الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي
جامعة أكلي محند أولحاج
-البويرة-

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique
Université Akli Mohand Oulhadj - Bouira -
Tasdawit Akli Muḥend Ulḥağ - Tubirett -

جامعة البويرة

كلية الحقوق والعلوم السياسية
قسم القانون العام

آليات مكافحة الجريمة المعلوماتية في التشريع الجزائري

مذكـرة لنيـل شهـادة المـاستـر في القـانـون
تخصص: قانون جنائي وعلوم جنائية

إعداد الطـالبـة:
غـربـي جميلة

إشـراف الأستـاذ :
د. خليفي سمير

أعضـاء لجـنـة المنـاقشة:

الأستـاذ(ة):..... رئيسًا

الأستـاذ:خليفي سمير.....مشرفًا ومقررًا

الأستـاذ(ة) :.....ممتحنا

السنة الجامعية 2020/ 2021

شكـر وعــرفـان

الحمد لله والصلاة والسلام على رسول الله القائل : (من لم يشكر الناس لم يشكر الله)

فالشكر لله الذي منّ علينـا ويسر لنا إتمام هذا البحث وندعـوه أن يجعل فيه النفع والفائدة

أمــا بــعـد

نتقدم بخالص الشكر والعرفان والإمتنان للأستاذ الدكتور خليفي سمير الذي تفضل بالإشراف على هذا البحث وكان لإهتمامه وتوجيهاته بالغ الأثر في إتمامه على ما هو عليه ولا يسعنا في هذا المقام إلا أن نسأل الله تعالى أن يجزيه الفردوس الأعلى ويرزقه صحبة الرسول صلى الله عليه وسلم وكل ما يتمنى في الدنيا والآخرة.

الشكر موصول كذلك للأساتذة الأفاضل أعضاء لجنة المناقشة الآتية أسمائهم :

الأستاذ ..... رئيسا

الأستاذ ..... عضوا

على ما تكرموا به من ملاحظات قيمة .

كما نتقدم بالشكرالجزيل إلى كل من شجعنا وساندنا وقدم لنا العون والمساعدة والنصح والمشورة وساهم في إخراج هذا العمل إلى النور ونسأل الله أن يجعل ذلك في ميزان حسناتهم
ويجزيهم عنا كل خير وأن يجعل هذا العمل خالص لوجهه سبحانه إنه سميع مجيب الدعاء .
وآخر دعوانا أن الحمد لله رب العالمين والصلاة والسلام على أشرف الأنبياء والمرسلين سيدنا محمد وصحبه أجمعين.

مختصـــرات

أولا : مختصرات باللغة العربية

ق.ع.....قانون العقوبات.

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

ص..... صفحة.

ج.ر.....الجريدة الرسمية.

ط .....طبعة.

مقدمة:

شهد القرن العشرين تطورا هائلا في مجال الاتصال واصبحت الشبكة المعلوماتية الدولية (الانترنت) من عجائب القرن العشرين التي امتدت عبر كامل انحاء المعمورة وربطت بين شعوبها، فأصبحت وسيلة التعامل اليومي بين أفراد مختلف الطبقات والمجتمعات.

يعيش العالم اليوم أزهى عصوره العلمية والتكنولوجية، والتي يعود الفضل فيها للثورة المعلوماتية، التي حققت طفرة ملحوظة في مستويات التقدم التقني والعلمي شملت معظم نواحي الحياة، خاصة التطور الهائل في مجالات الاتصالات وأنظمة المعلومات، وأضحى العصر عصر المعلومات بإمتياز.

ولقد وفرت هذه التقنيات العديد من الميزات سرعت من وتيرة تبادل السندات والمعلومات والبيانات في أوقات جد قياسية، كما مكنت المتعاملين في حقل تكنولوجيا المعلوماتية من تخزين واعادة استرجاع كميات هائلة من المعلومات في مدة قصيرة، وبذلك أصبحت مكنة في يد من يستطيع التحكم بها ومصدر قوة.

ومقابل تباين الذهنيات والمستويات العلمية لمستعملي شبكة الانترنت ظهرت ممارسات غير مشروعة، فأصبحت هذه الشبكة أداة ارتكابها أو محلا لها حسب الحالة، مما أدى إلى ظهور طائفة جديدة من الجرائم مختلفة عن باقي الجرائم التقليدية، وقد سميت بالجرائم المعلوماتية.

وهي جرائم مبتكرة ومستحدثة تمثل ضربا من ضروب الذكاء الإجرامي، تطورت وتنامت بسرعة في ظل العولمة، بما أدى إلى استخدام شبكة الانترنت في تنفيذ العديد من الجرائم فأصبحت الجريمة تتم وتنظم إلكترونيا، مما أضفى على هذا النمط من الجرائم سمة التعقيد وصعوبة السيطرة والملاحقة القانونية والإجرائية، وبالتالي استعصى إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية وحتى الأجنبية،وأسفر عن الكثير من المشكلات القانونية.ما أوجب تطوير البنية التشريعية الجنائية الوطنية بذكاء تشريعي مماثل تعكس فيه الدقة الواجبة على المستوى القانوني وسائر جوانب وأبعاد تلك التقنيات الجديدة، بما يضمن في الأحوال كافة احترام مبدأ الشرعية من ناحية، وضرورة التكامل في الدور والهدف مع المعاهدات الدولية من ناحية اخرى.

كل هذا جعل المشرع الجزائري مضطرا لمتابعة هذه المستجدات والتعامل معها من خلال التدخل التشريعي لمكافحة هذا النوع الخطير من الجرائم من أجل الحفاظ على مصالح الفرد والدولة، فعمل على تنقيح قوانينه الداخلية وسن قوانين لتستجيب والتحولات الراهنة لمكافحة هذه الجريمة من خلال القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 المتضمن تعديل قانون العقوبات[1]، والقانون رقم 04/09 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها[2]. بالاضافة الى نصوص اخرى نجد أثرها في قانون الاجراءات الجزائية، وكذلك سن نصوص جديدة وخاصة تتعلق بهذا النوع من الاجرام رغبة منه في تأمين أنظمة المعلومات من اعتداءات المجرمين.

بناء على ما تقدم، تتجلى أهمية موضوع الجرائم المعلوماتية في الانتشار الواسع لهذا النوع من الجرائم، فقد أصبحت الجريمة المعلوماتية متلازمة مع التطور السريع والهائل في مجال تكنولوجيا الاتصالات والمعلومات، فنتيجة للتقدم الكبير في استخدامات الشبكة العنكبوتية، طفت الجريمة المعلوماتية بأشكالها المختلفة، وأصبحت تهدد الأمن المعلوماتي للأفراد، المؤسسات والحكومات.

كما أن هذه الجرائم المعلوماتية حديثة النشأة ويمتد تاثيرها إلى جميع الأصعدة لارتباطها بتطور تكنولوجيا الاعلام والاتصال والتي تستخدم في جميع مجالات الحياة سواء من طرف الافراد او المؤسسات، حيث بلغ الضرر درجة لا يمكن تجاهلها واصبحت ظاهرة معروفة دعت على إثرها العديد من الدول الى سن قوانين وتشريعات لمكافحة هذه الجرائم.

ولعل اهم الاسباب التي دفعتني للخوض في هذا الموضوع حداثة الموضوع ومحاولة جمع شتات الموضوع عبر التقصي في التشريع الداخلي عن العناصر ذات الصلة، ورغبتي الخاصة في الكتابة فيه خصوصا لما لمسته من مستجدات كثيرة واشكالات افرزها الواقع العملي.

وتهدف دراسة هذا الموضوع إلى تسليط الضوء على ظاهرة اجرامية يزداد انتشارها بمعدلات قياسية مع الانتشار الهائل لاستعمال جهاز الكومبيوتر والاستعمال المتزايد لشبكة

---

[1] القانون رقم 04-15 المؤرخ في 2004/11/10 المعدل والمتمم للامر رقم 156/66 المؤرخ في 1966/06/08، المتضمن قانون العقوبات، ج ر، العدد 71، الصادرة في 2004/11/10.

[2] القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، جر، العدد 47، الصادرة في 16 أوت 2009.

الانترنت،ومحاولة الكشف عن الأساليب الحديثة والمبتكرة في ارتكاب الجريمة من خلال استعراض مجموعة من الجرائم الأكثر انتشارا، ومعرفة موقف المشرع الجزائري في تصديه لهذه الظاهرة باعتبارها شكلا من أشكال الجريمة المنظمة.

تأسيسا على ما تقدم يمكن بلورة الإشكالية الأساسية للموضوع في:مدى فعالية الآليات القانونية الموضوعية والاجرائية الذي خصه المشرع الجزائري لمكافحة الجريمة المعلوماتية والحد منها؟

وللاجابة على هذه الإشكالية إتبعنا المنهج التحليلي خاصة لاستنباط الاحكام المختلفة التي تحكم هذه الحماية، وذلك دون الاستغناء عن المذهب الوصفي إذا اقتضت الضرورة ذلك.

وقمنا بتقسيم هذا البحث إلى فصلين، الفصل الأول نتناول فيه الإطار المفاهيمي للجريمة المعلوماتية، الذي يتضمن مبحثين حيث نتناول في المبحث الاول ماهية الجريمة المعلوماتية وفي المبحث الثاني نتعرض فيه إلى المجرم المعلوماتي.

أما الفصل الثاني نعالج فيه سبل مواجهة الجريمة المعلوماتية في التشريع الجزائري، ويحتوي على مبحثين، حيث نتناول في المبحث الاول المواجهة الموضوعية للجريمة المعلوماتية، وفي المبحث الثاني نتطرق إلى المواجهة الإجرائية للجريمة المعلوماتية.

وفي الأخير نصل إلى خاتمة ندرج فيها النتائج المتوصل إليها من خلال هذا البحث متبوعة ببعض الإقتراحات والتوصيات.

الفصل الأول:
الإطار المفاهيمي للجريمة المعلوماتية

في ظل عصر السرعة وثورة التكنولوجيا لا يستطيع أحد أن ينكر أهمية الانترنت، أحد أهم دعائم تكنولوجيا الاتصال والمعلومات. ولكن هناك على الجانب الأخر أثار سلبية من أهمها ظهور نوع جديد من الجرائم يدعى بجرائم المعلوماتية، تعتبر الجريمة المعلوماتية كظاهرة تضرب في عمق المجتمع وتدمره في وضع يتميز بالهدوء والسكينة.

لحداثة هذه الجريمة فقد كانت هناك عدة اتجاهات مختلفة في تعريفها،كما انها اتسمت بمجموعة من الخصائص والسمات التي ميزتها عن غيرها من الجرائم الأخرى،كما افرزت معها طائفة جديدة من المجرمين اصطلح على تسميتهم بمجرمي المعلوماتية،والمجرم المعلوماتي ليس كأي مجرم متخصص ومحترف.

وعليه سوف نتناول في هذا الفصل تعريف الجريمة المعلوماتية وأهم الخصائص التي تميز الجريمة المعلوماتية عن باقي الجرائم في (المبحث الأول)، كما سنتطرق الى دراسة أركان وتصنيفات الجريمة المعلوماتية والمجرم المعلوماتي من حيث صفاته ودوافعه في (المبحث الثاني).

المبحث الاول:
ماهية الجريمة المعلوماتية

ان التطور التكنولوجي الرهيب الذي شهده العالم في السنوات الأخيرة افرز لنا العديد من الجرائم بما فيها الجريمة المعلوماتية، موضوع هذه الدراسة خصوصا على الصعيد المالي و الاقتصادي، فالجرائم المستحدثة والتي ظهرت في عصرنا الحديث، والسبب يعود الى ارتباط هذه الجرائم بوسائل التقنيات الحديثة من أجهزة كمبيوتر وشبكات الانترنت والمواقع الالكترونية، وتعد الأنترنت من أكبر شبكات الكمبيوتر ذات الاتصال الوثيق بالجرائم المعلوماتية، حيث يستطيع المجرمون العصريون ارتكاب أبشع الجرائم ليس فقط دون إراقة دماء، ولكن أيضا دون الانتقال من أماكنهم، بل ترتكب الجريمة في أمن وهدوء، وهو ما جعل البعض يصفها "الجريمة الناعمة"، فبمجرد لمس لوحة المفاتيح يحدث دمارا وخرابا في

اقتصاديات كبرى الشركات، وهذا النوع من الجرائم أصبح مشكلة عالمية وليس مقصورا على منطقة، أو دولة معينة.

