي عن طريق نظام كومبيوتر في إقليمه، بيانات كومبيوتر مخزنة موجودة في طرف آخر، وذلك في حالة حصول ذلك الطرف على الموافقة القانونية والطوعية من الشخص الذي له السلطة القانونية في الكشف عن البيانات لذلك الطرف من خلال نظام الكومبيوتر المذكور".

في هذا الصدد ثار نقاش مطول بشأن المادة السابقة بين واضعي هذه الاتفاقية قبل إقراره بحالته هذه، حيث كان موضوع النقاش هو متى يكون مسموحا لأي دولة أن تدخل بشكل منفرد إلى بيانات ومعلومات مخزنة على إقليم دولة أخرى، وقد توصلوا من خلال مناقشتهم لعدة حلول مختلفة إلى تحديد الحالات التي يمكن أن يقبل فيها الدخول بشكل فردي، وتلك التي لا يجوز أن

---

[1] هلالي عبد الله أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست، المرجع السابق، ص278-280.

[2] يقابلها المادة 39 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

[3] يقابلها المادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

تكون مقبولة، وفي نهاية المطاف خلص أطراف النقاش إلى أن الحلول التي اتفق عليها الجميع بخصوص الدخول بشكل فردي هي ما يجب أن تتضمنه المادة 32 والتي جاءت بحالتين؛ الأولى عندما تكون المعلومات والبيانات التي تم الوصول إليها متاحة للجمهور أصلا، والثانية عندما يتم الوصول إلى هذه البيانات المخزنة خارج النطاق الإقليمي لدولة طرف أو تلقيها من خلال نظام معلوماتي يقع على إقليمها، وذلك بناء على موافقة قانونية أو إرادية من شخص يملك سلطة قانونية للكشف عنها[1].

فقد يحدث في الواقع أن تكون المعلومات المراد الإطلاع عليها بمناسبة التحقيق في جريمة مخزنة في نظام معلوماتي تقع خارج إقليم الدولة التي تجري التحقيق، ففي مثل هذه الحالة يكون بمقدور هؤلاء الأشخاص استعادة البيانات شريطة أن يكون لديهم سلطة قانونية تخولهم ذلك، بالإضافة إلى سلطة الكشف عنها وذلك بمحض إرادتهم لسلطات تنفيذ القانون، أو أن يسمحوا لهذه السلطات بالدخول إلى هذه البيانات، يستحسن هنا ومن باب احترام سيادة الدول والمجاملات الدولية، وتفاديا لأي إشكالية قد تثور بين الدول الأطراف بشأن تفتيش نظام معلوماتي يقع على إقليم إحداهما أن يتم إضافة شرط بالنسبة للحالة التي تقوم فيها سلطات الدولة بالدخول إلى النظام المعلوماتي الموجود في إقليم الدولة أخرى وتفتيشه وضبط ما بداخله من معلومات، مفاد هذا الشرط إخطار وإحاطة الدولة التي يقع في إقليمها النظام المعلوماتي المراد تفتيشه، بعملية الدخول وموافقة صاحب السلطة القانونية على تلك المعلومات والبيانات.

3- المساعدة المتبادلة في بخصوص جمع بيانات المرور في الوقت الفعلي: يقصد ببيانات المرور أو خط سير البيانات وفقا لأحكام المادة الأولى من اتفاقية بودابست، بيانات الكومبيوتر المتعلقة بالاتصال عن طريق منظومة كومبيوتر والتي تنشأ عن منظومة كومبيوتر، تشكل جوا في سلسلة الاتصالات، توضح مصدر الاتصال، والوجهة المرسلة إليها، والطريق الذي تسلكه ووقت وتاريخ، وحجم، ومدة، ونوع الخدمة المذكورة.

ففي الكثير من الأحيان، قد لا يكون بإمكان سلطات التحقيق ضمان تتبع خط سير الاتصال للوصول إلى مصدر الاتصال لاتباع أثره من خلال التسجيلات الخاصة برسائل سابقة، وذلك نتيجة قيام مزود الخدمة بحذف بيانات المرور بشكل آلي من حلقات الاتصال التي تمر بها عملية نقل الرسالة، لذا فإنه من الضروري بالنسبة لسلطات التحقيق في كل دولة أن يكون لها القدرة على الحصول على بيانات المرور خلال الوقت الفعلي بالنسبة للاتصالات التي تمر من خلال نظام معلوماتي لدى دولة أخرى.

في هذا الصدد نصت المادة 33[2] من نفس الاتفاقية على أنه: "1- يقدم الأطراف المساعدة المتبادلة لبعضهم البعض فيما يتعلق بتجميع خط سير البيانات بصورة عاجلة، والتي تكون لها علاقة باتصالات محددة في إقليمهم يتم نقلها بواسطة نظام كومبيوتر، وطبقا لنصوص الفقرة الثانية فإن هذه المساعدات تحكمها الشروط والإجراءات المنصوص عليها في القانون الوطني، 2- يقوم كل طرف بتقديم مثل هذه المساعدة على الأقل فيما يتعلق بالجرائم الجنائية التي يكون فيها تجميع خط سير البيانات بصورة عاجلة متاحة في قضية محلية مماثلة".

---

[1] يمكن تعريف الشخص الذي يملك سلطة قانونية للكشف عن البيانات والمعلومات الإلكترونية بأنه كل شخص طبيعي أو معنوي له كافة السلطات الممكنة بموجب قانون أو اتفاق على البيانات والمعلومات المخزنة إلكترونيا، بحيث يحق له استعماله واستغلاله والتصرف فيه. هلالي عبد الله أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست، المرجع السابق، ص288-290.

[2] يقابلها المادة 41 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

يتضح لنا من خلال هذا النص الزامية كل طرف بتجميع خط سير البيانات بصورة عاجلة وفي الوقت الفعلي لمصلحة الطرف الآخر الذي قد يكون الطريقة الوحيدة الجوهرية لتحديد هوية مرتكب الجريمة المتصلة بالتكنولوجيا الحديثة، فبالرغم من أن هذا الإجراء أقل تطفلا أو تدخلا، إلا أن الفقرة الثانية من الاتفاقية قد استخدمت مصطلح على الأقل لجميع الدول الأطراف على السماح بأوسع نطاق ممكن للمساعدة المتبادلة بهذا الشأن حتى في ظل غياب مبدأ التجريم المزدوج.

4- المساعدة المتبادلة في مسالة اعتراض بيانات المحتوي: نصت المادة 34 من ذات الاتفاقية على أنه: "يقدم الأطراف المساعدة المتبادلة لبعضهم البعض فيما يتعلق بتجميع أو تسجيل محتوى البيانات بصورة عاجلة والتي تتعلق باتصالات محددة يتم نقلها بواسطة نظام كومبيوتر وذلك بالحد الذي تجيزه الاتفاقيات والقوانين الوطنية واجبة التطبيق".

انطلاقا لما يشكله هذا الإجراء من مساس بحقوق الأفراد في الخصوصية لأنه ينطوي على تجميع وتسجيل البيانات التي يتم نقلها بواسطة نظام معلوماتي معين، فقد تم تحديد الالتزام بتوفير المساعدة المتبادلة المتعلقة بهذا الخصوص، كما أنه يجب أن يكون تقديم المساعدة المتبادلة في الحدود التي تسمح بها المعاهدات والقوانين الداخلية المطبقة لدى الدول الأطراف[1]، ونلاحظ أن هذا الإجراء مماثل لإجراء مراقبة المحادثات والمراسلات السلكية واللاسلكية أو تسجيل الأحاديث لمصلحة التحقيق الذي سنتعرض له بالبحث لاحقا.

الفرع الثاني: نظام تسليم المجرمين

يعتبر نظام تسليم المجرمين شكلا من أشكال التعاون بين الدول في مجال مكافحة جرائم التكنولوجيا الحديثة وحماية المجتمعات من أثرها الخطير، والتعاون الدولي في هذا المجال هو نتيجة طبيعية للتطورات التي حدثت في كافة المجالات ولم تعد الحدود القائمة بين الدول تشكل عائقا أمام مرتكبي هذه الجرائم، ولم يعد نشاطهم الإجرامي قاصرا على إقليم دولة واحدة بل يمتد أثره ليشمل عدة دول، فقد يحضر المجرم في بلد معين لارتكاب جريمته المتصلة بالتكنولوجيا الحديثة ويقوم في بلد آخر بالتنفيذ ويفر إلى بلد ثالث للابتعاد عن العدالة، وبذلك أصبح المجرم هنا دوليا.

ولما كانت أجهزة الدولة تعمل على تنفيذ القانون ولا تستطيع تجاوز حدودها الإقليمية لممارسة الأعمال القضائية على المجرمين الفارين خارج حدود الدولة، كان لابد من التعاون الدولي في مجال تسليم المجرمين الفارين وهذا يستتبع بدوره وجود تعاون تشريعي وقضائي وتنفيذي، فالدولة مادامت عضوا في المجتمع الدولي لابد لها من الإيفاء بالالتزامات المترتبة على ذلك ومنها استلام وتسليم المجرمين الهاربين من العدالة، وقد حرصت أغلب دول المجتمع الدولي على سن التشريعات الخاصة بتسليم المجرمين بالإضافة إلى عقد العديد من الاتفاقيات الإقليمية والدولية في هذا الصدد.

البند الأول: ماهية نظام تسليم المجرمين

يقصد بنظام تسليم المجرمين قيام الدولة المطلوب فيها التسليم، بتسليم شخص متهم موجود في إقليمها إلى الدولة طالبة التسليم، بناء على طلبها بغرض محاكمته عن جريمة معينة، وقد يكون التسليم بغرض تنفيذ حكم قد صدر ضده بالعقاب، والتسليم

[1] هلالي عبد الله أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست، المرجع السابق، ص292 و293.

بالمعنى السابق يختلف عن مفاهيم أخرى قد تختلط به فهو لا يعتبر من قبيل الإبعاد الذي يعد عملا إداريا تستقل باتخاذه الجهة الإدارية في حالات لا يمكن حصرها، ولا يعتبر كذلك من قبيل الطرد الذي تمارسه الدولة بما لها من سيادة على إقليمها متى ما رأت أن بقاء الشخص على إقليمها من شأنه أن يؤثر على وجودها أو أمنها، وتقوم فكرة التسليم على وجود علاقة بين دولتين سواء كان ذلك في اتفاقية تسمح لهما بذلك أو بناء على علاقات قوية أو تشريع قانوني يسمح بذلك.

أولا: مصادر نظام تسليم المجرمين، استقر الفقه على تصنيفها إلى ثلاثة مصادر كالآتي:

1- المعاهدات والاتفاقيات بين الدول: قد تكون هذه الاتفاقيات ثنائية، وهي التي تتم بين دولتين وفقا لشروط وضوابط موضوعة من قبل الدولتين، وقد تكون اتفاقيات ومعاهدات التسليم متعددة الأطراف، وقد وضعت الأمم المتحدة عام 1990 معاهدة نموذجية لتسليم المجرمين لتكون إطارا يساعد الدول التي تكون بصدد التفاوض على اتفاقيات التسليم، كما أقر مجلس وزراء الداخلية العرب قانونا نموذجيا لتسليم المجرمين.

2- القوانين الداخلية للدول: والتي تنظم عملية تسليم المجرمين، فهي تعتبر إحدى مصادر التسليم.

3- العرف الدولي: يمكن تطبيقه في حالة عدم وجود قانون داخلي أو اتفاقية لتسليم المجرمين.

ثانيا: أنواع نظام تسليم المجرمين، هناك عدة طرق لتسليم المجرمين وتختلف الطريقة في كل دولة بحسب نوع النظام التي تأخذ به، ويمكن إجمال هذه الأنظمة المتبعة في تسليم المجرمين فيما يلي:

1- التسليم القضائي: تكون فيه الجهة القضائية في الدولة هي صاحبة قرار التسليم ولا شأن لأي جهة أخرى بهذا الخصوص، قد تكون المحكمة هي المختصة بقرار التسليم بناء على الطلب المعروض لها من قبل النيابة العامة التي تلقت القرار فالمحكمة هي التي تفصل في طلب التسليم وقد يكون ذلك بإعطاء النائب العام السلطة في إصدار القرار من عدمه، ومن مميزات التسليم القضائي بأنه يمكن الشخص المطلوب تسليمه من تقديم دفاعه كما أنه لا وجود للمجاملات الدولية، إلا أننا نسجل له بعض السلبيات منها عدم وجود توازن بين الخبرة القانونية والأبعاد السياسية الدولية، والتي قد لا تتوافر لجميع القضاة بالسلطة القضائية وأيضا طول فترة المحاكمة التي من شأنها أن تدفع بالمحكمة إلى إصدار أمر بالإفراج المؤقت عن المطلوب تسليمه وعند ذلك يمكن للمطلوب تسليمه أن يهرب إلى دولة أخرى.

2- التسليم الإداري: يعد هذا النوع من تسليم المجرمين عملا من أعمال السيادة، أو تدبيرا من تدابير السلطة التنفيذية والتي لها كامل الصلاحية في إقرار التسليم من عدمه، ووفقا للاعتبار الذي تراه ملائما لها وهذا النوع من التسليم يكون بطلب من الإنتربول للدولة طالبة التسليم بشأن القبض على المتهم المطلوب إلى الدولة المطلوب منها التسليم، والتي تحيل الطلب إلى السلطة الإدارية المختصة للدراسة والبحث ومن ثم إصدار قرار الموافقة على التسليم، ومن إيجابيات هذا النظام السرعة في البت في طلب التسليم ويمتاز أيضا بالابتعاد عن الإجراءات الطويلة والمعقدة التي قد تحتاج إلى نفقات باهظة فيما إذا لجأت الدولة إلى النظام القضائي وأيضا يساعد على تحسين العلاقات بين الدول[1].

[1] يوسف المصري، الجرائم المعلوماتية والرقمية للحاسوب والإنترنت، دار العدالة للطباعة والنشر، القاهرة، ط1، 2011، ص107 وما بعدها.

ولهذا النظام بعض السلبيات نذكر منها إهداره لحقوق الأفراد في الدفاع عن أنفسهم، ووجود المجاملات والواسطة الدولية التي قد تحدث لصالح الدولة طالبة التسليم ويقع ضحيتها المتهم نفسه، ومن السلبيات الأخرى أنه غالبا ما يتم عن طريق السلطة التنفيذية التي ربما قد لا تتوافر لها ملكية الفحص القانوني لطلب التسليم وذلك لعدم توافر الثقافة القانونية المؤهلة لصلاحية إصدار مثل هذا القرار، ناهيك على أنه يتم في إطار من الكتمان مما يعني بعده عن الأجهزة الرقابية سواء القضائية أو التشريعية.

3- التسليم المختلط: هو أكثر أنواع التسليم انتشارا، يجمع بين التسليم القضائي والإداري، لأنه يوازي بين المصلحتين المتعارضتين -مصلحة الدولة طالبة التسليم ومصلحة الشخص المطلوب تسليمه-؛ فالسلطة القضائية تفحص الطلب وتمنح الشخص المطلوب تسليمه كافة الضمانات القانونية ويدافع عن نفسه بشرط ألا تقحم الدولة المطلوب منها التسليم نفسها في فحص وقائع الدعوى وتكتفي بما يرد إليها من مستندات ووثائق من الدولة الطالبة للتسليم.

البند الثاني: شروط وإجراءات تسليم المجرمين

يمكن حصر شروط وإجراءات التسليم فيما يلي:

أولا: شروط التسليم، غالبا ما تتفق شروط التسليم من حيث العناصر، لكنها تبقى محل اختلاف من حيث الموضوع وذلك بحسب حاجتها للتسليم واعتبارات المصالح الدولية التي تراعيها كل دولة.

1- التجريم المزدوج: يقصد به أن يكون الفعل المطلوب التسليم من أجله مجرما في تشريع كل من الدولة طالبة التسليم وكذلك تشريع الدولة المطلوب إليها التسليم، ولا عبرة للوصف أو التكييف القانوني الذي يطلق على الفعل عند تقرير توافر هذه الشروط والمعاقبة عليه فقد يختلف التكييف القانوني الذي توصف به الجريمة، فمثلا قد يكون الفعل معاقبا عليه في تشريع الدولة طالبة التسليم تحت مسمى جريمة توظيف الأموال بينما الفعل نفسه معاقبا عليه تحت مسمى جريمة النصب والاحتيال في الدولة المطلوب منها التسليم، وذلك لا يمنع من توافر شرط ثنائية أو ازدواجية التجريم، والتجريم المزدوج يجد أساسه في أن الدولة طالبة التسليم تبتغي من وراء طلبها محاكمة من نسب إليه ارتكاب السلوك الإجرامي أو تنفيذ العقوبة المحكوم بها عليه، وهذا يفترض بداهة أن السلوك مجرم في تشريعها، فإذا لم يكن مجرما فلا يتصور قيام حكم جزائي يقضي بعقوبة عليه هذا من ناحية، ومن ناحية أخرى لا يجوز مطالبة الدولة المطلوب إليها التسليم بإيقاع عقوبة على ارتكاب سلوك ما هو في الأساس غير مجرم وفقا لقانونها.

ونجد الكثير من الاتفاقيات والمعاهدات الدولية المتعلقة بتسليم المجرمين قد أكدت على شرط التجريم المزدوج، فنجد مثلا المادة الثانية من المعاهدة النموذجية للأمم المتحدة بشأن تسليم المجرمين، المادة الثالثة من اتفاقية جامعة الدول العربية للتعاون القضائي والمادة 24 من الاتفاقية الأوروبية للإجرام، واشترطت أيضا بالإضافة لازدواجية التجريم أن تكون الجريمة المطلوب من أجلها التسليم جناية أو جنحة معاقبا عليها بالسجن مدة معينة.

2- الشروط المتعلقة بالأشخاص المطلوب تسليمهم: هناك بعض الأشخاص لا يجوز تسليمهم، ويمكن تعدادهم على النحو التالي:

أ- عدم جواز تسليم الرعايا، وهو مبدأ استقر عليه المجتمع الدولي نصت عليه معظم التشريعات الوطنية والاتفاقيات فإذا ما قام شخص من رعايا الدولة بجريمة فلا يجوز تسليمه.

ب- عدم جواز تسليم من تم منحهم حق اللجوء السياسي، وهذا أيضا مبدأ سائر في أغلب التشريعات والاتفاقيات الدولية والإقليمية المتعلقة بتسليم المجرمين.

ج- عدم جواز تسليم من تمت محاكمته عن تلك الجريمة المطلوب تسليمهم لأجلها، وذلك متى كان الشخص المطلوب تسليمه قد ثبتت محاكمته عن الجريمة المطلوب تسليمه لأجلها فبرأ أو عوقب عنها ولا يجوز أيضا التسليم إذا كانت الجريمة قيد التحقيق وذلك حتى لا يتعرض الشخص المطلوب تسليمه لعقوبة مزدوجة.

3- الشروط المتعلقة بالجريمة المطلوب التسليم لأجلها: هناك ثلاثة اتجاهات تتبعها الدول لتحديد طبيعة الجرائم التي يجوز فيها التسليم نوجزها فيما يلي:

أ- أسلوب الحصر، يعتمد هذا الأسلوب على إدراج مجموعة من الجرائم على سبيل الحصر (قتل، نصب، غسيل الأموال،...إلخ) في قائمة ضمن القانون أو تلحق بالاتفاقية لتكون هذه الجرائم دون غيرها هي التي يتم التسليم من أجلها، ويعد هذا الأسلوب أقل الأساليب شيوعا بين الدول لأنه يؤدي إلى إفلات بعض المجرمين من العقاب متى كانت الجريمة المرتكبة غير واردة في القائمة.

ب- أسلوب جسامة الجريمة أو الحد الأدنى للعقوبة، هو الأسلوب الأكثر شيوعا في تحديد الجرائم التي يجوز التسليم فيها، وهو يعني أن تحدد الدول في تشريعاتها الداخلية أو في المعاهدات الثنائية أو متعددة الأطراف الحد الأدنى للعقوبة المقررة للجرائم التي يمكن أن يتم التسليم لأجلها.

ج- النظام المختلط، وهذا الأسلوب في تسليم المجرمين من الأساليب الشائعة، يضمن هذا الأسلوب درجة معينة من جسامة الجريمة المعاقب عليها في البلدين ليتم التسليم وفقا لها، كما أنه يضمن خضوع جرائم محددة تمثل خطرا على الدول الأطراف للتسليم دون النظر إلى جسامة الجريمة أو العقوبة المقررة لها.

وتجدر الإشارة أن المجتمع الدولي يسوده اتجاه عام يقضي بعدم التسليم من الجرائم السياسية؛ وذلك لأن المجرم السياسي لا يعتبر مجرما بالمعنى الذي يحمله هذا الاصطلاح في علم الإجرام أو علم الاجتماع من معنى، إذ غالبا ما يرتكب السلوك بهدف تحقيق أغراض وأهداف قومية قد تنطوي على أعمال بطولية لتحرير الأرض واستقلال الوطن والدفاع عن مبادئ سامية، وهذا الاتجاه له تطبيق في المادة الثالثة من معاهدة الأمم المتحدة النموذجية بشأن تسليم المجرمين، إضافة إلى المادة 30 من الاتفاقية الأمنية لدول مجلس التعاون الخليجي، ويشترط لجواز التسليم ألا تكون الدعوى العمومية أو الحكم القاضي يفرض عقوبة قد انقضت بأحد أساليب الانقضاء المحددة في التشريعات الوطنية للدولة الطالبة والمطلوب منها التسليم أو الدولة التي ارتكبت الجريمة على أرضها.

ثانيا: إجراءات التسليم، يقصد بها القواعد الإجرائية التي تتبع مع الدول الأطراف في عملية التسليم بهدف المحافظة على حقوق الإنسان وحريته وتأمين الصالح العام، وهذه الإجراءات تتقاسمها الدولتان الطالبة والمطلوب منها التسليم، تتقيد هذه الإجراءات ببعض الالتزامات الدولية أو التعاهدية، وسوف نحاول شرح إجراءات التسليم في العنصرين التاليين:

1- إجراءات الدولة طالبة التسليم: تبدأ الدولة طالبة التسليم إجراءاتها بالطلب وبرغبتها في استلام الشخص المطلوب تسليمه، فدونه لا يمكن أن ينشأ الحق في التسليم، ويقدم هذا الطلب كتابيا فلا يجوز أن يكون هذا الطلب شفاهيا، كأن يرسل برقيا أو تلغرافيا أو عن طريق الاتصال الإلكتروني، إلا في بعض الحالات المعينة التي تتميز بصفة الاستعجال وعلى سبيل الاستثناء.

ويكون مع طلب التسليم المستندات الدالة على ارتكاب الشخص المطلوب تسليمه والتي من شأنها إعانة أجهزة الدولة المطالبة بالتسليم على تعقب الشخص المطلوب والقبض عليه، وأيضا أن تشمل المستندات صورة من النصوص القانونية التي تعاقب على الفعل والأدلة التي تثبت مسؤولية الشخص المطلوب، وتتعهد الدولة طالبة التسليم بأنها لن تلاحق أو تحاكم أو تعاقب المطلوب تسليمه من أجل جريمة سابقة على التسليم غير الجريمة أو الجرائم التي كانت محل طلب التسليم، وتتعهد بمحاكمة الشخص المطلوب تسليمه محاكمة عادلة ونزيهة، وأن توفر له ضمانات الدفاع عن نفسه، ويكون النظام القضائي للدول هو الجهة التي يناط بها إعداد طلب التسليم.

2- **إجراءات الدولة المطلوب منها التسليم**: يمكن تقسيمها إلى ثلاث مراحل أساسية:

أ- المرحلة الأولى: تكون في تلقي الطلب واتخاذ الإجراءات التي من شأنها التحري وجمع الأدلة والقبض على الشخص المطلوب ويكون ذلك من اختصاص الشرطة.

ب- المرحلة الثانية: تتمثل في سؤال واستجواب الشخص المقبوض عليه وحبسه احتياطيا أو إطلاق سراحه بكفالة أو بغير كفالة أو منعه من السفر إلى أن يتم الفصل في الطلب ويختص بذلك الادعاء العام.

ج- المرحلة الثالثة: وتشمل فحص الطلب من المحكمة المختصة، والبت في الطلب بالقبول أو الرفض، وتدرس المحكمة توافر بعض الشروط الشكلية من قبل الدولة طالبة التسليم كوجود ملف للتسليم واحتوائه على جميع الأوراق والوثائق المصدقة من الجهات المختصة في الدولة طالبة التسليم، وأيضا توافر بعض الشروط الموضوعية مثل شرط ازدواجية التجريم أو عدم انقضاء الدعوى العمومية أو العقوبة ومن عدم وجود أي من موانع التسليم المنصوص عليها في القانون، ويعتبر قرار المحكمة بالتسليم قرارا استشاريا حيث يعود الأمر إلى الحكومة في تسليم الشخص من عدمه، وإذا تخلفت الشروط السابقة فللمحكمة أن ترفض طلب التسليم، وفي هذه الحالة يتعين على الحكومة رفض الطلب أيضا.

وفي حالة الموافقة على طلب التسليم فإن القانون أوجب على الدولة طالبة التسليم أن تتقدم لاستلامه خلال 30 يوما من تاريخ إخطارها بالموافقة على طلب التسليم، والأوجب إخلاء سبيله ولا يجوز القبض عليه مرة ثانية أو اتخاذ إجراء في شأنه إلا بناء على طلب جديد، يستلم الشخص أغراضه التي كانت في حوزته أثناء القبض عليه، وفيما يتعلق بنفقات التسليم فإنه وفقا لما هو مستقر عليه تكون على الدولة طالبة التسليم ما لم يتم الاتفاق على غير ذلك[1].

البند الثالث: مظاهر التعاون الدولي في مجال تسليم المجرمين

تؤدي جرائم التكنولوجيا الحديثة غالبا إلى أضرار مادية وأخرى معنوية تلحق بالأشخاص والمشروعات العاملة في مجال تقنية المعلومات، وهو الأمر الذي يثير التساؤل حول الوسائل الوقائية لمكافحة هذه الجرائم، وأدى ذلك إلى الاهتمام دوليا في مواجهة الجرائم المتصلة بالتكنولوجيا الحديثة، على أن النظر إلى الجهود المبذولة على المستوى الدولي لمكافحة هذه الجرائم المستحدثة إنما يتحدد أساسا في ضوء الاتفاقيات الدولية المناهضة لهذه الأخيرة من ناحية أولى ثم المؤتمرات الدولية التي انعقدت في هذا الشأن من

[1] يوسف المصري، المرجع السابق، ص111 وما بعدها.

إيجاد الحلول التشريعية لمواجهة هذه الجرائم والندوات والملتقيات الدولية المنعقدة لمناقشة هذه الجرائم والاتفاقيات الدولية الثنائية أو متعددة الأطراف لمكافحة هذه الجرائم من ناحية ثانية[1].

ومن أبرز الاتفاقيات الدولية التي أبرمت لمكافحة جرائم التكنولوجيا الحديثة تبرز لنا الاتفاقية التي وقعت في العاصمة المجرية بودابست في عام 2001 التي صيغت من طرف عدد كبير من خبراء القانون في أوروبا ودول أخرى[2]، وفي مجال تسليم المجرمين نجد من الاتفاقيات متعددة الأطراف بشأن تسليم المجرمين، الاتفاقية الأوروبية المتعلقة بتسليم المجرمين سنة 1957 وبروتوكولاتها الإضافية سنة 1975-1978، والاتفاقية الأمنية الخليجية لعام 1994، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية في سنة 2000، بالإضافة إلى ما سبق يوجد نوع آخر من مظاهر التعاون الدولي في مجال تسليم المجرمين يتمثل في الاعتراف المتبادل بأوامر القبض أو الحبس أو التوقيف وبمقتضاه تصدر السلطة المختصة بإحدى الدول أمرا بالقبض أو الحبس أو التوقيف، وتعترف بصلاحية دولة أخرى أو أكثر ويتعين تنفيذه.

الفرع الثالث: الصعوبات التي تواجه التعاون الدولي وطرق الحد منها

نظرا لتطور التقنية في شبكات الاتصال، تنقل المعلومات والبيانات من مناطق متباعدة باستخدام تقنيات لا يكفل لها أمنا كاملا، ويتاح في ظلها التلاعب عبر الحدود بتلك المعطيات المنقولة أو المخزنة مما قد يسبب لبعض الدول أو الأفراد أو الشركات أضرارا فادحة، ولذلك لابد من التعاون في مكافحة هذه الجرائم، إلا أن هذا التعاون والمناداة به تواجهه صعوبات ومعيقات تحول دون تحققه وتجعله صعب المنال.

البند الأول: الصعوبات التي تواجه التعاون الدولي

حتى يسهل لكل دولة الاستمرار والعيش مع غيرها من الدول فإنها تحتاج إلى قدر من الأمن والنظام، وتشكل جرائم التكنولوجيا الحديثة إحدى القضايا الرئيسية في الكثير من دول العالم، وتشغل بال الحكومات والمختصين والأفراد على حد سواء ولقد أثبت الواقع العملي أن أي دولة لا تستطيع بجهودها المنفردة القضاء على هذا النوع من الجرائم مع هذا التطور الملموس والمذهل في كافة ميادين الحياة نتيجة لتطور الاتصالات وتكنولوجيا المعلومات وظهور الإنترنت والانتشار الواسع والسريع لها، التي باتت تشكل خطرا لا على سرية النظم والبرمجيات أو سلامتها أو توافرها فحسب، بل تعدت إلى أمن البنى الأساسية الحرجة[3]، مما استوجب تعاونا دوليا في هذا المجال لمكافحة هذا الإجرام المستحدث، إلا أنه ثمة صعوبات ومعوقات تقف دون تحقيقه أهمها:

أولا: عدم وجود نموذج موحد للنشاط الإجرامي، نظرا لعدم وجود مفهوم عام مشترك بين الدول حول نماذج النشاط المتعلق بجرائم التكنولوجيا الحديثة، ونظرا لاختلاف المفاهيم الخاصة بها التي ترجع إلى اختلاف التقاليد والأعراف القانونية الدولية

---

[1] محمد علي العريان، المرجع السابق، ص23 وما بعدها.

[2] هلالي عبد الله أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001، المرجع السابق، ص01 وما بعدها.

[3] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، القاهرة، 2005، ص102.

فإن هذا يضعف من منظومة القانون الدولي في مجال ضبط تلك الجرائم، وبالتالي يسهل على الجناة الإفلات من المساءلة الجنائية[1].

يضفي عدم توفر تعريف موحد للجريمة المتصلة بالتكنولوجيا الحديثة إلى بقاء بعض الأفعال الجرمية دون تجريم، فتكون أفعالا مجرمة في تشريع ما، ومباحة في تشريع آخر لاختلاف تحديد عناصر الجرم المعلوماتي بين الدولتين المعنيتين[2]، وتثير الطبيعة الدولية للجريمة –محل دراستنا– مشاكلا فيما يتعلق بتحديد القانون الواجب التطبيق (قانون الدولة التي ارتكب فيها الفعل أم قانون الدولة التي ظهرت فيهما الآثار الضارة)، إضافة إلى تعارض القوانين من الناحية الموضوعية والإجرائية الأمر الذي يستلزم ضرورة العمل على توحيد التشريعات فيما يتعلق بمكافحة الجرائم المتصلة بالتكنولوجيا الحديثة إضافة إلى إبرام الاتفاقيات في هذا المجال[3].

ثانيا: تنوع واختلاف النظم القانونية الإجرائية، يرجع سبب تنوع واختلاف النظم القانونية الإجرائية إلى طرق التحري والتحقيق والمحاكمة التي تثبت فائدتها وفاعليتها في دولة ما وقد تكون عديمة الفائدة في دولة أخرى أو قد لا يسمح بإجرائها، كما هو الحال بالنسبة للمراقبة الإلكترونية، والتسليم المراقب والعمليات المستترة، وغيرها من الإجراءات الشبيهة، فإذا ما اعتبرت طريقة ما من طرق جمع الأدلة أو التحقيق أنها قانونية في دولة معينة، فإنها قد تكون غير مشروعة في دولة أخرى، بالإضافة إلى أن السلطات القضائية لدى الدولة الثانية قد لا تسمح باستخدام أي دليل إثبات تم جمعه بطرق ترى هذه الدولة أنها طرق غير مشروعة حتى وإن كان هذا الدليل تم الحصول عليه في اختصاص قضائي وبشكل مشروع[4]، وتعتبر قضية الدودة الحاسوبية التي اعتمدت في الفلبين عام 2000، وقيل أنها عطلت ملايين الحواسيب في جميع أنحاء العالم، أحسن مثال على اختلاف النهج القانوني بين الدول، أين أعاقت هذه القضية التحقيقات بسبب أن ذلك العمل المؤذي والضار لم يكن آنذاك مجرما بشكل كاف في الفلبين[5].

ثالثا: عدم وجود قنوات اتصال، يعد الحصول على المعلومات والبيانات المتعلقة بالجريمة والمجرمين أهم الأهداف المرجوة من التعاون الدولي في هذا المجال، ولتحقيق هذا الهدف كان لزاما توفر نظام يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة أو معلومات مهمة، فعدم وجود مثل هذا النظام يعني عدم القدرة على جمع الأدلة والمعلومات العملية التي غالبا ما تكون مفيدة في التصدي لجرائم معينة ولمجرمين معينين، وبالتالي تنعدم الفائدة من هذا التعاون[6]، ويعتبر عدم وجود الاتصال والتنسيق فيما يتعلق بالإجراءات الجنائية المتبعة في شأن الجريمة المتصلة بالتكنولوجيا الحديثة بين الدول المختلفة، خاصة ما تعلق منها بأعمال الإستدلال أو التحقيق، سيما وأن عملية الحصول على الدليل في مثل هذه الجرائم خارج نطاق حدود الدولة عن طريق

---

[1] إيهاب ماهر السنباطي ميخائيل السنباطي، الجرائم الإلكترونية، الجرائم السيبرانية، قضية جديدة أم فئة مختلفة؟، التناغم القانوني هو السبيل الوحيد الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، يونيو 2007.

[2] فريد منعم جبور، المرجع السابق، ص215.

[3] عواطف محمد عثمان عبد الحليم، جرائم المعلوماتية، صورها وجهود مكافحتها دوليا، إقليميا ووطنيا، مجلة العدل، العدد 24، السنة 10، وزارة العدل إدارة التأصيل والبحوث والتدريب، السودان، 2008، ص68.

[4] براء منذر كمال عبد اللطيف، ناظر أحمد منديل، التعاون القضائي الدولي في مواجهة جرائم الانترنت، المؤتمر العلمي الأول، تحولات القانون العام في مطلع الألفية الثالثة، كلية القانون، جامعة تكريت، العراق، 2009، ص11.

[5] مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، البند الثامن من جدول الأعمال المؤقت، التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة بما فيها الجرائم الحاسوبية، المنعقد بالبرازيل في الفترة 12-19 أفريل 2010، رقم A/CONF 213/9.

[6] براء منذر كمال عبد اللطيف، ناظر أحمد منديل، المرجع السابق، ص12.

الضبط أو التفتيش في نظام معلوماتي معين هو أمر غاية في الصعوبة، فضلا عن الصعوبة الفنية في الحصول على الدليل ذاته[1].

رابعا: مشكلة الاختصاص، أثارت جرائم التكنولوجيا الحديثة مسألة الاختصاص على المستوى الدولي، بالرغم من أنه لا توجد أي مشكلة بالنسبة للاختصاص على المستوى الوطني، حيث يتم الرجوع إلى المعايير المحددة قانونا لذلك، ينجم عن اختلاف التشريعات والنظم القانونية تنازع في الاختصاص بين الدول في إطار الجرائم المتصلة بالتكنولوجيا الحديثة التي تتسم بعبورها للحدود.

فقد يحدث أن ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي، فهنا تكون الجريمة خاضعة للاختصاص الجنائي للدولة الأولى استنادا إلى مبدأ الاختصاص الشخصي، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى فتدخل عندئذ في اختصاصها استنادا إلى مبدأ العينية، كما تثار فكرة تنازع الاختصاص القضائي في حالة تأسيس الاختصاص على مبدأ الإقليمية كما لو قام الجاني ببث الصور الخليعة ذات الطابع الإباحي من إقليم دولة معينة وتم الإطلاع عليها في دولة أخرى، ففي هذه الحالة يثبت الاختصاص وفقا لمبدأ الإقليمية لكل دولة من الدول التي مستها الجريمة[2].

يلاحظ أن الاختصاص القضائي بنظر الجرائم التي تتم عبر شبكة الإنترنت والقانون الواجب تطبيقه على الفعل لا يحظ بالوضوح أو القبول أمام حقيقة أن غالبية هذه الأفعال تتم من قبل أشخاص من خارج حدود الدولة أو أنها تمر عبر شبكات معلومات وأنظمة معلومات خارج الحدود، حتى عندما يرتكبها شخص من داخل الدولة على نظام في الدولة نفسها، وهو ما يبرز أهمية اختبار مدى ملائمة قواعد الاختصاص والقانون الواجب تطبيقه وما إذا كانت النظريات والقواعد القائمة في هذا الحقل تطال هذه الجرائم أو يتعين إفراد قواعد خاصة بها في ضوء خصوصيتها وما تثيره من مشكلات في حقل الاختصاص القضائي، ويرتبط بمشكلات الاختصاص وتطبيق القانون مشكلات امتداد أنشطة الملاحقة والتحري والضبط والتفتيش خارج الحدود[3]، فقد أدى البعد الوطني لهذه الجرائم لتشتت الجهود وإعاقة التعاون الدولي في مجال التصدي لهذا النوع من الإجرام وذلك لاختلاف الإجراءات الجنائية أو النزاع حول القانون الواجب التطبيق[4].

خامسا: التجريم المزدوج، يعتبر شرط التجريم المزدوج من أهم الشروط الخاصة بنظام تسليم المجرمين، فهو شرط منصوص عليه في أغلب التشريعات الوطنية والاتفاقيات الدولية المعنية بتسليم المجرمين، وعلى الرغم من أهميتهإلا أنه يشكل عقبة أمام التعاون الدولي في مجال تسليم المجرمين في مجال جرائم التكنولوجيا الحديثة، سيما وأن معظم الدول لا تجرم هذه الجرائم، بالإضافة إلى أنه من الصعوبة تحديد فيما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تنطبق على الجرائم –محل دراستنا–.

يجد شرط التجريم المزدوج أساسه في أن الدولة طالبة التسليم تبتغي من وراء طلبها محاكمة من نسب إليه ارتكاب السلوك الإجرامي أو تنفيذ العقوبة المحكوم بها عليه وهذا يفترض بداهة أن السلوك مجرم في تشريعها، حيث أنه إذا لم يكن مجرما فلا يتصور

---

[1] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، المرجع السابق ص104 و105.

[2] حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الإنترنت، المرجع السابق، ص52 و53.

[3] عبد الله عبد الكريم، جرائم المعلوماتية والإنترنت، الجرائم الإلكترونية، دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والإنترنت مع الاشارة إلى جهود مكافحتها محليا وعربيا ودوليا، المرجع السابق، ص47 و48.

[4] محمود أحمد عبابنة، المرجع السابق، ص35.

وجود دعوى عمومية أو ملاحقة جزائية ضد الشخص المتهم كما لا يتصور قيام حكم جزائي يقضي بعقوبة من ناحية، ومن ناحية أخرى لا يجوز مطالبة الدولة المطلوب منها التسليم بتوقيع عقوبة على ارتكاب سلوك ما هو في الأساس غير مجرم وفقا لقانونها[1] ويرجع هذا إلى عدم وجود معاهدات ثنائية أو جماعية بين الدول على نحو يسمح بالتعاون المثمر في مجال هذه الجرائم، وحتى في حال وجودها فإن هذه المعاهدات قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم التكنولوجيا، ما يستدعي تطور هذه الجرائم بذات السرعة ومن ثم يظهر الأثر السلبي في التعاون الدولي[2].

سادسا: الصعوبات الخاصة بالإنابة القضائية الدولية، تنبعث الإنابة القضائية الدولية من الواجبات أو الالتزامات التي يفرضها القانون الدولي العام على الأمم المتحدة، وبموجبها يعهد للسلطات القضائية –المطلوب منها اتخاذ إجراء – القيام بالتحقيق أو بالعديد من التحقيقات، لمصلحة السلطة القضائية المختصة في الدول الطالبة للمساعدة، مع مراعاة احترام حقوق وحريات الإنسان المعترف بها عالميا، وبمقابل ذلك تتعهد الدولة الطالبة للمساعدة بالمعاملة بالمثل، واحترام النتائج القانونية التي توصلت إليها الدولة المطلوب منها المساعدة القانونية[3]، تهدف الإنابة القضائية إلى نقل الإجراءات في المسائل الجنائية، لمواجهة ما تشهده الظواهر الإجرامية من تطور، وتذليل العقبات التي تعترض سير الإجراءات الجنائية المتعلقة بقضايا تمتد خارج الوطن، والإنابة القضائية تجد أساسها في القوانين الوطنية والاتفاقيات الدولية ومبدأ المعاملة بالمثل، يتم إرسال طلب الإنابة القضائية عبر القنوات الدبلوماسية فمثلا طلب الحصول علي دليل إثبات وهو عادة من شأن النيابة العامة تقوم المحكمة المختصة في الدولة الطالبة بتوثيقه، ثم يمر بعد ذلك عن طريق وزارة الخارجية إلى سفارة الدولة متلقية الطلب، لتقوم هذه الأخيرة بإرساله بعد ذلك إلى السلطات القضائية المختصة في الدولة متلقية الطلب[4].

تتسم أعمال الإنابة القضائية الدولية بالبطء والتعقيد، الأمر الذي قد يتعارض مع طبيعة جرائم التكنولوجيا الحديثة، وما تتميز به من سرعة، كذلك من الصعوبات الكبيرة في مجال المساعدات القضائية الدولية المتبادلة التباطؤ في الرد، حيث أن الدولة متلقية الطلب غالبا ما تكون متباطئة في الرد سواء بسبب نقص الموظفين المدربين أو نتيجة الصعوبات اللغوية أو الفوارق في الإجراءات التي تعقد الاستجابة وغيرها من الأسباب.

في هذا الصدد أبرمت العديد من الاتفاقيات الجديدة التي ساهمت في تقصير الوقت واختصار الإجراءات عن طريق الاتصال المباشر بين السلطات المعنية بالتحقيق، مثال ذلك الاتفاقية الأمريكية الكندية التي تنص على إمكانية تبادل المعلومات شفويا في حالة الاستعجال، ونفس الشيء نجده في البند الثاني من المادة 30 من معاهد منظمة المؤتمر الإسلامي لمكافحة الإرهاب

---

[1] حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الإنترنت، المرجع السابق، ص26.

[2] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، المرجع السابق ص105.

[3] تعرف الإنابة القضائية بأنها طلب من السلطة القضائية المنيبة إلى السلطة المنابة، قضائية كانت أم دبلوماسية، أساسه التبادل باتخاذ إجراء من إجراءات التحقيق أو جمع الأدلة في الخارج، وكذا أي إجراء قضائي آخر يلزم اتخاذه للفصل في المسألة المثارة أو المحتمل اثارتها في المستقبل أمام القاضي المنيب ليس في مقدوره القيام به في نطاق دائرة اختصاصه. شائف علي محمد الشيباني، الإنابة القضائية الدولية في القانون اليمني، دراسة مقارنة، مقال موجه لدائرة التدريب والتأهيل، النيابة العامة، اليمن، 2006، ص10.

[4] حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الإنترنت، المرجع السابق، ص14.

الدولي عام 1999، والمادة 15 من اتفاقية الرياض العربية للتعاون القضائي لسنة 1983، والمادة 53 من اتفاقية شنغين[1] لعام 1990 والخاصة باستخدام الاتصالات المباشرة بين السلطات القضائية في الدول الأطراف إضافة إلى الفقرة 13 من المادة 46 من اتفاقية الأمم المتحدة لمكافحة الفساد، ويعتبر عامل السرعة من العوامل الرئيسية والهامة في مكافحة جرائم التكنولوجيا الحديثة ولكون غالبية هذه الاتفاقيات صدرت في وقت لم تكن شبكة الإنترنت قد ظهرت أو كانت محدودة فإن تعديل هذه الاتفاقيات التقليدية للتعاون الدولي أصبح ضرورة ملحة خاصة مع التطور الكبير في تكنولوجيا المعلومات والاتصالات[2].

البند الثاني: طرق القضاء على التحديات التي تواجه التعاون الدولي

هناك بعض الحلول التي يمكن عن طريقها القضاء على التحديات التي تواجه التعاون الدولي في مكافحة جرائم التكنولوجيا الحديثة، وفيما يتعلق بالعقبة الأولية المتمثلة في عدم وجود نموذج موحد للنشاط الإجرامي فإن الأمر يقتضي توحيد هذه النظم القانونية، ولاستحالة هذا الأمر فإنه لا مناص من البحث عن وسيلة أخرى تساعد على إيجاد تعاون دولي يتفق مع طبيعة هذا النوع المستحدث من الجرائم ويخفف من غلو الفوارق بين الأنظمة العقابية الداخلية، وتتمثل هذه الوسيلة في تحديث التشريعات المحلية المعنية بالجرائم المتصلة بالتكنولوجيا الحديثة، وإبرام اتفاقيات خاصة يراعى فيها هذا النوع من الجرائم، وأن تتم مراجعة لهذه الاتفاقيات بصفة دورية، وبالنسبة للعقبة الثانية والخاصة بتنوع واختلاف النظم القانونية الإجرائية نجد أن المواثيق الدولية الصادرة عن الأمم المتحدة غالبا ما تشجع الأطراف فيها على السماح باستخدام بعض تقنيات التحقيق الخاصة، الأمر الذي يفتح المجال أمام تعاون دولي فعال.

فمثلا المادة 20 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطن تشير في هذا الصدد إلى التسليم المراقب والمراقبة الإلكترونية وغيرها من أشكال المراقبة والعمليات المستترة[3]، والتي تعتبر من أهم التقنيات المستخدمة في التصدي للجماعات الإجرامية المنظمة، بسبب الأخطار والصعوبات الكامنة وراء محاولة الوصول إلى عملياتها وتجميع المعلومات وأدلة الإثبات لاستخدامها فيما بعد في الملاحقات القضائية المحلية منها أو الدولية في دول أطراف؛ في سياق نظم المساعدة القانونية المتبادلة.

وهذا ما أكدت عليه الاتفاقية الأوربية للإجرام المعلوماتي حيث تضمنت المادة 29 منها على سرية حفظ البيانات المعلوماتية المخزنة وأجازت لكل طرف أن يطلب من الطرف الآخر الحفظ السريع للمعلومات المخزنة عن طريق إحدى الوسائل

---

[1] يتكون نظام معلومات شنغين من قسم مركزي مقره مدينة ستراسبورغ، وأقسام وطنية في كل دولة من الدول المنظمة، كذلك به بنك معلومات كبير تسجل فيه المعلومات التي ترسله اليه قوات الشرطة والسلطات القضائية في كل دولة، من بين هذه المعلومات عناوين الأفراد سواء المطلوب تسليمهم من قبل دول اخرى، أو الممنوعين من دخول أرض دولة ما، أو المعلن اختفاؤهم أو المطلوب تقديمهم للعدالة بأمر قضائي لأي سبب كان، ولا يتم الرجوع لنظام المعلومات شنغين إلا في حالة القيام بإجراءات المراقبة على الحدود من طرف الشرطة والجمارك، وكذلك تسليم تأشيرات الدخول وكذا الإقامات.
جون فرونسوا هنروت، أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، 19 و20 يونيو 2007، ص109.

[2] براء منذر كمال عبد اللطيف، ناظر أحمد منديل، المرجع السابق، ص12.

[3] المادة 11 من اتفاقية 1988 بشأن التسليم المراقب، والمادة 50 من اتفاقية الأمم المتحدة لمكافحة الفساد.

الإلكترونية الموجودة داخل النطاق المكاني للطرف الآخر، والتي ينوي الطرف طالب المساعدة أن يقدم طلبا للمساعدة بشأنها بغرض القيام بالتفتيش أو الدخول بأي طريقة مماثلة، وضبط أو الحصول أو الكشف عن البيانات المشار إليها.

كما أكدت المادة 30 من ذات الاتفاقية على الكشف السريع عن البيانات المحفوظة حيث نصت على أنه عند تنفيذ طلب حفظ البيانات المتعلقة بالتجارة غير المشروعة والمتعلقة باتصال خاص تطبيقا لما هو وارد في المادة 29 فإن الطرف المساند إذا اكتشف أن مؤدي الخدمة في بلد آخر قد شارك في نقل هذا الاتصال فإن عليه أن يكشف على وجه السرعة إلى الطرف طالب المساعدة كمية كافية من البيانات المتعلقة بالتجارة غير المشروعة حتى يمكن تحديد هوية مؤدي الخدمة، وهذا الطريق الذي تم الاتصال من خلاله[1].

كما أشارت المادة 31 من هذه الاتفاقية إلى المساعدة المتعلقة بالدخول إلى البيانات المحفوظة، حيث أجازت لأي طرف أن يطلب من أي طرف آخر أن يقوم بالتفتيش أو أن يدخل بأي طريقة مشابهة وأن يضبط أو يحصل بطريقة مماثلة، وأن يكشف عن البيانات المحفوظة بواسطة شبكة المعلومات داخل النطاق المكاني لذلك الطرف والتي يدخل فيها أيضا البيانات المحفوظة وفقا للمادة 29، ويجب الاستجابة لمثل هذا الطلب بأسرع ما يمكن، ويمنح كل طرف تلك المساعدة على الأقل بالنسبة للجرائم التي يكون جميع المعلومات بشأنها في الوقت الحقيقي متوافر في الأمور المشابهة على المستوى المحلي، وجاء في المادة 34 من ذات الاتفاقية والتي نصت على التعاون في مجال التقاط البيانات المتعلقة بمضمون الاتصالات النوعية التي تتم عن طريق إحدى شبكات المعلومات.

نلاحظ مما سبق أن الاتفاقية الأوربية للإجرام المعلوماتي أوجدت بعض الحلول التي من شأنها التغلب على مشكلة اختلاف النظم الإجرائية أمام التعاون الدولي لمواجهة الجرائم التكنولوجيا الحديثة، وللحد من ظاهرة عدم وجود قنوات اتصال بين جهات تنفيذ القانون، فنلاحظ أنه غالبا ما تشجع المواثيق الدولية مجموع الدول إلى التعاون فيما بينها وتدعوها إلى إنشاء قنوات اتصال بين سلطاتها المختصة ووكالاتها ودوائرها المتخصصة بغية التيسير في الحصول على هذه المعلومات وتبادلها[2].

ومن الأمثلة على هذه المواثيق الدولية اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة في المادة 27 منها، والمادة 09 من اتفاقية 1988، والمادة 48 من اتفاقية الأمم المتحدة لمكافحة الفساد، والبند الثاني من المادة 27 من الاتفاقية الأوربية بشأن الإجرام المعلوماتي، والمادة 35 من ذات الاتفاقية الأوربية والتي أوجبت على الدول الأطراف فيها ضرورة تحديد نقطة اتصال تعمل لمدة 24 ساعة يوميا طوال أيام الأسبوع لكي تؤمن المساعدة المباشرة للتحقيقات المتعلقة بجرائم البيانات والشبكات، أو استقبال الأدلة ذات الشكل الإلكتروني، وهذه المساعدة تشمل تطبيق الإجراءات التالية بصفة مباشرة، إسداء النصيحة الفنية، حفظ البيانات وفقا للمادتين 29 و30، وجمع الأدلة وإعطاء المعلومات ذات الطابع القضائي وتحديد أماكن المشتبه فيهم[3].

---

[1] بلال عبد الكريم غالي، الحماية القانونية للإنسان من مخاطر المعلومات، أطروحة دكتوراه، كلية العلوم القانونية والاقتصادية والاجتماعية، الرباط 1995، ص18.

[2] ما جاء بتوصية المجلس الأوربي رقم R95-13 الصادرة في 1999/09/11، بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات.

[3] Charlotte-Marie et Pitrat-Laurent le veneux, Protection du consommateur et des données personnelles. Voir le site: www.finance.gouv.fr. Thierry Léonard, E-marketing et protection des données à caractère personnel, Publié le 22/05/2000, site : https://www.droit-technologie.org/dossiers/e-marketing-et-protection-des-donnees-a-caractere-personnel/

كما أوجبت ذات المادة على الدول الأطراف ضرورة أن تتمكن نقطة الاتصال من الاتصال السريع بنقطة اتصال الطرف الآخر، وأن يعمل كل طرف على تسهيل عمل الشبكة، أما بالنسبة لمشكلة الاختصاص في الجرائم المتصلة بالتكنولوجيا الحديثة فثمة حاجة ملحة إلى إبرام اتفاقيات دولية ثنائية كانت أو جماعية يتم فيها توحيد وجهات النظر فيما يتعلق بقواعد الاختصاص القضائي[1] بالإضافة إلى تحديث القوانين الجنائية الموضوعية منها والإجرائية بما يتناسب والتطور الكبير التي تشهده تكنولوجيا المعلومات والاتصالات، ولأجل القضاء على مشكلة التجريم المزدوج والذي يعد من أهم الشروط الخاصة بنظام تسليم المجرمين ركزت الاتجاهات والتطورات التشريعية على تخفيف التطبيق الصارم لهذا الشرط، وذلك بإدراج أحكام عامة في المعاهدات والاتفاقيات المعنية بتسليم المجرمين ويتم إما بسرد الأفعال التي تتطلب التجريم كجرائم أو أفعال مخلة بمقتضى قوانين الدولتين معا، أو بمجرد السماح بالتسليم لأي سلوك يتم تجريمه ويخضع لمستوى معين من العقوبة في كل دولة[2].

أما فيما يتعلق بالصعوبات الخاصة بالمساعدات القضائية الدولية والتباطؤ في الرد، فإننا نجد الحاجة ملحة إلى إيجاد سبل تتسم بالسرعة، تسلم من خلالها طلبات الإنابة كتعيين سلطة مركزية مثلا أو السماح بالاتصال المباشر بين الجهات المختصة في نظر مثل هذه الطلبات للقضاء على مشكلة البطء والتعقيد في تسليم طلبات الإنابة[3]، وهذا بالفعل ما أكد عليه مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية فحث على ضرورة تعزيز فعالية السلطات المركزية المعنية الضالعة في أعمال المساعدة القانونية المتبادلة وإقامة قنوات مباشرة للاتصال فيما بينها بغية ضمان تنفيذ الطلبات في الوقت المناسب.

أما بالنسبة للرد على طلبات التماس المساعدة فإنه من الضرورة بمكان الاستجابة الفورية والسريعة على هذه الطلبات لأجل ذلك تنص غالبية المعاهدات والاتفاقيات الخاصة بالمساعدات القضائية المتبادلة على ضرورة الاستجابة الفورية والسريعة على طلبات التماس المساعدة، وهذا ما أكدت عليه الفقرة الثالثة من المادة 25 من الاتفاقية الأوربية للإجرام المعلوماتي حيث نصت على أنه: "يمكن لكل طرف، في الحالات الطارئة أن يوجه طلبا للمعاونة أو للاتصالات المتعلقة بها عن طريق وسائل الاتصال السريعة مثل الفاكس أو البريد الإلكتروني..."، على أن تستوفي هذه الوسائل الشروط الكافية المتعلقة بالأمن وصحتها مع تأكيد رسمي لاحق إذا اقتضت الدولة المطلوب منها المساعدة في ذلك، وتقوم الدولة بالموافقة على هذا الطلب والرد عليه عن طريق إحدى وسائل الاتصال السريعة[4].

---

[1] المادة 22 من الاتفاقية الأوربية بشأن الإجرام المعلوماتي.

[2] أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، 1988، ص85.

[3] مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، 2001، ص77.

[4] أثارت هذه الحماية جدلا كبيرا في فرنسا قبل تدخل المشرع الفرنسي بالنص عليها صراحة في القانون رقم 85-660 الصادر في 03 يوليو 1985 وتباينت آراء الفقه والقضاء حول امتداد حماية حق المؤلف إلى برامج الحاسب الآلي بسبب الاختلاف حول توافر شروط المصنف المحمي في برامج الحاسب الآلي. محمد حسام محمود لطفي، الحماية القانونية لبرامج الحساب الآلي، دار الثقافة للطباعة والنشر، القاهرة، ط2، 1987، ص87 وما بعدها.

الفصل الثاني: الأحكام الإجرائية لمكافحة جرائم التكنولوجيا الحديثة

ترتكب جرائم التكنولوجيا الحديثة كما هو معلوم باستخدام التقنية المعلوماتية مما يعني أنها ترتكب في فضاء افتراضي مفرغ سواء ارتكبت عبر شبكة الإنترنت أو من خلالها، فهي بذلك تثير مشكلات موضوعية في تطبيق القواعد التقليدية لقانون العقوبات الذي صيغت جل نصوصه ونظمه الأساسية لتواجه سلوكا ماديا يرتكب في عالم مادي ملموس، فإذا كان ذلك هو حال القواعد الموضوعية للتجريم والعقاب، فما هو حال القواعد الإجرائية لهذا الفرع من القانون الجنائي في مواجهة هذا النوع من الجرائم، وهو ذلك الفرع الذي يتأسس في كل النظم القانونية المختلفة على مبدأ دستوري هو شرعية التجريم والعقاب، الذي تنبثق عنها قاعدة الشرعية الإجرائية[1].

ما يميز هذه الجريمة إذن هو أنها ترتكب في نطاق رقمي يختلف كليا عن النطاق التقليدي الذي ترتكب فيه الجريمة حيث يتم الإستدلال عليها وضبطها وإثباتها بالوسائل التقليدية المتمثلة في إجراءات الإستدلال والتحقيق، فهي إجراءات صيغت لضبط وإثبات جرائم ترتكب في عالم ملموس ماديا، يلعب فيه السلوك المادي الدور الأكبر والأهم، وهنا يثور التساؤل حول مدى صلاحية هذه الإجراءات لضبط وإثبات جريمة ارتكبت في عالم افتراضي غير ملموس.

