جامعة مولود معمري – تيزي وزو–
كلية الحقوق و العلوم السياسية
قسم القانون – نظام (ل.م.د)

عنوان المذكرة:

الحماية الجنائية من جرائم الانترنت في القانون الجزائري

مذكرة لنيل شهادة الماستر في القانون العام
تخصص : القانون الجنائي والعلوم الإجرامية

إعداد الطلبة:
آفـلـو سعـاد
واقيني ناديـة

إشـراف الأستاذة:
د/ د وا ن فاطمـة

لجنة المناقشة:

د/ حدوش وردية، أستاذة محاضرة (ب)، جامعة مولود معمري، تيزي وزو .....رئيسة؛

د/ دوان فاطمـة، أستاذة مساعدة قسم (ب)، جامعة مولود معمري، تيزي وزو..... مشرفة و مقررة؛

د/ زرورو ناصر، أستاذ محاضر (ب)، جامعة مولود معمري، تيزي وزو..... ممتحنا.

تاريخ المناقشة: 03-07-2018

إهداء

أهدي هذا العمل المتواضع إلى الوالدين العزيزين، حفظهما الله و أطال في عمرهما،

إلى إخوتي وأخواتي،

إلى الزميلة "سعاد" التي شاركتني العناء في إعداد هذه المذكرة،

وإلى كل من كان لنا عوناً في إنجازه من قريب أو بعيد.

ناديـــــة

إهداء

أهدي هذا العمل المتواضع إلى الوالدين العزيزين، حفظهما الله و أطال في عمرهما،

إلى إخوتي وأخواتي،

إلى الزميلة "نادية" التي شاركتني العناء في إعداد هذه المذكرة،

وإلى كل من كان لنا عوناً في إنجازه من قريب أو بعيد.

سعـــــاد

كلمة شكر و عرفان

نحمد الله ونشكره على توفيقه لنا في إنجاز هذه المذكرة.

كما نتقدم بشكرنا العميق للدكتورة دوان فاطمــة، على مساعدتها لنا وتوجيهاتها التي كان لها دور كبير في إنجاز هذه المذكرة.

كما نتوجه بالشكر إلى الأساتذة أعضاء لجنة المناقشة، على اطلاعهم للمذكرة وإبداء ملاحظاتهم فيها من أجل إثراءها.

صفحة المختصرات

الهيئة : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

ج ر : جريدة رسمية

د ج : دينار جزائري

ق.إ.ج.ج : قانون الإجراءات الجزائية الجزائري

ص : صفحة

ص ص : من صفحة إلى صفحة

م : المادة

مقدمـــة

ارتبطت الجريمة بالإنسان منذ أول وجود له على وجه الأرض، ولأنه اجتماعي بطبعه فإن الاحتكاك بغيره من البشر هو أمر حتمي وضروري. غير أن هذا الاحتكاك قد يشكل في العديد من الأحيان السبيل أمام التعرض لاعتداءات تصل إلى درجة وصفها بالجريمة، فهذه الأخيرة هي نتاج طبيعي للحياة الاجتماعية واختلاف وتضارب مصالح الأفراد داخل الجماعة.

وقد تطورت الجريمة مع المراحل المختلفة التي يمر بها الإنسان باختلاف المجالات التي يخوضها مهما كانت متعددة أو حديثة العهد، إذ أن العديد من الجرائم لم يعد لها وجود أو رفع عنها وصف الجريمة، في حين هناك البعض الآخر يعرف تطوراً يتماشى مع المستجدات التي تطرأ على الحياة الاجتماعية للإنسان عبر مختلف الأزمنة والأمكنة، فتباين هذه الأخيرة أدى إلى تباين التكييف الذي تتخذه بعض الأفعال، فتعتبر مباحة في مكان ما أو في حقبة زمنية معينة في حين تتخذ وصف الجريمة في مكان آخر أو حقبة زمنية أخرى، خاضعة في ذلك إلى الاختلاف في النظام الاجتماعي والسياسي للمجتمعات، والمستوى الثقافي والعلمي والمعتقد الديني والأعراف المتبعة فيها الذي يلعب دوراً كبيراً في تكريس هذا التباين والاختلاف في التكييف.

شهد العالم خصوصاً في الآونة الأخيرة، ثورة غير مألوفة أفرزتها العولمة، وهي ما يطلق عليها بتسمية "الثورة المعلوماتية"، التي مست العديد من الجوانب في حياة الفرد والدول على حد سواء. هذه الثورة التي ساهمت بشكل كبير في تقدم النمط المعيشي لاسيما من خلال توفير عاملي السرعة والشمولية، فأصبحت من الضروريات التي لا يمكن الاستغناء عنها من أجل تسيير الحياة اليومية للأفراد والمؤسسات.

تثير هذه الثورة المعلوماتية بالرغم من مجموع المزايا التي تحظى بها وأهميتها البالغة في شتى المجالات، العديد من الإشكالات لاسيما ما يتعلق بالجانب الإجرامي، حيث أصبحت في الوقت ذاته الوسيلة والغاية لارتكاب العديد من الجرائم، حيث تجاوز استخدامها الهدف المرجو من اختراعها، الذي كان يقتصر على تطوير مختلف المجالات لاسيما المجال العسكري والبحث العلمي بما يخدم البشرية جمعاء، ليمتد هذا الاستخدام ليشكل خطراً حقيقياً وجسيماً لها.

ساهم الإقبال الكبير الذي تشهده شبكة الانترنت في انتشار الجرائم المتصلة بهذا المجال، سواء تلك التي ترتكز على استخدام الأجهزة الالكترونية المتصلة بهذه الشبكة كوسيلة متطورة لارتكاب جرائم عرفتها البشرية منذ القدم، أو تلك التي ترتكب على مستخدميها سواءً لاسيما عن طريق المساس بخصوصيات العالم الافتراضي الذي نجح في القضاء على الحواجز الجغرافية والسياسية للمجتمعات في مختلف أنحاء العالم.

أصبح للإجرام صورة أكثر تطوراً وأكثر خطورة، نظراً لكونها ترتكب بأحدث الوسائل والأجهزة الالكترونية من جهة، التي تضمن السرية وسهولة ارتكابها وإخفاء آثارها من جهة أخرى. هذا التطور الذي لحق بشكل الجريمة كان له دور أساسي في بروز شبكات إجرامية لا تحتاج لتشكيلها تنظيم مادي ومقرات محددة لممارسة نشاطها، والتنقل عبر مختلف النقاط من الدولة الواحدة أو مختلف الدول من أجل التنفيذ، وإنما يكفي التواجد المادي للجاني أمام جهاز الكمبيوتر المتصل بشبكة عنكبوتية حتى تتحقق هذه الجريمة، وإن كانت الخبرة والدراية تعتبر شرط أساسي لارتكاب بعض الجرائم الالكترونية ذات الطابع الخاص كالجوسسة مثلا، إلا أنها غير ضرورية بل يكفي المعرفة السطحية لاستخدام هذا الجهاز من أجل ارتكاب جرائم تؤدي إلى الإضرار بالأشخاص في أموالهم وشخصهم واعتبارهم وشرفهم.

تتجسد خطورة هذه الجرائم كذلك، من خلال اتخاذها الطابع الدولي بحيث ترتب آثار قد تتجاوز إقليم الدولة الواحدة، لاسيما عندما تستهدف بشكل أساسي الأمن الاقتصادي والسياسي للدول. ولعل لجوء الناشطين في هذا المجال الذين يحملون تسمية "القراصنة" إلى عقد مؤتمرات بهدف تبادل المعلومات والخبرات وفنون استخدام تكنولوجيا المعلومات وتعليم كيفية استخدام البرامج الخاصة المستحدثة لاختراق الحواسيب، من بين أهم العوامل التي أضفت الطابع العالمي لهذه الجريمة.

سعت الدول على هذا النحو، إلى بذل جهود داخلية وأخرى دولية من أجل الحد من هذه الجرائم والعمل على محو آثارها واستدراك القصور لاسيما التشريعي الذي تشهده مختلف الدول في هذا المجال، حيث حاولت وضع نصوص قانونية وتدابير أمنية في سبيل تحقيق ذلك، والتي تميزت في معظمها بالطابع العام وصعوبة التحيين والمواكبة.

يشكل وضع الإطار القانوني لمكافحة هذه الجرائم، من بين الانشغالات التي تشغل بال الدول لاسيما تلك التي تعاني من نقص في الخبرة والعتاد التكنولوجي كـ(الجزائر) مثلاً، وذلك لكون مواجهة مثل هذا النوع من الجرائم يحتاج إلى تكاثف جهود تشريعية ومؤسساتية مدعمة بإمكانيات مادية وبشرية وتقنية تعمل على عدم تمكين الجناة من الإفلات من العقاب.

وعليه تتمركز إشكالية هذه الدراسة على وجه الخصوص في معرفة **النظام القانوني الجنائي الذي اعتمده المشرع الجزائري من أجل مكافحة جرائم الانترنت؟**

حاولنا الإجابة على هذه الإشكالية باعتماد منهجي الاستقراء والتحليل لنصوص قانون العقوبات بشكل عام والنصوص القانونية ذات الصلة بجرائم الانترنت بشكل خاص، من أجل تبيان مضمون هذه الجرائم وتكييفها والجوانب المتعلقة بنظامها القانوني (الفصل الأول)، إضافة إلى التركيز على سبل الوقاية والمكافحة التي اعتمدها المشرع الجزائري من أجل الحد منها ومعاقبة مرتكبيها (الفصل الثاني).

الفصل الأول

النظام القانوني لجرائـــــم الانترنـــت

تعد جرائم الانترنت من الجرائم الحديثة العهد، التي تتمتع بخطورة جسيمة على الفرد والمجتمع معاً، وقد ساعد في بروز هذه الخطورة العديد من المميزات التي يتمتع بها الانترنت كنظام معلوماتي متقدم، بحيث تدفع بالمجرمين إلى ارتكابها قصد تحقيق أهداف شخصية وأرباح مادية معتبرة.

ويعتبر الانترنت سلاح ذو حدين، يتقرر دوره الإيجابي أو السلبي بحسب طريقة استخدامه، بحيث يلعب دورا هاماً في تسهيل المعاملات وكسب الوقت والمال والجهد عند استخدامه بشكل فعال وضمن ما تنص عليه القوانين الخاصة به. غير أنه قد يصبح وسيلة جد خطيرة يعكس سلباً على المجتمع بصفة عامة وعلى المستهدفين من العمليات الإجرامية بصفة خاصة (المبحث الأول)، هذه الممارسات الإجرامية لا تقتصر على جانب معين فحسب وإنما تمتد لتشمل مختلف المجالات الاقتصادية، والسياسية والاجتماعية (المبحث الثاني).

المبحث الأول

ماهية جرائـــم الانترنــت

ساهمت العولمة بشكل كبير في بروز جرائم الانترنت، التي أخذت حيزاً كبيراً في الدراسات الأكاديمية التي ركزت على التعريف بها وتبيان مفهومها (المطلب الأول)، كما تتميز بمجموعة من الخصائص التي تنفرد بها على خلاف الجرائم الأخرى وإن كانت تشترك معها في عدم مشروعية الفعل الإجرامي (المطلب الثاني)، ويستعين الجاني في هذه الجرائم بعدة أساليب لارتكابها تتميز بارتباطها الوثيق بعالم التكنولوجيا الحديثة (المطلب الثالث).

المطلب الأول

مفهوم جرائم الانترنـــــت

سبق الذكر أن جرائم الانترنت من الجرائم الحديثة، لذا تثير العديد من الإشكالات القانونية والعملية، ومنه كانت التعريفات الواردة بخصوصها متعددة ومتباينة ضيقاً واتساعاً (الفرع الأول)، لتتميز عن بقية الجرائم بمجموعة من الخصائص (الفرع الثاني)، مما يؤدي بنا إلى استنتاج طبيعتها القانونية (الفرع الثالث)، ودوافع ارتكابها (الفرع الرابع).

الفرع الأول

تعريف جرائم الانترنـــت

اختلف كل من الفقه (أولا)، والتشريع (ثانيا)، في تعريف جرائم الانترنت بحيث استقل كل منهما بتعريفه الخاص به.

أولا: التعريف الفقهـــــي

نشير في البداية أن الفقهاء يطلقون على جرائم الانترنت مصطلحات متعددة[1]، فنجد من يعرفها على أنها "*جريمة الحاسب الآلي هي الغش والسرقة والابتزاز وغيرها من أنواع الجريمة وذلك بتسخير أو إساءة استخدام الحاسب الآلي*"[2]، وهناك من يطلق عليها مصطلح "*الجريمة السبيرانية*" الذي يعد من المصطلحات الأكثر استعمالاً لاسيما في الدراسات الأكاديمية، ويقصد بالنظام السبيراني: "*كل مكونات الحاسب الآلي المادية HardWare والمعنوية SoftWare، وشبكات الاتصال الخاصة به NetWorks، أو هي مجموع عناصر مادية وغير مادية يمكن باجتماعها العمل الفوري مع المعلومة*"[3]، أما المقصود بالجريمة السبيرانية، فهي : " *فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات، يهدف إلى الاعتداء على الأموال المادية أو المعنوية [أو الاعتداء على خصوصية للأفراد]، أو هي عمل أو امتناع يأتيه الإنسان إضراراً بمكونات الحاسب وشبكات الاتصال الخاصة به ... هي الجريمة التي يكون النظام المعلوماتي فيها وسيلة لارتكاب جريمة تقليدية، إما ضد الأموال كالتحويل الالكتروني غير المشروع للأموال، أو ضد الأشخاص كجريمة السب أو القذف عبر الانترنت*"[4].

---

[1]– يعود السبب وراء التباين الذي تشهده هذه الجريمة من حيث المصطلحات إلى تباين الأساس الذي تقوم عليه، فهناك من يطلق عليها بجرائم معلوماتية بالنظر إلى كونها تستهدف المعلومات المخزنة في الأجهزة، أو جرائم الحاسوب باعتبارها تنصب على أجهزة الكمبيوتر، وتسمى أيضا بجرائم الانترنت لأنها تشترط من أجل إتمام هذه الجريمة اتصال الضحية بشبكة الانترنت. حول عدم توحيد المصطلح المطلق على جرائم الانترنت، أنظر: حديد نوفيل وبوزيد هجيرة سومية، "نجاح مشروع الحكومة الالكترونية اجتناب الفشل من خلال إدراك المخاطر الالكترونية"، مجلة علوم الاقتصاد والتسيير والتجارة، العدد 31، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة الجزائر3، 2015، ص197.

[2]– نقلا عن: حفصي عباس، جرائم التزوير الالكترونية، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في العلوم الإسلامية، تخصص شريعة وقانون، كلية العلوم الإنسانية والعلوم الإسلامية، جامعة وهران 1 أحمد بن بلة، 2015، ص 3.

[3]– دريس نبيل، "الجريمة السيبرانية بين المفاهيم والنصوص التشريعية الجزائر أنموذجا"، مجلة القانون والمجتمع، المجلد 5، العدد 2، جامعة أدرار، 2017، ص 24.

[4]– دريس نبيل، المرجع نفسه، ص30.

غير أن مثل هذه التعريفات تنصب على الجريمة الالكترونية التي تكتمل أركانها حتى بدون استخدام شبكة الانترنت، لذا نلاحظ عدم الدقة في التعريف الوارد بخصوص هذه الجريمة.

نجد في المقابل بعض التعريفات التي اعتمدت بشكل أساسي على شبكة الانترنت لتحديد مضمون هذه الجريمة، بحيث تعرف على أنها: "*كل فعل، أو امتناع عمدي، ينشأ عن الاستعمال غير المشروع للانترنت، بطريقة مباشرة أو غير مباشرة، بهدف الاعتداء على الأموال والأشياء المعنوية*"[1].

وقد عرفها "محمد علي العريان" بأنها: "*كل فعل إيجابي أو سلبي عمدي، يهدف إلى الاعتداء على تقنية المعلوماتية أيا كان غرض الجاني*"[2].

كما عرفها الفقيه الفرنسي "Massa" بأنها: "*الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية لغرض تحقيق الربح*"، أما الفقيه الألماني "تاديمان" فحاول تعريفها بكونها: "*كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب الآلي*"، في حين تم تعريفها في الفقه القانوني المصري بأنها: "*نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف إلى الاعتداء على الأموال أو المعنوية*"، أما خبراء المنظمة الأوروبية للتعاون والتنمية الاقتصادية فقد عرفتها بأنها: "*كل سلوك غير مشروع ومناف للأخلاق أو غير مسموح به يرتبط بالمعالجة الآلية للبيانات أو بنقلها*"[3].

---

[1]– نقلا عن: بعرة سعيدة، الجريمة الالكترونية في التشريع الجزائري – دراسة مقارنة، مذكرة لنيل شهادة ماستر، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2016، ص 13.

[2]– نقلا عن: بعرة سعيدة، المرجع نفسه، ص 13.

[3]– نقلا عن: الشمري غانم مرضي، الجرائم المعلوماتية، الدار العلمية الدولية للنشر والتوزيع، الطبعة الأولى، عمان، 2016، ص ص 24 – 26.

ثانيا: التعريـــف القانونـــي

عرف المشرع الجزائري الجريمة الالكترونية من خلال م1/2 من القانون المتضمن "القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها"، التي تنص على أن: "*جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية*"[1].

نلاحظ من خلال هذه المادة أنها تتميز بالطابع التنفيذي لنصوص قانون العقوبات، لاسيما ما يتعلق بالقسم السابع مكرر المعنون بـ "*المساس بأنظمة المعالجة الآلية للمعطيات*"[2]، المندرج ضمن الفصل الثالث المعنون بـ "الجنايات والجنح ضد الأموال" منه[3]، والذي سلط الضوء على العقوبات المقررة لهذه الجريمة دون التطرق إلى تعريفها أو تحديد أركانها، وإنما تم التأكيد على كون هذه الجريمة من الجنح والجنايات الذي يثبت مدى خطورتها وجسامتها.

تعرف جرائم الانترنت عموماً في نطاق القانون الجنائي بأنها: "فعل غير مشروع، صادر عن إرادة إجرامية يقرر له القانون عقوبة، أو تدبيراً احترازياً..."، وعليه فإن هذه الجريمة تتأسس

---

[1]– أنظر م1/2 من قانون رقم 09 – 04 المؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 47 صادر بتاريخ 16 أوت 2009.

[2]– يعرف نظام المعالجة الآلية للمعطيات بأنه: "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، والتي تتكون كل منها الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط والتي تربط بينها مجموعة من العلاقات التي عن طريقها يتم تحقيق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضعا لنظام المعالجة الفنية". نقلا عن: بوزيدي مختارية، ماهية الجريمة الالكترونية، مداخلة مقدمة في الملتقى الوطني المعنون بـ "آليات مكافحة الجرائم الالكترونية في التشريع الجزائري"، الجزائر، مركز جيل البحث العلمي، 29 مارس 2017، ص 12.

[3]– تم تنظيم العقوبات المقررة لهذه الجريمة في المواد 394 مكرر إلى م394 مكرر7 من القسم السابع مكرر المعنون بـ "المساس بأنظمة المعالجة الآلية للمعطيات". الأمر رقم 66 – 156 المؤرخ في 08 جوان 1966، يتضمن قانون العقوبات، المعدل والمتمم بـ المعدل والمتمم بالقانون رقم 04 – 15 المؤرخ في 10 نوفمبر 2004، ج ر عدد 71 صادر بتاريخ 10 نوفمبر 2004.

على تبيان عناصرها المحددة قانوناً التي تشكل الركن الشرعي لها، والذي يعد الأساس الجوهري للمساءلة الجنائية إعمالاً لمبدأ "لا جريمة ولا عقوبة إلا بنص"، ومن ثمة فإنه يتم استبعاد كل أشكال القياس في هذا النوع من الجرائم الذي يتم اللجوء إليه فقط في حالة دراسة الظاهرة الإجرامية وليس الجريمة في حد ذاتها[1].