فهي تنشأ في العالم الإفتراضي الذي يعتبر أرض خصبة لمن يتحكم فيها، فلم تعد الحدود عائقا على انتشارها مادام تتم في هذا المجال الذي يجعل العالم قرية صغيرة، وبالتالي تسهيل عملية الاختراق والاعتداء على المعلومات والبيانات في الشكل الإلكتروني.

وعليه، سوف يتم الحديث من خلال هذا المبحث عن مفهوم الجريمة المعلوماتية وخائصها في (المطلب الاول)، ليتسنى لنا الحديث عن أركان الجريمة المعلوماتية وتصنيفاتها في (المطلب الثاني).

المطلب الأول:
مفهوم الجريمة المعلوماتية

لقد فتح اختراع الحاسب الالي الأفاق أمام الفكر الإنساني وأدى إلى إحداث الثورة التي يعيشها العالم اليوم.

إن المعلوماتية أو ما يسمى أيضا بعلم المعلومات، هو ذلك العلم الذي يهتم بالموضوعات والمعارف المتصلة بأصل المعلومات وتجميعها وتنظيمها وتخزينها واسترجاعها وتغيرها وكذا تحويلها واستخدامها.كما يهتم هذا العلم بدراسة أساليب معالجة المعلومات كالأنظمة المعلوماتية ونظم المبرمجة، وبهذا المفهوم تعتبر المعلوماتية علما متصلا بالعديد من العلوم الأخرى.

كما عرفها أخر بأنها:"عمل غير قانوني منظم لنسخ أو تغيير أوحذف أو الوصول إلى المعلومات المخزونة داخل الكمبيوتر أو التي تحول عن طريقه، وهي جريمة من أنماط الجرائم المعروفة في قانون العقوبات والتي ينال القائم بها عقوبة تتناسب مع مستوى الفعل الإجرامي الغير مشروع.

الفرع الأول: تعريف الجريمة المعلوماتية

في البداية نشير إلى أنه لا يوجد اتفاق على مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها، فالبعض يطلق عليها جريمة الغش

المعلوماتي، والبعض الأخر يطلق عليها جريمة الاختلاس المعلوماتي أو الاحتيال المعلوماتي، واخرون يفضلون تسميتها بالجريمة المعلوماتية.

لقد اختلف الفقهاء حول وضع تعريف موحد للجريمة المعلوماتية ويعود ذلك للاختلاف حول تحديد نطاق هذه الجريمة، فالبعض ينظر إليها بمفهوم ضيق (أولا)، والبعض الأخر ينظر إليها بمفهوم موسع (ثانيا).

أولا: التعاريف المضيقة للجريمة المعلوماتية

انطلق أنصار التعريف الضيق للجريمة المعلوماتية من النقطة المتعلقة بضرورة تحديد العلاقة بين المعلوماتية والأفعال غير المشروعة لتحديد ما إذا كانت تلك الأفعال تدخل في نطاق الجريمة المعلوماتية أم لا.

من التعريفات المضيقة لمفهوم الجريمة المعلوماتية تعريفها على أنها:" كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية ولملاحقاته وتحقيقه من ناحية أخرى"[3].

وحسب هذا التعريف يجب أن تتوافر معرفة كبيرة بتقنيات الحاسوب ليس فقط لارتكاب الجريمة بل كذلك لملاحقتها والتحقيق فيها، وهذا التعريف يضيق بدرجة كبيرة من الجريمة المعلوماتية.

كذلك تعرف الجريمة بأنها:" الفعل غير المشروع الذي يتورط في ارتكابه الحاسب، أو هي الفعل الإجرامي الذي يستخدم في اقترافه الحاسوب باعتباره أداة رئيسية".

وعرفت أيضا بأنها:" الجرائم التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دورا هاما، أو هي كل فعل إجرامي يستخدم الحاسب الالي في ارتكابه كأداة رئيسية"[4].

---

[3] نائلة عادل محمد فريد قورة، جرائم الحاسب الالي الاقتصادية دراسة نظرية وتطبيقية، ط1، منشورات الحلبي الحقوقية،بيروت، 2005، ص 21.

[4] ونوغي نبيل، زيوش عبد الرؤوف، الجريمة المعلوماتية في التشريع الجزائري، مجلة العلوم القانونية والإجتماعية، المجلد الرابع، العدد الثالث، جامعة زيان عاشور بالجلفة –الجزائر،سبتمبر 2019، ص 130.

ويعرف جانب آخر من الفقه المعلوماتية بالنظر إلى نتيجة الإعتداء، إذ يرى الفقيه الفرنسي "mass" بأنها:" الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح".

كذلك عرفها الأستاذ "Rosenblatt" إلى تعريفها أنها:" نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزونة داخل الحاسوب أو تغييرها أو حذفها أو الوصول أو التي تحول عن طريقه"[5].

من خلال التعريفات السابقة للجريمة المعلوماتية نلاحظ أنها قاصرة عن الإحاطة بأوجه ظاهرة الإجرام المعلوماتي إذ ركز البعض على موضوع الجريمة، وركز البعض الآخر على وسيلة ارتكبها بينما ركز آخرون على فاعل الجريمة، بينما نرى أن الجريمة قد تقع على الحاسب الآلي بشقيه المادي والمعنوي ممثلا بالكيان المنطقي بالاعتداء على البيانات المخزنة والمتبادلة بين الحاسب الآلي وشبكاته الخاصة والعامة، عبر خطوط قنوات الاتصال.

ثانيا: التعاريف الموسعة للجريمة المعلوماتية

على عكس الاتجاه السابق، فإن هناك تعريفات حاولت التوسع في مفهوم الجريمة المعلوماتية نتيجة الانتقادات التي واجهت الإتجاه الأول، فأنصار هذا الاتجاه يرى من الضروري التوسع من مفهوم الجريمة المعلوماتية، لتفادي أوجه القصور التي شابت تعريفات الاتجاه المضيق للتصدي لظاهرة الإجرام المعلوماتي.

فعرفها البعض أنها:" كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الاعتداء على الأموال المادية أو الأشياء المعنوية". وبأنها:" مل سلوك سلبي أم إيجابي يتم بموجبه الاعتداء على البرامج أو المعلومات للإستفادة منها بأية صورة كانت"[6].

كما تمتد هذه الجريمة لتشمل الإعتداءات المادية، سواء كان هذا الإعتداء على جهاز الحاسوب ذاته، أو المعدات المتصلة به، وكذلك الاستخدام غير المشروع لبطاقات الإئتمان، وانتهاك ماكينات الحسابات الآلية، بما يتضمنه من شبكات تكويل الحسابات المالية بطريقة

[5] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الاردن، 2010، ص 48.

[6] نفس المرجع، ص 49.

إلكترونية، وتزييف المكونات المادية والمعنوية للحاسوب، بل وسرقة الحاسوب في حد ذاته أو مكون من مكوناته.

وقد عرفت الجريمة المعلوماتية في إطار المنظمات الأوروبية للتعاون والتنمية الاقتصادية بأنها:" كل فعل أو امتناع من شأنه أن يؤدي إلى الاعتداء على الأموال المادية أو المعنوية، يكون ناتجا بطريقة مباشرة عن تدخل التقنية المعلوماتية الإلكترونية"[7].

وحديثا تبنى مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين تعريفا جامعا لجرائم الحاسب الآلي وشبكاته حيث عرف الجريمة المعلوماتية بأنها:" أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"[8]. ويلاحظ في هذا التعريف أنه لا يقتصر على جرائم الكمبيوتر والانترنت، ذلك أن المعالجة الآلية للبيانات تمتد لتشمل كل ما يمكن القيان به عن طريق الاتصالات السلكية واللاسلكية، بما في ذلك الهاتف الأرضي والمحمول.

فمن خلال هذه التعريفات تبين لنا أن هذا الاتجاه يوسع من مفهوم الجريمة المعلوماتية حيث أن مجرد مشاركة الحاسب الالي في السلوك الإجرامي يضفي عليه وصف الجريمة المعلوماتية.

أما بخصوص التعريفات التشريعية، قدم نظام مكافحة جرائم المعلوماتية للملكة العربية السعودية الصادر بتاريخ 2007/03/26 تعريفا مباشرا للجريمة المعلوماتية، حيث جاء في المادة الأولى فقرة 8 بأنها:" أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام". وكذلك عرفت المادة الأولى من القانون النموذجي الموحد في شأن مكافحة سوء استخدام تكنولوجيا المعلومات والإتصالات المصري، الجريمة المعلوماتية كما يلي:" كل فعل مؤثم يتم ارتكابه عبر أي وسيط إلكتروني، ويقصد في تطبيق أحكام هذا القانون بالكلمات والعبارات الآتية، المعنى المبينة قرين كل منها الوسيط الإلكتروني..."[9].

---

[7] ونوغي نبيل، زيوش عبد الرؤوف، مرجع سابق، ص 131.

[8] نهلا عبد القادر المومني، مرجع سابق، ص 50.

[9] حوالف عبد الصمد، رحمان يوسف، الآليات القانونية لتلافي الجريمة المعلوماتية والحد من انتشارها وفقا للتشريع الجزائري، مجلة الفكر القانوني والسياسي، العدد الرابع، منشورة على الموقع:

أما المشرع الجزائري فقد اصطلح على تسمية الجريمة المعلوماتية بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، وعرفها في المادة الثانية من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، على أنها:" جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالاتالإلكترونية".

ما يمكن ملاحظته من هذا التعريف، أن المشرع ركز في تعريفه على عدة معطيات، منها وسيلة ارتكاب الجريمة وهو نظام الاتصالات الالكتروني، وموضوع الجريمة والمتمثل في المساس بأنظمة المعالجة الآلية للمعطيات الآلية، وكذلك الركن الشلاعي للجريمة المنصوص عليها في قانون العقوبات، كما أقر أن هذه الجريمة ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، وهذا ما يوسع نطاق مجال الجرائم المعلوماتية في القانون الجزائري.

الفرع الثاني: خصائص الجريمة المعلوماتية

الجريمة المعلوماتية تتميز بخصائص وصفات تميزها عن غيرها من أنواع الجرائم الأخرى فأول ما يلفت النظر في الجريمة المعلوماتية هو نعومتها وبعدها عن العنف فلا تتطلب لارتكابها العنف ولا استعمال الأدوات الخطرة كالأسلحة وغيرها، فنقل بيانات ممنوعة أو التلاعب بأرصدة البنوك مثلا لا تحتاج إلا إلى لمسات أزرار.

ومن بين الخصائص والسمات المميزة لهذه الجريمة عن الجرائم التقليدية ما يلي:

أولا: الجرائم المعلوماتية جريمة عابرة للحدود

تعد الجرائم المعلوماتية من الجرائم غير المقيدة والمرتبطة بمنطقة جغرافية معينة، فمن المتصور أن ترتكب الجريمة في أي وقت دون الالتزام والتقيد بدولة ما أو منطقة ما أو بقرب المسافات أو تباعدها، ويتم ارتكاب الجرائم المعلوماتية بواسطة الحواسيب وعن طريق الشبكة المعلوماتية.

إن شبكة الاتصالات العالمية(الانترنت) ألغت الحدود الجغرافية فيما بين الدول وبعضها وجعلتها قرية صغيرة؛ لذلك يقال ان الجريمة المعلوماتية أحيانا تتخطى حدود الدولة الواحدة؛

---

https://www.asjp.ceriste.dz/en/article.

فهي تتميز بالبعد الدولي بين الجاني والمجني عليه ومن الوجهة التقنية بين الجاني والمعطيات أو البيانات محل الجريمة[10].

هذه الطبيعة التي تتميز بها الجريمة المعلوماتية كونها جريمة عابرة للحدود خلقت العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب تطبيقه بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام.

ثانيا: صعوبة اكتشاف الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بصعوبة اكتشافها، وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة. وتعني الصعوبة في اكتشاف أن هناك جريمة وقعت، بغض النظر عن مرتكبيها، فقد تقع جريمة معلوماتية دون أن يشعر أحد بأن هناك جريمة وقعت إلا بعد مرور فترة من الزمن.

وغالبا لا يتم الإبلاغ عن هذه الجرائم إما لعدم اكتشاف الضحية لها وإما خشية من التشهير، أصنف إلى ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي تم اكتشافها[11].