كما أثار انتشار المعلومات بشكل واسع وكبير على شبكة الإنترنت بعض التساؤلات حول مسؤولية مزودي ووسطاء الإنترنت بخصوص ما ينشر من معلومات بواسطتهم، إذ تعتبر مسؤولية أشخاص الإنترنت من أهم المسائل التي دار النقاش حولها لأن هذا الموضوع يجمع بين ثناياه مسائل تتعلق بالمساس بحرية التعبير، وبإضفاء صفة الفضاء الحر وغير المقيد على شبكة الإنترنت أو يتعلق بما يدعو له البعض من ضرورة فرض الرقابة على شبكة الإنترنت بناء على جوانب أخلاقية بهدف حماية الحقوق الشخصية للأفراد على الشبكة، ذلك أنه كلما تشددنا في إقامة مسؤولية مزودي ووسطاء الإنترنت كلما زاد حرصهم على فرض الرقابة الذاتية على المعلومات لدرء المسؤولية عنهم مما قد يؤدي إلى تقييد حرية التعبير والحد من انتشار الإنترنت[2]، بالمقابل كلما تجاهلنا إقامة مسؤولية هؤلاء المزودين كلما أدى ذلك إلى وجود أكبر للمعلومات غير المشروعة على الشبكة، مما يزيد تبعا لذلك تقاعس المزودين عن استخدام الوسائل اللازمة لمنع انتشار هذه المعلومات غير المشروعة.

وقد ثار الجدل حول المركز القانوني لمقدمي الخدمات، ودورهم في الوصول الأمثل لاستخدام الشبكة، الذين تذرعوا كثيرا من أجل التخفيف من الالتزامات التي ألقاها القضاء في بداياته على عاتقهم لإرساء نظام خاص يعفيهم من المسؤولية، سواء عن إخلالهم بتقديم الخدمة أو عن عدم مشروعية المضمون المعلوماتي المتداول عبر أجهزتهم، الأمر الذي ولد الكثير من الإشكاليات القانونية والفنية، مما أوجب تدخل مختلف التشريعات لحسم الجدل، ولوضع نظام قانوني خاص بمقدمي خدمات الإنترنت، حددت من خلاله بدقة الأحكام الخاصة بمسؤوليتهم عما يحدث من مخالفات عبر الشبكة.

---

[1] هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، المرجع السابق، ص18. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، المرجع السابق، ص113 وما بعدها.

[2] عايد رجا الخلايلة، المسؤولية التقصيرية الإلكترونية، المسؤولية الناشئة عن إساءة استخدام أجهزة الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمان 2009، ص207.

فالإشكالية هنا تكمن في محاولة تحديد من سيكون مسؤولا عن المعلومة غير المشروعة المنتشرة على شبكة الإنترنت في ضوء تعدد الأشخاص المتدخلين في عملية نشر المعلومة، بدءا من مؤلف المعلومة، إلى منتجها، وموردها، ثم إلى الشخص الذي يتولى توريد منافذ الدخول وإيصال المشتركين بالشبكة، فمورد أو متعهد الإيواء الذي يتولى تخزين المعلومات، وإيواءها على موقعه، يضاف إلى ذلك الدور الذي يقوم به كل من محركات البحث والمنتديات...إلخ، لذلك غالبا ما يجد الضحية نفسه متضررا من المعلومة غير المشروعة دون أن يتمكن من تحديد المسؤول عن الضرر الذي لحقه.

وعلى ذلك سوف نقسم الفصل إلى المبحثين التاليين:

المبحث الأول: إجراءات جمع الدليل الإلكتروني

المبحث الثاني: المسؤولية الجنائية الناشئة عن جرائم التكنولوجيا الحديثة والعقوبات المقررة لها

المبحث الأول: إجراءات جمع الدليل الإلكتروني

تمثل قواعد الإثبات أهمية خاصة، هذا أن الحق موضوع التقاضي يتجرد من كل قيمة إذا لم يقم الدليل على الواقعة التي يستند إليها، فالدليل هو عصب الواقعة[1]، أو هو النتيجة التي تحققت باستعمال وسائل الإثبات المختلفة في إنتاج الدليل[2]، ويقصد بهذا الإثبات القواعد المتعلقة بالبحث عن الأدلة وإقامتها أمام القضاء وتقديرها من جانبه[3]، فالإثبات هو مجموع الأسباب المنتجة لليقين، مما يعني أن الإثبات في المواد الجنائية ما هو إلا كافة الأدلة التي تؤكد وقوع الجريمة، وتحقق حالة اليقين لدى القاضي لإدانة المتهم، أو ترجح حالة الشك لديه فيقضي بالبراءة، أو هو كل ما يؤدي إلى إظهار الحقيقة، ولأجل الحكم على المتهم في المسائل الجنائية يجب ثبوت وقوع الجريمة في ذاتها وأن المتهم هو المرتكب لها، أو بعبارة أخرى وقوع الجريمة بوجه عام ونسبتها للمتهم بوجه خاص[4]، وحتى يتحقق الدليل اللازم للإثبات؛ فإنه لا بد من جمع عناصر التحقيق والدعوى، وتقديم هذه العناصر إلى سلطة التحقيق الابتدائي، فإذا أسفر هذا التحقيق عن دليل أو أدلة ترجح معها إدانة المتهم فإن ذلك يستلزم تقديمه إلى المحكمة في مرحلة المحاكمة التي تعد أهم المراحل، لأنها مرحلة الجزم بتوافر دليل أو أدلة يقتنع بها القاضي بإدانة المتهم وإلا قضى ببراءته.

رتب الاستخدام غير المشروع لتقنية الوسائل والوسائط الإلكترونية العديد من الإشكاليات الإجرائية في مجال إجراءات الملاحقة الجنائية، التي تتبع من أجل كشف الجريمة وإقامة الدليل على وقوعها ونسبتها إلى مرتكبيها الذين يستخدمون التقنية المتطورة في ارتكابها وفي إخفاء معالمها وعدم ترك أية آثار مادية دالة عليها، وهذه صعوبة مع الصعوبات الأخرى التي تواجه الحصول على الدليل أدت إلى تدخل مشرعي بعض الدول لمواجهة هذا النوع من الجرائم، وذلك بإصدار قوانين خاصة بملاحقتها وتنظيم الإجراءات التي تناسبها دون مساس بحقوق الأفراد وحرياتهم الأساسية.

---

[1] أحمد ضياء الدين محمد خليل، مشروعية الدليل في المواد الجنائية، دراسة تحليلية مقارنة لنظريتي الإثبات والمشروعية في مجال الإجراءات الجنائية، أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، أكاديمية الشرطة، القاهرة، 1982، ص395 وما بعدها.

[2] رأفت عبد الفتاح حلاوة، الإثبات الجنائي قواعده وأدلته، دراسة مقارنة بالشريعة الإسلامية، دار النهضة العربية، القاهرة، ط1، 1996، ص05.

[3] محمد زكي أبو عامر، الإثبات في المواد الجنائية، الفنية للطباعة والنشر، الإسكندرية، 1985، ص19.

[4] Mutter Maler (C.J.A.), Traite de la preuve en matière criminelle, Trad Alexandre IMP Librairie générale de jurisprudence, Paris, 1884, p03.

أصبحت جرائم التكنولوجيا الحديثة تمثل ضربا من ضروب الذكاء الإجرامي الجديد، وباتت تتخذ أنماطا جديدة لا يجدي معها إتباع الإجراءات التقليدية، لما تثيره طبيعتها غير المادية من إشكاليات وما تؤديه التقنية الحديثة من دور في ارتكابها، وما توفره لها من مسرح غالبا ما يكون أقل ظهورا لحقائق موضوع البحث وأدلته، وذلك لوقوعها في عالم افتراضي، وطبيعة أدلتها غير ملموسة كما أن التطور التقني في شبكة الإنترنت سوف يقود دون شك إلى تغيير كبير –إن لم يكن كليا– في المفاهيم السائدة حول الدليل الإلكتروني من حيث ضرورة الاستعانة بالمختصين في مجال النزاع، وعلى ذلك سنتناول في هذا المبحث إجراءات جمع الدليل الإلكترونية التقليدية والحديثة مع التطرق لمفهوم الدليل الإلكتروني واختصاص الضبطية القضائية في هذا المجال.

المطلب الأول: دور الضبط القضائي في جرائم التكنولوجيا الحديثة

تحظى نظرية الإثبات باهتمام بالغ، خصوصا على الصعيد الجنائي، أين يتجرد الحق موضوع التقاضي من كل قيمة إذا لم يقم الدليل على الواقعة محل البحث، فالدليل هو قوام حياة الإثبات، لذا فإن نظرية الإثبات من أهم وأخطر النظريات القانونية فلا تنقطع المحاكم عن تطبيقها في كل ما يعرض عليها من القضايا.

الفرع الأول: تعريف الدليل الإلكتروني

يختلف الوسط الذي ترتكب فيه الجريمة من وسط مادي إلى ما يعرف بالوسط الافتراضي نتيجة التطور العلمي وانتشار التقنية الرقمية في التعاملات اليومية، وهو ما استتبع ظهور طائفة جديدة من الأدلة تتفق وطبيعة الوسط الذي ارتكبت فيه الجريمة وهي أدلة إلكترونية أو ما يسمى أدلة رقمية.

البند الأول: مفهوم الدليل الرقمي

ينشأ الدليل الجنائي بنشأة الجريمة ذاتها، انطلاقا من الإعداد لها وتنفيذها وتحقيق نتائجها حتى جني متحصلاتها أو التخلص من آثارها وأدواتها والوسائل المستخدمة في ارتكابها، فكل جريمة تصنع أدلتها، والمتمثلة في الآثار والمخلفات المادية والرقمية وكل المتغيرات التي تطرأ على النظام المعلوماتي.

يعرف الدليل على أنه: "برهان قائم على المنطق والعقل، في إطار الشرعية الإجرائية لإثبات صحة افتراض، أو رفع أو خفض درجة اليقين الإقناعي في واقعة محل الخلاف"[1]، كما يعرف بأنه: "وسيلة إثباتية مشروعة تسهم في تحقيق حالة يقين لدى القاضي بطريقة يطمئن إليها"[2]، أما فيما يتعلق بالدليل الرقمي نظرا لحداثة أسلوب تلك الجرائم، فقد تم التطرق إلى تعريفه بأنه دليل مأخوذ من أجهزة كمبيوتر أو الوسائل الإلكترونية الذكية، يكون في شكل مجالات أو نبضات مغناطيسية يمكن تجميعها وتحليلها باستخدام برامج أو تطبيقات تكنولوجية، وهي مكون رقمي لتقديم معلومات في أشكال متنوعة، مثل: كتابات أو صور أو أصوات أو أشكال أو رسوم، وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون، كما يمكن القول بأنه مجموعة مجالات أو نبضات

[1] أحمد أبو القاسم أحمد، الدليل المادي وأهميته في الإثبات الجنائي، دار الكتب القومية، القاهرة، ط2، 2005، ص142.

[2] عبد الحافظ عبد الهادي عابد، الإثبات الجنائي بالقرائن، مطابع الطوبجي التجارية، 1989، ص198.

مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية.

بناء على ما سبق يمكن تعريف الدليل الرقمي على أنه ذلك الدليل المستمد من أي نظام معلوماتي بمكوناته المادية أو المنطقية، في إطار من الشرعية الإجرائية لتقديمه للقاضي لتحقيق حالة اليقين لديه في الجريمة محل الدعوى، لتقرير البراءة أو الإدانة فيها، يتضح من هذا التعريف أن هناك بعض الشروط الواجب توافرها في الدليل الرقمي يمكن إجمالها أساسا فيما يلي:

– أن تكون هناك جريمة وقعت بالفعل، وبدأت جهات التحقيق في العمل على كشف غموض الجريمة لضبط الجناة وتقديمهم للمحاكمة تحقيقا للعدالة.

– أن يستمد هذا الدليل من أجهزة إلكترونية كالحاسب الآلي بمكوناته المادية من شاشة أو أجهزة ملحقة به من طابعة وماسح ضوئي أو أقراص مرنة...إلخ، أو مكوناته المنطقية (البرامج)، أو أي نظام معلوماتي آخر، مثل: التليفون المحمول، اللوحات الرقمية وماكينات السحب بالبنوك...إلخ.

– أن يتم استخراج الدليل الرقمي بطرق إجرائية مشروعة، حتى لا يفقد الدليل قيمته في عملية الإثبات الجنائي.

نستنتج أن الدليل الرقمي قد يكون رسالة، أو صورة، أو نص...إلخ، ويتم الوصول للدليل الرقمي لجريمة الإنترنت عن طريق الـ IP الخاص بالجهاز المستخدم في الجريمة، وهو مكون من أربع خانات، يشير الجزء الأول من اليسار للمنطقة الجغرافية التي يقع فيها الجهاز، والثاني للجهة المسؤولة عن الإنترنت في البلد، والثالث لشركة الإنترنت المشترك مع الجهاز، والرابع لجهاز الحاسب الآلي الذي تم الاتصال منه أثناء ارتكاب الجريمة.

البند الثاني: خصائص الدليل الإلكتروني

يتميز الدليل الجنائي بعدة خصائص عامة، سواء كانت مادية، فنية أو معنوية، وحتى يؤدي الدليل الجنائي وظيفته في الإثبات، فإنه يلزم أن تتوافر فيه بعض المقومات لتعطيه المكانة القضائية تتمثل إجمالا فيما يلي:

أولا: الجريمة تصنع أدلتها، الجريمة المتصلة بالتكنولوجيا الحديثة عبارة عن سلوك منحرف قام به الجاني للاعتداء على النظام المعلوماتي في حقوق ومصالح خاصة بالأفراد أو متعلقة بالمصلحة العامة للدولة أو المؤسسات التي تحظى بالحماية القانونية وقد ينطوي هذا السلوك على مواقف إيجابية قام بها الجاني كان يجب الامتناع عنها، أو مواقف سلبية يتخذها الجاني فيما يجب القيام به[1]، فكل ما يطرأمن أحداث على المسرح المعلوماتي من متغيرات مادية أو رقمية مستحدثة ما كانت لتحدث لولا وقوع الجريمة فالجريمة هي التي تصنع أدلتها التي تتشكل مقوماتها بمناسبة اقترافها.

ثانيا: كفاءة ممثلي السلطة ومدى التنسيق بينهم، إن كشف الدليل في الجرائم المتصلة بالتكنولوجيا الحديثة هو عملية تفكير وتخطيط ومتابعة محكمة من طرف موارد بشرية متمكنة في التعامل مع الأجهزة الإلكترونية وبرامجها، ولها القدرة على البحث عن الأدلة وفقا للحالة المعروضة أمامها وظروفها الخاصة، وقد حدد القانون الخطوات الإجرائية والشكلية التي تلتزم السلطات باتباعها

[1] برهامي أبو بكر عزمي، الشرعية الإجرائية للأدلة العلمية، دراسة تحليلية لأعمال الخبرة، دار النهضة العربية، القاهرة، 2006، ص109.

من كشف وقوع الجريمة حتى الفصل في الدعوى الناشئة عنها، كما صان المشرع الحريات الشخصية، وأقر عدم المساس بها إلا في الحدود التي يجيزها القانون، وهذه القواعد الإجرائية لا تحدد كيفية تنفيذ التفتيش ولا كيفية كشف المخابئ الخفية حتى يعطي هذا الإجراء أفضل النتائج الإيجابية، بل إن أمر ذلك متروك لفطنة المحقق حسب مدى كفاءته وخبراته السابقة.

ثالثا: صعوبة استخلاص الدليل، يختلف الإثبات الجنائي في الجرائم المتصلة بالتكنولوجيا الحديثة اختلافا جذريا عن الدليل في الجرائم التقليدية، إذ أنه ينصب في الغالب على اعتداء تم خلسة وانقضى، فتدخل السلطات التي يقع عليها عبء الإثبات يكون تدخلا لاحقا لوقوع الجريمة، التي قد تنتهي أغلب آثارها وأدلتها بضغطة زر واحدة، إذ أن الجريمة تقع في الغالب بغتة فتكون مفاجئة للمجني عليه والسلطات[1]، ويمثل الإثبات الإلكتروني الرقمي تحديا كبيرا للمحقق الجنائي لصعوبة اكتشاف الجريمة وإثباتها، كما أن هناك قدرا من الخفاء حيث يستطيع الجناة أن يخفوا شخصيتهم للقيام ببعض الأفعال المجرمة، ولهذا فإن التقدم التكنولوجي السريع في المجتمع من خلال رقمية المعلومات والبيانات يمثل تحديا أمام المحققين الذين تتطلب فيهم المهارة للصول لهدفهم المنشود[2].

رابعا: الأدلة الجنائية هي وسيلة إثبات، تقع الجريمة المعلوماتية ويكتشف أمرها في أي وقت طال أو قصر، التي تفرض التنقل إلى مسرح الجريمة لجمع الإستدلالات اللازمة من أجل اتخاذ إجراءات التحفظ على أجهزة النظام المعلوماتي المعتدى عليها تمهيدا لمباشرة سلطات التحقيق الابتدائي، ومنذ بداية تنفيذ الإجراءات الجنائية في الواقعة تبقى الصلة المباشرة بين وقائع الجريمة وبين أعضاء هيئة المحكمة والقاضي منقطعة، فلا مناص من أن تكون الأدلة الجنائية الرقمية هي الوسيلة الوحيدة لنقل هذه الأحداث إلى علم القاضي وإدراكه[3].

خامسا: تساند الدليل مع غيره من الأدلة، القاعدة الأساسية في الإثبات الجنائي أن الأدلة تساعد بعضها البعض مما يمكن القاضي من تكوين عقيدته في تقرير الإدانة أو البراءة، وذلك من خلال النظر إلى الأدلة مجتمعة، وقد يؤدي دليل واحد لترجيح كفة البراءة أو الإدانة، وللمحكمة الحق في تبيين الواقعة على حقيقتها، وأن ترد الواقعة لصورتها الصحيحة من مجموع الأدلة المطروحة دون التقيد بدليل معين.

سادسا: قطعية الدليل، يعبر اليقين عن حالة ذهنية أو عقلانية تؤكد وجود الحقيقة، يتم الوصول إلى ذلك عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من وقائع الدعوى، وما ينطبع في ذهنه من تصورات واحتمالات ذات درجة ثقة عالية من التوكيد، وترجح قطعية الدليل حينما يتوافر فيه اليقين ويرتبط بالركن المادي للجريمة، ولا يتعارض معه في عناصر الدعوي دليلا ماديا آخرا على مستواه من القيمة الثبوتية[4].

سابعا: الدليل الإلكتروني دليل تكنولوجي، إذا كان الدليل الإلكتروني هو دليل علمي فإن ذلك يثبت بالضرورة أن التقنية هي الخاصية الثانية التي يتمتع بها الدليل الإلكتروني، مما يوجب التعامل معه من قبل تقنيين متخصصين في العالم الافتراضي فالدليل الرقمي راجع أساسا لما تنتجه التقنية من نبضات رقمية تشكل قيمتها في إمكانية تعاملها مع القطع الصلبة التي تشكل

---

[1] برهامي أبو بكر عزمي، المرجع السابق، ص114.

[2] Thomas A. Johnson, Op.Cit., p05.

[3] برهامي أبو بكر عزمي، المرجع السابق، ص116.

[4] أحمد أبو القاسم أحمد، المرجع السابق، ص538.

الحاسب الآلي والأجهزة الإلكترونية الذكية بمختلف أنواعها[1].

وبالنظر لهذه الخاصية نجد أنه لابد على سلطات الضبط والتحقيق بناء منطق يقوم على أساس الخبرة، فمثلا سلطات التحقيق الجنائي في العديد من الدول كالولايات المتحدة الأمريكية توفر لسلطات الإستدلال والتحقيق كافة المقومات التكنولوجية الكاملة، وهو ما يعني وجوب الفصل بين الخبرة وسلطات الإستدلال والتحقيق فيما يتعلق بالدليل الإلكتروني، مع احتواء هذه السلطات على عناصر ذات خبرات عالية الكفاءة فيما يخص هذا الدليل[2].

والعلاقة في إطار بحث هذه الخاصية يجب أن تبنى على أساس الدور الذي يمكن أن تقوم به التقنية في كشف الدليل التقني، ومثل هذه العلاقة تحتاج إلى ملاحظة من ناحيتين، فمن ناحية يجب الاهتمام بتقنية البرامج التي تتعامل مع الدليل الرقمي من حيث اكتسابه أو التحفظ عليه، وتحليله وتقديمه، ومن ناحية أخرى فإن هذه البرامج ذاتها والتي تساهم تقنيتها في الحصول على الدليل يجب أن تكون موضع قبول لدى المحكمة وبما يفيد دلالته، ويجب أن يشار في محضر الإستدلال أو التحقيق أو الخبرة إلى التقنية البرمجية المستخدمة في الحصول على الدليل الرقمي.

يمكن أن تكون هذه الخاصية دعوة إلى سلطات الضبط القضائي والتحقيق لكي يمكنهما الشروع في بناء منطق لا ينسب إلى الخبرة، فمثلا سلطات التحقيق الجنائي في العديد من الدول وعلى رأسها الولايات المتحدة الأمريكية لديها مقومات الإستدلال والتحقيق والتقنية الكاملة وهو أمر يستفاد منه الفصل بين الخبرة وبين السلطات الأخرى كسلطات الإستدلال والتحقيق.

وذلك نتيجة لما تحظى به مؤسساتهم من هيكلة تقنية كبيرة، بل إنه يمكن القول إن مؤسسات الضبط القضائي وسلطات التحقيق في الولايات المتحدة الأمريكية وألمانيا ساهمت بشكل كبير في تطوير تكنولوجيا المعلومات من خلال البحث المستمر فيها ومن ثم فإن إطلاق الصفة الرقمية إنما تعني أنه ينبغي أن يكون هناك توافق بين الدليل المرصود وبين البيئة التي يعيش فيها، سواء كانت الجريمة المرتكبة احتيالا على بنوك أو مؤسسات مالية، أو كانت الجريمة قذفا وسبا أو تشهيرا علنيا في حلقات النقاش أو القوائم التراسلية أو غيرها وكذلك بثا وتداولا لصور وأفلام دعارة أطفال، وهذا ما يحتم استنباط الدليل من بيئته التي يعيش فيها وهي البيئة الرقمية أو التقنية، وهي في إطار جرائم التكنولوجيا الحديثة ممثلة في العالم الرقمي الذي يطلق عليه العالم الافتراضي، وهو العالم الكامن في الحاسب الآلي والخوادم والمضيفات والشبكات ويتم تداول الحركة فيه عبرها[3].

نتيجة لما سبق يمكن القول إن هناك إمكانيات كبيرة لتطوير المختصين في البحث الجنائي من حيث تطوير أدوات البحث في الدليل الرقمي، ثم إنه يمكن أيضا الاستفادة من منظور فهم التحفظ على الدليل الرقمي الذي يحتاج إلى تكاتف الجهود في هذا الإطار فيتوقع أن تكون عملية التحفظ على الدليل الرقمي بشكل مختلف عما هو عليه الحال في الدليل المادي، إذ لا يخضع الأمر لقواعد التفسير والتأويل والتي تحتاج إلى مراحل زمنية لكي يمكن إرساء فهم لها، فالأمر هنا يحتاج إلى تفاعل التقنية مع ذاتها.

---

[1] Christine Sgarlata Chung and David J. Byer, The Electronic Paper Trail, Evidentiary Obstacles to Discovery and Admission of Electronic Evidence, Boston University, Journal of Science & Technology Law, Boston, Massachusetts, USA, 22/11/1998, p19.

[2] فتحي محمد أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، دار الفكر والقانون، المنصورة، ط1، 2010، ص650 و651.

[3] Christine Sgarlata Chung and David J. Byer, Op.Cit., p20.

البند الثالث: مزايا وعيوب الدليل الإلكتروني

يتمتع الدليل الإلكتروني بمجموعة من المزايا والمساوئ يمكن إجمال أهمها فيما يلي:

أولا: مزايا الدليل الإلكتروني، يتميز الدليل الرقمي بسمات تميزه عن الدليل الجنائي التقليدي، وأهمها أن الدليل الرقمي يوجد بصفة أساسية في أجهزة الحاسب الآلي والأجهزة الإلكترونية الذكية أو شبكات الإنترنت، ما يتطلب دراية تامة ببعض السمات الفنية في التعامل معه، نحاول تلخيص كل واحدة منها على حدى.

1- الدليل الرقمي دليل علمي: يحتاج الدليل الرقمي إلى مجال تقني للتعامل معه، فلا يمكن الحصول على الدليل الرقمي سوى باستخدام الأساليب العلمية الحديثة، ومن ثم يجب أن يتعامل كل من رجال الضبط القضائي والتحقيق والمحاكمة مع الدليل الرقمي بأساليب علمية متطورة، سواء في استخراجه، حفظه، أو تقديمه كدليل إثبات حتى لا تسقط حجيته[1].

وغالبا ما يتم الاستعانة بالخبير، باعتباره الوحيد القادر على فهم وترجمة الدليل الرقمي، وإبداء الرأي في المسائل الفنية التي تحتاج إلى دراسة وتخصيص لا صلة لها بالقانون، وقد يحتاج القضاء إلى الاستعانة بالخبراء في الفصل والتعامل مع هذه الأدلة والاستفادة مما يقدمونه مباشرة بناء على الدليل المستمد من تقرير الخبير في بعض المسائل التي تحتاج إلى خبرة فنية.

2- الدليل الرقمي متطور ومتنوع: يمكن تقسيم الدليل الرقمي إلى ثلاث مجموعات كالتالي[2]:

أ- السجلات المحفوظة؛ في الحاسب الآلي ومختلف الأجهزة على البريد الإلكتروني، ورسائل غرف المحادثة على شبكة الإنترنت.

ب- السجلات التي تم إنشاؤها؛ بواسطة الحاسب الآلي، مثل log files، وسجلات الهاتف، وسجلات ماكينات الصرف بالبنوك، وفي جميع مخرجات برامج الحاسب الآلي.

ج- السجلات التي حفظ جزء منها بالإدخال وجزء آخر تم إنشاؤه بواسطة الحاسب الآلي، مثال: أوراق العمل التي تم إدخالها على برنامج مثل Excel.

وبالنظر إلى ذلك التقسيم نجد أن الدليل الرقمي متنوع تبعا للمصدر المستمد منه؛ ولذلك فالدليل الرقمي يشمل كافة أنواع البيانات الرقمية ذات الصلة بالجريمة التي يمكن استخراجها رقميا، لأن الدليل الرقمي يحتوي في داخله على مجموعة البيانات الرقمية المختلفة التي قد تكون نصوصا، صورا، وسمعيات ومرئيات...إلخ.

3- الدليل الرقمي يصعب التخلص منه: يتميز الدليل الرقمي بصعوبة التخلص منه بالمقارنة بغيره من الأدلة التقليدية كبصمة الإصبع، أو شهادة الشهود، أو الأوراق المكتوبة باليد، إلا أننا نجد أن بصمة الإصبع يمكن التخلص منها عن طريق مسح الدليل، وشهادة الشهود يمكن التخلص منها بأساليب كثيرة لتغيير شهادتهم.

أما الدليل الرقمي يمكن استرجاعه باستخدام برامج خاصة عند محاولة الجناة التخلص منه بالمسح أو التشفير، فلا يخفى علينا أنه عندما يشطب ملف من جهاز الحاسب الآلي مثلا يبقى موجودا على القرص الصلب، وباستخدام برمجيات من الطبيعة

---

[1] أحمد سعد محمد الحسيني، المرجع السابق، ص154.

[2] أحمد سعد محمد الحسيني، المرجع نفسه، ص156.

الرقمية ذاتها يمكن بمقتضاها استرداد كافة الملفات التي تم إلغاؤها أو إزالتها من الحاسب الآلي مثلا، ومن هذه البرامج (X Tree Pro Gold)، وهو برنامج يمكن المحقق من العثور على الملفات في أي مكان على الشبكة أو على القرص الصلب؛ ويستخدم البرنامج لقراءة البرامج في صورتها الأصلية، وبرنامج كشف الديسك (Ama Disk View Disk)، ومكن من الحصول على محفوظات القرص المرن، وبرنامج بدء تشغيل الحاسب الآلي (Bootable Diskette)، يمكن المحقق من تشغيل الكمبيوتر إذا كان نظام التشغيل فيه محميا بكلمة مرور.

أوصى بعض الخبراء في مرحلة جمع الأدلة الرقمية بوجوب جمع الأدلة بشكل دقيق، لأنه بمجرد مغادرة مسرح الجريمة يصبح من الصعب العثور على أية أدلة في حالة ما إذا أعيد التفتيش مرة أخرى، وذلك لكثرة المعلومات والمواقع التي يتم فحصها مع إمكانية محو الأدلة بضغطة زر واحدة، ويكون من السهل باستخدام الأدوات الصحيحة تحديد الدليل الرقمي والتعديل الذي أدخل عليه وذلك بمقارنته بالنسخة الأصلية[1].

4- إمكانية النسخ: يمكن نسخ الدليل الرقمي بنسخة مطابقة للأصل تماما، بحيث يمكن إجراء الفحص المعلوماتي على هذه النسخة لتفادي خطر إتلاف النسخة الأصلية أثناء عملية الفحص، وهذه الميزة لا تتوفر في الأدلة التقليدية[2].

5- إمكانية كشف التعديل: قد يتعرض الدليل الرقمي للتعديل المقصود من قبل الجاني، أو التعديل غير المقصود من قبل المحقق أو الخبير المعلوماتي أثناء عملية جمع الدليل، وفي كلتا الحالتين يمكن معرفة ما إذا كان الدليل الرقمي قد تعرض للتعديل أم لا وذلك باستخدام برمجيات تقنية معينة تستخدم في هذا الخصوص، إضافة إلى إمكانية إجراء المقارنة مع النسخة الأصلية إن وجدت[3].

ثانيا: مساوئ الدليل الإلكتروني، للدليل الرقمي عدة مساوئ، لعل أهمها ما يلي:

1- الدليل الرقمي دليل غير مرئي، ليس للدليل الرقمي طبيعة مادية ملموسة كما هو الحال في الأدلة التقليدية، فكل ما تنتجه التقنية هو عبارة عن نبضات إلكترونية يمكن أن تدل في مجموعها على أنماط السلوك الإنساني، والواقع أن هذه الطبيعة غير المرئية للدليل الرقمي تلقي بظلالها على أجهزة الضبط القضائي التي تتعامل مع هذه الجرائم المستحدثة، لأن غياب الدليل المرئي يشكل عقبة كبيرة أمام كشفها[4].

2- الحجم الكبير للبيانات التي يوجد فيها الدليل الرقمي: يحتوي القرص الصلب مثلا على حجم كبير من البيانات والمعلومات غير المرتبة، ولكن ما يتعلق بالجريمة قد يشكل جزءا صغيرا فقط من هذه المعلومات، ويمكن تشبيه حجم المعلومات بموجات الراديو الموجودة في الهواء والتي تحتوي على بيانات متشابكة، الأمر الذي يصعب معرفة مكان الإشارة المطلوبة وترجمتها إلى بيانات مفهومة، فالوصول إلى الدليل الرقمي المطلوب يشكل تحديا أمام الخبير المعلوماتي.

---

[1] Eoghan Casey, Digital Evidence and Computer Crime, Forensic Science, Computers, and the Internet, Academic Press, Cambridge, Massachusetts, United States, 3rd Ed., 2011, p16.

[2] Eoghan Casey, Op.Cit., p25.

[3] Eoghan Casey, Ibid., p25.

[4] جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، 2002، ص04.

3- الدليل الرقمي دليل ظرفي، الدليل الرقمي هو عادة دليل ظرفي، فمعرفة عنوان الإنترنت IP مثلا يشير إلى الحاسوب الذي ارتكبت الجريمة بواسطته فقط، دون أن يحدد مرتكب الجريمة بالذات، الأمر الذي يجعل من الصعوبة نسبة النشاط الجرمي إلى شخص ما، ما لم يتم القيام بالعديد من التحقيقات للتأكد من ذلك.

ففي إحدى القضايا التي عرضت على المحاكم الأمريكية، نازع المدعى عليه في جميع الأدلة التي وجدت على حاسوبه، لأن المحققين لم يستطيعوا إثبات أنه هو الشخص الذي قام بالنشاطات غير الشرعية على الإنترنت[1]، وتجدر الملاحظة في هذا المجال إلى أن المساوئ المشار إليها، والتي تقف في وجه الدليل الرقمي في هذه الأيام قد لا يكون لها أثرا في القريب العاجل، لأن التطور المتسارع للبرمجيات في عصر الثورة الرقمية قادر على إزالة معظم الصعوبات التي تقف حائلا دون نمو هذا الدليل المستحدث.

البند الرابع: مصادر الدليل الإلكتروني وقواعد حفظه

يمكن حصر مصادر الدليل الإلكتروني المتعلق بجرائم التكنولوجيا الحديثة وطرق حفظه فيما يلي:

أولا: مصادر الدليل الإلكتروني، يمكن الوصول إلى الدليل الرقمي أو الإلكتروني عن طريق البحث في المصدرين التاليين:

1-أنظمة الوسائل وملحقاتها: تعد الوسائل الإلكترونية كالحاسب الآلي مصدرا غنيا بالأدلة الرقمية، خاصة تلك الحواسيب الشخصية التي تعد بمثابة أرشيف لسلوكية للأفراد، فهذه الحواسيب تحتوي على الكثير من المعلومات المتعلقة بنشاطات الأفراد ورغباتهم. فالملفات الشخصية أو ملفات النظام وغيرها من أنواع الملفات التي تكون مخزنة عادة في الأقراص الصلبة أو الأقراص الليزرية أو بطاقات الذاكرة كثيرا ما تحتوي على معلومات تتعلق بالجريمة وتفيد في عملية التحقيق[2]، وعملية حجز الجهاز أو ضبطه بقصد فحصه تعد نقطة البداية في الكشف عن خفايا الجريمة المتصلة بالتكنولوجيا الحديثة، لأن الحاسوب أيا كان شكله هو وسيلة النفاذ إلى هذه الشبكة، ويجب أن تشمل عملية الفحص جميع البرمجيات الموجودة أو التي تم إلغاؤها من ذي قبل والمخزنة في المكونات الصلبة أو بطاقات الذاكرة الملحقة بالحاسوب، كما يجب التأكد من أن المكونات الصلبة والبرمجيات تعمل بشكل سليم ومنتظم وأن الحاسوب غير مصاب بفيروس يؤثر على نظامه أو على ملفات التشغيل أو التنفيذ، لأن ذلك يمكن أن ينال من صحة الدليل الرقمي المستخلص عند عرضه على القضاء[3].

2- أنظمة الاتصال بالإنترنت، تشمل عملية فحص أنظمة الاتصال بالإنترنت فحص حركة التنزيل والتحميل ودرجة الاستيعاب، والشبكات المحلية، والنظام الأمني المحاط بالإنترنت...إلخ، فعملية الفحص هذه قد تؤدي إلى الحصول على دليل رقمي يفيد في كشف الحقيقة[4].

---

[1] Eoghan Casey, Op.Cit., pp25-26.

[2] Eoghan Casey, Ibid., p21. Albert Marcella Jr., Robert S. Greenfield, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes Auerbach Publications, CRC Press, 1st Ed., 2002, ISBN: 9780849309557, pp94-95. Robin P. Bryant, Investigating Digital Crime, Wiley, 2008, p50.

[3] عمر محمد أبو بكر ابن يونس، الجرائم الناشئة عن استخدام الإنترنت، أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة، 2004، ص1008 و1009.

[4] عمر محمد أبو بكر ابن يونس، الجرائم الناشئة عن استخدام الإنترنت، المرجع نفسه، ص333.

ولعل أهم المسائل المثارة في صدد فحص أنظمة الاتصال بالإنترنت هي مسألة تحديد مكان الجريمة، أو الجهاز الذي ارتكب بواسطته النشاط الجرمي، حيث يمكن معرفة هذا الأخير عن طريق تتبع الحركة العكسية لمسار الإنترنت[1]، ويستخدم في عملية التتبع هذه نظام فحص إلكتروني يطلق عليه علم البصمات المعاصر، وهو منهج تم استخدامه في العديد من الجرائم، مثل تتبع مبتكر فيروس ميليسا، وكذلك في التوصل إلى الشخص الذي ابتكر موقع خدمات بلو مبرمج لأخبار المال، وهو موقع احتيالي يرفع أسعار الأسهم بطريقة الخداع[2].

ومن الملاحظ أن ما يتم التوصل إليه بفضل تتبع الحركة العكسية لمسار الإنترنت هو عنوان رقمي فقط IP، وهذا الدليل الرقمي لا يكفي لنسبة الجريمة إلى مالك الجهاز، إذ من الممكن ألا يكون هو مرتكب الجريمة، كما لو كان جهازه مسروقا، أو مؤجرا في أحد مقاهي الإنترنت، أو أن يكون عنوانه الرقمي الخاص مسروقا، أو أن يكون هناك من يستخدم حاسوبه احتيالا، أو أن المشتبه به لا يعرف أي شيء عن الإنترنت...إلخ، الأمر الذي يتطلب من جهات التحقيق توفير الدليل المادي كالاعتراف أو الشهادة أو الخبرة...إلخ، إلى جانب الدليل الرقمي حتى يمكن أن تنسب الجريمة إلى مرتكبها[3].

أما خدمات شبكة الإنترنت، فهي تحتوي على الكثير من المعلومات حول أنماط سلوك الأفراد في وقت محدد، فيمكن عن طريق فحص هذه الخدمات معرفة الرسائل الإلكترونية التي قام الجاني أو المجني عليه بإرسالها أو استقبالها، والمواقع الإلكترونية التي سبقت زيارتها، وغرف الدردشة التي تم الدخول إليها، حيث يستطيع المحقق أو الخبير المعلوماتي بعد أن يصل إلى هذه المعلومات أن يتصل بجميع الأفراد الذين كانوا على اتصال مع الجاني أو المجني عليه قبل ارتكاب الجريمة[4]، وعلى المحقق أو الخبير المعلوماتي أن يوثق جميع مراحل عملية البحث، بحيث يشير إلى زمان البحث ومكان المعلومة وكيفية الحصول عليها، وأن يستخدم البرمجيات التي تحافظ على مواقع الوب التي عمل بها؛ لأنه من المعروف أن المعلومات تتغير على الإنترنت من لحظة إلى أخرى[5].

وقد يتخذ الدليل الرقمي شكل المخرجات الورقية التي يتم الحصول عليها عن طريق الطابعات مثلا، كما يمكن أن يتخذ الشكل الإلكتروني كالأشرطة والأقراص الليزرية وغيرها من الأشكال الإلكترونية، إلى جانب عرض المعلومات والبيانات المتعلقة بالدليل الرقمي عن طريق شاشة الحاسوب، ويطلق على جميع هذه الأشكال مصطلح مخرجات الحاسوب[6].

ثانيا: قواعد حفظ الدليل الإلكتروني، يختلف الدليل في جرائم التكنولوجيا الحديثة عن الدليل في الجرائم التقليدية، حيث يتمثل الدليل المادي في الجرائم المستحدثة عامة في ذبذبات أو نبضات إلكترونية مسجلة على وسائط ممغنطة؛ ولذلك يجب أن

---

[1] يقصد بمسار الإنترنت تلك الحركة التراسلية للنشاط الممارس من خلال الإنترنت، فالحاسوب بمجرد أن يتعرف على المسار، يقوم تلقائيا باختيار البروتوكول التراسلي الذي من خلاله يقوم باستدعاء البيانات، وهذه هي الحركة التي أشار إليها علماء الإنترنت بأنها تتشابه مع شبكة العنكبوت من حيث عدم انتظام شكل المسار الاتصالي والتواصلي عبرها. عمر محمد أبو بكر ابن يونس، الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص998.

[2] عمر محمد أبو بكر ابن يونس، الجرائم الناشئة عن استخدام الإنترنت، المرجع نفسه، ص998.

[3] عمر محمد أبو بكر ابن يونس، الجرائم الناشئة عن استخدام الإنترنت، المرجع نفسه، ص999.

[4] Eoghan Casey, Op.Cit., p451.

[5] Eoghan Casey, Ibid., p452.

[6] هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص15 و16.

يكون المحقق الجنائي مؤهلا ومدربا على التعامل مع تلك الأدلة حتى لا يتسبب في إتلاف وإفساد الدليل، لذا يجب مراعاة بعض النقاط عند حفظ الأدلة وتحريرها لتأمينها من التلف وهي كالتالي[1]:

1- ضبط الدعائم الأصلية للبيانات: يشدد الخبراء على بعض الإرشادات الواجب مراعاتها في التحقيق في الجرائم المتصلة بالتكنولوجيا الحديثة، من أهمها أن يكون الضبط للدعائم الأصلية للبيانات مع السماح للجهة التي تحوزها باستخراج نسخ منها لاستخدامها حتى لا يتوقف عملها.

2- مراعاة ظروف الحرارة والرطوبة المناسبة لتخزين الدليل[2]: يجب على المحقق الجنائي مراعاة درجة الحرارة في أماكن حفظ الدليل الرقمي، على أن تتراوح بين (40-90) درجة فهرنهايت (04°-32°)، كما يجب أن تكون نسبة الرطوبة فيها ما بين (20%-80%)، وهذا ما يؤدي إلى إمكانية تخزين هذه الأدلة (الأقراص الممغنطة) لمدة طويلة كما يجوز أيضا حفظ الأدلة الأخرى من بطاقات ورقية مثقبة أو الأوراق المستخدمة في طباعة مخرجات الحاسب الآلي في ظروف الحرارة والرطوبة السابق ذكرها.

3- الالتزام بالقواعد الفنية في نقل الأحراز المعلوماتية وحملها: يراعى عند نقل الأدلة الحفاظ عليها من الصدمات فقد يؤدي بعضها إلى إتلاف كلي أو جزئي لمحتوياتها مهما ضعف مقدار هذه الصدمة، كما يجب عدم المرور بها أو حملها داخل ممرات أو مجالات مغناطيسية أو تخزينها على مقربة من محطة إرسال لاسلكي، كما يجب الحفاظ عليها بعدم تعريضها للغبار والأتربة مما قد يؤدي عدم مراعاة ذلك إلى إتلاف الدليل ومحو ما به من أدلة.

4- تأمين البرامج المضبوطة قبل تشغيلها: يقتضي ذلك مراعاة عدم تشغيل البرامج المضبوطة أو الوسائط قبل تأمينها فنيا وعمل نسخ أخرى سليمة وكاملة.

5- إحكام الحلقات الإجرائية للضبط: ضرورة الاهتمام ببيان التسلسل والترابط وتوضيح الأحكام الإجرائية التي مرت بها المادة المعلوماتية، تأمينا لسلامتها منذ لحظة اكتشافها حتى لحظة عرضها على القضاء، على أن يكون البيان شاملا لكل من كانت له صلة بالدليل في سائر مراحله.

6- تمييز المادة المضبوطة: بوضع علامة مادية خاصة عليى الدليل، مع ختم الأشرطة الممغنطة بعد إتمام التسجيل ووضع الاسم والتوقيع وتدوين البيانات اللازمة.

الفرع الثاني: الاختصاص القضائي في جرائم التكنولوجيا الحديثة

إجراءات التحقيق الابتدائي هي مجموعة من الأعمال التي تباشرها الضبطية القضائية بشأن واقعة جنائية معروضة عليها وذلك بالبحث عن الأدلة المثبتة لها، وهو ما يمهد الطريق أمام القضاء باتخاذ جميع الإجراءات الضرورية للكشف عن الحقيقة وللوصول إلى هذا الهدف يلجأ المحقق إلى مجموعة من الإجراءات بعضها يهدف للحصول على الدليل، وتسمى إجراءات جمع الدليل، وبعضها الآخر يعرف بالإجراءات الاحتياطية ضد المتهم كالقبض والحبس المؤقت.

---

[1] هشام محمد فريد رستم، جرائم الفضاء الافتراضي، المرجع السابق، ص128 وما بعدها.

[2] هشام محمد فريد رستم، جرائم الفضاء الافتراضي، المرجع نفسه، ص131.

فعلى الرغم من وجود تشابه كبير بين التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية وبين التحقيق في الجرائم الأخرى من حيث الإجراءات، إلا أنها تتفرق في عديد النقاط التقنية، وهذا بالطبع يستدعي تطوير أساليب التحقيق الجنائي وإجراءاته بصورة تتلاءم مع هذه الخصوصية وتمكن المحقق من كشف الجريمة والتعرف على مرتكبيها بالسرعة والدقة اللازمين، فالتحقيق في هذا النوع من الجرائم يستدعي إلى جانب السرعة والدقة، الدراية الواسعة وذلك على أساس أن أغلب الإجراءات تتم في بيئة رقمية افتراضية سرعان ما تتغير ويضمحل معها الدليل، مما يمكن الجاني افلات المتابعة القانونية.

وعليه وقبل التفصيل في الاختصاص والإجراءات يجب الحديث عن المهارات الفنية التي ينبغي أن يكتسبها المحقق في الجرائم المتصلة بتكنولوجيا المعلوماتية المتمثلة أساسا في التعرف على المكونات المادية للوسائل الإلكترونية وكيفية التعامل معها، معرفة أساسيات عمل الشبكات وأهم مصطلحاتها، تمييز أنظمة التشغيل المختلفة والتعامل المبدئي معها، التعرف على الصيغ المختلفة للملفات والتطبيقات الرئيسية محل التعامل، إجادة التعامل مع خدمات الإنترنت، معرفة أهم تقنيات الأمن المعلوماتي وأدواتها وطريقة عملها، معرفة جرائم التكنولوجيا الحديثة، خصائصها وكذا الأدوات والأساليب المستخدمة في ارتكابها.

إن الإمام بهذه النقاط هو بمثابة إنطلاقة جيدة لنجاح المحقق والقاضي في مواجهة هذا النوع من الجرائم، وبالتوازي مع هذه المعارف التقنية؛ يجب على رجال الضبطية القضائية وكذا قضاة النيابة والتحقيق أن يكونوا ملمين بالأطر القانونية الإجرائية بهدف كشف الحقيقة دون المساس بالحريات الفردية.

من خلال هذا الفرع سنتطرق إلى الاختصاص القضائي في الجرائم المتصلة بتكنولوجيا الحديثة ثم الوسائل القانونية المتاحة في ظل التشريع الجزائري لمحاربة جرائم التكنولوجيا الحديثة، مع العلم أن الدراسة ستقتصر على جهات النيابة والتحقيق دون جهات الحكم، مفصلين في نقطتين أساسيتين، تتعلق الأولى بقواعدخ، أما الثانية تتناول أهم الإشكالات المتعلقة به.

البند الأول: قواعد الاختصاص في الجريمة المتصلة بالتكنولوجيا الحديثة

يتحدد الاختصاص المحلي للنيابة العامة وفقا للمادة 37 ق.إ.ج بمكان وقوع الجريمة ومحل إقامة أحد الأشخاص المشتبه في مساهمتهم أو بالمكان الذي تم في دائرته القبض، وبالتالي فإن اختصاص وكيل الجمهورية يجب ألا يتعدى ذلك، وبالنسبة إلى قاضي التحقيق وفيما يخص الاختصاص المحلي فقد نظمته المادة 40 ق.إ.ج، والتي أخذت بالمعايير المنصوص عليها في المادة 37 المذكورة آنفا، وطبقا لنص المادة 67 ق.إ.ج، فإنه لا يجوز لقاضي التحقيق أن يجري تحقيقا إلا بموجب طلب من وكيل الجمهورية لإجراء ذلك، وعليه فإن قاض التحقيق وبالتبعية يخضع لأحكام المادة 37 ق.إ.ج.

لكن لما كانت الجريمة المتصلة بالتكنولوجيا الحديثة؛ جريمة قد ترتكب في مكان معين وتكون آثارها في مكان آخر فإن المشرع الجزائري بموجب المادة 2/37 ق.إ.ج أجاز تمديد الاختصاص المحلي لكل من وكيل الجمهورية وكذا قاض التحقيق بالقطب الجزائي المتخصص إلى دائرة اختصاص المحاكم الأخرى المحددة في التنظيم[1]، ويتعين على ضباط الشرطة القضائية طبقا للمادة 40 مكرر1 ق.إ.ج الجزائري أن يقوموا بإخبار وكيل الجمهورية لدى المحكمة الكائن بها الجريمة ويبلغونه بالوثيقة الأصل ونسختين من

[1] مرسوم تنفيذي رقم 06-348 مؤرخ في 12 رمضان 1427ه الموافق لـ 05 أكتوبر 2006م، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج.ر، العدد 63، مؤرخة في 05 أكتوبر 2006.

إجراءات البحث أين يرسل هذا الأخير فورا النسخة الثانية إلى النائب العام لدى المجلس القضائي التابعة له المحكمة المختصة طبقا للمادة 40 مكرر01 ق.إ.ج، إلا أن المواد 40 مكرر وما يليها ق.إ.ج لم ترد بالوضوح الكافي، مما جعل عديد الإشكالات القانونية تطفوا على الساحة القضائية، سواء من حيث علاقة الضبطية القضائية بكل من وكيل الجمهورية صاحب الاختصاص وكذا النائب العام لدى القطب الجزائي المتخصص، وكذا علاقة كل من وكيل الجمهورية بالنائب العام، وعلاقة هاذين الآخيرين بالنائب العام لدى القطب الجزائي المتخصص، وذلك أنه طبقا للمادة 40 مكرر2 يمكن للنائب العام بالجهة القضائية المتخصصة أن يطالب من قانون الإجراءات الجزائية بالإجراءات فورا إذا رأى أن الجريمة تدخل ضمن اختصاص المحكمة المذكورة في المادة 40 مكرر من هذا القانون مبديا بذلك تمسكه بالاختصاص ومنهيا لحالة الاختصاص المشترك.

وتنص المادة 15 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها: "زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبي وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني"، وهو خروج على المبادئ العامة للاختصاص المحلي المقرر في قانون الإجراءات الجزائية، بعدما كان الأصل أن المحاكم الجزائرية لها إقليم يشمل إقليم الدولة فقط، وهنا تطرح عديد الإشكالات نتطرق لها لاحقا.

كما تنص المادة 04 من ذات القانون والمتضمنة الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية، يختص النائب العام لدى مجلس قضاء الجزائر العاصمة بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13، إذنا لمدة 06 أشهر قابلا للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعلمة والأغراض الموجهة لها.

أما بالنسبة لضباط الشرطة القضائية المنصوص عليهم في المادة 15 ق.إ.ج فإنه يتحدد اختصاصهم طبقا للمادة 16 من ذات القانون، ونميز ثلاثة حالات:

- في الجرائم العادية، يحدد اختصاصهم المحلي بالحدود التي يباشرون فيها وظائفهم المعتادة.
- في حالة الاستعجال، يحدد اختصاصهم المحلي بالاختصاص المحلي للمجلس القضائي الذي يزاولون فيه نشاطهم كما يجوز لهم مباشرة مهمتهم في كافة الإقليم الوطني.
- في الجرائم الخاصة، يمتد الاختصاص المحلي إلى كافة الإقليم الوطني.

فيما يخص ضباط الشرطة التابعين لمصالح الأمن العسكري فلهم اختصاص شامل، يختص النائب العام لدى مجلس قضاء الجزائر العاصمة بمنحهم الإذن للقيام بوضع ترتيبات تقنية مراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية وذلك في إطار الإجراءات الوقائية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، إلا أن القانون رقم 09-04 لم يحدد الاختصاص الإقليمي لهذه الفئة من ضباط الشرطة القضائية والأرجح أنه اختصاص شامل لكافة التراب الوطني.

يخضع ضباط الشرطة القضائية التابعين للهيئة خارج حالة الإجراءات الوقائية من الأفعال الموصوفة بالإرهابية للقواعد العامة المقررة في قانون الإجراءات الجزائية، فالأصل أن يخضع ضباط الشرطة القضائية أثناء قيامهم بمهام الضبط القضائي لإدارة وكيل

الجمهورية المباشر في دائرة كل محكمة، ولإشراف النائب العام في دائرة المجلس القضائي، ورقابة غرفة الاتهام لذات المجلس طبقا لأحكام المادة 12 ق.إ.ج دون الإخلال بأحكام المادة 208 المتعلقة بضباط الشرطة القضائية العسكريين، وتنص المادة 18 مكرر من ذات القانون على أن يمسك النائب العام ملفا فرديا لكل ضابط شرطة قضائية يمارس سلطات الضبط القضائي في دائرة اختصاص المجلس القضائي في حين يتولى وكيل الجمهورية تحت سلطة النائب العام تنقيط ضباط الشرطة القضائية العاملين بدائرة اختصاص المحكمة، وهو ما يطرح التساؤل حول آليات تطبيق الرقابة المنصوص عليها في مواد قانون الإجراءات الجزائية المبينة أعلاه وكذا المتعلقة بها، خصوصا في حال ارتكاب خطأ مرتبط بصفة الضبطية القضائية لاسيما أنه يغلب على عمل ضباط الشرطة التابعين للهيئة طابع العمل القضائي من تحري وتفتيش وغيره.

البند الثاني: إشكالات الاختصاص في الجريمة المتصلة بتكنولوجيا المعلوماتية

إن أهم الإشكاليات المطروحة والمتعلقة بالاختصاص القضائي في الجرائم المتصلة بتكنولوجيا المعلومات الحديثة، تتمثل في إشكالية الاختصاص المحلي في الجرائم الواقعة خارج الإقليم الوطني وكذا إشكالية الإجراءات أمام الأقطاب القضائية المتخصصة.

أولا: إشكالية الاختصاص المحلي في الجرائم الواقعة خارج الإقليم الوطني، تخضع قواعد القانون الجنائي بشقيه الموضوعي والإجرائي في تطبيقها من حيث المكان لمبدأ مستقر ومعروف، ألا وهو مبدأ الإقليمية، والأصل أن عناصر الركن المادي للجريمة تكتمل في مكان واحد، وعلى ضوء ذلك يتحدد القانون الواجب التطبيق، وبالتبعية المحكمة المختصة بنظر الدعوى، بيد أن جرائم التكنولوجيا الحديثة يتجاوز مداها أحيانا حدود الدولة، فيمكن وقوع السلوك في مكان أو عدة أمكنة متباعدة، في حين تتحقق النتيجة الإجرامية الضارة في نطاق إقليم دولة أخرى، وهذا يقودنا إلى التساؤل عن مكان وقوع الجريمة في هذه الحالة.

انقسمت الآراء الفقهية إلى ثلاثة اتجاهات، فذهب الاتجاه الأول إلى أن العبرة في تحديد مكان وقوع الجريمة بالمكان الذي وقع فيه السلوك بغض النظر عن المكان الذي تحققت فيه النتيجة، وفي المقابل، ذهب اتجاه آخر إلى أن مكان وقوع الجريمة يتحدد بالمكان الذي تحققت فيه النتيجة أو كان من المفترض تحققها فيه، وبين هذا وذاك اتجه رأي ثالث إلى أن العبرة في ذلك تكون بمكان حصول أي منهما (السلوك أو النتيجة)، أي أن الفعل يتنازعه ثلاثة قوانين، قانون دولة الإقليم على أساس مبدأ الإقليمية، وفي الوقت ذاته قد يخضع لقانون دولة الجاني عملا بمبدأ الشخصية الإيجابية وقانون دولة ثالثة متى كانت الجريمة ماسة بمصالحها الحيوية وفقا لمبدأ العينية.

اكتفى المشرع الجزائري في هذا الشأن بما جاء في الفقرة الثانية من نص المادة 15 من القانون رقم 09-04 والتي تنص على أنه: "تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبي وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني"، ما علينا قوله هو أن هذه المبادرة تحسب للمشرع الجزائري، إلا أنها لا ترقى إلى المستوى المطلوب لمواجهة جرائم التكنولوجيا الحديثة.

ثانيا: إشكالية الإجراءات أمام الأقطاب القضائية المتخصصة، بالرجوع إلى المادة 40 مكرر 1 ق.إ.ج نجد أنها أبقت على العلاقة التقليدية المنظمة للعلاقة التدرجية بين وكيل الجمهورية المختص إقليميا والضبطية القضائية في مجال التحري في الجرائم المنصوص عليها في المادة 37 من نفس القانون من خلال الإخبار الفوري لوكيل الجمهورية المختص إقليميا من قبل ضابط الشرطة

القضائية، إرسال ملف الإجراءات الخاص بالتحقيق المنجز إلى نفس القاضي وتحويل النسخة الثانية من ملف التحقيق الابتدائي إلى النائب العام لدى الجهة المتخصصة يتم عن طريق وكيل الجمهورية.

وهنا تتبادر إلى أذهاننا عديد التساؤلات تتعلق أساسا ببقاء النائب العام لدى الجهة القضائية المتخصصة بعيدا عن مجال التحقيق الابتدائي وبالتالي حرمانه من الإخبار المبكر بتحريك الدعوى العمومية وكذا إبعاده عن تطورات التحقيق الابتدائي وهو ما يؤدي إلى التقليل من فعالية حقه في المطالبة بالملف في الوقت المناسب، وعليه يكون من الأنجع أن يفيد وكيل الجمهورية الذي وقع الجرم بدائرة اختصاصه النائب العام بنسخة ثانية من التقرير الإخباري الأولي فور تلقيه من عناصر الضبطية القضائية كلما تعلق الأمر بإحدى الجرائم المنصوص عليها في المادة 37 ق.إ.ج.

تجدر الإشارة إلى أن التدابير الجديدة لم تغير من طبيعة العلاقة الموجودة بين نيابة الجمهورية والنيابة العامة، بل يجب احترام مبدأ التدرج بالنسبة للتنازع بين النائب العام ووكيل الجمهورية، في هذه الحالات يمكن تصور فرضيتين:

- إذا كان كل من وكيل الجمهورية المختص إقليميا والنائب العام لدى الجهة القضائية ذات الاختصاص الموسع ينتميان إلى مجلس قضائي واحد وهنا لا يثار أي إشكال.
- إذا كان النائب العام لدى الجهة القضائية المتخصصة ووكيل الجمهورية المختص إقليميا ينتميان إلى مجلسين مختلفين، هنا تثار إشكالية بين النائبين العامين مما يستلزم ضرورة تدخل وزارة العدل.