الفرع الثاني

خصائص جرائم الانترنت

تتمتع جرائم الانترنت على خلاف الجرائم الأخرى بخصائص تنفرد بها، بحيث تعتبر من الجرائم الحديثة النشأة (أولا) والعابرة للحدود (ثانيا)، والتي تتميز بالسرية في ارتكابها وسهولة إخفاء آثارها (ثالثا)، مما يجعلها تأخذ وصف "الجريمة الناعمة" (رابعا)، وهو ما يؤدي إلى صعوبة إثباتها (خامسا).

أولا: جرائم الانترنت جرائم حديثة النشأة

تعتبر جرائم الانترنت من الجرائم التي برزت في القرن الأخير[2] والتي ساهمت العولمة بشكل كبير في بروزها، بحيث أن التقدم التكنولوجي الذي شهدته الحقبة الأخيرة من الزمن استعجل في ميلاد شبكة عنكبوتية نجحت في ربط الاتصال بين دول العالم وجعله قرية صغيرة، ملغياً بذلك البعد الزماني والجغرافي. وتتميز هذه الجرائم باستخدام تقنيات تفوق قدرة الأجهزة

[1]– سياب حكيم، الإعلام الآلي والقانون، الطبعة الأولى، دار وائل للنشر والتوزيع، عمان، 2014، ص 127.

[2]– يعود أول بروز لجرائم الانترنت في الستينات من القرن الماضي، تجسدت من خلال المساس بالبيانات المسجلة في أجهزة الكمبيوتر وأعمال التجسس، غير أنها لم تبرز كظاهرة إجرامية إلا في سنوات السبعينات نظراً للتطور الحاصل في مجال الدراسات القانونية والأكاديمية لهذه الظاهرة. لأكثر تفصيل حول هذا التطور في بروز جرائم الانترنت، أنظر: بونعارة ياسمينة، "الجريمة الالكترونية"، مجلة المعيار، كلية أصول الدين، جامعة الأمير عبد القادر، قسنطينة، 2015، ص5.

الرقابية للدولة، الأمر الذي يشكل خطراً حقيقياً على أمن الدول وسلامتها نظراً لعدم توفر الوسائل الكفيلة بمواجهتها ومكافحتها[1].

ثانيا: جرائم الانترنت جرائم عابرة للحدود

يعود السبب في انتشار شبكة الانترنت عبر العالم إلى الاستخدام الواسع لأجهزة الحاسوب، ونظراً لانتفاء القيود الزمنية والمكانية لهذا الاستخدام، فإن هذه الجريمة قد تتحقق في إقليم دولة واحدة كما قد تمتد لتشمل أقاليم دول مختلفة، ومن ثمة اختلاف مكان ارتكاب الجريمة عن مكان المجني عليه، الأمر الذي دفع بضرورة التعاون في مجال مكافحة هذه الجريمة عن طريق تكريس قوانين داخلية وأخرى دولية، وبخصوص هذه الأخيرة نجد أن التباين والاختلاف في تكييف هذه الأفعال التي قد تكون أفعال مباحة في بلد ما في حين تكون مجرمة في بلد آخر ساهم في صعوبة توحيد سبل مكافحتها وردعها[2].

نشير في هذا الصدد أن جرائم الانترنت في الجزائر عرفت تطوراً من حيث ارتكابها، فبعد أن كانت جريمة فردية يقتصر ارتكابها على مجموعة من الأفراد كل على حدى، أصبحت جريمة منظمة ترتكب من خلال شبكات إجرامية تستهدف فئات مختلفة من المجتمع وذلك لتحقيق أهداف مادية أو استخدامها كوسيلة لارتكاب جرائم أخرى كاختطاف الأطفال أو الابتزاز ومن ثمة تحولها من جريمة بسيطة إلى جريمة مركبة ومن جريمة وقتية إلى جريمة مستمرة[3].

---

[1]– جواحي عبد الستار، جرائم الحاسوب – دراسة مقارنة بين الشريعة الإسلامية والقانون الجزائري، مذكرة لنيل شهادة الماستر في العلوم الإسلامية، كلية العلوم الاجتماعية والإنسانية، جامعة السعيد حمه لخضر، الوادي، 2015، ص 9.

[2]– عبد الله دغش العجمي ، المشكلات العملية والقانونية للجرائم الالكترونية – دراسة مقارنة، رسالة لنيل شهادة ماجستير في القانون العام، جامعة الشرق الأوسط، الكويت، 2014، ص 20.

[3]– لأكثر تفصيل حول تحول جرائم الانترنت من جرائم فردية إلى جرائم منظمة، أنظر: لطرش فيروز وبن عزوز حاتم، "الجريمة الالكترونية في الجزائر: من جريمة فردية إلى جريمة منظمة"، مجلة آفاق للعلوم، مجلة دولية محكمة للعلوم الإنسانية والاجتماعية والاقتصادية، العدد الأول، جامعة الجلفة، 2016، ص ص331 – 332.

ثالثا: السرية في الممارسة وسهولة إخفاء عناصر الجريمة

تتميز جرائم الانترنت بميزتي السرية والإخفاء. بحيث تتحقق السرية من خلال عدم تمكن الضحية من ملاحظتها حتى لو كان متصلاً عبر شبكة الانترنت، فإنه من الصعب التنبؤ بها أو اكتشافها بالوسائل البسيطة أو الملاحظة البسيطة، بحيث يلجأ الجاني إلى استخدام تقنيات تكنولوجية عالية في ارتكاب هذه الجريمة لاسيما وأن التقدم التكنولوجي ساهم في اكتساب المعارف الجد متطورة في هذا المجال. بل ونلاحظ ترابط بين مرتكبي هذه الجرائم فيما يتعلق بتبادل الخبرات والقدرات وابتكار وسائل أكثر تعقيداً تعجز التشريعات الداخلية والدولية عن معالجتها، وفي المقابل فإن هذه التقنيات التكنولوجية العالية التطور ساهمت أيضاً في تمكين المجرمين من إخفاء عناصر الجريمة لاسيما ما يتعلق بمرتكبيها ومكان ارتكابها[1].

رابعا: الجريمة الناعمـــــة

أطلق على جرائم الانترنت وصف "الجرائم الناعمة" بالنظر إلى سهولة ارتكابها، فهي لا تتطلب جهداً أو ممارسة عنف جسدي معين، إذ ينتفي كل أثر لها من حيث التنفيذ يمكن ملاحظته لذا يطلق عليها أيضاً بـ "الجريمة النظيفة" نظراً لاعتمادها على مجرد أرقام وبيانات يتم تغييرها أو محوها أو نقلها من الوسائط الالكترونية، على خلاف الجرائم الأخرى التي تتطلب جهد عضلي كالسرقة والقتل مثلا. صفة "النعومة" التي ارتبطت بهذه الجريمة يعود السبب فيها إلى كونها من الجرائم الهادئة، إذ تتطلب في الجاني الخبرة والقدرة في مجال شبكة الانترنت والاحترافية في عالم تكنولوجيا المعلومات لارتكاب مختلف الجرائم كالتجسس أو اختراق الحسابات الالكترونية أو البنكية ذات البعد الرقمي[2].

---

[1]– صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013، ص ص 14 – 15؛ أنظر كذلك: جراحي عبد الستار، مرجع سابق، ص 10.

[2]– صغير يوسف، المرجع نفسه، ص 16.

خامسا: الصعوبة في الإثبات

تنفرد جرائم الانترنت عن بقية الجرائم الأخرى من حيث صعوبة إثباتها، إذ أن انعدام الأثر الخارجي لارتكاب هذه الجرائم ساهم في طمس الآثار المادية التي تُبْنى عليها المسؤولية الجنائية، بحيث أنها لا يمكن إعمال الأدلة المادية بشأنها كالبحث عن البصمات أو الاستعانة بالشهود. إن لجوء الجناة إلى محو آثار هذه الجرائم من خلال تدمير ومحو الأدلة في فترة وجيزة لا تعد بالدقائق وبمجرد الضغط على بعض الأزرار، ساهم بشكل كبير في صعوبة إثباتها، يضاف إلى ذلك نقص الخبرة الذي تعاني منه الشرطة ورجال الضبطية القضائية في هذا المجال وعدم قدرة التشريعات على احتواءها لأساليب ارتكابها وحصرها[1].

ساهمت الاحترافية التي يتمتع بها الجناة، في إحباط كل محاولات للحماية الرقمية باستخدام نظام الترميز والتشفير، وهو ما يشكل عائقاً كبيراً يحول دون التوصل إلى الأدلة اللازمة لملاحقة مرتكبي جرائم الانترنت لاسيما وأنهم يسعون في كل عملية إلى حماية البيانات المتعلقة بمكان وتاريخ الدخول إلى الجهاز المستخدم كوسيلة لارتكاب الجريمة أو محل ارتكابها عن طريق كلمات مرور يستعصي على ذوي الخبرة فكها، ومن ثمة يبقى الدليل العلمي المستخلص من خلال إعمال القرائن السبيل الوحيد لإثبات هذه الجريمة، والذي يخضع للسلطة التقديرية للقاضي[2].

[1]– البداينة ذياب موسى، الجرائم الالكترونية المفهوم والأسباب، ملتقى علمي بعنوان "الجرائم المستحدثة في ظل التغيرات والتحولات الاقليمية والدولية"، كلية الشرطة للعلوم الاستراتيجية، وزارة الداخلية، قطر، 2014، ص 20.

[2]– سحتوت نادية، "التنظيم القانوني للجريمة المعلوماتية أدلة إثبات الجريمة المعلوماتية"، مجلة دراسات وأبحاث، المجلد الأول، العدد الأول، جامعة زيان عاشور، الجلفة، 2009، ص48.

الفرع الثالث

الطبيعة القانونية لجرائم الانترنت

تندرج جرائم الانترنت ضمن الجرائم المنصوص عليها في قانون العقوبات، ومن ثمة تعتبر من الجرائم التي تحظى بتبيان عناصرها والأركان التي تقوم عليها والعقوبات المقررة لها، غير أن الاستخدام المتطور لوسائل ارتكابها جعل من التشريعات عاجزة أمام احتواء كل العناصر والسبل الفعالة لمكافحتها، ولعل عدم القدرة على تحديد طبيعتها القانونية يعتبر من بين أحد أهم مظاهر هذا العجز، بحيث من الصعب تحديد مرتكبيها أو مكان ارتكابها أو إيجاد الدليل المادي لارتكابها نظراً لسهولة محو آثارها كما سبقت الإشارة إلى ذلك، الأمر الذي يستتبع بالضرورة صعوبة ملاحقة مرتكبيها لاسيما إذا كان يتواجد في دولة أخرى تنعدم بينها وبين دولة الضحية أية اتفاقية دولية في إطار التعاون لمكافحتها، وعليه فإن الطبيعة القانونية لهذه الجرائم هي ذات طبيعة خاصة تختلف باختلاف الأنظمة القانونية المعتمدة في كل دولة[1].

لم يقتصر الاختلاف والتباين في تحديد الطبيعة القانونية لهذه الجريمة على الدول بحسب أنظمتها القانونية فحسب، بل يشهد الفقه القانوني اختلاف لذات الأسباب، إذ انقسم في ذلك إلى اتجاهين، اتجاه يعتبر جرائم الانترنت جرائم من نوع خاص مؤسسين رأيهم على كون المعلومة هي محل الحماية القانونية على أنها مجرد من أية قيمة مادية، وهو ما اعتبره الاتجاه الثاني مخالفا للفكر القانوني الجنائي الحديث، الأمر الذي دفع بهم إلى القول بأن هذه الجريمة هي جريمة مستحدثة تتمتع مثلها مثل الجرائم التقليدية بالحماية الجنائية[2].

---

[1]– بعرة سعيدة، مرجع سابق، ص ص 33 – 35.

[2]– لأكثر تفصيل حول الاختلاف الفقهي في تحديد الطبيعة القانونية لجرائم الانترنت، أنظر: ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه العلوم، تخصص: قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة1، 2016، ص ص 32 – 34.

نشير في هذا الصدد، أنه بالرغم من عدم إعطاء طبيعة قانونية موحدة لهذه الجريمة واختلاف التشريعات الجنائية حولها، فإنها تتفق في اعتبارها مرتبطة ارتباطاً وثيقا بالأمن المعلوماتي الذي يقوم على تأمين المكونات الخاصة بالحاسوب والعمل على حمايتها وتكريس خصائصها لاسيما ما يتعلق بالسرية[1].

الفرع الرابـــع

دوافع ارتكاب جرائم الانترنت

تختلف دوافع وأسباب ارتكاب جرائم الانترنت من شخص إلى آخر[2]، لذا نميز بين الدوافع الشخصية المرتبطة بمرتكب الجريمة (أولا)، والدوافع الخارجية التي تحيط به (ثانيا).

أولا: الدوافـــــع الشخصية

ترتبط هذه الدوافع ارتباطاً وثيقاً بتحقيق الربح المادي للجاني (أ)، كما قد ترتكب نتيجة للضغوطات النفسية والذهنية التي قد يعاني منها (ب).

---

[1]– إن إدراج جرائم الانترنت ضمن مجال الأمن المعلوماتي يعد نتيجة طبيعية وحتمية كرستها طبيعة هذه الجرائم القائمة على استخدام تكنولوجيا المعلومات كوسيلة أو استهدافها كمحل للجريمة، ومن ثمة فإن الأمن المعلوماتي يعمل على اتخاذ التدابير اللازمة لحماية المعلومات المخزنة في أجهزة الحاسوب من أي اعتداء عليها سواءً كان بالتخريب أو التدمير أو السرقة. لأكثر تفصيل حول الأمن المعلوماتي، أنظر: ربيعي حسين، مرجع سابق، ص ص 18 – 21.

[2]– وردت عدة تصنيفات لمرتكبي جرائم الانترنت، غير أن افضل تصنيف يمكن الاعتماد عليه هو التصنيف الذي جاء به كل من "David Icove" و"William Vonstroch" و"Seger"، بحيث يصنفون الجاني إلى مخترقون أي المتطفلون دافعهم الأساسي لارتكاب هذه الجرائم هو التحدي ومحاولة إثبات المقدرة، وفئة المحترفون الذين يتميزون بالخبرة والدراية الواسعة في مجال تكنولوجيا المعلومات ويعتمدون في ممارسة نشاطهم الإجرامي على التخطيط وغالبا ما يتم الاستعانة بهم من أجل اختراق الأنظمة التقنية للشركات الاقتصادية الكبرى أو الأجهزة الأمنية الخاصة بالدول، وأخيرا نجد فئة الحاقدون الذين تنعدم فيهم الخبرة والدراية ولا يسعون إلى تحقيق مكاسب مادية كما هو الشأن بالنسبة للفئتين الأولى والثانية، ويبقى الانتقام هو الدافع الأساسي لهذه الفئة لارتكاب هذه الجرائم. لأكثر تفصيل، أنظر: شعبان سمير، "الجريمة الالكترونية مقاربة تحليلية لتحديد مفهوم الجريمة والمجرم"، مجلة دراسات وأبحاث، المجلد الأول، العدد الأول، جامعة زيان عاشور، الجلفة، 2009، ص ص 123 – 125.

أ. الدافع المادي:

يلعب الدافع المادي دوراً أساسياً في سعي الجاني إلى ارتكاب جرائم الانترنت، نظراً لما تحققه من أرباح مادية معتبرة، فهي من الجرائم التي تتطلب تقنيات تكنولوجية كبيرة وخبرة في المجال لا تتوفر لدى العامة من الناس، لذا فإن اللجوء إلى ذوي الخبرة والكفاءة في هذا المجال يتطلب أموال طائلة لاسيما إذا كان الجاني يعاني من الفقر أو الحرمان الاجتماعي فإن ارتكاب هذه الجريمة تعتبر السبيل الفعال للتخلص من هذا الوضع المزري[1].

ب.الدافع النفسي:

يتمثل الدافع النفسي للجاني في عدة عوامل، يمكن إيجازها على النحو الآتي:

1) رغبة الجاني في تحقيق انتصار على الأنظمة المعلوماتية وحباً لإثبات الذات، دون تحقق النية الإجرامية، ونشير أن فئة المراهقين هم الأكثر شيوعاً نظراً لحساسية الفترة التي يخضعون لها وسعياً منهم لإظهار تفوقهم وبراعتهم الخاصة في هذا المجال لاسيما عند بروز تقنية جديدة[2].

2) اللهو أوالحقد أوبدافع الانتقام، ويعتبر هذا الأخير من أخطر الدوافع على الإطلاق، وقد سجلت عدة حالات انتقام في مجال العمل نتيجة للضغوط النفسية والمادية التي يتعرض لها بعض العمال بسبب سوء معاملة أصحاب العمل واستغلالهم[3]، ونذكر على سبيل المثال حالة انتقام موظف حكومي في شركة تأمين بـ (الو.م.أ) الذي قام بإدخال فيروس في أجهزة الشركة كرد فعل على

---

[1]– سوير سفيان، الجرائم المعلوماتية، مذكرة لنيل شهادة ماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2011، ص 26.

[2]– سوير سفيان، مرجع سابق، ص 27.

[3]– شعبان سمير، مرجع سابق، ص 128.

قرارها بالفصل الصادر في حقه، والذي ألحق بالشركة أضراراً فادحة تقدر بـ 150 ألف دولار بسبب ضياع 160 سجلا من السجلات الخاصة بالعملاء[1].

ثانيا: الدوافـــــع الخارجيـــة

تتخذ الدوافع الخارجية طابع ارهابي من جهة (أ)، وآخر سياسي اقتصادي من جهة أخرى (ب).

أ. الدوافع الإرهابية:

نشير في هذا الصدد أن المشرع الجزائري قد جعل من استخدام تكنولوجيات الإعلام والاتصال فعلاً مجرماً معاقب عليه قانوناً، متى كان الهدف من هذا الاستخدام تمويل الأعمال الإرهابية مادياً أو بشرياً[2].

ونقصد بالدوافع الإرهابية تلك التي تتعلق بالنشاط الإرهابي، ذات الاستخدام الواسع في الأنشطة الإجرامية العابرة للحدود، بحيث تؤمن شبكة الانترنت وسائل تقنية حديثة وسهولة التواصل بين القادة وأعضاء المنظمات الإرهابية[3]، كما تساهم في نقل أفكارها ومعتقداتها وتبادل المعلومات فيما بينها. وقد أثبتت الدراسات مساهمة شبكة الانترنت في تعليم كيفية صنع الأسلحة والمتفجرات والوسائل المختلفة التي يتم من خلالها ارتكاب الجرائم الإرهابية، ونذكر

---

[1]– صغير يوسف، مرجع سابق، ص 42.

[2]– جاء في م87 مكرر 11 الفقرة 4 ما يلي: "... – يستخدم تكنولوجيات الإعلام والاتصال لارتكاب الأفعال المذكورة في هذه المادة". أنظر الأمر رقم 66 – 156 المؤرخ المتضمن قانون العقوبات، مرجع سابق.

[3]– لم يقتصر إضفاء الطابع الإرهابي على الوسائل المستخدمة في تسهيل الأنشطة الإرهابية وإنما امتد ليشمل بعض هذه الأنشطة التي تتصل بشكل وثيق بشبكة الانترنت مما تولد عنه بروز ما يطلق عليه بالإرهاب المعلوماتي الذي يعرف على أنه: "القيام بعملية من شأنها المساس وإحداث خلل ماس باستقرار دولة او بهدف الضغط على حكومة، باستعمال طرق تدخل في صنف جرائم المعلوماتية". نقلا عن: دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير، تخصص القانون الجنائي، كلية الحقوق، جامعة منتوري، قسنطينة، 2013، ص 148.

على سبيل المثال قيام جماعات إرهابية في أوروبا بتدمير 60 مركزاً للحواسيب الآلية وذلك خلال فترة الثمانينات من أجل لفت الانتباه إليها[1].