ويمكن رد الأسباب التي تقف وراء الصعوبة في اكتشاف الجريمة المعلوماتية إلى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية، كما أن الجاني يمكنه ارتكاب هذه الجريمة في دول وقارات أخرى. وكذلك فإن قدرة الجاني على تدمير دليل الإدانة في أقل من الثانية الواحدة، يشكل عاملا إضافيا في صعوبة اكتشاف هذا النوع من الجرائم.

ثالثا: صعوبة اثبات الجريمة المعلوماتية

---

[10] بردال سمير، الجريمة المعلوماتية في التشريع الجزائري، مجلة القانون، العدد الثاني، جويلية 2010، ص 182. منشورة على الموقع:

https://www.asjp.ceriste.dz/en/article

[11] عبد القادر نشادي، الجرائم المعلوماتية في وسائل الاتصال الحديثة –دراسة وصفية تحليلية لمجموعة من الجرائم المرتكبة عبر الوسائط الاتصالية الحديثة في الجزائر، أطروحة لنيل شهادة الدكتوراه في علوم الإعلام والإتصال، كلية علوم الإعلام والإتصال، قسم الإتصال، جامعة الجزائر 3، 2016-2017، ص ص 70-71.

يعتبر اكتشاف الجريمة المعلوماتية-أمر كما سبق وذكرنا- ليس بالهين والسهل، ولكن حتى في حال اكتشافها والإبلاغ عنها، فإن اثباتها أمر تحيط به الكثير من الصعاب[12]. أي الصعوبة في اثبات وقوع الجريمة بعد اكتشافها.

معظم هذه الجرائم لا تترك ورائها أثار تقليدية،مثل البصمات والأثار المادية في الجريمة العادية، فهي جريمة تقع في بيئة إلكترونية يتم فيها نقل المعلومات وتداولها بالنبضات الإلكترونية غير المرئية ولا توجد مستندات ورقية ولا شهود في القضية[13].

ولعل أسباب صعوبة اثبات الجريمة المعلوماتية تعود للاتي[14]:

- إنها لا تترك أثرا بعد ارتكابها يلمس أو يرى بالعين المجردة.
- صعوبة الاحتفاظ الفني بأثارها إن وجدت.
- ضعف الخبرة الفنية لدى المحقق التقليدي مما يصعب عليه التعامل معها والتحقيق فيها.
- أنها جرائم ترتكب غالبا في الخفاء.
- سهولة محو الدليل والتخلص منه في ثوان معدودة.
- ترتكب الجريمة في دولة ما وتتحقق النتيجة الإجرامية في دولة أخرى، أي أنها جريمة ليس لها حدود.

رابعا: أسلوب ارتكاب الجريمة المعلوماتية

من خصائص الجرائم المعلوماتية أنها تبرر بصورة أكثر وضوحا في أسلوب ارتكابها وطريقتها، فإن كانت الجرائم التقليدية تتطلب نوعا من المجهود العضلي الذي قد يكون في ضوء ممارسة العنف والإيذاء كما هو الحال في جريمة القتل والاختطاف، أو في صورة الكسر وتقليد المفاتيح، كما هو الحال في جريمة السرقة[15].

---

[12]حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، مذكرة ماجستير في العلوم القانونية تخصص علم الإجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2011-2012، ص22.

[13] عبد الرحمان نشادي، مرجع سابق، ص 71.

[14]بردال سمير، مرجع سابق، ص 181.

[15]حمزة بن عقون، مرجع سابق، ص 24.

فإن الجريمة المعلوماتية جرائم هادئة بطبعها لا تحتاج إلى العنف، بل كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة.

كما تحتاج كذلك إلى وجود شبكة المعلومات الدولية (الانترنت) مع وجود مجرم يوظف خبرته أو قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير أو التغرير بالقاصرين كل ذلك دون حاجة لسفك الدماء[16].

هي جريمة هادئة لا تتطلب العنف، بالرغم من ذلك فإن البعض يشبه هذه الجرائم بجرائم العنف، نظرا لتماثل دوافع المعتدين على نظم الحاسب الالي مع مرتكبي العنف.

خامسا: الجريمة المعلوماتية تتم بتعاون أكثر من شخص

تتميز الجريمة المعلوماتية بأنها تتم عادة بتعاون أكثر من شخص على ارتكابها اضرارا بالجهة المجني عليها، وغالبا ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والأنترنت يقوم بالجانب الفني عليها لتغطية التلاعب، وتحويل المكاسب إليه.

والاشتراك من إخراج الجريمة المعلوماتية إلى حيز الوجود قد يكون اشتراكا سلبيا وهو الذي يترجم بالصمت من جانب من يعلم بوقوع الجريمة في محاولة منه لتسهيل اهتمامها، وقد يكون اشتراكا إيجابيا وهو غالبا كذلك يتمثل في مساعدة فنية أو مادية[17].

سادسا: خصوصية مجرمي المعلوماتية

يتصف المجرم المعلوماتي الذي يقترف الجريمة المعلوماتية الذي يطلق عليه المجرم المعلوماتي بخصائص معينة تميزه عن المجرم الذي يقترف الجرائم التقليدية (المجرم التقليدي). فإذا كانت الجرائم التقليدية لا تتطلب مستوى علمي ومعرفي للمجرم في عملية ارتكابها، فإن الأمر يختلف بالنسبة للجرائم المعلوماتية، فهي جرائم فنية تقنية في الغالب الأعم، والأشخاص الذين يقومون بارتكاب عادة يكونون من ذوي الاختصاص في مجال تقنية المعلومات أو على

[16] نهلا عبد القادر المومني،مرجع سابق، ص 58.

[17] نهلا عبد القادر المومني،مرجع سابق، ص 58.

الأقل شخص لديه حد أدنى من المعرفة والقدرة على استعمال الحاسوب والتعامل مع شبكة الأنترنت[18].

فعلى سبيل المثال، فإن الجرائم المعلوماتية ذات الطابع الاقتصادي مثل التحويل الإلكتروني غير المشروع للأموال يتطلب مهارة وقدرة فنية تقنية عالية جدا من قبل مرتكبها، كذلك فإن البواعث على ارتكاب المجرم المعلوماتي لهذا النوع من الإجرام المعلوماتي قد تكون مختلفة عن بواعث ارتكاب الجرائم من قبل المجرم التقليدي.

المطلب الثاني:
أركان الجريمة المعلوماتية وتصنيفاتها

تعد أركان الجريمة الأساس والأصل لقيام أي جريمة، فالمشرع الجزائي اشترط لقيام أي جريمة وجود ثلاث أركان أساسية، وهي الركن المادي والركن المعنوي والركن الشرعي، فالركن المادي يمثل كيانها الملموس ويعبر عن إرادة الفاعل بصورة يمكن اثباتها، أما الركن المعنوي يعبر عن إرادة المجرم المعلوماتي، أما الركن الشرعي فنعني به وجود نص قانوني يحدد الجريمة والجزاء الجنائي على سلوكيات معينة والذي ينقلها من دائرة الإباحة إلى دائرة التأميم.

ومن الصعب تصنيف الجرائم المعلوماتية، نظرا لحداثتها، واختلافها من مجتمع لأخر من حيث تطوره، ومدى استخدامه للحاسوب، ودرجة اعتماده عليه في مختلف القطاعات. لا الفقه والقضاء استقروا على تقسيم معين أو معيار واحد لتصنيف الجرائم المعلوماتية، لذلك تعددت التصنيفات، فهناك من عددها بحسب موضوع الجريمة وأخر قسمها بحسب طريقه ارتكابها، وعلى هذا الأساس نعتمد في تقسيم هذا المطلب إلى مختلف معايير التصنيف وهي على أساس الجرائم الواقعة على الأموال والواقعة على الأشخاص وأخرى الجرائم الواقعة على أمن الدولة، وأيضا سنحاول في هذا المطلب التطرق إلى أركان الجريمة المعلوماتية في الفروع التالية:

[18] حمزة بن عقون، مرجع سابق، ص 25.

الفرع الأول: أركان الجريمة المعلوماتية

حتى يتسنى معاقبة الجاني على إتيان فعل ما ونكون أمام تصرف يعاقب عليه القانون، لابد من توفر الأركان الأساسية للجريمة، وهي تلك العناصر التي لا وجود للجريمة بدونها، حيث تدور الجريمة معها وجودا وعدما، وتتمثل في الركن المادي للجريمة، والركن المعنوي الذي يقوم على القصد الجنائي وإتجاه إرادة الشخص نحو ارتكاب الفعل، والركن الشرعي وهو النص الذي يحوي النموذج القانوني للفعل أو الامتناع المجرم. وهذه الأركان متوفرة سواء كانت الجريمة تقليدية أو في شكلها الإلكتروني. وعليه سنتناول هذه الأركان بالتفصيل في الفروع التالية:

أولا: الركن الشرعي

تعتبر الجريمة عمل غير مشروع يجرمه القانون ويعاقب عليه وذلك بالنظر لما يقرره القانون الجنائي والقوانين المكلمة له من أوامر ونواهي تجرم وتعاقب على كل سلوك أو فعل ترى فيه السلطة المختصة بالتشريع أنه يرقى لدرجة التجريم بما يشكله من مساس بمصالح الجماعة بعريضها بوجه عام للخطر[19].

ويقوم الركن الشرعي على النص التشريعي المجرم للسلوك والمحدد للعقوبة المقررة له، تطبيقا لنص المادة الأولى من قانون العقوبات بقول:" لا جريمة ولا عقوبة أو تدبير أمن بغير قانون". وما يتماشى مع المادة 160 من دستور 2016 التي تنص على أن:" تخضع العقوبات الجزائية إلى مبدأ الشرعية والشخصية"[20].

وقد خص المشرع الجزائري الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بقسم خاص ضمن قانون العقوبات وهو القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، ويشتمل على ثمانية مواد تضمنت كل أنواع الاعتداءات على الأنظمة المعلوماتية.

---

[19] بوخبزة عائشة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، الجزائر، 2012-2013، ص 62.

[20] الصادر بموجب القانون رقم 01/16 مؤرخ ففي 6 مارس 2016، يتضمن التعديل الدستوري، ج ر، العدد 14، الصادرة في 7 مارس 2016.

كما أنه ومن أجل الحد من هذه الجريمة، أصدر قانون خاص يعمل على وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها طبقا لقانون 04/09 الصادر بتاريخ 2009/08/05، وهذا تطبيقا لمبدأ الشرعية وعدم جواز متابعة الشخص بأفعال غير مجرمة قانونا.

ثانيا: الركن المادي

يسبق الفعل الإجرامي أعمال تحضيرية من شأنها تفعيل الركن المادي في هذه الجريمة، كإمتلاك حاسب آلي واتصاله بشبكة الأنترنت، وامتلاكه برنامج للإختراق ذاو بقوم هو باستحداث هذا البرنامج، وغيرها من هذه السمات. رغم أن هذه التقنيات مشروعة بحسب الأصل ما لم تستعمل في أفعال مجرمة، لذلك يشترط في الركن المادي مباشرة التصرف التقني وأن تكون لهذا الفاعل دراية كافية وتحكم في هذه الوسائل[21].

وهذا ما أورده المشرع في المادة الثانية من القانون رقم 04/09 السابق الذكر"جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية".

كما تناولت المادة 394 مكرر من ق.ع الأعمال المادية لهذه الجريمة كالدخول أو البقاء بطريقة غير مشروعة في كل أو جزء من المنظومة للمعالجة الآلية المعلوماتية أو يحاول ذلك. فمجرد محاولة تعتبر جريمة يعاقب عليها القانون، وتشدد العقوبة على هذا الفعل، كما تضلعف العقوبة في حالة المساس بهذه المعطيات سواء كان ذلك بالحذف، أو تغيير. فالفعل المادي قد يتحقق بالنتيجة كدخول وتخريب، أو زيادة، أو محو، أو بدون نتيجة كمحاولة واكتشاف المرتكب ومتابعته من خلال المنظومة الأمنية لأي دولة.

ثالثا: الركن المعنوي

الجريمة المعلوماتية مثلها مثل الجريمة التقليدية، تقوم على عنصرين: الأول، العلم بأن الفعل مجرم، والثاني الإرادة التي تتجه إلى تحقيق نتيجة يعاقب عليها القانون.