ولتفادي الوقوع في مثل هذه الحالات نرى وجوب الاخبار المبكر والمستمر للمصالح المركزية للوزارة بتطور الإجراءات والتحقيق للتدخل في الوقت المناسب، أما فيما يخص النزاع بين النائب العام وقاض التحقيق، فتجدر الإشارة إلى أن القانون لم يحدد الآلية الإجرائية لكيفية إخطار النائب العام بتطور الإجراءات على مستوى التحقيق، فتتم المطالبة بالملف بموجب التباسات يقدمها وكيل الجمهورية المختص إقليميا إلى قاضي التحقيق، ويفصل قاضي التحقيق في هذه الالتماسات بموجب أمر وهنا نكون أمام فرضيتان كذلك:

– الأولى؛ في حالة ما إذا كان قاضي التحقيق لا يعارض التماسات وكيل الجمهورية ولا يصدر أمرا بالتخلي لصالح زميله بالجهة القضائية ذات الاختصاص المحلي الموسع، هنا لا نجد أي إشكال بالنسبة لقاض التحقيق المتخلي، لكن تقوم إشكالات لدى قاض التحقيق بالجهات القضائية ذات الاختصاص الموسع منها:

- طريقة الإخطار، أي مدى ضرورة طلب افتتاحي جديد.
- من يمضي هذا الطلب وماذا يكون محتوى الطلب لاسيما في حال تقدم قاضي التحقيق الأول في الإجراءات.
- هل من الضروري إجراء السماع لدى الحضور الأول من جديد.
- ما هي القيمة القانونية للإجراءات السابقة.
- هل قاضي التحقيق لدى القطب الجزائي المتخصص ملزم بالتحقيق، أو بعبارة أخرى هل بإمكانه رفض التحقيق أو التصريح بعدم الاختصاص.

– أما الفرضية الثانية؛ قد يكون لقاضي التحقيق رأي مخالف ويرى أن الوقائع موضوع التحقيق لا تدخل ضمن مجال الاختصاص النوعي للجهة القضائية ذات الاختصاص المحلي الموسع أو أن الطلب جاء سابقا لأوانه بسبب عدم اتضاح معالم الجريمة.

ثالثا: سبل اتصال الضبطية القضائية بجرائم التكنولوجيا الحديثة، تختلف سبل اتصال الضبطية القضائية بالجريمة حسب طبيعة الجريمة بحد ذاتها، وبما أننا بصدد دارسة الجرائم المتصلة بتكنولوجيا المعلومات الحديثة فسنسعى إلى التركيز على ما يتناسب وخصوصية هذا الصنف في الجرائم، وكذا ما يمكن تطبيقه في هذا المجال.

1- التبليغ: وهو إجراء يتم بواسطة شخص لم يتضرر من الجريمة بالإبلاغ عنها لدى الجهات المختصة، وقد يكون التبليغ رسميا إذا كان صادرا من قبل جهات رسمية، كما قد يكون عاديا إذا صدر من قبل الأشخاص العاديين وقد يكون في شكل مكتوب أو في شكل تصريحات.

ونتيجة للتطور التكنولوجي ظهرت صور جديدة للتبليغ مثل التبليغ عن طريق البريد الإلكتروني والتبليغ من خلال مواقع مخصصة لذلك...إلخ، وتلقي البلاغات في الجزائر من اختصاص ضباط الشرطة القضائية طبقا للمادة 17 ق.إ.ج، وبالتالي نرى أن هناك تأخر بخصوص تطوير وسائل تلقي البلاغات لاسيما فيما يتعلق بالجرائم المتصلة بتكنولوجيا المعلوماتية.

ونشير إلى أن المادة 17 ق.إ.ج، تجيز للضبطية القضائية مطالبة أي عنوان أو لسان أو سند إعلامي بنشر إشعارات أو أوصاف أو صور لأشخاص مبحوث عنهم وذلك بعد الحصول على إذن من النائب العام، وبالتالي يمكن تخصيص موقع أو إضافة صفحة على المواقع الرسمية للضبطية القضائية تختص بتلقي البلاغات والشكاوى المتعلقة بالجرائم المتصلة بالتكنولوجيا الحديثة وكذا نشر كل ما من شأنه المساعدة في البحث عن المجرمين.

2- الشكوى: وهو إجراء يقوم به المجني عليه أو ذوي الحقوق يهدف من خلاله إلى إبلاغ نبأ وقوع الجريمة عليه إلى السلطات المختصة، وتكون الشكوى أمام ضباط الشرطة القضائية طبقا للمادة 17 ق.إ.ج، كما قد تكون أمام قضاة النيابة طبقا لنص المادة 36 من ذات القانون، كما قد تكون في شكل شكوى مصحوبة بادعاء مدني أمام قضاة التحقيق طبقا لنص المادة 72 من نفس القانون.

المطلب الثاني: الإجراءات التقليدية لجمع الدليل الإلكتروني

أدى التقدم العلمي الكبير إلى ظهور علامات بارزة في معالم نظام الإثبات الجنائي، تتمثل في استحداث وسائل علمية جديدة تستطيع التغلب على كل محاولات المتهم لتضليل العدالة وكشف ما قد يطمسه من آثار في سعيه نحو إثبات براءته بشتى الطرق، وإذا كانت الجريمة المعاصرة قد تغيرت أبعادها وتميزت بسمات خاصة وأنماط جديدة، فإنه يصبح من الضروري أن يتغير تبعا لذلك أسلوب كشفها وطريقة إثباتها.

وعليه يصبح للدليل المادي لارتباطه بالتطور العلمي دورا رئيسيا في كشف الجريمة المعاصرة وتقديم أدلة الإدانة فيها[1]، فغالبا ما يترك الجاني عند ارتكاب جريمته آثارا مادية مكان الجريمة، لأنه مهما احتاط وحرص ومحا كل الآثار الناجمة عن الجريمة إلا أنه وفي

[1] أحمد أبو القاسم، الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص، أطروحة دكتوراه، المركز العربي للدراسات الأمنية والتدريب، الرياض 1414هـ، ص138.

النهاية لابد وأن يترك أي أثر، والسبب في ذلك في رأي العلماء الحالة النفسية والانفعالات التي تصاحب الجاني والقلق الذي يسيطر عليه سواء أثناء التنفيذ أو بعده[1].

الفرع الأول: التفتيش

التفتيش هو إجراء من إجراءات التحقيق يتم عقب وقوع الجريمة وليس إجراء لمنع وقوع الجرائم[2] يقوم به موظف مختص طبقا للإجراءات المقررة قانونا في محل يتمتع بالحرمة بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها لإثبات ارتكابها أو نسبها إلى المتهم[3]، والتفتيش بطبيعة الحال هو إجراء يمس حق المتهم في سرية حياته الخاصة، كما أنه لا يجوز أن يترتب على حق الدولة في ممارسة سلطتها في العقاب تجاوزا في حق الأشخاص في الحفاظ على سرية حياتهم الخاصة؛ فالحياة الخاصة بما فيها مكان العمل والأقارب تتمتع بحرية وخصوصية لا يجوز اقتحامها إلا وفقا لإجراءات قانونية خاصة وفي أضيق الحدود[4].

البند الأول: الشروط الشكلية والموضوعية للإذن بالتفتيش

كرس التشريع الجزائري كسائر التشريعات العالمية مبدأ الحرية الفردية وحرمة المساكن والأشخاص وضمان الحريات الأساسية الفردية، وعليه خصص في دستوره مبادئ خاصة بحرمة وحياة المواطن وحرمة مسكنه، حسب المواد 46 و47 منه، كما خصص بعض المواد في قانون الإجراءات الجزائية متعلقة أساسا بإجراء التفتيش في القسم المتعلق بالجرائم المتلبس بها، في القسم المتعلق بالتحقيق الابتدائي، وكذا القسم المتعلق بسلطات التحقيق.

الأصل أنه لا يجوز إجراء أي تفتيش إلا بإذن مكتوب من وكيل الجمهورية أو قاضي التحقيق ويمكن أن يتم التفتيش برضا صريح من المعني طبقا للمادة 64 ق.إ.ج، ويجب على ضابط الشرطة القضائية أن يستظهر بالإذن قبل الدخول أو الشروع في التفتيش طبقا لنص المادة 44 ق.إ.ج، كما يجب أن يتضمن الإذن وصف الجرم محل التحري وعنوان الأماكن التي سيتم تفتيشها.

يتم التفتيش في المسكن بحضور المشتبه فيه، فإن تعذر عليه ذلك يكلفه ضابط الشرطة القضائية بتعيين ممثل له، أما إذا امتنع عن الحضور أو كان في حالة فرار، يعين ضابط الشرطة القضائية المكلف بالتفتيش شاهدين من غير موظفيه طبقا لأحكام المادة 1/45 ق.إ.ج في حالة ما ذا كان المشتبه فيه موقوف وكان نقله يشكل خطورة على النظام العام، فله الحق في أن يختار وكيلا عنه أو يكتفي بحضور شاهدين بعلم وموافقة وكيل الجمهورية، كما يجب اتخاذ كل التدابير اللازمة لضمان احترام السر في الأماكن التي تم تفتيشها والتي تحاط بواجب السر المهني.

---

[1] إبراهيم صادق الجندي، حسين حسن الحصيني، تطبيقات البصمة الوراثية D.N.A في التحقيق والطب الشرعي، جامعة نايف العربية للعلوم الأمنية الرياض، 2002، ص9.

[2] أحمد فتحي سرور، المرجع السابق، ص450.

[3] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، المرجع السابق ص192.

[4] Jean Larguier, Anne-Marie Larguier, La protection des droits de l'homme dans le procès pénal RIDP (Revue internationale de droit pénal) Vol. 37, n°01, 1966, p95.

لا يجوز بدء التفتيش قبل الخامسة صباحا ولا بعد الثامنة مساء إلا بطلب من صاحب المسكن أو نداءات موجهة من الداخل أو في الحالات الاستثنائية التي حددها القانون طبقا لنص المادة 47 ق.إ.ج، والمتمثلة في الجرائم المعاقب عليها في المواد من 342 إلى 348 ق.ع، إذ يمكن إجراء التفتيش دون التقييد بالحدود الوقتية المذكورة بالأماكن المحددة بالمادة 2/47 ق.إ.ج إضافة إلى الجرائم المحددة بالمادة 3/47 ق.إ.ج، والتي تعطي لضابط الشرطة القضائية الصلاحيات للتفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في أي ساعة من الليل أو النهار بإذن مسبق من وكيل الجمهورية، وهاته الجرائم هي: جرائم المخدرات الجريمة المنظمة العابرة للحدود الوطنية، الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات، تبييض الأموال، جرائم الإرهاب، جرائم الصرف وحركة رؤوس الأموال.

والشرط الموضوعي الأساسي لإجراء التفتيش هو سبب التفتيش، والسبب القانوني الأصيل يكون الحصول على دليل في جريمة ما، أي وجود احتمال قوي على توفر دليل أو قرائن في مسكن شخص معين تدل على ارتكابه الجريمة، وهو ما يدفع السلطة المختصة إلى إصدار قرارها بالتفتيش، وقد نوه المشرع الجزائري إلى سلطات إصدار الأمر بالتفتيش في المادة 44 ق.إ.ج، كما أشارت نفس المادة على أن الإذن بالتفتيش تفويض تصدره سلطة قضائية –قاضي التحقيق أو وكيل الجمهورية– إلى أحد مأموري الضبط القضائي مخولا له إجراء التفتيش الذي تختص به تلك السلطة، وبعبارة أخرى هي ندب أحد ضباط الشرطة القضائية للقيام بالتفتيش،ولقد جاء في المواد 44 إلى 47 ق.إ.ج الشروط الواجب توفرها لصحة الإذن بالتفتيش تحت طائلة البطلان، وهذه الشروط منها ما يتعلق بمصدر الإذن ومنها ما يتعلق بمن يصدر له الإذن، ومنا ما يتعلق بالإذن نفسه وهذا ما يستشف من نص المادة 44 ق.إ.ج.

بالإضافة إلى مجموعة من الشروط الشكلية التي يجب توافرها لصحة الاذن بالتفتيش إلا أنه وعند الحديث عن التفتيش في الجرائم المتصلة بالتكنولوجيا الحديثة، لاسيما التفتيش في البيئة الرقمية نجد أن الأمر يختلف وتطرح إشكالات عديدة منها مدى قابلية المكونات الرقمية أو المنطقية للوسائل الإلكترونية لعملية التفتيش، وهو محل جدل فقهي، فهناك من يرى بجواز ضبط البيانات الإلكترونية بمختلف أشكالها، استنادا في ذلك إلى أن القوانين الإجرائية عندما تنص على إصدار الإذن بضبط أي شيء، فإن ذلك يجب تفسيره بحيث يشمل البيانات المحسوسة وغير المحسوسة، بينما ذهب رأي آخر إلى عدم انطباق المفهوم المادي على هذه البيانات غير المرئية أو غير الملموسة، فذهب إلى أنه يجب أن يقع الضبط عليها إذا اتخذت شكلا ماديا، وهنا يجب إيجاد نص صريح يخص المكونات المنطقية للوسائل الإلكترونية.

ويثور الخلاف أيضا حول موضوع الشبكات ومدى خضوعها للتفتيش عن بعد، فالبيانات التي تحتوي على أدلة قد تتوزع عبر شبكة حاسوبية في أماكن مجهولة بعيدة تماما عن الموقع المادي للتفتيش، وإن ظل من الممكن الوصول إليها من خلال حواسيب تقع في الأبنية الجاري تفتيشها، وقد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي آخر أو حتى في بلد آخر، ففي الاحتمال الأول وهو اتصال حاسب المتهم بحاسب آخر مثلا، أو نهاية طرفية موجودة في مكان آخر داخل الدولة، يثار التساؤل حول مدى إمكانية امتداد الحق في التفتيش إذا تبين أن الحاسب أو النهاية الطرفية في منزل المتهم متصلة بجهاز أو نهاية طرفية في مكان آخر مملوك لشخص غير المتهم.

بالرجوع إلى التشريع الداخلي نجد أن المشرع الجزائري قد تعرض لعملية تفتيش المنظومة المعلوماتية من خلال الفصل الثالث من القانون رقم 09-04 المعنون بالقواعد الإجرائية، تفتيش المنظومة المعلوماتية، ضمن المادة 05 منه التي تنص على أنه: "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 أعلاه، الدخول، بغرض التفتيش، ولو عن بعد، إلى:

أ- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب-منظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة أ من هذه المادة، إذا كانت هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها إنطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها إنطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة، ووفقا لمبدأ المعاملة بالمثل.

يمكن للسلطة المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها."

بناء على ما سبق نجد أن المشرع الجزائري ومن خلال هذه المادة قد فصل في عديد الإشكاليات الإجرائية، فزيادة على ما هو منصوص عليه في قانون الإجراءات الجزائية -السابق عرضه- فقد أضاف المشرع محلين للتفتيش وهما المنظومة المعلوماتية أو جزء منها والمعطيات المعلوماتية المخزنة فيها، وكذا منظومة تخزين معلوماتية، وبالتالي وضع نهاية لجدال فقهي لا تزال عديد الدول تتخبط فيه، كما نص صراحة على إمكانية التفتيش عن بعد، إلا أن حصر إمكانية تمديد التفتيش في الشبكة على الحالة أ من المادة 04 -للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة- يتنافى وطبيعة الجرائم المتصلة بالتكنولوجيا الحديثة فالأحرى أن تكون إمكانية تمديد التفتيش في الشبكة في حال ما إذا كانت هناك أسبابا تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها إنطلاقا من المنظومة الأولى متاحة لجميع الجهات القضائية لاسيما وأن عملية التمديد مقترنة بإخطار الجهات القضائية المختصة.

إضافة إلى ما سبق فإننا نرى أن المشرع الجزائري بالغ في احترام سيادة الدول الأخرى من خلال منع التفتيش في الأنظمة المعلوماتية التابعة لإقليمها[1]، إذ نص في المادة 05 على أنه إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها إنطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل، في حين كان من الواجب التفصيل في طبيعة

[1] خلاف لنص المادة 32 من الاتفاقية الأوربية بشأن الجرائم المعلوماتية، والتي تنص على إمكانية الدخول بغرض التفتيش والضبط في أجهزة أو شبكات تابعة لدولة أخري بدون إذنها في حالتين: الأولى إذا تعلق التفتيش بمعلومات أو بيانات مباحة للجمهور، والثانية إذا رضي صاحب أو حائز هذه البيانات بهذا التفتيش.

المعطيات المبحوث عنها والواقعة خارج التراب الوطني، فإن كانت متاحة للجمهور جاز الحصول عليها دون إذن مسبق أو في إطار التعاون الدولي.

البند الثاني: تنفيذ التفتيش

تتم عملية التفتيش تحت إشراف ضابط شرطة قضائية مؤهل، والذي بدوره يجب أن يكون ملما بأبجديات التحقيق الرقمي والتي نوجزها في نقطتين أساسيتين، الأولى تتعلق بالإرشادات التقنية الأولية لعملية التفتيش، أما الثانية فتتعلق بالإطار العلمي لاستخلاص الدليل الرقمي وجمعه من مسرح الجريمة.

أولا: الإرشادات التقنية الأولية لعملية التفتيش، يمكن تقسيمها إلى ثلاثة نقاط أساسية:

1- القواعد الأساسية للتفتيش: هذه القواعد مفيدة وضرورية لتتبع الأدلة وإدارتها، كما أنها تشكل حماية ضد أي طعن بهذه الأدلة بسبب احتمال سوء التعامل معها[1]، وهذه القواعد هي:

- تخزين الدليل الأصلي وعدم التغيير فيه.
- عدم السماح للمشتبه به بالتعامل مع أجهزة مسرح الجريمة.
- حضر تنفيذ البرامج على أجهزة مسرح الجريمة.
- توثيق جميع نشاطات التحقيق.
- إعداد نسخة احتياطية عن وسائط تخزين المعلومات الموجودة في مسرح الجريمة.
- العرض المناسب للدليل أمام القضاء.

2- التخطيط: قبل وصول المحققين إلى مسرح الجريمة يجب إعداد خطة عمل بشكل شامل ويقترح قسم جرائم التكنولوجيا الحديثة في مكتب التحقيقات الفيدرالية الأمريكي FBI إتباع الخطوات التالية:

- إعداد الشكل المبدئي للأوراق المطلوبة لتوثيق التفتيش.
- إعداد المواد والمغلفات الضرورية لمثل هذا التفتيش.
- التأكد من إدراك المختصين بأشكال الأدلة بالإضافة إلى التعامل المناسب معها.
- مناقشة التفتيش مع المشتركين فيه قبل الوصول إلى مسرح الجريمة إذا أمكن.
- تعيين شخص مسؤول قبل الوصول إلى مسرح الجريمة.
- إعداد مهام الطاقم الأساسية قبل الوصول.
- تقييم مهام الطاقم المطلوبة لمعالجة مسرح الجريمة بشكل ناجح.
- تقييم النتائج القانونية لتفتيش مسرح جريمة الحاسوب.
- الأخذ بعين الاعتبار أمن وراحة طاقم التفتيش عند مواجهة مسرح جريمة خطير.

[1] http://online.securityfocus.com/infocus/1246

3- عملية التفتيش: بعد التفتيش المبدئي لمسرح الجريمة يتم توثيق الوسائل والوسائط الإلكترونية وإعدادها للنقل إلى مختبر الأدلة وتتألف هذه العملية من مجموعة من المراحل أهمها:

أ- تسجيل أدلة التفتيش والمحجوزات: يجب أخذ صور للجهاز وللكوابل وللطرفيات المرتبطة به بالنسبة للوسائل الإلكترونية، وأخد ملاحظة فيما إذا كان الحاسوب مشغلا، ومرتبطا مع شبكة، ذلك لاحتمال فقد المعلومات بسبب التهديدات الخارجية مثل الطقس والكهرباء والمجال المغناطيسي، أما الأدوات والوسائط فيجب أخذ صور لواجهة وخلفية وجوانب الأداة وللكوابل المرتبطة مع الأداة وتسجيل فيما إذا كانت الأداة تعمل أم مطفأة وماذا كانت تعمل.

ب- إغلاق أجهزة الحاسوب العاملة وتعليم الأجهزة والكوابل والوسائط: في حالة ما إذا أغلق الجهاز فيجب على المحقق أن يدرك بأن هناك معلومات قد تكون مخزنة على RAM وفي هذه الحالة يجب اتخاذ الخطوات الكفيلة بعمل backup ويجب أخذ ملاحظات لذلك التقييم.

ج- تجهيز الحاسوب والوسائط والأدوات للنقل: تغليف كوابل وأجهزة الحاسوب في صناديق كرتونية وتعليمها بملصق تعبر عن محتوياته[1]، وفق لما هو منصوص عليه في قانون الإجراءات الجزائية.

ثانيا: الإطار العلمي لاستخلاص الدليل الرقمي وجمعه، من شأن علوم الأدلة الجنائية تقديم منظور علمي لتحليل أي شكل من أشكال الأدلة الرقمية، وتساهم علوم التحليل السلوكي للأدلة الرقمية في الربط المحدد بين المعارف التكنولوجية وبين الطرق العلمية والقانونية لاستخلاص الدليل الرقمي، وعلى ذلك فإن هذه العلوم مجتمعة تساهم فيما يلي الكشف عن الدليل الرقمي وتحديد خصائصه الفريدة، إجراء الاختبارات التكنولوجية والعلمية على الدليل الرقمي لاختباره والتحقق من أصالته ومصدره كدليل يمكن تقديمه لجهات الحكم، إصلاح الدليل وإعادة تجميعه من المكونات المادية للأجهزة الإلكترونية وعمل نسخة أصلية للتأكد من عدم وجود معلومات مفقودة أثناء عملية استخلاص الدليل، جمع الآثار المعلوماتية الرقمية التي قد تكون تبدلت خلال الشبكة المعلوماتية، استخدام الخوارزميات للتأكد من أن الدليل لم يتم العبث به أو تعديله، بالإضافة إلى حفظ الدليل الرقمي لإثبات أنه أصيل وموثوق به ويقع ضمن سلسلة الأدلة المقدمة في الدعوى.

تجدر الإشارة هنا إلى أنه غالبا ما توجد الأدلة الرقمية في مخرجات الطابعة والتقارير والرسوم وفي أجهزة الكمبيوتر وملحقاتها وفي الأقراص المرنة والصلبة وأشرطة تخزين المعلومات وفي أجهزة المودم والبرامج وأجهزة التصوير ومواقع الوب والبريد الإلكتروني ولذلك تستخدم عدة طرق وأدوات تساهم في جمع الأدلة الرقمية منها:

- برنامج إذن التفتيش، وهو برنامج قاعدة بيانات يسمح بإدخال كل المعلومات الهامة المطلوبة لترقيم الأدلة وتسجيل البيانات منها، ويمكن لهذا البرنامج أن يصدر إيصالات باستلام الأدلة والبحث في قوائم الأدلة المضبوطة لتحديد مكان دليل معين أو تحديد ظروف ضبط هذا الدليل.

- قرص بدء تشغيل الكمبيوتر، يمكن المحقق من تشغيل الكمبيوتر إذا كان نظام التشغيل فيه محميا بكلمة مرور، ويجب أن يكون القرص مزودا ببرنامج مضاعفة المساحة، فربما كان المتهم قد استخدم هذا البرنامج لمضاعفة مساحة القرص الصلب.

---

[1] Eoghan Casey, Op.Cit., p15.

– **برنامج معالجة الملفات**، هو برنامج يمكن المحقق من العثور على الملفات في أي مكان على الشبكة أو على القرص الصلب، ويستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم أو الأقراص المرنة المضبوطة أو يستخدم لقراءة البرامج في صورتها الأصلية، كما يمكن من البحث عن كلمات معينة أو عن أسماء ملفات أو غيرها.

– **برنامج النسخ**، هو برنامج يمكن تشغيله من قرص مرن ويسمح بنسخ البيانات من الكمبيوتر الخاص بالمتهم ونقلها إلى قرص آخر سواء على التوازي أو على التوالي وهو برنامج مفيد للحصول على نسخة من المعلومات قبل أي محاولة لتدميرها.

– **برامج كشف الأقراص**، ويمكن من خلال هذه البرامج الحصول على محتويات القرص المرن مهما كانت أساليب تهيئته ومثل هذه البرامج غالبا ما تتوافر في نسخة عادية خاصة بالأفراد وأخرى احترافية خاصة بأجهزة الأمن.

الفرع الثاني: المعاينة

تعد المعاينة من المراحل الأولى للإستدلال ومن أهم المراحل على الإطلاق، نظرا لما يمكن أن توفره من أدلة إثبات الجريمة[1] وتزداد أهميتها في الجرائم المتصلة بالتكنولوجيا الحديثة، وذلك راجع إلى الطبيعة الخاصة للسلوك الإجرامي فيها بالإضافة إلى اعتبارها من الجرائم المستحدثة، مما استوجب ابتكار إجراءات خاصة بالمعاينة في هذا المجال.

أولا: تعريف المعاينة، تعني المعاينة رؤية أماكن ارتكاب الوقائع الجنائية، كما تنصرف إلى فحص جسم المجني عليه والمتهم واثبات ما يوجد بها من آثار، وقيل في المعاينة بأنها: "إجراء يتطلب إثبات حالة الأمكنة والأشياء والأشخاص ووجود الجريمة، وهي إجراء لا يتضمن إكراه أو اعتداء على حرمة الأشياء والأشخاص"[2]، وجاء تعريفها أيضا على أنها دليل مباشر أو عام باعتبار أن المحقق يلمس بنفسه العناصر المادية التي تفيد في كشف الحقيقة[3].

ويقصد بالمعاينة في القانون الجنائي بأنها إثبات مباشر ومادي لحالة الشيء أو شخص معين ويكون ذلك من خلال الرؤية أو الفحص المباشر للشيء أو للشخص[4]، وتعد المعاينة الإجراء الذي يتضمن وصف مكان الحادث بما فيه من أشياء وأشخاص والفحص الدقيق لكافة المحتويات بهدف كشف آثار الجاني بالمكان، والتي تشير إلى شخصيته أو شركائه إضافة إلى كل ما يفيد في إثبات ارتكاب الجريمة، وتوضح قدرا من الاستنتاجات المنطقية التي تشكل في حد ذاتها الأساس الذي يقوم عليه التحقيق والبحث[5].

نلاحظ من خلال المفاهيم والدلالات السابقة أن جوهر المعاينة هو ملاحظة وفحص حسي مباشرة لمكان أو شخص أو شيء له علاقة بالجريمة ولإثبات حالته والكشف والتحفظ على كل ما يفيد من الأشياء في كشف الحقيقة، والمعاينة تختلف عن

---

[1] يرى البعض أن أهمية المعاينة تتضاءل في جرائم التكنولوجيا الحديثة وذلك لندرة تخلف آثار مادية عند ارتكاب الجريمة، أما عن طول الفترة بين وقوع الجريمة أو ارتكابها وبين اكتشافها يكون له التأثير السلبي على الآثار الناجمة عنها بسبب العبث أو المحو أو التلف لتلك الآثار. هشام محمد فريد رستم الجرائم المعلوماتية، أصول التحقيق الجنائي الفني وآليات التدريب التخصصي للمحققين، المؤتمر الدولي تحت عنوان الكمبيوتر والإنترنت بين الشريعة والقانون، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، الإمارات العربية المتحدة، 2000.

[2] سامي حسني الحسيني، النظرية العامة للتفتيش في القانون المصري والمقارن، أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة، 1972، ص50.

[3] مأمون محمد سلامة، الإجراءات الجنائية في التشريع المصري، ج01، دار النهضة العربية، القاهرة، 2008، ص347.

[4] أحمد فتحي سرور، المرجع السابق، ص390.

[5] محمد فاروق عبد الحميد كامل، القواعد الفنية الشرطية للتحقيق والبحث الجنائي، أكاديمية نايف للعلوم الأمنية، الرياض، ط1، 2006، ص66.

التفتيش، إذ ينصب الاهتمام بالمعاينة على الأجهزة الإلكترونية مثل الحاسب الآلي وملحقاته من وسائل اتصال بالشبكة العنكبوتية مثل الطابعة، جهاز الماسح الضوئي وجميع الوسائل التي من الممكن أن يكون محملا عليها أدلة إلكترونية، وإجراء المعاينة يتطلب سرعة الانتقال إلى محل الجريمة للمحافظة على آثار الجريمة قبل العبث فيها أو إتلافها أو التخلص منها، وهي إجراء هادف غايته كشف وصيانة العناصر المادية التي تتعلق بالجريمة وتفيد في التحقيق الجاري بشأنها، فإذا انعدمت بالنسبة للتحقيق جدواها وفائدتها لا يكون ثمة مجال أو مقتضى لإجرائها، ولا تجدي في كشف الحقيقة بشأنه المعاينة مثل جريمة التزوير المعنوي وجريمة القذف والسب التي تقع بالقول في غير العلانية وغيرها[1].

ثانيا: مسرح الجريمة الإلكترونية المرتكبة، ينبغي عند البدء في جمع الأدلة من مسرح الجريمة المتصلة بالتكنولوجيا الحديثة التفرقة بين مسرحين للجريمة المرتكبة، الأول؛ مسرح تقليدي ويقع خارج البيئة الرقمية ويتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، وهو أقرب ما يكون إلى مسرح أية جريمة تقليدية قد يترك الجاني فيها أثارا عديدة كالبصمات وغيرها، وربما يترك متعلقات شخصية أو وسائط تخزينية رقمية، ويتعامل أعضاء فريق التحقيق مع الأدلة الموجودة فيه كل حسب تخصصه، أما الثاني؛ مسرح إلكتروني يقع داخل البيئة الرقمية يتكون من البيانات الرقمية التي تتواجد وتنتقل داخل بيئة الأجهزة الإلكترونية وشبكاتها، في ذاكرتها وفي الأقراص الصلبة الموجودة بداخلها أحيانا، وننوه هنا إلى أن التعامل مع الأدلة الموجودة في هذا المسرح يجب ألا يتم إلا على يد خبير متخصص في التعامل مع الأدلة الرقمية، والمعاينة في الجريمة المتصلة بالتكنولوجيا الحديثة تتم على جزء خاص بمعاينة المكونات المادية، وجزء خاص بالمكونات غير المادية وهي البرامج والبيانات المتواجدة على الجهاز.

1- معاينة المكونات المادية، يتطلب هذا الجزء من المحقق الانتقال إلى مسرح الجريمة والتحفظ السريع على مكونات الأجهزة الإلكترونية بكافة مشتملاتها قبل العبث بها وهذه المشتملات قد تكون عبارة عن الحاسب الآلي مثلا وملحقاته ووسائل الاتصال بالإنترنت، وهذه المعاينة أقرب إلى المعاينة العادية في الجرائم الجنائية العادية.

2- معاينة المكونات غير المادية، يفترض التفتيش داخل الأجهزة الإلكترونية وما تحتويه من بيانات وبرامج في القائمين بهذه المعاينة الإلمام الجيد بها وبمختلف البرمجيات لأن التفتيش يتم داخل الأجهزة ذاتها أو في شبكة الإنترنت عن طريق بيانات المتهم على الشبكة، فيمكن من خلال الأجهزة نفسها الولوج إلى البريد الإلكتروني الخاص بالمتهم وفحص رسائل التهديد التي قام بإرسالها للضحية مثلا، أو معرفة حسابه على مواقع التواصل الاجتماعي وكلمة المرور الخاصة به، ومن خلال حسابه يمكن التعرف على ما قام به من نشر أفكار متطرفة أو إشاعات كاذبة أخلت بالأمن والسلم الاجتماعي... وهكذا.

نظرا لخطورة نتائج المعاينة في الكثير من التحقيقات، فإنه يمكن إجراؤها عبر شبكة الإنترنت والولوج إلى الجهاز المراد معاينته عن طريق بعض البرامج المختلفة، مما يستوجب مراعاة عدة نقاط قبل معاينة مكان جرائم التكنولوجيا الحديثة نذكر على سبيل المثال الإعداد الجيد قبل المعاينة لعدم تسرب الأدلة أو إتلافها، اصطحاب الخبراء المتخصصين لمرافقة فريق التحقيقات، مع توفرهم على مجموعة من البرامج المختلفة قبل المعاينة، خاصة تلك المتعلقة باستعادة الملفات المحذوفة، وبرامج كسر كلمة المرور، وبرامج فحص

[1] هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني وآليات التدريب التخصصي للمحققين، المرجع السابق، ص483.

الهواتف المحمولة، بالإضافة إلى وسيلة توليد كهرباء بديلة وآمنة حتى لا ينقطع التيار الكهربائي أثناء الفحص وهو ما يهدد بإتلاف مكونات الأجهزة وبالتالي تلف الدليل.

كما أن هناك بعض الإجراءات الواجب اتخاذها عند القيام بالمعاينة مثل:

- تصوير الجهاز وملحقاته ووضعه في المكان الذي يوجد فيه.
- فحص سلة المهملات لمعرفة الملفات التي تم حذفها مؤخرا، بالإضافة إلى استخدام برامج إعادة الملفات المحذوفة نهائيا.
- التحفظ على المستندات الخاصة بالإدخال وكذلك ملحقات الأجهزة المادية والورقية والمرتبطة بالجريمة وما قد يوجد عليها من آثار.
- الحرص على عدم إتلاف أي بيانات يتم استخراجها من الجهاز وكذلك التأكد من وجود نسخة منها محفوظة على الجهاز نفسه.
- الفحص بدقة لكل ملفات الجهاز وخاصة ملفات log file للتعرف على جميع العمليات التي قام بها مستخدم الجهاز والمواقع التي ارتادها على شبكة الإنترنت وكذلك أسماء حساباته في مواقع التواصل الاجتماعي وكلمات المرور الخاصة به.

ثالثا: أهمية المعاينة، تتسم المعاينة بمركزها المحوري لدورها الفعال في تصور وقوع الجريمة وظروف وملابسات ارتكابها وتوفير الأدلة المادية من المادة التي تجمع عن طريقها وتمحيص وتقييم الأدلة الأخرى والتنسيق بينها في ضوء المعلومات التي تتوافر، بما يكفل في ذات الوقت التخطيط السليم لعمليات البحث، والتحقيق الجنائي وتطورها، إلا أن دورها في مجال كشف غموض الجرائم المتصلة بالتكنولوجيا الحديثة، وضبط الأشياء التي قد تفيد في إثبات وقوعها ونسبتها إلى مرتكبها، لا يرقى إلى نفس الدرجة من الأهمية، ويمكن رد ذلك إلى أن هناك على الدوام تقريبا مسرحا للجريمة التقليدية جرت عليه الأحداث، وتركت آثارها المادية التي تنبثق عنها الأدلة، والمعاينة في مسرح الجريمة تتيح المجال أمام الباحث والمحقق الجنائي للكشف عن الآثار المادية التي خلفها ارتكاب الجريمة، والتحفظ على الأشياء التي تفيد في التحقيق الجاري بشأنها، بينما لا يوجد عادة مسرح مماثل لجرائم التكنولوجيا الحديثة المرتكبة، وأقرب تشبيها لمسرحها، قد يكون في الموقع أو المكتب الذي توجد فيه المعدات والأنظمة الإلكترونية، التي كانت محلا للجريمة أو أداتها[1].

ويقلل مثل هذا المسرح إلى حد كبير من فرص إفصاحه عن الحقائق المراد التوصل إليها من وراء معاينته لسببين رئيسيين أولهما؛ أن الجرائم التي تقع بواسطة الأنظمة الإلكترونية قلما تخلف آثارا مادية، وثانيهما؛ أن عددا كبيرا من الأشخاص يكون قد تردد على مسرح الجريمة خلال الفترة الزمنية الطويلة نسبيا التي قد تنقضي عادة بين ارتكاب الجريمة واكتشافها، مما يفسح المجال لحدوث تغيير أو تلف أو عبث بالآثار المادية أو زوال بعضها وهو ما يلقى ظلالا من الشك حول الدليل المستقى من المعاينة[2].

وفي كل الأحوال عند تلقي بلاغ عن وقوع إحدى الجرائم المتصلة بالتكنولوجيا الحديثة، وبعد التأكد من البيانات الضرورية في البلاغ يتم الانتقال إلى مسرح الجريمة لمعاينته، ومسرح الجريمة الإلكترونية يختلف عن مسرح الجريمة التقليدية كالقتل والسرقة، فجريمة

---

[1] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص101.

[2] أمير فرج يوسف، المرجع السابق، ص220.

التكنولوجيا الحديثة قد تكون جريمة مستمرة كما في حالة الجرائم الاقتصادية –السرقة والاحتيال–، وقد يكون مسرحها كالجرائم الأخرى كما في التزوير وإتلاف البرامج وتفجير المباني والمنشآت.

ففي حالة الجريمة المستمرة ذات الأهداف الاقتصادية؛ يكون هدف المعاينة المداهمة وضبط الأدلة على الطبيعة، وفي الحالة الثانية؛ –بعد وقوع الجريمة– فالأمر متوقف على اعترافات المتهمين متى تم القبض عليهم وكذلك شهادة الشهود والقرائن، وعند إجراء المعاينة بعد وقوع الجريمة في المجال الافتراضي يجب مراعاة الضوابط التالية[1]:

– إخطار الفريق الذي سيتولى المعاينة قبل موعدها بوقت كاف حتى يستعد من الناحية الفنية والعملية، وذلك لكي يضع الخطة المناسبة لضبط أدلة الجريمة حال معاينتها.

– إعداد خطة المعاينة موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها على أكمل الوجه.

– تصوير الوسائل الإلكترونية والأجهزة الطرفية المتصلة بها، على أن يتم معرفة وقت وتاريخ ومكان التقاط كل صورة.

– العناية بالطريقة التي تم بها إعداد النظام.

– ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عمليات المقارنة والتحليل حين عرض الأمر فيما بعد على المحكمة.

– عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقعها من أي مجال لقوى مغناطيسية يمكن أن يتسبب في تلف البيانات المسجلة.

– التحفظ على معلومات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة، وفحصها، ورفع البصمات ذات الصلة بالجريمة.

– التحفظ على مستندات الإدخال والمخرجات الورقية ذات الصلة بالجريمة.

– قصر مباشرة المعاينة على الباحثين والمحققين الذين تتوافر لهم الكفاءة العلمية والخبرة الفنية في المجال الإلكتروني[2].

– أن تتم هذه الإجراءات وفق مبدأ المشروعية، في إطار ما تنص علية القوانين الجنائية.

ويتم توثيق مسرح الجريمة ووصفه بكامل محتوياته بشكل جيد مع توثيق كل دليل على حدى بما فيها الأدلة الرقمية، بحيث يتم توضيح مكان الضبط والهيئة التي كان عليها، ومن قام برفعه وتحريره وكيف ومتى تم ذلك، وهناك رأي يرى أن التوثيق يجب أن يشمل كافة المصادر المتاحة على الشبكة التي ترتبط بها الأجهزة محل التحقيق، ولعل أبرز الأماكن التي يحتمل وجود الأدلة الجنائية

[1] Leonard Territo, Neil C. Chamelin, Charles R Swanson, Robert W Taylor, Criminal Investigation, McGraw-Hill Education, New York, United States, 5th Ed., 1992, p450.

[2] محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية مركز البحوث والدراسات، أكاديمية شرطة دبي، الإمارات العربية المتحدة، 28 نيسان 2003.

المتعلقة بجرائم التكنولوجيا الحديثة فيها ما يلي[1]؛ الورق، المكونات المادية[2]، البرامج[3]، وسائط التخزين المتحركة[4]، دليل الاستخدام[5] كلمات السر أو أرقام الهاتف...إلخ.

الفرع الثالث: الخبرة الفنية في جرائم التكنولوجيا الحديثة

تعاظم دور الإثبات العلمي للدليل مع ظهور الجرائم المتصلة بالتكنولوجيا الحديثة وضرورة اشتقاق الأدلة الرقمية المطلوبة للإثبات في هذه الجرائم وكشف أنماط الجرائم المرتكبة باستخدام الأجهزة الإلكترونية، وهو الدور الذي يطلع به الخبراء القضائيون فأصبح إنشاء المعامل الجنائية الرقمية مطلبا ملحا لفحص الأدلة الرقمية لتقييم عملية الإثبات الرقمي وتحليل الجرائم في نطاق ما يعرف باسم نظم الخبرة الأمنية[6].

البند الأول: القواعد القانونية التي تحكم الخبرة القضائية في الجرائم الإلكترونية

تقضي المبادئ القانونية أن القاضي لا يلجا إلى الخبرة الفنية إلا بالنسبة للوقائع التي يقضي العلم بها أو تفسيرها معرفة خاصة لا تتوافر فيه، وتكون غير ثابتة أو غير واضحة من خلال الوثائق والمستندات، أو الأدلة الواردة في الدعوى، أو تلك الوقائع التي لا يمكن إثباتها بوسيلة أخرى كالشهادة أو القرائن أو المعاينة، لذلك فهو يستعين بالخبير أو الفني لتوضيحها وتقديم المشورة الفنية التي يحتاجها للفصل في الدعوى[7].

أولا: ماهية الخبرة، عرفت الخبرة الفنية القضائية بأنها: "إجراء يتعلق بموضوع يتطلب الإلمام بمعلومات فنية لإمكان استخلاص الدليل منه"[8]، وقد عرفها البعض بأنها تلك الاستشارة الفنية التي يستعين بها القاضي في مجال الإثبات لمساعدته في تقدير بعض المسائل التي يحتاج تقديرها إلى معلومات خاصة وكفاية علمية أو فنية لا تتوافر لديه بحكم عمله وثقافته[9].

والخبرة كدليل في الإثبات تنصرف إلى رأي الخبير الذي يثبته في تقريره[10]، وبما أن تقرير الخبير يعتبر من الأدلة الفنية فإن

---

[1] محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة 01-03 مايو 2000، ص158.

[2] Eoghan Casey, Op.Cit., p273.

[3] Anthony Sammes, Brian Jenkinson, Forensic Computing: A Practitioner's Guide, Springer Science & Business Media, Berlin, Germany, 2013, p183.

[4] Eoghan Casey, Op.Cit., p274.

[5] حسين بن سعيد بن سيف الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت، مقال منشور على موقع شبكة قوانين الشرق: www.eastlaws.com

[6] ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص09.

[7] Rene Garraud, Traité Théorique et Pratique d'Instruction Criminelle et de Procédure Pénale Vol. 01, Creative Media Partners, 2018, p592. Roger Merle, et André Vitu, "Traité de droit criminel–Problèmes généraux de la science criminelle". Droit pénal général, 6ème Éd., 2000 p211.

[8] مأمون محمد سلامة، المرجع السابق، ص645.

[9] أمال عبد الرحيم عثمان، الخبرة الفنية، المسائل الجنائية، دراسة قانونية مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة، 1964، ص19.

[10] مأمون محمد سلامة، المرجع السابق، ص645.

إجراء ندب الخبير هو من إجراءات جمع الأدلة، فللمحقق الاستعانة بالخبراء ليستطلع رأيهم في بعض الأمور التي تعرض له أثناء تأدية مهمته في التحقيق الذي ينتهي بإصدار قرار بأن لا وجه لإقامة الدعوى أو بإحالتها إلى محكمة الموضوع، أما الخبرة في مرحلة المحاكمة فإنها تساعد القاضي في تكوين عقيدته للفصل في القضية[1].

تنحصر الوقائع التي يمكن تقرير الخبرة بشأنها في الوقائع المادية دون المسائل القانونية التي تبقى من صلاحية القاضي وحده إذ لا يجوز للقاضي تفويض صلاحيته تلك لشخص آخر، فقد يلجأ القاضي المكلف بالفصل بالدعوى إلى الخبرة الفنية القضائية كلما اعترضه مسألة فنية يتوقف عليها الفصل في القضية، فلا يتصور أن يتفهم القاضي جميع المسائل الفنية التي تعرض عليه وحتى يتمكن من الفصل فيها بينة تامة فصلا يريح ضميره ويحقق العدالة[2].

والخبير هو كل شخص له دراية خاصة بمسألة من المسائل، وقد يستدعي التحقيق فحص مسألة يستلزم لفحصها كفاءة خاصة فنية أو علمية لا يشعر المحقق بتوافرها في نفسه فيمكنه أن يستشير فيها خبيرا، كما هو الحال في تمرير الصفة التشريحية في جرائم القتل أو تحليل المادة المطعومة في جريمة تسمم أو فحص لخطوط الكتابة المدعى بتزويرها[3].

وقد أجاز المشرع لجهات التحقيق ندب الخبراء إذا كانت طبيعة الجريمة محل التحقيق تقتضي الاستعانة بالخبرة لحسم مسألة فنية معينة، أو للبحث عن أدلة الجريمة وضبطها، كما أن للمحكمة أن تتخذ ما تراه من وسائل –بما في ذلك ندب الخبراء– لبحث وفهم أية واقعة فنية اعترضتها.

وإذا كان لندب الخبراء أهمية في الجرائم التقليدية، فإن أهميته أكثر وضرورتها أشد في إجراءات جمع أدلة المكونات المعنوية في كل وحدات التخزين وتحليلها وكشف أي تلاعب في البرامج والمعلومات، غير أن ذلك لا يعني عدم الاكتراث بمسألة تأهيل سلطات الملاحقة وتزويد أفرادها بالمعرفة العلمية والتقنية ليكونوا على دراية فيما يستلزم ندب الخبراء وفهم ما يقدمونه من آراء.

ثانيا: مدى حجية تقرير الخبير، يظهر الواقع العملي أن القاضي غالبا ما يسلم بما خلص إليه الخبير في تقريره، ويبني حكمه على أساسه، وهذا تصرف منطقي، فلا شك في أن رأي الخبير إذا ورد في موضوع فني لا اختصاص للقاضي به، وليس من شأن ثقافته أو خبرته القضائية أن تتيح له الفصل فيه بالإضافة إلى ذلك فهو الذي انتدب الخبير ووثق فيه ورأى أنه مناسب لمهمته[4] فلابد أن يأخذ برأيه، ويؤكد بعض الفقه على ضرورة إعطاء قوة إلزامية لتقرير الخبير[5]، وذلك على أساس أن القاضي إذا رفض رأي الخبير فقد تعارض مع نفسه، إذ يعني ذلك أنه أراد أن يفصل بنفسه في مسألة سبق أن اعترف في بادئ الأمر بأن الخبير يتمتع فيها بمعرفة ودراية تفوق معرفته الشخصية.

---

[1] فوزية عبد الستار، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1986، ص322.

[2] عصام محمود عبد الحليم يوسف، المسؤولية الجنائية للمصابين بالأمراض العصبية والنفسية، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة، 2014 ص374.

[3] أحمد فتحي سرور، المرجع السابق، ص457 وما بعدها.

[4] Jean Pradel, Les rôles respectifs du juge et du technicien dans l'administration de la preuve en matière pénale, Institut d'Etudes Judiciaires, Presses Universitaires de France, Paris, 1976 p67.

[5] أمال عبد الرحيم عثمان، الخبرة الفنية، المسائل الجنائية، دراسة قانونية مقارنة، المرجع السابق، ص307 وما بعدها.

ثالثا: الأدلة المتحصلة بالوسائل الإلكترونية عن طريق الخبرة الفنية، الخبرة هي بحث لمسائل مادية أو فنية يصعب على المحقق أن يشق طريقه فيها وحده، ويعجز عن جمع الأدلة بالنسبة لها بالوسائل التقليدية للإثبات، كالتأكد من حقيقة صور تم تعديلها، أو نسبة أصوات إلى أصحابها، أو التأكد من حقيقة مشهد فيديو تم التلاعب فيه أم لا.

ولأجل الوقوف على الحقيقة في مثل هذه المسائل العلمية والفنية؛ فإن القانون أجاز للمحقق أن يستعين بخبير متخصص في المسألة موضوع الخبرة، ويعد ندب المحقق للخبير؛ إجراء من إجراءات التحقيق يقطع التقادم، وذات الشأن بالنسبة لإيداع تقرير الخبرة، لكن أعمال الخبرة ذاتها لا أثر لها على التقادم لأنها أعمال مادية[1].

وبالنظر لما حدث من ثورة في عالم تكنولوجيا الاتصالات عن بعد نجد أنها قد أتت بتقنيات علمية ذات طبيعة فنية متقدمة، وقد أفرزت هذه التقنيات جرائم ذات طبيعة فنية وعلمية معقدة، يحتاج جمع الدليل بالنسبة لها إلى بحث مسائل علمية وفنية، فالأدلة قد تكون غير مرئية ويلزم تحويلها إلى أدلة مقروءة، وقد تكون نتيجة تلاعب في حسابات معينة أو في نظم إلكترونية معينة بحيث يحتاج الكشف عنها إلى متخصصين لإثبات هذا التلاعب، وقد يحتاج الأمر إلى عمليات فنية دقيقة لإمكان الدخول إلى أنظمة الوسائل الإلكترونية نتيجة استخدام الشفرات وكلمات المرور السرية، وإذا كان الهدف من الخبرة الوصول إلى الحقيقة في مسائل علمية وفنية ومادية فإنها لا تكون حكرا على سلطة التحقيق وإنما يحق للمحكمة أن تأمر بها.

وبالنسبة إلى الجرائم المتصلة بالتكنولوجيا الحديثة؛ ونظرا إلى الطبيعة الخاصة بها فإن اكتشافها وبيان حقيقتها قد يحتاج إلى خبرة فنية قد تظهر الحاجة إليها منذ بدء مرحلة التحري عن هذه الجرائم، ثم تستمر الحاجة إليها في مرحلتي التحقيق والمحاكمة نظرا للطابع الفني الخاص بأساليب ارتكابها والطبيعة المعنوية لمحل الاعتداء[2].

رابعا: الإقرار بحجية الوسائل الإلكترونية في الإثبات، تجمع النظم القانونية كالقانون الفرنسي والأمريكي في الوقت الراهن على حجية الملفات المخزنة في نظم ومستخرجات الأجهزة الإلكترونية والبيانات المسترجعة من نظم الميكروفيلم مثلا، وحجية الملفات ذات المدلول التقني البحت، والإقرار بصحة التوقيع الإلكتروني وتساويه في الحجة مع التوقيع التقليدي، والتخلي شيئا فشيئا عن أية قيود تحد من الإثبات في البيئة التقنية، والسنوات القادمة ستشهد تطورا أيضا في الاتجاه نحو قبول الملفات الصوتية والتناظرية والملفات ذات المحتوى المرئي وغيرها[3].

خامسا: مجالات الخبرة الفنية القضائية، أفرز التطور الهائل في مجال تكنولوجيا المعلومات والاتصالات –العصر الرقمي أو الإلكتروني– العديد من الأنشطة المستحدثة التي تتم باستخدام الوسائل الإلكترونية، والتي قوامها النظم والبرامج وشبكات الاتصالات العالمية، كأعمال التجارة الإلكترونية والمصارف، الإدارة الإلكترونية، والحكومة الإلكترونية، مما ترتب عليه تنوع الجرائم التي تقع على هذه العمليات وفقا لتنوع الوسائل الإلكترونية المستخدمة في ارتكابها، ومن أمثلة هذه الجرائم[4]تزوير المستندات المدخلة

---

[1] محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات التشريعية، ترجمة وتحقيق: فوزية عبد الستار، دار النهضة العربية، القاهرة ط6، 2019، ص162.

[2] مفتاح أبو بكر المطردي، المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، جمهورية السودان، 23 إلى 25 سبتمبر 2012.

[3] هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، ط2، 2008، ص27.

[4] هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، القاهرة، 2000، ص137.

في أنظمة الأجهزة الإلكترونية أو الناتجة بعد المعالجة، التلاعب في البيانات، التلاعب في البرامج الأساسية أو برامج التطبيقات والغش أثناء نقل وبث البيانات.

البند الثاني: الصعوبات التي تواجه الخبير ومتطلباته في جرائم التكنولوجيا الحديثة

للدليل الجنائي الرقمي أهمية كبرى ودور أساسي في معرفة كيفية حدوث الجريمة، ولتأكيد ذلك لا بد وأن يحتوي التحقيق الجنائي الرقمي على هذا الدليل ويجب أن تكون المنشأة على استعداد وتأهب لمثل هذه الأمور غير الاعتيادية، كما يجب أن يكون الأشخاص المسؤولون عن التعامل مع هذه الأمور على فهم واضطلاع كبير بالأمور التقنية وألاعيبها وكيفية التعامل معها.

فجرائم التكنولوجيا الحديثة تتسم بصعوبة اكتشافها وإثباتها بحكم أنها تتم في بيئة لا علاقة لها بالأوراق أو المستندات، ما يمكن الجاني من العبث في البيانات والبرامج عن طريق نبضات إلكترونية غير مرئية، وذلك في وقت قياسي قد يكون جزءا من الثانية وهذه البيانات أو المعلومات التي يتم العبث بها يمكن محوها كذلك في زمن قياسي قبل أن تصل إلى يد العدالة، لاسيما وأن عملية الضبط لا تتم سوى بمعرفة خبير فني أو متخصص[1].

أولا: الصعوبات التي يواجها الخبير في جمع الأدلة الإلكترونية، يواجه الخبير الجنائي صعوبات متعددة في سبيل جمع الأدلة الرقمية من الأجهزة الإلكترونية أو الشبكات الرقمية نذكر منها:

– فقد جزء كبير من المعلومات والأوامر التي تشكل الأدلة الرقمية في حال إغلاق جهاز الحاسب الآلي بطريقة غير صحيحة، أو في حالة القطع المفاجئ للتيار الكهربائي عن الجهاز، فإن مثل هذا الفعل قد يؤدي إلى محو المعلومات من ذاكرة الجهاز أو العمل على تحريف بيانات هامة وحدوث ضرر في أجهزة الجوانب المادية أو منع إعادة التحميل وبالتالي فقدان للأدلة الجوهرية.

– قيام الجاني بتهيئة جهاز الحاسب الآلي للتفجير أو التدمير بمجرد تشغيله بالضغط على زر توصيل الطاقة.

– طبيعة مسرح الجريمة في الشبكات المنتشرة على مستوى العالم، لذا فقد لا يكون ممكنا الحصول على دليل في حالة توزيع مسرح الجريمة بين أكثر من دولة بسبب تعقيد الإجراءات أو وجود مشاكل عملية وتشريعية في بعض الدول مما يحول دون الحصول علي دليل إلكتروني، كما أن سرعة مرور البيانات الرقمية عبر الشبكات مع مهارة المجرمين في تدمير الأدلة أو تحريف أو تعديل البيانات لحماية أنفسهم وكذلك حجم البيانات الضخمة التي تمر عبر الشبكات يكون له التأثير العكسي عند البحث عن دليل الإدانة أو البراءة.

– إخفاء الهوية، إن تعمد المستخدم إخفاء هويته عند استخدام الإنترنت سواء القيام ببعض الإجراءات أو استخدام بعض البرامج والتطبيقات التي تؤدي لطمس الهوية يشكل عائقا أمام المحقق الجنائي أو الخبير الفني.

– إخفاء المعلومات، أو وجود بعض البرامج الخاصة بإخفاء المعلومات أو البيانات، وذلك لخلق ما يعرف بنظام ملفات آمن عبر استخدام الشبكة العالمية مما يجعل عملية استعادة الأدلة أو إعادة تركيبها في غاية الصعوبة أمام المحقق الجنائي أو الخبير ومن ذلك يتضح أن صعوبة الحصول على الأدلة الجنائية الرقمية يتطلب خبرة ومهارة كبيرة في التكنولوجيا الرقمية الحديثة.

---

[1] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، المرجع السابق ص24.

ثانيا: متطلبات أعمال الخبرة القضائية في مجال جرائم التكنولوجيا الحديثة، تتنوع الوسائل الإلكترونية والأجهزة التي تستخدم نظم الحاسبات الآلية كما تتنوع شبكات الاتصال بينها، وتتمايز خصائصها الفنية فتندرج تحت تخصصات فنية وعلمية دقيقة مما يستوجب أن تدقق جهات التحقيق والمحاكمة عند اختيارها للخبير، فيجب أن تتيقن أنه تتوافر لديه الإمكانيات والقدرات العلمية والفنية في مجال التخصص الدقيق للحقل الذي يطلب منه بحثه، ولا يكفي في ذلك حصول الخبير على درجة علمية معينة وإنما يجب أن تتوافر لديه أيضا الخبرة العلمية التي تمكنه من اكتساب كفاءة فنية عالية[1]، وبالنظر إلى الطبيعة الفنية والعلمية للخبرة في مجال الجرائم المتصلة بالتكنولوجيا الحديثة فإنه يمكن تحديد هذه الخبرة في الموضوعات الآتية[2]:

– الإلمام بتركيب الأجهزة الإلكترونية وصناعتها ونظم تشغيلها الرئيسة والفرعية، والأجهزة الطرفية الملحقة بها، وكلمات المرور أو السر وأكواد التشفير.

– طبيعة البيئة التي يعمل في ظلها الجهاز الإلكتروني من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية، وتحديد أماكن التخزين والوسائل المستخدمة في ذلك.

– قدرة الخبير على إتقان مأموريته دون أن يترتب على ذلك إتلاف أو تدمير الأدلة المتحصلة من الوسائل الإلكترونية.

– التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة، أو المحافظة على دعاماتها لحين القيام بأعمال الخبرة بغير أن يلحقها تدمير أو إتلاف، مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجل على الأجهزة الإلكترونية محل البحث أو النظام أو الشبكة[3].

علاوة على ذلك فإن الخبير الإلكتروني أو المعلوماتي يجب أن يكون لديه العلم والخبرة والمهارة التي تمكنه من أداء مهمته على الوجه الأمثل لذا يجب أن يكون ملما بما يلي:

– نظم الأجهزة الإلكترونية بمكوناتها المادية والبرمجية.

– رسائل وبرامج وطرق فحص النظم والبرمجيات، كبرامج كشف وإزالة الفيروسات، وبرامج استرجاع البيانات والمعلومات وإصلاح التالف منها وإظهار المخفي منها، وبرامج فك الشفرات وكلمات السر...إلخ.

– رسائل وبرامج نسخ البرامج والملفات، وعمل نسخ طبق الأصل من القرص الصلب.