ب.الدوافع ذات البعد السياسي والاقتصادي:

يلعب التنافس السياسي والاقتصادي دوراً بارزاً في انتشار جرائم الانترنت، بحيث يتم اللجوء إلى الوسائل غير القانونية من أجل البقاء في المركز السياسي أو للحفاظ على مركز اقتصادي معين، وقد سجلت (روسيا) قيام مجموعة من القراصنة باختراق الأنظمة الالكترونية الحكومية التابعة للجهاز العسكري لـ (الو.م.أ)[2]، كما قد يتم اللجوء إلى ارتكاب هذه الجريمة من أجل تشويه سمعة الأفراد والمؤسسات ذوي النفوذ في المجالين السياسي والاقتصادي وذلك لإلحاق الضرر بهم[3].

تضاف إلى مجموعة هذه الدوافع، دوافع أخرى ذات طابع استراتيجي كالتجسس أو في إطار التنافس في مجال الحرب الالكترونية وغيرها من الدوافع الأخرى التي تتعدد بتعدد المجالات والقطاعات[4].

المطلب الثاني

أركان قيام جرائم الانترنت

تقوم جرائم الانترنت كغيرها من الجرائم الأخرى، على مجموعة من الأركان، تتنوع بين الركن الشرعي (الفرع الأول)، والركن المادي (الفرع الثاني)، إضافة إلى الركن المعنوي (الفرع الثالث).

---

[1]– جواحي عبد الستار، مرجع سابق، ص ص 41 – 42.

[2]– رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الانترنت، مذكرة لنيل شهادة ماجستير في القانون العام، كلية الحقوق والعلوم السياسية، جامعة تلمسان، 2012، ص ص 67 – 68.

[3]– لطرش فيروز وبن عزوز حاتم، مرجع سابق، ص 328.

[4]– لأكثر تفصيل أنظر: لطرش فيروز وبن عزوز حاتم، المرجع نفسه، ص 328؛ أنظر أيضا: شعبان سمير، مرجع سابق، ص 129.

الفرع الأول

الركن الشرعـــــي

يقصد بالركن الشرعي، نص قانون يؤكد أن الفعل المرتكب هو فعل غير مشروع معاقب عليه وقت ارتكابه، وذلك إعمالا لنص المادة الأولى من قانون العقوبات التي تنص: "لا جريمة ولا عقوبة ولا تدابير أمن إلا بنص"[1] المعروف بـ "مبدأ الشرعية".

بالنظر إلى عدم كفاية النصوص القانونية التي تعمل على معالجة جرائم الانترنت، فإن القضاء يجد صعوبة للفصل في القضايا المعروضة عليه، لاسيما أن الوسائل المسخرة لمواجهتها هي وسائل أقل تطوراً من الوسائل المستخدمة لارتكابها.

تختلف الدول في التأطير الشرعي لهذه الجرائم، إذ نجد من الدول السباقة في مجال تجريم هذه الأنشطة المرتبكة عبر الانترنت كل من (الو.م.أ) و(فرنسا)، في حين أن هناك من الدول الأخرى التي لم تخصص قوانين لمكافحتها واكتفت بالتفسير الموسع لنصوصها الداخلية وهو ما يتعارض مع مبدأ الشرعية من جهة، ويساعد على إفلات الجاني من العقاب من جهة أخرى[2].

الفرع الثاني

الركن المـــــادي

سبقت الإشارة إلى أن جرائم الانترنت من أصعب الجرائم من حيث إثبات الدليل المادي لارتكابها، نظراً للتقنيات التكنولوجية المستخدمة فيها، وسهولة محو آثارها، غير أن ذلك لا

[1]– المادة الأولى من الأمر رقم 66 – 156 المتضمن قانون العقوبات المعدل والمتمم، مرجع سابق.

[2]– صغير يوسف، مرجع سابق، ص ص 59 – 64.

يتنافى مع تمتع هذه الجرائم بالركن المادي الذي يعتبر ركن جوهري لقيام أية جريمة مهما كان نوعها.

يتحقق الوجود المادي لجرائم الانترنت من خلال ضرورة وجود بيئة رقمية واتصال بشبكة الانترنت، ويضاف إليه الشروع في ارتكاب الجريمة وتحقق النتيجة المراد من ارتكابها. بحيث يقوم الجاني بتجهيز الحاسوب الذي يتم من خلال تنفيذ العملية الإجرامية وإعداد وتحضير البرامج الخاصة بالاختراق، وبرامج الفيروسات التي تساهم في محو وتعطيل الأجهزة الالكترونية المستهدفة. كما يمكن له اللجوء إلى تهيئة وإنشاء صفحات ومواقع تتولى نشر المواد الإباحية في الجرائم الإباحية والمخلة بالآداب العامة. ونلاحظ أن جرائم الانترنت على خلاف الجرائم الأخرى يعتبر التحضير لارتكابها فعلاً معاقباً عليها قانوناً كشراء برامج الاختراق، والمعدات الخاصة لفك الثغرات والتشفير وكلمات السر الخاصة بالدخول إلى الأنظمة الالكترونية والحسابات وغيرها من العتاد الخاص بارتكاب هذه الجرائم[1].

الفرع الثالث

الركن المعنـــــوي

يتمثل الركن المعنوي في الحالة النفسية لمرتكب جرائم الانترنت، فهي تلعب دوراً كبيراً في الربط بينها وبين السلوك المادي للجاني، والذي يساعد القاضي على معرفة مدى خطورته والعقوبة الملائمة له التي تستهدف بالدرجة الأولى إصلاحه والحد من خطورته. وانطلاقا من كون جرائم الانترنت من الجرائم العمدية فإن القصد الجنائي يتوفر عند توفر عنصري العلم والإرادة لدى الجاني، وإن اختلف شكل القصد بين القصد العام والقصد الخاص وذلك بحسب كل جريمة على حدى، إلا أنه من الضروري أن يكون الجاني على دراية بأن الفعل المرتكب

[1]– حجازي محمد، جرائم الحاسبات والانترنت – الجرائم المعلوماتية، المركز المصري للملكة الفكرية، مصر، 2005، ص 23.

هو فعل مجرم ومعاقب عليه قانونا، واتجاه إرادته إلى ترتيب السلوك غير المشروع حتى لو لم تتحقق النتيجة[1].

تختلف الطريقة التي يستدل بها إلى الركن المعنوي لجرائم الانترنت باختلاف الجرائم المرتكبة، حيث يعتمد على مدى اعتماد الجاني على الغش في كل من جريمة الدخول أو البقاء غير المصرح به وجريمة التعامل في معطيات غير مشروعة وهو ما أكدت عليه المادتين 394مكرر و394مكرر2[2]، ويتجسد هذا الركن في جريمة التلاعب بالمعطيات من خلال قيام الجاني بتعديل أو إزالة البيانات المخزنة في أجهزة الحاسوب أو التلاعب بالمعطيات في الحسابات الالكترونية محل الاختراق[3].

المطلب الثالـــــث

أساليب ارتكـــــاب جرائم الانترنـــت

تتعدد الأساليب التي يعتمد عليها الجاني في ارتكاب الجرائم الالكترونية بتعدد الوسائل الالكترونية المستخدمة في ذلك، ولعل من بين أهم هذه الوسائل الأكثر شيوعاً والتي أثارت جدلاً وقلقاً على الصعيد الوطني والدولي، استخدام الفيروسات لتدمير أو تعطيل الأجهزة الالكترونية والأنظمة المعلوماتية التابعة للدولة أو الخواص على حد سواء (الفرع الأول)، أو عن طريق القرصنة المعلوماتية (الفرع الثاني).

---

[1]– حمودي ناصر، "الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري"، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 02، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، بجاية، 2016، ص78.

[2]– أنظر م 394 مكرر و394مكرر2 من الأمر رقم 66 – 156 المتضمن قانون العقوبات المعدل والمتمم، مرجع سابق .

[3]– خليفة محمد، "خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها"، مجلة دراسات وأبحاث، العدد الأول، جامعة زيان عاشور، الجلفة، 2009، ص ص 378 و383 و386.

الفرع الأول

ارتكاب جرائم الانترنت عن طريق نشر الفيروسات

يعتمد أغلب مرتكبي جرائم الانترنت على إدخال الفيروسات في برامج معينة تستهدف بذلك تعطيل أجهزة الحاسوب أو أنظمة تكنولوجية معينة وذلك عن طريق الاتصال بشبكة الانترنت، ويعرف الفيروس المعلوماتي على أنه: *"تعليمة أو عدة تعليمات طفيلية خبيثة في شكل برامج صغيرة، موجهة من جهة للانتشار في الكمبيوتر وتعديل بطريقة سلبية نظام الاستغلال وكذا تحطيم أو التأثير سلبيا على المعلومات المعلوماتية في مختلف أنواعها (معطيات، بيانات، برامج)، أي كل ما له وجود منطقي في نظام معلوماتي سليم بمعنى إفساد السير العادي للنظام المعلوماتي بعد استقرارها في ذاكرة الكمبيوتر كالقرص المرن"*[1].

ويعود أول لجوء إلى استخدام الفيروسات في عالم الانترنت إلى منتصف الثمانينات في (باكستان) على يد أخوين يعملان في مجال الحواسيب الآلية، لتستمر بعد ذلك في التطور والانتشار إلى أن أصبح مجال الفيروسات متزايد بشكل ملحوظ بنسبة 200 فيروس في الشهر الواحد[2]، ويترتب عن تعدد الفيروسات وأشكالها إلى تعدد الأضرار الناتجة عنها، إذ أن البعض منها يكون مرتبطاً بشكل وثيق بالملفات العادية ولا يتم تفعيلها أو تنشيطها إلا عن تشغيل هذه الملفات، بينما يعمل البعض الآخر على إتلاف الملفات المتواجدة في القرص الصلب أو إتلافه بشكل كامل، كما انتشرت في الآونة الأخيرة فيروسات من نوع آخر يمتد تأثيرها من حاسوب

[1]– دردور نسيم، مرجع سابق، ص 42.

[2]– تتجسد هذه الفيروسات في برامج خبيثة تستهدف تدمير وتعطيل أجهزة الحاسوب سواءً كانت بسيطة أو متكاثرة ذاتيا. أنظر: حديد نوفيل وبوزيد هجيرة سومية، مرجع سابق، ص ص 202 – 204.

إلى آخر يتم انتقاله عبر شبكة الانترنت بشكل سريع، وتتولى هذه الفيروسات تعطيل المواقع المركزية أو الحد من فعالية الشبكة العنكبوتية أو إحداث شلل كلي فيها[1].

ظهر أيضا فيروس أكثر تطوراً أطلق عليه بتسمية "حصان طروادة Trogan Horse"، يعمل بشكل متخفي بحيث يقوم بإحداث ثغرة أمنية حتى يتمكن المخترقين من الدخول بسهولة إلى الجهاز المستهدف وإجراء الفعل المراد تحقيقه سواء تعلق الأمر بالعبث بالملفات الموجودة به أو محوها أو نقلها أو الحصول على المعلومات اللازمة منها، وتسبب هذه الفيروسات خسائر فادحة لاسيما بالنسبة للأجهزة الكبرى الخاصة بالمؤسسات سواء العامة أو الخاصة، وهو ما حدث في (الو.م.أ) بالنسبة لفيروس (WS32.SOBIG) الذي أدى إلى فقد العديد من الملفات التي نتج عنها خسارة أكثر من 50 مليون دولار[2].

الفرع الثاني

ارتكاب جرائم الانترنت عن طريق القرصنة المعلوماتية

تعتبر جريمة القرصنة من الجرائم الأكثر انتشاراً، بحيث يتم استهداف جهاز الكمبيوتر وذلك إما من طرف هواة يمارسون مثل هذا النشاط باعتباره فن وتحدي لا غير، كما يمكن ارتكابها من طرف محترفين من أجل الحصول على أرباح مادية[3].

يطلق على مرتكبي القرصنة المعلوماتية بمصطلح "الهاكرز" والذين يعرفون على أنهم: *"الشباب البالغ المفتون بالمعلوماتية والحاسب الآلي الذين لديهم قدرة فائقة على اختراق الشبكات*

[1]– محمد حجازي، مرجع سابق، ص ص 15 – 16.

[2]– محمد حجازي، المرجع نفسه، ص ص 15 – 16.

[3]– حامدي محمد الصالح، "علاقة تكنولوجيا المعلومات بظاهرة الاتجار بالبشر في عصر العولمة ومدى تأثيرها على دولة قطر"، المجلة العربية الدولية للمعلوماتية، المجلد الأول، العدد الثاني، معهد الملك سلمان للدراسات والخدمات الاستشارية، جامعة المجمعة، السعودية، 2012، ص 4.

والإبحار في عالم البيانات دون أهمية لحواجز كلمات المرور أو الشفرات"[1]. ويندرج هؤلاء ضمن فئة الارهابيين المعلوماتيين، والذين ينقسمون إلى عدة فئات تتولى كل فئة مهمة معينة من بينها القرصنة المعلوماتية التي تتعلق أساسا بوسائل الاتصال السلكية واللاسلكية[2].

ويتم ارتكابها بعدة طرق، نذكر من بينها القرصنة عن طريق استخدام "حصان طروادة"، بحيث تعتمد على آلية التجسس مستهدفاً بذلك جهاز الضحية، فيتم اختراقه بواسطة هذا البرنامج عبر البريد الالكتروني أو المحادثات أو غرف الدردشة، ويتسم هذا البرنامج بالفعالية نظراً لصعوبة الكشف عن مرتكب القرصنة وعدم القدرة على متابعته قضائيا[3].

[1]– بونعارة ياسمينة، مرجع سابق، ص 9.

[2]– دردور نسيم، مرجع سابق، ص 151.

[3]– حديد نوفيل وبوزيد هجيرة سومية، مرجع سابق، ص 205.

المبحث الثاني

أشكال جرائم الانترنـــت

تتميز جرائم الانترنت بازدواجية التكييف، إذ تكون وسيلة فعالة لارتكاب جرائم أخرى أو لتسهيل ارتكابها (المطلب الأول)، أو تكون جرائم قائمة بذاتها، وإن كانت تخضع مثلها مثل الجرائم الأخرى للقواعد والأحكام التي ينص عليها كل من قانون العقوبات لاسيما بموجب قانون رقم 04 – 15 الذي جاء النص فيه على مجموعة محددة من هذه الجرائم (المطلب الثاني).

المطلب الأول

جرائم الانترنت وسيلة لارتكاب بعض الجرائم الأخرى

تتعدد أشكال جرائم الانترنت بحسب الاستخدام، غير أن أغلبها تكون الوسيلة الفعالة لتحقيق المكاسب المالية الضخمة، لاسيما الجرائم الواقعة على الأموال (الفرع الأول)، أو التي تستهدف الأنظمة المعلوماتية (الفرع الثاني)، والجريمة الإباحية التي أصبحت جريمة العصر لما تشهده من انتشار وتأثير سلبي على المجتمعات (الفرع الثالث).

الفرع الأول

الجرائم الواقعة على الأمـــــوال

تتجسد جرائم الانترنت في الجانب المالي عندما يتعلق الأمر بجريمة التزوير (أولا)، والطابع الإجرامي للعبة القمار (ثانيا)، إضافة إلى جريمة غسيل الأموال التي تعرف ممارسة واسعة لارتكاب مثل هذه الجرائم فيها (ثالثا).

أولا: جريمة التزويـــر

تعتبر جرائم التزوير من الجرائم التي تشغل بال الدول في مختلف أنحاء العالم، نظراً لخطورتها ومساسها بالمصلحة العامة للدولة أو المصلحة الخاصة للأفراد.

يتم ارتكاب هذه الجريمة عن طريق استخدام أجهزة الحاسوب ولعل أبرز صورة يمكن إبرازها فيما يتعلق بهذه الجريمة، نجد التعامل الالكتروني في مجال البيع والشراء عن طريق الانترنت وكذا التوقيع الالكتروني على عقود البيع الالكترونية، وقد شكل هذا الأخير جدلاً واسعاً بحيث أصبح من السهل الحصول على منظومة التوقيع الالكتروني الخاصة بالشخص المستهدف واستخدامها من أجل توقيع المحررات الالكترونية، وتزداد خطورة هذه الجريمة بالنظر إلى صعوبة إثبات التوقيع المزور عن طريق مضاهاة الخطوط[1].

كما أضحت المؤسسات سواء العمومية أو الخاصة تعتمد بشكل أساسي على الحاسوب الآلي من أجل حفظ البيانات الخاصة بأنشطتها، ومع التطور الحاصل في مجال تحويل النقود الذي أصبح يتم عن طريق وسائل جد متطورة تضمن عنصري الثقة والسهولة في التعامل، بحيث أصبحت بطاقات الائتمان تحل محل النقود والشيكات في الوفاء، كل هذا ساهم في بروز جرائم مالية، لاسيما جريمة التزوير عن طريق الاستخدام غير المشروع لهذه البطاقات، وذلك وفق أشكال متعددة نذكر من بينها ما يلي[2]:

- استخدام بطاقات ائتمان مزيفة جزئيا أو كليا.
- استخدام بطاقات ائتمان مسروقة.
- استخدام بطاقات ائتمان غير مزيفة إلا أنها صدرت بطريقة غير مشروعة.

---

[1]– لأكثر تفصيل حول جريمة تزوير التوقيع الالكتروني، أنظر: حفصي عباس، مرجع سابق، ص ص 95 – 105.

[2]– حشاشي أمينة، "ماهية الجريمة المعلوماتية"، مجلة دراسات وأبحاث، المجلد الأول، العدد الأول، جامعة زيان عاشور، الجلفة، 2009، ص 455..

ثانيا: الطابع الإجرامي للعبة القمـــــــار

استوجب في الماضي اللجوء إلى لعبة القمار الوجود المادي للاعبين على طاولة اللعب، إلا أن التطور الحاصل في عالم التكنولوجيا لم يعد الوجود المادي شرطاً أساسياً لمباشرة هذه اللعبة وممارستها، وإنما أصبحت تتم في عالم الانترنت من خلال ما يطلق عليه بـ "الكازينوهات الافتراضية Virtual Casino"، وقد ساهم هذا التقدم التكنولوجي في هذا المجال إلى ارتفاع العائدات التي تترتب عنها لاسيما في (الو.م.أ) بحيث أثبتت الإحصاءات هذا الارتفاع من خلال تسجيل زيادة معتبرة في المبلغ الإجمالي للعائدات الناتجة عن هذه اللعبة في العالم الافتراضي من سنة 2001 التي سجلت ما يتجاوز 3 مليار دولار ليرتفع سنة 2010 إلى 24 مليار دولار[1].

وإن كانت هذه اللعبة لا تشكل في بعض الدول فعلاً إجرامياً إلا أن هناك دول أخرى لاسيما في الدول العربية يعتبر الانضمام إلى هذه اللعبة عن طريق الانترنت من الأفعال التي لا يجيزها القانون بصفة عامة ولاسيما القانون الجنائي بصفة خاصة.

ثالثا: جريمة غسيل الأمـــوال

تعتبر جريمة غسيل الأموال من إحدى أبرز صور الجرائم الاقتصادية التي تعاني منها الدول لاسيما في الآونة الأخيرة، نظرا للهدف الخفي الذي تعمل على تحقيقه هذه الجريمة لاسيما ما يتعلق بإخفاء المصدر الحقيقي للأموال المتحصل عليها بطرق غير قانونية، كالمتاجرة بالمخدرات، وتهريب الأسلحة، والإرهاب الدولي ...الخ.

تعمل هذه الجريمة على إضفاء الشرعية على الأموال المكتسبة من مصادر غير مشروعة، وذلك من خلال عدة طرق، نذكر من بينها على سبيل المثال ما يلي[2]:

---

[1]– بونعارة ياسمينة، مرجع سابق، ص ص 23 – 24.

[2]– صغير يوسف، مرجع سابق، ص ص 46 – 47.

1) استثمار الأموال المتحصل عليها في تجارة قانونية أو صبها في نظام مصرفي معين.