[21] حوالف عبد الصمد، رحمان يوسف، مرجع سابق، ص 89.

ويتخذ القصد الجنائي عدة صور منها القصد الخاص والقصد العام، فهذا الأخير هو الهدف الفوري والمباشر للسلوك الإجرامي وينحصر في حدود تحقيق الغرض من الجريمة أي لا يمتد لما بعدها. أما القصد الجنائي الخاص هو ما يتطلب توافره في بعض الجرائم فلا يمفي مجرد تحقيق الغرض من الجريمة بل هو أبعد من ذلك أي أنه يبحث في نوايا المجرم. فما هو القصد الذي يجب توافره في الجريمة المعلوماتية؟

إن المجرم المعلوماتي يتوجه من أجل ارتكاب فعل غير مشروع أو غير مسموح مع علم هذا المجرم بأركان الجريمة، وبالرغم من أن بعض المخترقين يبررون أفعالهم بأنهم مجرد فضوليون وأنهم قد تسللوا صدفة، فلا انتفاء للعلم كركن للقصد الجنائي، وكان يجب عليهم أن يتراجعوا بمجرد دخولهم ولا يستمروا في الإطلاع على أسرار الأفراد والمؤسسات لأن جميع المجرمين والأشخاص الذين يرتكبون هذه الأفعال يتمتعون بمهارات عقلية زمعرفية كبيرة تصل في كثير من الأحيان إلى حد العبقرية.

فالقصد الجنائي متوافر في جميع الجرائم المعلوماتية دون أي استثناء ولكن هذا لا يمنع أن هناك بعض الجرائم المعلوماتية تتطلب أن يتوافر فيها القصد الجنائي الخاص مثل جرائم تشويه السمعة عبر الأنترنت، أما جرائم نشر الفيروسات عبر الشبكة فهي تتوفر على القصد الجنائي الخاص، فالمجرم يهدف إلى تعطيل عمل الشبكة وفي جميع الظروف المشرع هو من يختص بتحديد الحالات التي يشترط فيها توافر القصد الجنائي الخاص[22].

وبذلك إذا تحققت الأركان السالف ذكرها، نكون أمام جريمة معلوماتية سخر لها المشرع كل الآليات القانونية من أجل الحد منها.

الفرع الثاني: تصنيف الجرائم المعلوماتية

هناك أنواع كثيرة للجرائم المعلوماتية حيث لم يوضع لها معايير محددة من أجل تصنيفها وهذا راجع إلى التطور المستمر للشبكة والخدمات التي تقدمها.

[22] ونوغي نبيل، زيوش عبد الرؤوف، مرجع سابق، ص 137.

وقد تضاربت الأراء لتحديد أنواع جرائم الأنترنت وتعددت التصنيفات، فهناك من عددها بحسب موضوع الجريمة، وأخر قسمها بحسب طريقة ارتكابها.

وقد صنفها معهد العدالة القومي بالولايات المتحدة الأمريكية عام 1714 بحسب علاقتها بالجرائم التقليدية.

-**الصنف الأول:** يتمثل في الجرائم المنصوص عليها في قانون العقوبات متى ارتكبتباستعمال الشبكة.

-**الصنف الثاني:** تضمن دعم الأنشطةالإجرامية ويتعلق الأمر بما تلعبه الشبكة من دور فيدعم جرائم غسيل الأموال، المخدرات الاتجار بالأسلحة، واستعمال الشبكة كسوق للترويج غير المشروع في هذه المجالات.

-**الصنف الثالث:** بجرائم الدخول في نظام المعالجة الآلية للمعطيات، وتقع على البيانات والمعلومات المكونة للحاسوب وتغييرها أو تعديلها أو حذفها مما يغير مجرى عمل الحاسوب.

-**الصنف الرابع:** فتضمن جرائم الاتصال وتشمل كل ما يرتبط بشبكات الهاتف، وما يمكن أنيقع عليها من انتهاكات باستعمال ثغرات شبكة الانترنت.

وأخيرا صنف الجرائم المتعلقة بالاعتداء على حقوق الملكية الفكرية ويتمثل فيعمليات نسخ البرامج دون وجه حق، وسرقة حقوق الملكية الفكرية المعروضة على الشبكة دون إذن من صاحبها بطبعها وتسويقها واستغلالها بأي صورة طبقا لقانون حماية الملكية الفكرية.

إن تقسيم الجرائم المعلوماتية بما أنها ترتكب باستخدام الحاسوب كأداة أساسية، فدور الحاسوب في تلك الجرائم يكون هدفا للجريمة أو أداة لها[23].

[23] محمد أبو بكر بن يونس، الأحكام الموضوعية والجوانب الإجرائية – الجرائم الناتجة عن استخدام الأنترنت، دار النهضة العربية، مصر، 2004، ص 60.

أولا: الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي

وهنا لا يكون النظام المعلوماتي هو محل الجريمة، بل يكون الحاسب الالي هو الوسيلة لتسهيل النتيجة الاجرامي باستخدام النظام المعلوماتي، ويكون الهدف من ورائها الربح بطريق غير مشروع، الاعتداء على أموال الغير، الاعتداء على الأشخاص وسالمتهم وحياتهم الخاصة، أو في سمعتهم وشرفهم والاعتداء على أمن الدولة وأسرارها.

1- الجرائم الواقعة على الأشخاص

فرغم الايجابيات والفوائد التي جاءت بها الشبكة المعلوماتية والتسهيلات المقدمة للفرد، إلا أنها جعلته أكثر عرضة للانتهاك ومنها:

1-1- **جريمة التهديد:** وهو الوعيد يقصد به زرع الخوف في النفس، بالضغط على إرادةالانسان، وتخويفه من أضرار ما ستلحقه أو ستلحق أشخاص له بها صلة، ويجب أن يكون التهديد على قدر من الجسامة المتمثلة بالوعيد بإلحاق الاذى ضد نفس المجني عليه أو ماله أو ضد نفس او مال الغير، ولا يشترط أن يتم إلحاق الأذى فعلا أي تنفيذ الوعيد، لأنها تشكل جريمة أخرى قائمة بذاتها، تخرج من إطار التهديد الى التنفيذ الفعلي، وقد يكون التهديد مصحوبا بالأمر أو طلب لقيام بفعل أو الامتناع عن الفعل، أو لمجرد الانتقام، ولقد أصبحت الانترنت الوسيلة لارتكاب جرائم التهديد، والتي في حد ذاتها تحتوي عدة وسائل لإيصال التهديد للمجني عليه لما تتضمنه من نوافذ وجدت للمعرفة كالبريد الإلكتروني أو الويب...

1-2-انتحال شخصية: وهو استخدام شخصية فرد للاستفادة من ماله أو سمعته أو مكانتهولقد تميزت بسرعة الانتشار خاصة في الأوساط التجارية. وتتم بجمع قدر كبير من المعلومات الشخصية المراد انتحال شخصيته، للاستفادة منها لارتكاب جرائمه عن طريق استدراج الشخص ليدلي بمعلوماته الشخصية الكاملة، كالاسم، العنوان الشخصي،رقم بطاقة الائتمان للتمكن من الوصول لماله أو سمعته...عن طريق الغش.

1-3-انتحال شخصية أحد المواقع: ويتم ذلك عن طريق اختراق أحد المواقع للسيطرةعليه، ليقوم بتركيب برنامج خاص به هناك، باسم الموقع المشهور.

1-4- **جرائم السب و القذف:** للمساس بشرف الغير وسمعتهم، واعتبارهم، ويكون القذف والسب كتابيا،أو عن طريق المطبوعات أو رسوم، عبر البريد الالكتروني أو الصوتي، صفحات الويب، بعبارات تمس الشرف.

فيقوم المجرم بنشر معلومات تكون مغلوطة عن الضحية، وقد يكون شخصا طبيعيا أو معنويا، لتصل المعلومات المراد نشرها إلى أعداد كبيرة من مستخدمي شبكة الانترنت.

1-5- المواقع الإباحية والدعارة: وجود مواقع على شبكة الانترنت تحرض على ممارسةالجنس للكبار والقصر،وذلك بنشر صور جنسية للتحريض على ممارسة المحرماتوالجرائمالمخلة بالحياء عن طريق صور، أفلام، رسائل... بالإضافة إلى انتشار الصور ومقاطع الفيديو المخلة بالاداب على مواقع الانترنت من قبل الغزو الفكري لكي يتداولها الشباب وإفساد أفكارهم واضعاف إيمانهم.

وتوفر الشبكة تسهيلا للدعارة، عبر ألاف المواقع الإباحية،وتسوق الدعارة وتستثمر لها مبالغ ضخمة مع استخدام أحدث التقنيات.

1-6- التشهير وتشويه السمعة: يقوم المجرم بنشر معلومات قد تكون سرية أو مضللة أومغلوطة عن ضحيته، والذي قد يكون فرداً أو مؤسسة تجارية أو سياسية، تتعدد الوسائل المستخدمة في هذا النوع من الجرائم، لكن في مقدمة هذه الوسائل إنشاء موقع على الشبكة يحوي المعلومات المطلوب نشرها أو إرسال هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين، ويضم لهذه الجرائم كذلك تشويه السمعة، الشائعاتوالأخبار الكاذبة لمحاربة الرموز السياسية والفكرية وحتى الدينية من أجل تشكيك الناس في مصداقية هؤلاء الأفراد،وقد يكون الهدف من ذلك هو الابتزاز[24].

كل هذه الجرائم الماسة بالأشخاص تدخل ضمن الحياة الخاصة للأفراد التي كفلها القانون و في مقدمته الدستور الجزائري حيث تنص المادة **44** منه: " تضمن الدولة عدم انتهاك حرمة الانسان".

وعليه، يمكن استخدام الشبكة المعلوماتية في الاعتداء على حرمة الفرد وحياته الخاصة حرمته، والحريات العامة للأفراد، وهو مخالف للقانون ومعاقب عليه.

2-الجرائم الواقعة على الأموال: أصبحت المعاملات الشراء، البيع والإيجار تتم عبر الشبكة المعلوماتية، ومانجرّعليهمن وسائل الدفع والوفاء، فابتكرت معه طرق ووسائل للسطو على هذا التداول المالي بطريق غير مشروع، كالتحويل الإلكتروني، السرقة، القرصنة وغيرها.

[24]محمد أبو بكر بن يونس، مرجع سابق، ص ص 63-64.

2-1-السرقة الواقعة على البنوك: يتم سرقة المال بالطرق المعلوماتية عن طريق اختلاس البيانات والمعلومات الشخصية للمجني عليهم، والاستخدام لشخصية الضحية ليقوم بعملية السرقة المتخفية، ما يؤدي بالبنك إلى التحويل البنكي للأموالالالكتروني أو المادي إلى الجاني. حيث يستخدم الجاني الحاسب الالي لدخول شبكة الانترنت والوصول إلى المصارف والبنوك، وتحويل الأموال الخاصة بالعملات إلى حسابات أخرى. وعملية السرقةالإلكترونية كالاستلاء على ماكينات الصرف الالي والبنوك، يتم فيها نسخ البيانات الإلكترونية لبطاقة الصراف الالي ومن ثم استخدامها لصرف أموال من حساب الضحية، أو إنشاء صفحة انترنت مماثلة جدا لموقع أحد البنوك الكبرى أو المؤسسات المالية الضخمة لتطلب من العميل إدخال بياناته أو تحديث معلوماته بقصد الحصول على بياناته المصرفية وسرقتها. رسائل البريد الواردة من مصادر مجهولة التي توهم صاحب البريد الإلكتروني بفوزه بإحدى الجوائز أو اليانصيب وتطالبه بموافاة الجهة برقم حسابه المصرفي، والأمثلة كثيرة...

2-2-**تجارة المخدرات عبر الانترنت:** تتعلق بالترويج للمخدرات وبيعها، والتحريض علىاستخدامها، وصناعتها بمختلف أنواعها.

2-3-**غسيل الأموال:** تمارس عبر الانترنت، حيث استفاد الجناة ما وصلت إليه عصرالتقنية المعلوماتية لتوسيع نشاطهم الغير مشروع في غسيل أموالهم، بتوفير السرعة، وتفادي الحدود الجغرافية، ولقوانين المعيقة لغسيل الأموال، وكذا لتشفير عملياتهم وسهولة نقل الأموال و استثمارها لإعطائها الصبغة الشرعية.