– كيفية الربط بين الدليل المادي والدليل الرقمي في الوقائع محل البحث.

– كيفية تفسير الملاحظات والربط بين الأشياء واستخلاص نتائج ذات دلالة علمية فنية قضائية.

ثالثا: عملية استخلاص الأدلة، تعد عملية الحصول على الأدلة الجنائية الرقمية أمرا صعب الوصول إليه لما تتطلبه من خبرة ومهارة كبيرة في الفضاء الافتراضي، ويرجع ذلك لتعدد صور وأشكال جرائم التكنولوجيا الحديثة ما بين مهاجمة المعلومات بغرض تدميرها أو الاستيلاء عليها أو قد يكون المقصود بالهجوم هو الأجهزة، كنشر فيروس يعمل على إتلاف وحداته الرئيسية

---

[1] هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، المرجع السابق، ص140 و141.

[2] هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، المرجع نفسه، ص142 و143.

[3] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، المرجع السابق ص98.

مثلا، وقد يكون الأمر مجرد اختراق لكلمة سر خاصة ببنك أو مؤسسة كبرى بغرض الاحتيال والحصول على الأموال، أو قد تكون لمجرد إثبات الذات، ولما كانت عملية تجميع الأدلة العلمية الجنائية في الجرائم الإلكترونية أو الرقمية تعد من أهم وأصعب الأمور التي تواجه عملية الإثبات الجنائي، لذا كان لزاما أن يتم اللجوء إلى خبير قضائي معلوماتي أو رقمي؛ متخصص لاشتقاق الدليل العلمي الفني الجنائي، وهو الخبير المتخصص والمدرب على معالجة جميع أنواع الأدلة الرقمية وفحصها وتحليلها[1].

ويرى بعض المتخصصين أن عملية تجميع واستخلاص الأدلة في الجرائم التي تتم عبر الشبكة العالمية تتم عبر ثلاثة مراحل[2]:

1- المرحلة الأولى: تجميع المعلومات المخزنة لدى مقدم الخدمة لتتبع الأجهزة التي دخل المجرم منها ومحاولة اقتفاء أثره.

2- المرحلة الثانية: مرحلة المراقبة؛ فهناك فرضية بأن المجرم لابد أن يعود أو يحوم حول مسرح جريمته وتتعدد طرق مراقبة هذه الحواسب نذكر منها:

- استخدام برامج مراقبة يمكن تحميلها من أجل البحث عن المعلومات المشتبه فيها وحصر وتسجيل بيانات الدخول والخروج بالموقع.

- استخدام كاميرات مراقبة لشاشة الحاسب الآلي معدة للاستخدام التجاري وأبسط الطرق لمراقبة الحاسب هي الدخول لمكان وجوده وزرعه.

- وهناك وسيلة أخرى أصعب نوعا ما، وهي زرع فيروس الحاسب الآلي أو دودة من نوع حصان طروادة وهذه الوسيلة لها ميزة أنها تستطيع مراقبة أكثر من جهاز واحد ولكن يجب عدم السماح للفيروس بالانتشار والا فسوف يصبح هدفا لبرامج الدفاع ضد الفيروسات.

3- المرحلة الثالثة: ضبط الأجهزة المشتبه فيها وفحصها فحصا فنيا شرعيا، في هذه المرحلة يبدأ عمل الخبير المعلوماتي في فحص نظام جهاز المشتبه فيه بمكوناته المادية والبرمجية سعيا لاشتقاق الدليل لتقديمه لجهة التحقيق أو الحكم، لتقرير مدى وقوع الجريمة باستخدام النظام المضبوط من عدمه، ولتقرير إدانة المتهم أو تأكيد براءته، كل ذلك وفق الأسس والقواعد الفنية المتعارف عليها والمتبعة في مجال الخبرة الإلكترونية، مع مراعاة القواعد القانونية لمبدأ المشروعية.

ويتعين على الخبير الإلكتروني التنسيق مع المحقق الجنائي قبل محاكمة الجاني عن الجريمة المرتكبة في العالم الرقمي، على أن يشمل اللقاء كافة الخبراء الذين ساهموا مع سلطات الضبط أو التحقيق في تلقي البلاغ أو إجراءات الضبط والتفتيش أو فحص البرامج وجمع الأدلة الجنائية، على أن يتم في هذا اللقاء حصر الأدلة المتوافرة وترتيبها وفقا لأهمية كل دليل أو قرينة، كما يجب على المحقق الجنائي أن يشرح لهؤلاء الخبراء الجوانب القانونية لطبيعة عملهم مع التأكيد على ربط الأدلة بالخبرة العلمية بعناصر وأركان الجريمة ضد المتهم[3].

---

[1] محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، المرجع السابق، ص243.

[2] Orin S. Kerr, Digital evidence and the new criminal procedure, Columbia Law Review, Vol. 105, 2005, p258.

[3] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، المرجع السابق ص99.

وتجدر الإشارة كذلك إلى أنه وإن كان من المقرر أن المحكمة تملك سلطة تقديرية بالنسبة لتقدير الخبير الذي يرد إليها، إلا أن ذلك لا يمتد إلى المسائل الفنية فلا يجوز لها تفنيدها إلا بأسانيد فنية تخضع للتقدير المطلق لمحكمة الموضوع، ومن ثم فلا تستطيع المحكمة أن تفندها وترد عليها إلا بأسانيد فنية قد يصعب عليها أن تشق طريقها فيها إلا عن طريق خبرة فنية أخرى[1].

المطلب الثالث: الإجراءات الحديثة لجمع الدليل الإلكتروني

نظرا للتطور السريع في وسائل الاتصالات وتكنولوجيا المعلومات ونقل البيانات تواجه الخبير الإلكتروني في مجال جمع الأدلة الرقمية صعوبات عديدة من الأجهزة الإلكترونية أو الشبكات الرقمية، فقد أدى هذا الازدهار إلى تطور مواز في طرق ارتكاب الجرائم سواء التقليدية أو تلك المستحدثة، وهذا الاستخدام السلبي لوسائل التكنولوجيا الحديثة أدى إلى صعوبة تعقب المجرمين والحصول على الأدلة المتخلفة من جراء تلك الجرائم، وهو ما دفع المجتمع الدولي إلى محاولة الحصول على أدلة بطرق حديثة تواكب التطور الحادث في مجال الجريمة.

الفرع الأول: التسرب كإجراء حديث لجمع الدليل الإلكتروني

بالنظر إلى التطور السريع الذي تعرفه جرائم التكنولوجيا الحديثة، ومن أجل التمكن من مكافحتها والقضاء عليها كان لزاما على المشرع الجزائري استحداث أساليب خاصة للبحث والتحري تختلف عن تلك المعمول بها في مواجهة الجرائم العادية، ومن بين الأساليب الجديدة التي استحدثها المشرع الجزائري في ميدان التحقيق في الجرائم المستحدثة نجد ما يسمى بأسلوب التسرب، أو الاختراق كما سماه المشرع في القانون المتعلق بالوقاية من الفساد ومكافحته، إذ يشكل هذا الأخير إحدى الصلاحيات الجديدة التي منحها قانون الإجراءات الجزائية لقاضي التحقيق التي لم يكن يتمتع بها من قبل، وذلك لمواجهة أنواع معينة من الجرائم التي تتسم على وجه التحديد بالخطورة والطبيعة الخاصة، إذ تتمثل هذه الصلاحيات في اعتراض المراسلات وتسجيل الأصوات –التنصت الهاتفي– والتقاط الصور، إضافة إلى الإذن بإجراء عملية التسرب لأجل مراقبة الأشخاص بإيهامهم من قبل الشخص المتسرب بأنه فاعل معهم أو شريك لهم أو خاف.

البند الأول، تعريف إجراء التسرب

يعتبر أسلوب التسرب تقنية من تقنيات التحري والتحقيق الخاصة تسمح لضابط أو عون الشرطة القضائية بالتوغل داخل جماعة إجرامية وذلك تحت مسؤولية ضابط شرطة قضائية آخر مكلف بتنسيق عملية التسرب، بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية وذلك بإخفاء الهوية الحقيقة، ويقدم المتسرب نفسه على أنه فاعل أو شريك.

أما فيما يخص التعريف القانوني للتسرب فقد تناوله المشرع الجزائري في المادة 65 مكرر 12 من قانون الإجراءات الجزائية بقولها: "يقصد بالتسرب قيام ضباط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة

[1] علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، الإمارات العربية المتحدة، 26 و27 أبريل 2003.

الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف".

من خلال التعريف السابق يتضح أن التسرب هو عبارة عن عملية ميدانية تستخدم أسلوب التحري لجمع الوقائع المادية والأدلة من داخل العملية الإجرامية وكذا الاحتكاك شخصيا بالمشتبه بهم والمتهمين وهذا ينطوي على خطورة بالغة تحتاج إلى دقة وتركيز وتخطيط سليم، ومن ثم يمكن القول إن التسرب هو أكثر الوسائل تعقيدا وخطورة، لأنه يتطلب من ضابط الشرطة القضائية وأعوانه القيام بمناورات وتصرفات توحي بأن القائم بها مساهم في ارتكاب الجريمة مع بقية أفراد العصابة، لكنه في حقيقة الأمر يخدعهم ويتحايل عليهم فقط، حتى يطلع على أسرارهم من الداخل ويجمع ما يستطيع من أدلة إثبات، ويبلغ السلطات بذلك فتتمكن من ضبط المجرمين ووضع حد للجريمة.

من هنا نلاحظ أن عملية التسرب ترتكز على ضرورة الحصول على صورة حقيقية على الوسط المراد استكشافه لمعرفة طبيعة سيره وأهدافه وكذا معرفة تاريخ هذه الجماعة وكيفية نشأتها واختصاصات كل فرد من عناصرها، وأيضا الوسائل التي تعمل بها كوسائل النقل والاتصال وتحديد نقاط قوة وضعف هذه الجماعة، وبعد دراسة الوسط المستهدف يتم اختيار الأشخاص المناسبين لتولي مهمة التسرب.

البند الثاني: شروط وإجراءات التسرب

نظرا لما تتسم به عملية التسرب من خطورة وأهمية فقد أحاطها المشرع بمجموعة من الشروط والإجراءات الشكلية والموضوعية لضمان السير القانوني للعملية، إذ اشترط المشرع في المادة 65 مكرر 11 من قانون الإجراءات الجزائية وجوب أن تقتضي ضروريات التحري أو التحقيق إجراء عملية التسرب، وبمفهوم المخالفة فإن وجود أدلة كافية تعزز الاشتباه أو تدعم الاتهام فإنه لا داعي للمخاطرة بإجراء عمليات تسرب وعليه فإن هذه الأخيرة تجري عند الضرورة فقط المتمثلة في قلة أو صعوبة الحصول على أدلة وبراهين كافية لتحريك الدعوى العمومية.

كما اشترط المشرع في اللجوء إلى هذا الأسلوب ضرورة ارتكاب أنواع محددة من الجرائم التي تتسم بالخطورة والتعقيد، من ثم فإن الأمر بإجراء عمليات التسرب ليس مفتوحا لكل الجرائم بل هو خاص بمجموعة محددة من الجرائم على سبيل الحصر المذكورة في المادة 65 مكرر 5 ق.إ.ج، هذه الجرائم هي جرائم المخدرات، أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، أو جرائم تبييض الأموال، أو الإرهاب، أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد فلا يجوز استخدام هذا الأسلوب فيما عدا هذه الجرائم[1]، كما أن هناك عدة إجراءات تطلبها المشرع لصحة عمليات التسرب لإضفاء طابع الشرعية في الحصول على الدليل تطبيقا لمبدأ المشروعية الذي يمثل أساسا لكل إجراء صحيح، سواء من حيث الجهات صاحبة السلطة في الإذن بإجراء عمليات التسرب أو من حيث الجهات المختصة بمباشرة هذا الإجراء.

وضمانا لمشروعية الدليل المستمد من إجراء عملية التسرب في جرائم التكنولوجيا الحديثة؛ اشترط المشرع ضرورة حصول المتسرب على إذن من وكيل الجمهورية المختص وأن تتم عملية التسرب تحت إشرافه ومراقبته، فإن قرر قاضي التحقيق مباشرة هذا

[1] محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2009، ص134.

الإجراء وجب عليه أولا إخطار وكيل الجمهورية بذلك ثم يقوم بمنح إذن مكتوب لضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، على أن يتم ذكر هويته فيه[1].

يجوز لوكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد وهذا ما تناولته المادة 65 مكرر 11، التي اشترطت ضرورة أن تتم العملية تحت رقابة قاضي يقدر هذه العملية ويراقبها خطوة بخطوة لتلافي حدوث تجاوزات للقانون، ويكون هذا الإذن القضائي مكتوبا ومسببا تحت طائلة البطلان طبقا لأحكام المادة 65 مكرر 15، وكما هو معلوم فإن بطلان الإذن يرتب بطلان كافة الإجراءات المتخذة بناء عليه، إذ يشترط أن يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية التي تتم العملية تحت مسؤوليته ويحرر بهذا الإذن مدة عملية التسرب والتي لا يمكن أن تتجاوز أربعة (04) أشهر ويمكن تجديدها حسب مقتضيات التحري والتحقيق كما يجوز للقاضي الذي رخص بها أن يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة وتودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب.

يسمح القانون طبقا لأحكام المادة 65 مكرر 14 لضابط أو لعون الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة وأن يرتكب عند الضرورة الأعمال التالية؛ اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو المستعملة في ارتكابها، واستعمال أو وضع تحت تصرف مرتكبي الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل والتخزين أو الإيداع أو الحفظ أو الاتصال، اعتبر جانب من الفقهاء في هذا الصدد أن هذه الأعمال خروجا عن مبدأ نزاهة ومشروعية الدليل الجنائي للوصول لغاية أسمى هي ضرورة حماية المجتمع عندما تعجز الأساليب التقليدية للتحري والتحقيق عن مواجهة بعض الجرائم.

يحرر ضابط الشرطة القضائية المكلف بالتنسيق تقريرا يتضمن العناصر الضرورية لمعاينة الجرائم غير تلك التي قد تعرض للخطر أمن الضابط العون المتسرب، وكذا الأشخاص المسخرين لهذا الغرض وهذا ما تناولته المادة 65 مكرر 13، وإذا تقرر وقف العملية أو عند انقضاء المهلة المحددة في رخصة التسرب وفي حالة عدم تمديديها يمكن للعون المتسرب مواصلة المهمة للوقت الضروري الباقي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسؤولا جزائيا على أن يتجاوز ذلك مدة أربعة 04 أشهر وإذا انقضت مدة أربعة أشهر دون أن يتمكن العون المتسرب من توقيف نشاطه في ظروف تضمن أمنه يجب إخبار القاضي المرخص الذي يستطيع أن يرخص بتمديدها لمدة أربعة أشهر أخرى على الأكثر.

للإشارة فإنه يجوز سماع ضابط الشرطة القضائية الذي تجري العملية تحت مسؤوليته دون سواه لوضعه شاهدا عن العملية كما يرتب القانون عقوبات جزائية على كل من يكشف هوية ضابط أو أعوان الشرطة القضائية الذين باشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات حسب ما تضمنته المادة 65 مكرر 16، أما عن الجهات المخولة بإجراء عمليات

[1] محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2008، ص115.

التسرب؛ فهم ضباط الشرطة القضائية المذكورون في المادة 15 ق.إ.ج، ويستثنى من هؤلاء لاعتبارات ميدانية الولاة ورؤساء المجالس الشعبية البلدية بالإضافة إلى مساعدي ضباط الشرطة القضائية وهم الأعوان الذين جاء ذكرهم في المادة 19 من نفس القانون فالأعوان يمارسون مهامهم تحت مسؤولية ضباط الشرطة القضائية المكلفين بتنسيق العملية وتصدر باسمهم، كما أضافت المادة 65 مكرر 13 مصطلح المسخرين ويقصد بهم كل الأشخاص من الجنسين يراه ضابط الشرطة القضائية القائم بتنسيق عملية التسرب مفيدا لإنجاز مهمته، وهذا دائما تحت رقابة القضاء.

تجدر الإشارة إلى أن ضابط الشرطة القضائية عند البحث والتحري في جرائم التكنولوجيا الحديثة لا يتقيد باختصاص إقليمي معين، وإنما يشمل كافة التراب الوطني والهدف من ذلك ضمان السرعة والفعالية وكذا تركز التحقيق وعدم تجزئته على عدة دوائر إقليمية، والملاحظ أن هذه الجرائم هي نفسها الجرائم المذكورة في المادة 65 مكرر 5 والخاصة بأساليب التحري الخاصة باستثناء جرائم الفساد التي لم يرد ذكرها في المادة 06/16 ق.إ.ج.

وعليه فالتسرب في هذه الجرائم يتم عبر كامل الإقليم الوطني، غير أنه وبعد الحصول على الإذن والبدء في عملية التسرب قد يصطدم القائم بها بعقبة أخرى وهي أن الجماعة الإجرامية لها نشاطات خارج الإقليم الوطني، وأن أغلب هذه الجرائم تشكل صورة من صور الجريمة المنظمة تتم في إطار عصابات إجرامية لها أنشطة خارج الإقليم الوطني، وهي الحالة التي لم يتطرق لها المشرع الجزائري، فكان بإمكانه النص –في هذه الحالة– على إمكانية إنشاء هيئات تحقيق مشتركة وذلك عن طريق إبرام اتفاقات أو ترتيبات ثنائية، وقد نصت على هذا الشكل من أشكال التعاون المادة 19 من اتفاقية مكافحة الجريمة المنظمة بقولها: "يتعين على الدول الأطراف أن تنظر في إبرام اتفاقات أو ترتيبات ثنائية أو متعددة الأطراف تجيز للسلطات المعنية أن تنشئ هيئات تحقيق مشتركة فيما يتعلق بالمسائل التي هي موضع تحقيقات أو ملاحقات أو إجراءات قضائية في دولة أو أكثر، وفي حالة عدم وجود اتفاقات أو ترتيبات كهذه، يجوز القيام بالتحقيقات المشتركة بالاتفاق في كل حالة على حده ويتعين على الدول الأطراف المعنية أن تكفل الاحترام التام لسيادة الدولة الطرف التي سيجري ذلك التحقيق داخل إقليميها"، وتساعد هذه الوسيلة في كسب الوقت وتقديم نتائج أفضل كما تسمح بتجنب ازدواجية المتابعة وتجنب المشاكل الناتجة عن تنازع الاختصاصات.

إضافة إلى الشروط الشكلية سالفة الذكر يتطلب اللجوء إلى عملية التسرب مجموعة من الشروط الموضوعية تتمثل في:

1– دوافع اللجوء إلى عملية التسرب: بالنظر إلى خطورة عملية التسرب فإنه لا يتم اللجوء إلى هذه العملية إلا إذا اقتضت ضرورة التحري والتحقيق في إحدى الجرائم المذكورة في المادة 65 مكررة وهذا طبقا للمادة 65 مكرر 11، كما يجب أن تنصب عملية التسرب على جناية أو جنحة متعلقة بالجرائم المنصوص عليها في المادة 65 مكرر، وأن يكون هو الإجراء الوحيد أو الأنسب الذي بواسطته يمكن إظهار الحقيقة بعد أن أثبتت الإجراءات الأخرى عدم نجاعتها.

غير أنه وأثناء قيام المتسرب بتنفيذ العملية قد تكتشف جرائم أخرى غير تلك التي تسرب من أجلها وغير واردة في إذن التسرب، فبالرجوع إلى المواد التي تتناول إجراء التسرب نجد أنها جاءت خالية من النص على هذه الحالة، ولم يتناول الجرائم التي تكشف عرضا، على العكس بالنسبة لإجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في المادة 65 مكرر 02/06 ق.إ.ج "إذا اكتشفت جرائم أخرى غير تلك التي ورد ذكرها في إذن القاضي، فإن ذلك لا يكون سببا لبطلان الإجراءات العارضة".

2- صور تنفيذ عملية التسرب: لم يكتف المشرع الجزائري بتبيين الأساليب أو الأفعال التي يمكن للمتسرب القيام بها بل قام يتبين صور تنفيذ العملية في المادة 65 مكرر12 كما يلي:

أ- المتسرب كفاعل: ورد تعريف الفاعل في المادة 41 ق.ع: "يعتبر فاعلا كل من ساهم مساهمة مباشرة في تنفيذ الجريمة أو حرض على ارتكاب الفعل بالهبة أو الوعد أو التهديد أو إساءة استعمال السلطة أو الولاية أو التحايل أو التدليس الإجرامي" وطبقا للمادة 65 مكرر 12؛ يمكن للشخص الذي يتولى القيام بعملية التسرب عن طريق التمويه أن يتخذ صورة فاعل أساسي في الجريمة ويقوم بالأفعال المنصوص عليها في المادة 65 مكرر 14، وفي هذا الصدد لابد من التفريق بين إيهام الغير بأنه فاعل وبين التحريض على ارتكاب الجريمة.

ب- المتسرب كشريك: ورد تعريف الشريك في المادتين 42 و43 ق.ع، فالشريك حسب المادة 42 هو كل من ساعد بكل الطرق أو عاون الفاعل أو الفاعلين على ارتكاب الأفعال التحضيرية أو المسهلة أو المنفذة لها مع علمه بذلك، ويدخل في حكم الشريك طبقا للمادة 43 كل من اعتاد تقديم مسكن أو ملجأ أو مكان للاجتماع لواحد أو أكثر من الأشرار الذين يمارسون اللصوصية أو عنف ضد أمن الدولة أو الأمن العام أو ضد الأشخاص أو الأموال مع علمه بسلوكهم الإجرامي.

ج- المتسرب كخاف: يقصد بذلك أن يقوم المتسرب بإيهام أعضاء الجماعة الإجرامية بأنه واحد منهم من خلال قيامه بإخفاء أشياء قد تكون أدلة ارتكابهم الجرائم أو العائدات التي تم تحصيلها من خلال ارتكاب الجرائم، وقد ورد النص على إخفاء الأشياء في المواد 387 ق.ع: "كل من أخفى أشياء مختلسة أو مبددة أو متحصلة من جناية أو جنحة في مجموعها، أو في جزء منها..."، كما يستطيع المتسرب إخفاء الأشياء المتحصل عليها من الجريمة أثناء قيامه بمهامه دون أن تقوم مسؤوليته الجنائية طبقا للمادة 65 مكرر 12.

البند الثالث: الحماية القانونية المقررة للمتسرب

بالنظر إلى الطبيعة الخاصة لنظام التسرب وخطورته على القائم به، فقد خصه قانون الإجراءات الجزائية بتدابير خاصة من أجل حمايته والحفاظ على أمنه وسلامته من أي أعمال انتقامية قد يكون عرضة لها سواء أثناء العملية أو بعدها.

أولا: الهوية المستعارة، نظرا للخطورة التي قد يتعرض لها ضابط أو عون الشرطة القضائية القائم بعملية التسرب، تناول المشرع الجزائري في المادة 65 مكرر 02/12 العمليات التي يتم إجراؤها تحت هوية مستعارة، ولا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشروا عملية التسرب في أي مرحلة من مراحل الإجراءات طبقا للمادة 65 مكرر 01/16 ويعاقب كل من يكشف هوية الضابط أو العون المتسرب بالحبس من سنتين إلى خمس سنوات وغرامة من 50.000 إلى 200.000 دج، وإذا تسبب كشف هوية الضابط أو العون في أعمال عنف أو جرح على أحد هؤلاء أو أزواجهم أو أبنائهم أو أصولهم المباشرين تشدد عقوبة الحبس من خمس سنوات إلى عشر سنوات، وغرامة من 200.000 إلى 500.000 دج، أما إذا تسبب الكشف في موت أحد هؤلاء تشدد عقوبة الحبس من عشرة إلى عشرين سنة وغرامة من 500.000 إلى 1.000.000دج.

والملاحظ أن المشرع الجزائري عاقب كل شخص يؤدي إلى الكشف عن المتسرب أو معاونيه، إلا أنه تناقض مع مبادئ التجريم والعقاب، فلم يعتد بالخطورة الإجرامية والمتمثلة في الكشف عن الهوية الحقيقية للمتسرب؛ وإنما أخذ بالنتائج المترتبة عن

ذلك، واستعمال الهوية المستعارة يتطلب إصدار وثائق إدارية ورسمية تتضمن الهوية المستعارة، وهو ما يستلزم التنسيق بين جميع المصالح الإدارية والأمنية لاستخراج هذه الوثائق اللازمة كبطاقة التعريف الوطنية، رخصة السياقة وجواز السفر ولذلك فمن الضروري تنظيم هذه الحالة بتحديد هذه الوثائق وكيفية الحصول عليها.

ثانيا: الشهادة القانونية، الحماية القانونية للمتسرب لا تكون فقط أثناء قيامه بالعملية بل تمتد أيضا بعد انتهاء العملية حيث يتم سماع أقوال ضابط الشرطة القضائية المسؤول عن العملية بصفته شاهدا عن العملية دون سواه، وهذا حفاظا على سلامته طبقا للمادة 65 مكرر 18، حيث قام المشرع الجزائري باستثناء العون المتسرب الذي قام بالعملية على الرغم من أنه الشاهد الحقيقي في القضية على الأفعال الإجرامية التي حدثت خلال فترة قيامه بالعملية لاعتبارات أمنية وللحفاظ على سرية هوية المتسرب.

ولم يبين المشرع الجزائري قيمة التصريحات التي يدلي بها الضابط وبالتالي ينبغي الرجوع إلى القواعد العامة، حيث تؤخذ تصريحاته على سبيل الإستدلال ولا ترقى إلى دليل ما لم تقترن بدلائل أخرى والأمر متروك لقاضي الموضوع في الأخذ بها من عدمه.

الفرع الثاني: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

نظرا لعجز وسائل التحري والتحقيق الكلاسيكية عن مواجهة الجرائم الحديثة استحدثت التشريعات المقارنة وسائل تحري وتحقيق حديثة، ومن أهمها اعتراض المراسلات والتقاط الصور وتسجيل الأصوات، والمشرع الجزائري بدوره استحدث هذه الإجراءات في قانون الإجراءات الجزائية في المادة 65 مكرر 5 إلى 65 مكرر 10 حيث أجاز لوكيل الجمهورية أو قاضي التحقيق في المادة 65 مكرر 5 أن يأذن بهذا الإجراء عندما تقتضي ضرورات التحري والتحقيق في إحدى الجرائم المذكورة[1].

فقد تضطر الشرطة القضائية لاستعمال كاميرات خفية أو أجهزة تنصت، لكن يجب أن يكون ذلك في إطار احترام الشرعية الإجرائية حفاظا على كرامة الحياة الخاصة للإنسان، كما يمكن لضابط الشرطة القضائية تصوير جسم ومكان الجريمة بشكلها العام في إطار ممارسة مهامه، لكنه يمنع من الإطلاع أو تسجيل المكالمات أو الأحاديث الخاصة إلا بإذن مسبق من طرف السلطات القضائية، حيث منح للشرطة القضائية حق اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية ووضع ترتيبات تقنية دون موافقة المعنيين من أجل التقاط الصور وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن عامة أو خاصة وتنفذ هذه الإجراءات بموجب إذن من وكيل الجمهورية ويخص فقط التحري في الجريمة المتلبس بها أو التحقيق الابتدائي؛ الخاصة بجرائم محددة ومن بينها جرائم التكنولوجيا الحديثة.

البند الأول: مفهوم اعتراض المراسلات، تسجيل الأصوات والتقاط الصور

الاعتراض والتسجيل والالتقاط هي عدة تسميات لا تخرج عن كونها رقابة مشروعة لشخص أو مكان أو أحاديث أو مراسلات مكتوبة أو مسموعة أو مرئية، نتيجة الاشتباه في تصرفات غير قانونية وذلك بصورة لا يحس معها الغير بمباشرتها لطابع السرية التي يكتنفها، على أن تكون مؤقتة مع اقتصارها على جرائم المخدرات والجريمة المنظمة العابرة للحدود والجرائم الماسة بأنظمة

[1] حصرت المادة 65 مكرر 5 هذه الجرائم في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو جرائم الصرف، أو جرائم الفساد.

المعالجة الألية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد التي حددت على سبيل الحصر، فبسبب هذه الجرائم أصبح بإمكان قاضي التحقيق قانونا:

أولا: اعتراض المراسلات، الاعتراض؛ يعني الاستيلاء بغتة، والمشرع الجزائري خص بالذكر المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية[1] في المادة 65 مكرر 5 ق.إ.ج، وكذا تلك المواد الواردة في قانون البريد والاتصالات الالكترونية ونظرا للتطور الذي عرفه مجال الاتصال فإن نص المادة 65 مكرر 5 سالف الذكر جاء موسعا، أي لم يقصر الاعتراض على المكالمات الهاتفية بل وسعه لمختلف أنواع الاتصال السلكية واللاسلكية، والمشرع لم يول أهمية لأداة الاعتراض فقد تكون تقليدية أو بأحدث ما تم ابتكاره في هذا المجال.

ثانيا: تسجيل الأصوات، تسجيل الأصوات المقصود به تسجيل أحاديث المتهم وشركائه، عن واقعة معينة من الوقائع المنصوص عليها في المادة 65 مكرر 5 سالفة الذكر خلسة[2].

فبعدما أعطى المشرع للمتهم الحق في الصمت، فإنه وبشكل غير مباشر أورد استثناء عليه بموجب المادة 65 مكرر سالفة الذكر، أين أصبح من الممكن أخذ اعتراف الشخص ضد نفسه بشكل خفي ودون رضاه وموافقته عن طريق تسجيل كل ما يتفوه به من كلام بصفة خاصة أو سرية.

ثالثا: التقاط الصور، لم يكتف المشرع الجزائري بالسماح لقاضي التحقيق تسجيل الأصوات، بل مكنه أيضا من إمكانية التقاط الصور، فبموجب المادة 65 مكرر 5 سالفة الذكر سمح قانون الإجراءات الجزائية الجزائري لقاضي التحقيق أن يمد عين الكاميرا إلى الأماكن الخاصة التي تعد مستودعات أسرار المعنيين بالمراقبة.

حتى وإن أعطى المشرع الصبغة القانونية لإمكانية إثبات دليل الجريمة عن طريق تسجيل الأصوات والتقاط الصور، إلا أن هذا الأسلوب من الناحية الفنية والتقنية قيل فيه الكثير، خاصة مع التطور التكنولوجي لعمليات التركيب (المونتاج).

البند الثاني: شروط اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

بالنظر لطبيعة اعتراض المراسلات وتسجيل الأصوات والتقاط الصور كإجراءات غير عادية، فإن المشرع إنطلاقا من أولوية رعاية المصلحة العامة على الحفاظ على أسرار الحياة الخاصة للأشخاص أقر العمل بها، ولكن وفق شروط شكلية وأخرى موضوعية دقيقة مما يحول معه دون التعسف في اللجوء إليها على نطاق واسع وتعميمها على كل الجرائم.

أولا: الشروط الشكلية لإجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، الاستثناء عن القاعدة العامة هو مشروعية اعتراض مراسلات الأشخاص وتسجيل أصواتهم والتقاط صور لهم، والغرض من مشروعية مثل هذه الأعمال هو تحقيق

---

[1] يعتبر وسيلة من وسائل الاتصال السلكي واللاسلكي كل استقبال أو إرسال لإشارة أو كتابة أو صورة أو صوت أو معلومة من أي نوع كانت عبر الأسلاك أو الألياف البصرية أو الكهرباء لا سلكية أو بمختلف الأنظمة الكهرومغناطيسية أو الأقمار الصناعية.

[2] محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، المرجع السابق، ص767. سمير الأمين، مراقبة التليفون والتسجيلات الصوتية والمرئية، دار الكتاب الذهبي، مصر، 2000، ص43.

نوع من التوازن بين حق الشخص في الخصوصية والسرية، وحق المجتمع في مكافحة أخطر أنواع الجرائم بوسائل فعالة تتلاءم وخطورتها[1]، وبالنظر لطبيعة هذه الجرائم، خصها المشرع بمجموعة شروط شكلية يمكن إجمالها فيما يلي:

1- الإذن باعتراض المراسلات وتسجيل الأصوات والتقاط الصور: لم يتطلب المشرع الجزائري في الإذن الصادر بإجراء هذه العمليات شكلا معينا، وإن كان قد اشترط أن يكون مكتوبا ومتضمنا كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سكنية كانت أو غيرها، والجريمة التي تبرر اللجوء إلى هذه التدابير مع الإشارة إلى مدة إنجاز هذه العمليات على أن يكون أقصاها أربعة أشهر قابلة للتجديد حسب ما تضمنته المادة 65 مكرر 7 ق.إ.ج.

والملاحظ على هذه المادة أنها قصرت الإذن على تدبير اعتراض المراسلات المطلوب التقاطها دون التسجيل الصوتي أو السمعي البصري، إضافة إلى أن المشرع الجزائري لم يراع العامل الزمني، فلم يحدد عدد مرات قابلية هذا الإذن إلى التجديد، كما لم ينص صراحة على ما إذا كان يجوز لقاضي التحقيق الذي أذن بهذه العمليات توقيفها قبل الموعد المحدد في الإذن، كما لم يشترط فيها تسبيبا للإذن من قاضي التحقيق، مما يضعف معه أوجه الدفاع تجاه هذا الإذن، بالإضافة إلى أن المشرع في هذه المادة لم يشترط أن يكون الإذن مسبوقا بطلبات النيابة، كما لم يشر إلى إمكانية إخطار وكيل الجمهورية به، ولم يرتب أي جزاء على مخالفة أحكام هذه المادة، رغم أن المادة بدأت فقرتها بعبارة يجب التي تفيد الإلزام، ولعل أهم ملاحظة تستدعي الانتباه والتوقف عندها هي، إذا كان المشرع في كل مرة يستعمل مصطلح الأمر عندما يتعلق الأمر باتخاذ إجراء من إجراءات التحقيق، إلا أنه في إجراءات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور نلاحظ بأنه أستبدل مصطلح الأمر بالإذن.

2- إجراء عمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور: يعطي الحق لحامل الإذن المكتوب المسلم لضابط الشرطة القضائية المنتدب من قاضي التحقيق لتولي تدابير اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، الاستعانة بأهل الخبرة، إذ له أن يسخر لأداء مهامه خاصة عند اعتراض المراسلات كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعملية حسب المادة 65 مكرر 5 ق.إ.ج.

ولكن ما لم يشر إليه المشرع في النصوص المنظمة لهذه التدابير، على من يقتصر الإطلاع على التسجيلات المتحصل عليها من إجراء هذه العمليات، على سبيل المثال بإمكان الفنيين المسخرين من ضابط الشرطة القضائية المنتدب الإطلاع على التسجيلات الصوتية أو السمعية البصرية والمراسلات التي تم تسجيلها أم أن هذا الأمر يقتصر على قاضي التحقيق وضابط الشرطة القضائية المنتدب لإجراء العمليات فقط، على أن يقتصر دور من تم تسخيرهم من فنيين على إنجاح الترتيبات التقنية والفنية والضبط دون الإطلاع، هذا ويخول الإذن كذلك لضابط الشرطة القضائية المنتدب لإجراء عمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور الحق في وضع الترتيبات التقنية اللازمة دون انتظار موافقة من سيكون محلا لها وفق المادة 65 مكرر 05 ق.إ.ج.

والمشرع الجزائري في المادة 65 مكرر 6 ق.إ.ج، لم يقيد في هذه العمليات كلها قاضي التحقيق أو الضابط المنتدب لإجراء هذه العمليات إلا باتخاذ الإجراءات اللازمة لضمان عدم المساس بالسر المهني، فالمشرع الجزائري أطلق العنان لمنفذ إذن قاضي التحقيق، لاعتراض المراسلات وتسجيل الأصوات والتقاط الصور، فبخلاف القيد المقرر في المادة 65 مكرر6 المذكورة أعلاه فإن

[1] سمير الأمين، المرجع السابق، ص23.

كل الوسائل تصبح مشروعة لبلوغ الهدف، فالحريات الفردية وحرمات الأمكنة وحرية الاتصال وحرمة الحياة الخاصة كمبادئ دستورية تصبح بدون معنى أمام هذا الإذن بمجرد تسبيبه بعبارة لقد اقتضى التحقيق.

من هنا، نرى أنه كان على المشرع –على الأقل تفاديا للتعسف في استعمال السلطة– أن يرتب بعض الجزاءات عند مخالفة بعض أحكام المواد المنظمة لهذه العمليات، فالواقع أثبت أن قاضي التحقيق ما هو إلا إنسان يتصرف بمفرده وهو دوما معرض للخطأ ينبغي على المشرع أن يضع نصوصا تكون ضابطا لتصرفاته، ولا يترك له مطلق الحرية في التصرف دون رقيب أو حسيب.

3– محضر اعتراض المراسلات وتسجيل الأصوات والتقاط الصور: إن طبيعة عمليات الاعتراض والتسجيل والالتقاط لا يتم انتظار بلوغ مرحلتها النهائية لتحرير محضر بشأنها، فقاضي التحقيق بحكم مراقبته المباشرة للعمليات وضابط الشرطة القضائية المنتدب لإجراء العمليات عليهما بتحرير محاضر عن كل مرحلة على حدى، إذ يحرر بشكل منفصل محضر الترتيبات التقنية ومحضر الدخول إلى المساكن ومحضر الالتقاط ومحضر التثبيت ومحضر التسجيل الصوتي أو محضر التسجيل السمعي البصري ومحضر عملية الاعتراض ومحضر تسجيل المراسلات[1].

ويشمل كل محضر من هذه المحاضر حسب المادة 65 مكرر9 ق.إ.ج؛ على تاريخ وساعة بداية العملية وكذا تاريخ وساعة الانتهاء منها، أما المادة 65 مكرر 10 فأكدت على ضرورة أن يرفق ملف الدعوى محضرا يتضمن وصفا أو نسخة من المراسلات والصور أو المحادثات المفيدة في إظهار الحقيقة وعند الاقتضاء إذا كانت المكالمات التي تم اعتراضها والتسجيلات الصوتية أو السمعية البصرية بلغة أجنبية تتم ترجمتها بمساعدة مترجم يتم تسخيره لهذا الغرض.

ولكن ما تجدر إليه الإشارة في إعداد محاضر هذه العمليات أن المشرع لم يحل، سواء في المادة 65 مكرر9 أو 65 مكرر10 سالفتي الذكر على المادتين 94 و95 من نفس القانون المتعلقتين بالشروط الواجب توفرها في المحضر، وحتى عندما تعرض للاستعانة بمترجم لم يحل على أحكام المادتين 91 و92 ق.إ.ج المتعلقتين باستدعاء مترجم، خاصة وأن المادة 65 مكرر 02/10 السالفة الذكر لم تشير إلى وجوب تحليف المترجم اليمين إذا لم يسبق له أداؤه.

هذا وما لم يبينه المشرع الجزائري في النصوص المنظمة لهذه التدابير هو كيفية حفظ التسجيلات والنسخ والصور التي ترفق بالملف، هل يتم وضعها في أحراز مغلقة ومختومة بختم قاضي التحقيق كما هو الشأن عند حجز الأشياء في الحالات العادية، أم أنها تترك بدون حماية وهو ما قد يعرضها لإمكانية التلاعب بها، وعليه نقول بأنه كان الأجدر على المشرع حسب رأينا وبالنظر لخطورة ما يتم تسجيله أثناء هذه العمليات إحاطتها بحماية شبيهة بتلك المعمول بها عند إجراء الحجز في الحالات العادية، فضلا على ذلك لم يحدد المشرع المصير النهائي لهذه التسجيلات والنسخ والصور التي ترفق بالمحاضر، هل يتم الحفاظ عليها أو إتلافها عند انتهاء الغرض الذي أعدت من أجله.

ثانيا: الشروط الموضوعية لاعتراض المراسلات وتسجيل الأصوات والتقاط الصور، كقاعدة عامة لا يجوز اعتراض المراسلات واستراق الأصوات وتسجيلها والتقاط الصور غفلة دون موافقة وعلم مسبق ممن يكون محلا لها، غير أن مصلحة التحقيق

[1] Jacques Georgel, Les libertés de communication : contrôle d'identité, écoute téléphonique vidéosurveillance, Dalloz, Paris, 1996, pp85-86.

وضروراته قد تستلزم القيام بمثل هذه العمليات عندما يتعلق الأمر بالجرائم التي عددتها الفقرة الأولى من المادة 65 مكرر 5 ق.إ.ج أين تكون هذه المصلحة أولى بالرعاية من الحفاظ على أسرار الحياة الخاصة.

1- السلطة المخول لها إجراء هذه العمليات: حتى وإن كان قاضي التحقيق لا يقوم باعتراض المراسلات وتسجيل الأصوات والتقاط الصور بنفسه، إلا أن ذلك يتم تحت مراقبته المباشرة، فمثل هذه العمليات تقتضي في كثير من الأحيان اللجوء إلى تقنيات لا يتحكم فيها هذا القاضي، لذا يتكفل بها أهل الخبرة في الميدان ويقتصر دور قاضي التحقيق على السهر على أن تتم في إطارها الشرعي وحسب مقتضيات القانون.

بالنظر لحداثة مثل هذه الإجراءات في قانون الإجراءات الجزائية الجزائري، فإننا نقول إنطلاقا من المادة 65 مكرر 5 ق.إ.ج أن المراقبة المباشرة لهذه العمليات ينبغي أن تبقى حكرا على قاضي التحقيق لخطورتها وتعلقها مباشرة بالحريات والحق في الخصوصية التي حماها الدستور[1]، فلا مجال لتركها بين أيدي ضباط الشرطة القضائية تنفيذا وإشرافا، لأن ميولات الشرطي بصفة عامة معروفة بتوجهها نحو البحث عن أدلة الإثبات أكثر من البحث عن أدلة النفي، وهو ما قد يترتب عليه تجاوزات تكون ضحيتها الأولى الحريات والحرمات الخاصة، وعليه فحسب رأينا ينبغي ألا يمس الانتداب في إطار الإنابة القضائية عملية المراقبة المباشرة لهذه العمليات.

وتجدر الإشارة إلى أن قانون الإجراءات الجزائية لم يضع قيودا زمنية ولا مكانية لإجراء عمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، بحيث أجاز إجراءها في كل ساعة من ساعات النهار والليل، وفي كل مكان عام أو خاص، وكاستثناء عن القاعدة، القيد الوحيد الذي نص عليه صراحة هو المتعلق باتخاذ الإجراءات اللازمة لضمان احترام كتمان سر المهنة، ويتفرع عنه احترام سرية المراسلات والمحادثات الهاتفية بين المحامي وموكله مثلا[2].

وفي حالة خروج الملزم بكتمان السر المهني عن دوره ورسالته وأضحى فاعلا مع المتهم أو شريكا له بالجرائم المنصوص عليها في المادة 65 مكرر 01/05 ق.إ.ج، فذلك يحول دون تمكنه من التحصن بغطاء سر المهنة، لأن المشرع إنما حصن احترام سر المهنة وليس القائم بها، فضلا عن هذا القيد المنصوص عليه صراحة، هناك قيد آخر ولو لم يشر إليه المشرع، فإن مقر السفارات والقنصليات الأجنبية تستثني من الأمكنة التي يمكن أن تخضع لهذه العمليات.

2- عدم مسؤولية القائم أو المشرف على هذه العمليات: إن الاعتداء على الحياة الخاصة بتسجيل أصوات الأشخاص والتقاط صور لهم خلسة ودخول مساكنهم دون رضاهم، في كل ساعة من ساعات النهار والليل بالكسر وتسلق الجدران وفتح الأقفال، واللجوء إلى أساليب الخداع وافشاء السر المهني، كلها جرائم لا يتحمل القائمون بها المسؤولية الجنائية بسببها إذا ما تمت أثناء أدائهم لعمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور بموجب إذن من قاضي التحقيق في إطار تحقيق قضائي يتعلق بالجرائم التي عددتها المادة 65 مكرر 1/5 ق.إ.ج.

---

[1] حسب ما تقضيه الفقرة الثانية من المادة 32 من الدستور الجزائري بأن سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة.

[2] Jean Larguier, La procédure pénale, Dalloz, Paris, 17ème Ed., 1999, p151. Georges Levasseur Droit pénal général et procédure pénale, Sirey, 1999, p226. Corinne Renault-Brahinsky Procédure pénale, Gualino Editeur, Paris, 7ème Ed., 2006, p186.

3- ضرورة التحقيق تبيح المحظورات نتيجة خطورة الجرائم محل التحقيق: إن وقوع جريمة من الجرائم التي عددتها الفقرة الأولى من المادة 65 مكرر 5 ق.إ.ج وحده لا يعد مبررا كافيا للجوء قاضي التحقيق لاعتراض مراسلات وتسجيل أصوات والتقاط صور من كان محلا للمتابعة بسببها، بل يجب فضلا عن ذلك أن تقتضي مصلحة التحقيق ذلك، بأن يكون الإذن بها له فائدة في إظهار الحقيقة، فضلا عن ذلك يقتضي اللجوء لهذا النوع من العمليات وجود دلائل قوية على وقوع الجريمة ونسبتها إلى المتهم بأن تشير أصابع الاتهام بدلائلها الجدية والكافية على شخص أو أشخاص هم من ارتكبوها أو لديهم معلومات بشأنها تفيد في إظهار الحقيقة أو بحوزتهم أشياء تتعلق بها، وفي جميع الأحوال مسألة تقدير ضرورة اللجوء إلى هذه العمليات من عدمه، هي دائما متروكة لتقدير قاضي التحقيق حسب ما تضمنته المادة 65 مكرر 5 ق.إ.ج.

أما فيما يتعلق بالجرائم التي تكتشف عرضا أثناء تدابير اعتراض المراسلات وتسجيل الأصوات والتقاط الصور فإن الأصل ينصب على الجريمة التي تبرر اللجوء إلى هذه التدابير، وعلى الأشخاص الذين تضمن الإذن الإشارة إليهم دون غيرهم، غير أن هذه التدابير لها ميزة خاصة، وبالخصوص عملية اعتراض المراسلات السلكية واللاسلكية، بحيث لا يقتصر الاعتراض على ما يصدر عن المتهم من إشارات وأصوات أو حركات، وإنما يتعداه إلى الأطراف الأخرى التي اتصلت به، مما يعني في مثل هذه الوضعية تعارض مصلحتين، مصلحة التحقيق في إظهار الحقيقة عن طريق كشف اتصالات المتهم، ومصلحة الغير الذي ينبغي أن يحافظ له على سرية محادثته[1]، في مثل هذا الوضع أولى المشرع الجزائري عناية بمصلحة التحقيق والمصلحة العامة على مصلحة الغير، وما يدل على ذلك ما جاء في الفقرة الثانية من المادة 65 مكرر 6 ق.إ.ج، التي قضت بأنه: "إذا اكتشفت جرائم أخرى غير تلك التي ورد ذكرها في إذن القاضي، فإن ذلك لا يكون سببا لبطلان الإجراءات العارضة"، بمعنى أن الجرائم الجديدة التي تم اكتشافها عرضا وغير المعنية بالإذن يمكن إخطار وكيل الجمهورية المختص بها ليتخذ ما يراه بشأنها.

الفرع الثالث: مراقبة الاتصالات الإلكترونية

أفرز التقدم العلمي والتكنولوجي لاسيما في مجال الاتصال أساليب عالية الكفاءة أحدثت أشكالا جديدة من الإجرام وثورة في قانون الإجراءات الجزائية ووسائل الإثبات التقليدية التي لم تعد كافية لمواكبة هذا التطور، وعليه أصبح لا بد من استخدام وسائل تقنية حديثة، وهذا ما قام به المشرع الجزائري بموجب التعديل الجديد لقانون الإجراءات الجزائية وذلك باستحداثه لأساليب تحري خاصة في مجال البحث والتحري عن الجرائم، وكذا القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

فقد وضع المشرع الجزائري طبقا لنص المادة 03 من القانون 09-04[2]، بين أيدي الجهات المختصة بمكافحة جرائم التكنولوجيا الحديثة وسيلة قانونية جديدة من خلال وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في

---

[1] حسن صادق المرصفاوي، المرصفاوي في المحقق الجنائي، منشأة المعارف، الإسكندرية، 1990، ص67.

[2] تنص المادة 03 على أنه: "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية، ووفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية".

حينها وهو ما أطلق عليه مصطلح مراقبة الاتصالات الإلكترونية في عنونة الفصل الثاني من ذات القانون، وهنا يجدر القول إلى أن المشرع الجزائري تأرجح بين إقراره لحماية الاتصالات بكافة أشكالها سواء كانت تقليدية أو إلكترونية إلا أنه أباح مراقبتها.

البند الأول: حضر مراقبة الاتصالات الإلكترونية

قبل التطرق إلى النصوص التي جاء بها المشرع الجزائري التي بموجبها منع مراقبة الاتصالات الإلكترونية وأقر حماية خاصة للحياة الخاصة، يجدر بنا تحديد المقصود بمراقبة الاتصالات الإلكترونية.

أولا: تعريف مراقبة الاتصالات الإلكترونية، لم يتطرق المشرع الجزائري إلى تحديد المقصود بمراقبة الاتصالات الإلكترونية وإنما اكتفى بتحديد مفهوم الاتصالات الإلكترونية، فعرفها بموجب الفقرة و من المادة 02 من القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على أنها: "أي تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية"، وتم التطرق إلى تعريف الاتصالات الإلكترونية كذلك بموجب المادة 10 من القانون المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية بأنها: "كل إرسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها، عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية".

ثانيا: حضر مراقبة الاتصالات الإلكترونية في التشريع الجزائري، جاءت النصوص التشريعية والتطبيقات القضائية بما يؤكد الحماية.

1- حضر مراقبة الاتصالات الإلكترونية في الدستور الجزائري، بموجب التعديل الجديد للدستور الجزائري نلاحظ أنه كان أكثر وضوحا وتوسعا في مجال حماية حقوق وحريات الأشخاص في الفصل الرابع منه تحت عنوان الحقوق والحريات، كما أنه قام بتعديل المادة 39 بالمادة 46، والتي جاء فيها: "لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ويحميها القانون، سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة، لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية ويعاقب القانون على انتهاك هذا الحكم، حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه"

نلاحظ أنه تطرق في الفقرة الثالثة إلى الاستثناء الذي يجعل من المساس بسرية المراسلات والاتصالات الخاصة أمرا مشروعا ألا وهو أمر معلل من السلطة القضائية، وهذا حتى تتوافق نصوصه مع ما جاء به كل من قانون الإجراءات الجزائية وكذا القانون رقم 09-04، من إباحة مراقبة الاتصالات والمراسلات بشروط، وبالمقابل يجعل من أحكام هذين القانونين أحكاما دستورية؛ ثم يرجع ويؤكد على الحماية في حالة انتهاك هذا الحكم، كما لو يتم الاعتداء على سرية المراسلات والاتصالات الخاصة دون أمر معلل من السلطة القضائية مما يعرض صاحبه إلى العقاب الذي يقره القانون، كما أقر حماية الحياة الخاصة للأشخاص بكافة أشكالها بما فيها المراسلات والاتصالات لأنها تتميز بطابع السرية، وهذا في إطار المعالجة الآلية للمعطيات، أي باستخدام التقنيات الحديثة، ويتزامن هذا مع السياسية التي تنتهجها الجزائر في عصرنة كافة القطاعات، مما يجعل من حقوق الأشخاص ذات الطابع الشخصي أكثر عرضة للانتهاك.

2- حضر مراقبة الاتصالات الإلكترونية في قانون العقوبات الجزائري، تبني المشرع الجزائري نصا نوعيا يحمي حرمة الحياة الخاصة بما فيها سرية المراسلات بموجب تعديل قانون العقوبات.

فلقد جاء في المادة 303 مكرر على أنه يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 50.000 دج إلى 300.000 دج، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت وذلك،

- التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.
- التقاط أو تسجيل أو نقل صورة من مكان خاص بدون إذنه أو رضاه

كما أقر المشرع عقوبة في حالة نشر هذه التسجيلات أو الصور المتحصل عليها، حيث جاء في المادة 303 مكرر 1 "...كل من احتفظ، أو وضع، أو سمح بوضع في متناول الجمهور أو الغير، أو استخدام بأية وسيلة كانت التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة 303 مكرر".

وتجدر الإشارة في هذا الإطار أن هناك اتجاه من الفقه يرى أن المادة 303 مكرر تخص المحادثات الخاصة، أو التي تتم في مكان خاص، دون المحادثات التي تتم عن طريق الوسائل الإلكترونية أو التي تتخذ شكل البريد الإلكتروني[1]، إلا أننا لا يمكننا القول بهذا الاتجاه لأن المشرع لم يحدد وسيلة نقل المحادثات أو تسجيلها إن كانت بخط تليفوني أو غير ذلك بصريح العبارة، وإنما أقر أيضا حماية المراسلات التي تتم عن طريق الوسائل الإلكترونية، وذلك باستعماله مصطلح بأي طريقة تقنية كانت، ومعنى ذلك أن الاتصالات الإلكترونية تشمل كافة الطرق سواء كانت اتصالات سلكية أو خلوية (الهاتف النقال، الفاكس، البريد الإلكتروني، مواقع الدردشة على الإنترنت كفيسبوك، سكايب، وحتى المنتديات...إلخ).

البند الثاني: مشروعية مراقبة الاتصالات الإلكترونية

رأينا سابقا أن المشرع الجزائري أقر حماية قانونية لسرية المراسلات بكل أشكالها باعتبارها صورة من صور الحياة الخاصة لكنه مع ذلك أباح مراقبة الاتصالات الإلكترونية إذا اقتضت ضرورة التحري ذلك، وهذا مع عدم المساس ببعض الضمانات القانونية.

أولا: إقرار المراقبة الإلكترونية، استحدث المشرع الجزائري نصوصا قانونية تتضمن مصطلحات تحمل مفاهيم تقنية تتناسب مع ضبط الرسائل الإلكترونية، في حالة التلبس، أو التحقيق الابتدائي بصدد عدد من الجرائم منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، التي تتميز عن النصوص التقليدية في كونها تضمنت جوانب تقنية تسمح بمقتضاها لقاضي التحقيق، أو ضابط الشرطة القضائية المناب أو المأذون له باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، فقد نصت المادة الثالثة من القانون رقم 09-04 سالف الذكر على أنه: "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية".

---

[1] رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية للمعطيات في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، بيروت، ط1، 2012 ص372.

ونشير إلى أن المشرع الجزائري وإن أباح مراقبة الاتصالات الإلكترونية في خمس جرائم فقط محددة على سبيل الحصر وفقا للمادة 65 مكرر 5، إلا أنه رجع في نص المادة 03 من القانون رقم 09-04 وجعلها في حالات محددة وهي: في حالة حماية النظام العام، أو لمستلزمات التحريات، أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وكذا القانون رقم 09-04 هذا مع عدم المساس بجملة من الضمانات.

كما جاء في المادة 04 من القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، أنه يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 03 من ذات القانون في الحالات الآتية:

– الوقاية من الأفعال الموصوفة بجرائم الإرهاب، أو التخريب، أو الجرائم الماسة بأمن الدولة، يفهم هنا أن المشرع أجاز المراقبة المسبقة للاتصالات الإلكترونية، أي قبل ارتكاب الجريمة فالوقاية هنا تسبق عملية البدء في التنفيذ وتسبق حتى عملية التحضير للجريمة، وعليه فبمجرد توافر شكوك ولو بسيطة أن هناك احتمال قيام شخص أو مجموعة من الأشخاص بالتحضير لإحدى الجرائم سالفة الذكر، يجعل مراقبة اتصالاتهم الإلكترونية من قبل السلطة المختصة فعلا مشروعا.

ومع هذا يمكننا القول إنه إجراء وقائي أقره المشرع للوقاية من جرائم محددة على سبيل الحصر لما تتسم به من خطورة بالغة على الدولة، كما يمكن أن يصل مداها إلى المجتمع الدولي ككل.

– في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام، أو الدفاع الوطني، أو مؤسسات الدولة، أو الاقتصاد الوطني، نشير إلى أن المشرع أجاز المراقبة المسبقة للاتصالات الإلكترونية حماية لمجموعة من المصالح والهيئات، وعليه فهذا الإجراء هو الآخر إجراء وقائي، لأنه بمجرد توافر معلومات عن احتمال اعتداء على منظومة معلوماتية تمس بالمصالح السابقة، يجعل من إجراء الرقابة الإلكترونية فعلا مشروعا ويستوي أن تتوفر هذه المعلومات من قبل السلطات ذاتها، أو من قبل البلاغات والشكاوى التي ترد إليها من قبل المواطنين، المهم أن تنبئ هذه المعلومات عن احتمال اعتداء على هذه المصالح والهيئات سالفة الذكر، ونشير إلى أن المشرع لم يكتف هنا بمجرد الشك وإنما اشترط أن تتوفر معلومات عن احتمال اعتداء على منظومة معلوماتية تمس بهذه الهيئات والمصالح.

ويعتبر هذا النوع من الجرائم من أخطر الجرائم على الإطلاق، خاصة مع السياسة التي اعتمدت عليها البلاد في عصرنة كافة القطاعات، وذلك بالاعتماد المتزايد على أنظمة المعلومات فحساسية هذه القطاعات كالدفاع الوطني تستوجب المراقبة السابقة لما لها من تأثير على كيان الدولة ككل في حالة المساس بها.

– لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية، لا يعتبر هذا الإجراء وقائيا فحسب وإنما هو إجراء قضائي، لأنه يتم في مرحلة البحث والتقصي عن الدليل وليس في مرحلة ما قبل الشروع في الجريمة كما جاء سابقا، ونشير إلى أن اللجوء إلى مراقبة الاتصالات الإلكترونية هنا لا ينحصر على تلك الجرائم المحددة سابقا، وإنما يتعداها إلى كافة جرائم القانون العام، بشرط أن تكون هناك صعوبة في الحصول على نتيجة تهم الأبحاث دون اللجوء إلى المراقبة الإلكترونية.

– في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة، يدخل في هذا في الإطار التعاون الدولي للحد من الجرائم العابرة للحدود كما هو الشأن بالنسبة للجرائم المتصلة بتكنولوجيات الإعلام والاتصال، دون المساس بالاتفاقيات الدولية ومبدأ المعاملة بالمثل.