2) اللجوء إلى تعاملات معقدة ومتعددة من أجل التمويه على مصدر الأموال غير المشروعة.

3) إجراء عملية دمج للأموال غير المشروعة ضمن الأموال المشروعة وتبرير سند ملكيتها.

ونشير في هذا الصدد أن الخبراء في صندوق النقد الدولي أشاروا إلى أن حجم الأموال التي يتم غسلها سنويا تتراوح ما بين 620 مليار دولار و 1600 مليار دولار، وهي أرقام تبين حجم الخسائر الذي يتعرض له الاقتصاد القومي للدول كافة[1].

الفرع الثاني

الجرائم الواقعة على نظم المعلومات

تتجسد جرائم الانترنت بالدرجة الأولى من خلال المساس بنظم المعلومات سواء تعلقت بالأجهزة الالكترونية (أولا)، أو تعلقت بالحسابات الشخصية للأشخاص (ثانيا).

أولا: جرائم الإضرار ببيانات الأجهزة الالكترونية

يتم استهداف البيانات المسجلة في الحاسوب الآلي بشكل أساسي نظرا لاعتماد أغلب المؤسسات على النظام المعلوماتي لتسييرها وممارسة أنشطتها، ويعتبر هذا النوع من الجرائم الأشد خطورة نظرا لحجم الخسائر التي تتكبدها المؤسسات نتيجة مثل هذه الممارسات الإجرامية.

[1]– صغير يوسف، مرجع سابق، ص 47.

يتحقق الركن المادي لهذه الجريمة من خلال إجراء تعديل أو محو أو سرقة أو إتلاف أو تعطيل العمل للمعلومات والبيانات الموجودة على الحاسوب سواءً كان متصلاً بالشبكة العنكبوتية أو غير ذلك، كما ترتكب هذه الجريمة عن طريق الدخول بطريقة غير مشروعة إلى الحسابات سواء الخاصة بالأفراد أو المؤسسات.

يعود السبب في ممارسة مثل هذه الأنشطة الإجرامية إلى عدة عوامل لاسيما النفسية كالكره والانتقام، أو مادية كمحاولة البحث عن ربح مادي غير مشروع، أو سياسي أو ديني وفي إطار المنافسة التي تشهدها خصوصاً المؤسسات الاقتصادية والتجارية، ومن هنا يتضح أن العامل النفسي يلعب دوراً بارزاً في تحديد صنف مرتكبي جرائم الانترنت[1].

ثانيا: الجرائم الواقعة على حسابات وبيانات الأشخاص

نشير في البداية إلى أن مثل هذه الجرائم لا تتم إلا بتوفر الشبكة العنكبوتية، إذ أن الركن المادي لهذه الجريمة يكون شبه منعدم باعتبار أن الأثر الذي يصيب الأشخاص هو أثر معنوي وليس مادي، بحيث تتمثل في كل من السب والقذف والتشهير بالشخص سواءً كان شخص طبيعي أو شخص معنوي.

من بين أبرز صور هذه الجرائم نجد على سبيل المثال[2]:

- نشر أخبار ومعلومات من شأنها الإضرار الأدبي أو المعنوي.
- الدخول إلى الحسابات الشخصية للأفراد وتغيير محتوياتها أو نشر معلومات خاطئة بهدف تشويه سمعته والتشهير به من خلال الدخول إلى مواقع الاستضافة المجانية لصفحات الانترنت.

---

[1]– تعددت تصنيفات مرتكبي جرائم الانترنت بتعدد الزاوية التي ينظر إليهم منها، بحيث نجد كل من اللصوص والمنتقمون والجواسيس والنشطاء إذا ما أخذنا بعين الاعتبار الدوافع التي دفعت بهم إلى ارتكابها، كما نجد الخبراء والمبتدئين والذين يندرج ضمن هؤلاء أصحاب القبعات البيضاء والسوداء وأخرون. لأكثر تفصيل حول تصنيف مجرمو الانترنت، أنظر: لطرش فيروز وبن عزوز حاتم، مرجع سابق، ص ص 326 – 327.

[2]– شعبان سمير، مرجع سابق، ص ص 120 – 121.

- الاعتداء على الملكية الفكرية للأسماء الخاصة بالمواقع الالكترونية، واللجوء إلى إعادة توجيهها، أي توجيه المستخدمين إلى موقع آخر غير الموقع المعتاد الدخول إليه.

الفرع الثالث

الجريمة الإباحية الالكترونية

تعتبر الجرائم الإباحية[1] من الجرائم التي لاقت رواجاَ كبيراَ عبر الانترنت، لاسيما عند فئة المراهقين والقصر، بحيث يتم استغلال فضولهم وسعيهم لإشباع رغباتهم الجنسية من خلال مواقع إباحية (أولا)، تقوم بعرض أفلام وصور ومحادثات تتنافى مع الأخلاق والآداب العامة (ثانيا).

أولا: طرق ارتكاب الجريمة الإباحيــة

يتم ارتكاب الجريمة الإباحية من خلال العديد من الصور لاسيما عن طريق إنشاء مواقع إباحية (أولا)، أو عن طريق اختراق المواقع المحجوبة (ثانيا).

أ) إنشاء المواقع الإباحيـــة:

تعتبر المواقع الإباحية من بين الأسباب المباشرة لتفشي بعض الآفات الإجرامية لاسيما جريمة الاغتصاب الواقعة على فئة القصر والأطفال بصفة خاصة، وقد أثبتت الاحصائيات أن نسبة 15% من مستخدمي الانترنت يقومون بتصفح هذه المواقع.

[1]– نشير في هذا الصدد أن جرائم الانترنت التي تمس بالأخلاق والآداب العامة هي من بين جرائم المحتوى أي أنها تنصب على المحتوى غير المشروع. أنظر: بوشكيوه عبد الحليم، "آليات مكافحة الجرائم الماسة بالأخلاق والآداب العامة على الانترنت"، مجلة دراسات وأبحاث، العدد الأول، جامعة زيان عاشور، الجلفة، 2009، ص 3.

وقد حرمت الشريعة الإسلامية مشاهدة مثل هذه المواقع عملاً بقول الله عز وجل في كتابه العزيز الحكيم بعد بسم الله الرحمن الرحيم: "*قُل لِّلْمُؤْمِنِينَ يَغُضُّوا مِنْ أَبْصَارِهِمْ وَيَحْفَظُوا فُرُوجَهُمْ ذَٰلِكَ أَزْكَىٰ لَهُم إِنَّ اللَّهَ خَبِيرٌ بِمَا يَصْنَعُونَ(30)*"[1].

ترتبط المشاهدة وارتياد المواقع الإباحية ارتباطاً وثيقاً بالممارسات الجنسية غير الأخلاقية، حيث أن النظر إلى الصور الجنسية العارية ستؤدي لا محالة إلى ارتكاب الزنا التي تعد من الكبائر، لذا كان من الضروري تجنب هذه المواقع تحقيقا لمصلحة المجتمع بصفة عامة ومصلحة الأفراد بصفة خاصة[2].

ب) اختراق المواقع الإباحية المحجوبة:

تعتمد بعض المواقع الإباحية سياسية الحجب واشتراط سن الرشد وإثبات الهوية من أجل السماح بالدخول إليها، فيطلق عليها بالمواقع الإباحية المحجوبة. وعلى الرغم من هذه السياسة المعتمدة التي تستهدف بالدرجة الأولى حماية فئة القصر والأطفال إلا أن هناك فئة كبيرة منها تسعى بكل الطرق للوصول إلى هذه المواقع، وذلك عن طريق اختراقها سواءً بإدخال هوية مزورة أو اللجوء إلى استخدام بعض البرامج الالكترونية كبرنامج (البروكس) الذي يقوم بحصر ارتباط جميع مستخدمي الانترنت في جهة واحدة ضمن جهاز موحد، ليساهم بذلك في تسهيل عملية الاختراق[3].

ثانيا: صور الاعتداء الأدبي والأخلاقي للجريمة الإباحية

تعتمد الجريمة الإباحية في ارتكابها على انتهاك حرمة الشخص، من خلال اللجوء إلى العديد من الصور، نذكر من بينها ما يلي[4]:

---

[1]– القرآن الكريم، سورة النور، الآية 30.

[2]– الشمري غانم مرضي، مرجع سابق، ص ص 70 – 71.

[3]– الشمري غانم مرضي، المرجع نفسه، ص 72.

[4]– عثمان طارق، "حماية الأطفال من الاستغلال في المواد الإباحية عبر الانترنت في التشريع الجزائري"، مجلة المفكر، العدد 13، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2016، ص ص 420 – 421.

1) عرض الصور الفاضحة.
2) عرض أفلام إباحية، والتي أصبحت تتم عن طريق شركات عالمية نظرا لما تدره من أرباح مالية ضخمة.
3) الابتزاز الجنسي.
4) استغلال حالات الاغتصاب والتعذيب الجنسي لتمويل المواقع الإباحية بالمادة السمعية والبصرية.
5) إنشاء غرف الحوار من أجل تبادل المحادثات الجنسية كما هو الشأن في (الو.م.أ) التي تم فيها تخصيص خط اتصال داعر لإثارة الشهوات والغرائز الجنسية.

المطلب الثاني

الجرائم المحددة بموجب قانون رقم 04 – 15

اتجهت الجزائر على غرار الدول الأخرى، نحو مكافحة جرائم الانترنت من خلال بذل العديد من الجهود لاسيما التشريعية منها. ويتجسد ذلك من خلال اعتماد العديد من النصوص القانونية المتعلقة بهذا المجال، ولعل قانون رقم 09 – 04 الذي كرست من خلاله القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، يشكل تطوراً ملحوظاً في المنظومة القانونية الجنائية، إلا أنه يعتبر الوسيلة الوقائية من هذه الجرائم، بينما تم تحديد هذه الجرائم بموجب القانون رقم 04 – 15 المعدل لقانون العقوبات الجزائري.

وتتمثل هذه الجرائم في كل من جريمة الدخول أو البقاء غير المصرح به داخل منظومة للمعالجة الآلية للمعطيات (الفرع الأول)، وجريمة التلاعب غير المصرح به بالمعطيات (الفرع الثاني)، إضافة إلى جريمة التعامل في معلومات غير مشروعة (الفرع الثالث).

الفرع الأول

جريمة الدخول أو البقاء غير المصرح به داخل منظومة للمعالجة الآلية للمعطيات

تستمد هذه الجريمة أساسها القانوني من القانون رقم 04 – 15 المعدل لقانون العقوبات (أولا)، ولا يتم المعاقبة عليها إلا بتوفر مجموعة من الأركان (ثانيا).

أولا: الأساس القانوني

تجد جريمة الدخول أو البقاء غير المصرح به داخل منظومة للمعالجة الآلية للمعطيات أساسها القانوني في نص م394 مكرر التي جاء فيها:

"يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 150.000دج"[1].

ثانيا: أركان قيام جريمة الدخول أو البقاء غير المصرح به داخل نظام المعالجة الآلية للمعطيات

تقوم جريمة الدخول أو البقاء غير المصرح به داخل منظمة للمعالجة الآلية للمعطيات على الوجود المادي للفعل المجرم المشكل للركن المادي (أ)، وتوفر القصد الجنائي لدى مرتكبها (ب).

[1]– أنظر م394 مكرر من الأمر 66 – 156 المتضمن قانون العقوبات المعدل والمتمم، مرجع سابق.

أ) الركن المادي:

يتحقق الركن المادي لجريمة الدخول أو البقاء غير المصرح به داخل منظومة للمعالجة الآلية للمعطيات، بتحقق السلوك المادي المتمثل في الدخول إلى نظام معلوماتي على أن يتم دون رضا المجني عليه، سواءً تم تغييب هذا الرضا تماماً أو أكره على ذلك، ويستوي أن يكون الدخول كلياً أو جزئياً، محققاَ أو مجرد محاولة وأيا كانت الطريقة أو الوسيلة المستعملة للدخول، بل أكثر من ذلك نجد أنه في حالة وجود التصريح بالدخول لابد على المصرح له عدم تجاوز حدود التصريح[1].

كما يتحقق السلوك المادي أيضا عند البقاء غير المصرح به في المنظومة الخاصة بالمعالجة الآلية للمعطيات، فيفترض الدخول إليها عن طريق الصدفة أو الخطأ مما ينتفي في سلوك الدخول القصد الجنائي، غير أن وصف الجريمة يتخذ بعد الدخول على إثر بقاء الجاني متصلاً في المنظومة على الرغم من عدم جواز ذلك، مما يضفي على هذه الجريمة الصفة الاستمرارية على خلاف جريمة الدخول التي تكون مؤقتة، وبالرغم من اختلافهما إلا أنهما تجتمعان عندما يتعلق الأمر بجريمة البقاء غير المصرح به، فهذه الأخيرة لا تتحقق إلا بواقعة الدخول غير أنه في هذه الحالة تكون مشروعة ولا تتخذ وصف الجريمة[2].

غير أن هذا السلوك يكون أكثر تشديداً ومرتباً لعقوبات أكثر صرامة، عندما يترتب عن الدخول أو البقاء محو أو تعديل المعطيات التي تحتويها المنظومة أو تعطيل وظيفتها، وعلى هذا النحو يعتبر المحو أو التعديل بحد ذاته اعتداء معاقب عليه حتى لو لم تتحقق النتيجة، يكفي لقيام المسؤولية الجنائية إثبات العلاقة السببية بين الدخول أو البقاء غير المصرح به وعملية المحو أو التعديل للمعطيات[3].

---

[1]– حمودي ناصر، مرجع سابق، ص 74.

[2]– حمودي ناصر، المرجع نفسه، ص 75.

[3]– فشار عطاء الله، "مواجهة الجريمة المعلوماتية في التشريع الجزائري"، مجلة دراسات وأبحاث، المجلد الأول، العدد الأول، جامعة زيان عاشور، الجلفة، 2009، ص ص 489 – 490.

ب) الركن المعنوي:

سبق القول عند الحديث عن أركان جرائم الانترنت بصفة عامة، أنه يتطلب لكل جريمة شكل معين لتحقيق الركن المعنوي فيها، يتجسد هذا الأخير في جريمة الدخول أو البقاء غير المصرح به، عند توفر كل من علم الجاني بأن سلوكه يرتكز على منظومة خاصة بمعالجة المعطيات وأن الدخول أو البقاء غير مسموح به على أن يتم ذلك كله عن طريق الغش مما يجعل لجوء الجاني إلى هذا الأخير لا يدع مجالاً للشك أن سلوكه عمدي، مما يجعل علمه بالجريمة مقترناً باتجاه ارادته إلى إحداث هذا السلوك المادي وهذا عندما يتعلق الأمر بالصورة المبسطة لهذه الجريمة، في حين يشترط أن تتجه إرادة الجاني إلى إحداث النتيجة المتمثلة في محو وتعديل المعطيات ومن ثمه اعتباره ظرفاً مشدداً[1].

يلعب الركن المعنوي لهذه الجريمة دوراً كبيراً في ترتيب المسؤولية الجزائية للجاني، بل يصل البعض إلى عدم الاكتراث بالسلوك المادي المتمثل في الدخول أو البقاء غير المصرح به ما لم تتجه نية الشخص إلى ارتكاب جريمة لاحقة على سلوك الدخول أو البقاء[2].

الفرع الثاني

جريمة التلاعب غير المصرح به بالمعطيات

يعتبر التلاعب غير المصرح به بالمعطيات من جرائم الانترنت المعاقب عليها بموجب قانون العقوبات المعدل بموجب قانون رقم 09 – 04 في م394 مكرر1 (أولا)، وهي تقوم على أركان توجب من خلالها قيام المسؤولية الجزائية لمرتكبها (ثانيا).

[1]– حمودي ناصر، مرجع سابق، ص 78.

[2]– عباوي نجاة، "الإشكالات القانونية في تجريم الاعتداء على أنظمة المعلومات"، دفاتر السياسة والقانون، العدد 16، جامعة قاصدي مرباح، ورقلة، جانفي 2017، ص 282.

أولا: الأساس القانوني لجريمة التلاعب غير المصرح به بالمعطيات

تستمد جريمة التلاعب غير المصرح به بالمعطيات أساسها القانون من نص م394 مكرر 1، والتي تنص على أنه:

"يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"[1].

ثانيا: أركان جريمة التلاعب غير المصرح به بالمعطيات

تقوم جريمة التلاعب غير المصرح به بالمعطيات على سلوك صادر عن الجاني يشكل الركن المادي لها(أ)، وتحقق القصد الجنائي لدى الجاني من توقيع العقوبة عليه(ب).

أ) الركن المادي:

يتحقق الركن المعنوي لهذه الجريمة من خلال قيام الجاني بفعل الإدخال أيا كانت صورته إيجابية من خلال إدخال معلومات صحيحة غير أنها غير مصرح بإدخالها أو غير صحيحة، أو إدخال برامج خبيثة كالفيروسات، كما يتحقق من خلال اعتماد تقنية تعديل المعطيات عن طريق الغش سواءً تعلقت هذه المعطيات بمعلومات شخصية للضحية أو معطيات متعلمة بالنظام المعلوماتي ومن ثمة التعديل في التصميم الذي يقوم عليه، ويضاف إلى ذلك عملية الإزالة[2] التي تؤدي إلى الإضرار بهذا النظام[3].

---

[1]– أنظر م394 مكرر 1 من الأمر 66 – 156 المتضمن قانون العقوبات المعدل والمتمم، مرجع سابق.

[2]– لأكثر تفصيل حول أشكال التلاعب بالمعطيات المتمثلة في كل من الإدخال والمحو والتعديل، أنظر: فشار عطاء الله، مرجع سابق، ص 492 – 493.

[3]– حمودي ناصر، مرجع سابق، ص ص 79 – 80.

تجدر الإشارة في هذا الصدد أن هذه السلوك الإجرامي يقع بمجرد إتيان هذه الأفعال حتى لو كانت الأنظمة المستهدفة في حالة عطل أو ارتكب الفعل خارج ساعات العمل القانونية، بينما تنتفي الصفة الإجرامية عنها إذا ارتكبت بصدد برامج لم يتم تفعيل خدمتها بعد، أو لم تعد في الخدمة بأن تم الاستغناء عن هذه البرامج استغناء تام[1].

تعتبر الأنظمة الخاصة بالتحويل الآلي للأموال من بين أهم الأنظمة المستهدفة بهذه الجريمة، حيث يتم التلاعب بمعطياتها في سبيل استخدامها من أجل الاحتيال والنصب أو من أجل تحويلات مالية غير مشروعة أو لاستصدار بطاقات إئتمانية مزدوجة أو بتزوير بطاقات ائتمان انطلاقا من المعطيات الواردة في هذه الأنظمة وغيرها من صور التلاعب التي يمكن أن تطال هذا المجال[2].

ب) الركن المعنوي:

يشترط لقيام الركن المعنوي لجريمة التلاعب غير المصرح به للمعطيات، توفر القصد الجنائي العام لدى الجاني ، الذي يتحقق بإثبات علم الجاني بكون الأفعال السابقة معاقب عليها قانوناً وبالأضرار التي قد تلحق النظام المعلوماتي المستهدف سواءً بالتعديل أو الإزالة، في حين لم يشترط المشرع الجزائري القصد الخاص في هذه الجريمة وهو ما يمكن استنباطه من خلال عبارة "الغش" التي اعتمدها في صياغة نص م394 مكرر1[3].

[1]– فشار عطاء الله، مرجع سابق، ص 485.

[2]– عباوي نجاة، مرجع سابق، ص 286.

[3]– حمودي ناصر، مرجع سابق، ص 81.

الفرع الثالث

جريمة التعامل في معلومات غير مشروعة

يعتبر تجريم التعامل في معلومات غير مشروعة استكمال لسلسة التعامل غير المشروع بأنظمة المعالجة الآلية للمعطيات، وقد أحسن المشرع الجزائري بإدراج هذه الجريمة في قانون العقوبات (أولا)، بحيث يكون قد أحاط بمختلف التصرفات غير المشروعة التي قد تتعرض لها هذه الأنظمة، والتي تتحقق بإتيان الجاني بركنيها المادي والمعنوي(ثانيا).