2-4-الاستعمال الغير الشرعي للبطاقات الائتمانية: رافق استخدام البطاقات الائتمانية الاستيلاء عليها باعتبارها نقود الكترونية وذلك إما بسرقة أرقام البطاقات ثم بيع المعلومات للأخرين، من خلال الحصول على كلمة السرالمدرجة في ملفات أنظمة الحاسب الالي للضحية عن طريق الاحتيال، وذلك بإيهامه بحصول ربح، فيقدم الضحية معلومات تمكن الجاني من التصرف في ماله، أو إساءة استخدام الغير البطاقات الائتمانية، كأن يقوم السارق باستعمال البطاقة للحصول على السلع والخدمات أو سحب مبالغ مالية بموجبها من أجهزة التوزيع الالي أو السحب باستخدام بطاقات مزورة.

2-5-الجرائم الواقعة على حقوق الملكية الفكرية والأدبية: كذلك يكون النظام المعلوماتيوسيلة لاعتداء على حقوق الملكية الفكرية، وذلك بالسطو على المعلومات التي

يتضمنهانظام معلوماتي آخر، وتخزين واستخدام هذه المعلومات دون إذن صاحبها، حيث يعدّ اعتداء على الحقوق المعنوية وعلى قيمتها المادية.

2-6-قرصنة البرمجيات: هي عملية نسخ أو تقليد لبرامج إحدى الشركات العالمية علىاسطوانات وبيعها للناس بسعر أقل، وجريمة نسخ المؤلفات العلمية والأدبية بالطرق الإلكترونية المستحدثة. حيث أن المعلومة الأدبية والفكرية ذات قيمة أدبية ومادية بالإضافة إلى براءات الاختراع التي تخول لمالكها حق معنوي وآخر مالي[25].

نص عليها المشرع في الدستور في المادة **44**:" حقوق المؤلف يحميها القانون" , بالإضافة إلى القوانين المتعلقة بحقوق المؤلف والحقوق المجاورة، وبراءات الاختراع.

3-الجرائم الواقعة على أمن الدولة

تقع هذه الجرائم باستعمال النظام المعلوماتي سواء لإفشاء الأسرار التي تخص مصالح الدولة ونظام الدفاع الوطني، أوالإرهاب، التجسس.. نصت عليها المادة**394**مكرر**2**: "تضاعف العقوبة المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الاخلال بتطبيق عقوبات أشد".

3-1-الإرهاب: تستخدم المجموعات الإرهابية حالياً تقنية المعلومات لتسهيل الأشكال النمطيةمن الأعمال الإجرامية. وهم لا يتوانون عن استخدام الوسائل المتقدمة مثل: الاتصالات والتنسيق، وبث الأخبار المغلوطة، وتوظيف بعض صغار السن، وتحويل بعض الأموال في سبيل تحقيق أهدافهم.

ويقوم الإرهابيون باستخدام الانترنتلاستغلال المؤيدين لأفكارهم وجمع الأموال لتمويل برامجهم الإرهابية، والاستلاء على المواقع الحساسة وسرقة المعلومات وامتلاك القدرة علىنشر الفيروسات، وذلك يرجع إلى العدد المتزايد من برامج الكمبيوتر القوية والسهلة الاستخدام والتي يمكن تحميلها مجانا.

3-2-التجسس: يقوم المجرمون بالتجسس على الدول والمنظمات والشخصيات والمؤسساتالوطنية أو الدولية، وتستهدف خاصة: التجسس العسكري، السياسي، والاقتصادي،

[25]محمد أبو بكر بن يونس، مرجع سابق، ص 68.

وذلك باستخدام التقنية المعلوماتية، وتمارس من قبل دولة على دولة، أو من شركة على شركة ...

وذلك بالاطلاع على المعلومات الخاصة المؤمنة في جهاز آلي، وغير مسموح بالاطلاع عليها، كأن تكون من قبيل أسرار الدولة[26].

ثانيا: الجرائم المعلوماتية الواقعة على النظام المعلوماتي:

وهي الجرائم الواقعة على النظام المعلوماتي التي قد تستهدف سواء المكونات المادية لنظام المعلومات أو برامج النظام المعلوماتي، أو المعلومات المدرجة بالنظام المعلوماتي على النحو التالي:

1-الجرائم الواقعة على المكونات المادية للنظام المعلوماتي

ويقصد به الأجهزة والمعدات الملحقة به والتي تستخدم في تشغيله كالأسطوانات، الكابلات... والاعتداء عليها يكون بالسرقة لهذه المعدات أو عن طريق الإتلاف العمدي كإحراقها، ضرب الألات بشيء ثقيل، العبث بمفاتيح التشغيل خربشة الأسطوانات لكيلا تصبح صالحة لاستعمال.

2-الاعتداء على برامج النظام المعلوماتي

ويتوجب هنا معرفة ودراية ذات درجة عالية في مجال البرمجة، وتقع هذه الجرائم إما على البرامج التطبيقية أو برامج التشغيل.

البرامج التطبيقية: وهنا يقوم الجاني بتحديد البرنامج ثم التلاعب فيه للاستفادة منه ماديا، وذلك بتعديل البرنامج: ويكون الهدف من تعديل البرامج اختلاس النقود، حتى ولو كان باستقطاع مبالغ قليلة لكن لفترات زمنية طويلة لتحقيق الفائدة بدون إثارة الشبهات.

أما التلاعب: فيأخذ عدة أشكال، فقد يكون عن طريق زرع برنامج فرعي في البرنامج الأصليمثلا يسمح له الدخول غير المشروع في العناصر الضرورية للنظام المعلوماتي، حيث يصعب اكتشاف هذا البرنامج لدقته وصغر حجمه.

[26] تسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعرف، الإسكندرية، 2008، ص 91.

برامج التشغيل: وهي البرامج المسئولة عن عمل نظام معلوماتي من حيث قيامها بتنظيم وضبط ترتيب التعليمات الخاصة بالنظام.

وتقوم الجريمة هنا عن طريق تزويد البرنامج بمجموعة تعليمات إضافية ليسهل الوصول إليها بواسطة شفرة تسمح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي. وتأخذ شكلين هما المصيدة: وهو إعداد برنامج به ممرات وفراغات في البرنامج وتفرعات إضافية، وهنا يمكن للمبرمج استخدام البرنامج في أي وقت، ويصبح المهيمن على النظام وعلى صاحب العمل.

أما تصميم برنامج: هو قيام برنامج خصيصا يصعب اكتشافه لارتكاب الجريمة ومراقبة تنفيذها.

3-الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي

إن المعلومات المعالجة آليا هي أساس عمل النظام المعلوماتي، لأنها ذات قيمة مادية واقتصادية، لذلك تعد هدفا للجرائم الإلكترونية من خلال التلاعب فيها أو إتلافها.

يكون التلاعب في المعلومات الموجودة على النظام المعلوماتي بطريقة مباشرة أو غير مباشرة، فيتم التلاعب المباشر عن طريق إدخال معلومات بمعرفة المسئول عن القسم المعلوماتي، كضم مستخدمين غير موجودين بالعمل بهدف الحصول على مرتباتهم، الإبقاء على مستخدمين تركوا العمل للحصول على مبالغ شهرية، أو عن طريق تحويل لمبالغ وهمية لدى العاملين بالبنوك باستخدام النظام المعلوماتي بالبنك، وتسجيلها وإعادة ترحيلها وإرسالهالحساب آخر في بنك آخر، بهدف اختلاس الأموال. أما التلاعب الغير مباشر، فيتم عن طريق التدخل لدى المعلومات المسجلة بالنظام المعلوماتي باستخدام أحد وسائط التخزين، أو التلاعب عن بعد بمعرفة أرقام وشفرات الحسابات، قصد التلاعب في الشرائط الممغنطة، أو باستخدام الجاني كلمة السر أو مفتاح الشفرة، وإمكانية تسلل الجاني إلى المعلومات المخزنة والحصول على المنفعة المالية من مسافات بعيدة[27].

[27]محمد أبو بكر بن يونس، مرجع سابق، ص ص 69-70.

إتلاف المعلومات في مجال المعلوماتية بالاعتداء على الوظائف الطبيعية للحاسب الالي ، وذلك بالتعدي على البرامج والبيانات المخزنة والمتبادلة بين الحواسب وشبكاته، وتدخل ضمن الجرائم الماسة بسالمة المعطيات المخزنة ضمن النظام المعلوماتي، ويكون الإتلاف العمدي للبرامج والبيانات كمحوها أو تدميرها الكترونيا، أو تشويهها على نحو يجعلها غير صالحة للاستعمال.

المبحث الثاني:

المجرم المعلوماتي

أضافت المعلوماتية الكثير من الجوانب الايجابية إلى حياتنا إلا أنها في المقابل جلبت معها أنماطا جديدة من الجريمة والمجرمين اصطلح على تسميتهم بمجرمي المعلوماتية.

فالمجرم المعلوماتي يعتبر هو أساس الجريمة المعلوماتية، وهو يختلف عن المجرم العادي لدرايته الكافية إن لم نقل الكبيرة بتقنيات الحواسب.

يرتبط الإجرام المعلوماتي ارتباطا وثيقا بشخصية المجرم، فالنتائج المرتبطة على هذا الفعل الإجرامي تتوقف على شخصية المجرم ودوافعه إلى ارتكاب الجريمة، فإنه لا يمكن للعقوبة أن تحقق هدفها ما لم تضع في الاعتبار شخصية المجرم. وإذا كنا في مجال الإجرام المعلوماتي فيجب أن ننظر إلى المجرم المعلوماتي من حيث صفاته وسماته وكذا من حيث أصنافه وأنماطه، وكذلك على دوافعه لارتكاب الفعل.

وبناء على ما تقدم، سنتناول في هذا المبحث دراسة شخصية المجرم المعلوماتي من حيث سماته في (المطلب الأول)، ونتعرض بعد ذلك إلى أبرز طوائف وفئات مجرمي المعلوماتية، وفي الأخير نلقي الضوء على أهم الدوافع التي تحمل المجرم المعلوماتي على ارتكاب هذا السلوك الإجرامي وذلك في (المطلب الثاني).

المطلب الأول:

السمات الخاصة بالمجرم المعلوماتي وفئاته

تتدرج الجرائم في مجال الحاسب الالي من الجرائم البسيطة إلى الجرائم الإرهابية وذلك تبعا لشخصية المجرم المعلوماتي وما لديه من خبرة في مجال استخدام الحاسب الالي والغرض من ارتكاب الجريمة.

فمجال التقنيات الحديثة ساهم بدوره في التطور السريع لأنماط جريمة تقنية المعلومات بصفة عامة مما أصبح عائقا أمام دراسات علم الإجرام الحديثة التي تسعى إلى وضع تصنيف ثابت لمجرمي المعلوماتية.

يتميز المجرم المعلوماتي عن غيره من الجرمين مرتكبي الجرائم التقليدية بصفات وخصائص معينة جعلته محل الأبحاث والدراسات؛ فالمجرم المعلوماتي أيضا يتمتع بقدر كبير من الذكاء ودرجة علمية وثقافية عالية لكي يتمكنوا من استخدام أجهزة الحاسب الالي.

من خلال الخصائص السالفة الذكر في المجرم المعلوماتي يمكن تصنيف مرتكبي الجرائم المعلوماتية إلى مجموعة من الطوائف، إلا أن هذه التصنيفات لا تعني أن كل مجرم معلوماتي يندرج تحت فئة محددة دون غيرها، بل يمكن أن يكون المجرم الواحد مزيجا من أكثر من طائفة أو فئة. ولهذا يمكن لنا وفقا لما توصلت له الدراسات والأبحاث التي تناولت مجرمي المعلوماتية أن نبين بعض هذه الأنماط لهؤلاء المجرمين، ونستخلص مجموعة من السمات والخصائص التي يتميز بها المجرم المعلوماتي عن غيره من المجرمين وذلك كالاتي:

الفرع الأول: السمات الخاصة بالمجرم المعلوماتي

تتمثل سمات المجرم المعلوماتي فيما يلي:

أولا: المجرم المعلوماتي يتمتع بالمهارة والمعرفة والذكاء

يعتبر الذكاء من أهم صفات مرتكب الجرائم المعلوماتية، لأن ذلك يتطلب المعرفة التقنية لكيفية الدخول إلى أنظمة الحاسب الالي والقدرة على التعديل والتغيير في البرامج وارتكاب

جرائم السرقة والنصب وغيرها من الجرائم التي تتطلب أن يكون مرتكب الجريمة على درجة كبيرة من المعرفة لكي يتمكن من ارتكاب تلك الجرائم.[28]

حيث يمتلك هذا المجرم من المهارات ما يؤهله للقيام بتعديل وتطوير في الأنظمة الأمنية، حتى لا يستطيع أن تلاحقه وتتبع أعماله الإجرامية من خلال الشبكات أو داخل أجهزة الحواسيب.