ثانيا: إجراءات تنفيذ مراقبة الاتصالات الإلكترونية، تتم مراقبة الاتصالات الإلكترونية باتخاذ الإجراءات التالية:

– **سرية الإجراءات**، تتم العملية بسرية تامة في مواجهة الأشخاص بدون علمهم ودون رضاهم، كما أنها تتم بسرية في مواجهة الكافة احتراما لمبدأ السر المهني المقرر في المادة 45 ق.إ.ج.

– **التسخير**، يجوز لوكيل الجمهورية، أو لقاضي التحقيق، أو لضابط الشرطة القضائية أن يسخر عونا مؤهلا لدى هيئة مكلفة بالاتصالات سواء كانت عامة أو خاصة للقيام بهذا الإجراء.

– **المحاضر**، يحرر المكلف بالعملية محضرا يحوي العناصر الأساسية للعملية؛ التاريخ، ساعة بداية ونهاية الإجراء، نسخ المراسلات أو الصور، تحميل البيانات المفيدة للتحقيق...إلخ، ويودع المحضر لدى الجهة القضائية المكلفة، بمعنى أمام وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق.

– **حماية المعطيات المتحصل عليها**، حيث أنه جاء في المادة التاسعة من القانون رقم 09-04 أنه لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية.

– **الإذن**: أشار المشرع الجزائري في المادة 04 من القانون رقم 09-04 على أنه يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها إذنا لمدة ستة أشهر قابلة للتجديد، وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

وما نلاحظه هو تقارب كبير بين الإجراءات المنصوص عليها في المادة 65 مكرر 5 ق.إ.ج وما تم النص عليه في المادة 04 من القانون 09-04، فإجراء المراقبة الإلكترونية هو أحد وسائل اعتراض المراسلات وتسجيل الأصوات والتقاط الصور جاءت صياغة الفقرة أ من المادة 04 من القانون رقم 09-04 بالشكل الآتي "...للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة..."، على عكس المادة 65 مكرر 05 ق.إ.ج والتي ذكرت الجرائم دون استعمال عبارة الوقاية وكذلك الحال بالنسبة لبقية فقرات المادة 04 من القانون رقم 09-04.

بناء على ما سبق يمكنا القول إن الإذن الممنوح في الحالات الثانية والثالثة والرابعة من المادة 04 من القانون 09-04 هي حالات تتعلق بجرائم ارتكبت أو على وشك الوقوع، وهو بذلك يخضع لأحكام المادة 65 مكرر 05 وما يليها ق.إ.ج طبقا لنص المادة 03 من القانون رقم 09-04، وأن الإذن الممنوح من قبل النائب العام لدى مجلس قضاء العاصمة هو استثناء يكون في حالة الوقاية من الجرائم المذكورة في الفقرة أ، وبالتالي وفي حال وقعت تلك الجرائم، فإن الإذن يختص بإصداره وكيل الجمهورية بعد مطالبة النائب العام لدى القطب الجزائي المتخصص بالإجراءات، وأن مدته تخضع لأحكام المادة 65 مكرر 05 وما يليها.

بما أن الإذن في هذا الشأن يمنح من قبل النائب العام لدى مجلس قضاء الجزائر العاصمة، فإن الجهة التي تتحصل على هذا الإذن يكون لها اختصاص على كافة الإقليم الوطني، وهم ضباط الشرطة التابعين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

– **مسائلة ضباط الشرطة القضائية في حالة مساسهم بالحرية الشخصية للفرد:** جاء في نص المادة 107 ق.ع على أنه: "يعاقب الموظف العمومي بالسجن المؤقت من خمس سنوات إلى عشر سنوات إذا أمر بعمل تحكمي أو ماس بالحرية الشخصية للفرد أو بالحقوق الوطنية لمواطن أو أكثر"، ونشير هنا إلى أن ضابط الشرطة القضائية ملزم بالإجراءات التي وضعها القانون حماية لحقوق الأفراد وحرياتهم الشخصية، كما أنه ملزم بالتقيد بالإذن المقدم له سواء من قبل قاضي التحقيق أو وكيل الجمهورية.

– **خضوعها لسلطة القضاء:** يعتبر خضوع مراقبة الاتصالات الإلكترونية لسلطة القضاء المشار إليها سابقا ضمانة الضمانات، وذلك لأنها تقع تحت إشراف رقابة القضاء، مما لا يدع مجالا للقول بمساس الضبطية القضائية بحقوق الأفراد.

المبحث الثاني: حجية الدليل الرقمي في إثبات جرائم التكنولوجيا الحديثة

دعت الثورة التكنولوجية الجديدة التي نعيشها في عصرنا الحالي الحاجة الماسة إلى تطوير نظم المعلومات في جميع قطاعات الحياة، بما يساير التطورات التكنولوجية والاجتماعية والاقتصادية التي تتزايد يوما بعد يوم، وذلك لأجل الاستفادة من الآثار الإيجابية لهذه الثورة، خاصة وأن العالم يشهد المزيد من التطور في نظم المعلومات بعد إن اتصلت هذه النظم بالأقمار الصناعية ودخوله عصرا جديدا سمي بعصر الإلكترونيات.

وقد تمكن الإنسان عن طريق الوسائل الإلكترونية المستحدثة من ارتكاب العديد من الجرائم ضد الأشخاص والأموال وضد الأسرار الاقتصادية والسياسية والعسكرية للدولة، ومما يزيد من خطورة هذا النوع الجديد من الجرائم أنها قد تتعدى حدود المكان ويصعب بالنسبة لها حساب الزمان، كما وأن محلها قد يتعدى القيم المادية ليكون قيمة معنوية لا تلمسها الأيدي ولا تبصرها الأعين كالبرامج الخاصة بالحاسب الآلي والبيانات المخزنة، لذلك ليس بمستغرب أن يستفيد المجرم من التكنولوجيا الحديثة في الاتصالات في المزيد من التنصت والتلصص على الحياة الخاصة لبني جنسه باستخدام الوسائل الإلكترونية الدقيقة، والتي عن طريقها قد تكون حياتهم الخاصة وأسرارهم المالية بدون حجاب، فالسمة الرئيسة التي تتميز بها التكنولوجيا الحديثة للمعلومات أنها تعتمد على تحويل البيانات أو المعطيات وهي غير ملموسة من شكل إلى آخر، وذلك إما عن طريق معالجتها بواسطة الوسائل الإلكترونية أو بنقلها من مكان إلى آخر، من شخص إلى آخر[1].

والتطور الهائل الذي لحق شبكة الإنترنت وانتشار مختلف الأجهزة الإلكترونية، قد تسبب في تهديد الحريات الفردية بخطر الاعتداء عليها، وهو ما يتطلب إيجاد الوسيلة المناسبة للرقابة عليها لتجنب هذا الخطر في الوقت المناسب، فالتطور الحالي الذي انعكس أثره على قانون العقوبات، قد انعكس أثره أيضا على قانون الإجراءات الجنائية، لإن هذا القانون الأخير قد لا يطبق بسبب عجز القانون الأول عن استيعاب الجرائم المستحدثة التي ترتكب بالوسائل الإلكترونية، كما وأن الإثبات الجنائي وهو أحد الموضوعات

[1] علي محمود علي حمودة، المرجع السابق.

الهامة لهذا القانون قد تأثر بدوره بالتطور الهائل الذي لحق بالأدلة الجنائية بسبب تطور طرق ارتكاب الجريمة، الأمر الذي يتعين معه تغير النظرة إلى طرق الإثبات الجنائية لكي تقترب الحقيقة العلمية في واقعها الحالي من الحقيقة القضائية.

ومما يزيد من خطورة هذا الأمر أن النصوص العقابية المطبقة لا تكفي لحماية حرمة الحياة الخاصة من الاعتداء عليها باستخدام الوسائل الإلكترونية المستحدثة، باعتبار أن هذا الاعتداء لا يعاقب عليه قانون العقوبات إلا إذا كان مرتبطا بمكان خاص أما تخزين المعلومات عن الأفراد وتسجيلها في هذه الوسائل فإنه لا يخضع للتأثيم وفقا للقواعد العامة، وعليه قد يتم الاعتماد على الوسائل العلمية المستحدثة في الإثبات الجنائي، ومن ذلك مشروعية التنصت الهاتفي والتسجيل الصوتي، والتقاط الصور والتصوير المرئي، ومدى قبول الدليل المستمد منهم في تكوين عقيدة القاضي، فمن المستقر عليه أن القاضي الجنائي أن يكون عقيدته من أي عنصر مشروع من عناصر الدعوى، وتلك القاعدة لا استثناء عليها وتمثل أصلا من أصول المحاكمات الجنائية بصفة عامة، فمشروعية الدليل ضمانا للحريات العامة ولا يقبل أن يحتج بدليل غير مشروع حتى وإن كان يتفق مع الحقيقة.

من ذلك طرح التقدم العلمي والتكنولوجي تحديات كبيرة، كما أثار تساؤلات مهمة في نطاق القانون الجنائي بشقيه الموضوعي حول مدى قابلية نص التجريم للتطبيق –دون إخلال بمبدأ الشرعية– والإجرائي حول إمكانية الاستناد دائما إلى مبدأ حرية الإثبات لقبول أي دليل يستند إلى اكتشاف علمي أو تقني مستحدث[1]؛ وعلى ذلك فنظرية الإثبات هي المحور الذي تدور حوله قواعد الإجراءات الجنائية من لحظة وقوع الجريمة إلى غاية إصدار الحكم النهائي بشأنها، هذا الحكم يكون نتيجة العملية المنطقية التي يمارسها القاضي الجنائي بناء على السلطة الممنوحة له في تقدير الأدلة التي تختلف حسب نوع نظام الإثبات الذي يتبناه المشرع.

المطلب الأول: مدى اقتناع القاضي بالدليل الرقمي

يسعى التشريع إلى تنظيم العلاقات بين الأفراد داخل المجتمع، وكذا تنظيم العلاقات بين السلطات المختلفة، ويهدف القضاء إلى الوصول إلى الحقيقة وإصدار أحكام تكون عنوانا لهذه الحقيقة، والقاضي وهو يمارس هذه المهمة عليه أن يسلك كافة السبل القانونية في عملية الإثبات من خلال جمع الأدلة اللازمة لإظهار الحقيقة، ثم عليه أن يستخلص من تلك الأدلة ما يحقق له القناعة اللازمة من كونها كافية أو غير كافية لنسبة الفعل الإجرامي إلى المتهم.

يتمتع القاضي الجنائي إذن بقدرة كبيرة من السلطة التقديرية ومتسعا من الحرية ليستطيع أن يمارس دورا إيجابيا للوصول إلى هذه الحقيقة، وهذا هو ما استقرت عليه معظم التشريعات الجنائية فمنحت قاضي الموضوع الحرية في الاقتناع بالأدلة وتكوين عقيدته منها، وأصبحت هذه القاعدة هي المبدأ الذي يحكم عمله، كون هذه الأدلة هي المحور الأساسي في عملية الاثبات الجنائي.

الفرع الأول: سلطة القاضي في تقدير الأدلة الإلكترونية

يحكم سلطة القاضي في تقدير الأدلة المطروحة أمامه مبدأ الحرية في تكوين عقيدته، ولكي نصل إلى ماهية مبدأ الاقتناع الشخصي للقاضي لابد قبل ذلك أن نعرف ماهية الإثبات الجنائي، وذلك لأنه متصل اتصالا وثيقا بأي عمل قضائي في سبيل

[1] Coralie Ambroise-Castérot, Recherche et administration des preuves en procédure pénale, la quête du Graal de la Vérité, Actualité Juridique Pénal, Dalloz, Paris, 2005, p261.

إظهار الحقيقة والوصول إلى الحكم النهائي[1]، وقد جرى الفقه القانوني على القول إن الإثبات في المسائل الجنائية حر، غير أنه ليس متوقعا أن يجري هذا القول على إطلاقه، فلا يتصور في دولة القانون عدم إخضاع الدليل للقانون؛ لذا لابد أن تتسق حرية الإثبات مع مشروعية الدليل الجنائي المتحصل من الاستعانة بالوسائل العلمية[2].

البند الأول: الإثبات الجنائي

يقصد بالإثبات الجنائي، إثبات الوقائع؛ أي إقامة الدليل على وقوع الجريمة ونسبتها إلى المتهم[3]، وهو ما يعني أن الإثبات في المسائل الجنائية يهدف إلى كل ما يؤدي إلى إظهار الحقيقة، وكلمة الإثبات تعني أن يتذرع بها أطراف الرابطة الإجرائية للوصول إلى الدليل بالمعاينة أو الخبرة أو الكتابة أو الشهادة أو القرائن، مما يعني أن الإثبات هو مجموع الأسباب المنتجة لليقين، أي النتيجة التي تحققت باستعمال وسائل الإثبات المختلفة أي إنتاج الدليل[4].

يتمتع القاضي الجنائي في نظام الإثبات الجنائي بالحرية الكاملة في إطار البحث عن الحقيقة وبكافة الوسائل الممكنة بشرط مشروعية تلك الوسائل، فالقاضي في نظام الإثبات الحر يقوم بدور إيجابي في الدعوى الجنائية، فهو يتمتع بسلطة واسعة في قبول الأدلة وهو أهم ما يميز هذا النظام القضائي، وقد ذهب جانب من الفقه[5] إلى تعريف الإثبات في المواد الجنائية بأنه: "إقامة الدليل لدى السلطات المختصة بالإجراءات الجنائية على حقيقة واقعة ذات أهمية قانونية، وذلك بالطرق التي حددها القانون، ووفق القواعد التي أخضعها لها".

كما عرف الإثبات الجنائي بأنه الوصول بالدليل المقدم في الدعوى الجنائية في مراحلها المختلفة سواء بالنفي أو الإثبات وبطريقة مشروعة إلى مبلغ اليقين القضائي[6]، وهو ما يعني أن الدليل في الإثبات الجنائي لا يهدف فقط إلى إثبات التهمة على الجاني ولكن يظهر أثره أيضا في دفع الاتهام عن المتهم، أي أنه يشمل أدلة الدعوى سواء في النفي أو في الثبوت وبطريقة مشروعة وأن يكون يقينيا، أي أن يكون مؤسسا على أدلة صحيحة في القانون وطرحت للمناقشة في الجلسة، ذلك أن الأصل في الإنسان البراءة فإذا كانت الواقعة غير ثابتة فإن المحكمة تحكم ببراءة المتهم[7]، إذ يقوم في نطاق الدعوى العمومية إثبات الجريمة وإسنادها لمرتكبها بحسب الأصل بطرق الإثبات كافة[8].

---

[1] عصام محمود عبد الحليم يوسف، المسؤولية الجنائية للمصابين بالأمراض العصبية والنفسية، المرجع السابق، ص326.

[2] Jean Pradel, Procédure pénale, Cujas, Paris, 10ème Ed., 2001, p681.

[3] حسن محمد ربيع، حماية حقوق الإنسان والوسائل المستحدثة للتحقيق الجنائي، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة، 1985، ص12.

[4] محمد زكي أبو عامر، المرجع السابق، ص17-24. أبو العلا علي أبو العلا النمر، الإثبات الجنائي، دراسة تحليلية لتحديد موطن القوة والضعف في الدليل الجنائي، دار النهضة العربية، القاهرة، 1991، ص05.

[5] محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات التشريعية، المرجع السابق، ص767.

[6] عبد الحافظ عبد الهادي عابد، المرجع السابق، ص65. هلالي عبد الله أحمد، النظرية العامة للإثبات في المواد الجنائية، دراسة مقارنة بين النظم الإجرائية اللاتينية والجرمانية والاشتراكية والأنجلوسكسونية والشريعة الإسلامية، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة، 1987، ص15 وما بعدها.

[7] عصام محمود عبد الحليم يوسف، المسؤولية الجنائية للمصابين بالأمراض العصبية والنفسية، المرجع السابق، ص328.

[8] Michèle-Laure Rassat, Procédure pénale, 2ème Ed., Presses Universitaires de France, 1995 p206.

وقد فتح القانون الجنائي –فيما عدا ما استلزمه من وسائل خاصة في الإثبات– بابه أمام القاضي الجنائي على مصراعيه يختار من كل طرقه ما يراه موصلا إلى الكشف عن الحقيقة ويزن قوة الإثبات المستمدة من كل عنصر مع حرية مطلقة في تقدير ما يعرض عليه ووزن قوته الثبوتية في كل حالة حسبما يستفاد من وقائع كل الأدلة وظروفها.

وهناك مجموعة مبررات يستند إليها مبدأ حرية الإثبات تجعل من الصعوبة التخلي عنه، فمن ناحية، إن مبدأ حرية الإثبات يحقق مصلحة المتهم، حيث يتيح له إمكانية الدفاع عن نفسه بالطرق كافة[1]، ومن ناحية أخرى، لا تتناسب طبيعة الوقائع الجنائية موضوع الإثبات مع إمكانية إعداد الدليل المسبق، فقد ظهر مبدآن إجرائيان في الإثبات الجنائي ميزاه عن غيره، وهما قرينة البراءة القانونية وحرية الإثبات[2].

غير أن الأهم من هذين المبررين ذلك الذي يستند إلى فاعلية العدالة الجنائية، فستفقد هذه العدالة فاعليتها وستتجرد من أسلحتها في مواجهة مجرمين يرتكبون على الأغلب جرائمهم بعيدا عن أعين السلطة العامة، ويسعون إلى استخدام جميع الوسائل الممكنة من أجل طمس ما يمكن من الأدلة التي تؤدي إلى إدانتهم، إذا انعدمت إمكانية إثبات الجرائم وإسنادها إلى مرتكبيها بجميع طرق الإثبات[3]، ولذلك ستغدو عملية مكافحة الجريمة عمليا مهمة مستحيلة إذا خضعت الأدلة لنظام صارم يحدد مسبقا الأدلة التي يمكن الأخذ بها[4]، وترتب عن كون الإثبات حر نتيجتان، أولهما؛ عدم استبعاد أدلة معينة، وثانيهما؛ عدم فرض أدلة معينة.

أولا: عدم استبعاد أي دليل، سبق القول بأن المقصود من مبدأ حرية الإثبات هو قبول كافة أنواع الأدلة التي تنطبق عليها شروط القبول بصفة عامة، وليس للقاضي أن يستبعد أي دليل مسبقا قبل فحصه ما دام أن هذا الدليل قد يساهم في إثبات الدعوى المقامة أمامه، وحظر استبعاد القاضي الجنائي للأدلة المقدمة أمامه يطال الأدلة التي يقدمها الأفراد.

وقد ذهب بعض الفقه إلى القول بعدم قبول واستبعاد اللجوء إلى ما يطلق عليه رسائل الإثبات الحديثة أو الأدلة العلمية مثل البصمة الوراثية، التسجيلات الصوتية والمرئية وأجهزة كشف الكذب[5]، وهناك أسباب لتبرير رفض القضاء والفقه للوسائل الحديثة منها، أن النتائج المترتبة عن استخدام بعضها مشكوك في دلالتها، أو أن استخدام قسم منها ينتقص من الاحترام الواجب لكيان الإنسان، فيكون مثلا لجهاز كشف الكذب أحيانا بعض النتائج الإيجابية التي قد تساعد المحققين في كشف الحقيقة أو بعضها، أو على أقل تقدير يساهم في توجيه المحققين إلى الوجهة السليمة للبحث والتنقيب عن الحقيقة، من خلال الاستجواب أو الاستماع إلى المحقق معهم، أثناء تعرضهم للفحص بواسطة هذا الجهاز[6]، إلا أن وجه الاعتراض على الجهاز هو في نتائج الجهاز ذاته فهي إلى الآن ليست محل ثقة للكثير من المتعاملين معه ونتائجه يجانبها الخطأ في كثير من الأحيان.

---

[1] معتصم خميس مشعشع، إثبات الجريمة بالأدلة العلمية، مجلة الشريعة والقانون، العدد 56، السنة 27، كلية القانون، جامعة الامارات العربية المتحدة أكتوبر 2013، ص08.

[2] Pierre Bouzat, La loyauté dans la recherche des preuves, Mélanges Hugueney, Sirey, 1964 n° 03, p157.

[3] Michèle-Laure Rassat, Op.Cit., p324. Jean Pradel, Op.Cit., p332.

[4] Roger Merle, et André Vitu, Op.Cit., p161.

[5] Michèle-Laure Rassat, Op.Cit., p327.

[6] Jean Pradel, Op.Cit., p371.

يعترض أصحاب هذا الرأي أيضا على الإثبات بواسطة ما تعارف عليه باسم التنويم المغناطيسي أو التنويم بالإيحاء، أو من خلال أدوية معينة تصل بالمتهم إلى مرحلة وسط ما بين الوعي واللاوعي فيدلي بأقوال خارج عن إرادته، وهو ما يعرف بمصل الحقيقة وذلك لما فيه من اعتداء بدني وجسدي على متهم مازال قيد التحقيق ولم تثبت عليه التهمة بعد، كما أنه من غير المقبول في المنطق القانوني الحصول على اعتراف بارتكاب جريمة من خلال إضعاف قدرات المشتبه به بواسطة حقنه بمواد مخدرة أو استعمال طرق علمية أخرى من قبل رجال السلطة العامة، ولا يغير في الأمر أن يقع استعمال هذه الطرق بموافقة المشتبه به، فلا تأثير للقبول عندما يتعلق بالتنازل عن حقوق أساسية[1]، بالإضافة إلى عدم ثقة القول بأن كل ما يمكن أن يدلي به شخص وهو تحت تأثير التخدير أو فاقدا السيطرة على تصرفاته يطابق الحقيقة، فاحتمال ألا يتطابق ما يدلي به الشخص الذي يكون في مثل هذه الحالات مع الحقيقة يبقى قائما.

فالصفة العلمية للدليل ليست هي السبب الذي يبرر استبعاده من وسائل الإثبات، حيث يتعارض حتما مثل هذا الاستبعاد مع مبدأ حرية الإثبات، وإنما السبب الرئيسي وراء استبعاد العديد من الأدلة العلمية هو عدم الثقة في النتائج التي تؤدي إليها هذه الأدلة، أي عدم الثقة في الدليل هو الذي يجيز رفض استخدامه في الإثبات، وعلى العكس من ذلك عندما يكون الدليل العلمي محل ثقة فليس ثمة ما يمنع من استخدامه وإن تضمن مساسا بحقوق الانسان الأساسية.

ثانيا: عدم فرض أدلة محددة، المقصود بمبدأ حرية الإثبات هو قبول كافة أنواع الأدلة والتي تنطبق عليها شروط القبول بصفة عامة مثل مشروعية الحصول عليها، الأمر الذي يعني حظر فرض أدلة معينة وتقييد الإثبات بهذه الأدلة، إلا أن عدم جواز فرض أدلة معينة هو منع للقاضي ولا يقيد المشرع، يحق للقاضي من خلال هذا الغرض اللجوء إلى أي دليل أو وسيلة مشروعة يراها مناسبة للوصول إلى الحقيقة، والحكم بما تطمئن به نفسه من أنه بذل القدر الكافي من أجل الوصول إلى العدالة المنشودة في حكمه.

تجدر الإشارة إلى أن تطبيق هذا المبدأ لا ينحصر في مرحة المحاكمة فقط؛ إنما يبدأ تطبيقه في مراحل أخرى قبل المحاكمة ويعود سبب ذلك إلى أن نظرية الإثبات واحدة في مراحل الدعوى كافة، وعلى ذلك فمبدأ حرية الإثبات يتمتع بقوة تجعل النص التشريعي الذي يقيد من هذا المبدأ –من خلال حصر الأدلة المقبولة في إثبات جريمة معينة– مجرد نص استرشادي.

البند الثاني: علاقة الدليل الرقمي بحرمة الحياة الخاصة

يعد الحق في حرمة الحياة الخاصة عصب الحرية الشخصية، وركيزة أساسية لحقوق الإنسان والحريات العامة، تبعا لذلك يقتضي هذا الحق الاحترام من قبل السلطة والأفراد، كما يقتضي في الوقت ذاته أن تكفل له السلطات الحماية الدستورية والقانونية ضد الانتهاك غير المشروع، إلا أن الحق في حرمة الحياة الخاصة ليس حقا مطلقا بل تقيده اعتبارات المصلحة العامة، متى كانت مصلحة المجتمع أولى بالرعاية من حق الفرد في الخصوصية، ولا ينفي ذلك حقيقة أن الانتقاد الأهم الذي يوجه لاستخدام الأدلة العلمية يقوم على ضرورة احترام حقوق الإنسان؛ وعلى وجه التحديد الحق في حرمة الحياة الخاصة، بل إن الرأي المناهض لاستخدام

[1] Coralie Ambroise-Castérot, La preuve, une question de loyauté?, Actualité Juridique Pénal 2005, pp264-279.

الأدلة العلمية في الإثبات الجنائي يستند إلى ضرورة صيانة حقوق الإنسان ومراعاتها وعدم جواز الاعتداء عليها ورفض استخدام هذا النوع من الأدلة، غير أن هذا الاتجاه يتجاوز عن أهمية الدور الذي يؤديه القضاء الجنائي[1].

يقوم التشريع والقضاء الجنائي بدور هام في الموازنة بين حقوق الأشخاص والمصالح العليا للمجتمع، ولكي يتمكن من تأدية هذه الوظيفة على أكمل وجه فلا بد له أن يتسلح بأدوات فعالة، وكلما ازداد تعرض المصالح الاجتماعية للخطر ازدادت الحاجة إلى وسائل تؤمن لها الحماية، وعندما يؤدي اللجوء إلى هذه الوسائل إهدارا لبعض حقوق الإنسان فإن ذلك سيكون ضمن اختيار أقل الضررين.

والحق في الخصوصية من أساسيات حقوق الإنسان يحظى بحماية قانونية واسعة، فعلى مستوى المشروعية الدولية هناك نصوصا عديدة تضمن حماية هذا الحق في مواجهة أي تدخل من السلطات العامة في الحياة الخاصة بصورة تعسفية أو غير قانونية[2] وعليه تعد الخصوصية نطاقا واسعا يصعب وضع حدود ومعالم واضحة له[3]، ومع ذلك يعني الحق في حرمة الحياة الخاصة بالمفهوم الواسع العيش بمنأى عن تلصص الغير، ويحظى هذا المفهوم للحياة الخاصة بأهمية كبيرة في مواجهة وسائل التحقيق الحديثة التي تملكها السلطات العامة[4]، حيث يساهم التطور العلمي والتقني في ظهور أشكال مختلفة من الاعتداء على الحياة الخاصة، لذا تظهر بصورة أكبر من أي وقت مضى أهمية الضمانات التي يتعين أن تحاط بها الأماكن التي تمارس فيها الحياة الخاصة.

البند الثالث: مبدأ الاقتناع الشخصي للقاضي في تقدير الأدلة

يقوم مبدأ حرية القاضي في تكوين عقيدته على أساس استبعاد تدخل القانون في تحديد الأدلة التي يستند إليها أو يستبعدها في حكمه، فهو حر في التنقيب عن الأدلة، وجمعها وتقديمها ومناقشتها، وهو حر أيضا في تقديرها تبعا لاقتناعه الشخصي، فيعد مبدأ الاقتناع القضائي من السمات المميزة الآن للنظم الإجرائية الحديثة، لأن القاضي لا يتقيد بأي قيد أو شرط يفرض عليه من الخارج، وإنما هو مقيد بضميره الوجداني عن الأهواء والأغراض الشخصية، حر في تقدير الأدلة المقدمة إليه من الخصوم، لا دخل للمشرع في فرض أو تحديد قيمة الدليل[5].

أولا: مفهوم مبدأ الاقتناع الشخصي للقاضي في تقدير الأدلة، تكمن الغاية النهائية للأدلة العلمية القضائية التي يجريها القاضي في التوصل إلى الحقيقة الواقعية، فكل نشاط أو جهد ذهني يبذله القاضي خلال إجراء هذه العملية يستوجب التوصل إلى حقيقة الوقائع كما حدثت في الواقع أو العالم الخارجي، لا كما يصورها الخصوم، ولا يمكن أن تظهر الحقيقة الواقعية إلا بعد البحث عنها وثبوتها بالأدلة، وهو لا يصل إليها ما لم يكن قد اقتنع بها وتكون لديه يقين بحدوثها وهذا عملا بمبدأ الاقتناع الشخصي في

---

[1] Jean Pradel, Op.Cit., p371.

[2] المادة 17 من الاتفاقية الدولية لحماية الحقوق المدنية والسياسية، المادة 08 من الاتفاقية الأوربية لحقوق الإنسان، المادة 12 من الإعلان العالمي لحقوق الإنسان، المادة 21 من الميثاق العربي لحقوق الانسان.

[3] حسام الدين كامل الأهواني، الحق في احترام الحياة الخاصة، الحق في الخصوصية، دراسة مقارنة، دار النهضة العربية، القاهرة، 1978، ص47.

[4] Frédéric Sudre, Droit international et Européen des droits de l'homme. Presses Universitaires de France-PUF, 1995, p248.

[5] أحمد يوسف الطحاوي، الأدلة الإلكترونية ودورها في الإثبات الجنائي، دراسة مقارنة، دار النهضة العربية، القاهرة، 2015، ص258.

تقدير الأدلة[1]، وبموجب هذا المبدأ يتمتع القاضي بسلطة تقديرية واسعة سواء من حيث قبول الأدلة ذاتها، أو من حيث تقديره الشخصي لقيمة كل منها، كل ذلك تبعا لما يطمئن إليه، غير أن ذلك لا يعني أن الأنظمة التشريعية التي تعتنق هذا المبدأ تكرس لفكرة واستبداد القاضي، لأنها تضع شروطا لكل دليل وتحدد طرق استخلاصه وتقديمه إلى الجهات المسؤولة، لذلك فإن الاقتناع الشخصي للقاضي هو المبدأ العام الذي يحكم سلطته في تقدير الأدلة، وهو من أهم المبادئ المستقرة في القوانين الإجرائية الحديثة[2].

ويلاحظ أن حرية القاضي الجنائي في الإثبات لها وجهان أولهما؛ أن لقاضي الجنائي يستمد قناعته من أي دليل يطمئن إليه، دون أن يتقيد في تكوين قناعته بدليل معين فجميع طرق الإثبات أمامه سواء، وثانيهما؛ أن القاضي نفسه الذي يقدر بحسب اقتناعه الذاتي القيمة الثبوتية لكل دليل[3]، ذلك أن للقاضي الجنائي دور دورا إيجابيا عكس دور القاضي المدني الذي يقتصر على الموازنة بين الأدلة التي يقدمها أطراف الدعوى، ثم يرجح أيها أغلب، فمن حقه بل من واجبه أن يتحرى الحقيقة، وذلك بكافة الطرق، ثم يقتنع بمنتهى الحرية[4]، فالقاضي في ضوء هذا المبدأ يقدر قيمة الأدلة بحرية تامة[5] في ترجيح بعض الأدلة على بعض.

لذلك يمثل الاقتناع الشخصي للقاضي الأثر النهائي لعملية إستدلال واستنتاج تتلاقى فيها جميع الأدلة القضائية المطروحة بالدعوى، دعائمها العقل والمنطق والوجدان الحي للقاضي أين يقوم فيها بالتمحيص والتقدير والموازنة بين أكثر الأدلة عمقا واتصالا بالحقيقة، فيحدد الحكم على أساسها[6].

وقد تعددت مفاهيم الفقهاء بخصوص مبدأ الاقتناع الشخصي للقاضي الجنائي، فذهب جانب من الفقه إلى القول بأنه ذلك التقدير الحر المسبب لعناصر الإثبات في الدعوى، وهو البديل عن نظام الأدلة القانونية، كما قيل أيضا بأنه تلك الحالة الذهنية أو النفسية، أو ذلك المظهر الذي يوضح وصول القاضي باقتناعه لدرجة اليقين بحقيقة واقعة لم تحدث تحت بصره بصورة عامة[7] غير أن مبدأ حرية القاضي في الاقتناع لا يعني أن يؤسس اقتناعه بناء على عواطفه وإنما هو اقتناع عقلي يجد مصدره في العقل لا في العاطفة، من ذلك فالقضاة ملتزمون ببناء هذا الاقتناع بالعمل الذهني الشاق والمتبصر والواعي والذي يخضعون فيه لقواعد المنطق والجدلية الذهنية التي ترقي بالحس إلى العقل[8]، لذلك فحرية القاضي الجنائي في التثبت أمر يختلف عن التحكم، فالتثبت؛ يعني أن القاضي حر في تقييم أدلة الإثبات دون قيد غير مراعاة واجبه القضائي، وليس معناه أن يقضي بما يشاء فهذا هو التحكم بعينه فلا يجوز له أن يقضي وفقا لهواه، أو يحتكم في قضائه لمحض عاطفته، بل على العكس من ذلك هو ملزم بأن يتحرى المنطق الدقيق في تفكيره الذي قاده إلى اقتناعه[9].

---

[1] كمال عبد الواحد الجوهري، تأسيس الاقتناع القضائي والمحاكمة الجنائية العادلة، دار محمود للنشر والتوزيع، 1999، ص14.

[2] Roger Merle, et André Vitu, Op.Cit., p172.

[3] محمد زكي أبو عامر، المرجع السابق، ص104.

[4] مصطفى مجدي هرجة، الإثبات في المواد الجنائية في ضوء أحكام محكمة النقض، دار المطبوعات الجامعية، الإسكندرية، 1992، ص54.

[5] أحمد فتحي سرور، المرجع السابق، ص747.

[6] مفيدة سعد سويدان، نظرية الاقتناع الذاتي للقاضي الجنائي، دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة، 1985، ص178.

[7] مفيدة سعد سويدان، المرجع نفسه، ص175.

[8] عبد الحكم فودة، حجية الدليل الفني في المواد الجنائية والمدنية، دار الفكر الجامعي، الإسكندرية، 1996، ص23 و24.

[9] محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات التشريعية، المرجع السابق، ص777 و778.

بعد أن يتكون لدى القاضي الجنائي اقتناعه الشخصي بما توصل إليه من نتائج في الدعوى المطروحة أمامه، عليه أن يجرب تطبيقها بشكل افتراضي عكسي لهذه النتائج، فإذا ما كانت نتيجة الافتراض العكسي هو نتائج مخالفة، فإن ذلك يعني أن الاقتناع لديه قد بني على تأكيدات سليمة، وعندئذ يمكن القول بأن اليقين قد ثبت وأصبح جازما، وهذا ما ينبغي أن تبنى عليه الأحكام الجنائية[1]، ولكي تكون الحقيقة القضائية في أقرب صورها إلى الحقيقة الواقعية طالب البعض بضرورة إيجاد معايير لضبط ورقابة عملية تكوين الاقتناع عن طريق أسس المنطق، وأن يكون الاقتناع مسببا، ومدعاة هذه المطالبة هي الخصائص التي تتسم بها القناعة القضائية من كونها ذاتية نسبية[2]، كما نادوا بضرورة التخصص في مجال العمل القضائي، مع وجوب إلمام القاضي بصفة خاصة بالعلوم المساعدة للقانون الجنائي، وخاصة علم النفس، المكون لفكره اقتناعه[3].

ثانيا: مبررات مبدأ الاقتناع الشخصي للقاضي الجنائي، تعتبر الدعوى الجنائية ذات مصلحتين متعارضتين، فهناك مصلحة الجماعة في حفظ أمنها ونظامها، ومصلحة المتهم في حفظ حريته وشرفه، مما استوجب على القاضي الجنائي أن يقوم بدور إيجابي في الكشف عن الحقيقة، فمبدأ الاقتناع الشخصي للقاضي الجنائي يسعى إلى الكشف عن الحقيقة فقط دون الحقيقة التي يحددها أو يسعى الخصوم لإثباتها، لذلك فإن عبء الإثبات ليس على المدعى وحده أو على المتهم في دحض أدلة المدعي، بل يقع كذلك على القاضي الجنائي فعليه إثبات الجريمة والخطورة الإجرامية بكل الوسائل، واتخاذ التدابير اللازمة حسبما تقتضيه المصلحة الاجتماعية لإثبات الإدانة أو البراءة[4]، وهو ما يعني أن الكشف عن الحقيقة ذاتها تتطلب مثل هذا المبدأ[5]، تحقيقا للتوازن بين مصلحة المجتمع ومصلحة المتهم[6].

ويضاف إلى ذلك أن الإثبات في المواد الجنائية يرد على وقائع مادية ونفسية وليس أعمال أو تصرفات قانونية، حيث لا يمكن إعداد الدليل بشأنها، كما أن الإثبات الجنائي يتسم بصعوبة أكبر نظرا لما يلجأ إليه المجرمون من وسائل مختلفة للتهرب من قبضة القانون الأمر الذي أدى إلى العمل على تسهيله بإتاحة الفرصة لأي دليل يوصل إلى الحقيقة.

أدى تطور وسائل التحقيق العلمية الحديثة إلى إخضاعها لاقتناع القاضي كضمان لما قد يرافق هذه الوسائل من أخطاء تترتب عليها أضرار كبيرة في حالة التسليم بها دون تقدير قيمتها الفعلية، بالإضافة إلى ما تنطوي عليه من اعتداء على الحريات الشخصية[7]، كما أن هذه الأدلة لا تقبل بطبيعتها إخضاع القاضي لأي قيود بشأنها، بل ينبغي أن يترك الأمر في تقديرها لمحض سلطة القاضي، فتقدير الأدلة هي مسألة تتعلق بجوهر العدالة وهي في أساسها وإن قامت على قواعد من العقل والمنطق إلا أنها تبقى ذات حس إنساني لا يمكن تصوره في أية آلة مهما كانت دقة تقنيتها[8]، لذلك فالحقيقة تحتاج دوما إلى البحث والتقصي من

---

[1] فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة، دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان، ط1، 2006، ص120.

[2] فاضل زيدان محمد، المرجع نفسه، ص118.

[3] مصطفى مجدي هرجة، المرجع السابق، ص63.

[4] محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، المرجع السابق، ص778.

[5] محمد عيد الغريب، حرية القاضي الجنائي في الاقتناع اليقيني وأثره في تسبيب الأحكام الجنائية، النسر الذهبي للطباعة، القاهرة، 1997، ص46.

[6] Ali Rached, de l'intime conviction de juge, thèse, Paris, 1942.

[7] فاضل زيدان محمد، المرجع السابق، ص101.

[8] فاضل زيدان محمد، المرجع نفسه، ص102.

أجل الوصول إليها، مما يتطلب تخويل القاضي الجنائي سلطة اللجوء إلى أي سبيل يجده مؤديا إليها، فلا يبقى إلا فتح الباب على مصراعيه أمام القاضي الجنائي لإثباتها بكافة طرق الإثبات.

ومما تجدر الاشارة إليه أيضا؛ أن عقيدة القاضي الجنائي لا تقيد قاضي آخر، وعقيدة محكمة جنائية لا تقيد محكمة أخرى في نفس درجتها، ومن المستقر عليه فقها وقضاء أن أحكام النقض أكدت على حرية القاضي الجنائي في وزن وتقدير كل عناصر أدلة الدعوى، وحرية القاضي في تقديرها لتكوين عقيدته مقدمة حتى لو ترتب على حكمه قيام تناقض بينه وبين حكم سابق أصدرته هيئة أخرى على متهم آخر في ذات الواقعة، وعلى ذلك فإذا كانت مصلحة الفرد واعتبارات حماية الحرية الفردية، قد استوجبت افتراض براءته، فإن مصلحة المجتمع في مكافحة الجريمة، واكتشاف حقيقة الأمر في الدعوى الجنائية تستوجب قانونا؛ قبول جميع طرق الإثبات لكشف الحقيقة، ثم إن مبدأ الاقتناع الشخصي للقاضي الجنائي يفيد الدفاع كما يفيد الاتهام.

ثالثا: الانتقادات الموجهة إلى مبدأ الاقتناع الشخصي للقاضي الجنائي، بالرغم مما تقدم من مبررات وما تطرحه من أسس يرتكز عليها مبدأ الاقتناع الشخصي للقاضي الجنائي، لم ينتف مبدأ الاقتناع الشخصي من بعض الانتقادات التي يمكن حصرها في أن هذا المبدأ يهدر ثقة القواعد القانونية الخاصة بعبء الإثبات في المواد الجنائية الناتج عن أصل البراءة.

بما أن القاضي حر في تكوين عقيدته فلا يهم أن يكون مصدر الإقناع دليلا يقدمه الاتهام أو يقدمه الدفاع، ويجعل قاعدة أن الشك يفسر لمصلحة المتهم لا معنى لها، حيث يستطيع بإعلان اقتناعه الشخصي أن يفسر الشك ضد المتهم[1]، كما أن هذا المبدأ وإن قصد به مصلحة المتهم إلا أنه في الواقع يخل بحقوق الدفاع، لأنه يسمح للقاضي بأن يعتمد على اعتراف تم العدول عنه كما أنه يعوق حرية الدفاع لأنه يترك المتهم في حيرة من الانطباع الذي يمكن أن يحدثه هذا العنصر من عناصر الإثبات أو ذاك على نفسية القاضي، وبذلك يجعل المتهم في حالة يصعب عليه فيها تحديد السلوك الذي يجب أن يسلكه للدفاع عن نفسه[2].

فالاقتناع الشخصي للقاضي لا يعبر في جميع الحالات عن اليقين باعتبار أنه نتيجة عمل ذهني وباعتبار أن القاضي إنسان يتأثر كغيره من البشر ببعض العوامل والبواعث المختلفة التي تؤثر على ضميره حينما يكون بصدد تحليل وتقييم الوقائع المعروضة عليه من أجل الوصول إلى الاقتناع الذي سيبني عليه حكمه، ومن ذلك أفكاره التي يعتنقها، ومن ثم قد يحاول القاضي أن يوجه مسار التحقيقات وتفسير الوقائع من الفكرة التي تكونت في الذهن فيزداد اقتناعا في الاتجاه غير الصحيح، ويخطئ في تقديره للأمور وبذلك لا يمكن القطع بالوصول إلى اليقين التام[3].

وقد ذهب جانب من الفقه إلى أن هذا المبدأ يحرم القاضي نفسه من وسيلة حماية ضد مخاطر الزلل وعدم الإحاطة بجميع أدلة الدعوى مما ينعكس بأثر سيء على العدالة، ولذلك فإن البعض يرى أن السيطرة المطلقة لقاضي الموضوع على تقدير القيمة الإقناعية لعناصر الإثبات في الدعوى لا تتفق مع الضمانات التي تمنحها الاتفاقية الأوروبية لحقوق الإنسان للمتقاضي، ومن أبرز هذه الحقوق هو أصل براءة الذمة، إذ أن هذا المبدأ يعطي القاضي الجنائي فرصة اللجوء إلى وسائل الإثبات غير المنصوص عليها في

---

[1] Stefani Gaston, Georges Levasseur, Bernard Bouloc, Procédure pénale, Dalloz, Paris, 1993 p25.

[2] Stefani Gaston, Georges Levasseur, Bernard Bouloc, Procédure pénale, Ibid., p26.

[3] هلالي عبد الله أحمد، النظرية العامة للإثبات في المواد الجنائية، المرجع السابق، ص401.

القانون ولا يتوافر للأطراف فيها أية ضمانات، وعلى ذلك يتعين الأخذ بمبدأ حصر وسائل الإثبات في المواد الجنائية لتلافي خطر الاستعانة بوسائل جديدة للإثبات لم ينص عليها المشرع، وقد تتنافى مع الأخلاق أو تعسف بحقوق الأفراد وحرياتهم[1].

إلا أنه وبالرغم من هذه الانتقادات فإن القاضي ليس حرا في الاقتناع بما يحلو له، ولا يبني إعتقاده على مجرد تصورات شخصية، بل يجب أن يكون هذا الاقتناع مبنيا على منطق سليم في التفكير، ومستقا من خلال أدلة مشروعة متساندة طرحت عليه في الدعوى، وخضعت للمناقشة وأدت في سياقها العقلي والمنطقي إلى تلك النتيجة التي توصل إليها في حكمه.

كما يجب على القاضي أن يذكر في حكمه الأدلة التي اعتمد عليها وكانت مصدرا لاقتناعه، لذلك فإن التزامه بتسبيب الأحكام يعد بمثابة فرصة له حتى يراجعها ويتريث في إصدارها، وبهذا يكون التسبيب بمثابة الحاجز الذي يحمي القاضي من التصورات الشخصية البحتة[2].

الفرع الثاني: سلطة القاضي الجنائي في قبول الأدلة الإلكترونية

إذا كان الأصل أن القاضي الجنائي حر في أن يستمد قناعته من أي دليل يطمئن إليه فإن هذا الأصل ترد عليه بعض الضوابط التي يتعين على القاضي الالتزام بها وهو بصدد اختبار الأدلة التي يستمد منها اقتناعه، فلا يمكن له أن يستمد قناعته من أي دليل، بل فقط من الأدلة التي تتوافر فيها الشروط أو الضوابط التي حددها القانون، وهذه الضوابط المتعلقة بالأدلة تتمثل أساسا في مشروعية الأدلة[3].

تزايدت أهمية الأدلة الرقمية مع بزوغ العصر الحديث التي جعلت للخبرة الفنية مكان الصدارة في مجال الإثبات الجنائي، إذ أن الرغبة في كشف حقيقة الجريمة المرتكبة، وتطور وسائل ارتكابها، استلزم تطورا آخر في وسيلة إثباتها، بيد أن القواعد القانونية ليست هي الوحيدة التي تحكم وسائل البحث عن الأدلة، فإلى جانب هذه القواعد يوجد مبدأ نزاهة الدليل الجنائي.

فقد تثار في الواقع العملي أمور كثيرة من شأنها التأثير على إرادة المتهم بشكل أو بآخر كتلك التي تتعلق بعمليات البحث والتحري والاستجواب وجمع الأدلة، مثل الإكراه المادي والمعنوي أو التنصت الهاتفي أو تسجيل الأحاديث الخاصة أو التقاط الصور خلسة في مكان خاص أو الاستجواب المطول أو النفسي وغيرها من الأمور، في حين حظر مبدأ نزاهة الدليل الجنائي كل تلك الأمور، مما يعني التطابق بين وسيلة البحث عن الدليل مع احترام حقوق الفرد وكرامته الإنسانية واعتبارات العدالة، فيحظر بإعمال ذلك المبدأ أي أسلوب غير مطابق للمبادئ الأساسية للنظام القضائي بقصد الحصول على عناصر الدليل.

ومبدأ نزاهة الدليل الجنائي يساهم أيضا في تحديد الأطر التي يجب أن تجري في حدودها عملية البحث عن الأدلة، فالنزاهة مبدأ يجب أن يحكم عمل أجهزة السلطة العامة في البحث عن الأدلة العلمية المستحدثة، وتختلف النزاهة عن القواعد القانونية من حيث مصدرها، فالنزاهة تستند إلى قواعد مصدرها الأخلاق[4].

---

[1] جوفاني ليون، مبدأ الاقتناع والمشاكل المرتبطة به، ترجمة رمسيس بهنام، مجلة القانون والاقتصاد، العدد 04، القاهرة، 1964، ص934.

[2] هلالي عبد الله أحمد، النظرية العامة للإثبات في المواد الجنائية، المرجع السابق، ص126.

[3] مأمون محمد سلامة، المرجع السابق، ص161.

[4] معتصم خميس مشعشع، المرجع السابق.

وتنطوي إجراءات البحث عن الأدلة العلمية المستحدثة على المساس بالحقوق الأساسية للإنسان، هذا المساس الذي يبرره ضرورة الوصول إلى الحقيقة وإظهارها بشكل واضح، ويعود سبب ذلك إلى الإعتقاد بأن الوصول إلى الحقيقة التي لا يعتريها الشك؛ يتحقق من خلال استخدام هذا النوع من الأدلة، الأمر الذي يضفي بدوره أهمية خاصة على مبدأ النزاهة الذي يجب أن يحكم البحث عن هذا النوع من الأدلة المستحدثة[1].

ويكون الدليل الإلكتروني المتحصل من خلال الوسائل العلمية باطلا إذا تم تحصيله عن طريق غير مشروع أو مخالف للقانون، فإذا كان الدليل الباطل هو الدليل الوحيد في الدعوى فلا يصح الاستناد عليه في إدانة المتهم، فإذ ما شاب التفتيش الواقع على النظم والبرمجيات مخالفة قانونية فإنه يكون باطلا بطلانا مطلقا ولا يجوز التمسك بما ورد في محضر التفتيش كما لا يجوز للمحكمة أن تعتمد عليه في حكمها[2].

البند الأول: مبدأ النزاهة في الحصول على الدليل الرقمي

إن مبدأ النزاهة الجنائية مبدأ عام لم يرد عليه نص في القانون، نجد أنه يبحث عن أدلة الجريمة ويستمد وجوده من المبادئ الأخلاقية التي يجب أن يخضع لها القضاة وأفراد السلطة العامة عند قيامهم بالأعمال الموكل إليهم القيام بها، ومن خلال استقراء غالبية النصوص الإجرائية نجد أنها خلت من ذكر ذلك المبدأ صراحة، فيكون الاعتماد عليه وفق ما جاء في الفقه والقضاء والمواثيق الدولية والإقليمية التي أسهبت في التحدث عنه.

فعلى الرغم من أن التقنيات العلمية تتيح وسائل أكثر فاعلية بالإمكان استخدامها من أجل الوصول إلى الدليل، لكن وفي الوقت ذاته، يضيق هذا الاستخدام من مساحة النزاهة التي يجب أن تتصف بها عملية البحث عن الأدلة وجمعها، الأمر الذي دفع جانب من الفقه إلى القول: إن الفاعلية لا تتوافق غالبا مع النزاهة، فيجمع بين الوسائل العلمية التي تستخدم في جمع الأدلة سمة مشتركة هي أنها تتضمن اعتداء على حرية الإرادة، وبسبب ذلك تظهر الإشكالية المتمثلة في تطبيق مبدأ النزاهة عند استخدام هذا النوع من الوسائل، مما يعني أن أية محاولة ترمي إلى تحديد النزاهة في مجال البحث عن الأدلة لا بد أن تنطلق من ضرورة احترام حرية الإرادة، فأي عمل تقوم به السلطة المختصة بالبحث عن أدلة الجريمة وجمعها قد يتسم بعدم النزاهة إذا كان من شأنه أن يضعف حرية الإرادة أو يعدمها، مما يدفعنا إلى القول بأن هذا البحث قد وقع بوسائل تفتقد إلى النزاهة[3].

تمثل الوظيفة التي يؤديها مبدأ النزاهة الحد من حرية الإثبات إحدى أهم المعطيات التي يمكن الاستناد إليها في بيان أطر المبدأ، الأمر الذي يقتضي بيان الدور الذي يؤديه في الموازنة بين حق الأفراد والحفاظ على حريتهم وحق المجتمع في حياة آمنة[4].

أولا: احترام حقوق الإنسان وحريته، يجب أن يتم البحث عن الدليل في إطار من النزاهة؛ إلى جانب الحق في المحاكمة العادلة والضمانات التي تتعلق بالحق في الدفاع التي يكفلها القانون من خلال تنظيم إجراءات التحري والتحقيق والمحاكمة، حيث

---

[1] هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص14.

[2] نائل عبد الرحمن صالح، محاضرات في أصول المحاكمات الجزائية، قانون أصول المحاكمات الجزائية، قانون محكمة الجنايات الكبرى، دار الفكر العربي عمان، ط1، 1997، ص17.

[3] Jean Pradel, Op.Cit., p390.

[4] Emmanuel Molina, Op.Cit., p450.

يصعب عزل النزاهة التي يجب أن يجري في إطارها البحث عن الدليل على احترام الاعتبار الواجب للإنسان، فمتطلبات هذا الاعتبار تحول دون الحصول على الاعتراف دون مراعاة إرادة المعترف الحرة[1]، وإذا كان يحظر استخدام التعذيب في الحصول على أدلة الجريمة فإنه من الأولى أن يتم حظر استعمال أية وسيلة من شأنها المساس بالحق في السلامة الجسدية أو النفسية للفرد.

ومن غير المقبول إجبار المتهم على الاعتراف بجريمة ما لكي يحل مكانه استعمال وسائل علمية من شأنها الحط من الاعتبار الواجب للإنسان، فأي استعمال لهذه الوسائل لا بد أن يراعي كحد أدنى، الجوانب الإنسانية التي يجب أن يتم بها الاعتراف، أي أن يكون حرا، واعيا وإراديا، وأن تحترم وسائل الحصول عليه حق المشتبه فيه بالصمت[2]، وهذا يعني أن النزاهة تعتبر مطلبا لمشروعية إجراءات البحث عن الأدلة، وتمثل صمام الأمان في مواجهة التعسف الذي قد يحيط بتطبيق حرية الإثبات، حيث تتخذ أحكام القانون ومبادئ الأخلاق من أجل العمل على الحد من وقوع أي تعسف ممكن، وتتمثل أهمية المبدأ في الحد من سلطة القاضي في قبول أدلة قد تم الحصول عليها بطرق غير مشروعة[3].

ثانيا: حق المجتمع في حياة آمنة، إن حاجة الجماعة لإشباع الشعور بالأمن تدفع أفراد المجتمع إلى أن توقع فاعلية كاملة في قمع الجرائم[4]، لكن دون القبول بأن يتم ذلك دون تجاوز المشروعية في البحث عن الأدلة[5]، لذلك يقع كبح الجرائم على عاتق الأجهزة القائمة على تحقيق العدالة الجنائية، لكن يتعين عليها أن تؤدي هذه المهمة بنزاهة، أي الامتناع عن انتهاج طرق لا تتسق مع الاحترام والثقة اللذين يتوقعهما المجتمع من السلطات القائمة على حماية هذه العدالة[6]، من أجل ذلك فإن موضوع النزاهة في مجال البحث عن الأدلة الرقمية يطرح جدلية العلاقة بين الغاية والوسيلة، فمن ناحية؛ يضفي استبعاد أدنى درجة من عدم النزاهة أعلى درجات الشرعية على الإجراء الذي تقوم به السلطة، لكن من ناحية أخرى؛ يجب أن تكون هذه الشرعية فعالة[7].

وبما أن مرحلة التحقيق الأولي أكثر المراحل فاعلية في البحث عن الأدلة، فإن ما يقبل من أفراد الضبطية القضائية القيام به في هذه المرحلة يكون محل اعتراض إذا لجات إليه النيابة العامة، ويكون الاعتراض أكبر عندما يكون قاضي الحكم المستخدم لهذه الوسائل، فطبيعة إجراء البحث على الدليل هي التي تحدد مقبوليته أو عدمها، وليست صفة القائم به[8]، ومن ثم يتضح أن مشروعية الدليل الجنائي تستلزم ضرورة أن يكون الإجراء المستمد منه الدليل مشروعا، هذا ما يستلزم التمييز بين ما إذا كان هذا الدليل هو دليل إدانة أم دليل براءة وذلك على النحو التالي:

---

[1] Renée Koering-Joulin, "La dignité de la personne humaine en droit pénal." dans Marie-Luce Pavia, Thierry Revet, La dignité de la personne humaine, Economica, Paris, 1999, pp67-84.

[2] Emmanuel Molina, La liberté de la preuve des infractions en droit français contemporain Presses Universitaires d'Aix-Marseille, 2001, p457.

[3] Emmanuel Molina, Ibid., p457.

[4] Jacques Faget, Sociologie de la délinquance et de la justice pénale, Erès, Toulouse, France 2002, p136.

[5] Rene Garraud, Op.Cit., p04.

[6] P. Bouzat, La loyauté dans la recherche des preuves, in problèmes contemporains de procédure pénale, Mélanges Hugueney, Sirey, 1964, p165.

[7] Jean Pradel, Op.Cit., p165.

[8] Emmanuel Molina, Op.Cit., p460 et Suivant.

1- حالة دليل الإدانة، إنطلاقا من قاعدة أن الأصل في الإنسان البراءة، فإن المتهم يجب أن يعامل على أساس أنه بريء في مختلف مراحل الدعوى العمومية إلى غاية صدور حكم بات في حقه، وهذا يقتضي أن تكون الأدلة التي يؤسس عليها حكم الإدانة مشروعة، وأي دليل يتم الحصول عليه بطريقة غير مشروعة أو بوسيلة مخالفة للقانون لا تكون له قيمة في الإثبات.

فمشروعية الإثبات الجنائي تستلزم عدم قبول أي دليل كان البحث عنه أو الحصول عليه قد تم بطريق غير مشروع، ومن ثم لا يجوز للقاضي أن يستمد قناعته من استجواب جرى على وجه يخالف القانون، أو من محرر مسروق، أو عن طريق التجسس واستراق السمع، أو تسجيل الأحاديث خلسة، أو التقاط الصور أو التصوير المرئي في مكان خاص دون علم صاحبه، أو على ضبط شيء جاء نتيجة قبض غير قانوني، أو كان وليد إجراء تفتيش باطل، أو اعتراف باطل، أو من دليل جاء نتيجة إجراءات باطلة[1] كما يحظر إطالة الاستجواب بقصد وضع المتهم في حالة نفسية سيئة لحمله على الاعتراف، أو توجيه أسئلة إيحائية له، أو استعمال الحيلة والخداع معه لانتزاع اعترافه رغما عنه.

فإذا ثبت من الأوراق أن رجل الضبطية القضائية وصل إلى الدليل بعد القيام بإجراء غير مشروع المتهم فهو إجراء باطل والدليل المستمد منه منعدم قانونا ولا يصلح للتعويل عليه في الإدانة، كذلك الحال في مرحلة التحقيق القضائي[2]، فمتى كان الحصول على الدليل بإجراءات تخرج عن إطار الشرعية فإن هذه الإجراءات يطالها البطلان، ومتى ما تقرر بطلان أي إجراء من الإجراءات يجب استبعاد ما ينتج عنه من أدلة وما يترتب عن تلك الأدلة من آثار للمحافظة على حرية المواطنين وكرامتهم وحياتهم الشخصية.