أولا: الأساس القانوني لجريمة التعامل في معلومات غير مشروعة

يتجسد الركن الشرعي لجريمة التعامل في معلومات غير مشروعة من خلال نص م394 مكرر2 التي تنص على أنه:

"يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمدا وعن طريق الغش بما يأتي:

1. تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2. حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم"[1].

ثانيا: أركان جريمة التعامل في معلومات غير مشروعة

تقوم جريمة التعامل في معلومات غـــير مشروعة على ركن مادي (أ)، وآخـــــر معنوي (ب).

[1]- أنظر م394 مكرر2 من الأمر 66 – 156 المتضمن قانون العقوبات المعدل والمتمم، مرجع سابق.

أ) الركن المادي:

جاء في نص م394 مكرر2 بصريح العبارة على الأفعال التي تشكل الركن المادي لجريمة التعامل في معلومات غير مشروعة، والتي تم تصنيفها بإرادة المشرع إلى قسمين، قسم يتكون من أفعال من شأنها المساهمة في ارتكاب جرائم منصوص عليها في قانون العقوبات، وتستهدف المعطيات سواءً كانت مخزنة أو معالجة أو مرسل. ونذكر هذه الأفعال على النحو الآتي[1]:

1. التصميم.
2. البحث.
3. التجميع.
4. التوفير.
5. النشر.
6. الاتجار.

يضاف إلى هذه الأفعال، أفعال أخرى صنفها المشرع الجزائري باعتبارها ناتجة عن جرائم وهي كل من[2]:

1. الحيازة.
2. الإفشاء.
3. النشر.
4. الاستعمال.

[1]– لأكثر تفصيل حول هذه الأفعال، أنظر: حمودي ناصر، مرجع سابق، ص ص 82 – 83.

[2]– لمعرفة مضمون هذه الأفعال والمقصود بها، أنظر: حمودي ناصر، المرجع نفسه، ص 83.

تجدر الإشارة في هذا الصدد، أن هذه الأفعال يعاقب عليها متى تم اللجوء إليها من أجل ارتكاب أو كانت نتيجة لارتكاب إحدى الجرائم المنصوص عليها في القسم الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات وهو ما أكده المشرع في كلا الفقرتين من خلال عبارة "الجرائم المنصوص عليها في هذا القسم". كما يجب أن يتم اللجوء إلى هذه الأفعال بشكل عمدي وعن طريق الغش[1].

ب) الركن المعنوي:

يتعين لإثارة المسؤولية الجنائية للجاني، توفر القصد الجنائي العام لديه، بحيث يكون على دراية بالوصف الإجرامي لهذه الأفعال وعدم مشروعية المعلومات التي يتعامل بها، كما يجب أن تتجه إرادته إلى إحداث سلوك ينتج عنه ارتكاب هذه الأفعال بغض النظر عن النتيجة المراد تحقيقها. أما بالنسبة للقصد الجنائي الخاص فعلى الرغم من كون الأفعال التي تساهم في ارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات تتطلب قيام الجاني بعملية الاعداد والتمهيد لارتكابها على خلاف الأفعال الأخرى التي تكون ناتجة عن ارتكاب الجريمة التي يكفي فيها القصد الجنائي العام لقيامها، إلا أن المشرع لم يشترط القصد الجنائي الخاص لقيامها[2].

[1]– فشار عطاء الله، مرجع سابق، ص 495.

[2]– حمودي ناصر، مرجع سابق، ص ص 84 – 85.

الفصل الثاني

جرائم الانترنت بين المنع والقمع

تتعدد المخاطر الناتجة عن استخدام الانترنت، منها ما يتعلق بانتحال الشخصيات أو اختراق المواقع والعبث بمحتواها والاستخدام غير المرخص به وغيرها من المخاطر الأخرى، الأمر الذي يجعل من مهمة تقرير الوقاية والحماية الجزائية من جرائم الانترنت مهمة صعبة، تعترضها صعوبات بسبب حداثة الموضوع وتميزه بطبيعة علمية بحتة تخرج من مجال تكوين رجال القانون، مما يستوجب إخضاعها لنظام حماية سابق على ارتكابها في إطار الوقاية منها (المبحث الأول).

يضاف إلى الحماية السابقة التي تضمن الحد من ارتكاب جرائم الانترنت، جانب آخر من الحماية يطغى عليه الطابع العقابي في إطار قمعها وعدم تمكين مرتكبيها من الإفلات من العقاب، وبالنظر إلى مكان ارتكابها الذي يتجسد أساساً في الوسائط الالكترونية المتصلة بشبكة الانترنت ومعظم الاعتداءات والجرائم المرتكبة تكون في العالم الافتراضي، فإنها تتمتع بمتابعة جزائية خاصة بها على خلاف الجرائم الأخرى (المبحث الثاني).

المبحث الأول

الوقايـــــة من جرائم الانترنت

يعتبر التطور التكنولوجي الذي يشهده العالم، الذي ساهم في إزالة القيود الجغرافية والتفتح في مختلف المجالات والقطاعات، العامل الأساسي في زيادة وتيرة استخدام التكنولوجيا لاسيما في مجال التواصل، من خلال إنشاء العديد من الحسابات الشخصية سواءً للأفراد أو المؤسسات عن طريق بيانات تكون عرضة لخطر الاعتداء، وعليه كان من الضروري وضع آليات لحمايتها بشكل مسبق، الأمر الذي يستوجب التعرف على مفهوم الحماية الخصوصية المعلوماتية لهذه البيانات (المطلب الأول)، إضافة إلى تبيان الجهود الوطنية والدولية المكرسة لتحقيق مثل هذا النوع من الحماية (المطلب الثاني).

المطلب الأول

حماية الخصوصية المعلوماتية

يرتبط مفهوم الخصوصية بمفهوم حماية البيانات الشخصية، بالنظر إلى كون هذه الأخيرة تنبثق من الأولى، لذا كان لزاماً البحث عن مفهومها (الفرع الأول)، وتحديد وسائل الحماية المكرسة لها (الفرع الثاني).

الفرع الأول

مفهوم الخصوصية المعلوماتيـــــة

تنفرد الخصوصية بتعريف لغوي وقانوني خاص بها (أولا)، كما أن هذا التعريف يجد رابطاً للوصل بينها وبين مجال المعلوماتية التي تتميز بالحداثة وسرعة الانتشار من حيث الممارسة (ثانيا).

أولا: تعريف مصطلح الخصوصية

تعرف الخصوصية من الناحية اللغوية بأنها: "*حق الأفراد في الحماية من التدخل في شؤونهم، وشؤون عائلاتهم بوسائل مادية مباشرة أو عن طريق نشر المعلومات عنهم*"[1]، وقد كانت الشريعة الإسلامية السباقة في الاعتراف بالحق في الحياة الخاصة، ومن أبرز المظاهر التي تدل على ذلك تكريس حق الفرد في حرمة مسكنه ومنع أي تطفل ضده، وقد أكد على ذلك كمبدأ أخلاقي والتزام ديني في قول الله عز وجل: " *يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّىٰ تَسْتَأْنِسُوا وَتُسَلِّمُوا عَلَىٰ أَهْلِهَا ذَٰلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُونَ (27) فَإِن لَّمْ تَجِدُوا فِيهَا أَحَدًا فَلَا تَدْخُلُوهَا حَتَّىٰ يُؤْذَنَ لَكُمْ وَإِن قِيلَ لَكُمُ ارْجِعُوا فَارْجِعُوا هُوَ أَزْكَىٰ لَكُمْ وَاللَّهُ بِمَا تَعْمَلُونَ عَلِيمٌ (28) لَّيْسَ عَلَيْكُمْ جُنَاحٌ أَن تَدْخُلُوا بُيُوتًا غَيْرَ مَسْكُونَةٍ فِيهَا مَتَاعٌ لَّكُمْ وَاللَّهُ يَعْلَمُ مَا تُبْدُونَ وَمَا تَكْتُمُونَ(29)* "[2]، هذه الآيات تؤكد على النهي عن أهم مظاهر الاعتداء على الخصوصية المتمثلة في الاستراق البصري واقتحام المسكن.

أما من الناحية القانونية نجد "*الماجناكارتا*" أول مدونة دستورية خاصة بحقوق الإنسان، أخذت بفكرة الخصوصية، وهي وثيقة بريطانية صدرت سنة 1215 ويطلق عليها بمصطلح

[1]– مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت بين القانون الدولي الاتفاقي والقانون الوطني، الطبعة الأولى، مركز الدراسات العربية للنشر والتوزيع، مصر، 2016، ص 39.

[2]– القرآن الكريم، سورة النور، الآيات 27 – 29.

"العهد الأعظم"، حيث يتم بموجبها التنازل عن سلطات الملك المطلقة تجاه الأفراد من خلال منح عهد يتضمن عدم الاعتداء على الأفراد أو حبسهم أو نفيهم أو مصادرة أموالهم إلا في إطار القانون[1].

ثانيا: ارتباط مفهوم الخصوصية بالمعلوماتية

ترتبط التقنية والحق الشرعي في الخصوصية، من خلال الدمج بين عمليتي تجميع البيانات الشخصية في الانترنت ومشاركتها، وقد تكون هذه الأخيرة مطلقة للعام والخاص أو مقيدة ومحددة بين أشخاص معينين وقد تكون مقتصرة على الشخص ذاته، فعدم مشاركة بعض البيانات الشخصية كالانتساب الديني والسياسي والأنشطة المتعلقة بحياته الشخصية والمهنية مع الغير لا يمس بحقه في الحماية، بل تأكيد لها بحيث تخضع المشاركة لعدة معايير تتعلق خصوصاً بتجنب المعاملة العنصرية أو العرقية والمحافظة على الطابع السري للبيانات بالنسبة للحسابات ذات الاعتبار الخاص، لاسيما وأن الخصوصية المعلوماتية تتعلق ببيانات متصلة بهوية الشخص وحسابه المالي وسجله الحكومي[2].

يتضح من خلال ما سبق أن مفهوم الخصوصية المرتبط بتكنولوجيا المعلومات، يرتكز على وصفه حق بالنسبة لصاحب البيانات في الادلاء بها وفقاً لإرادته الحرة ومشاركتها بشكل مطلق أو مقيد أو عدم مشاركتها وفق ما يتماشى مع مصالحه الشخصية والمهنية، وفي نفس الوقت يتصف بكونه واجب يتضمن فكرة عدم الاعتداء من طرف الغير وذلك تحت طائلة المتابعة الجزائية، فهي على هذا النحو تجسد ضمانة قانونية وأخلاقية في آن واحد.

[1]– مروة زين العابدين صالح، مرجع سابق، ص 31.

[2]– مروة زين العابدين صالح، المرجع نفسه، ص ص 59 – 60.

الفرع الثاني

وسائل حماية الخصوصية المعلوماتية

تنقسم الوسائل الخاصة بحماية الخصوصية المعلوماتية إلى وسائل تقنية (أولا)، وأخرى تنظيمية (ثانيا).

أولا: الوسائل التقنية لحماية الخصوصية

تتمثل الوسائل التقنية المكرسة لحماية الخصوصية المعلوماتية في كل من: التشفير (أ) وتقنية العقلية (ب)، وجدران الحماية (ج)، وكلمة السر(د).

أ) التشفـــــير:

لجأت العديد من الدول إلى اعتماد مختلف صور الحماية الخاصة للأفراد في مجال نظام معالجة المعلومات، ومن بين أهم هذه الصور نجد التشفير الذي يأتي في صدارة هذه الوسائل، والذي يعمل على توفير الأمن للبيانات وضمان سريتها.

يعرف التشفير أو ما يطلق عليه أيضا بمصطلح "التعميه"، على أنه الرسالة التي تمنع الاعتراض على البيانات والمعلومات الخاصة بحيث يمنع الولوج إلى النظام الرقمي لمختلف الحسابات والرسائل الالكترونية أو تغيير شكلها الحقيقي وإبرازها بشكل آخر غير واضح ويصعب على المعتدي فهمها واستنباطها. وقد عرفه الأستاذ "بوير" بأنه: *"تشفير المعلومات هو تغيير مظهرها بحيث يختفي مظهرها الحقيقي فتكون غير مفهومة لمن يتجسس عليها"*[1].

[1]– وافد يوسف، النظام القانوني للدفع الالكتروني، مذكرة لنيل درجة ماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2011، ص ص 161 – 162.

يتم استخدام التشفير باعتباره أداة فعالة لحماية الخصوصية وسلامة البيانات من كل أشكال الاعتداء، وفق طريقتين هما[1]:

1. تشفير الوصلة:

بموجب هذه الطريقة يتم تشفير البيانات قبل وضعها في شبكة الاتصالات المادية، حيث تفتح الشفرة بموجب دخول اتصالات الحاسوب المستلم، وتتلائم هذه الطريقة عندما يكون خط الإرسال ضعيفا بينما يتمتع بقية المضيفين بالأمان في شبكة الانترنت، وعلى هذا النحو يتم حماية الرسالة عند إرسالها بين الحاسوبين على أن تكون واضحة ومفهومة فقط بين المضيفين.

2. تشفير نهاية إلى نهاية:

يؤمن حماية من نهاية واحدة من التراسل إلى النهاية الأخرى يمكن استخدام التشفير باستخدام جهاز التشفير بين المستخدم والمضيف والخيار الآخر باستخدام برمجيات تنفذ على الحاسوب المضيق في كلتا الحالتين.

ب) تقنية العقلية:

نجد إلى جانب التشفير تقنية أخرى وهي تقنية العقلية، فنظرا لما تشكوه الانترنت من نقص على مستوى الأمن، ما يشكل تهديداً للحياة الشخصية، بالأخص حق المستخدم للشبكة في احترام سرية الاتصالات التي يجريها، وهذا ما دفع إلى ابتكار أساليب وتقنيات جديدة لتأمين اتصالاتهم عبر الانترنت بصورة محكمة ومستمرة، وذلك بواسطة معدات يطلق عليها تسمية "أجهزة معاودة الإرسال بشكل معقل" ومثال ذلك: المداخلات والحوارات التي تجرى داخل المنتديات والمجموعات الإخبارية والتي تكون مخصصة لمواضيع معينة طبية واجتماعية

[1]– نقلا عن: سعد عبد العزيز العاتي و علاء حسين الحمامي، تكنولوجيا الأمنية للمعلومات وأنظمة الحماية، الطبعة الأولى، دار وائل للنشر، عمان، 2007، ص 78.

وسياسية، فيتم حفظ وتوثيق هذه الحوارات والمداولات، ويمكن لمن يشاء الاطلاع عليها، وذلك بعملية بسيطة يمكن العثور على أسماء وأصحاب الرسائل وعناوينهم.

يعاب على هذه التقنية بالرغم من المنافع التي تتمتع بها والتي تعمل على حماية الحياة الخاصة للأفراد، إلا أنها ذات تأثير سلبي في حالة الاساءة في استعمالها، بحيث تسهل النشاطات غير المشروعة والإجرامية على شبكة الانترنت كأن تستخدم هذه التقنية في التشهير، ولذلك عملت شركات حماية خصوصية المعلومات والأنظمة على تطوير أحدث التطبيقات كما هو الشأن بالنسبة لتكريس ما يسمى بجدران الحماية، وبرامج مكافحة الفيروسات، وتطبيقات الحماية ضد محاولات اختراقات الأنظمة المعلوماتية[1].

ت) جدران الحماية:

يطلق عليها أيضا بمصطلح "الجدران النارية"، وهي أدوات الكترونية أمنية تمنع الوصول غير المسموح به إلى الحاسب الشخصي، وذلك عن طريق إقامة حاجز يفصل بين الشبكة والحواسيب الشخصية، حيث تحول دون تحقيق عمليات الدخول والخروج إذ تتصدى لجميع محاولات الدخول بدون صفة، لكن هذه الوسيلة لا تكفي لوحدها لحماية المعلومات بشكل كلي، ولذلك توجب استخدام تقنيات الأمن الشامل التي تنظم العديد من الأنظمة والأجهزة الالكترونية مثل وسائل أمن الملفات ووسائل كشف الاقتحام وأجهزة الرقابة[2].

ث) كلمة السر:

تنقسم كلمة السر إلى نظامين، نظام هوية المستخدم (1)، ونظام كلمة السر التي لا تتكرر (2).

---

[1]– عدنان سوزان ، انتهاك حرمة الحياة الخاصة عبر الانترنت – دراسة مقارنة، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 29، العدد الثالث، كلية الحقوق، جامعة دمشق، 2013، ص 443.

[2]– حابت آمال، التجارة الالكترونية في الجزائر، رسالة لنيل شهادة دكتوراه في العلوم، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2015، ص 279.

1. نظام هوية المستخدم وكلمة السر:

يصادق المستخدم عند دخوله للاستفادة من الخدمات الالكترونية، وجوب إدخال هويته وكذا كلمة السر فبدون هذين النظامين لا يمكنه الدخول مرة أخرى وإتمام أي عملية إلا باستخدامهما. لكن ورغم هذه الاحتياطات المتخذة إلا أن محترفوا الإجرام عبر الانترنت وبفضل ابتكاراتهم وخبرتهم التقنية، يتم التمكن من دخول ومعرفة وكشف كلمة السر وهو ما يشكل خطورة خاصة بالنسبة المؤسسات البنكية، إذ يمكن للجاني القيام بتحويل الأموال إلى حسابات أخرى دون ترك أي أثر[1].

2. نظام كلمة السر التي لا تتكرر:

أطلق عليها هذا الاسم نظراً لأن كلمة السر لا تكون صالحة إلا مرة واحدة، فلا يمكن معاودة استخدامها مرة أخرى، وهو نظام تستخدمه خاصة البنوك وذلك في عملياتها التي تتضمن أوامر بالدفع، وهو نظام يعتمد على معرفة كل من العميل والبنك التوصل إلى كلمة السر، فهو عمل مشترك بينهما، ويتم تزويدها بنفس كلمة المرور وعدد مرات إدخالها[2].

ثانيا: الوسائل التنظيمية لحماية الخصوصية

يعتبر التنظيم الذاتي من الأعراف والقواعد السلوكية المتكونة ضمن القطاعات المهنية والتجارية المختلفة، لمزاولة نشاطاتها عبر شبكة الانترنت، فنجد أرباب العمل يتبعون غالبا قواعد سلوكية ذاتية، تحكم علاقاتهم المهنية وتنظيمها، فيرى كثيرون أن طرح التنظيم الذاتي لشبكة الانترنت بمثابة الحل المثالي، في تنظيم استخدام الشبكة، فكان لغرفة التجارة الدولية

[1]– حابت آمال، مرجع سابق، ص ص 275 – 276.

[2]– حابت آمال، المرجع نفسه، ص 276.

ومجلس أوربا دور متقدم في عقود نقل البيانات وذلك بوضع نماذج هذه العقود ليتم استخدامها لتسهيل عمليات نقل البيانات وضمان الالتزام بقواعد الحماية[1].

انطلاقا مما سبق يتضح أن إشكالية الحماية التي تطرحها جرائم الانترنت، هي ذات بعد دولي وليس خاص بدولة معينة، لذا كان لزاماً العمل على مكافحتها وبذل جهود كبيرة سواءً على المستوى الداخلي أو الدولي للحد من الآثار الوخيمة التي ترتبها هذه الجرائم على المجتمعات والمصالح الأمنية للدولة.

المطلب الثاني

الجهود الوطنية والدولية لمكافحة جرائم الانترنت

أصبحت جرائم الانترنت هاجس يثير قلق مختلف الدول لكونها جريمة عابرة للحدود يصعب التحكم فيها، فهي ليست محصورة في نطاق محدد أو وليدة بيئة معينة وهذا ما جعل رجال العلم والقانون على المستوى الوطني يبذلون من الجهود ما يحقق مكافحتها والحد منها(الفرع الأول)، إضافة إلى الجهود الدولية التي تعد دعامة حقيقية تستعين بها الدول في تكريس الحماية التشريعية من هذه الجرائم (الفرع الثاني).