بل إن بعض مرتكبي هذه الجرائم هم من المتخصصين في مجال معالجة المعلومات ألليا، فتنفيذ الجريمة المعلوماتية يتطلب قدرا من المهارة لدى الفاعل التي قد يكتسبها عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات.[29]

فالمجرم المعلوماتي يستخدم قدراته العقلية ولا يلجأ إلى استخدام العنف أو الإتلاف المادي بل يحاول أن يحقق أهدافه بهدوء، فالمجرم المعلوماتي هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف، فالمجرم المعلوماتي يسعى بشغف إلى معرفة طرق جديدة مبتكرة لا يعرفها أحد سواه، وذلك من أجل اختراق الحواجز الأمنية في البيئة الإلكترونية، ومن ثم تحقيق مراده[30].

ثانيا:المجرم المعلوماتي انسان اجتماعي

المجرم المعلوماتي بصفته انسان ذكي فهو اجتماعي، فهو لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به، بل إنه انسان يستطيع التوافق والتصالح مع مجتمعه، فهو شخص مرتفع الذكاء مما يساعده على عملية التكيف مع المجتمع.

فالذكاء في نظر الكثيرين ليس سوى القدرة على التكيف؛ ولا يعني ذلك التقليل من شأن المجرم المعلوماتي، بل أن خطورته الإجرامية قد تزيد إذا زاد تكيفه الاجتماعي مع توافر الشخصية الإجرامية لديه[31].

---

[28] أيمن عبد الحفيظ، الإتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دون دار وبلد النشر، 2005، ص 50.

[29] نهلا عبد القادر المومني، مرجع سابق، ص77.

[30] حمزة بن عقون، مرجع سابق، ص 30.

[31] نهلا عبد القادر المومني، مرجع سابق، ص 79.

المجرم عند شعوره أنه محل ثقة في مجتمعه وشعوره بأنه خارج إطار الشبهات قد يدفعه إلى التمادي في ارتكاب جرائمه التي قد لا تكتشف، وإذا اكتشفت فإنها تواجه صعوبة الإثبات ونقص الأدلة ونقص الخبرة لدى المحققين ولدى رجال القضاء.

ومن الملاحظ أن تكيف هؤلاء الأشخاص في المجتمع يكون محدودا وغالبا ما يكونون منعزلين عن المجتمع.

ثالثا: المجرم المعلوماتي يبرر ارتكاب جريمته

توصلت بعض الدراسات أنه لا يوجد شعور لدى مرتكب فعل الإجرام المعلوماتي بعدم أخلاقية ما يقوم به أو بمساسه بمصالح أو قيم يحرص المجتمع على حمايتها بل لا يعتبر أن ما يقوم به يدخل في عداد الجرائم، خاصة في الحالات التي يقف فيها السلوك عند حد قهر نظام الحاسوب وتخطي الحماية المفروضة حوله.

فإن كثيرا من العاملين في مجال المعلوماتية لا يجدون أي خطأ في استعمال الشفرات السرية الخاصة بالدخول إلى أنظمة الحاسبات الألية للمؤسسات التابعين لها لأغراض شخصية. وما ساعد على ذلك عدم وجود احتكاك مباشر بين الأشخاص[32].

فالتباعد في العلاقة الثنائية بين الفاعل والمجني عليه يسهل المرور إلى الفعل غير المشروع ويساعد على إيجاد نوع من الإقرار الشرعي الذاتي بمشروعية هذا الفعل. ففي الكثير من الأحيان يقوم العاملون بالمؤسسات المختلفة باستخدام أجهزة الحاسوب لأغراض شخصية بوصفه سلوكا شائعا بين الجميع ولا ينظر بوصفه فعلا اجراميا[33].

الشعور بعدم أخلاقية هذه الأفعال الإجرامية المعلوماتية لدى فئة من مرتكبيها لا ينفي وجود مجرمين يرتكبون الإجرام المعلوماتي وهم على دراية بعدم مشروعية وأخلاقية هذا الفعل.

رابعا: خوف المجرم المعلوماتي من كشف جريمته

[32] سعيداني نعيم، أليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، شهادة الماجستير في العلوم القانونية تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، الجزائر، 2013، ص 12.

[33] حمزة بن عقون، مرجع سابق، ص 32.

يتصف مجرموا المعلوماتية بالخوف من كشف جرائمهم، وبالرغم من أن هذه الخشية تصاحب المجرمين على اختلاف أنماطهم، إلا أنها تميزهم (مجرمي المعلوماتية) بصفة خاصة لما يترتب على كشف أمرهم من ارتباك مالي وفقد المركز الوظيفي في كثير من الأحيان.[34]

كما أن طبيعة الأنظمة المعلوماتية نفسها تساعد الجاني على الحفاظ على سرية أفعاله، ذلك أن كثير ما يعرض المجرم إلى اكتشاف أمره، هو أن يطرأ أثناء تنفيذ جريمته عوامل غير متوقعة، في حين أهم الأسباب التي تساعد على نجاح الجريمة المعلوماتية هي الحواسيب إنما تؤدي عملها غالبا بطريقة ألية، بحيث لا تتغير المراحل المختلفة التي تمر بها، أي من العمليات التي يقوم بها من مرة إلى أخرى.

خوف المجرم المعلوماتي من انكشاف أمره، عائد إلى انتمائه في الغالب إلى وسط اجتماعي، سواء من حيث التعليم أو الثقافة أو المستوى المهني وطبيعة العمل.

خامسا: المجرم المعلوماتي يتمتع بالسلطة اتجاه النظام المعلوماتي

نعني بالسلطة الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته، وهذه السلطة إما تكون مباشرة كالشفرة الخاصة بالدخول إلى النظام المعلوماتي التي تعطي للفاعل مزايا متعددة مثل فتح الملفات ومحو أو تعديل محتوياتها أو مجرد قراءتها أو كتابتها[35].

وأيضا قد تتمثل هذه السلطة في الحق في: استعمال الأنظمة المعلوماتية، أو اجراء بعض التعاملات، أو مجرد الدخول إلى الأماكن التي تحتوي على هذه الأنظمة.

الفرع الثاني: الفئات المختلفة للمجرم المعلوماتي

وتتمثل فئات المجرم المعلوماتي فيما يلي:

---

[34] نهلا عبد المومني، مرجع سابق، ص 79.

[35] سوير سفيان، جرائم المعلوماتية، مذكرة الماجستير في العلوم الجنائية وعلوم الإجرام، كلية الحقوق والعلوم السياسية، 2010جامعة أبو بكر بلقايد، تلمسان، الجزائر،2011، ص24.

أولا: فئة صغار مجرمي المعلوماتية

كما يسميهم البعض صغار نوابغ المعلوماتية، لفظ يطلق على المجموعات التي تميل للتحدي الفكري وهم غالبا ما يكونون في مرحلة المراهقة وعلى الرغم من صغر سنهم إلا أنهم قادرون على اقتحام كافة أنواع الأنظمة البنكية والشركات والمؤسسات المالية.[36]

هذه الفئة من الشباب لا يدركون ولا يقدرون مطلقا النتائج المحتملة التي يمكن أن تؤدي إليها أفعالهم غير المشروعة بالنسبة لنشاط منشأة أو شركة تجارية، لان لديهم ببساطة ميلا للمغامرة والتحدي والرغبة في الاكتشاف ونادرا ما تكون أهداف أفعالهم المحظورة غير شريفة.

يثير مجرموا المعلوماتية من هذه الطائفة جدلا واسعا، فالبعض يرى أنه:" لا يبدو من المناسب أن نصنف هؤلاء الشباب في طائفة من الطوائف الإجرامية"، في الوقت الذي يعتبرها الأخر ممن يقدم خدمة لأمن المعلومات ووسائل الحماية ويصفهم بالأخيار، وهناك من يصف هذه الفئة ضمن مجرمي المعلوماتية كغيرهم من المجرمين، وفي الحقيقة يجب عدم التقليل بخطورة هؤلاء الشباب فقد تتعدى مرحلة الميل للمغامرة والتحدي[37].

ثانيا: القراصنة

هم أشخاص عادة مبرمجون من أصحاب الخبرة ينتهكون أمن النظام ولديهم نوايا خبيثة، كذلك لديهم مهارة متقدمة بأجهزة الكمبيوتر والشبكات والمهارات اللازمة لتدمير أي موقعوتهكيره ويمكن تصنيف القراصنة إلى صنفين هما:

1-القراصنة الهواة العابثون أو (الهاكرز) HAEKERS

هذا النوع من القراصنة أو ما يطلق على تسميتهم "بالهاكرز" يرون في اختراق الأنظمة المعلوماتية تحديا لقدراتهم الذاتية، وهذه الطائفة غالبا ما تكون من هواة الحاسوب، فيقومون بأعمالهم هذه لمجرد إظهار أنهم قادرون على اقتحام المواقع الأمنية أحيانا أو لمجرد ترك بصماتهم التي تثبت وصولهم إلى تلك المواقع أحيانا أخرى.[38]

---

[36] أيمن عبد الحفيظ، مرجع سابق، ص 13.

[37] نهلا عبد القادر المومني، مرجع سابق، ص 81.

[38] نفس المرجع، ص 83.

وهم يدعون أنه لا توجد هناك دوافع تخريبية وراء أعمالهم، بل قد يكون الفضول وحب المعرفة والتعمق في عمل الأنظمة المعلوماتية هو دافعهم الأول ومجرموا المعلوماتية من هذا الصنف هم عادة أشخاص عاديون يشغلون مناصب محل ثقة ولديهم الكفاءة الخاصة والمعرفة والمهارة المطلوبة في مجال الحواسيب الإلكترونية. هم لا يهدفون إلا للمغامرة وإظهار القدرات فلا توجد عادة عند هؤلاء أطماع مالية.[39]

إلا أن في الحقيقة هؤلاء الهواة ساهموا في كشف الفجوات الأمنية للأنظمة المعلوماتية في المؤسسة المالية وغيرها، الأمر الذي ساهم في تطوير نظم الأمن ضد الاختراقات الأمنية التي قد يقوم بها مجرمو المعلوماتية.

2-القراصنة المحترفين (CRACKERS)

تعد فئة المجرمون المحترفون من أخطر الفئات ومواجهتهم تتسم دائما بالصعوبة ولعل من أخطر هؤلاء الفئات " فئة الياقات البيضاء"[40].

حيث يقومون بارتكاب جرائم السرقة والنصب والاحتيال من على بعد استخدام شبكات الحاسب الالي في تحويل مبالغ مالية من أي الجهات، ومن أخطر جرائم هذه الفئات جريمة التجسس سواء في المجال الصناعي أوالتجاري أو في المجال السياسي أو العسكري.

أثبتت الدراسات أن محترفي الجرائم المعلوماتية من الجيل الحديث هم غالبا من الشباب الذين تتراوح أعمارهم من25-45 سنة، تعكس هذه الفئة اعتداءاتهم ميولا إجرامية خطرة تنبئ عن رغبتها في احداث التخريب، ويتميز هؤلاء بقدراتهم التقنية الواسعة وخبرتهم في مجال أنظمة الحاسوب والشبكات وهم أكثر خطورة من الصنف الأول فقد يحدثون أضرارا كبيرة.[41]

---

[39] نهلا عبد القادر المومني، مرجع سابق، ص 84.

[40]يطلق لفظ ذوي الياقات البيضاء على هؤلاء الذين يقومون بارتكاب جرائمهم عن طريق استخدام التكنولوجيا الحديثة فلم يعد هناك داع للإراقة الدماء أو استخدام أسلحة قاتلة لسرقة بضعة جنيهات لأن هذه الفئة تقوم بتحويل ملايين الجنيهات باستخدام أزرار الكمبيوتر من خلال الدخول على أنظمة أحد البنوك أو عن طريق سرقة كروت الائتمان للاستفادة منها في عمليات البيع والشراء. أنظر: أيمن عبد الحفيظ، مرجع سابق، ص 34.