2- حالة دليل بالبراءة، يجب أن يبنى حكم الإدانة على دليل مشروع، إلا أنه وفيما يتعلق بدليل البراءة يذهب جانب من الفقه[3] إلى القول بأنه ليس ثمة ما يمنع من تأسيس حكم البراءة عليه، فالمحكمة لم تكن في حاجة إلى إثباته بالإضافة إلى أن بطلان الدليل المستمد بوسيلة غير مشروعة؛ شرع أساسا لحماية حرية المتهم، ومن ثم فإنه من غير المعقول أن ينقلب الدليل وبالا عليه، كما أنه لو تمسكنا بعدم قبول دليل البراءة بحجة أنه غير مشروع فإننا سوف نصل إلى نتيجة خطيرة للغاية وهي إدانة بريء وفي هذه الحالة يتحمل المجتمع ضررين إفلات مجرم من العقاب وزيادة على ذلك عقاب بريء قام دليل على براءته، بالإضافة إلى هذا فإنه وفي حالة وجود شك فإن القاضي يحكم ببراءة المتهم، ومن باب أولى أن يحكم ببراءة الشخص الذي توافر دليل على براءته وليس مجرد شك في إدانته[4].

البند الثاني: معايير وضوابط البحث عن الدليل الرقمي

تضطلع السلطة العامة بالتحقيق من أجل كشف جرائم التكنولوجيا الحديثة والوقوف على أدلتها حتى يمكن لها تقديمها أمام القضاء لكي تساهم في بناء قناعة القاضي الجنائي وتمكينه من الحكم، ويقع عبء الإثبات على السلطات العامة، لكن ذلك

---

[1] رؤوف عبيد، ضوابط تسبيب الأحكام الجنائية وأوامر التصرف في التحقيق، دار الجيل للطباعة، مكتبة الوفاء القانونية، بيروت، 1986، ص500.

[2] عبد الحكم فودة، البراءة وعدم العقاب في الدعوى الجنائية، منشأة المعارف، الإسكندرية، 2000، ص419.

[3] أحمد فتحي سرور، المرجع السابق، ص752. محمود محمود مصطفى، الإثبات في المواد الجنائية في القانون المقارن، الجزء 1، النظرية العامة، مطبعة جامعة القاهرة والكتاب الجامعي، القاهرة، 1977، ص114.

[4] هلالي عبد الله أحمد، النظرية العامة للإثبات في المواد الجنائية، المرجع السابق، ص506.

لا يمنع الشخص العادي من البحث كذلك عن أدلة الجريمة التي يدعي وقوعها، ويقع على كل منهما عدة التزامات أثناء رحلة البحث عن الأدلة.

أولا: التزام السلطة العامة بالنزاهة أثناء جمع الأدلة، أجمع الفقه على ضرورة التزام القاضي والضبطية القضائية بالنزاهة أثناء البحث عن الأدلة[1]، إلا ان هذه الأخيرة يمكن أن تتمتع بمرونة كبيرة خلال عملها في البحث عن الدليل، الأمر الذي يعني أن يكون للنزاهة دورا أقل صرامة في مرحلة التحري، وذلك لأن تحقيق العدالة قد يؤدي في بعض الأحيان إلى عدم الالتزام التام بقواعد النزاهة في رحلة البحث عن الأدلة لمصلحة التوسع في حرية الإثبات[2]، ويرجع ذلك إلى ما يلي:

– يكمن عمل الضبطية القضائية أساسا في العمل على منع وقوع الجرائم، وفي حالة وقوعها تكون وظيفتها البحث عن مرتكبيها ومحاولة الوصول إلى الأدلة الخاصة بتلك الجريمة سواء بالنفي أو الإثبات وهذا في مرحلة ما قبل التحقيق القضائي، والحق أن هذا العمل على درجة كبيرة من الصعوبة ويتطلب القيام به حرية أكبر في الحركة، حيث إن التحري لا يضع –على الأغلب– عند بدايته متهما في مواجهة المجتمع، على خلاف الحال في الدعوى الجنائية وإنما تكون الصورة أقل وضوحا، حيث يواجه مأمورو الضبطية القضائية في الواقع عالم المجرمين، وانعدام أدلة يمكن الاستناد اليها في الاشتباه بهم، ويجري ذلك تحت ضغط الرأي العام الذي يطالب بالكشف عن ملابسات الجريمة على وجه السرعة والفعالية.

– تهدف الإجراءات التي يقوم به رجال الضبط القضائي إلى تحقيق غاية نهائية واحدة هي كشف الحقيقة وإقامة العدالة إلا أن العمل الذي يقوم به رجال الأمن؛ الذين يشكلون المكون الرئيسي للضبطية القضائية تختلف طبيعته عن دور النيابة العامة أو قضاة الحكم، فمأمور الضبط القضائي باعتباره محققا مكلفا بالتحري عن الجرائم، يتحتم عليه أن تكون علاقته مباشرة بالجريمة والمجرم، بينما يأتي دور النيابة العامة التي تتولى التحقيق في مرتبة تالية إذ تقترب من قضاة الحكم[3].

ولا يبرر الأثر النسبي للنزاهة لرجال الضبطية القضائية التجاوز أثناء القيام بأعمال التحقيق بناء على إنابة من النيابة العامة حيث يكون رجالة الضبطية القضائية ملزمون باحترام متطلبات النزاهة التي تقيد عمل النيابة العامة في استقصاء الجرائم وتعقب مرتكبيها، وليس للضبطية القضائية تجاوز متطلبات النزاهة التي ترسم حدود حرية البحث عن الدليل في مرحلة التحقيق النهائي فنسبية النزاهة في تقييد الحرية لا تعني مطلقا تحلل الضبطية القضائية من التزام النزاهة في البحث عن الأدلة في مرحلة التحقيق الأولي ويمكن توضيح ذلك من خلال استخدام الضبطية القضائية لبعض الوسائل غير المشروعة مثل التحريض على ارتكاب الجريمة أو استخدام الحيل والخداع، فيعد خارج إطار النزاهة التي يجب أن تحكم البحث عن الدليل مساهمة من سلطة التحقيق في خلق فكرة الجريمة لدى الشخص للإيقاع به[4].

غير أنه تصعب التفرقة في الكثير من الأحيان، بين التحريض على الجريمة والتحريض على الدليل الذي لا يعد محظورا فيعرف التحريض من الناحية القانونية بأنه حمل الغير على ارتكاب جريمة بتأثير في حرية الشخص واختياره، من هنا يتعين من أجل

---

[1] Jean Pradel, Op.Cit., p390.
[2] Emmanuel Molina, Op.Cit., p460.
[3] M. Blondet, Les ruses et artifices de la police au cours de l'enquête préliminaire Juris-Classeur périodique, 2ème Ed., 1958, pp14-19.
[4] A. Decocq, J. Montreuil, J. Buisson, Le droit de la police, Litec, 2ème Ed., n°1400, 1998, p691.

الوقوف على التحريض المحظور، إعمال التفرقة بين التحريض على الجريمة، والذي يعد بدوره جريمة، والتحريض على الدليل الذي يخرج عن نطاق التجريم[1]، ومن المتفق عليه أن اتخاذ مأموري الضبط القضائي موقفا سلبيا من وقوع الجريمة، أي ترك الجريمة تقع تحت مراقبتهم من أجل القبض على جميع المساهمين فيها في حالة التلبس لا يدخل ضمن التحريض على ارتكاب الجريمة، فيتطلب التحريض الذي يحظره القانون مساهمة إيجابية في وقوع الجريمة، لكن تصبح المسألة أكثر تعقيدا عندما يقوم مأمور الضبط القضائي بفعل إيجابي.

كما يجب التمييز بين التحريض على ارتكاب الجريمة لاقتناص دليل على إدانة مرتكبها وبين استخدام المهارة في ضبط الدليل، فقد تقتضي ظروف ارتكاب الجريمة وجسامتها ووسيلة ارتكابها أن يلجأ مأمور الضبط القضائي إلى وسائل تنبني على المهارة في الممارسة لضبط أدلة هذه الجريمة، نظرا لصعوبة إثباتها بالوسائل العادية ويتوقف ذلك على ما تقتضيه الضرورة ومراعاة التناسب بين الوسيلة المتبعة والهدف المقصود[2]، بالتالي يتعين على القاضي أن يتبين في كل واقعة البحث عما إذا كان التحريض قد أدى إلى وقوع الجريمة، أم أن دوره قد توقف عند جمع أدلة جريمة قد وقعت أو بدأ بتنفيذها.

إنطلاقا من ذلك سيكون بإمكان القاضي أن يقرر إباحة التحريض إذا كان هدفه الوصول إلى أدلة الجريمة، ويتحقق ذلك في التحريض الذي يأتي بعد وقوع الجريمة أو في أثناء وقوعها فيمنع الاستمرار بها، بينما يكون التحريض محظورا عندما يؤدي إلى وقوع جريمة ما كانت ستقع لولا تحريض مأمور الضبط القضائي، وعلى ذلك فالنزاهة قيد على عمل السلطات المختلفة في البحث عن الأدلة.

وتعد من الطرق غير المشروعة أيضا من طرق التدليس أو الغش أو الخداع في الحصول على الأدلة الإلكترونية، ولقد صادقت لجنة الوزراء التابعة للمجلس الأوروبي في 28 يناير 1941 علي اتفاقية خاصة بحماية الأشخاص في مواجهة مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية، ومن المحاور المهمة التي تناولتها الاتفاقية ضرورة أن تكون البيانات المضبوطة صحيحة وكاملة ودقيقة، ومستمدة بطرق مشروعة، ومدة حفظها محددة زمنيا، وعدم إفشائها أو استعمالها في غير الأغراض المخصصة لها، وحق الشخص المعني في التعرف والإطلاع على البيانات المسجلة المتعلقة به وتصحيحها وتعديلها ومناقضتها ومحوها إذا كانت باطلة[3].

في هذا الصدد طبق القضاء الفرنسي مبدأ التناسب على الأدلة الجنائية، وأضفى مرونة على تطبيق النزاهة في البحث عن الأدلة مدفوعا بالحاجة إلى مكافحة الجريمة بطرق أكثر فاعلية، فقد لاحظ جانب من الفقه إلى أن هناك اتجاها قضائيا يتجه نحو التوسع في قبول بعض وسائل التحري التي تعد من قبيل الحيلة والخداع، فبالرغم من الاعتراف بعدم اتساقها مع متطلبات النزاهة إلا أنها تهدف إلى تحقيق الفاعلية في البحث عن الأدلة، وعلى وجه الخصوص عندما تدخل المسألة في نطاق مكافحة بعض أشكال الإجرام الخطرة صعبة الإثبات كالجرائم المتصلة بالتكنولوجيا الحديثة، وعلى ذلك فإن تقرير ما إذا كانت الإجراءات تتسم بجملتها بمراعاة مبادئ العدالة يقوم أيضا على ضرورة مراعاة المصلحة العامة في مكافحة بعض أنواع الجرائم وملاحقة مرتكبيها.

---

[1] Emmanuel Molina, Op.Cit., p485.

[2] أحمد فتحي سرور، المرجع السابق، ص599.

[3] جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، (أجهزة الرادار –الحاسبات الآلية –البصمة الوراثية)، دراسة مقارنة، دار النهضة العربية، القاهرة، 2002، ص112.

ثانيا: إلزام الأشخاص العاديين بالنزاهة في البحث عن الأدلة، إذا نظرنا إلى التنظيم القانوني للبحث عن الأدلة نجد أنه ينصب على تنظيم الإجراءات التي يقوم بها أفراد السلطة العامة من مأموري الضبطية القضائية أو أعضاء النيابة العامة أو قضاة الحكم، ولكن لا يمتد هذا التنظيم لكي يطال الدور الذي قد تؤديه الأطراف الخاصة في الدعوى الجنائية للبحث عن الدليل الرقمي فطابع الإجراءات التفتيشي يستدعي على أن الدعوى الجنائية هي مسؤولية الدولة، وليس للأطراف الخاصة في هذا النظام دور مهم في الدعوى، غير أنه لم يعد حاليا لهذا النظام المفاهيم التقليدية ذاتها.

يساعد تطور الوسائل العلمية والتقنية في زيادة أهمية دور المجني عليه، ويتعاظم هذا الدور أيضا بسبب عدم تقييده بالقيود التي تحد من حرية الإثبات التي تفيد السلطة العامة، فالمجني عليه قد يمتلك من خلال تسجيل المكالمات أو الاستعانة بكاميرات المراقبة أو أجهزة التصوير، وسائل فعالة تساعد في الكشف عن مرتكب الجريمة التي وقعت ضده والوقوف على أدلتها، لكن استخدام هذه الوسائل يشوبه عدم النزاهة وربما يمثل استخدام بعضها جرائم يعاقب عليها القانون[1].

يتضح مما تقدم أنه ليس لمبدأ النزاهة نفس الدور عندما يجري هذا البحث بواسطة المجني عليه؛ حيث يملك هذا الأخير اللجوء إلى وسائل الإثبات كافة من أجل الوصول إلى الدليل على وقوع الجريمة وإسنادها إلى الفاعل، وإن اتسمت بعدم النزاهة ويستند هذا القول إلى مجموعة أسباب أهمها:

– لا يعد البحث عن الدليل بواسطة المجني عليه من إجراءات البحث عن الأدلة القضائية، ويتحدد معنى إجراءات التحقيق بالتحقيق الرسمي، سواء كان أوليا، ابتدائيا أم نهائيا.

– لا يعد ما يقدمه المجني عليه أمام القضاء من أجل إثبات الجريمة التي وقعت ضده دليل، إنما من قبيل الدلائل التي تفتقد إلى الصفة الرسمية التي يتمتع بها الدليل.

وقد استنبط بعض الفقهاء[2]، من أحكام القضاء الفرنسي التي تسمح بقبول الدليل الذي تم التوصل إليه بوسيلة غير مشروعة، أن محكمة النقض الفرنسية تضع ثلاثة شروط لقبول الدليل:

– أن يكون أحد الأطراف الخاصة في الدعوى هو الذي تحصل على الدليل.

– ألا تكون عدم مشروعية الوسائل المستخدمة على درجة كبيرة من الجسامة، فليس مقبولا استخدام العنف مثلا في الحصول على الدليل.

– يتعين احترام مبدأ المواجهة الذي يقضي بالسماح لأطراف الدعوى بمناقشة الدليل لاسيما خلال المحاكمة.

وهنا نخلص إلى أن القول بعدم تقييد أعمال السلطة العامة بالنزاهة من أجل تحقيق فاعلية أكبر في مكافحة الجريمة وإظهار الحقيقة ينطوي على خطورة ليس بالإمكان إغفالها.

---

[1] Coralie Ambroise-Castérot, Recherche et administration des preuves en procédure pénale, la quête du Graal de la Vérité, Actualité Juridique Pénal, Op.Cit., p261.

[2] Jean Pradel, André Varinard, Les grands arrêts de la procédure pénale, Dalloz, Paris, 2003.

المطلب الثاني: المسؤولية الناشئة عن جرائم التكنولوجيا الحديثة والعقوبات المقررة لها

أثار انتشار المعلومات بشكل واسع وكبير على شبكة الأنترنت بعض علامات الاستفهام حول مسؤولية مزودي هذه الشبكة بخصوص ما ينشر من معلومات بواسطتهم، من هنا اعتبرت مسؤولية أشخاص الأنترنت من أهم المسائل التي دار النقاش حولها، خصوصا أن هذا الموضوع يجمع بين ثناياه مسائل تتعلق بالمساس بحرية التعبير، أو يتعلق بما يدعو له البعض من ضرورة فرض الرقابة على شبكة الإنترنت بناء على جوانب أخلاقية بهدف حماية الحقوق الشخصية للأفراد، ذلك أنه كلما تشددنا في إقامة مسؤولية مزودي الإنترنت كلما زاد حرصهم على فرض الرقابة الذاتية على المعلومات لدرء المسؤولية عنهم، مما قد يؤدي إلى تقييد حرية التعبير والحد من انتشار الإنترنت[1]، بالمقابل كلما تجاهلنا إقامة مسؤولية هؤلاء المقدمين كلما أدى ذلك إلى وجود أكبر للمعلومات غير المشروعة على الشبكة، ولازداد تبعا لذلك تقاعس المزودون عن استخدام الوسائل اللازمة للحد أو لمنع انتشار المعلومات غير المشروعة[2].

الأمر الذي أثار كذلك الكثير من الإشكاليات القانونية والفنية مما استدعى تدخل مختلف التشريعات المعاصرة لحسم الجدل، ولوضع نظام قانوني خاص بمقدمي خدمات الإنترنت، فحددت من خلاله بدقة الالتزامات الملقاة على عاتقهم، والأحكام الخاصة بمسؤوليتهم عما يحدث من مخالفات عبر الشبكة بالإضافة إلى تحديد العقوبات المقررة لها.

فالإشكالية هنا تكمن في محاولة تحديد من سيكون مسؤولا عن المعلومة غير المشروعة، أو المضرة والمنتشرة على شبكة الإنترنت في ضوء تعدد الأشخاص المتدخلين في عملية نشر المعلومة، بدءا من مؤلف المعلومة، إلى منتجها، وموردها، ثم إلى الشخص الذي يتولى توريد منافذ الدخول وإيصال المشتركين بالشبكة، فمورد أو متعهد الإيواء الذي يتولى تخزين المعلومات، وإيوائها على موقعه، يضاف إلى ذلك الدور الذي يقوم به كل من محركات البحث والمنتديات...إلخ، لذلك غالبا ما يجد الضحية نفسه متضررا من المعلومة غير المشروعة دون أن يتمكن من تحديد المسؤول عن الضرر الذي لحقه.

الفرع الأول: المسؤولية الناتجة عن جرائم التكنولوجيا الحديثة

المسؤولية الجنائية عن الجرائم المتصلة بتكنولوجيا المعلومات الحديثة يكتنفها العديد من الصعوبات الناجمة عن صعوبة معرفة مرتكبيها، نظرا لتعدد مستخدمي الشبكة العالمية للإنترنت، فضلا عن صعوبة الإثبات في هذه الجرائم، ناهيك عن صعوبة اتخاذ الإجراءات الجنائية سواء تلك المتعلقة بالبحث والتحري والإستدلال أو التحقيق الابتدائي أو المحاكمة، ونظرا لاتسام المسؤولية الجنائية للمتدخلين في الإنترنت خاصة المهنيين بأحكام خاصة، أقرب ما تكون للأحكام الخاصة بالمسؤولية الجنائية للمتدخلين في أعمال الصحافة، نحاول عرض النصوص التجريمية لهذه الجرائم، ثم نشير إلى مدى المساءلة الجنائية للمتدخلين عبر الإنترنت.

[1] عايد رجا الخلايلة، المرجع السابق، ص207.

[2] Disponible sur le site: www.droit-technologie.org

البند الأول: المسؤولية الناتجة عن جرائم الصحافة المرتبطة بالتكنولوجيا الحديثة

إن جرائم الصحافة المتصلة بالتكنولوجيا الحديثة من الجرائم واسعة الانتشار في العالم المعاصر، وهذا ما تبنته المادة 04 من القانون العضوي رقم 12-05 المتعلق بالإعلام، لذلك كانت محل عدد كبير من الأبحاث التي حاولت إيجاد حل لمشكلة المسؤولية الجنائية للصحفي على نحو يحافظ على اعتبارات العدالة، ومن هذه الحلول نجد نظم المسؤولية التي لا تخرج عن ثلاث اتجاهات وهي: المسؤولية التضامنية، المسؤولية بالتتابع والمسؤولية على أساس الإهمال في حين يمكن أن تنتفي هذه المسؤولية لسبب من أسباب الإباحة أو لمانع من موانع المسؤولية، وبالرغم من اتفاق معظم التشريعات على تجريم الأشخاص المسؤولين على ارتكابها، إلا أنها قد اختلفت في كيفية تنظيم المسؤولية للأشخاص المتدخلين في ارتكاب الجريمة الصحفية، ولكن هذه التشريعات لم تخرج عن ثلاث حلول في تنظيم هذه المسؤوليات أو الحلول والتي سنتناولها بالدراسة فيما يلي.

أولا: نظام المسؤولية التضامنية، يجد هذا النظام جذوره من خلال فكرة التضامن، فتقوم هذه الفكرة على أساس حصر المسؤولين في الشخص المسؤول على سياسة الصحيفة، والذي عن طريقه يمكن الحصول على الإجازة بالنشر من عدمه، أي رئيس التحرير أو الناشر، وذلك بحسب الحالة، ويكون مسؤولا باعتباره فاعلا أصليا للجريمة المرتكبة بواسطة الصحيفة، أما المؤلف الذي صدرت عنه الكتابة أو النشر أو غير ذلك، فيكون شريكا له في ارتكاب هذه الجريمة طبقا للقواعد العامة في المسؤولية الجنائية دون أن تتعدى المسؤولية إلى غيرهم من المستوردين والطابعين[1].

أقر المشرع الجزائري في عام 1990 بالمسؤولية التضامنية والمسؤولية على أساس التتابع والتي سندرسها لاحقا معا، أي أنه أقر مسؤولية المدير والناشر مع افتراض المسؤولية إلى ما دونه في الترتيب من المؤلف والطابع وغيرهم ليخالف المشرع بذلك مبدأين أساسيين هما مبدأ شخصية العقوبة ومبدأ قرينة البراءة.

أما بالنسبة للقانون ساري المفعول فقد تبنى نفس النظام الذي تبناه قانون 1982 بأخذه المسؤولية التضامنية حسب المادة 115 على أنه يتحمل المدير مسؤول النشرية أو مدير جهاز الصحافة الإلكترونية، وكذا صاحب الكتابة أو الرسم مسؤولية كل كتابة أو رسم يتم نشرها من طرف نشرية دورية أو صحافة إلكترونية، ويتحمل مدير خدمة الاتصال السمعي البصري أو عبر الإنترنت وصاحب الخبر الذي تم بثه المسؤولية عن الخبر السمعي و/أو البصري المبث من قبل خدمة الاتصال السمعي البصري أو عبر الإنترنت، حيث يتم اختيار هؤلاء المسؤولين في مجال الصحافة أساسا من الصلاحيات التي ينفرد بها هؤلاء المدراء الذي يملكون قبل كل شيء وبشكل حصري سلطة النشر وواجب المراقبة، فطبقا لنص المادة 115 دائما فإن الجزائر اتبعت نظام المسؤولية التضامنية في المسؤولية الجنائية.

ثانيا: المسؤولية على أساس الإهمال، تقوم هذه النظرية على أساس فصل الجريمة المسندة إلى المؤلف عن جريمة كل من رئيس التحرير، الناشر، أو الطابع، على غرار النظريات السابقة التي أقرت بوحدة الجريمة ويعاقب رئيس التحرير بذات العقوبات المقررة للمؤلف، فعندما ترتكب جريمة عن طريق صحيفة ما، فإن مسؤولية المؤلف تكون على أساس ارتكاب تلك الجريمة ومعاقبته

[1] مريوان عمر سليمان، القذف في نطاق النقد الصحفي، دراسة مقارنة، المركز القومي للإصدارات القانونية، القاهرة، ط1، 2014، ص252.

بالعقوبة المقررة لها، أما مسؤولية رئيس التحرير، الناشر، أو الطابع فتكون عن جريمة خاصة، ألا وهي جريمة الإهمال في القيام بواجب الرقابة والإشراف على عملية النشر ومن ثم معاقبته على هذا الأساس، لأن وظيفة التحرير مراقبة ما يكتب وينشر[1].

ويعيب على هذه الفكرة أن رئيس التحرير يسأل مسؤولية عمدية باعتباره فاعلا أصليا للجريمة العمدية التي ارتكبت في صحيفته، وهنا لا يمكننا أن نفسر العمد بالإهمال، فلا يمكن أن نسأل شخصا عن جريمة عمدية ونفسر هذه المسؤولية بالقول بأنه أهمل في أداء وظيفته، بالإضافة إلى أن هذه الفكرة تعترف بازدواجية الجريمة، فرئيس التحرير يتحمل المسؤولية عن جريمة خاصة تختلف عن أصل الجريمة الصحفية وذلك بسبب الإهمال في عدم مراقبة ما ينشر، وكان من الممكن قبول هذه الفكرة لو أن الجريمة المنسوبة إلى رئيس التحرير أو المدير المسؤول هي جريمة غير عمدية[2].

ثالثا: نظام المسؤولية على أساس التتابع، تقوم هذه الفكرة على حصر المسؤولين في نظر القانون وترتيبهم على نحو معين، بحيث لا يسأل منهم شخص ما دام يوجد غيره ممن تقدم ترتيب القانون عليه، أي هناك تسلسل هرمي معين حسب أهمية الدور الذي يقوم به الشخص الذي يسبقه في الترتيب[3]، فتقوم المسؤولية الجنائية هنا على الشخص الموجود في قمة ترتيب الأشخاص المسؤولين جنائيا، فإذا كان غير معروف يسأل الشخص الذي يليه حتى تصل إلى الشخص الأخير، ولكن لا يسأل المتهم إذا وجد غيره ممن قدمه القانون عليه في الترتيب[4]، وهذا النظام يقوم على استبعاد قواعد الاشتراك وبالتالي لا يستلزم توافر القصد الجنائي لدى المتهم في حالة كونه عنصرا في الترتيب، فمجرد وجوده في ذلك الترتيب حقت عليه المسؤولية دون النظر إلى ما دونه في الترتيب حتى لو كان قد ساهم بالفعل في عملية النشر[5].

ولا شك أنه إذا كان من الجائز قبول فكرة التتابع في المسؤولية الجنائية في نطاق الصحافة وغيرها من جرائم النشر المتصلة بالتكنولوجيا الحديثة، فمرد ذلك أنه في مثل هذه الجرائم يندر معرفة المؤلف أو الكاتب، بل ومن الصعب أيضا إزاء كثرة المتدخلين في إعداد المطبوع ونشره وتعدد الأدوار التي يقومون بها وتداخلها وإخفائها، وعليه يمكن مساءلتهم عنها بوصفهم فاعلا أصليا لها أو شريكا فيها[6]، وبمقتضى نظام المسؤولية المتابعة فإن المسؤولية في جرائم الصحافة تشمل كل من:

– **المؤلف:** هو مصدر الكتابة أو الرسوم أو الصور أو غيرها من طرق التمثيل سواء كان هو الذي ابتكرها أو كتبها أو اقتصر دوره على مجرد تقديمها باسمه لا باسم صاحبها الأصلي إلى رئيس التحرير أو الناشر[7].

---

[1] سعد صالح شكطي الجبوري، مسؤولية الصحفي الجنائية عن جرائم النشر، دراسة مقارنة، دار الجامعة الجديدة للنشر، الإسكندرية، 2013، ص292.

[2] مريوان عمر سليمان، المرجع السابق، ص259.

[3] مريوان عمر سليمان، المرجع نفسه، ص255. عمر سالم، نحو قانون جنائي للصحافة، القسم العام، دار النهضة العربية، القاهرة، مصر، ط1، 1995 ص138.

[4] يسري محمد حسن القصاص، الضوابط الجنائية لحرية الرأي والتعبير، دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة طنطا، مصر، 2013 ص89.

[5] سعد صالح شكطي الجبوري، المرجع السابق، ص256.

[6] مريوان عمر سليمان، المرجع السابق، ص257 و258.

[7] أمال عبد الرحيم عثمان، جريمة القذف، دراسة مقارنة في القانون المصري المقارن بالقانون الفرنسي والقانون الإيطالي، مجلة القانون والاقتصاد، العدد 04، السنة 38، القاهرة، 1968 ص764.

– **رئيس التحرير**: هو الذي يتولى الإشراف الفعلي على كل ما يتم تحريره في القسم المسؤول عنه، ويسأل بصفته فاعلا أصليا بمجرد النشر.

– **الناشر**: هو الشخص الذي يتولى نشر أي مطبوع، ويسأل عن نشر المطبوع المتضمن جريمة وهو يعلم حقيقته ويريد وقوع هذه الجريمة، ويعتبر في هذه الحالة فاعلا أصليا لجريمة النشر، ويعد ذلك تطبيقا للقواعد العامة للمسؤولية الجنائية.

– **الطابع**: يسأل كفاعل أصلي إذا لم يعرف مرتكب الجريمة، كأن يكون مرتكب الجريمة موجودا وقت النشر في الخارج أو إذا كانت الكتابة وما في حكمها قد نشرت بالخارج وكان المؤلف غير معروف[1].

– **المستورد**: هو الذي يقوم باستيراد الصحف والمطبوعات من الخارج ويدخلها داخل البلد، ويسأل جنائيا متى كان المطبوع المتضمن للجريمة قد نشر في الخارج[2].

– **القائم بالنقل والترجمة وترديد الشائعات**: هو ذلك الشخص الذي يقوم بنقل المقال المتضمن جريمة والمنشور من جريدة إلى جريدة أخرى، فيسأل باعتباره فاعلا أصليا لأن هذا النقل يعتبر نشرا جديدا ونفس الأمر فيمن يترجم مصنفا يعد عملا من أعمال التأليف[3].

البند الثاني: تحديد المسؤولية الجنائية للمتدخلين في الإنترنت

قد يكون المتدخلون في الإنترنت مهنيين أو مستخدمين.

أولا: المسؤولية الجنائية للمهنيين المتدخلين في الإنترنت، يعد كل من متعهد الوصول، متعهد الإيواء، المنتج، ناقل المعلومات، مورد المعلومات، مؤلف الرسالة، مورد الوسائل الفنية، ومتعهد الخدمات مجموع المهنيون؛ متدخلون في الإنترنت.

1– المسؤولية الجنائية لمتعهد الوصول: يقتضي الدخول إلى الإنترنت في جميع الأحوال اللجوء إلى متعهد الوصول وهذا الأخير هو مقدم الخدمات الفنية الذي يدير الآلة المتصلة فعلا بالإنترنت ويتيح للمستخدم الوصول إلى الشبكة، فمتعهد الوصول يقدم خدمات من طبيعة فنية تتمثل في ربط المشتركين بالمواقع أو بالمستخدمين الآخرين بالشبكة، وذلك عن طريق وضع الحاسب الخادم الخاص به تحت تصرف المشتركين مما يتيح لهم الولوج، التجوال، وإرسال الحزم المعلوماتية في هذه الشبكة، فمتعهد الوصول لا يقوم إلا بدور فني يتمثل في توفير الربط بين الجمهور المتصل بشبكة الإنترنت، فهو لا يقدم المعلومة أو محتوى الحزمة المعلوماتية، وقد يكون شخصا معنويا أو طبيعيا[4].

وقد اختلف الفقه حول مدى مساءلته جنائيا، فهناك من ينكر أية مسؤولية جنائية له في أي حال من الأحوال استنادا إلى أن دوره لا يتعدى كونه دورا فنيا ومن ثم لا يستطيع أن يحكم على ما إذا كان المحتوى مشروعا أم غير مشروع، وعلى العكس

---

[1] أمال عبد الرحيم عثمان، جريمة القذف، دراسة مقارنة في القانون المصري المقارن بالقانون الفرنسي والقانون الإيطالي، المرجع السابق، ص771.

[2] عمر سالم، المرجع السابق، ص159.

[3] علي محمد حسن عبد الله، حماية برامج الحاسب بقانون براءة الاختراع في الولايات المتحدة الأمريكية، مجلة الشريعة والقانون، العدد 47، الإمارات العربية المتحدة، 2011، ص90 و91.

[4] شيماء عبد الغني محمد عطا الله، المرجع السابق، ص165 و166.

هناك من يرى مساءلته بصفته فاعلا وفقا لنظام المسؤولية بالتتابع التي أقرها المشرع في جرائم الصحافة المتصلة بالتكنولوجيا الحديثة باعتباره أحد الأشخاص الذين يدخلون في هذه السلسلة، ومن ثم يتعين إلزامه بمنع أو محو المعلومات غير المشروعة، فهو يعد بمثابة الموزع للصحافة، استنادا إلى أنه كان يتعين عليه منع نشر المعلومة الإلكترونية متى كانت مخالفة للقوانين، وذلك بغلق الموقع أو الصفحة التي تحتوي على مادة معاقب على نشرها[1].

الواقع أن المسؤولية الجنائية لمزودي الخدمة الإلكترونية تتوقف على طبيعة دوره وعلى ظروف كل واقعة على حدى ومدى ارتباط الواقعة بالدور المسند إليها، فإذا كان دوره يقتصر على توصيل المستخدم بالإنترنت، فإنه لا يسأل جنائيا، ولا يحتج بإقرار المساءلة بالتتابع، نظرا للطابع الاستثنائي المنتقد لهذه المسؤولية، وعلى العكس يسأل جنائيا متى ثبت علمه بمحتوى المعلومة الإلكترونية وبعدم تدخله لغلق الموقع، وأيضا لا يسال كشريك لأنه لا يقوم بتوصيل الجاني إلى الموقع وإنما يقوم بتوصيل عميله بالموقع الذي يريده، فضلا على أن وضع المعلومات غير المشروعة على الشبكة يمكن أن يتحقق قبل ربط المشترك بالموقع عن طريق متعهد الوصول، والأكثر من ذلك قد تكون موجودة قبل وجود متعهد الوصول نفسه[2].

2- المسؤولية الجنائية لمتعهد الإيواء: متعهد الإيواء هو الذي يسمح بالوصول إلى الموقع من خلال شبكة الإنترنت وهو عبارة عن شركة تجارية أو أحد أشخاص القانون العام يقوم بعرض إيواء صفحات الوب على حاسباته الخادمة -في الغالب مقابل أجر-، فهو يعتبر بمثابة مؤجر يقوم بتأجير مكان على الوب للمستأجر الذي ينشر عليه كل ما يريد.

ونرى أن متعهد الاستضافة يسأل جنائيا وفقا للقواعد العامة للمسؤولية الجنائية استنادا إلى الدور المنسوب إليه، فهو الذي يأوي المعلومة الإلكترونية ويساهم في عملية النشر عن طريق المساحة المحددة التي يؤجرها لمنشئ الصفحة الشخصية، ومسؤوليته هنا تكون بصفته شريكا في الجريمة، متى كان يعلم بمضمون المعلومة الإلكترونية غير مشروعة على صفحاته عبر شبكة الإنترنت نظرا لالتزامه بمراقبتها والتدخل الفوري لحجبها[3].

تجدر الإشارة هنا إلى ضرورة التمييز بين نشر رسالة غير مشروعة ونشر صفحة على صفحات الوب، نظرا لأن الأولى ذات طبيعة وقتية على عكس الثانية التي هي ذات طبيعة مستمرة، وعليه إذا تعلق النشر برسالة فإن العلم اللاحق بعد عملية النشر ينفي دور المرسل كشريك في الجريمة، على عكس العلم اللاحق لناشر صفحة على الوب فيسأل كشريك إذا ثبت عدم اتخاذه أي إجراء بصددها بعد علمه هذا، ويأخذ حكم رئيس التحرير، ومن ثم يخضع لقواعد المسؤولية بالتتابع.

3- المسؤولية الجنائية لناقل المعلومة: ناقل المعلومات هو العامل الفني الذي يقوم بالربط بين الشبكات، ويؤمن نقل المعلومات من جهاز المستخدم إلى الحاسب الخادم لمتعهد الوصول، ثم نقلها من هذا الحاسب الأخير إلى الاجهزة المرتبطة بمواقع الإنترنت أو مستخدمي الشبكة الآخرين، ونري عدم مساءلته جنائيا لاقتصار دوره على الطابع الفني، إلا إذا كان يعلم بعدم مشروعية المعلومة التي يقوم بنقلها عبر شبكات الإنترنت، لكونه يملك سلطة وقفها أو محوها وعدم تمريرها.

---

[1] شيماء عبد الغني محمد عطا الله، المرجع السابق، ص167.

[2] علي حسن محمد الطوالبة، الجرائم الإلكترونية، دراسة مقارنة، مطبوعات جامعة العلوم التطبيقية، جامعة العلوم التطبيقية، ط1، 2008، ص255 و256.

[3] شيماء عبد الغني محمد عطا الله، المرجع السابق، ص176.

4- المسؤولية الجنائية لمورد المعلومة: مورد المعلومة هو ذلك الشخص الذي يقوم بتجميعها حول موضوع معين وتحميلها على الجهاز، ونري مساءلته جنائيا استنادا إلى ما يملكه من سيطرة كاملة على المعلومات التي يبثها على الشبكة، وعليه يتحمل بثه لأي معلومات غير قانونية، ومن ثم يسأل جنائيا إذا ثبت أو سجل مثلا صورا مخلة بالآداب العامة بهدف نشرها، ويأخذ حكم مدير التحرير في الصحافة.

5- مساءلة متعهد الخدمات الإلكتروني جنائيا: متعهد الخدمات (ناشر الموقع)؛ هو المسؤول الأول عن المعلومات التي تعبر الشبكة لأنه الوحيد الذي يملك مراقبة المعلومات المنشورة، ويتصور أن يكون ناشر الموقع هو نفسه مقدم المعلومة أو مزود الخدمة، أو متعهد الاستضافة، ويأخذ حكم الناشر في الصحافة[1].

مما لا شك فيه أن متعهد الخدمات يعد مسؤولا عن بث المعلومة الإلكترونية غير المشروعة عبر شبكة الإنترنت لأنه ملتزم بحسن تنفيذ الخدمة المعلوماتية بما يتفق مع أعراف المهنة، كما أنه ملتزم بالإعلام عن وسائل الدخول إلى الخدمة، وبمراقبة مضمون الرسائل التي تصل إليه وإقرار عدم نشرها متى كانت غير مشروعة، ويأخذ حكم الناشر في الصحافة.

6- المسؤولية الجنائية لمؤلف الرسالة غير المشروعة جنائيا: يأخذ مؤلف الرسالة حكم المحرر بالصحافة المتصلة بالتكنولوجيا الحديثة، ونرى مساءلته جنائيا وفقا للقواعد العامة للمسؤولية الجنائية لكونه هو الذي كتبها.

7- مسؤولية مالك الموقع: يسأل صاحب الموقع عما يبث في موقعه مما قد يعد بثه مشكلا لجريمة، والواقع أن صاحب الموقع شريك متعهد الإيواء عن الجرائم التي تقع على موقعه ما دام أنه قد قدم المادة المعاقب عليها للنشر على الشبكة وتوافر لديه الركن المعنوي في تلك الجرائم[2].

ثانيا: المسؤولية الجنائية لمستخدمي الإنترنت: مستخدم الإنترنت هو الشخص الذي يرتبط بمتعهد الوصول (الشبكة) بواسطة خط تليفوني بهدف الحصول على المعلومات أو بثها أو تبادلها من خلال الكمبيوتر الخاص به، وفيما يتعلق بمدى مساءلته جنائيا، يمكن القول إن تحديد هذه المساءلة يتوقف دون شك على مدى تجريم المشرع لجرائم التكنولوجيا الحديثة استنادا إلى مبدأ الشرعية الجنائية.

ويمكن القول أيضا بأن التشريعات المقارنة لم تسلك مسلكا واحدا إزاء الجرائم المتصلة بالتكنولوجيا الحديثة، والواقع أننا لا يمكننا القول بمدى إقرار مساءلة المستخدم جنائيا عن جرائم الإنترنت قولا واحدا، وإنما تختلف الإجابة باختلاف نهج التشريعات ونطاق التجريم الذي سنته، ومدى انطباقه على كل جريمة على حدى، ونظرا لسبق تناولنا لجرائم التكنولوجيا الحديثة، فإننا نحيل إليها للوقوف على مدى تجريم المشرع لهذه الصور الإجرامية، ونكتفي هنا بالإشارة إلى أمرين:

الأول، يتعلق بأحكام المسؤولية الجنائية لمستخدمي الكمبيوتر والإنترنت: يمكن القول إن المشرع الجزائري وغيره من التشريعات المقارنة على اختلاف اتجاهاتها قد أقر أحكام المسؤولية الجنائية العادية على مرتكبي هذه الجرائم من المستخدمين أي دون

---

[1] Patrick Auvret, L'application du droit de la presse au réseau internet, Juris-Classeur périodique, Paris, Vol. 108, n°08, 1999, p222.

[2] شيماء عبد الغني محمد عطا الله، المرجع السابق، ص185-187.

إقرار لأي قواعد استثنائية في هذا الصدد، على عكس نهجه بالنسبة للمتدخلين في الإنترنت من المهنيين وإقراره لنظام المسؤولية الجنائية المتابعة على النحو السابق إيضاحه.

أما الثاني، يتعلق بمدى اعتبار قيام المستخدم أو مورد المعلومة مرتكبا لجريمة إخفاء أشياء متحصله من جناية أو جنحة: يمكن القول بأنه إذا قام مثلا بجمع الرسائل المخلة والصور الإباحية أو التي تتضمن دعارة أطفال من خلال المواقع الموجودة على شبكة الإنترنت وتخزينها على دعامة مادية اعتبرت منقولا، ومن ثم تصلح لأن تكون محلا لجريمة الإخفاء، بينما لا تعد جريمة إخفاء إذا لم يتم تخزينها على دعامة وظلت مختزنة على الشبكات.

الفرع الثاني: العقوبات المقررة لجرائم التكنولوجيا الحديثة

نظرا لخطورة هذه الجرائم المتصلة بالتكنولوجيا الحديثة فقد سعي المشرع الجزائري للحيلولة دون وقوعها، إذ قام بتجريم مراحل متقدمة يمر بها الجاني قبل أن يصل إلى المرحلة النهائية وارتكاب الجريمة كاملة، ومن الأفعال التي جرمها المشرع وقرر العقاب على مرتكبيها، الاتفاق الجنائي على التحضير والإعداد لارتكاب هذه الجرائم إذا تجسد بفعل أو أفعال مادية، ونعلم أن المشرع يعاقب على الاتفاق الجنائي في الجنايات إلا أنه ورغبة منه في مكافحة هذه الجرائم بصفتها جنحا فكان لابد من النص عليه، ونفس الأمر بالنسبة للشروع حيث أن الشروع في الجنح لا يكون إلا بنص صريح، إضافة إلى ذلك فقد نص المشرع الجزائري على مساءلة الأشخاص المعنوية في ارتكابهم لمثل هذه الجرائم لأن هذه الأخيرة محصورة في الحالات التي يحددها القانون، وضاعف في العقوبة في حالة ارتكابها من طرف هذه الأخيرة.

والهدف من العقاب على هذه الجرائم هو حماية المصالح المحمية (البرامج والمعلومات)، ولم يحدد المشرع نوعا معينا من المعلومات والبرامج أو الجهة التي تنتمي لها هذه الأخيرة، إلا أنه عزز حماية المعلومات التي تتعلق بالدفاع الوطني أو الجهات العامة نظرا لتعلقها بالمصلحة العامة، فشدد العقوبة إلى ضعف العقوبة المقررة للشخص الطبيعي، فضلا عن العقوبات الأصلية التي قررها المشرع لهذه الجرائم فقد قرر عقوبات تكميلية تتمثل في المصادرة والغلق.

البند الأول: نطاق العقوبة

تشترك جرائم التكنولوجيا الحديثة في شرط تواجد نظام المعالجة الآلية للمعطيات، كما أنها تشترك في أن المشرع وضع عقوبات تكميلية واحدة لكل منها، وقد عاقب على الاتفاق الجنائي المجسد في أعمال مادية وكذا العقاب على الشروع في هذا النوع من الجرائم، وفيما يلي سنتطرق إلى مجمل هذه الأحكام المشتركة.

أولا: العقاب على الاتفاق الجنائي في جرائم التكنولوجيا الحديثة، قبل التفصيل في هذا العنصر نتطرق أولا للجدل الفقهي الذي دار حول مدى ملائمة تجريم المشرع الجزائري للاتفاق الجنائي من عدمه، حيث ظهر هناك اتجاهان؛ فذهب اتجاه إلى القول إن الاتفاق الجنائي عزم إجرامي، وتجريمه لا يعتبر استثناء يرد على قاعدة عدم العقاب على مجرد العزم الإجرامي، ويستند هذا الرأي إلى أن المشرع لا يعاقب على الاتفاق الجنائي كخطوة للجريمة المتفق عليها، وإنما يعاقب عليه في حد ذاته كجريمة خاصة تامة وتبرير المعاقبة عليه أنه في الاتفاق الجنائي يظهر العزم الجنائي الجماعي بمظهر خارجي مادي، لأن كل عضو فيه يعلن عزمه إلى سائر

الأعضاء فتتحد إرادتهم على ارتكاب الجريمة، وبذلك يكون الاتفاق معلوما ويمكن إثباته، ومن جهة ثانية؛ الاتفاق الجنائي ظاهرة خطرة تهدد الأمن العام تهديدا فعليا، كما أن هدف المشرع من العقاب على الاتفاق هو الوقاية، لأن نتيجة إحباط الاتفاق الجنائي هي الحيلولة بين الجناة وتحقيق خططهم الإجرامية[1].

في حين يرى اتجاه آخر أن تجريم مجرد الاتفاق فقط ستكون له انعكاسات سلبية، ذلك لما يخلقه من دفع للمجرمين بإتمام ما تم الاتفاق عليه نظرا لأن اتفاقهم قد تم تجريمه، حيث أن العدول عن هذا الاتفاق وفقا للرأي السابق لا يمنع من تقرير العقوبة لأن الاتفاق حسبهم جريمة مستقلة بذاتها لذلك ذهب هذا الاتجاه للقول بأن حجج الرأي السابق غير قويمة ويكفي لدحضها جميعا المقارنة بين خطورة الاتفاق الجنائي على نحو ما صوره أصحاب الاتجاه السابق، وبين خطورة الأعمال التحضيرية التي تصدر عن شخص يسعى إلى ارتكاب الجريمة بمفرده، فالاتفاق الجنائي يكون في مرحلة مبكرة بالنسبة للتحضير للجريمة، إذ أنها ترد إلى المرحلة النفسية أي إلى مرحلة اتخاذ القرار وعقد العزم على ارتكاب الجريمة، بينما التحضير للجريمة يعقب هذه المرحلة النفسية، لهذا لو صحت خطورة الاتفاق الجنائي تبريرا لمعاقبة المتفقين في هذه المرحلة المبكرة من المراحل التي تمر بها الجريمة لوجب على المشرع أن يجرم مرحلة التحضير للجريمة من باب أولى[2]، وذلك ما سار عليه المشرع الجزائري والفرنسي من خلال اشتراطهما أن يكون التحضير مجسدا بأفعال مادية، أي تجنب المشرع العقاب على المرحلة النفسية، وذلك ما نص عليه في جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات، وللإحاطة أكثر بجريمة الاتفاق الجنائي في جرائم التكنولوجيا الحديثة نتناولها من خلال التطرق لكل من الركنين المادي والمعنوي لهذه الجريمة.

1- **الركن المادي للاتفاق الجنائي**، لتناول الركن المادي لهذه الجريمة نتطرق لثلاث عناصر تتمثل في فعل الاتفاق وموضوع الاتفاق وتعدد المتفقين.

أ- فعل الاتفاق، تضمنت المادة 176 ق.ع بقولها: "كل جمعية أو اتفاق مهما كانت مدته وعدد أعضائه تشكل أو تؤلف بغرض الإعداد لجناية أو أكثر، أو لجنحة أو أكثر معاقب عليها بخمس (05) سنوات حبس على الأقل ضد الأشخاص أو الأملاك تكوين جمعية أشرار، وتقوم هذه الجريمة بمجرد التصميم المشترك على القيام بالفعل"، والمشرع الجزائري لم يخضع فعل الاتفاق في مجال المعاملات الإلكترونية لنص المادة السابقة الذكر وإنما أخضع الفعل لنص المادة 394 مكرر 5 ق.ع[3].

ويستشف من نص المادة 176 ق.ع، أن فعل الاتفاق هو انعقاد إرادتين أو أكثر واجتماعهما على موضوع معين وللاتفاق بطبيعته مظهر مادي ملموس، إذ يفترض تعبير كل واحد من أطرافه عن إرادته بحيث يعلم بها زملاؤه في الاتفاق فيتحقق لهم أن إرادتهم تسير في اتجاه واحد وتتلاقى عند موضوع معين، والتعبير عن الإرادة يفترض ماديات كالقول الشفوي أو العبارات المكتوبة أو الإيماء إن كانت لها دلالة مفهومة، والاتفاق يقوم بغض النظر عما استغرقه انعقاد الإيرادات من وقت؛ قصيرا كان أم

[1] محمد خليفة، المرجع السابق، ص112.

[2] محمد خليفة، المرجع نفسه، ص113.

[3] أمال قارة، المرجع السابق، ص130.

طويلا، وسواء كان الاتفاق منظما مفصلا فيتخذ شكل الجمعية الإجرامية، أو اقتصر أعضاؤه على مجرد العزم على جريمة معينة دون تعيين لكيفية تنفيذها أو تحديد لكل دور منهم فيها[1].

تجدر الإشارة في هذا الصدد أن المادة 394 مكرر 5 لم تكتف بمجرد الاتفاق بل اشترطت أن يكون التحضير أو الاتفاق مجسدا بفعل أو عدة أفعال مادية، حيث تنص المادة 394 مكرر 5 ق.ع على أنه: "كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها"، أثارت هذه المادة جدلا فقهيا حول مدى تحقق الأعمال المادية في صورة بدء تنفيذ الأعمال التحضيرية، مما استوجبهم إعطاء مفهوم أوسع للمادية لأن مجرد تبادل المعلومات في صورة مناسبة قد يعد كافيا لتحقيق هذه الجرائم[2].

ومن أمثلة الأعمال التحضيرية في مجال المعلوماتية تبادل المعلومات الهامة لارتكاب الجريمة كالإعلان عن كلمة المرور، أو رمز الدخول (Code d'accès)...إلخ[3].

ومن جانبنا نرى ضرورة تأييد الرأي الفقهي القائل بتوسيع نطاق الأفعال المادية، ليدخل في نطاقه مجرد تبادل المعلومات متى كان لها دورا في الجريمة، كما أن فعل الاتفاق يمكن أن يمتد ليشمل كل من يساهم في المساعدة أو الاتفاق، الأمر الذي يجعل من الممكن أن تكون هناك جماعة مساهمة في تحقيق هذه الجرائم شرط أن تمارس نشاط إيجابي، وفي هذه الحالة فإن العقاب لن يشمل رئيس الجماعة فقط يمتد لكافة أفرادها.

من خلال ما سبق؛ تجدر الإشارة إلى أنه يجب التمييز بين الركن المادي لجريمة الاتفاق والركن المادي للجريمة المتفق عليها لأن الركن المادي للجريمة لأولى يستكمل عناصره بتوافر الإرادات ولو لم تنفذ الجريمة المتفق عليها، وأن عدولهم عن تنفيذها لا يحول دون العقاب على جريمة الاتفاق الجنائي، لأن هذا العدول لا يمس الركن المادي الذي توافرت كل عناصره.

ب- موضوع الاتفاق: يستمد الاتفاق صفته الجنائية من موضوعه، فإذا لم تكن لموضوعه صفة إجرامية أي كان فعلا مشروعا ولم تكن له صلة بجريمة ما، فليس الاتفاق جنائيا والملاحظ أن نص المادة 176 ق.ع، الذي نص على الاتفاق الجنائي العام في الجنايات ضد الأشخاص والأموال يجرم الاتفاق المنصب على ارتكاب جريمة أو الإعداد لها، بينما اقتصر نص المادة 394 مكرر 5 على تجريم الاتفاق على أعمال الإعداد والتحضير لجرائم التكنولوجيا الحديثة دون الاتفاق على ارتكابها[4].

ووفقا للمادة 394 مكرر 5 فإنه إذا كان موضوع الاتفاق أعمال التحضير والإعداد لتلك الجرائم فإن الاتفاق يكتسب صفته الجنائية ولو كانت الأعمال في ذاتها مشروعة[5]، فالاتفاق على تعليم كيفية تصميم المعطيات وتجميعها ونشرها هو اتفاق مشروع في الأصل، لكنه يصبح غير مشروع إذا كان الاتفاق على تعليم ذلك بغية استعماله في الجرائم التي تنص عليها المادة 394 مكرر

---

[1] محمد خليفة، المرجع السابق، ص113.

[2] عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا، دراسة مقارنة، المرجع السابق، ص102.

[3] أمال قارة، المرجع السابق، ص132.

[4] محمد خليفة، المرجع السابق، ص115.

[5] أمال قارة، المرجع السابق، ص132.

02[1]، وموضوع الاتفاق أو محله الذي نصت عليه المادة 394 مكرر5 هو الإعداد لأي من الجرائم التي نصت عليها المواد 394 مكرر والخاصة بالدخول والبقاء غير المصرح بهما والمادة 394 مكرر 1 الخاصة بالتلاعب بالمعطيات والمادة 394 مكرر 2 المتعلقة بالمساس بحقوق الأشخاص عن طريق المعلوماتية، كجمع المعلومات أو نشرها أو الاتجار فيها أو إفشائها.

فالاتفاق يكون بهدف التحضير لارتكاب إحدى الجرائم المنصوص عليها والمتصلة بالتكنولوجيا الحديثة، ويترتب على ذلك أنه يخرج من إطار تطبيق هذا النص حالة النوادي المعلوماتية، لأن هذه النوادي يمارس داخلها الأعضاء هواياتهم المتصلة بالمعلومات بطريقة قد توحي في بعض الأحيان بأنها تنم عن الاتفاق لارتكاب جريمة ما، أو المساعدة على ارتكابها، ويرجع عدم تطبيق هذا النص عليها لأن هذا الاتفاق لا يتم بقصد ارتكاب إحدى هذه الجرائم، ومن جهة أخرى فإنه لا مجال لتطبيق هذا النص إذا كان الاتفاق قد تم بغرض ارتكاب جريمة غير واردة بالنصوص المعنية في المواد 394 مكرر إلى 394 مكرر 2 ق.ع[2].

ج- تعدد الجناة: تتطلب جريمة الاتفاق تعددا ضروريا للجناة والحد الأدنى لهذه التعداد هو شخصان بينما لا يرد قيد على الحد الأقصى حسب نص المادة 176 ق.ع، ويستوي أن يكون أعضاء الاتفاق في صورة شركة أو مؤسسة أو شخص معنوي أو جماعة، كما يستوي أن يعرف أشخاص الاتفاق بعضهم البعض كما في العصابة أم تكون مجرد مجموعة من الأشخاص لا يعرف أحدهم الآخر من قبل ولكن اتفقوا فيما بينهم على القيام بالنشاط الإجرامي، والمهم في ذلك أن يتم الاتفاق بين شخصين على الأقل، فإذا ارتكب العمل التحضيري المادي شخص واحد بمفرده وبمعزل عن غيره فلا يعاقب في هذه الحالة على الاتفاق، فالعقاب لا يتقرر إلا في حالة اجتماع شخصين أو أكثر[3]، ويجب أن يكون الشخصان المتفقان مسؤولان جنائيا، فإذا كان أحدهما غير مسؤول جنائيا كأن يكون صغيرا أو فاقدا للإدراك والتمييز لتعاطيه مسكرا دون علم منه أو مجنونا فلا يقوم الاتفاق.

2- الركن المعنوي للاتفاق الجنائي، جريمة الاتفاق جريمة عمدية لابد لقيامها من توافر القصد الجنائي وهذا الأخير يقوم على عنصري العلم والإرادة.

أ- العلم، يجب أن يعلم كل عضو في الاتفاق بماهية الفعل أو الأفعال موضوع الاتفاق وبما لها من خصائص التي يعتمد عليها المشرع في إضفاء الصفة الإجرامية عليها، يترتب على ذلك أن من يجهل الغرض من الاتفاق وهو ارتكاب جناية أو جنحة أو التحضير لهما لا يعد القصد الجنائي متوافرا لديه، فمن ينضم إلى اتفاق معتقدا أنه للاتجار في برامج ومعطيات عادية ثم يتبين أن الاتجار كان ببرامج خبيثة أو برامج اختراق، فمثل هذا لا يعد القصد الجنائي متوافرا لديه وذلك لانتفاء علمه بموضوع الاتفاق الجنائي لكن القصد الجنائي يتوافر لدى هذا الشخص إذا علم بعد دخوله الاتفاق بموضوعه غير المشروع ومع ذلك بقي في الاتفاق[4]، فيجب أن يكون الشخص على وعي بأنه يساهم في مساعدة ما بغرض ارتكاب إحدى الجرائم المنصوص عليها[5].

---

[1] محمد خليفة، المرجع السابق، ص115.

[2] عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا، دراسة مقارنة، المرجع السابق، ص102.

[3] أمال قارة، المرجع السابق، ص131.

[4] محمد خليفة، المرجع السابق، ص117.

[5] عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا، دراسة مقارنة، المرجع السابق، ص122.

ب– الإرادة، لا بد أن تتوافر الإرادة الجادة لشخصين على الأقل للدخول والاتفاق، أي إرادة كل واحد أن يكون طرفا في هذا الاتفاق وأن يقوم بالدور الذي سيعهد به إليه فلابد أن تكون هذه الإرادة جادة، فالذي يدخل الاتفاق بقصد الوشاية ببقية المتفقين أو للإطلاع على أمرهم، لا يعد القصد الجنائي متوافر لديه لغياب الإرادة الجادة[1].

يجب أن تتجه إرادة كل عضو إذن إلى تحقيق نشاط إجرامي معين يتمثل في العمل التحضيري لتلك الجريمة أي النشاط المادي لفعل الاتفاق، ومما سبق تناوله في الركن المادي أو الركن المعنوي يتبين أن الحكمة التي ارتآها المشرع من تجريم الاشتراك في مجموعة أو اتفاق بغرض الإعداد لجريمة متصلة بالتكنولوجيا الحديثة هو أن مثل هذه الجرائم تتم عادة في إطار مجموعات، كما أن المشرع ورغبة منه في توسيع نطاق العقوبة أخضع الأعمال التحضيرية التي تسبق البدء في التنفيذ للعقوبة إذا تمت في إطار اتفاق جنائي، بمعنى آخر أن الأعمال التحضيرية المرتكبة من طرف شخص منفرد غير مشمولة بالنص.

ويعاقب المشرع الجزائري على الاشتراك في الاتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها فإذا تعددت الجرائم التي يتم التحضير لها تكون العقوبة هي عقوبة الجريمة الأشد[2]، كما أن العقوبة تطبق في حالة عدم إتمام الجريمة التي تم الإعداد لها وذلك استنادا إلى أن جريمة الاتفاق تعد جريمة مستقلة بذاتها عن الجرائم الأخرى وتقوم بمجرد الاتفاق دون الإتمام.