الفرع الأول

الجهود الوطنية لمكافحة جرائم الانترنت

تعد جرائم الانترنت من الجرائم الحديثة المرتبطة بتطور تكنولوجيات الإعلام والاتصال التي تستدعي إمكانات وخبرات تقنية لا يمكن مواكبتها إلا بإنشاء هيئات ومراكز متخصصة لمكافحة الجرائم المتصلة بها. ولذا قام المشرع الجزائري وفي إطار مكافحة الجريمة المعلوماتية

[1]– عدنان سوزان ، مرجع سابق، ص 444.

اتخاذ العديد من التدابير من أجل مواجهة هذه الجرائم سواءً من خلال قانون رقم 04 – 15 المعدل لقانون العقوبات (أولا)، والقانون رقم 09 – 04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها(ثانيا).

أولا: الجهود الوطنية المبذولة في إطار القانون رقم 04 – 15

سبق وأن أشرنا إلى الجرائم التي تناولها القانون رقم 04 – 15 المعدل لقانون العقوبات من خلال إدراج قسم آخر وهو القسم السابع مكرر المعنون بـ "المساس بأنظمة المعالجة الآلية للمعطيات"، الذي تدارك المشرع الجزائري به الفراغ القانوني الذي كانت تعاني منه المنظومة التشريعية في مجال الإجرام عبر الانترنت.

يتضمن هذا القسم 8 مواد نصت على مجموعة من الجرائم كجريمة الدخول أو البقاء غير المصرح به داخل منظومة للمعالجة الآلية للمعطيات، وجريمة التلاعب غير المصرح به للمعطيات وجريمة التعامل في معلومات غير مشروعة وذلك في المواد من 394 مكرر إلى م394 مكرر2[1]، كما نصت على الظروف المشددة والشروع في ارتكاب هذه الجرائم والمساهمة الجنائية[2] فيها إضافة إلى إقرار عقوبة المصادرة للأجهزة والبرامج المستخدمة في ارتكابها من خلال المواد 394 مكرر3 إلى م394 مكرر7[3].

[1]– أنظر المواد من 394 مكرر إلى م394 مكرر2 من الأمر 66 – 156 المتضمن قانون العقوبات المعدل والمتمم، مرجع سابق.

[2]– أكد المشرع الجزائري على تجريم الاشتراك سواءً صدر من طرف شخص طبيعي أو شخص معنوي، ضمن مجموعة أو عن طريق اتفاق بغرض الإعداد لارتكاب إحدى الجرائم السالفة، والخضوع لنفس العقوبة المقررة لمرتكبيها، سواءً كان هذا الإعداد مجسداً بفعل أو بعدة أفعال مادية. أنظر: صغير يوسف، مرجع سابق، ص 111.

[3]– أنظر المواد من 394 مكرر3 إلى م394 مكرر7 من الأمر 66 – 156 المتضمن قانون العقوبات المعدل والمتمم، مرجع سابق.

ثانيا: الجهود الوطنية المبذولة في إطار القانون رقم 09 – 04

جاء القانون رقم 09 – 04 من أجل سد الفراغ الذي أحدثه القانون رقم 04 – 15 المتضمن تعديل قانون العقوبات. فمن خلال هذا القانون تم إنشاء هيئة وطنية من أجل مكافحة الجريمة المعلوماتية وذلك بموجب م 13، التي تنص على أنه: *"تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها"*[1]، تتولى هذه الهيئة 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[2]، وقد تم تحديد كيفية تشكيل وتنظيم عمل الهيئة بموجب المرسوم الرئاسي رقم 15 – 261، الذي أكد على استقلاليتها وتمتعها بالشخصية المعنوية وارتباطها بوزارة العدل وخضوعها لرقابة السلطة القضائية[3].

تلعب هذه الهيئة دوراً بارزاً في مكافحة جرائم الانترنت[4] لاسيما ما يتعلق بالإرهاب الالكتروني، بحيث تتولى الهيئة بمراقبة الاتصالات الالكترونية الخاصة بالشبكات الإرهابية وذلك بمشاركة الوحدات المرخص لها قضائيا بعملية المراقبة، وقد ساهمت من خلالها تعاونها

---

[1]– أنظر م 13 من القانون رقم 09 – 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

[2]– حابت آمال، مرجع سابق، ص ص 354 – 355.

[3]– أنظر المادتين 2 و4 من مرسوم رئاسي رقم 15 – 261 مؤرخ في 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر العدد 53 صادر بتاريخ 08 أكتوبر 2015.

[4]– يعاب على تشكيلة الهيئة تغييب الجهات الفاعلة التي تلعب دور أساسي في إنجاح عملها لاسيما ما يتعلق بالوزير المنتدب لدة وزارة المالية المكلف بالاقتصاد الرقمي لما له من صلة وثيقة بالهدف المرجو من إنشاء هذه الهيئة. حول تشكيلة الهيئة والنقائص التي تعاني منها، أنظر: ناني لحسن، التحقيق في الجرائم المتصلة بتكنولوجية المعلوماتية بين النصوص التشريعية والخصوصية التقنية، النشر الجامعي الجديد للطباعة والنشر والتوزيع، الجزائر، 2017، ص ص 86 – 87.

مع الأجهزة الأمنية الوطنية في معالجة أكثر من 1000 جريمة الكترونية من بينها 16 قضية متعلقة بالإرهاب الالكتروني، ترتب عنها توقيف 58 إرهابي[1].

تتمتع سلطة الضبط القضائي بدور فعال في ضبط أدلة الإجرام ومرتكبيها وكشف كل ما يتعلق بحال وقوعها، لكن في الجرائم المستحدثة تلقى المزيد من الأعباء على عاتقها نظراً لضعف خبرتها في هذه الجرائم كون ضباط الشرطة القضائية غير قادرين على التعامل بوسائل الاستدلال والإجراءات التقليدية مع هذا النوع من الجرائم، وقد يفشل هذا الجهاز في تقدير أهمية الجريمة نظراً لنقص الخبرة والتدريب، لهذا كان من أولويات السياسة الوطنية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال تكوين وتأهيل سلك ضباط الشرطة القضائية وأعوانهم، فعلى مستوى الدرك الوطني الذي باشر منذ سنة 2004 في عمليات تكوين مستخدمين من أجل إنشاء مركز وطني لمكافحة جرائم الانترنت، فبموجب هذا العمل فإن الكثير من إطارات الدرك الوطني استفادوا من التكوين في مؤسسات وطنية مثل مركز الدراسات والبحوث في الإعلام الآلي والتقني CERIST، الذي يستهدف من خلال هذا التكوين إلى تطوير كفاءات سلك الدرك الوطني حتى تكون أكثر فعالية في مجال مكافحة هذه الجرائم[2].

الفرع الثاني

الجهـود الدوليـــة للحد من جرائم الانترنت

سجلت العديد من الجهود في مجال مكافحة جرائم الانترنت، ونذكر من بينها الجهود المبذولة من طرف الاتحاد الدولي للاتصالات لحماية الفضاء الالكتروني (أولا)، والجهود

[1]– نقلا عن: بن صويلح آمال، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الالكتروني بالجزائر، مداخلة مقدمة في الملتقى الدولي الثالث حول "الإجرام السيبراني المفاهيم والتحديات"، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي، برج بوعريريج، يومي 11 و12 أفريل 2017، ص 8.

[2]– أحمد مسعود مريم، آليات مكافحة تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 09 – 04، مذكرة لنيل شهادة الماجستير، تخصص: قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2013، ص ص 46 – 47.

العربية التي تجسدت من خلال عقد العديد من المؤتمرات ذات الصلة بمكافحة جرائم الانترنت (ثانيا).

أولا: جهود الاتحاد الدولي للاتصالات لحماية الفضاء الالكتروني

وضع الاتحاد الدولي للاتصالات لحماية الفضاء الالكتروني، مجموعة من التوصيات بيّن فيها الأطر التنظيمية والإجراءات العملية التي تهدف إلى منع الاستعمال غير المصرح به، مع تحديد السبل المسموح بها لاستعمال المعلومات وأنظمة الاتصالات الالكترونية، وشدد على عدة مبادئ منها:

- خصوصية المعطيات والمعلومات، ومن ثمة تم التركيز على التصريح في كل عملية تخضع لها هذه المعطيات، سواءً تعلق الأمر بالتصريح بالدخول أو الاستعمال أو البقاء في المنظومة الاكلترونية.
- الحرص على إيجاد السبل الكفيلة لحماية المواطنين والمستخدمين لهذه التقنيات من كافة المخاطر التي قد ترتب عن استعمالها، واختراق الشبكات بهدف سرقة المعلومات والأسرار ذات الأهمية الخاصة.
- حماية الاقتصاد بشكل عام والبيانات والمعلومات المخزنة بشكل خاص.

دعى كل ذلك إلى مواجهة كل التحديات بتضافر الجهود والقوانين والأنظمة والإجراءات العملية والتكنولوجية، ووضع إجراءات حماية فعالة والتشديد على تطبيقها، واستخدام جدران الحماية مع كلمات السر والترميز والتشفير[1].

[1]– لاروش راضية، أمن التوقيع الالكتروني، مذكرة لنيل شهادة الماجستير في القانون، فرع القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012، ص ص 172 – 173.

ثانيا: المؤتمرات الدولية المنعقدة في الدول العربية لمكافحة جرائم الانترنت

اقتصرت الجهود العربية في مجال مكافحة جرائم الانترنت، على بعض المؤتمرات التي انعقدت لمكافحة جرائم تقنية المعلومات، والتي نذكر من بينها ما يلي[1]:

أ) **مؤتمر مكافحة جرائم تقنية المعلومات:** انعقد هذا المؤتمر في دولة الإمارات العربية المتحدة في الفترة ما بين 26 و27 نوفمبر 2006، حيث ارتكز المؤتمر على ثلاث محاور رئيسية وهي: الجريمة المعلوماتية ووسائل ارتكابها وآثارها، والوسائل القانونية في مكافحة الجريمة المعلوماتية وحماية تقنية المعلومات، والوسائل الأمنية والفنية في حماية تقنية المعلومات، والذي انتهى إلى التأكيد على ضرورة اعتماد قانون مكافحة تقنية المعلومات الإماراتي رقم 2 لسنة 2006، وقانون المعاملات الالكترونية رقم 1 لسنة 2006، كقانونين نموذجيين يحتذى بهما في التشريع الوطني.

ب) **المؤتمر البنغازي الأول حول المعلوماتية والقانون:** والذي انعقد في 10 أوت 2009 بليبيا، وقد ركز على ضرورة مواكبة نصوص القانون المدني للتطورات الحاصلة في مجال تكنولوجيا المعلومات والعمل على مواجهة الجرائم.

ج) **المؤتمر الدولي الثاني لمكافحة جرائم تقنية المعلومات:** انعقد في الإمارات العربية المتحدة سنة 2008، والذي يهدف إلى تكثيف الجهود لمكافحة الجريمة المنظمة ومكافحة جرائم تقنية المعلومات، والدعوة إلى إعادة دراسة ومراجعة القانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات.

[1]– نقلا عن: قنديل أشرف عبد القادر، الإثبات الجنائي في الجريمة الالكترونية، دار الجامعة الجديدة للنشر، الاسكندرية، 2015، ص ص 99 – 101.

د) **مؤتمر التحديات التشريعية في عصر تكنولوجيا المعلومات والاتصال:** أقيم هذا المؤتمر في القاهرة سنة 2009، تناول فيه المشاركون الجوانب القانونية في الجرائم المعلوماتية من حيث تعريفها وخصائصها ودوافع ارتكابها وبداية نشأة شبكة الانترنت، وتمت التوصية بضرورة اعداد مشروع قانون لمكافحة الجرائم المعلوماتية، وضرورة توعية فئة الشباب للدور الذي تلعبه شبكة الانترنت.

ذ) **مؤتمر الجريمة الالكترونية وتحديات التنمية الاقتصادية:** انعقد هذا المؤتمر في القاهرة سنة 2009 تحت عنوان"تحديات تكنولوجيا المعلومات والتنمية الاقتصادية"، الذي أوصى فيه المشاركون بضرورة المتابعة الجزائية لمرتكبي جرائم الانترنت ووضع التشريعات موضع تحيين وتعديل.

المبحث الثاني

المتابعة الجزائية لمرتكبي جرائم الانترنت

تدارك المشرع الجزائري خلال السنوات الأخيرة ولو نسبيا الفراغ القانوني الذي شهدته المنظومة التشريعية في مجال مكافحة جرائم الانترنت، في مجال الإجرام المعلوماتي عموما والإجرام عبر الانترنت خصوصا، من خلال تكريس العديد من التدابير والقواعد الإجرائية بموجب القانون رقم 09 – 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها (المطلب الأول)، مع فرض عقوبات تختلف من حيث الشدة باختلاف ارتكابها (المطلب الثاني)، غير أن هذه الجهود غالباً ما تصطدم بعدة عراقيل وإشكالات تتعلق بالمتابعة الجزائية (المطلب الثالث).

المطلب الأول

إجراءات المتابعة الجزائية لمرتكبي جرائم الانترنت على ضوء القانون رقم 09 – 04

أبرز المشرع الجزائري في مجال مكافحة جرائم الانترنت قانون رقم 09 – 04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الذي جاء بتقنيات جديدة وأحكام أخرى توضح القواعد الإجرائية لهذه الجرائم (الفرع الأول)، مؤكداً على أهمية التعاون والمساعدة القضائية الدولية في مكافحتها(الفرع الثاني).

الفرع الأول

القواعد الإجرائية لمكافحة جرائم الانترنت

يهدف القانون رقم 09 – 04 السالف الذكر، إلى سن قواعد الوقاية من الجرائم التي تتعلق بتكنولوجيات الإعلام والاتصال، والتي تتمثل في جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأيّ جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية، وهذا ما نصت عليه المادة الأولى من هذا القانون، والتي جاء فيها *"يهدف هذا القانون إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها"*[1].

نذكر من بين أهم هذه الإجراءات الجزائية التي جاء بها هذا القانون إضافة إلى القواعد العامة الواردة في ق.إ.ج.ج، والمتخذة لمكافحة جرائم الانترنت، إجراء مراقبة الاتصالات الالكترونية (أولا)، وإجراء التفتيش (ثانيا)، إضافـــة إلى إجراء حجز المعطيات المعلوماتية(ثالثا).

أولا: إجراء مراقبة الاتصالات الالكترونية

ذكرت المادة 4 من القانون رقم 09 – 04 الحالات التي تسمح باللجوء إلى المراقبة الالكترونية، التي تكمن في القيام بعمليات المراقبة المنصوص عليها في المادة 3 والتي تتمثل في ترتيبات تقنية لمراقبة الاتصالات الالكترونية، وتجميع وتسجيل محتواها في حينها والقيام

[1]– أنظر المادة الأولى من قانون رقم 09 – 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

بإجراءات التفتيش والحجز داخل منظومة معلوماتية وذلك بهدف حماية الحياة الخاصة للفرد، في الحالات الآتية[1]:

أ) الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

ب) في حالة توفر معلومات من احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام، أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

ت) لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.

ث) في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

ولا يجوز إجراء عمليات المراقبة في الحالات المذكورة إلا بإذن مكتوب من الجهة القضائية المختصة.

يختص النائب العام لدى مجلس قضاء الجزائر وفق ما ورد في الفقرة "أ" من المادة السابقة الذكر، بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في م 13 إذن لمدة ستة (6) أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

وتكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الفقرة "أ" من هذه المادة موجهة حصرياً لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتها، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

[1]– أنظر م4 من القانون رقم 09 – 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

ثانيا: إجراء التفتيـــش

التفتيش إجراء من إجراءات التحقيق الابتدائي، يعمل على البحث عن دليل متعلق بجريمة تم ارتكابها، سواءً تعلق التفتيش بشخص أو بمسكن، وعليه يمتاز هذا الإجراء بالخطورة نظراً لمساسه بالحريات الشخصية للمواطنين وحرمة مسكنهم[1].

كرس المشرع الجزائري الطابع الدستوري لإجراء التفتيش بموجب م40 منه التي جاء فيها: *"فلا تفتيش إلا بمقتضى القانون وفي إطار احترامه، ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة"*[2]، وهو ما يجسد ضمانة قانونية اتجاه أي اعتداء لحرية الأشخاص وكرامتهم، لذا استلزم الأمر تقييد هذا الإجراء بمجموعة من الضوابط التي يجب مراعاتها قبل إصداره وأثناء تنفيذه.

تقوم في الأصل السلطة المختصة بتفتيش النظم المعلوماتية بنفسها، وذلك بندب ضابط أو ضباط الشرطة القضائية وفقاً لقواعد اجرائية محددة، كوجوب ذكر وتحديد المكان والأشياء المراد تفتيشها وضبطها في إذن التفتيش كالحاسوب والمصنفات الالكترونية محل التفتيش[3]. تهدف هذه القواعد إلى تجنب التفتيش الاستكشافي فلا يترك التفتيش للسلطة التقديرية لضابط الشرطة الذي يقوم بالتنفيذ، إذ أن أي تفتيش يرد على أشياء غير مذكورة في الإذن يعرض الإجراء إلى الإبطال، وقد أطلق القضاء الأمريكي على التفتيش المخالف لهذه القواعد بمصطلح

---

[1]– زبيخة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للنشر والتوزيع، الجزائر، 2011، ص 130.

[2]– المادة 40 من مرسوم رئاسي رقم 96 – 438 مؤرخ في 7 ديسمبر 1996، يتضمن الدستور المصادق عليه في استفتاء 28 نوفمبر 1996، ج ر العدد 76 صادر في 8 ديسمبر 1996، المعدل والمتمم بموجب القانون رقم 02 – 03 مؤرخ في 10 أفريل 2004 ج ر عدد 25 صادر بتاريخ 14 أفريل 2002، المعدل والمتمم بموجب القانون رقم 08 – 09 في 15 نوفمبر 2008 ج ر العدد 63 صادر بتاريخ 16 نوفمبر 2008، المعدل والمتمم بموجب القانون رقم 16 – 01 المؤرخ في 06 مارس 2016 ج ر عدد 14 صادر في 07 مارس 2017.

[3]– مكاري نزيهة ، "إثبات جرائم الاعتداء على حق المؤلف عبر الانترنت في التشريع الجزائري (دراسة مقارنة)"، مجلة العلوم الاقتصادية وعلوم التسيير، العدد 9، معهد علوم التسيير والاقتصاد، المركز الجامعي برج بوعريريج، 2009، ص ص 132 – 134.

"المخالفة الواضحة للإذن" وهو اعتداء على حياة الأشخاص الخاصة. كما يجب توفر الخبرة في المجال الالكتروني وخاضع لفترة تدريبية تتعلق بكيفية التعامل مع تقنية المعلومات وأنظمة معالجة المعطيات لدى القائم بالتفتيش، حتى يتم الاستفادة من هذه المعطيات بشكل فعال وتفادي تعرضها للتلف والضياع من جهاز الحاسوب[1].

كرست م5 من القانون رقم 09 – 04 السالف الذكر إجراء تفتيش المنظومات المعلوماتية كقاعدة من القواعد الإجرائية التي تتخذها الجهة القضائية في جرائم الانترنت إذا تعلق الأمر بمنظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، أو تعلق الأمر بمنظومة تخزين معلوماتية[2].