[41] نهلا عبد المومني، مرجع سابق، ص 84.

وعادة ما يعود المجرم المحترف بالجريمة المعلوماتية إلى ارتكاب الجريمة مرة أخرى حيث تزداد سوابقه القضائية، وهو يعيش لسنوات طويلة عن عائد جرائمه، وهذا المجرم لا يفضل الأفكار المتطرفة وإنما الأفكار التي تدر عليه الأرباح.

ثالثا: طائفة الموظفون العاملون في مجال الأنظمة المعلوماتية

بحكم طبيعة عمل هؤلاء الموظفين ونظرا لأن النظام المعلوماتي هو مجال عملهم الأساسي، ونظرا للمهارات والمعرفة التقنية التي يتمتعون بها فإنهم يقترفون بعض الجرائم المعلوماتية التي من الممكن أن تحقق أهدافهم الشخصية، وأهمها الكسب المادي، فالعلاقة الوظيفية التي تربط بين الموظف والمجني عليه تجعل عملية ارتكابه للجريمة المعلوماتية أسهل نظرا للثقة التي يتمتع بها.[42]

وهناك فئة من الموظفين الحاقدين على أعمالهم أو على مؤسساتهم، الذين قد يقدمون على أعمال إجرامية لا تهدف إلى الكسب المادي، أو لتحقيق هدف سياسي، إنما يحرك أنشطتهم الرغبة في الانتقام والثأر من صاحب العمل معهم وهذه الفئة يذهب البعض إلى تسميتها "بفئة مجرمي المعلوماتية الحاقدين[43]. وهم لا يسعون إلى الإشادة بالتفوق العلمي مثل صغار نوابغ المعلوماتية، وإمنا هدفهم هو الانتقام.

رابعا: طائفة مجرموا المعلوماتية أصحاب الآراء المتطرفة

تضم هذه الجماعات الإرهابية أو المتطرفة، والتي تتكون من مجموعة من الأشخاص لديهم معتقدات وأفكار اجتماعية أو سياسية أو دينية، ويرغبون في فرض هذه المعتقدات باللجوء أحيانا إلى النشاط الإجرامي، وعادة ما يكون هذا النشاط يرتكز على العنف من أجل لفت الأنظار إلى ما يدعون إليه، إن اهتمام الجماعة الإرهابية يتجه إلى نوع جديد من النشاط الإجرامي ألا وهو الجريمة المعلوماتية.

إن اعتماد المؤسسات المختلفة داخل الدول على أنظمة الحاسبات الالية في انجاز أعمالها والأهمية القصوى للمعلومات التي تحتويها في أغلب الحالات قد جعل من هذه الأنظمة هدفا جذابا لهذه الجماعات. ومن الأمثلة الشهيرة في هذا الخصوص قيام إحدى الجماعات الإرهابية

[42] بن عقون حمزة، مرجع سابق، ص 43.

[43] نفس المرجع.

المعروفة في أوروبا باسم "The Red Brigades" بتدمير ما يزيد عن 60 مركزا للحاسبات الالية خلال الثمانينات لتلفت النظر إلى أفكارها ومعتقداتها[44].

خامسا: مجرموا المعلوماتية في إطار الجريمة المنظمة

الجريمة المنظمة بالمعنى الدقيق تطلق على عصابات المافيا، ورغم عدم دخول الجريمة المنظمة عالم الإجرام المعلوماتي بشكل كبير حتى الأن، إلا أنه من المتوقع دخولها هذا المجال على نحو واسع، وذلك لارتفاع عائد الجريمة المعلوماتية، ورغبة منها عدم اقتصار نشاطها على الجرائم التقليدية.[45]

ومن التعريفات التي قيلت في الجريمة المنظمة أنها:" تعبير عن مجتمع اجرامي يعمل خارج إطار الشعب والحكومة ويضم بين طياته الاف المجرمين الذين يعملون وفقا لنظام بالغ الدقة والتعقيد يفوق النظم التي تتبعها أكثر المؤسسات تطورا وتقدما، كما يخضع أفرادها لأحكام قانونية سنوها لأنفسهم وتفرض احكاما بالغة القسوة على من خرج عن أعراف الجماعة، ويلتزمون في أداء أنشطتهم الإجرامية بخطط دقيقة يلتزمون بها ويجنون من ورائها الأموال الطائلة[46].

منظمات الجريمة المنظمة تطور أساليب عملها باستمرار بما يحقق أهدافها وغاياتها، فهي تسعى دوما إلى استغلال الوسائل التقنية الحديثة في القيام بنشاطاتها، فاستفادت هذه المنظمات عبر سنوات عملها من أحدث وسائل الاتصال حتى تؤمن الترابط بين أفرادها وجماعاتها[47].

المطلب الثاني:
دوافع ارتكاب الجريمة المعلوماتية

مما سبق يتضح لنا أن فئات مرتكبي الجريمة المعلوماتية تختلف عن مرتكبي الجرائم التقليدية. فالدافع (الباعث) هو العامل المحرك للإرادة الذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والانتقام.

---

[44] نائلة عادل محمد فريد قورة، مرجع سابق، ص63.

[45] بن عقون حمزة، مرجع سابق، ص 43.

[46] نفس المرجع، ص 44.

[47] نهلا عبد المومني، مرجع سابق، ص85.

وللجريمة المعلوماتية عدة دوافع لارتكابها، فبعضها يرجع إلى دوافع شخصية والبعض الأخر يرجع إلى دوافع خارجية، وكل هذه الدوافع يكون مصدرها الرغبة الإجرامية وهذا ما سنتعرض له من خلال هذا المطلب في الفروع التالية:

الفرع الأول: الدوافع المادية "الربح وكسب المال"

تعد الرغبة في تحقيق الثراء من العوامل الرئيسية لارتكاب جرائم المعلوماتية، وهو من أهم الدوافع وأكثرها تحريكا للجناة، نظرا للربح الكبير الذي يمكن أن يحققه هذا النوع من الأنشطة الإجرامية.

وغالبا ما يكون الدافع لارتكاب هذه الجرائم وقوع الجاني بمشاكل مادية تعجزه عن سداد ديونه المستحقة، أو لوجود مشاكل عائلية تعود إلى عدم توفر الأموال، أو الحاجة لها للعب القمار، أو شراء المخدرات، أو القيام بأعمال المراهنة وغيرها، حيث يسعى الجاني للخروج من هذه المأزق إلى عمليات التلاعب بالأنظمة المعلوماتية للبنوك والمؤسسات المالية، وذلك بواسطة اختراق الأنظمة المعلوماتية لها، واكتشافه لفجواتها الأمنية.[48]

يقوم مرتكب الجرائم المعلوماتية ذو الكفاءة الفنية العالية، بما لديه من خبرة ومهارة في المجال التكنولوجي بتوجيه هذه الإمكانيات نحو المؤسسات المالية لمحاولة تحقيق المكاسب المادية إما بسرقة تلك الأموال أو بتحويلها لحسابه الشخصي داخل البنك. وفي حال نجاح المجرم في ارتكاب جريمته المعلوماتية، فإن ذلك قد يدر عليه أرباحا تكون هائلة في زمن قياسي[49].

الفرع الثاني: الرغبة في التعليم

هناك من يرتكب جرائم الحاسوب، بغية الحصول على الجديد من المعلومات وسبر أغوار هذه التقنية المتسارعة النمو والتطور. وهؤلاء الأشخاص يقومون بالبحث واكتشاف الأنظمة والعمل من خلال الجماعة وتعليم بعضهم، ويفضل هؤلاء القراصنة البقاء مجهولين أكبر وقت

[48] صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة الماجستير في القانون، تخصص القانون الدولي للاعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري-تيزي وزو، الجزائر، 2013، ص ص 38-39.

[49] أيمن عبد الحفيظ، مرجع سابق، ص 18.

ممكن حتى يتمكنوامن الاستمرار في التواجد داخل الأنظمة ويكرس البعض منهم كل وقته في تعلم كيفية اختراق المواقع الممنوعة والتقنيات الأمنية لأنظمة الحاسوبية.

يرى هؤلاء المجرمون أن جميع المعلومات المفيدة يجب أن تتاح حرية نسخها والاطلاع عليها، إلا أنهم يقرون بضرورة إغلاق بعض نظم المعلومات السرية التي تخص الأفراد[50].

وبالتالي يتضح أن المكسب المادي ليس دائما دافعهم إلى ارتكاب تلك الجريمة.

الفرع الثالث: المتعة والتحدي والرغبة في قهر النظام المعلوماتي واثبات الذات

قد تكون الدوافع لارتكاب الجريمة المعلوماتية مجرد رغبة في اثبات الذات وتحقيق انتصار على تقنية الأنظمة المعلوماتية دون أن يكون لهم نوايا أثمة، ويرجع ذلك إلى وجود عجز في التقنية التي تترك الفرصة لمشيدي برامج النظام المعلوماتي لارتكاب تلك الجرائم[51].

على صعيد أخر قد يكون الدافع وراء ارتكاب الجرائم المعلوماتية هو الرغبة في قصر الأنظمة الإلكترونية والتغلب عليها، إذ يميل مرتكبو هذه الجرائم إلى إظهار تفوقهم على وسائل التكنولوجيا الحديثة.

الفرع الرابع: الرغبة في الانتقام

الانتقام موجود داخل النفس البشرية، حيث يعد من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب جريمة، وغالبا ما يصدر من شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها لأنه غالبا ما يكون أحد موظفيها، ويقوم بهذا الدافع نتيجة إما لفصله من العمل أو تخطيه في الحوافز أو الترقية فهذه الأمور تجعله يقدم على ارتكاب جريمته[52]. أي يتولد لدى المجرم المعلوماتي الرغبة في الانتقام من رب العمل.

---

[50] نهلا عبد القادر المومني، مرجع سابق، ص 90.

[51] أحمد خليفة الملط، الجرائم المعلوماتية، ط 2، دار الفكر الجامعي، الإسكندرية، 2006، ص 90.

[52] أيمن عبد الحفيظ، مرجع سابق، ص 19.

ومثال ذلك فقد دفع الانتقام بمحاسب شاب إلى التلاعب بالبرامج المعلوماتية بحيث جعل هذه البرامج تعمل على إخفاء كل البيانات الحسابية الخاصة بديون الشركة التي يعمل فيها بعد رحيله بعدة أشهر، وقد تحقق هذا الأمر في التاريخ المحدد من طرفه[53].

الفرع الخامس: الدوافع الأخرى (الخارجية)

لا تعتبر الدوافع السابقة الذكر هي الوحيدة بل إن هناك دوافع أخرى تدفع بالمجرم المعلوماتي إلى ارتكاب الجريمة المعلوماتية. فمثلا المنافسة التجارية أو التجسس العسكري قد يكون من البواعث التي تدفع إلى ارتكاب الجريمة المعلوماتية بين الدول وهذا ما تعرضه مواقع القرصنة من خدمات للحصول على هذه المعلومات[54].

كما أن الدوافع السياسية والاقتصادية من أهم المحفزات إلى ارتكاب هذا السلوك الإجرامي، وترتكب عن طريق شبكة الانترنت بشكل شبه دائم لاختراق مواقع حكومية وتعطيلها.

ويمكن اعتبار التسابق الفضائي والعسكري الحاصل بين الدول، تدفع بالمجرم المعلوماتي إلى ارتكاب الجريمة المعلوماتية، كما أن مناهضة العولمة قد تكون احدى الأسباب لارتكاب هذا الفعل[55].

وأخيرا، يمكن القول ان الفعل الواحد قد يعكس دوافع متعددة وخاصة، فمحرك أنشطة الجريمة المعلوماتية دوافعه سياسية وايديولوجية، في حين أن أنشطة الاستلاء على الاسرار التجارية تحركها دوافع المنافسة، وقد تتداخل وتشترك هذه الدوافع في الفعل الواحد.

---

[53] محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، 1994، ص 92.

[54] نهلا عبد القادر المومني، مرجع سابق، ص 93.

[55] نفس المرجع.

في ختام هذا الفصل توصلنا إلى أنه إزاء التصدي لظاهرة الاجرام المعلوماتي، فان التعريفات التي تناولت هذه الظاهرة قد اختلفت فيما بينه، فمنها ما تناولها بالتعريف على نحو ضيق ومنها ما عرفها على نحو واسع.