ثانيا: العقاب على الشروع الجنائي في جرائم التكنولوجيا الحديثة، إذا كانت العلة من العقاب على أية جريمة هي أنها تحقق عدوانا على المصالح محل الحماية القانونية فإن العلة من العقاب على الشروع بوصفه جريمة لابد أن يأخذ في الشروع صورة الخطر الذي يهدد المصالح القانونية، ذلك أن المشرع لا يحمي المصالح القانونية من الضرر الذي ينزل بها فيقضي عليها جزءا أو كلا فحسب وإنما يوفر لها حماية لإزالة الخطر الذي يهددها لاحتمال القضاء عليها كلها، فلقد ثبت أن خطر الجريمة لا يقتصر على ما تحدثه من ضرر مادي بالفرد بل يتعدى ذلك إلى ما تحدثه من قلق واضطراب في الجماعة أيضا[3].

ومن المعلوم أن مجال نظام الشروع الأصلي هو الجنايات أما الجنح فلا يكون إلا في الخطيرة منها، وقد تعرض المشرع الجزائري للشروع تحت عنوان المحاولة، وذلك في المادة 30 ق.ع التي تنص على أنه: "كل محاولات لارتكاب جناية تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة إلى ارتكابها تعتبر كالجناية نفسها إذا لم توقف أو لم يخب أثرها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها حتى ولو لم يمكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها"، ونصت المادة 31 ق.ع على "المحاولة في الجنحة لا يعاقب عليها إلا بناء على نص صريح في القانون، والمحاولة في المخالفة لا يعاقب عليها إطلاقا".

ونظرا لخطورة جرائم التكنولوجيا الحديثة فقد أخضعها المشرع لنظام الشروع وذلك في نص المادة 394 مكرر 7 حيث نصت على: "يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقرر للجنحة ذاتها"، ثم أخضعها لنظام الشروع أيضا، لذلك سنتطرق لأركان الشروع، ثم للشروع في الاتفاق الجنائي وذلك على الشكل التالي:

1– أركان الشروع، تقوم جريمة الشروع كغيرها من الجرائم على كل من الركن المادي والركن المعنوي.

---

[1] محمد خليفة، المرجع السابق، ص117.

[2] أمال قارة، المرجع السابق، ص130.

[3] محمد خليفة، المرجع السابق، ص117.

أ– الركن المادي، يتمثل الركن المادي لجريمة الشروع أساسا في الأفعال المادية التي تمر بها هذه الجريمة، أي المراحل المجسدة في نشاط مادي دون المعنوي فمرحلة التفكير في الجريمة لا عقاب عليها، فمن يفكر في ارتكاب جريمة متصلة بالتكنولوجيا الحديثة وكانت هذه الجريمة في مرحلة التفكير وطي الكتمان دون أن تتخذ مظهرا خارجيا بارتكاب أي فعل يقع تحت طائلة القانون، كالبدء في التنفيذ أو غير ذلك من الأعمال الخارجية فإن الفعل يخرج عن دائرة التجريم والعقاب، وهو ما ينطبق أيضا على مرحلة التحضير للجريمة فهي كمرحلة التفكير لا عقاب عليها ما لم تشكل هذه الأعمال جريمة قائمة بذاتها.

فالعقاب هنا يستند على تحضير تجهيزات لارتكاب جريمة متصلة بالتكنولوجيا الحديثة، كإعداد البرامج المستخدمة مثل الفيروس أو برامج معدة للقرصنة المعلوماتية أو لسرقة المعلومات بطريقة النسخ غير المشروع عن طريق النهايات الطرفية للشبكة المعلوماتية، أو إعداد مادة حامضة لوضعها على الشرائط الممغنطة لتلفها، والقاعدة العامة هنا أنه لا عقاب على هذه الأعمال لأنها لا تعد شروعا.

لكن الأفعال سابقة الذكر متى تجسدت في شكل مادي، أي أن يكون ذلك التحضير متبوعا بأعمال مادية فإنه يدخل في نص المادة 394 مكرر 5 حيث يتخذ ذلك التحضير صورة الاتفاق الجنائي، ويجد الركن المادي للشروع ضالته في مرحلة البدء في التنفيذ، فإذا تمكن الجاني من تحقيق النتيجة الإجرامية فإن الجريمة تكون قد وقعت تامة، وإذا لم يتمكن من تحقيق النتيجة لظرف طارئ خارج عن إرادته فإن الشروع يكون متحققا في هذه الحالة، وإذا عدل الجاني من نشاطه الإجرامي بإرادته فإن هذا يعد عدولا اختياريا ولا عقاب على ذلك، وقد يحدث العدول الاختياري في نطاق المعاملات الإلكترونية كما لو قام الجاني بإعداد الأجهزة التي سوف يستخدمها في جريمة تزوير مستند معالجا آليا أو برنامجا محضرا للاعتداء على شبكة معلوماتية، وقبل أن يدخل بفعله حيز التنفيذ يعدل عن الجريمة بإرادته الحرة فلا عقاب في هذه الحالة، فالشروع هنا هو جريمة ناقصة، وهذا النقصان لا يعتري الركن المعنوي فيها لأن القصد ثابت لدى الفاعل وإنما يعتري الركن المادي؛ لأن الفاعل يقدم على أفعال تعتبر بدءا في التنفيذ لكنه لا يتمكن من تحقيق النتيجة لأسباب خارجة عن إرادته[1].

ب– الركن المعنوي، لا يكفي الشروع في ارتكاب جريمة متصلة بالتكنولوجيا الحديثة بركنها المادي فقط وإنما يلزم مع ذلك توافر الإرادة التي تنصرف إلى ارتكاب الجريمة، ويعتد في هذا القصد أن يكون معاصرا للبدء في التنفيذ فلا يعتد بالقصد السابق أو اللاحق على هذه المرحلة، ويشترط في الركن المعنوي للشروع أن تكون نية الجاني قد اتجهت إلى تحقيق جريمة معينة وفي مجال المعاملات الإلكترونية وأن تتجه نيته إلى إحداث جريمة من الجرائم المنصوص عليها في القانون، وعلى ذلك فإنه لا يتصور الشروع في حالة قيام عامل بإتلاف بعض البيانات عن طريق الخطأ وذلك أثناء أدائه لوظيفته والعلة في ذلك أن النتيجة المتحققة لم يكن يريدها العامل المتسبب فيها.

تجدر الإشارة هنا لنقطة مهمة لهذه الجريمة أثناء وقوعها على الجرائم المتصلة بالتكنولوجيا الحديثة، فالشروع وفقا للقواعد العامة غير متصور في الجرائم الشكلية، والمعلوم أن جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي هي جريمة شكلية حيث لا يتطلب لتمامها نتيجة معينة فمجرد الدخول أو البقاء يعد جريمة، أما الجرائم الواقعة بعد الدخول أو البقاء كتغيير المعطيات أو

[1] عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا، دراسة مقارنة، المرجع السابق، ص112 و114.

حذفها فقد اعتبرها المشرع ظرفا مشددا، فبالرغم من أن هذه الجرائم جرائم شكلية؛ إلا أن المشرع وضع للشروع فيها عقوبة تساوي عقوبة الجريمة ذاتها، والسبب في ذلك هو رغبة المشرع في توسيع نطاق العقوبة لتشمل العديد من الأفعال الماسة بالأنظمة المعلوماتية ورغبة منه أيضا في حماية المعاملات الإلكترونية نظرا لما تمتاز به من خصائص تختلف عن المعاملات العادية وذلك لما قد تلحقه من أضرار اقتصادية كبيرة نتيجة التعدي عليها، فالمشرع لا يقرر نظام الشروع في الجنحة إلا إذا لمس خطورتها وما يمكن أن تؤدي إليه من أضرار حال تمامها، وتبدو رغبة المشرع كبيرة في حماية المعاملات الإلكترونية وذلك في خروجه عن المبدأ العام لنظام الشروع الذي تكون عقوبته أقل في مقدراها من عقوبة الجريمة التامة، إلا أنه في مجال المعاملات الإلكترونية ساوى بين عقوبة الشروع وجرائم المساس بأنظمة المعالجة الآلية للمعطيات.

2- الشروع في الاتفاق، تكلم المشرع الجزائري عن الجرائم المتصلة بالتكنولوجيا الحديثة؛ وتناول معها جريمة الاتفاق الجنائي ثم أنهى النصوص العقابية بالنص على تجريم الشروع في الجرائم السابقة، وذهب الرأي الراجح في الفقه بالقول بأنه لا يوجد شروع في الاتفاق الجنائي مستندا في ذلك على أن الاتفاق حالة نفسية تتم بتلاقي الإرادات ولا تحمل بداية ولا نهاية، فهو لا يقع إلا كلاما ولا يحتمل بدءا في التنفيذ.

ذهب بعض الفقه للقول بأن الدعوة إلى الاتفاق لا تعد شروعا إنما يعاقب عليها كجريمة قائمة بذاتها[1]، وهناك رأي مخالف يرى غير ذلك متحججا بأنه طالما كانت أركان الشروع متصورة ولم يكن القانون متضمنا نصا خاصا يقضي بعدم العقاب عليه فلا وجه للقول بالرأي السابق، فإذا توافر القصد الجنائي ولم يتم الاتفاق لأسباب لا دخل لإرادة الجاني فيها فالعقاب على الشروع متعين إذا كان الاتفاق جناية حتى ولو انعدم نصا خاصا يتطلب العقاب، وإذا كان الاتفاق جنحة فلابد من وجود هذا النص.

من خلال استقراء نص المادة 394 مكرر 7 ق.ع نستنتج أن الجنحة الواردة بنص المادة 394 مكرر 5 ق.ع، يشملها نص المادة 394 مكرر 7 أي أن المشرع الجزائري أخذ بفكرة الشروع في الاتفاق الجنائي، أي تصور قيام الشروع في جنة الاتفاق الجنائي، وهذا المسلك منتقد لدى البعض، فإذا كان تجريم الاتفاق الجنائي في حد ذاته منتقدا وقد حكم بعدم دستوريته في مختلف التشريعات، وأنه يعاقب على مجرد العزم، فإن العقاب على مجرد الشروع في هذا الاتفاق أو العزم على العزم إن صح التعبير هو منتقد بصورة أشد، لأن المشرع هنا يقوم بالتجريم في مرحلة متقدمة جدا وهي الإرادة، هذه الإرادة التي لم تلتق مع إرادات أخرى لأنها لو التقت بإرادات أخرى لكان الاتفاق مكتملا وكأن المشرع بهذا قد اقترب من تجريم مجرد النوايا[2].

لكن ما تجدر الإشارة إليه أن المشرع الجزائري لم يعاقب على الاتفاق في المرحلة الأولى وإنما عاقب على الاتفاق المجسد بأعمال مادية حسب نص المادة 394 مكرر 5، لكن بتبنيه لنظام الشروع بعد الحديث عن الاتفاق الجنائي يمكن القول إن المشرع تبنى فكرة الشروع في الشروع، فالشروع نجده في كل الجرائم سواء الجرائم التقليدية أو تلك المتصلة بالتكنولوجيا الحديثة، لذلك ارتأينا أن نتكلم عن أهم الجرائم الواقعة في مجال المعاملات الإلكترونية، ثم نختم الحديث عنها بالتطرق لكل من الاتفاق الجنائي والشروع

[1] محمد خليفة، المرجع السابق، ص118.

[2] محمد خليفة، المرجع نفسه، ص119.

أين عالجه المشرع الجزائري وكفل بذلك الحماية للمعاملات الإلكترونية من خلال تجريمه لمجرد البدء في هذه الجرائم، إلا أنه لم يراعي في تلك النصوص أخذه بفكرة الشروع في الاتفاق الجنائي.

البند الثاني: مضمون العقوبة

إن تحليلنا للعقوبات المقررة –في قانون العقوبات– للجرائم المنصوص عليها في هذا القسم لا يكون مجرد دراسة وصفية تحليلية للنصوص المتضمنة لهذه العقوبات، بل سنحاول تحليلها للوصول إلى السياسة العقابية التي انتهجها المشرع لمواجهة والحد من هذه الجريمة المتصلة بالتكنولوجيا الحديثة، سواء كانت هذه العقوبات مقررة للشخص الطبيعي أو المعنوي، ونحن هنا نركز دراستنا على قانون العقوبات دون غيره من القوانين ذات الصلة بالجرائم المتصلة بالتكنولوجيا الحديثة.

أولا: العقوبات المقررة للشخص الطبيعي، لقد قرر المشرع الجزائري في قانون العقوبات؛ عقوبات أصلية وأخرى تكميلية للشخص الطبيعي وتختلف العقوبات الأصلية بحسب الجريمة المرتكبة المنصوص عليها في القسم السابع مكرر، أما العقوبات التكميلية فهي من الأحكام المشتركة في جرائم هذا القسم.

1– العقوبات الأصلية، إن العقوبات الأصلية المطبقة تمثل المؤشر الصريح للخطورة التي يضفيها المشرع على الأفعال التي يجرمها في قانون العقوبات، وعليه سنتعرض بالتدرج في هذه الجرائم حسب العقوبات المقررة لها.

أ– العقوبات المقررة لجرائم الاعتداء على سير النظام، سنتناول العقوبات المقررة لكل من جريمتي الدخول والبقاء غير المشروع سواء في صورتها البسيطة أو المشددة أولا، ثم جريمة الاعتداء على سير النظام ثانيا.

– عقوبة جريمة الدخول أو البقاء غير المشروع، تقرر الفقرة الأولى من المادة 394 مكرر ق.ع، عقوبتان أصليتان لجريمة الدخول أو البقاء غير المشروع في صورتها البسيطة.

• **عقوبة الجريمة في صورتها البسيطة**، يعاقب المشرع الجزائري على هذه الجريمة بالحبس من ثلاثة أشهر إلى سنة، والغرامة من خمسين ألف 50.000 دج إلى مائتي ألف 200.000 دج، وترك المشرع للقاضي السلطة التقديرية بأن جعل له حدا أدنى وحدا أقصى في تقدير العقوبة بحسب الوقائع المعروضة أمامه، حيث يختلف الباعث من شخص لآخر، لهذا وجب اختلاف التقدير[1].

• **عقوبة الجريمة في صورتها المشددة**، ضاعفت الفقرتان الثانية والثالثة من المادة 394 ق.ع، عقوبة جريمة الدخول أو البقاء غير المشروع إذا ترتب على هذا الأخير إما حذف أو تغيير للمعطيات، سواء في حدها الأدنى الذي أصبح ستة أشهر بعدما كان ثلاثة أشهر، أو في حدها الأقصى إلى سنتين بعدما كان سنة واحدة، أما بالنسبة للغرامة فتصبح 50.000 دج إلى 300.000 دج، أما إذا حدث تخريب لنظام المعالجة الآلية فتكون العقوبة بالحبس من ستة أشهر إلى سنتين، أما الغرامة من 50.000 دج إلى 300.000 دج، حيث ثبت الحد الأدنى للغرامة وارتفع حدها الأقصى وفقا للفقرة 03 من المادة 394 مكرر.

– عقوبة جريمة الإفساد أو تعطيل سير النظام، إذا كانت جريمة الاعتداء العمدي على المعطيات مثلها مثل جريمة الاعتداء العمدي على نظام المعالجة الآلية للبيانات تهدف إلى أفعال التخريب والقرصنة فإن التمييز بينهما ليس بالأمر السهل، ذلك

[1] محمد خليفة، المرجع السابق، ص171.

أن جريمة الاعتداء العمدي على النظام وإن كانت لا تقع بصفة أساسية على البرامج والشبكات إلا أنها تصيب المعطيات كنتيجة لأفعال الإفساد والتعييب والتوقيف، وبالمقابل فالاعتداء على المعطيات الذي تقوم عليه جريمة الاعتداء العمدي على المعطيات قد يؤثر على صلاحية النظام للقيام بوظائفه سواء على البرامج أو شبكات النقل والاتصال

وقد حاول الفقه[1] وضع معيار للتفرقة بين هاتين الجريمتين على أساس المحل الذي يقع عليه الاعتداء، فإذا كان الفعل يقع على العناصر المادية للنظام فإن الجريمة هي الاعتداء العمدي على نظام المعالجة الآلية للمعطيات، أما إذا كان الفعل يقع على العناصر المعنوية فإننا نكون أمام جريمة الاعتداء العمدي على المعطيات.

إلا أن هذا المعيار غير دقيق لذلك يقترح البعض[2] معيارا آخر يقوم على أساس ما إذا كان هذا الاعتداء غاية أو وسيلة فإذا كان الاعتداء الذي تم على المعطيات ما هو إلا وسيلة للوصول إلى الغاية وهو النظام، فالجريمة هنا هي جريمة الاعتداء العمدي على النظام، أما إذا كان الاعتداء على المعطيات هو الغاية فنكون أمام جريمة الاعتداء العمدي على المعطيات وهذا هو المعيار الصحيح من حيث المنطق، وفي جميع الأحوال لا يثير هذا التمييز أي إشكال وليس له أهمية تذكر لأن العقوبة المقررة لكل منهما واحدة، ويخضعان لأحكام مشتركة وقواعد عامة واحدة.

ب–العقوبات المقررة لجرائم الاعتداء على المعطيات، سنتناول العقوبات الأصلية التي قررها المشرع لكل من جريمتي الاعتداء العمدي على المعطيات الموجودة داخل النظام ثم العقوبات الأصلية لجريمة التعامل غير المشروع في المعطيات.

– عقوبة جريمة الاعتداء العمدي على المعطيات الموجودة داخل النظام، نصت المادة 394 مكرر1 ق.ع عن العقوبة الأصلية لمرتكب جريمة الاعتداء العمدي على المعطيات وهي الحبس من ستة أشهر إلى ثلاث سنوات وعقوبة الغرامة من 500.000 د.ج إلى 000 000 4 د.ج.

يلاحظ أن عقوبة الاعتداء العمدي على المعطيات تفوق عقوبة الدخول أو البقاء غير المشروع، سواء في صورتها المشددة أو البسيطة، حيث أن جريمة الدخول أو البقاء البسيطة لا تؤدي إلى أضرار معينة تلحق بالمعطيات أو النظام، أما صورتها المشددة وإن أدت إلى نفس النتائج التي تؤدي إليها جريمة الاعتداء العمدي على المعطيات فإن عقوبتها تبقى أكبر لأنها جريمة عمدية يجب توافر القصد الجنائي لدى مرتكبها بينما لا يتوافر هذا القصد لدى مرتكب جريمة الدخول أو البقاء غير المشروع في صورتها المشددة فالموقف النفسي اتجاه التلاعب بالمعطيات موجود في جريمة الاعتداء العمدي على المعطيات بينما ينتفي في جريمة الدخول أو البقاء المشددة.

– عقوبة جريمة التعامل غير المشروع بالمعطيات، نصت المادة 394 مكرر 2 على عقوبتان أصليتان هما الحبس والغرامة، وهذه العقوبة مقررة لكل من الصورتين.

1– **العقوبات الأصلية،** تتمثل العقوبة الأصلية في الحبس من شهرين إلى ثلاث سنوات وبغرامة من 100.000دج إلى 10.000.000 دج، وعليه يكون ترتيب هذه الجرائم من حيث العقوبة هو الثاني بين جريمتي الدخول أو البقاء غير المشروع سواء

[1] محمد خليفة، المرجع السابق، ص174.

[2] محمد خليفة، المرجع نفسه، ص173 و174.

في صورتها البسيطة أو المشددة وبين جريمة الاعتداء العمدي على المعطيات، إلا أن حدها الأدنى يقل عن كلتا الجريمتين بينما الحد الأقصى يزيد عن الحد الأقصى لجريمة الدخول أو البقاء غير المشروع في صورتيها ويبقى ترتيبها من حيث عقوبة الغرامة هو الأول حيث تفوق بكثير الجرائم السابقة.

2- العقوبات التكميلية، بالإضافة إلى العقوبات الأصلية المفروضة على مرتكبي الجرائم المتصلة بالتكنولوجيا الحديثة، قرر المشرع الجزائري عقوبات تكميلية تتمثل أساسا في المصادرة والغلق.

أ- المصادرة: تعرف المصادرة وفق المادة 15 ق.ع بأنها "الأيلولة النهائية إلى الدولة لمال أو مجموعة من أموال معينة أو ما يعادل قيمتها عند الاقتضاء"، فقد تكون المصادرة عامة؛ أي أيلولة كل أموال المحكوم عليه وإضافتها إلى ملكية الدولة، وقد تكون المصادرة خاصة؛ أي أيلولة مال من أموال المحكوم عليه وإضافتها إلى ملكية الدولة، وقد جاءت المادة 394 مكرر 6 ق.ع صريحة حيث يتم مصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب الجريمة، فالمصادرة هنا عينية رغم اتفاق المصادرة مع الغرامة، إذ تنص على أنه: "مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا للجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها"، فالمصادرة إذن هي نقل ملكية شيء مادي أو عيني مملوك للمحكوم عليه ونقله إلى الدولة، أما الغرامة هي تحميل ذمة المحكوم عليه بدين لها والمصادرة في الجرائم المتصلة بالتكنولوجيا الحديثة هي عقوبة تكميلية وجوبية ليس للقاضي السلطة التقديرية في الحكم بها.

نستنتج خلال نص المادة 394 مكرر6 ق.ع أنه لابد من توافر شروط معينة لتطبيق عقوبة المصادرة، وهي أن يحكم على المتهم بالعقوبة الأصلية بإحدى الجرائم المنصوص عليها في القسم الخاص بالاعتداء على أنظمة المعالجة الآلية للمعطيات، وأن تكون الأشياء التي تمت مصادرتها قد استخدمت في ارتكاب الجريمة، وتعتبر الأجهزة والبرامج واردة على سبيل المثال لا الحصر لأن المشرع استعمل مصطلح والوسائل المستخدمة، وبالتالي استيعاب كل الوسائل التي يمكن أن تستجد في ارتكاب هذه الجرائم سواء كانت وسيلة معلوماتية أو غير معلوماتية، ويجب أن تكون الأشياء المستخدمة مضبوطة حتى يمكن مصادرتها، سواء قدمها الجاني من تلقاء نفسه أو ضبطتها الشرطة، فلا يمكن مصادرة شيء غير مضبوط والحكم على الجاني بدفع قيمته.

ويجب ألا تخل المصادرة بحقوق الغير حسن النية، ويقصد به إذا كانت الوسائل المستخدمة مملوكة لغير المتهم، وهذا القيد نابع من الطبيعة القانونية للمصادرة كونها عقوبة، فلا بد أن تكون ذات طبيعة شخصية، والغير هنا هو كل أجنبي عن الجريمة تماما أي ليس فاعلا ولا شريكا وتثبت ملكيته للشيء المضبوط بشرط أن يكون حسن النية أي أنه يجهل أن هذه الوسائل قد تستخدم في ارتكاب الجريمة، أو على الأقل يعلم بذلك وبذل ما في وسعه للحيلولة دون استعمالها إلا أنها استعملت فعلا في ارتكاب الجريمة[1].

وحقوق الغير حسن النية غير قاصرة على حق الملكية فقط بل تمتد لتشمل أي حق عيني آخر على الشيء، كحق الانتفاع أو الرهن مثلا، أما الحقوق الشخصية فلا تحول دون المصادرة لأن محلها ذمة المدين وليس مالا معينا من أمواله حتى ولو كان الشيء المضبوط هو الضمان الوحيد له، ولا يهم إذا كان حق الغير حسن النية قد نشأ قبل أو بعد ارتكاب الجريمة ما دامت نيته حسنة

[1] محمد خليفة، المرجع السابق، ص121.

وقت ارتكاب الجريمة أو وقت نشأة حقه، وعليه فإذا كان للغير حسن النية حق على الأشياء المضبوطة كحق انتفاع مثلا أو رهن فلا يمكن الحكم بمصادرتها، وتحل الدولة محل المتهم فيصبح الغير حسن النية مالك على الشيوع مع الدولة، أو تنتقل الملكية للدولة مثقلة بحق الرهن أو الانتفاع في الحالة الثانية[1].

ب– الغلق: نصت المادة 394 مكرر 6 ق.ع إلى جانب عقوبة المصادرة، عقوبة الغلق كعقوبة تكميلية أخرى، وتشمل عقوبة الغلق، غلق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها في هذا القسم، كما يشمل الغلق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها.

والمقصود بالمواقع التي تكون محلا للجريمة إذا كانت هذه الأخيرة قد ارتكبت بعلم مالكها، تلك المواقع التي تقدم خدمات تسمح بالدخول غير المشروع لمختلف الأنظمة أو تسمح بالتلاعب بالمعطيات، وهناك مواقع تقوم بتعليم كيفية تصميم المعطيات غير المشروعة ونشرها والاتجار بها، أما المواقع التي تم الاعتداء عليها بالدخول غير المشروع أو التلاعب في معطياتها تعتبر هي الضحية في هذه الجرائم ولا يتصور غلقها، وكان من المستحسن استعمال عبارة المواقع التي تستعمل في ارتكاب الجريمة بدلا من المواقع محل الجريمة، لأن الأولى يقصد بها المواقع التي استعملت كوسيلة لارتكاب الجريمة، بينما الثانية هي المواقع التي وقعت عليها الجريمة[2].

إضافة إلى المواقع؛ يقع الغلق كذلك بالنسبة للمحل ومكان الاستغلال، أي المكان الذي استعمله الجناة لارتكاب الجريمة والذي يحوي الأجهزة التي استعملها في الدخول غير المصرح به أو التلاعب في المعطيات أو التعامل في معطيات غير مشروعة وبالنسبة لمدة الغلق لم تحدد المادة 394 مكرر 6 ق.ع مدة معينة، وعليه فهي تكون مؤقتة أو مؤبدة، وتشدد العقوبة في حالة ارتكاب الجريمة من طرف شخص معنوي أو إذا مست الجريمة الدفاع الوطني أو المؤسسات والهيئات العامة أي الجهات العامة.

ثانيا: العقوبات المقررة للشخص المعنوي، لقد تضمن تعديل قانون العقوبات الجزائري إقرارا للمسؤولية الجزائية للأشخاص المعنوية بنص عام وهو نص المادة 18 مكرر. ومن بين الجرائم التي يعاقب عنها الشخص المعنوي هي جرائم التكنولوجيا الحديثة، وقد شدد في عقوبة هذه الجرائم إذا ارتكبها شخص معنوي، أو كانت موجهة ضد الجهات العامة أي إذا كانت هذه المعطيات تابعة للدولة.

1–شروط تقرير المسؤولية الجزائية للشخص المعنوي: نصت المادة 394 مكرر 4 ق.ع على أنه: "يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمسة (05) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي".

جاءت المادة 51 مكرر ق.ع بنظام المسؤولية الجزائية للأشخاص المعنوية التي لا تستبعد الأشخاص الطبيعية فاعلين أو مساهمين الذين ارتكبوا نفس الوقائع، وعليه تنعقد المسؤولية الجزائية للشخص المعنوي عند قيامه بجرائم لها علاقة بالمجال الإلكتروني وفي إطار الاقتصاد الحالي تقوم الشركات بالبحث عن المعلومات بأية وسيلة، وهذا البحث يمكن أن يكون عن طريق الدخول أو البقاء غير المشروع في النظام المعلوماتي لشركة أخرى منافسة والإطلاع على ملفاتها وخططها، وبعد وجود المنتج المنافس تقوم

[1] محمد خليفة، المرجع السابق، ص121.

[2] محمد خليفة، المرجع نفسه، ص122.

بمنافستها على ذلك الأساس وبالتالي تقوم المنافسة غير المشروعة عن طريق ارتكاب جرائم متصلة بالتكنولوجيا الحديثة، إلا أن مسؤولية الأشخاص المعنوية بالنسبة لهذه الجرائم تطرح إشكالية تتعلق بجنحة الدخول غير المشروع قام بها شخص طبيعي على سبيل المثال، فهنا لا تستبعد المسؤولية الجزائية للأشخاص المعنوية الفاعلين أو المساهمين في نفس الوقائع.

شدد المشرع العقوبة على الشخص المعنوي لأن الكثير من الأشخاص المعنوية تنشأ بغرض تحقيق الربح فتقوم بالمنافسة غير المشروعة لمنافسيها عن طريق ارتكاب هذا النوع من الجرائم، حيث يتم الدخول إلى أنظمة الحاسبات المنافسة –كما قلنا سابقا– للإطلاع على ملفاتها وخططها ومنافستها بناء على ذلك، وقد يصل الأمر إلى حد التلاعب بمعطياتها[1].

أ– أنواع العقوبات المطبقة على الأشخاص المعنوية: إن العقوبة كانت من الحجج التي استند إليها المعارضون لمبدأ إقرار مسؤولية الشخص المعنوي، وذلك لأنهم رأوا أنه لا يمكن تطبيقها على هذا الأخير –خصوصا تلك السالبة والمقيدة للحرية– بعد اتساع عقوبة الغرامة وابتكار عقوبات جديدة تتلاءم وطبيعة الشخص المعنوي، ومن بين العقوبات المطبقة على الشخص المعنوي والتي نصت عليها المادة 18 مكرر ق.ع في مواد الجنايات والجنح ما يلي:

– الغرامة: نصت عليها المادة 394 مكرر 4 وهذه الغرامة ذات حد واحد وأوجبت الأخذ بالحد الأقصى لهذه العقوبة فيما يتعلق بالجرائم المتصلة بالتكنولوجيا الحديثة، والتي تساوي من مرة إلى خمس (05) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.

– واحدة أو أكثر من العقوبات التكميلية: تطبق حسب المادة 18 مكرر ق.ع واحدة أو أكثر العقوبات التكميلية التالية: حل الشخص المعنوي، غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس سنوات، المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر، أو غير مباشر، نهائيا أو لمدة لا تتجاوز خمس سنوات، مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نشأ عنها، نشر وتعليق حكم الإدانة، الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته.

ب– تشديد عقوبة الغرامة في جرائم التكنولوجيا الحديثة: تتمثل عقوبة الغرامة في مبلغ من المال يتم دفعه من قبل المحكوم عليه بها إلى خزينة الدولة، ولا حرج في الحكم بالغرامة على الشخص المعنوي ووفقا للمادة 18 مكرر ق.ع، فإن الغرامة تتراوح بين واحدة وخمس أضعاف تلك المقررة على الشخص الطبيعي، أما المادة 394 مكرر 4 من نفس القانون والتي تتعلق بعقوبة الغرامة على الشخص المعنوي في جرائم المعطيات فقد قيدت القاضي وألزمته بالحكم بالحد الأقصى لهذه الغرامة وهو خمسة أضعاف الغرامة المقررة على الشخص الطبيعي، هذا بالنسبة للجريمة المرتكبة من قبل الأشخاص المعنوية، أما إذا كانت الجريمة موجهة ضد الأشخاص المعنوية فقد قرر المشرع تشديد العقوبة في حالة ما إذا كان الضحية جهات عامة وهذا حفاظا على المصلحة العامة.

2– العقوبات المقررة في حالة الاعتداء على الجهات العامة: قد يشترط القانون بالنسبة لبعض الجرائم أن يكون موضوع النتيجة الإجرامية شيئا أو شخصا معينا تتوافر فيه صفات معينة حتى يقوم بتشديد العقوبة، أما فيما يتعلق بجرائم التكنولوجيا الحديثة نجد أن هذه المعطيات أو المعلومات قد تخص الأفراد أو شركات أو جهات معينة، ويأخذ المشرع في الاعتبار الجهة التي تتبعها

[1] محمد خليفة، المرجع السابق، ص124.

هذه المعطيات، ويولي اهتماما أكبر للمعطيات التي تتبع للدولة والجهات العامة، فهناك من المشرعين من يقصر الحماية على هذه الأخيرة دون المعطيات المتعلقة بالأفراد، إلا إذا كانت تمس بمصالح الدولة.

ونظرا لأن الاعتداء على المصلحة العامة أشد وأخطر من الاعتداء على المصالح الخاصة نجد تقدير مختلف التشريعات لذلك لاسيما إذا كانت هذه الجهة المعتدى عليها حساسة كالدفاع والأمن الوطنيين، وقد خطى المشرع الجزائري نفس المسلك حيث بسط حمايته على المعطيات بمختلف أنواعها والجهات التابعة لها، إلا أنه شدد العقوبة في حالة ما إذا كان الاعتداء على المعطيات يتعلق بالدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، وهذا ما جاء في المادة 394 مكرر 3 ق.ع، حيث نصت على أنه: "تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد"، ولقد خصت هذه المادة مؤسسة الدفاع الوطني نظرا لأهميتها في الحفاظ على سلامة التراب الوطني والأمن العام، وبالتالي خطورة الاعتداء على المعطيات التابعة لها، والحكمة من التشديد هو ما يتطلبه الأمر من وجوب العمل على سلامة وأمن القوة العسكرية والتي في حفظها وسلامتها حفظا وسلامة للدولة بأكملها[1].

كما شملت المادة كذلك الهيئات والمؤسسات التابعة للقانون العام، وشددت العقوبة إلى ضعف المطبقة على الاعتداء على المعطيات التابعة للأفراد العاديين وأشخاص القانون الخاص، أما إذا ما ارتكبت هذه الجريمة من طرف شخص معنوي على إحدى الجهات العامة فتضاعف العقوبات خمس مرات، أي مضاعفة الغرامة إذا ارتكبت الجريمة من طرف شخص معنوي على إحدى الجهات العامة عشر مرات الحد الأقصى من تلك المطبقة على الشخص الطبيعي.

[1] محمد خليفة، المرجع السابق، ص128.

خاتمة

إن الجرائم المتصلة بالتكنولوجيا الحديثة متميزة ومن نوع خاص تستهدف المعطيات ذات الطبيعة المعنوية، تتطلب في من يقترفها قدرا من الذكاء والمهارة الفنية والتقنية العالية التي تميزه عن غيره من المجرمين التقليديين الذين أضحت جرائمهم معروفة ومألوفة مما يستوجب تدخل المشرع الجنائي بنصوص جديدة من أجل القضاء على ظاهرة الإجرام التكنولوجي الحديث أو الحد منها بعد أن أصبحت بحق جرائم العصر، هذا التدخل تقتضيه السياسة الجنائية المعاصرة باعتبارها جوهر القانون الجنائي فهي التي تحدد المبادئ التي تسهل تنفيذ أهداف هذه السياسة الوقائية، العقابية والإصلاحية مما يستوجب تولي المشرع الجنائي صياغة النصوص التي تتناسب مع هذه الأخيرة، إذ يتوجب عليه الاتسام ببعد النظر والأخذ بمعيار التوقع والاحتمال لما تفرزه ثورة المعلومات التقنية والعلمية في المستقبل القريب.

لذا فإن المعيار المعتمد لتحقيق هذه المهمة الخطيرة والحساسة هو إيجاد النصوص الجنائية المناسبة وصياغتها بكل دقة من أجل معالجة ظاهرة الإجرام التكنولوجي الحديث، ومراعاة الخطورة الاجتماعية للفعل من جهة والفاعل من جهة أخرى، بناء على ذلك فإنه لا يهم أن يتحقق التجريم والعقاب سواء عن طريق تعديل نصوص قانون العقوبات أم إضافة نصوص جديدة له أم عن طريق إصدار قانون مستقل بجرائم التكنولوجيا الحديثة، فمفهوم هذه النصوص واحد وإن اختلفت مسمياتها مادام أنها صيغت وفقا لمبدأ شرعية الجرائم والعقوبات من جهة ومبدأ الشرعية الإجرائية من جهة أخرى.

لقد حاولت في هذه الدراسة تبيان الأحكام العامة لجريمة تكنولوجيا المعلومات الحديثة وملامح إطارها القانوني، ودراسة الأحكام الموضوعية للجرائم الناشئة عن استخدام هذه التقنية الحديثة بدءا من جرائم الاعتداء على حق الإنسان في سلامة الجسم والحياة وفي شرفه وسمعته وعدم مضايقته وحقه في حرمة حياته الخاصة، مرورا بالجرائم الجنسية، وانتهاء بجرائم الاعتداء على نظم المعلومات الإلكترونية، وجرائم التجسس والتحريض ضد أمن الدولة وإنشاء المواقع الإرهابية وتبادل معلومات الإرهاب عبر وسائل تقنية المعلومات الحديثة، من خلال بحث مدى كفاية النصوص الواردة في قانون العقوبات الجزائري ومواءمتها في الانطباق على هذه الجرائم، مع مقارنتها بما ورد في القوانين الحديثة ذات الصلة عند الاقتضاء.

وتباينت التعبيرات والاصطلاحات المستخدمة للدلالة على هذه الجرائم تباينا رافق مسيرة نشأة وتطور تلك التقنية، وأحاط بها الكثير من التساؤلات التي تتعلق بتحديد ماهيتها باعتبارها جريمة مستحدثة عن باقي الجرائم الكلاسيكية، وفي محاولة منا سد الفراغ التشريعي الذي أحدثته ثورة تكنولوجيا المعلومات التقنية نخلص إلى أهم النتائج التي توصلت لها الدراسة:

تكنولوجيا المعلومات الحديثة أو التقنية الحديثة، هي نظام إلكتروني يحقق نتيجة الدمج بين تقنية الحوسبة وتقنية الاتصال ذو قدرة على رقمنة الصوت والصورة وتحويلهما إلى مادة تفاعل بين المستخدم وبين المحتوى، والتعامل مع المعلومات إدخالا ومعالجة واسترجاعا ونقلا وتبادلا وتفاعلا، وتتمثل هذه التقنية بأي جهاز إلكتروني مغناطيسي، بصري، أو كهروكيميائي يتضمن نظام معالجة آلية للمعطيات ويكون مرتبطا بوسيط إلكتروني، بحيث يعد من وسائل تقنية المعلومات الحديثة كل جهاز تتوافر فيه البرمجيات المعطيات، والقدرة على القيام بالاتصالات.

ثمة مقبولية ومبررات لاستخدام اصطلاح جرائم تكنولوجيا المعلومات الحديثة أو جرائم تقنية المعلومات الحديثة، فهو اصطلاح شامل بدلالته التقنية الحديثة التي انتجها اندماج تكنولوجيا المعلومات مع تكنولوجيا الاتصالات، وبالتالي هو اصطلاح قادر على أن يطوي تحت جوانبه العديد من السلوكيات الضارة بالأفراد والجماعة، بالإضافة إلى غياب مفهوم عام متفق عليه بين الدول حول بيان مفهوم النشاط الإجرامي المتعلق بجرائم التكنولوجيا الحديثة والأنماط المكونة لها.

تبين من خلال دراسة خصائص الجريمة الإلكترونية أنها تتمتع بطبيعة قانونية مغايرة تماما للجريمة التقليدية، فهي تستهدف المساس بالمعلومات الإلكترونية المتواجدة في البيئة الرقمية على هيئة إشارات ونبضات غير مرئية تنساب عبر أجزاء النظام المعلوماتي وشبكات الاتصال العالمية.

نظرا لما تشكله جرائم التكنولوجيا الحديثة من خطورة من جهة، وقصور القوانين التقليدية أمام هذا النوع من الجرائم المستحدثة من جهة أخرى، فقد خصصت لها عدة تشريعات قوانين وهيئات لمكافحتها، كما فعل المشرع الجزائري حيث أصدر قانون يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

تفطن المشرع الجزائري على غرار أغلب التشريعات إلى هذا النوع الجديد من الجرائم الذي بدأ يغزو العالم قاطبا، وذلك نتيجة التطور التكنولوجي الهائل إلى جانب قدرة هذه التكنولوجيا على عبور الحدود، فقد منح لضباط الشرطة القضائية صلاحيات واسعة من أجل البحث والتحري عن جرائم التكنولوجيا الحديثة، كما استحدث هيئة الشرطة العلمية المنوط بها هذه المهام، إلا أنه من الضروري إنشاء جهاز خاص داخل الشرطة مكونا تكوينا كافيا في المجال الإلكتروني لمجابهة هذا النوع من الجرائم.

إن التطور التكنولوجي والتقني يحتم على المشرع تعديل قواعده القانونية، خاصة فيما يتعلق بحقوق الملكية الفكرية والحقوق المجاورة والتي لم تعد قابلة للتطبيق في البيئة الرقمية، لأن النصوص الوضعية لحماية حقوق المؤلف والحقوق المجاورة تعتبر غير كافية لمواجهة الاعتداءات الواقعة عليها عبر الانترنت.

تفعيل التعاون الدولي ودور المعاهدات الدولية ودور المساعدة القانونية والقضائية المتبادلة، إضافة إلى ضرورة تفعيل دور المجتمع المدني والمؤسسات لنشر الوعي بين المواطنين وخاصة الشباب بمخاطر التعامل مع المواقع السيئة والمشبوهة على الشبكات.

وأخيرا، أدى ظهور المعلوماتية الحديثة وتطبيقاتها المتعددة إلى بروز مشاكل قانونية وتفاقم أزمة القانون الجنائي في مواجهة هذا الواقع الافتراضي مما استدعى تحديث النظم والقواعد القانونية والنصوص التشريعية بشكل ومستوى يضمن حقوق المعنيين وينظم الإجراءات القانونية والقضائية، وهذا كان إطار البحث المبين في هذه الأطروحة.

قائمة المصادر والمراجع

I: باللغة العربية

أولا: القرآن الكريم

ثانيا: النصوص الرسمية

1- الدستور الجزائري الحالي المعدل

قانون رقم 16-01 مؤرخ في 26 جمادى الأولى 1437هـ الموافق لـ 06 مارس 2016م، يتضمن التعديل الدستوري ج.ر، العدد 14، مؤرخة في 07 مارس 2016.

2- القوانين

- قانون رقم 05-10 مؤرخ في 13 جمادى الأولى 1426ﻫ الموافق لـ 20 يونيو 2005م، المعدل والمتمم للأمر رقم 75-58 مؤرخ في 20 رمضان 1395ﻫ الموافق لـ 26 سبتمبر 1975م، يتضمن القانون المدني، ج.ر العدد 44 مؤرخة في 26 يونيو 2005.
- قانون رقم 08-01 مؤرخ في 15 محرم عام 1429ﻫ الموافق لـ 23 يناير 2008، ج.ر، العدد 04، مؤرخة في 19 محرم عام 1249ﻫ الموافق لـ 27 يناير 2008م، يتمم القانون رقم 83-11 مؤرخ في 21 رمضان عام 1403ﻫ الموافق لـ 02 يوليو 1983م والمتعلق بالتأمينات الاجتماعية.
- قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430ﻫ الموافق لـ 05 غشت 2009م، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر، العدد 47، مؤرخة في 16 غشت 2009.
- قانون رقم 12-05 مؤرخ في 18 صفر 1433ﻫ الموافق لـ 12 يناير 2012م يتعلق بالإعلام، ج.ر، العدد 02 مؤرخة في 2012/01/15.
- قانون رقم 15-04 مؤرخ في 11 ربيع الثاني 1436ﻫ الموافق لـ 01 فبراير 2015م، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج.ر، العدد 06، مؤرخة في 20 ربيع الثاني عام 1436ﻫ الموافق لـ 10 فبراير 2015م.
- قانون رقم 16-01 مؤرخ في 26 جمادى الأولى 1437ﻫ الموافق لـ 06 مارس 2016م، يتضمن التعديل الدستوري ج.ر، العدد 14، مؤرخة في 07 مارس 2016.
- قانون رقم 16-02 مؤرخ في 19 يونيو 2016 المتضمن قانون العقوبات، ج.ر، العدد 37، مؤرخة في 22 يونيو 2016، الصادر بموجب الأمر رقم 66-156 مؤرخ في 08 يونيو 1966، ج.ر، العدد 49، مؤرخة في 11 يونيو 1966، المعدل والمتمم.
- قانون رقم 18-04 مؤرخ في 24 شعبان عام 1439ﻫ الموافق لـ 10 مايو سنة 2018م، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج.ر، العدد 27، مؤرخة في 27 شعبان عام 1439ﻫ الموافق لـ 13 مايو سنة 2018م.

- قانون رقم 19-10 مؤرخ في 14 ربيع الثاني 1441ھ الموافق لـ 11 ديسمبر 2019م، يعدل ويتمم الأمر رقم 66-155 مؤرخ في 18 صفر 1386ھ الموافق لـ 08 يونيو 1966م، يتضمن قانون الإجراءات الجزائية، ج.ر، العدد 78 مؤرخة في 18 ديسمبر 2019.

3- الأوامر

- أمر رقم 03-05 مؤرخ في 19 جمادى الأولى 1424ھ الموافق لـ 19 يوليو 2003م، يتعلق بحقوق المؤلف والحقوق المجاورة، معدل للأمر رقم 97-10، ج.ر، العدد 44، مؤرخة في 23 يوليو 2003.
- أمر رقم 66-57 مؤرخ في 1966/03/19، المتعلق بعلامات المصنع والعلامات التجارية، المعدل والمتمم بالأمر رقم 67-233 مؤرخ في 1967/10/19، المتضمن أحكام العلامات التجارية، والمعدل بالأمر رقم 03-06 مؤرخ في 19 يوليو 2003، المتعلق بالعلامات، ج.ر، العدد 44، مؤرخة في 23 جويلية 2003.
- أمر رقم 03-07 مؤرخ في 19 جمادى الأولى عام 1424ھ الموافق لـ 19 يوليو 2003م، يتعلق ببراءات الاختراع ج.ر، العدد 44، مؤرخة في 23 جويلية 2003.

4- المراسيم

- مرسوم رئاسي رقم 97-341 المتضمن انضمام الجزائر بتحفظ إلى اتفاقية برن لحماية المصنفات الأدبية والفنية، ج.ر العدد 61، مؤرخة في 1997/09/14.
- مرسوم رئاسي رقم 19-172 مؤرخ في 03 شوال عام 1440ھ الموافق لـ 06 يونيو سنة 2019م، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج.ر، العدد 05، مؤرخة في 06 شوال عام 1440ھ الموافق لـ 09 يونيو 2019م.
- مرسوم تنفيذي رقم 06-348 مؤرخ في 12 رمضان 1427ھ الموافق لـ 05 أكتوبر 2006م، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج.ر، العدد 63، مؤرخة في 05 أكتوبر 2006.

ثالثا: الكتب

1- الكتب العامة

- إبراهيم صادق الجندي، حسين حسن الحصيني، تطبيقات البصمة الوراثية D.N.A في التحقيق والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، 2002.
- أبو العلا علي أبو العلا النمر، الإثبات الجنائي، دراسة تحليلية لتحديد موطن القوة والضعف في الدليل الجنائي، دار النهضة العربية، القاهرة، 1991.
- أبو اليزيد علي المتيت، حقوق المؤلف الأدبية، مكتبة النهضة العربية، القاهرة، 1989.
- أحمد أبو القاسم أحمد، الدليل المادي وأهميته في الإثبات الجنائي، دار الكتب القومية، القاهرة، ط2، 2005.

- أحمد جاد منصور، الحماية القضائية لحقوق الإنسان، حرية التنقل والإقامة في القضاء الإداري المصري، دار الكتب، مصر ط1، 1997.
- أحمد شوقي عمر أبو خطوة، شرح الأحكام العامة لقانون العقوبات، دار النهضة العربية، 2007.
- أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار الطباعة الحديثة، القاهرة، 1993، ص578.
- أسامة أحمد المناعسة، الوسيط في شرح قانون محكمة أمن الدولة، دار وائل للنشر، عمان، ط1، 2006.
- أكرم أنور كرارة، القيادة واتخاذ القرار الأمني، أكاديمية الشرطة، كلية الشرطة.
- إيمان عبد الرحمن أحمد محمود، دور الإذاعة في نشر التوعية الأمنية، الإذاعة السودانية نموذجا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2010.
- إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الائتمان، دار الجامعة الجديدة، الإسكندرية، 2007.
- برهامي أبو بكر عزمي، الشرعية الإجرائية للأدلة العلمية، دراسة تحليلية لأعمال الخبرة، دار النهضة العربية، القاهرة 2006.
- حسن صادق المرصفاوي، المرصفاوي في المحقق الجنائي، منشأة المعارف، الإسكندرية، 1990.
- حسن صادق المرصفاوي، المرصفاوي في قانون العقوبات، القسم الخاص، منشأة المعارف، الإسكندرية، 1987.
- حسنين إبراهيم صالح عبيد، الوجيز في قانون العقوبات، القسم الخاص، جرائم الاعتداء على الأشخاص والأموال، دار النهضة العربية، القاهرة، 1994.
- حمدي عبد العظيم، غسيل الأموال في مصر وفي العالم، الجريمة البيضاء، أبعادها، آثارها وكيفية معالجتها، الدار الجامعية الإسكندرية، ط3، 2007.
- رأفت عبد الفتاح حلاوة، الإثبات الجنائي قواعده وأدلته، دراسة مقارنة بالشريعة الإسلامية، دار النهضة العربية، القاهرة ط1، 1996.
- رؤوف عبيد، ضوابط تسبيب الأحكام الجنائية وأوامر التصرف في التحقيق، دار الجيل للطباعة، مكتبة الوفاء القانونية بيروت، 1986.
- رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، دار الجيل، بيروت، 1985، 2006.
- سالم روضان الموسوي، جرائم القذف والسب عبر القنوات الفضائية، دراسة مقارنة معززة بتطبيقات قضائية، منشورات الحلبي الحقوقية، بيروت، 2012.
- سعد صالح شكطي الجبوري، مسؤولية الصحفي الجنائية عن جرائم النشر، دراسة مقارنة، دار الجامعة الجديدة للنشر الإسكندرية، 2013.
- سمير عالية، شرح قانون العقوبات، المؤسسة الجامعية للدراسات، بيروت، 1998، ص200.

- صابر عبد العزيز سلامة، العقد الإلكتروني، دار النهضة العربية، القاهرة، ط2، 2007.
- طارق عبد الله الشدي، آلية البناء الأمني لنظم المعلومات، دار الوطن للطباعة والنشر والإعلام، الرياض، 2000.
- عادل بسيوني، تاريخ القانون المصري، مصر الإسلامية، مكتبة نهضة الشرق، القاهرة، 1985.
- عادل حسن علي السيد، تحديات التخطيط الأمني لمواجهة العولمة، جامعة نايف العربية للعلوم الأمنية، الرياض، ط1 2006.
- عادل رمضان الأبيوكي، التوقيع الإلكتروني في التشريعات الخليجية، دراسة مقارنة، المكتب الجامعي الحديث، الإسكندرية ط1، 2009.
- عبد الحافظ عبد الهادي عابد، الإثبات الجنائي بالقرائن، مطابع الطوبجي التجارية، 1989.
- عبد الحكم فودة، البراءة وعدم العقاب في الدعوى الجنائية، منشأة المعارف، الإسكندرية، 2000.
- عبد الحكم فودة، حجية الدليل الفني في المواد الجنائية والمدنية، دار الفكر الجامعي، الإسكندرية، 1996.
- عبد الفتاح مصطفى الصيفي، قانون العقوبات، النظرية العامة، دار الهدى للمطبوعات، مصر، 1998.
- عبد القادر عبد الله الفنتوخ، الإنترنت للمستخدم العربي، العبيكان للنشر، الرياض،2000.
- علاء الدين شحاتة، التعاون الدولي لمكافحة الجريمة، دراسة للاستراتيجية الوطنية للتعاون الدولي لمكافحة المخدرات، إيتراك للطباعة والنشر والتوزيع، مصر، ط1، 2000.
- علي الباز، الإعلام والإعلام الأمني، مركز الإشعاع الفني، الإسكندرية، ط1، 2001.
- علي عبد القادر القهوجي، قانون العقوبات، القسم الخاص، جرائم الاعتداء على المصلحة العامة وعلى الإنسان والمال منشورات الحلبي الحقوقية، بيروت، ط1، 2002.
- عماد علي الخليل، الحماية الجزائية لبطاقات الوفاء، دراسة تحليلية مقارنة، دار وائل، عمان، ط1، 2000.
- عمار عباس الحسيني، التجريم والعقاب في النظام التأديبي، قراءة معاصرة في النصوص الجنائية والتأديبية، منشورات الحلبي الحقوقية، بيروت، ط1، 2015.
- عمر سالم، نحو قانون جنائي للصحافة، القسم العام، دار النهضة العربية، القاهرة، مصر، ط1، 1995.
- غسان قاسم الأمين، إدارة التكنولوجيا، مفاهيم ومداخل تقنيات تطبيقات علمية، دار المناهج، ط1، عمان، 2006.
- فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة، دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان، ط1 2006.
- فخري عبد الرزاق الحديثي، شرح قانون العقوبات، القسم الخاص، مطبعة الزمان، بغداد، 1996، ص254 و255.
- فوزية عبد الستار، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1986.

- كمال عبد الواحد الجوهري، تأسيس الاقتناع القضائي والمحاكمة الجنائية العادلة، دار محمود للنشر والتوزيع، 1999.
- كميت طالب البغدادي، الاستخدام غير المشروع لبطاقات الائتمان، دار الثقافة للنشر والتوزيع، عمان، 2009.
- مأمون محمد سلامة، الإجراءات الجنائية في التشريع المصري، ج01، دار النهضة العربية، القاهرة، 2008.
- ماهر عبد شويش الدرة، شرح قانون العقوبات، القسم الخاص، المكتبة القانونية، بغداد، 1997.
- ماهر عبد شويش الدرة، شرح قانون العقوبات، القسم الخاص، المكتبة القانونية، بغداد، 1997.
- محمد الأمين البشري، علم ضحايا الجريمة وتطبيقاته في الدول العربية، دار الحامد للنشر والتوزيع، عمان، 2005.
- محمد الشناوي، جرائم النصب المستحدثة، تقديم مأمون سلامة، دار الكتب القانونية، مصر، ط1، 2008.
- محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2008.
- محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2009.
- محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر والتوزيع، الأردن، 2010.
- محمد زكي أبو عامر، الإثبات في المواد الجنائية، الفنية للطباعة والنشر، الإسكندرية، 1985.
- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، الهيئة المصرية العامة للكتاب، القاهرة، 2003.
- محمد عيد الغريب، حرية القاضي الجنائي في الاقتناع اليقيني وأثره في تسبيب الأحكام الجنائية، النسر الذهبي للطباعة القاهرة، 1997.
- محمد فاروق عبد الحميد كامل، القواعد الفنية الشرطية للتحقيق والبحث الجنائي، أكاديمية نايف للعلوم الأمنية، الرياض ط1، 2006.
- محمد محرم محمد علي، خالد كدفور المهيري، قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة فقها وقضاء، دار الفتح للطباعة والنشر، أبو ظبي، ط2، 1999.
- محمود محمود مصطفى، الإثبات في المواد الجنائية في القانون المقارن، الجزء 1، النظرية العامة، مطبعة جامعة القاهرة والكتاب الجامعي، القاهرة، 1977.
- محمود محمود مصطفى، شرح قانون العقوبات، القسم العام، قانون العقوبات ومجال تطبيقه، أسباب الإباحة، الركن المادي للجريمة، الركن المعنوي، الأهلية الجنائية، العقوبة، مطبعة جامعة القاهرة، القاهرة، 1983.
- محمود نجيب حسني، دروس في القانون الجنائي الدولي، دار النهضة العربية، القاهرة، 1960.
- محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات التشريعية، ترجمة وتحقيق: فوزية عبد الستار دار النهضة العربية، القاهرة، ط6، 2019.
- محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، النظرية العامة للجريمة، دار النهضة العربية، القاهرة، 1982.

- محمود نجيب حسني، شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الاحترازي دار النهضة العربية، القاهرة، ط1، 1989.
- مريوان عمر سليمان، القذف في نطاق النقد الصحفي، دراسة مقارنة، المركز القومي للإصدارات القانونية، القاهرة، ط1 2014.
- مصطفى مجدي هرجة، الإثبات في المواد الجنائية في ضوء أحكام محكمة النقض، دار المطبوعات الجامعية، الإسكندرية 1992.
- ممدوح بحر، حماية الحياة الخاصة في القانون الجنائي، مكتبة دار الثقافة، عمان، ط1، 1996.
- ممدوح محمد الجنبيهي، الشركات الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2008.
- ناظم محمد نوري الشمري، عبد الفتاح زهير، الصيرفة الإلكترونية، الأدوات والتطبيقات ومعيقات التوسع، دار وائل للنشر عمان، ط1، 2008.
- نائل عبد الرحمن صالح، محاضرات في أصول المحاكمات الجزائية، قانون أصول المحاكمات الجزائية، قانون محكمة الجنايات الكبرى، دار الفكر العربي، عمان، ط1، 1997.
- هدى حامد قشقوش، جريمة غسيل الأموال في نطاق التعاون الدولي، دار النهضة العربية، القاهرة، 2001.
- هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، مصر، 1992.
- يونس عرب، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، منشورات اتحاد المصارف العربية، ط1 الأردن، 2001.

2- الكتب المتخصصة

- أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، الحماية الجنائية للحاسب الآلي، دراسة مقارنة، دار النهضة العربية، القاهرة، 2000.
- أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، دراسة مقارنة، دار النهضة العربية، القاهرة، ط1 2010.
- أحمد يوسف الطحاوي، الأدلة الإلكترونية ودورها في الإثبات الجنائي، دراسة مقارنة، دار النهضة العربية، القاهرة، 2015.
- أرنود روفر، الإنترنت، ترجمة منى ملحيس ونيبال إدلبي، الدار العربية للعلوم، ط2.
- أسامة أحمد المناعسة وآخرون، جرائم الحاسب الآلي والإنترنت، دراسة تحليلية مقارنة، دار وائل، عمان، ط1، 2001.
- أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، 1988.
- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني، دراسة مقارنة، دار النهضة العربية، القاهرة، 2006.
- أكرم عبد الرزاق المشهداني، الجرائم التكنولوجية، دار الوفاق، بغداد، 2001.

- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة للنشر، الجزائر، ط2، 2007.
- انتصار نوري الغريب، أمن الكمبيوتر والقانون، دار الراتب الجامعية، بيروت، ط1، 1994.
- أورين كير، نطاق الجريمة الافتراضية، ترجمة عمر محمد أبوبكر بن يونس، دار النهضة العربية، القاهرة، 2004.
- أيمن عبد الحفيظ عبد الحميد سليمان، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، مطابع الشرطة، مصر 2005.
- أيمن عبد الله فكري، جرائم نظم المعلومات، دراسة مقارنة، دار الجامعة الجديدة للنشر، الإسكندرية، 2007.
- برنار أ. جالر، الملكية الفكرية وبرامج الحاسبات، حق المؤلف وبراءات الاختراع من وجهات النظر الفنية والقانونية، ترجمة محمد حسام محمود لطفي، الجمعية المصرية لنشر المعرفة والثقافة العالمية، مصر، ط1، 1998.
- بشير عباس العلاق، تكنولوجيا المعلومات والاتصالات وتطبيقاتها في مجال التجارة النقالة، المنظمة العربية للتنمية الإدارية القاهرة، 2007.
- توم فوريستر، مجتمع التقنية العالية، قصة ثورة تقنية المعلومات، ترجمة محمد كامل عبد العزيز، مركز الكتب الأردني، عمان ط1، 1989.
- جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات، رؤية جديدة للجريمة الحديثة، دار البداية، الأردن، ط1 2007.
- جعفر محمود المغربي وحسين شاكر عساف، المسؤولية المدنية عن الاعتداء على الحق في الصورة بواسطة الهاتف المحمول دار الثقافة والنشر والتوزيع، عمان، 2010.
- جلال محمد الزعبي وأسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان، ط1، 2010.
- جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002.
- جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، (أجهزة الرادار –الحاسبات الآلية –البصمة الوراثية) دراسة مقارنة، دار النهضة العربية، القاهرة، 2002.
- جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية القاهرة، 2012.
- جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، 2002.
- جون كيريللو، موسوعة الهاكرز (Hacks attack revealed)، ترجمة خالد العامري، دار الفاروق للنشر والتوزيع 2008.

- حسام الدين كامل الأهواني، الحق في احترام الحياة الخاصة، الحق في الخصوصية، دراسة مقارنة، دار النهضة العربية، القاهرة 1978.
- حسن سعيد عبد اللطيف، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية، القاهرة، ط1 1999.
- حسن طاهر داود، الحاسب وأمن المعلومات، معهد الإدارة العامة، الرياض، 2000.
- حسن طاهر داود، جرائم نظم المعلومات، مركز الدراسات والبحوث، أكاديمية نايف العربية للعوم الأمنية، الرياض، ط1 2000.
- حسني عبد السميع إبراهيم، الجرائم المستحدثة عن طريق الإنترنت، دراسة مقارنة بين الشريعة والقانون، دار النهضة العربية القاهرة، 2001.
- حسنين المحمدي بوادي، إرهاب الإنترنت، الخطر القادم، دار الفكر الجامعي، الإسكندرية، ط1، 2006.
- الحمود فداء يحيى، النظام القانوني لبطاقة الائتمان، دار الثقافة للنشر والتوزيع، عمان، 1999.
- حنان ريحان مبارك المضحكي، الجرائم المعلوماتية، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2014.
- خالد أبو الفتوح فضالة، مدخلك إلى فيروسات الحاسب، مرض التكنولوجيا الحديثة، دار الكتب العلمية، القاهرة، ط3 2000.
- خالد ممدوح ابراهيم، التقاضي الإلكتروني، الدعوى الإلكترونية وإجراءاتها أمام المحاكم، دار الفكر الجامعي، الإسكندرية 2008.
- خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط1، 2009.
- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2009.
- خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، أساليب وثغرات، دار الهدى، عين مليلة، الجزائر، 2017.
- ديالا عيسى ونسه، حماية حقوق التأليف على شبكة الإنترنت، دراسة مقارنة، المنشورات الحقوقية صادر، 2002.
- ذيب بن عايض القحطاني، أمن المعلومات، مدينة الملك عبد العزيز للعلوم والتقنية، الرياض، 2015.
- رأفت رضوان، عالم التجارة الإلكترونية، المنظمة العربية للتنمية، القاهرة، 1999.
- رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، دار النهضة العربية، القاهرة، ط1، 2011.
- رشا مصطفى أبو الغيط، تطور الحماية القانونية للكيانات المنطقية، دار الفكر الجامعي، الإسكندرية، ط1، 2006.
- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية للمعطيات في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية بيروت، ط1، 2012.

- روزا جعفر محمد الخامري، مشكلات الطبيعة القانونية لبرامج الحاسب الآلي، المكتب الجامعي الحديث، مصر، 2006.
- زياد عبد الكريم القاضي، أساسيات علم الحاسوب، دار صفاء للنشر والتوزيع، عمان، 1997.
- زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، 2011.
- سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الإسكندرية، 2007.
- سعد جاد الله الحيدر، النظام القانوني لعقد الاتصالات الحديثة، الهاتف النقال، دار الكتب القانونية، مصر، ط1 2012.
- سلامة محمد عبد الله أبو بكر، موسوعة جرائم المعلومات، منشأة المعارف، الإسكندرية، 2006.
- سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الإنترنت، منشورات الحلبي الحقوقية، ط1، 2011.
- سمير الأمين، مراقبة التليفون والتسجيلات الصوتية والمرئية، دار الكتاب الذهبي، مصر، 2000، ص43.
- شحاتة غريب شلقامي، الملكية الفكرية في القوانين العربية، دراسة لحقوق المؤلف والحقوق المجاورة ولخصوصية حماية برامج الحاسب الآلي، دار الجامعة الجديدة، مصر، 2008.
- ضياء يحيى السادات، مبادئ استخدام الحاسب الآلي والإنترنت، وجهود مكافحة الجرائم الناشئة عنهما، منشأة المعارف ط1، 2012.
- طارق عفيفي صادق أحمد، الخطر محل التأمين من المسئولية المدنية في مجال المعلوماتية، أطروحة دكتوراه، كلية الحقوق جامعة بني سويف، القاهرة، 2010.
- طوني ميشال عيسى، التنظيم القانوني لشبكة الإنترنت، دراسة مقارنة في ضوء القوانين الوضعية والمواثيق الدولية، مكتبة صادر، بيروت، ط1، 2001.
- عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونية، شبكة الإنترنت وشبكة الهواتف النقالة وعبر الوسائط التقليدية والآلية والمطبوعات، دراسة قانونية مقارنة، دار الثقافة للنشر والتوزيع، عمان، ط1، 2015.
- عادل يحيى قرني، السياسة الجنائية في مواجهة الجريمة المعلوماتية، دار النهضة العربية، القاهرة، ط1، 2014.
- عامر نزار فايز أبو علي، فيروسات الكمبيوتر، دار حنين للنشر والتوزيع، عمان، 1994.
- عايد رجا الخلايلة، المسؤولية التقصيرية الإلكترونية، المسؤولية الناشئة عن إساءة استخدام أجهزة الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمان، 2009.
- عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، الإسكندرية، ط1، 2006.
- عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر والإنترنت، منشأة المعارف، 2010.
- عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، منشأة المعارف، الإسكندرية ط1، 2009.

- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، القاهرة، 2005.
- عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الثاني، الحماية الجنائية لنظام التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2002.
- عبد الفتاح بيومي حجازي، جرائم غسل الأموال بين الوسائط الإلكترونية ونصوص التشريع، دار الفكر الجامعي الإسكندرية، 2005.
- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة 2007.
- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دراسة قانونية متعمقة في القانون المعلوماتي، دار الكتب القانونية، مصر، ط1، 2008.
- عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، ط1 2009.
- عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، دار الكتب والوثائق المصرية، 2007.
- عبد الله عبد الكريم، الحماية القانونية لحقوق الملكية الفكرية على شبكة الإنترنت، دراسة في الأطر القانونية للحماية مع شرح النظام القانوني للملكية الفكرية في التشريعات المصرية والأردنية والأوروبية والأمريكية ومعاهدتي الإنترنت، دار الجامعة الجديدة، مصر، 2008.
- عبد الله عبد الكريم، جرائم المعلوماتية والإنترنت، الجرائم الإلكترونية، دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والإنترنت مع الاشارة إلى جهود مكافحتها محليا وعربيا ودوليا، منشورات الحلبي الحقوقية، بيروت، ط1 2007.
- عبد الهادي بن زيطة، حماية برامج الحاسوب في التشريع الجزائري وفقا لأحكام قانون المؤلف الجديد رقم 03-05، دار الخلدونية للنشر والتوزيع، الجزائر، ط1، 2007.
- عفيفي كامل عفيفي وفتوح عبد الله الشاذلي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون منشورات الحلبي الحقوقية، بيروت، ط1، 2003.
- علي بن هادي البشري، الجهود القانونية للحد من جرائم الحاسب الآلي، الرياض، ط1، 1419ھ.
- علي جبار الحسناوي، جرائم الحاسوب والإنترنت، دار اليازوري العلمية للنشر والتوزيع، الأردن، 2009.
- علي حسن محمد الطوالبة، الجرائم الإلكترونية، دراسة مقارنة، مطبوعات جامعة العلوم التطبيقية، جامعة العلوم التطبيقية ط1، 2008.

- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية، بيروت، 1999.
- علي عدنان الفيل، الإجرام الإلكتروني، دراسة مقارنة، منشورات زين الحقوقية، لبنان، ط1، 2011.
- عماد محمد سلامة، الحماية القانونية لبرامج الحاسب الآلي ومشكلة قرصنة البرامج، دار وائل، عمان، 2005.
- عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا، دراسة مقارنة، دار النهضة العربية القاهرة، 2010.
- عمر محمد أبو بكر ابن يونس، المجتمع المعلوماتي والحكومة الإلكترونية، مقدمة إلى العالم الافتراضي، دار النهضة العربية القاهرة، 2004.
- عمرو عيسى الفقي، الجرائم المعلوماتية، جرائم الحاسب الآلي والإنترنت في مصر والدول العربية، المكتب الجامعي الحديث الإسكندرية، 2006.
- عوض منصور، مقدمة في علم الحاسب الإلكتروني وبرمجة بيسك، دار الأمل، عمان، 1991.
- غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت وجرائم الاحتيال المنظم باستعمال شبكة الإنترنت، دار الفكر والقانون، المنصورة، 2013.
- فاروق علي الحفناوي، موسوعة قانون الكمبيوتر ونظم المعلومات، دار الكتاب الحديث، القاهرة، 2001.
- فتحي محمد أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، دار الفكر والقانون، المنصورة ط1، 2010.
- فريد منعم جبور، حماية المستهلك عبر الإنترنت ومكافحة الجريمة الإلكترونية، دراسة مقارنة، منشورات الحلبي الحقوقية بيروت، ط2، 2012.
- محمد أحمد فكيرين، أساسيات الحاسب الآلي، دار الراتب الجامعية، بيروت، 1993.
- محمد الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة في مواجهة الصحافة، دار النهضة العربية، القاهرة، ط1، 2001.
- محمد الفيومي، مقدمة الحاسبات، تشغيل الحاسبات الصغيرة، الحاسبات الإلكترونية وأنظمة المعلومات، المكتب الجامعي الحديث، الإسكندرية، 1998.
- محمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنت، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، الأردن، ط4 2011.
- محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، مصر، 2003.
- محمد بلال الزعبي، أحمد الشرايعة، سهير عبد الله، خالدة الزعبي، الحاسوب والبرمجيات الجاهزة، دار وائل للنشر والتوزيع عمان، 2002.

- محمد بن عبد الله القاسم، عبد الرحمن بن عبد العزيز الحمدان، أساسيات أمن المعلومات، مكتبة الملك فهد الوطنية الرياض، ط2، 2008.
- محمد حسام محمود لطفي، الحماية القانونية لبرامج الحساب الآلي، دار الثقافة للطباعة والنشر، القاهرة، ط2، 1987.
- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية 2007.
- محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الإنترنت، الأحكام الموضوعية والأحكام الإجرائية، منشورات الحلبي الحقوقية، بيروت، ط1، 2011.
- محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دراسة مقارنة، دار النهضة العربية القاهرة، ط2، 2009.
- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2011.
- محمد فهمي طلبة عبد المنعم يوسف بلال، محمد علي الشرقاوي، مصطفي رضا عبد الوهاب، الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، موسوعة دلتا كمبيوتر، القاهرة، 1991.
- محمد محمد الألفي، جرائم النشر الإلكتروني، مركز تطوير الأداء والتنمية، مصر، 2009.
- محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، القاهرة، 2001.
- محمد محمد عنب، استخدام التكنولوجيا الحديثة في الإثبات الجنائي، مطبعة السلام الحديثة، الاسماعيلية، 2007.
- محمد محمود المكاوي، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية، المكتبة العصرية للنشر والتوزيع، المنصورة، 2010.
- محمد نزيه الدربني، مقدمة في أساسيات الحاسب الآلي، معهد الإدارة العامة، المملكة العربية السعودية، 1991.
- محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والإنترنت، دراسة مقارنة، دار الفكر والقانون، المنصورة، 2013.
- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، 2005.
- محمود الربيعي، أحمد أحمد شعبان دسوقي، عبد العزيز إبراهيم الجبيري، علي ابن صالح الغامدي، المعجم الشامل لمصطلحات الحاسب الآلي والإنترنت، مكتبة العبيكان، 2001.
- محمود الزهد، محمد عثمان البشير، مقدمة في الحاسب الآلي، معهد الإدارة العامة، الرياض، 1985.
- محمود عبد الرحمن محمد، نطاق الحق في الحياة الخاصة أو الخصوصية، دراسة مقارنة، دار النهضة العربية، القاهرة، 1994.
- محمود عبد الرحيم الديب، الحماية القانونية للملكية الفكرية في مجال الحاسب الآلي والإنترنت، دار الفكر الجامعي القاهرة، 2008.
- مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، 2001.

- مدحت عبد الحليم رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، ط1، 2000.
- مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية، ماهيتها، مكافحتها، دراسة مقارنة، دار الكتب القانونية، القاهرة 2005.
- مصطفى محمد موسى، التحري في جرائم مجتمع المعلومات والمجتمع الافتراضي، دار النهضة العربية، القاهرة، 2011.
- مصطفى محمد موسى، الجهاز الإلكتروني لمكافحة الجريمة، دار الكتب القانونية، القاهرة، 2006.
- مصطفى محمد موسى، السيرة الذاتية للفيروسات الإلكترونية بين الوقاية والمكافحة والعلاج، دار الكتب القانونية، القاهرة ط1، 2008.
- مغبغب نعيم، حماية برامج الكمبيوتر، الأساليب والثغرات، منشورات الحلبي الحقوقية، بيروت، 2006.
- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية مصر، 2006.
- منير محمد الجنبيهي، ممدوح محمد الجنبيهي، أمن المعلومات الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2005.
- منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي الإسكندرية، 2004.
- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، ط1 2005.
- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية 2013.
- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، ط2، 2010.
- هدى حامد قشقوش، السياسة الجنائية لمواجهة الجريمة المعلوماتية، دار النهضة العربية، القاهرة، 2012.
- هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992.
- هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، القاهرة 2000.
- هلالي عبد الله أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001، دار النهضة العربية، القاهرة، ط1، 2003.
- هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، ط2، 2008.
- هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، دار النهضة العربية، 1997.

- هلالي عبد الله أحمد، كيفية المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست، دار النهضة العربية، القاهرة، 2011.
- يوسف المصري، الجرائم المعلوماتية والرقمية للحاسوب والإنترنت، دار العدالة للطباعة والنشر، القاهرة، ط1، 2011.
- يوسف حسن يوسف، الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، القاهرة، ط1، 2011.
- يونس عرب، جرائم الكمبيوتر والإنترنت، دليل أمن المعلومات والخصوصة، ج1، اتحاد المصارف العربية، الأردن، ط1 2002.

رابعا: المعاجم والقواميس

- المفردات في غريب القرآن، أبو القاسم الحسين بن محمد المعروف بالراغب الأصفهاني، المتوفي عام 502ھ، تحقيق صفوان عدنان الداودي، دار القلم، بيروت، 2009.
- المنجد في اللغة، المطبعة الكاثوليكية، لويس معلوف، المجلد 01، بيروت.
- عبد الحسن الحسيني، القاموس الموسوعي في المعلومات والاتصالات والمعلوماتية القانونية، مكتبة صادر، بيروت، 2004، ص408.
- كتاب العين، الخليل بن أحمد الفراهيدي، تحقيق مهدي المخزومي، دار إحياء التراث العربي، بيروت، ط2، 2005.
- مختار الصحاح، محمد ابن أبي بكر ابن عبد القادر الرازي، مكتبة لبنان، لبنان، 1986.
- معجم مقاييس اللغة، أحمد ابن فارس بن زكريا أبو الحسين، المتوفي عام 395ھ، تحقيق وضبط عبد السلام محمد هارون دار الفكر، 1399ھ-1979م.

خامسا: المقالات والمداخلات

1- المقالات

- أسعد فاضل منديل الجياشي، دراسة قانونية بالأضرار الناتجة عن أبراج الهاتف النقالة، مجلة الحقوق، السنة الثانية، العدد الثالث، العراق، 2010.
- اسماعيل رضا، الوقاية من الجرائم الناشئة عن استخدام الحاسب الآلي، مجلة الاقتصاد الإسلامي، العدد 219، دبي 1999.
- أشرف السعيد أحمد حافظ، الاتصال والتواصل بين الإعلام الأمني ووسائل الإعلام، مجلة كلية التدريب والتنمية، العدد 28، القاهرة، مارس 2013.
- أمجد أبو جدي، الإدمان على الهاتف النقال وعلاقته بالكشف عن الذات لدى عينة من طلبة الجامعتين الأردنية وعمان الأهلية، المجلة الأردنية في العلوم التربوية، المجلد 04، العدد 02، الأردن، حزيران 2008.

- جواهر بنت عبد العزيز آل سعود، الجرائم الإلكترونية ومكافحتها، مجلة الاتصالات والعالم الرقمي، العدد 209، جدة 1428ھ.
- جوفاني ليون، مبدأ الاقتناع والمشاكل المرتبطة به، ترجمة رمسيس بهنام، مجلة القانون والاقتصاد، العدد 04، القاهرة 1964.
- حسن مظفر الرزو، الأمن المعلوماتي معالجة قانونية أولية، مجلة الأمن والقانون، العدد 01، السنة 12، أكاديمية الشرطة دبي، نيسان 2004.
- حسين بن سعيد بن سيف الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت، مقال منشور على موقع شبكة قوانين الشرقwww.eastlaws.com
- حسين بن سعيد بن سيف الغافري، الجاسوسية الرقمية، مقال منشور على الموقع الإلكتروني: www.omanlegal.net
- حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الإنترنت، مقال منشور على الموقع الإلكتروني: www.arablaws.com
- زينب أحمد عوين بديوي الشمري، عدم كفاية قواعد القانون الجنائي في مكافحة الجريمة المعلوماتية، مجلة كلية الحقوق العدد 01، المجلد 13، جامعة النهرين، بغداد، 2011.
- شائف علي محمد الشيباني، الإنابة القضائية الدولية في القانون اليمني، دراسة مقارنة، مقال موجه لدائرة التدريب والتأهيل النيابة العامة، اليمن، 2006.
- صفوت عبد السلام عوض الله، الآثار الاقتصادية لعمليات غسيل الأموال ودور البنوك في مكافحة هذه العمليات، مجلة كلية التدريب والتنمية، العدد 02، كانون الثاني 2000.
- عبد الرحيم الشحات البحطيطي، المخاطر المالية في نظم المدفوعات في التجارة الإلكترونية، كأحد التحديات التي تواجه النظم المصرفية، مجلة جامعة الملك عبد العزيز، الاقتصاد والإدارة، مجلد 21، العدد 02، السعودية، 1428ھ-2007م.
- عبد الله الصعيدي، دراسة في حجم الاقتصاد الخفي، مجلة الفكر الشرطي، المجلد 09، العدد 01، شرطة الشارقة، دولة الإمارات العربية المتحدة.
- علي محمد حسن عبد الله، حماية برامج الحاسب بقانون براءة الاختراع في الولايات المتحدة الأمريكية، مجلة الشريعة والقانون، العدد 47، الإمارات العربية المتحدة، 2011.
- عواطف محمد عثمان عبد الحليم، جرائم المعلوماتية، صورها وجهود مكافحتها دوليا، إقليميا ووطنيا، مجلة العدل، العدد 24، السنة 10، وزارة العدل إدارة التأصيل والبحوث والتدريب، السودان، 2008.
- مايكل سميث، الحرب بواسطة شبكات الاتصال، الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر، حوارات إنسانية في القانون والسياسات والعمل الإنساني، 2002.

- محمد ابن عبد العزيز الخضيري، أحكام التشهير، مجلة البيان، المنتدى الإسلامي، العدد 70.
- محمد حافظ الرهوان، عمليات غسل الأموال، مفهومها وخطورتها واستراتيجية مكافحتها، مجلة الأمن والقانون، العدد 02، السنة 10، أكاديمية الشرطة، دبي، يوليو 2002.
- محمد عبد الرحيم سلطان العلماء، جرائم الإنترنت والاحتساب عليها، المجلة العربية للدراسات الأمنية والتدريب، العدد 36، السنة 18، جامعة نايف العربية للعلوم الأمنية، الرياض، أكتوبر 2003.
- محمد عبد اللطيف فرج، تجريم عمليات غسيل الأموال في مصر والأنظمة المقارنة، مجلة مركز بحوث الشرطة، العدد 13 القاهرة، يناير 1998.
- محمد قدري حسن عبد الرحمن، جرائم الاحتيال الإلكتروني، مجلة الفكر الشرطي، المجلد 20، العدد 89، مركز بحوث الشرطة، الإمارات العربية المتحدة، أكتوبر 2011.
- معتصم خميس مشعشع، إثبات الجريمة بالأدلة العلمية، مجلة الشريعة والقانون، العدد 56، السنة 27، كلية القانون جامعة الامارات العربية المتحدة، أكتوبر 2013.
- ممدوح عبد الحميد عبد المطلب، دور الشرطة وضحايا الجريمة، مجلة كلية الدراسات العليا، العدد 13، أكاديمية الشرطة الرياض، 2005.
- هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، مجلة الأمن والقانون، العدد 02، كلية الشرطة دبي، 1999.
- هشام محمد فريد رستم، جرائم الحاسوب كصورة من صور الجرائم الاقتصادية المستحدثة، مجلة الدراسات القانونية، العدد 17، جامعة أسيوط، مصر، 1995.
- هشام محمد فريد رستم، جرائم الفضاء الافتراضي، مجلة أكاديمية الشرطة، كلية الشرطة، دبي، 2013.

2- المداخلات

- الأزرق عبد الله، أحمد عمراني، نظام المعلومات في القانون الجزائري واقع وآفاق، المؤتمر السادس لجمعية المكتبات والمعلومات السعودية، البيئة المعلوماتية الأمنة، المفاهيم والتشريعات والتطبيقات، الرياض، 06 و07 أفريل 2010.
- أسامة عبد الخالق الأنصاري، أثر تكنولوجيا المعلومات على مستقبل العلوم الشرطية، مؤتمر الشارقة الدولي لتأصيل العلوم الشرطية، مركز البحوث والدراسات بالشارقة، الإمارات، 1998.
- أمجد حسان، الفيروسات إرهابا تهدد نظام المعلومات، ملتقى الإرهاب في العصر الرقمي، المركز الجامعي بشار 2008/06/20، مقال منشور على الموقع الإلكتروني: www.kfse.edu.sa
- إيهاب ماهر السنباطي ميخائيل السنباطي، الجرائم الإلكترونية، الجرائم السبرانية، قضية جديدة أم فئة مختلفة؟، التناغم القانوني هو السبيل الوحيد، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، يونيو 2007.

- براء منذر كمال عبد اللطيف، ناظر أحمد منديل، التعاون القضائي الدولي في مواجهة جرائم الانترنت، المؤتمر العلمي الأول، تحولات القانون العام في مطلع الألفية الثالثة، كلية القانون، جامعة تكريت، العراق، 2009.
- ثناء أحمد محمد المغربي، الوجهة القانونية لبطاقات الائتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون -جامعة الإمارات العربية المتحدة، 2003.
- جعفر عبد السلام، دور التنظيم الدولي في مكافحة الجريمة، مؤتمر الوقاية من الجريمة في عصر العولمة، كلية الشريعة والقانون جامعة الإمارات العربية المتحدة، دبي، 06-08 مايو 2001.
- جميل عبد الباقي الصغير، الحاسب الآلي كوسيلة لإثبات الجرائم، ندوة المواجهة الأمنية للجريمة المعلوماتية، مركز بحوث الشرطة، أكاديمية الشرطة، 2009.
- جون فرونسوا هنروت، أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، 19 و20 يونيو 2007.
- حسين بن سعيد بن سيف الغافري، مؤتمر الجوانب القانونية للمعلوماتية بين النظرية والتطبيق، كلية الحقوق، جامعة السلطان قابوس، مسقط، 13 و14 مارس 2011.
- خالد بن محمد الطويل، التعامل مع الاعتداءات الإلكترونية من الناحية الأمنية، مركز المعلومات الوطني، وزارة الداخلية ورشة العمل الثالثة (أحكام في المعلوماتية) الذي نظمه مشروع الخطة الوطنية لتقنية المعلومات، الرياض 1423/10/19هـ.
- دياب موسى البدانية، دور الأجهزة الأمنية في مكافحة جرائم الإرهاب المعلوماتي، الدورة التدريبية المنعقدة بكلية التدريب القنيطرة، المملكة المغربية، 09 إلى 13 أفريل 2006.
- زكي أمين حسونة، جرائم الكمبيوتر الأخرى في مجال التكتيك المعلوماتي، المؤتمر السادس للجمعية المصرية للقانون الجنائي القاهرة، 25-28 أكتوبر 1993.
- سعد محمد سعد، المسائل القانونية التي تثيرها العلاقة الناشئة عن استخدام بطاقات الائتمان بين الجهة مصدرة البطاقة والتاجر، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة.
- عبد الرحمن بن عبد الله السند، وسائل الإرهاب الإلكتروني حكمها في الإسلام وطرق مكافحتها، السجل العلمي لمؤتمر موقف الإسلام من الإرهاب، جامعة الإمام محمد بن سعود الإسلامية، الرياض، 2004.
- عبد القادر دوحة، محمد بن حاج الطاهر، مدى مواكبة المشرع الجزائري لتطور الجريمة الإلكتروني، الملتقى الوطني الأول النظام القانوني للمجتمع الإلكتروني، معهد العلوم القانونية والإدارية، المركز الجامعي خميس مليانة، 11/10/09 مارس 2008.
- عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، المؤتمر الدولي الأول حول حماية أمن المعلومات والخصوصية في قانون الإنترنت، القاهرة، 02-04 يونيو 2008.

- عبد الله عبد العزيز اليوسف، التقنية والجرائم المستحدثة، الظواهر الإجرامية المستحدثة وسبل مواجهتها، ندوة علمية أكاديمية نايف للعلوم الأمنية، الرياض، 1999.
- عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، الرياض، 2007.
- علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، الإمارات العربية المتحدة، 26 و27 أبريل 2003.
- عمر مشهور حديثة الجازي، المبادئ الأساسية لقانون حق المؤلف، ندوة حق المؤلف في الأردن بين النظرية والتطبيق، كلية الحقوق، الجامعة الأردنية، 12 كانون الثاني 2004.
- كريستينا سكولمان، عن جرائم الإنترنت، طبيعتها وخصائصها، برنامج تعزيز حكم القانون في بعض الدول العربية مشروع تحديث النيابات العامة، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، ا 19 و20 يونيو 2007.
- مأمون التلهوني، حماية حقوق الملكية الفكرية وإنفاذها في الأردن، ندوة الوب الوطنية عن الملكية الفكرية للصحفيين تنظمها المنظمة العالمية للملكية الفكرية (الويبو) بالتعاون مع دائرة المكتبة الوطنية / وزارة الصناعة والتجارة ومركز الملك عبد الله الثاني للملكية الفكرية، عمان، 06 نيسان 2004.
- محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، مركز البحوث والدراسات، أكاديمية شرطة دبي، الإمارات العربية المتحدة، 28 نيسان 2003.
- محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 01-03 مايو 2000.
- محمد الأمين الضرير، بطاقة الائتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2003.
- محمد الشنبري، التحقيق في جرائم الحاسب الآلي، دراسة قانونية ضمن أعمال مؤتمر القانون، الكمبيوتر والإنترنت، كلية الشريعة والإنترنت، جامعة الإمارات، الإمارات العربية المتحدة، مايو 2005.
- محمد حسام محمود لطفي، المشكلات القانونية في مجال المعلوماتية، خواطر وتأملات، مؤتمر تحديات حماية الملكية الفكرية من منظور عربي ودولي، تحت رعاية الجمعية المصرية لحماية الملكية الصناعية، والجمعية الدولية لحماية الملكية الصناعية القاهرة، 21-23 أكتوبر 1997.

- محمد محمد الألفي، العوامل الفاعلة في انتشار جرائم الإرهاب عبر الإنترنت، المؤتمر الدولي الأول حول حماية أمن المعلومات والخصوصية في قانون الإنترنت، القاهرة، 02-04 يونيو 2008.
- محمد محمد الألفي، جرائم الاعتداء على البطاقات الائتمانية كأحد الأنماط الإجرامية المستحدثة، ندوة مكافحة الجريمة عبر الإنترنت على المستوى العربي، شرم الشيخ، مصر، 20-24 أبريل 2008.
- مفتاح أبو بكر المطردي، المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، جمهورية السودان، 23 إلى 25 سبتمبر 2012.
- مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، البند الثامن من جدول الأعمال المؤقت، التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة بما فيها الجرائم الحاسوبية المنعقد بالبرازيل في الفترة 12-19 أفريل 2010، رقم A/CONF 213/9.
- موسى عصام حنفي موسى، الطبيعة القانونية لبطاقات الائتمان، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون جامعة الإمارات العربية المتحدة، 2003.
- نادية أمين محمد علي، الفيروسات وطرق الوقاية منها كوسيلة لأمن المعلومات، المؤتمر الدولي لأمن المعلومات، محافظة مسقط، عمان، 18–20 ديسمبر 2005.
- نوارة حسين، آليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة إلكترونيا، الملتقى الوطني حول آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو الجزائر، 29 مارس 2017.
- هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني وآليات التدريب التخصصي للمحققين، المؤتمر الدولي تحت عنوان الكمبيوتر والإنترنت بين الشريعة والقانون، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة الإمارات العربية المتحدة، 2000.
- يونس عرب، الخصوصية وأمن المعلومات في الأعمال اللاسلكية بواسطة الهاتف الخلوي، منتدى العمل الإلكتروني بواسطة الهاتف الخلوي، اتحاد المصارف العربية، عمان، الأردن، 2001.
- يونس عرب، جرائم الحاسوب، جرائم الكمبيوتر والإنترنت، إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات، مؤتمر الأمن العربي، أبو ظبي، 10-12 فبراير 2002.
- يونس عرب، قراءة في الاتجاهات التشريعية للجرائم الإلكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان، ورقة عمل مقدمة بورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، هيئة تنظيم الاتصالات، مسقط، سلطنة عمان، 02-04 أبريل 2006.

سادسا: أطروحات الدكتوراه

- أحمد أبو القاسم، الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص، أطروحة دكتوراه، المركز العربي للدراسات الأمنية والتدريب، الرياض، 1414ه.
- أحمد سعد محمد الحسيني، الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية، أطروحة دكتوراه، جامعة عين شمس، كلية الحقوق، 2012.
- أحمد شحاتة بيومي، الجرائم الماسة بالحياء عبر وسائل الاتصال المستحدثة، أطروحة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة، 2009.
- أحمد ضياء الدين محمد خليل، مشروعية الدليل في المواد الجنائية، دراسة تحليلية مقارنة لنظريتي الإثبات والمشروعية في مجال الإجراءات الجنائية، أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، أكاديمية الشرطة، القاهرة، 1982.
- أمال عبد الرحيم عثمان، الخبرة الفنية، المسائل الجنائية، دراسة قانونية مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة، 1964.
- أيمن عبد الحفيظ عبد الحميد سليمان، استراتيجية مكافحة جرائم استخدام الحاسب الآلي، دراسة مقارنة، أطروحة دكتوراه كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، 2003.
- إيهاب ماهر السنباطي ميخائيل السنباطي، موسوعة الإطار القانوني للتجارة الإلكترونية، دار النهضة العربية، القاهرة 2007، ص80.
- براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2018.
- بشرى زلاسي المعطيات الحديثة للحاسب الإلكتروني(الكمبيوتر) وحجيتها في الإثبات المدني، أطروحة دكتوراه في الحقوق قسم القانون الخاص، كلية الحقوق، بن عكنون، جامعة الجزائر1، 2013.
- بلال عبد الكريم غالي، الحماية القانونية للإنسان من مخاطر المعلومات، أطروحة دكتوراه، كلية العلوم القانونية والاقتصادية والاجتماعية، الرباط، 1995.
- بن طالب ليندا، الدليل الإلكتروني ودوره في الإثبات الجنائي، دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2019.
- حسن محمد ربيع، حماية حقوق الإنسان والوسائل المستحدثة للتحقيق الجنائي، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة، 1985.
- حمود عبد الله عوض الخضير، دور الإعلام في تحقيق الوعي الأمني لدى الرأي العام بالتطبيق على دولة الكويت، أطروحة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، مصر، 2007.

- خالد حمد محمد الحمادي، غسل الأموال في ضوء الإجرام المنظم، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة، 2002.
- رشا علي الدين أحمد علي تقي الدين، النظام القانوني لحماية البرمجيات، دار الجامعة الجديدة، مصر، 2007.
- سامي حسني الحسيني، النظرية العامة للتفتيش في القانون المصري والمقارن، أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة، 1972.
- سعد أحمد محمود سلامة، التبليغ عن الجرائم، دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة الزقازيق، القاهرة 2003.
- سعود محمد موسى، شكوى المجني عليه، دراسة مقارنة، أطروحة دكتوراه، أكاديمية الشرطة، جامعة القاهرة، 1990.
- سليمان سعيد عبيد المرشدي، دور الشرطة في حماية ضحايا الجريمة، دراسة مقارنة، أطروحة دكتوراه، كلية الدراسات العليا أكاديمية الشرطة، القاهرة، 2006.
- شول بن شهرة، الحماية الجنائية للتجارة الإلكترونية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، 2011-2012.
- شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، أطروحة دكتوراه، كلية الحقوق، جامعة المنصورة مصر، 2005.
- صباح رمضان ياسين صالح، السياسة الجنائية في مواجهة الجرائم المعلوماتية، دراسة تحليلية، رسالة دكتوراه، سكول القانون والإدارة، جامعة كوية، إقليم كردستان، العراق، 2013.
- عصام محمود عبد الحليم يوسف، المسؤولية الجنائية للمصابين بالأمراض العصبية والنفسية، أطروحة دكتوراه، كلية الحقوق جامعة القاهرة، 2014.
- علي إسماعيل مجاهد، التنبؤ كأساس للتخطيط الأمني، أطروحة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة 2004.
- علي عبود جعفر، جرائم تكنولوجيا المعلومات الواقعة على الأشخاص وضد الحكومة، دراسة مقارنة، أطروحة دكتوراه كلية الحقوق والعلوم السياسية، بيروت، 2012.
- عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا، أطروحة دكتوراه، كلية الحقوق جامعة القاهرة، 2009.
- عمر محمد أبو بكر ابن يونس، الجرائم الناشئة عن استخدام الإنترنت، أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس القاهرة، 2004.
- فهد بن سيف بن راشد الحوسني، جرائم التجارة الإلكترونية ووسائل مواجهتها مع التطبيق على سلطنة عمان، أطروحة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة، 2007.

- معاذ سليمان راشد محمد الملا، المسؤولية الجنائية عن إساءة استعمال الهاتف المحمول، دارسة مقارنة، أطروحة دكتوراه كلية الحقوق، جامعة عين شمس، القاهرة، 2013.
- مفيدة سعد سويدان، نظرية الاقتناع الذاتي للقاضي الجنائي، دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة 1985.
- ميرفت ربيع عبد العالي، عقد المشورة في مجال نظم المعلومات، أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة 1998.
- هلالي عبد الله أحمد، النظرية العامة للإثبات في المواد الجنائية، دراسة مقارنة بين النظم الإجرائية اللاتينية والجرمانية والاشتراكية والأنجلوسكسونية والشريعة الإسلامية، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة، 1987.
- وليد سمير فهيم المعداوى، دور الشرطة في حماية الحياة الخاصة من أخطار المعلوماتية، أطروحة دكتوراه، أكاديمية الشرطة كلية الدراسات العليا، دبي، 2011.
- يسري محمد حسن القصاص، الضوابط الجنائية لحرية الرأي والتعبير، دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة طنطا، مصر، 2013.

سابعا: المواقع الإلكترونية

- djamakamel.over-blog.com/2014/11/54609acd-fdbb.html
- lightfragrance.wordpress.com/2010/06/15/digicam
- ngmelabdaa.own0.com/t138.topic
- online.securityfocus.com/infocus/1246
- www.aleqt.com/2010/12/26/article_483399.html
- www.aleqt.com/2013/07/24/article-7727190.html
- www.algeriepolice.dz
- www.arabipcenter.com/pulic/cybercrimelaws
- www.arableagueonline.org
- www.bolsadesantiago.com
- www.cert.org/erports/dsit-workshop.pdf
- www.cnn.com
- www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/default_en.asp
- www.droit-technologie.org
- www.droit-technologie.org/dossiers/e-marketing-et-protection-des-donnees-a-caractere-personnel/
- www.eastlaws.com

- www.ic3.gov
- www.iipa.com
- www.isecur1ty.org
- www.itp.net/arabic/574255
- www.namecheckr.com
- www.oecd.com
- www.waybackmachine.com

II. En Français

1- Les Ouvrages Généraux

- Claude Colombet, Propriété littéraire et artistique et droits voisins, Dalloz Paris, 9ème Éd., 1999.
- Corinne Renault-Brahinsky, Procédure pénale, Gualino Editeur, Paris 7ème Éd., 2006.
- Decocq, J. Montreuil, J. Buisson, Le droit de la police, Litec, 2ème Éd. n°1400, 1998.
- Frédéric Sudre, Droit international et Européen des droits de l'homme. Presses Universitaires de France-PUF, 1995.
- Georges Levasseur, Droit pénal général et procédure pénale, Sirey, 1999.
- Jacques Faget, Sociologie de la délinquance et de la justice pénale, Erès Toulouse, France, 2002.
- Jean Larguier, La procédure pénale, Dalloz, Paris, 17ème Éd., 1999.
- Jean Pradel, André Varinard, Les grands arrêts de la procédure pénale Dalloz, Paris, 2003.
- Jean Pradel, Les rôles respectifs du juge et du technicien dans l'administration de la preuve en matière pénale, Institut d'Études Judiciaires, Presses Universitaires de France, Paris, 1976.
- Jean Pradel, Procédure pénale, Cujas, Paris, 10ème Éd., 2001.
- Michèle-Laure Rassat, Procédure pénale, 2ème Éd., Presses Universitaires de France, 1995.
- Pierre Catala, Informatique et droit pénal, Éd. Cujas, Paris.
- Roger Merle, et André Vitu, "Traité de droit criminel–Problèmes généraux de la science criminelle". Droit pénal général, 6ème Éd., 2000.
- Stefani Gaston, Georges Levasseur, Bernard Bouloc, Procédure pénale Dalloz, Paris, 1993.

- Xavier Linant de Bellefonds, Alain Hollande, Droit de l'informatique et de la télématique, Delmas, 1990.

2- Les Ouvrages Spéciaux

- André Vitalis, Informatique, Pouvoir et Libertés, Economica, 1981.
- Basia Spalek, Crime Victims, Theory, Policy and Practice, Palgrave Macmillan, London, United Kingdom, 2nd Ed., 2006.
- Donn B. Parker, Combattre la criminalité informatique, Oros, Paris, 1985.
- Donn B. Parker, Fighting Computer Crime: A New Framework for Protecting Information, Wiley, Hoboken, New Jersey, United States, 1998.
- Emmanuel Molina, La liberté de la preuve des infractions en droit français contemporain, Presses Universitaires d'Aix-Marseille, 2001.
- H. Alterman, A. Bloch, La fraude informatique, Gazette du Palais, 1988.
- Jacques Georgel, Les libertés de communication : contrôle d'identité écoute téléphonique, vidéosurveillance, Dalloz, Paris, 1996.
- Larrffeu J., Protection d'une Marque Renommee Contre le Cyberpritage Expertises, 1999.

3- Les Articles

- Cecelia Bucki, Le Conflit entre Marque et Nom de Domaine, Revue du droit de la propriété intellectuelle, de l'information et de la concurrence Genève, 2000.
- Cédric Manara, A propos du caractère des noms de domaine, Droit du Commerce Électronique, Dalloz, n°08, 2000.
- Charlotte-Marie et Pitrat-Laurent le veneux, Protection du consommateur et des données personnelles.
- Coralie Ambroise-Castérot, La preuve, une question de loyauté?, Actualité Juridique Pénal, 2005.
- Coralie Ambroise-Castérot, Recherche et administration des preuves en procédure pénale, la quête du Graal de la Vérité, Actualité Juridique Pénal Dalloz, Paris, 2005.
- Etienne Montero, "Premières considérations sur les questions de responsabilité liées aux paiements par WAP." Transferts électroniques de fonds. Académia Bruylant, 2001.
- Francis Baillet, Internet: le droit du cybercommerce: le guide pratique et juridique. Éd., Strategies, Connecticut, United States, 2001.

- Jean Larguier, Anne-Marie Larguier, La protection des droits de l'homme dans le procès pénal, RIDP (Revue internationale de droit pénal) Vol. 37 n°01, 1966.
- M. Blondet, Les ruses et artifices de la police au cours de l’enquête préliminaire, Juris-Classeur périodique, 2ème Éd., 1958.
- Mutter Maler (C.J.A.), Traite de la preuve en matière criminelle, Trad Alexandre IMP, Librairie générale de jurisprudence, Paris, 1884.
- P. Bouzat, La loyauté dans la recherche des preuves, in problèmes contemporains de procédure pénale, Mélanges Hugueney, Sirey, 1964.
- Patrick Auvret, L'application du droit de la presse au réseau internet Juris-Classeur périodique, Paris, Vol. 108, n°08, 1999.
- Pierre Bouzat, La loyauté dans la recherche des preuves, Mélanges Hugueney, Sirey, 1964, n° 03.
- Rene Garraud, Traité Théorique et Pratique d'Instruction Criminelle et de Procédure Pénale, Vol. 01, Creative Media Partners, 2018.
- Renée Koering-Joulin, "La dignité de la personne humaine en droit pénal." dans Marie-Luce Pavia, Thierry Revet, La dignité de la personne humaine Economica, Paris, 1999.
- Thierry Léonard, E-marketing et protection des données à caractère personnel, Publié le 22/05/2000.

4- Les Thèses

- Ali Rached, de l'intime conviction de juge, thèse, Paris, 1942.

III. In English

1- General books

- Francois Debrix, Tabloid Terror: War, Culture, and Geopolitics, Routledge 2007.
- Malcolm Anderson, Policing the World: Interpol and the Politics of International Police Co-operation, Clarendon Press, Oxford, United Kingdom, 1989.
- Philipp Brunst, Cyberterrorism: The Use of the Internet for Terrorist Purposes, Council of Europe Publishing, 2007, p09.
- Teri Bidwell, Hack Proofing Your Identity in The Information Age Syngress, 2002.

2- Specialized books

- Albert Marcella Jr., Robert S. Greenfield, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes Auerbach Publications, CRC Press, 1st Ed., 2002, ISBN: 9780849309557.
- Basia Spalek, Crime Victims, Theory, Policy and Practice, Palgrave Macmillan, London, United Kingdom, 2nd Ed., 2006.
- Bryan Clough and Paul Mungo, Approaching Zero: Data Crime and the Computer Underworld, Faber & Faber, London, United Kingdom, 1992.
- David J. Icove, Karl A. Seger, William Von Storch, Computer crime: a crimefighter's handbook, O'Reilly & Associates, Sebastopol, California United States, 1995.
- David Wall, Crime and the Internet, Routledge, Abingdon, United Kingdom, 1st Ed., 2001.
- Donn B. Parker, Susan Nycum, S. Stephen Oüra, Computer abuse: final report, Stanford Research Institute, 1973.
- Eoghan Casey, Digital Evidence and Computer Crime, Forensic Science Computers, and the Internet, Academic Press, Cambridge, Massachusetts United States, 3rd Ed., 2011.
- Gregory Kipper, Wireless Crime and Forensic Investigation, CRC Press Florida, United States, 2007.
- Hugo Cornwall, Data Theft, Computer Fraud, Industrial Espionage and Information Crime, Mandarin, 1990.
- Ian Walden, Computer Crimes and Digital Investigations, Oxford University Press, Oxford, United Kingdom, 2007.

- Jeffrey Ian Ross, John L. French, Criminal Investigations: Cybercrime Chelsea House, Pennsylvania, United States, 2010.
- Johnny Nhan, Policing Cyberspace: A Structural and Cultural Analysis LFB Scholarly Publishing LLC., 2010.
- Jonathan Clough, Principles of Cybercrime, Cambridge University Press Cambridge, United Kingdom, 2nd Ed., 2015.
- Leonard Territo, Neil C. Chamelin, Charles R Swanson, Robert W Taylor Criminal Investigation, McGraw-Hill Education, New York, United States 5th Ed., 1992.
- Paul Bocij, Cyberstalking: Harassment in the Internet Age and how to Protect Your Family, Greenwood Publishing Group, Connecticut, United States, 2004.
- Paul E. Mullen, Michele Pathé, Rosemary Purcell, Stalkers, Their Victims Cambridge University Press, 2000.
- Peter Emeritus Grabosky, Peter Grabosky, Russell Gordon Smith, Gillian Dempsey, Electronic Theft: Unlawful Acquisition in Cyberspace Cambridge University Press, 2001.
- Peter N. Grabosky, Electronic Crime, Pearson Prentice Hall, New Jersey United States, 2007.
- Rein Turn, Willis Howard Ware, Privacy and Security in Computer Systems, RAND Corporation, California, United States, 1975.
- Robin P. Bryant, Investigating Digital Crime, Wiley, 2008.
- Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace ABC-CLIO, California, United States, 2010.
- Thomas A. Johnson, Forensic Computer Crime Investigation, CRC Press Florida, United States, 2005.
- Ulrich Sieber, The International Handbook on Computer Crime: Computer-related Economic Crime and the Infringements of Privacy Wiley, 1986.
- Vera Bergelson, Victims' Rights and Victims' Wrongs: Comparative Liability in Criminal Law, Stanford University Press, California, United States, 2009.

3- Dictionaries

- The Oxford English Dictionary, example first cited in 1984.

4- Articles

- Ann W. Burgess, Timothy Baker, Deborah Greening, Carol R. Hartman Allen G. Burgess, John E. Douglas, Richard Halloran, Stalking Behaviors Within Domestic Violence, Journal of Family Violence, Springer, Berlin Germany, Vol. 12, n°04, 1997.
- Anthony Sammes, Brian Jenkinson, Forensic Computing: A Practitioner's Guide, Springer Science & Business Media, Berlin, Germany, 2013.
- Bruce Sterling, The Hacker Crackdown, Law And Disorder On The Electronic Frontier, Bantam Books, New York, USA, 1992.
- Celia Wells, Stalking, The Criminal Law Response, Criminal Law Review London, England, 1997.
- Christine Sgarlata Chung and David J. Byer, The Electronic Paper Trail Evidentiary Obstacles to Discovery and Admission of Electronic Evidence Boston University, Journal of Science & Technology Law, Boston Massachusetts, USA, 22/11/1998.
- David Thompson, Current Trends in Computer Crime, Computer Control Quarterly, MCB University Press, Bingley, United Kingdom, Vol. 1, n°01 1991.
- Edward M. Wise, Computer Crimes and other Crimes against Information Technology in the United States, Revue Internationale de Droit Pénal Paris, v.64, 1993.
- Emma Ogilvie, Cyberstalking, Trends and issues in crime and criminal justice series, no. 166. Australian Institute of Criminology, Canberra, 2000 p166.
- Emma Ogilvie, Stalking: Legislative, Policing and Prosecution Patterns in Australia, Australian Institute of Criminology, 2000.
- Giorgio Bovenzi, Liabilities of System Operators on the Internet, Berkeley Technology Law Journal, Berkeley Law Admissions Office, University of California, Vol. 11, n°01, 1996.
- J. Laughren, Cyberstalking awareness and education - Sexuality research and social policy, Journal of NSRC, Vol. 04, n°02, 2007.
- Jared Strauss and Kenneth S. Rogerson, Policies for online privacy in the United States and the European Union, Telematics and Informatics Elsevier, Amsterdam, Netherlands, Vol. 19, n°02, 2002.

- John Arquilla, David Ronfeldt, Cyber crime Inquiry Submissions - Australian Banking Association, 2007.
- Jos Dumortier, Patrick Van Eecke, Legal issues and the internet. Internet European Compared Law, Sous la dir, de Georges Chatillon, Bruxelles Bruylant, Bruxelles, Belgique, 2000.
- Katie Dean, The Epidemic of Cyberstalking, WIRED Magazine (www.wired.com), 2000, visit: https://www.wired.com/2000/05/the-epidemic-of-cyberstalking/.
- L. Torrecillas, "Mobile phone addiction in teenagers may cause severe psychological disorder." Medical studies, Vol. 14. n°03, 2007.
- Louise Ellison, Yaman Akdeniz. "Cyber-stalking: the Regulation of Harassment on the Internet." Criminal Law Review, Sweet and Maxwell London, United Kingdom, N°29, 1998.
- McGraw D. K., Sexual harassment in cyberspace: The problem of unwelcome email. Rutgers Computer and Technology Law Journal, n°21 1995.
- Michael Kunz, Patrick Wilson, Computer crime and computer fraud Report Submitted to the Montgomery County Criminal Justice Coordinating Commission, State of Maryland, United States, 2004.
- Naomi Harlin Goodno, Cyberstalking, a new crime: Evaluating the effectiveness of current state and federal laws, Missouri Law Review, n°72 2007.
- Orin S. Kerr, Digital evidence and the new criminal procedure, Columbia Law Review, Vol. 105, 2005.
- Raymond Wacks, Privacy in cyberspace: personal information, free speech and the Internet, Privacy and Loyalty, Oxford, 1997.

5- Participations and Contributions

- B. Etter, Computer Crime, Australian Institute of Criminology, 4th National Outlook Symposium on Crime in Australia – New Crimes of New Responses, Australian Institute of Criminology, Canberra, 2001.

الفهرس

إهـــداء .....

شكر وعرفان .....

مقدمة 1

الباب الأول: ماهية جرائم التكنولوجيا الحديثة 9

الفصل الأول: المحددات المفاهيمية لجرائم التكنولوجيا الحديثة 10

المبحث الأول: مفهوم جرائم التكنولوجيا الحديثة 11

المطلب الأول: تعريف جرائم التكنولوجيا الحديثة 12

المطلب الثاني: نشأة وتطور جرائم التكنولوجيا الحديثة 25

المطلب الثالث: خصائص جرائم التكنولوجيا الحديثة 33

المبحث الثاني: ارتكاب جرائم التكنولوجيا الحديثة 44

المطلب الأول: أطراف جرائم التكنولوجيا الحديثة 45

المطلب الثاني: وسائل وتقنيات ارتكاب جرائم التكنولوجيا الحديثة 62

الفصل الثاني: أهم الجرائم المرتكبة باستخدام وسائل التكنولوجيا الحديثة 88

المبحث الأول: جرائم التكنولوجيا الحديثة المتعلقة بتقنية الاتصالات الحديثة 89

المطلب الأول: جرائم الاعتداء على الحياة الخاصة للأفراد 89

المطلب الثاني: جرائم التكنولوجيا الحديثة الماسة بالشرف والاعتبار 100

المطلب الثالث: الجرائم الجنسية الإباحية والواقعة على الآداب العامة عن طريق وسائل تقنية المعلومات الحديثة 110

المطلب الرابع: جرائم نظم الاتصالات 118

المطلب الخامس: جرائم التجسس وإنشاء المواقع الإرهابية 125

المبحث الثاني: جرائم التكنولوجيا الحديثة ذات الصبغة المالية 130

المطلب الأول: السرقة والتزوير في جرائم التكنولوجيا الحديثة 130

المطلب الثاني: النصب وإساءة الائتمان في جرائم التكنولوجيا الحديثة 137

المطلب الثالث: المساس بالملكية الفكرية في جرائم التكنولوجيا الحديثة 142
المطلب الرابع: جرائم غسيل الأموال والبطاقات المالية المتصلة بالتكنولوجيا الحديثة..... 147
الباب الثاني: آليات مكافحة جرائم التكنولوجيا الحديثة 157
الفصل الأول: الأحكام الموضوعية لمكافحة جرائم التكنولوجيا الحديثة 158
المبحث الأول: آفاق مكافحة جرائم التكنولوجيا الحديثة 159
المطلب الأول: الجهود المبذولة على المستوى الخارجي 159
المطلب الثاني: الجهود المبذولة على المستوى الداخلي 181
المبحث الثاني: دور الأجهزة الأمنية في التصدي لجرائم التكنولوجيا الحديثة 192
المطلب الأول: مواجهة السلطة التنفيذية لجرائم التكنولوجيا الحديثة 192
المطلب الثاني: التعاون الدولي في مواجهة جرائم التكنولوجيا الحديثة 208
الفصل الثاني: الأحكام الإجرائية لمكافحة جرائم التكنولوجيا الحديثة..... 226
المبحث الأول: إجراءات جمع الدليل الإلكتروني 227
المطلب الأول: دور الضبط القضائي في جرائم التكنولوجيا الحديثة 228
المطلب الثاني: الإجراءات التقليدية لجمع الدليل الإلكتروني..... 241
المطلب الثالث: الإجراءات الحديثة لجمع الدليل الإلكتروني 257
المبحث الثاني: حجية الدليل الرقمي في إثبات جرائم التكنولوجيا الحديثة 272
المطلب الأول: مدى اقتناع القاضي بالدليل الرقمي..... 273
المطلب الثاني: المسؤولية الناشئة عن جرائم التكنولوجيا الحديثة والعقوبات المقررة لها..... 288
خاتمة 307
قائمة المصادر والمراجع 309
الفهرس 338

ملخص

حقق التطور التكنولوجي في العصر الحديث في مجال التقنية والمعلوماتية للبشرية الرقي والازدهار في شتى مناحي الحياة خاصة في مجال الاتصالات السلكية واللاسلكية حتى أصبح يطلق عليه تسمية العصر الرقمي أو الافتراضي الذي صارت فيه المعلومات معيارا لتطور الشعوب ونموها، فبالرغم من هذا التطور العلمي الهائل إلا أنه جلب معه مخاطر جمة طوعها المجرم المعلوماتي وأصبحت سلاحا لا يستهان به في ممارسة النشاطات الإجرامية، وبهذا ظهرت طائفة جديدة من الجرائم المستحدثة فقد أدى سوء استخدام تقنية المعلومات الحديثة إلى تسهيل ارتكاب الكثير من الجرائم التقليدية على نطاق واسع على غرار جرائم السرقة وجرائم التجسس وانتهاك حرمة الحياة الخاصة والمراسلات والجرائم الإرهابية وتلك المخلة بالآداب العامة...إلخ، كما نتج عن سوء استخدام هذه التقنية إلى بروز نوع جديد من الجرائم ذو طبيعة خاصة أصطلح على تسميتها جرائم التكنولوجيا الحديثة.

فبالرغم من أهمية جرائم التكنولوجيا الحديثة وخطورتها وفداحة الأضرار التي تلحقها بالدول التي سارعت إلى إدخال التقنية المعلوماتية في أنظمتها الأمنية، الاجتماعية والاقتصادية، إلا أن هناك من الدول من تخلفت عن تكريس الإطار القانوني الذي يحمي تلك المنظومات من الاعتداء عليها أو سوء استخدامها، لاسيما من الأفعال الضارة التي ترقى إلى وصف الجرائم وتقصيها وتقديم مرتكبيها أمام العدالة وتعزيز مبدأ الإثبات بتكريس الدليل الإلكتروني وتقنينه. والجزائر ليست في منأى عن تأثير التكنولوجيا الحديثة فقد سعت في هذا الإطار إلى إقرار قانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بالإضافة إلى تعديل قانون العقوبات وكذا قانون الإجراءات الجزائية، ليس هذا فقط؛ بل أقر أيضا قانونا يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية لمواكبة التطورات التي أنتجتها التكنولوجيا الحديثة ووسائلها أين عجزت القوانين التقليدية الجزائية الموضوعية والإجرائية عن مواجهتها.

Summary

The modern age witnessed so much progress and prosperity due to breakthroughs made in the fields of technology and informatics – especially in the area of wired and wireless communication – that it has been termed as the digital age or the virtual one.

In this age, information has become the standard of measurement for the progress and development of communities. But it also gave rise to some major threats. The modern criminal now misuses such breakthroughs as an easy-to-use weapon that can't be countered with the same ease. This gave birth to a new type of unprecedented crimes such as electronic theft espionage, privacy violation, interception of communications, terrorism, disorderly conduct crimes … etc. One type of these unprecedented crimes related to our topic is crimes of modern technology.

So, despite the significance of modern technology crimes and the devastating impacts and damages in countries and communities that were among the first to integrate information technologies in their social, economic, and security systems, there are still many nations that remain without, or with a weak, legal framework to protect them. Such framework should protect them from offenses or misuses, especially harmful deeds that are considered as crimes. The framework should provide the abilities to conduct investigations and deliver offenders to justice, and support and legalize the principle of electronic proof. Algeria is no further from the effects of this age. Thus, it has sought to create the legal framework with the law 09-04 that states the regulations of protections against crimes related to modern technology, and also with embedding of changes to the criminal law and the law of penal procedures, as well as the issue of a law defining the general regularities related to postal services and elecrtronic communications. Its aim is to keep up with the innovations brought by modern technologies and means, which the traditional laws and penal procedures failed to face.