يلاحظ من خلال هذه المادة كذلك، أن التفتيش في الوضعيات المشار إليها آنفا يتخذ شكلين، فهو عبارة عن عمل من أعمال الاستدلال يقوم به ضباط الشرطة القضائية بناءً على أمر تصدره السلطة المختصة، أو عمل من أعمال التحقيق، كما يتبين أن هذا الإجراء قد يتم بصفة مباشرة بالانتقال إلى مسكن المتهم، أو المكان الذي تتواجد فيه الاجهزة المقصودة أو في الأماكن العامة حال حيازة شخص لجهاز الحاسوب الآلي أو أحد مكوناته المادية كوسائل التخزين، بحسب ما هو معمول به بموجب القواعد العامة في ق.إ.ج.ج، أو بصفة غير مباشر وذلك عن بعد الذي يقتضي الدخول إليها دون إذن صاحبها والولوج إلى النظام الذي يقوم عليه الحاسوب، فالتفتيش هنا يستهدف أشياء معنوية وفنية وليست مادية كالبرامج وقواعد البيانات.

سمح قانون رقم 09 – 04 من خلال هذه المادة أيضا للسلطة المكلفة بالتفتيش، باللجوء إلى الأشخاص المؤهلين كالخبراء والتقنيين المختصين في مجال الانترنت وذلك

[1]– حجازي عبد الفتاح بيومي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الفكر الجامعي، مصر، 2006، ص 355.

[2]– أنظر م5 من القانون رقم 09 – 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

بتسخيرهم في إطار القيام بعمليات تفتيش المنظومة المعلوماتية وحماية المعطيات المتحصلة وتزويد السلطة المكلفة بالتفتيش بالمعلومات الضرورية ومساعدتهم على إنجاز مهمتهم.

ثالثا: إجراء حجز المعطيات المعلوماتية

تنص م6 من قانون رقم 09 – 04 السالف الذكر، على أنه: *"عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.*

يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية.

غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات" [1].

يتضح من خلال نص هذه المادة أنه عند القيام بالتفتيش من طرف السلطة المختصة، يتم البحث عن معلومات ومعطيات تكون مخزنة في المنظومة المعلوماتية، كما تقوم بنسخ فقط المعطيات التي تخدم بحثها والتي تكون لازمة للكشف عن الجريمة، من خلال تخزينها على دعامة تكون قابلة للحجز وفقاً لما هو مقرر في ق.إ.ج.ج دون المساس بكل المنظومة، وذلك من أجل تأمين السلامة للمعطيات التي تجرى بها العملية وعدم تخريبها. كما أنه يمكن لها استعمال وسائل تقنية لتشكيل أو إعادة تشكيل تلك المعطيات حتى تكون قابلة للاستغلال وتلبية لمتطلبات التحقيق، مع مراعاة عدم الاضرار بمحتوى تلك المعطيات متى استدعت الضرورة ذلك.

[1]– ناني لحسن، مرجع سابق، ص ص 125 – 126.

تجدر الإشارة أن حجز البيانات والمعطيات كان محل جدل بين الفقهاء، وانقسموا في ذلك إلى اتجاهين، اتجاه أول يرى بأن انتفاء الكيان المادي في هذه البيانات يجعلها غير صالحة للحجز إلا باستخدام التصوير أو نقلها إلى كيان مادي ملموس، في حين يرى الاتجاه الثاني أن يرى بصلاحيتها للحجز طالما أنها قابلة للحفظ والتخزين لاسيما وأنها عبارة عن مجموعة من الذبذبات الالكترونية والموجات الكهرومغناطيسية التي تسمح بتحويلها إلى كيان مادي[1].

الفرع الثاني

التعاون والمساعدة القضائية في مجال مكافحة جرائم الانترنت

يرتبط التعاون والمساعدة القضائية بعدة مسائل نذكر من بينها: الاختصاص القضائي(أولا)، والمساعدة القضائية (ثانيا)، وتبادل المعلومات والإجراءات التحفظية (ثالثا).

أولا: الاختصاص القضائي

يعتبر الاختصاص القضائي من الجوانب المهمة في توطيد التعاون لمكافحة جرائم الانترنت، وقد أكدت على ذلك م15 من القانون رقم 09 – 04، التي جاء فيها: *"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 أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني"*[2].

نلاحظ من خلال هذه المادة حرص المشرع الجزائري على امتداد الاختصاص القضائي للمحاكم الجزائرية عندما ترتكب جرائم الانترنت ملحقة أضراراً بالأمن الوطني للدولة، حتى لو

[1]– الشمري غانم مرضي ، مرجع سابق، ص 174.

[2]– أنظر م15 من القانون رقم 09 – 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

ارتكبت خارج الإقليم الجزائري، ومن ثمة التطبيق العيني لنصوص قانون العقوبات نظراً لخطورة هذه الجريمة عند استهدافها للأجهزة الأمنية والمصالح الاستراتيجية للدولة.

ثانيا: آلية التبادل في مجال المساعدة القضائية الدولية

تهدف عملية التبادل في مجال المساعدة القضائية الدولية إلى جمع الأدلة لصالح الدولة الطالبة لهذه المساعدة، بحيث تكون بأمس الحاجة إليها من أجل استكمال تحرياتها الخاصة بالجرائم الالكترونية، التي تتم من طرف سلطاتها المختصة، وهو ما أكدت عليه م16 من نفس القانون، والتي تنص على أنه: *"في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الالكتروني.*

يمكن في حالة الاستعجال، ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى، إذ أوردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الالكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها" [1].

نستنتج من خلال هذه المادة أن السلطات الجزائرية المختصة بإمكانها تبادل المساعدات مع الدول الأخرى وتتبع الجرائم الالكترونية المرتكبة، وهذه المساعدة لا تتطلب اتباع رسميات وشكليات معينة وإنما يمكن في حالة الاستعجال اللجوء إلى وسائل الاتصال السريعة من أجل التأكد من صحة المعطيات الواردة إليها.

[1]– أنظر م16 من القانون رقم 09 – 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

ثالثا: تبادل المعلومات واتخاذ الإجراءات التحفظية

تستوجب المساعدة القضائية من أجل تبادل المعلومات وقبولها، اتخاذ بعض الإجراءات من طرف الدولة الطالبة للمساعدة وكذلك الدولة المستقبلة للطلب، بناءً على ما تنص عليه الاتفاقيات المبرمة فيما بينها سواء كان ثنائية أو جماعية، وهذا ما أوضحته نص م17 من القانون رقم 09 – 04، التي جاء فيها: *"تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل"* [1].

يتضح من خلال هذه المادة أن الاستجابة لطلبات المساعدة القضائية التي تهدف للحصول على معلومات واتخاذ تدابير تحفظية تجاه جرائم الانترنت، تتوقف على مدى انضمام الدولة الجزائرية للاتفاقيات الدولية المبرمة في هذا المجال، أو كان مصدر الاستجابة هو المعاملة بالمثل مع الدول التي تكون قد بادرت بتقديم طلبات المساعدة القضائية أو الاستجابة للطلبات المقدمة من طرف الدولة الجزائرية.

رابعا: القيود الواردة على طلبات المساعدة القضائية الدولية

تعتبر المساعدة القضائية الدولية من الإجراءات التي تلعب دوراً مهماً للحد من الجرائم الالكترونية على وجه الخصوص، لكن هذه المساعدة ليست مطلقة في نظر المشرع الجزائري بل قيدها بشروط نص عليها في م18 من القانون رقم 09 – 04، التي جاء فيها: *"يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام.*

يمكن أن تكون الاستجابة لطلبات المساعدة مقيدة، بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب.

[1]– أنظر م17 من القانون رقم 09 – 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

طلبات المساعدة القضائية غرضها هو تقديم المساعدة التي تشمل الخبرة والمواد التي الدولة الطالبة للمساعدة والقضاء على نوع تلك الجرائم، لكن إذا كانت هذه المساعدة تمس إما بالسيادة الوطنية أو النظام العام، فهذه الطلبات يتم رفضها، أو تكون هذه المساعدة لها شروط أي تقيد بشرط عدم استعمالها لأغراض أخرى غير ما هو موضح في طلب المساعدة أو تكون مقيدة بالمحافظة على سرية المعلومات المبلغة" [1].

يتضح من خلال هذه المادة أن المساعدات القضائية ليست مطلقة، فيمكن رفضها إذا كانت هذه الأخيرة تهدف إلى المساس بالسيادة الوطنية وكذا أمنه العام، لكن يمكن قبول بعضها على أن تبقى مقيدة بشروط كالإبقاء على الطابع السري للمعلومات أو عدم استعمالها لأغراض أخرى غير تلك الموضحة في طلب المساعدة.

المطلب الثاني

الجزاءات المقررة لجرائم الانترنت

استدركت أغلب الدول بمختلف أنظمتها القانونية الفشل في ملائمة القوانين النافذة استجابة للاعتداءات الحاصلة على الأنظمة المعالجة للبيانات ومن بين هذه التشريعات نجد المشرع الجزائري الذي تطرق إلى تجريم الأفعال التي تمس بهذه الأنظمة، ومن خلال تعديل قانون العقوبات بموجب القانون رقم 04 – 15 السالف الذكر، حيث نص على عدة عقوبات تتنوع بين عقوبات أصلية وأخرى تكميلية، مطبقة سواءً على الشخص الطبيعي (الفرع الأول)، أو على الشخص المعنوي (الفرع الثاني).

[1]– أنظر م18 من القانون رقم 09 – 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

الفرع الأول

العقوبات المقررة على الشخص الطبيعي

تطبق على الشخص الطبيعي عدة عقوبات، عقوبات أصلية (أولا)، وعقوبات تكميلية (ثانيا).

أولا: العقوبات الأصلية

من خلال استقراء النصوص القانونية المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية، يتبين وجود تدرج داخل النظام العقابي، فهذا التدرج يحدد الخطورة الإجرامية التي قدرها المشرع لهذه التصرفات[1]، إذ نجد سلم الخطورة تختلف باختلاف خطورة هذه الجرائم، سواء تعلق الأمر بالعقوبات المقررة لجريمة الدخول أو البقاء غير المصرح به داخل نظام المعالجة الآلية للمعطيات(أ)، أو جريمة التلاعب غير المصرح به بالمعطيات (ب)، أو لجريمة التعامل في معلومات غير مشروعة (ج).

أ) العقوبة المقررة لجريمة الدخول أو البقاء غير المصرح به في منظومة للمعالجة الآلية للمعطيات:

بالرجوع إلى نص م394 مكرر من قانون العقوبات[2]، فإن العقوبة المقررة لجريمة الدخول أو البقاء غير المصرح به في منظومة للمعالجة الآلية للمعطيات بالحبس من 3 أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000 دج، على أن تتضاعف العقوبة إلى الحبس من ستة (6) اشهر إلى سنتين وغرامة من 50.000 دج إلى 150.000 دج إذا ترتب

[1]– حابت آمال، مرجع سابق، ص 396.

[2]– أنظر م394 مكرر من الأمر 66 – 165 المتضمن قانون العقوبات المعدل والمتمم، مرجع سابق.

على ذلك حذف أو تغيير معطيات المنظومة ومن ثمة اعتباره ظرفاً مشدداً للعقوبة[1]، وذلك حرصاً من المشرع الجزائري على حمايتها وحماية المعطيات المخزنة فيها.

ب) جريمة التلاعب غير المصرح به بالمعطيات:

تعاقب م394 مكرر1 مرتكبي جريمة التلاعب غير المصربح به بالمعطيات بالحبس من ستة (06) أشهر إلى ثلاثة (03) سنوات وبغرامة 500.000 دج على 2.000.000دج[2].

يتضح من خلال نص المادة أن المشرع الجزائري قد عاقب كل تلاعب بمحو أو تعديل المعطيات داخل النظام بغض النظر عن النتائج المترتبة عنها، وذلك للحماية الجنائية للمنظومة المعلوماتية وبالتالي حماية الحياة الخاصة وهي تحتوي على ثلاث صور، الإدخال والمحو والتعديل، وقد وردت هذه الأخيرة على سبيل الحصر لا المثال، حيث أن غيرها من الصور لا تعتبر جريمة في نظر القانون كالنسخ والنقل.

ج) جريمة التعامل في معلومات غير مشروعة:

جاء النص على عقوبة جريمة التعامل في معلومات غير مشروعة، في م394 مكرر2 من قانون العقوبات[3]، والتي تتجسد في الحبس من شهرين (02) إلى ثلاثة (03) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج.

ثانيا: العقوبات التكميلية

تتمثل الجزاءات المقررة بموجب الفصل السابع مكرر في العقوبات الأصلية وهي عقوبة الحبس والغرامة المالية، بينما تم النص على العقوبات التكميلية في م394 مكرر6 التي جاء

[1]– تجدر الإشارة أن المشرع الجزائري نص على اعتبار الجرائم التي تستهدف الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، من الظروف المشددة التي تؤدي إلى مضاعفة العقوبات المقررة على الجرائم الواردة في القسم السابع مكرر من قانون العقوبات. أنظر: م394 مكرر3 من الأمر 66 – 156 المتضمن قانون العقوبات المعدل والمتمم، مرجع سابق.

[2]– أنظر م394 مكرر1 من الأمر 66 – 165 المتضمن قانون العقوبات المعدل والمتمم، المرجع نفسه.

[3]– أنظر م394 مكرر2 من الأمر 66 – 165 المتضمن قانون العقوبات المعدل والمتمم، المرجع نفسه.

فيها: "*مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها*"[1].

يتضح من خلال هذه المادة أن هناك العديد من أشكال العقوبة التكميلية المقررة في القسم السابع مكرر من قانون العقوبات، والتي تتمثل في العقوبات الآتي بيانها[2]:

1) **المصادرة:** وهي عقوبة تكميلية تشمل الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالأنظمة المعلوماتية مع مراعاة حقوق الغير حسن النية.
2) **إغلاق المواقع:** يتعلق الأمر بالمواقع الالكترونية التي تكون محلاً لجريمة من الجرائم الماسة بالأنظمة المعلوماتية.
3) **إغلاق المحل أو مكان الاستغلال:** إذا ارتكبت الجريمة بعلم مالكها فإنه يتعرض إلى إغلاق محله كإغلاق المقهى الالكتروني الذي ترتكب فيها هذه الجرائم.

كما نصت المادة 394 مكرر4، على توقيع العقوبة على الشخص المعنوي الذي يرتكب إحدى الجرائم الواردة في الفصل السابع مكرر بغرامة تعادل 5 مرات الحد الأقصى للغرامة المحددة للشخص الطبيعي[3].

[1]– أنظر م394 مكرر6 من الأمر 66 – 165 المتضمن قانون العقوبات المعدل والمتمم، مرجع سابق.
[2]– حابت آمال، مرجع سابق، ص 397.
[3]– أنظر م394 مكرر4 من الأمر 66 – 165 المتضمن قانون العقوبات المعدل والمتمم، مرجع سابق.

الفرع الثاني

العقوبات المقررة على الشخص المعنوي

أقر المشرع الجزائري في التعديل الأخير لقانون العقوبات المسؤولية الجزائية للشخص المعنوي، وذلك في نص م18 مكرر التي جاء فيها: *"العقوبات التي تطبق على الشخص المعنوي في مواد الجنايات والجنح هي:*

1. *الغرامة التي تساوي من مرة (1) إلى خمسة (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.*

2. *واحدة أو أكثر من العقوبات الآتية:*

- *حل الشخص المعنوي.*
- *غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 5 سنوات.*
- *الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس (05) سنوات.*
- *المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز خمس (05) سنوات.*
- *مطاردة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها نشر وتعليق حكم الإدانة.*
- *الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس (05) سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته"* [1].

[1]– أنظر م18 مكرر من القانون رقم 04 – 15، مرجع سابق.

المطلب الثالث

إشكالات المتابعة الجزائية لجرائم الانترنت

تمر جرائم الانترنت كغيرها من الجرائم الأخرى بمرحلة الاستدلال والتحقيق الجنائي، وما يترتب على ذلك من إجراءات قانونية، غير أنها تواجه هذه المرحلة صعوبات وإشكالات كثيرة، سواء تعلقت بتحديد عناصر وأدلة الجريمة (الفرع الأول)، أو تعلق الأمر بالجاني والمجني عليه (الفرع الثاني).

الفرع الأول

الصعوبات المتعلقة بتحديد عناصر ارتكاب جرائم الانترنت

تحيط جرائم الانترنت عدة صعوبات لاسيما من حيث تحديد مكان ارتكابها (أولا)، وصعوبة إثبات دليل ارتكابها (ثانيا).

أولا: صعوبة تحديد مكان ارتكاب جرائم الانترنت

ترتكب جرائم الانترنت عن طريق الاتصال بشبكة الانترنت، وبالتالي تتجاوز الحدود الدولية لتصل إلى إقليم دولة أخرى، مما يسمح للمجرم بارتكابها خارج مسرح الجريمة، وبعد ذلك تتباعد المسافة بين الفعل والنتيجة الإجرامية، وذلك ما يشكل صعوبة في كشف مكان ارتكاب الفعل غير المشروع، إلى جانب نقص خبرة الشرطة وجهات الادعاء والقضاء.

نذكر في هذا الصدد أن السلطات البريطانية قد أعلنت عن إيجادها لأكثر من عشرة آلاف أسطوانة تعليمية عن الايدز أدخلت إلى المستشفيات في كل من (بريطانيا) و(السويد) و(النرويج)، وقد اكتشفت أجهزة البيانات أنها مصابة بفيروس (نورجان) والذي له دور تخريبي سواءً البرامج التي تعمل عليها أجهزة الكمبيوتر الشخصية أو اتلاف الجهاز نفسه، فقد أثبتت

تحقيقات الشرطة، أن هذه الاسطوانات وصلت عبر البريد إلى الأشخاص من مصادر مختلفة بهدف تخريب البرامج المرسلة إليهم، وأن عددا من هذه الاسطوانات ظهرت في (بلجيكا)، (كاليفورنيا)، (زمبابوي)[1].

ثانيا: صعوبة إثبات جرائم الانترنت

يواجه رجال الضبطية القضائية والقضاة والمحققين، صعوبات عدة أثناء الإجراءات المتابعة الجزائية فيما يخص جرائم الانترنت، نظراً للطبيعة الخاصة للدليل في الجريمة الالكترونية كونه غير مرئي، لا يفصح عن شخصية معينة عادة في الجرائم التي ترتكب بواسطة البريد الالكتروني، إذ يكون صعباً على جهات التحري تحديد مصدر المرسل، فالجاني مثلا يمكن له التواجد إلى أي مقهى خاص بالانترنت والدخول إلى أحد المواقع، وإرسال رسالة تحوي عبارات سب وقذف على البريد الالكتروني الآخر، ويقوم بمحور الدليل وإعادة كل شيء كما كان دون ترك أي أثر[2].

تتمتع البيانات المخزنة الكترونيا بجدار من الحماية، تحيطه كبرى المواقع العالمية على الانترنت على بياناتها لمنع التسلل غير المشروع إليها، سواء لتدميرها أو نسخها ...الخ، إلى جانب استخدام الجاني كلمات مرور أو للتشفير بعد تخريب الموقع وهذا ما يصعب عملية الضبط والوصول إلى أي دليل وإذا وجدت هذه الأدلة أو تم الوصول إليها فهي تشير وتصادق عدة مشكلات، أمام القضاء من حيث حجيتها ومدى قبولها نظرا لأنها أدلة ذات طبيعة معنوية، مثل سجلات الكمبيوتر ومعلومات الدخول والاشتراك[3].

[1]– قنديل أشرف عبد القادر ، مرجع سابق، ص 105.

[2]– الشمري غانم مرضي ، مرجع سابق، ص 174.

[3]– عبد الله دغش العجمي، مرجع سابق، ص 85.

الفرع الثاني

الإشكالات المتعلقة بالجاني والمجني عليه

يجد مرتكبي جرائم الانترنت نوع من الحرية في ارتكابها نظراً لإحجام المجني عليه عن الإبلاغ عنها (أولا)، مما يجعل من الصعب ملاحقتهم والوصول إلى دليل لإدانتهم (ثانيا).

أولا: الإشكالات المتعلقة بالمجني عليه

سبق الذكر أن جرائم الانترنت من الجرائم المستترة التي تتم في خفاء، وبالتالي لابد من الإبلاغ عنها، وهذا من بين الصعوبات التي تواجهها النيابة العامة في تحريكها للدعوى الجنائية، فهذه الجرائم لا تصل إلى علم السلطات المعنية بالطرق العادية، كما هو الحال في الجرائم التقليدية، نظراً لصعوبة اكتشافها من قبل الأشخاص العاديين أو المؤسسات والشركات التي وقعت ضحية لهذه الجرائم، وخوفاً من الدعاية وعدم الابلاغ عن مرتكبي هذه الجرائم المعلوماتية أي الإحجام عن الإبلاغ لاسيما مع غياب نص يلزم الضحية على ذلك[1]، لذا وجب على سلطات الأمن وفي سبيل اكتشاف جرائم الانترنت، رصد حركة المعاملات التجارية داخل المؤسسات المالية وحولها، وجمع المعلومات السرية عن حركة السوق والتغيرات السلوكية للموظفين ورجال الأعمال، وكذا صغار الموظفين ذوي القدرات الفنية في مجال برامج الحاسب الآلي، إلى جانب ضرورة تطوير ثقافة الحاسب الآلي في وسط رجال الأمن لإنجاح عمل الأجهزة الأمنية ومواكبة ظاهرة الإجرام المعلوماتي[2].

[1]– الشمري غانم مرضي ، مرجع سابق، ص 174.

[2]– حجازي عبد الفتاح بيومي ، مرجع سابق، ص ص 109 – 110.

ثانيا: الإشكالات المتعلقة بجمع الأدلة الخاصة بإدانة الجاني

يتضح من خلال مراحل التفتيش وإجراءاته أن الغاية من كل ذلك هو الوصول إلى رصد الدليل على قيام جرائم الانترنت، ومعرفة المجرم المعلوماتي وتقديمه للمحاكمة غير أن الطابع الفني لهذه الجرائم يجعل الأمر أكثر تعقيداً، ويستخلص بالنسبة للمشرع الجزائري المبادرة إلى مواكبة التطور القانوني على المستوى الدولي تماشياً مع التطور التكنولوجي بتمهيده للطريق أمام استخلاص الدليل الالكتروني في القانون رقم 09 – 04 المتضمن تعديل قانون العقوبات، بالنص في م6 منه على حجز المعطيات المعلوماتية وذلك بإفراغها أو نسخها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحراز[1].

تظل السلطات المكلفة بالتفتيش تواجه صعوبات، نظراً لكون التخزين الالكتروني للبيانات أو تشفيرها يجعلها بمنأى عن وضع اليد على الدليل المستخلص منها، هذا فضلا عما قد تثيره مشكلة تخزين المعلومات عن طريق جهاز مرتبط بالخارج وبواسطة شبكة الاتصال عن بعد، وما يترتب على ذلك من المساس بسيادة الدول، ومهما تكن الضرورة التي قد تحيط بإجراءات المتابعة الجزائية إلا أن استخلاص الدليل لا يكون بشكل مخالف للقانون أو المبادئ الدستورية التي تكفل حماية خاصة للحريات الأساسية[2].

[1]– أنظر م6 من القانون رقم 09 – 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

[2]– زبيخة زيدان، مرجع سابق، ص 172.

خاتمــة

يتضح لنا من خلال دراستنا لموضوع الحماية الجنائية من جرائم الانترنت في القانون الجزائري، أن هذه الجرائم قد غيرت النظرة التقليدية التي كان ينظر بها إلى الجريمة، فهذا النوع من الجرائم أبرزت مفهوماً جديداً لم يكن يعرفه القانون، كونها تتمتع بخصوصية تميزها عن الجرائم التقليدية.

تكمن أول خصوصية تميز هذه الجرائم في صعوبة وضع تعريف موحد لها، فقد اختلفت هذه التعاريف في إعطاء وصف لهذه الظاهرة الاجرامية، فمنها من ركز على الجانب الموضوعي وآخر كونها وسيلة لارتكاب الجريمة بشكل عام، وهو ما يشكل عائق أمام التشريعات لتوحيد القواعد الخاصة بمكافحتها، لذا لابد من إعطاء تعريف جامع ومانع لهذه الجرائم يتم صياغته بشكل يشمل كل مظاهر السلوك الإجرامي الخاص بمنظومة الخاصة بالمعالجة الآلية للمعطيات، لاسيما وأنها ترتكب في عالم افتراضي غير ملموس وتتجاوز عناصر ارتكابها إقليم الدولة الواحدة مما يجعلها من مصف الجرائم العابرة للحدود.

تتمتع كغيرها من الجرائم التقليدية بأركان ثلاث، إلا أنها محاطة بمجموعة من الصعوبات من حيث تحديدها لاسيما ما يتعلق بالركنين المادي والمعنوي للجريمة، إذ غالبا ما تجد السلطات المختصة صعوبة في تحديد الجاني ومكان ارتكاب الجريمة، كما تشمل هذه الصعوبة كذلك مسألة إثبات القصد الجنائي لدى مرتكبيها، لذا يتعين على الدول وضع تقنيات موازية لجرائم الانترنت من حيث الوسائل والتقنيات التي تساهم في الوصول إلى أدلة ارتكابها وملاحقة مرتكبيها، خاصة وأن هناك العديد من الدوافع التي تجعلهم يلجؤون إلى ممارسة مثل هذا النشاط الإجرامي، إذ أن القصد الجنائي يتراوح بين الثبوت والنفي بحسب الدافع والنتيجة المراد تحقيقها منه.

يتبين من خلال دراستنا أن جرائم الانترنت ولكونها من الجرائم المستحدثة، تعرف أشكال متعددة، حاولنا إبراز أكثرها شيوعاً والمرتبطة بشكل وثيق بالاستخدام التكنولوجي سواءً كوسيلة لارتكابها كجرائم غسل الأموال والتزوير، أو كجريمة قائمة بذاتها تستهدف في معظمها الحسابات الالكترونية والبيانات المخزنة في أجهزة الحاسوب، وبالنظر إلى هذا الطابع المزدوج في التكييف لابد من تدعيم هذه الخاصية بنصوص قانونية أكثر فعالية لاحتواء جميع الصور الخاصة بهذه الجرائم.

جعلت الخصوصية التي تتميز بها جرائم الانترنت مختلف التشريعات في تدارك مدى خطورتها، ومدى التحديات التي تفرضها عليها مما أدى بها إلى المسارعة من أجل وضع طرق ناجعة وفعالة لمكافحتها، ولقد تمثلت هذه الوقاية أولاً في وضع وسائل الحماية الخصوصية للمعلومات حيث سارعت الدول في نشر الوعي بهذه الوسائل التي نذكر اعتماد سياسة الترميز من خلال وضع كلمات سر خاصة بالأنظمة الالكترونية والتشفير اللذان يساهمان بشكل كبير في تفعيل الدور الحمائي الوقائي لهذه الوسائل.

سعى المشرع الجزائري إلى تدعيم وسائل الحماية الفنية هيكليا من خلال إنشاء هيئة وطنية تتولى مهمة الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام، في حين تم إضافة قسم إضافي لقانون العقوبات يتضمن تجريم الأفعال الماسة بالأنظمة المتصلة بتكنولوجيات الإعلام والاتصال سنة 2004، ليتم تتويج العمل التشريعي بإنجاز آخر سنة 2009 بموجب القانون رقم 09 – 04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ليسد بذلك المشرع الجزائر فراغاً قانونياً كانت تعاني منه الجزائر في هذا المجال.

اصطدمت محاولات التصدي لجرائم الانترنت، بالعديد من الإشكالات لاسيما في مرحلة المتابعة الجزائية، خاصة في مرحلة التفتيش والتحري، وهو ما يدفعنا إلى ضرورة القول بأن الجزائر لا تزال تعاني نقصاً من حيث الخبرة الفنية التي تمكنها من مواجهة هذه الجرائم لاسيما وأنها قد تشكل خطراً حقيقياً يهدد أمنها الوطني واستقرارها السياسي، لذا لابد من تكثيف الجهود وتسخير الإمكانيات المادية والبشرية من أجل تطوير أجهزة الأمن وإخضاع رجال الضبطية القضائية لدورات تكوينية خاصة بمجال تكنولوجيا المعلومات، وضرورة إنشاء مراكز توعية للشباب من أجل الحد من مظاهر النشاط الإجرامي لدى هذه الفئة التي غالباً ما تلجأ إلى مثل هذا السلوك الإجرامي من باب الفضول وإرضاءً لغرور التفوق، الذي وان انتفعت معه كل بوادر للقصد الجنائي لدى مرتكبها إلا أنها تعود بآثار وخيمة على الأمن الداخلي للدول لاسيما في المجال الاقتصادي والاجتماعي والسياسي.

يتبين لنا أخيراً أن شبكة الانترنت ساهمت ولا تزال تساهم بشكل كبير في انتشار هذا النوع من الجرائم، الأمر الذي يستدعي استحداث قوانين موضوعية وأخرى إجرائية موحدة، تخضع لها جميع الدول، وفرض الرقابة المتبادلة على النشاطات التي تتزامن مع اتصال الأجهزة الالكترونية بهذه الشبكة، من أجل القضاء على كل مظاهر الإجرام الناتج عن استخدامها.

قائمة المصادر والمراجع

I. المصادر

- القرآن الكريم

II. المراجع

أولا: الكتب

1. الشمري غانم مرضي، الجرائم المعلوماتية، الدار العلمية الدولية للنشر والتوزيع، الطبعة الأولى، عمان، 2016.
2. حجازي عبد الفتاح بيومي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الفكر الجامعي، مصر، 2006.
3. حجازي محمد، جرائم الحاسبات والانترنت – الجرائم المعلوماتية، المركز المصري للمملكة الفكرية، مصر، 2005..
4. زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للنشر والتوزيع، الجزائر، 2011.
5. سعد عبد العزيز العاتي و علاء حسين الحمامي، تكنولوجيا الأمنية للمعلومات وأنظمة الحماية، الطبعة الأولى، دار وائل للنشر، عمان، 2007.
6. سياب حكيم، الإعلام الآلي والقانون، الطبعة الأولى، دار وائل للنشر والتوزيع، عمان، 2014.
7. قنديل أشرف عبد القادر، الإثبات الجنائي في الجريمة الالكترونية، دار الجامعة الجديدة للنشر، الاسكندرية، 2015.

8. مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت بين القانون الدولي الاتفاقي والقانون الوطني، الطبعة الأولى، مركز الدراسات العربية للنشر والتوزيع، مصر، 2016.

9. ناني لحسن، التحقيق في الجرائم المتصلة بتكنولوجية المعلوماتية بين النصوص التشريعية والخصوصية التقنية، النشر الجامعي الجديد للطباعة والنشر والتوزيع، الجزائر، 2017.

ثانيا: الرسائل و المذكرات الجامعية

أ) الرسائل

1. حابت آمال، التجارة الالكترونية في الجزائر، رسالة لنيل شهادة دكتوراه في العلوم، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2015.

2. حفصي عباس، جرائم التزوير الالكترونية، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في العلوم الإسلامية، تخصص شريعة وقانون، كلية العلوم الإنسانية والعلوم الإسلامية، جامعة وهران 1 أحمد بن بلة، 2015.

3. ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه العلوم، تخصص: قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة1، 2016.

ب)المذكرات

1) مذكرات الماجستير

1. **أحمد مسعود مريم**، آليات مكافحة تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 09 – 04، مذكرة لنيل شهادة الماجستير، تخصص: قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2013.
2. **دردور نسيم**، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير، تخصص القانون الجنائي، كلية الحقوق، جامعة منتوري، قسنطينة، 2013.
3. **رصاع فتيحة**، الحماية الجنائية للمعلومات على شبكة الانترنت، مذكرة لنيل شهادة ماجستير في القانون العام، كلية الحقوق والعلوم السياسية، جامعة تلمسان، 2012.
4. **سوير سفيان**، الجرائم المعلوماتية، مذكرة لنيل شهادة ماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2011.
5. **صغير يوسف**، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013.
6. **عبد الله دغش العجمي**، المشكلات العملية والقانونية للجرائم الالكترونية – دراسة مقارنة، رسالة لنيل شهادة ماجستير في القانون العام، جامعة الشرق الأوسط، الكويت، 2014.
7. **لاروش راضية**، أمن التوقيع الالكتروني، مذكرة لنيل شهادة الماجستير في القانون، فرع القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012.

8. **وافد يوسف**، النظام القانوني للدفع الالكتروني، مذكرة لنيل درجة ماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2011.

2) مذكرات الماستر

1. **بعرة سعيدة**، الجريمة الالكترونية في التشريع الجزائري – دراسة مقارنة، مذكرة لنيل شهادة ماستر، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2016.
2. **جواحي عبد الستار**، جرائم الحاسوب – دراسة مقارنة بين الشريعة الإسلامية والقانون الجزائري، مذكرة لنيل شهادة الماستر في العلوم الإسلامية، كلية العلوم الاجتماعية والإنسانية، جامعة السعيد حمه لخضر، الوادي، 2015.

ثالثا: المقالات

1. **بوشكيوه عبد الحليم**، "آليات مكافحة الجرائم الماسة بالأخلاق والآداب العامة على الانترنت"، مجلة دراسات وأبحاث، العدد الأول، جامعة زيان عاشور، الجلفة، 2009، (ص ص 08 – 33).
2. **بونعارة ياسمينة**، "الجريمة الالكترونية"، مجلة المعيار، كلية أصول الدين، جامعة الأمير عبد القادر، قسنطينة، 2015، (ص ص 01 – 30).
3. **حامدي محمد الصالح**، "علاقة تكنولوجيا المعلومات بظاهرة الاتجار بالبشر في عصر العولمة ومدى تأثيرها على دولة قطر"، المجلة العربية الدولية للمعلوماتية، المجلد الأول، العدد الثاني، معهد الملك سلمان للدراسات والخدمات الاستشارية، جامعة المجمعة، السعودية، 2012، (ص ص 01 – 18)

4. **حديد نوفيل وبوزيد هجيرة سومية،** "نجاح مشروع الحكومة الالكترونية اجتناب الفشل من خلال إدراك المخاطر الالكترونية"، مجلة علوم الاقتصاد والتسيير والتجارة، العدد 31، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة الجزائر3، 2015،(ص ص 193 – 210).
5. **حشاشي أمينة،** "ماهية الجريمة المعلوماتية"، مجلة دراسات وأبحاث، المجلد الأول، العدد الأول، جامعة زيان عاشور، جلفة، 2009، (ص ص 450 – 458).
6. **حمودي ناصر،** "الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري"، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 02، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، بجاية، 2016، (ص ص 67 91).
7. **خليفة محمد،** "خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها"، مجلة دراسات وأبحاث، العدد الأول، جامعة زيان عاشور، جلفة، 2009، (ص ص 370 – 389).
8. **دريس نبيل،** "الجريمة السيبرانية بين المفاهيم والنصوص التشريعية الجزائر أنموذجا"، مجلة القانون والمجتمع، المجلد 5، العدد 2، جامعة أدرار، 2017، (ص ص 20 – 40).
9. **سحتوت نادية،** "التنظيم القانوني للجريمة المعلوماتية أدلة إثبات الجريمة المعلوماتية"، مجلة دراسات وأبحاث، المجلد الأول، العدد الأول، جامعة زيان عاشور، الجلفة، 2009، (ص ص 48 – 54).
10. **شعبان سمير،** "الجريمة الالكترونية مقاربة تحليلية لتحديد مفهوم الجريمة والمجرم"، مجلة دراسات وأبحاث، المجلد الأول، العدد الأول، جامعة زيان عاشور، الجلفة، 2009، (ص ص 114 – 132).

11. **عباوي نجاة،** "الإشكالات القانونية في تجريم الاعتداء على أنظمة المعلومات"، دفاتر السياسة والقانون، العدد 16، جامعة قاصدي مرباح، ورقلة، جانفي 2017، (ص ص 279 – 292).

12. **عثمان طارق،** "حماية الأطفال من الاستغلال في المواد الإباحية عبر الانترنت في التشريع الجزائري"، مجلة المفكر، العدد 13، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2016، (ص ص 417 – 448).

13. **عدنان سوزان،** انتهاك حرمة الحياة الخاصة عبر الانترنت – دراسة مقارنة، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 29، العدد الثالث، كلية الحقوق، جامعة دمشق، 2013، (ص ص 421 – 455).

14. **فشار عطاء الله،** "مواجهة الجريمة المعلوماتية في التشريع الجزائري"، مجلة دراسات وأبحاث، المجلد الأول، العدد الأول، جامعة زيان عاشور، جلفة، 2009.، ص ص 489 – 490، (ص ص 459 – 512).

15. **لطرش فيروز وبن عزوز حاتم،** "الجريمة الالكترونية في الجزائر: من جريمة فردية إلى جريمة منظمة"، مجلة آفاق للعلوم، مجلة دولية محكمة للعلوم الإنسانية والاجتماعية والاقتصادية، العدد الأول، جامعة الجلفة، 2016، (ص ص 323 – 335).

16. **مكاري نزيهة،** "إثبات جرائم الاعتداء على حق المؤلف عبر الانترنت في التشريع الجزائري (دراسة مقارنة)"، مجلة العلوم الاقتصادية وعلوم التسيير، العدد 9، معهد علوم التسيير والاقتصاد، المركز الجامعي برج بوعريريج، 2009، (ص ص 123 – 145).

رابعا: المداخلات

1. **البداينة ذياب موسى**، الجرائم الالكترونية المفهوم والأسباب، ملتقى علمي بعنوان "الجرائم المستحدثة في ظل التغيرات والتحولات الاقليمية والدولية"، كلية الشرطة للعلوم الاستراتيجية، وزارة الداخلية، قطر، 2014، (ص ص 01 – 18).
2. **بن صويلح آمال**، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الالكتروني بالجزائر، مداخلة مقدمة في الملتقى الدولي الثالث حول "الإجرام السيبراني المفاهيم والتحديات"، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي، برج بوعريريج، يومي 11 و12 أفريل 2017، (ص ص 01 – 11).
3. **بوزيدي مختارية**، ماهية الجريمة الالكترونية، مداخلة مقدمة في الملتقى الوطني المعنون بـ "آليات مكافحة الجرائم الالكترونية في التشريع الجزائري"، الجزائر، مركز جيل البحث العلمي، 29 مارس 2017، (ص ص 07 – 22).

خامسا: النصوص القانونية

أ) النصوص التشريعية:

1) التشريع الأساسي:

- مرسوم رئاسي رقم 96 – 438 مؤرخ في 7 ديسمبر 1996، يتضمن الدستور المصادق عليه في استفتاء 28 نوفمبر 1996، ج ر العدد 76 صادر في 8 ديسمبر 1996، المعدل والمتمم بموجب القانون رقم 02 – 03 مؤرخ في 10 أفريل 2004 ج ر عدد 25 صادر بتاريخ 14 أفريل 2002، المعدل والمتمم بموجب القانون رقم 08 – 09 في 15 نوفمبر 2008 ج ر العدد 63 صادر بتاريخ 16

نوفمبر 2008، المعدل والمتمم بموجب القانون رقم 16 – 01 المؤرخ في 06 مارس 2016 ج ر عدد 14 صادر في 07 مارس 2017.

2) التشريع العادي:

- الأمر رقم 66 – 156 المؤرخ في 08 جوان 1966، يتضمن قانون العقوبات، المعدل والمتمم بـ المعدل والمتمم بالقانون رقم 04 – 15 المؤرخ في 10 نوفمبر 2004، ج ر عدد 71 صادر بتاريخ 10 نوفمبر 2004.
- قانون رقم 09 – 04 المؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 47 صادر بتاريخ 16 أوت 2009.

ب)النصوص التنظيمية:

- مرسوم رئاسي رقم 15 – 261 مؤرخ في 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر العدد 53 صادر بتاريخ 08 أكتوبر 2015.

فهرس الموضوعات