يمكن ان نعرف الجريمة المعلوماتية على انها كل اعتداء يقع على نظم الحاسب الالي وشبكاته أو بواسطتها.

ومن خلال التعريفات التي قدمها رجال القانون وما تم ايرده من نصوص قانونية في هذا الشأن، نجد هذه الجريمة تتميز عن غيرها من الجرائم بعدة خصائص منها، أنها ترتكز في وجودها على وسائل مادية كالحاسب اللآلي، وأنها جريمة لا تترك آثار مادية ظاهرة للعيان لان المتعاملين فيها يتميزون بقدرتهم في التحكم في تكنولوجيا المعلومات، أي لهم ملكات ذهنية تمكنهم من مباشرة هذا الفعل المجرم، كما أنها جريمة عابرة للحدود خاصة وأن التعامل يكون في الفضاء العالمي، أي الشبكة العنكبوتية الذي لا يعترف بالحدود الجغرافية مما يسهل ارتكاب الجريمة في أي بقعة من العالم.

وحتى يتسنى معاقبة الجاني على اتيان فعل ما ونكون أمام تصرف يعاقب عليه القانون، لابد من توفر الاركان الاساسية للجريمة، والجريمة المعلوماتية مثلها مثل الجريمة التقليدية، تقوم على اركان ثلاثة من توفر الركن الشرعي الذي يجسد مبدأ شرعية التدبير والعقوبة، والركن المادي الذي يتمثل في أفعال مادية تتم في عالم إفتراضي داخل منظومة معلوماتية خاصة، والركن المعنوي والذي يتمثل في القصد الجنائي وأن المجرم يعلم أنه يتعامل في جريمة معلوماتية خطيرة.

الفصل الثاني:
سبل مواجهة الجريمة المعلوماتية في التشريع الجزائري

بالرغم من المزايا الهائلة التي تتحققها تقنية المعلومات في شتى ميادين الحياة المعاصرة، فان هذه الثورة التكنولوجية المتنامية صاحبتها في المقابل ظهور الجريمة المعلوماتية، التي تمتاز بسمات متميزة عن الجرائم التقليدية، الامر الذي أدى إلى بروز مشاكل قانونية جديدة في نطاق القانون الجنائي وفي غيره من فروع القانون الاخرى في مواجهة واقع المعلوماتية، وبالتالي عدم امكانية تطبيق النصوص الموضوعية التقليدية لقانون العقوبات، فرض حلها البحث في الاوضاع القانونية القائمة ومدى ملاءمتها لمواجهة هذه المشاكل.

ولعل من اهم الاساليب التي استحدثتها الدول والمجتمع الدولي، لمحاولة تفادي الوقوع في هذا النوع من الجرائم، تتمثل في وضع نصوص قانونية خاصة إلا أنها اختلفت في أسلوب المعالجة التشريعية لذلك، تماشيا والتطور التكنولوجي والمعلوماتي وتغلغله في جميع ميادين الحياة والتي أصبحت تشكل خطر على هذه المجتمعات، مادامت تهدد خصوصيات وأمن المعلوماتي لدول وأفراد على حد السواء (المبحث الاول).

كما تثير الجريمة المعلوماتية من جهة أخرى نظرا لخصوصيتها، مشكلة عدم كفاية إجراءات التحري والتحقيق التقليدية في الحصول على الدليل الرقمي الناتج عن ارتكابها، استدعى الدول الى التطوير في سياستها الجنائية من خلال التطوير في الاحكام العامة للاجراءات التقليدية، بصورة تتلاءم مع هذه الخصوصية وتمكن رجال الشرطة القضائية والمحقق من كشف الجريمة والتوصل إلى مرتكبيها والتحقيق معهم وجمع الادلة بالسرعة والدقة اللازمين، وتقديمهم للمحكمة، وعن طريق خلق إجراءات جديدة وحديثة للتحقيق والتحري مختلفة عن تلك المتبعة في سبيل مكافحة الجرائم العادية (المبحث الثاني).

المبحث الاول:
المواجهة الموضوعية للجريمة المعلوماتية

من المعلوم أن الاجرام المعلوماتي في بلادنا لم يتخذ نفس الابعاد المحققة في الدول المتقدمة، لكن هذا لا ينفي ضرورة التصدي لبوادره التي بدأت تتجلى للعيان، وهذا حتى لا

تستفحل هذه الوضعية مع وتيرة النمو المتسارع في استخدام النظم المعلوماتية، فضلا عن العولمة والتطور التكنولوجي الهائل، ما يوفر مناخا ملائما لانتهاك حرمة البيانات الشخصية والمساس بالامن الوطني.

وبالفعل فان المشرع الجزائري سارع لتدارك هذا الامر مؤخرا، فاستحدث أحكاما قانونية لحماية البرامج وهذا ضمن الامر رقم 97-10 المؤرخ في 1997/03/06المتعلق بحق المؤلف والحقوق المجاورة[56]، وتم تعديله بموجب الامر رقم 05/03 المؤرخ في 2003/07/19 المتعلق بحقوق المؤلف والحقوق المجاورة[57]، وكذا تعديل قانون العقوبات 04-15 المؤرخ في 2004/11/10 الذي عالج فيه المساس بأنظمة المعالجة الآلية للبيانات.

وعليه سنتناول في هذا المطلب مواجهة الجريمة المعلوماتية في إطار قانون العقوبات في (الفرع الأول)، ثم نتعرض إلى مواجهة الجريمة المعلوماتية في إطار نصوص الملكية الفكرية في (الفرع الثاني).

المطلب الأول:

المواجهة الموضوعية للجريمة المعلوماتية في إطار قانون العقوبات

لم يبق المشرع الجزائري بمنأى عن التحولات الجارية في تكنولوجيا المعلومات وما صاحبها من أفعال مجرمة، فاستحدث نصوصا تجريمية للحد من الاعتداءات الصادرة ضد الانظمة المعلوماتية.

فقد تمم المشرع قانون العقوبات، الفصل الثالث من الباب الثاني من الكتاب الثالث بالقانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، بقسم سابع مكرر 1 تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، احتوى على أهم الجرائم التي تستهدف الأنظمة المعلوماتية، وذلك في المواد من 394 مكرر إلى 394 مكرر 7. وضع من خلاله حماية فعالة لانظمة المعالجة الآلية للمعطيات، فنص على مجموعة من الجرائم مقررا لها عقوبات مناسبة للحد من اقترافها،

---

[56] الامر رقم 97-10 المؤرخ في 1997/03/06، المتعلق بحق المؤلف والحقوق المجاورة، ج ر، العدد 13، الصادرة في 1997/03/12.

[57] الامر رقم 03-05 المؤرخ في 2003/07/19، المتعلق بحق المؤلف والحقوق المجاورة، ج ر، العدد 44، الصادرة في 2003/07/23.

إلا أنه تجدر الاشارة إلى أن المشرع الجزائري في هذا التعديل ركز على الاعتداءات الماسة بالأنظمة المعلوماتية، وأغفل الاعتداءات الماسة بمنتوجات الاعلام الآلي والمتمثلة في التزوير المعلوماتي.

ومما سبق، يقتضي الامر منا التعرض الى مفهوم نظام المعالجة الالية للمعطيات في (الفرع الأول)،ثم أشكال الاعتداء على نظم المعالجة الآلية للمعطيات في (الفرع الثاني)، وعقوبات جرائم الاعتداء على نظم المعالجة الآلية للمعطيات في (الفرع الثالث).

الفرع الأول: مفهوم نظام المعالجة الآلية للمعطيات

يمثل نظام المعالجة الآلية للمعطيات المسالة الأولية أو الشرط الأولي الذي يلزم تحققه حتى يمكن البحث في توافر أو عدم توافر أركان أية جريمة من جرائم الاعتداء على هذا النظام. فان ثبت تخلف هذا الشرط الأولي، لا يكون هناك مجال لهذا البحث، ويؤدي توافر هذا الشرط إلى الانتقال إلى المرحلة التالية وهي بحث توافر أركان أية جريمة من الجرائم السابقة، إذ أن هذا الشرط يعتبر عنصر لازما لكل منها، ولذلك يكون من الضروري تحديد مفهوم نظام الآلية للمعطيات.

نظام المعالجة الآلية للمعطيات تعبير فني تقني يصعب على المشتغل بالقانون إدراك حقيقته بسهولة، فضلا عن انه تعبير متطور يخضع للتطورات السريعة والمتلاحقة في مجال فن الحاسبات الآلية[58].

ولذلك فالمشرع الجزائري على غرار التشريع الفرنسي لم يعرف نظام المعالجة الآلية للمعطيات فأوكل بذلك مهمة تعريفه كل من الفقه والقضاء.

أما الاتفاقية الدولية للإجرام ألمعلوماتي فقد قدمت تعريف للنظام المعلوماتي في مادتها الأولى على النحو التالي:" يقصد بمنظومة الكومبيوتر أي جهاز أو مجموعة من الأجهزة المتصلة ببعضها البعض أو التي ذات صلة بذلك، ويقوم أحدها أو أكثر من واحد منها، تبعا للبرنامج بعمل معالجة آلية للبيانات". أما الفقه الفرنسي فقد عرفه بأنه مجموع العمليات المنجزة

[58]علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، بيروت، 1999، ص ص 119-120.

بواسطة وسائل الاعلام الآلي المرتبطة بتجميع، تسجيل، إعداد، حفظ وتخريب معلومات اسمية وأيضا كل العمليات من طبيعة واحدة مرتبطة باستغلال الملفات أو قاعدة المعطيات وخاصة ربط أو تقريب أو فحص أو نشر معلومات اسمية[59].

بناء على التعريفات السابقة، تخلص إلى أن تعريف نظام المعالجة الآلية للمعطيات يتضمن عنصرين: الأول، مركب يتكون من عناصر مادية ومعنوية مختلفة ترتبط بينهما نتيجة علاقات توحدهما نحو تحقيق هدف محدد، والثاني ضرورة خضوع النظام لحماية فنية.

✓ **مكونات نظام المعالجة الآلية:**

وهذه العناصر المادية والمعنوية التي يتكون منها المركب واردة على سبيل المثال لا الحصر، وهذا يفتح المجال أمام إضافة عناصر جديدة أو حذف بعضها حسب ما يفرزه التطور التقني في هذا المجال، وعلى ذلك لا يتوافر نظام المعالجة الآلية للمعطيات، ولا تقع بالتالي أي جريمة من جرائم الاعتداء عليه المنصوص عليها إذا وقع الاعتداء على برامج معروضة للبيع، أو على جهاز حاسب لم يدخل الخدمة أو على عنصر مودع بالمخازن، أو على قطع الغيار، أو على الأجهزة التي مازالت في حالة التجربة، أو حتى الأنظمة التي خرجت من الخدمة تماما.و لكن على العكس من ذلك، تقع الجريمة إذا وقع الاعتداء على النظام خارج ساعات تشغيله العادية، أو إذا كانت أحد عناصره في حالة عطل أو حتى لو كان النظام كله في حالة عطل تام، و كان يمكن إصلاحه.

✓ **ضرورة خضوع النظام لحماية فنية:**

يسعى المتخصصون بأمن المعلومات للحفاظ على خصوصية البيانات المتناقلة عبر الشبكات وبالأخص شبكة الانترانت، فهم يسعون لتامين سرية الرسائل الالكترونية وسرية البيانات المتناقلة وخاصة بالأعمال التجارية الرقمية. ويمثل التشفير أفضل وسيلة للحفاظ على سرية البيانات المتناقلة.

وتنقسم أنظمة المعالجة الآلية إلى ثلاثة أنواع:

- أنظمة مفتوحة للجمهور.

[59] بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الولي والداخلي، أطروحة لنيل شهادة دكتوراه علوم تخصص قانون عام، كلية الحقوق، جامعة الجزائر1، 2017-2018، ص 155.

- أنظمة قاصرة على أصحاب الحق فيها ولكن بدون حماية فنية.
- أنظمة قاصرة على أصحاب الحق فيها وتتمتع بحماية فنية.

ومقتضى تطبيق هذا العنصر فإن النوع الثالث فقط من تلك الأنظمة هو الذي يتمتع بالحماية الجنائية أما النوع الأول والثاني فلا يتمتعان بتلك الحماية[60].

وهناك من يرى أن الحماية الجنائية يجب أن تقتصر على الأنظمة المحمية فنيا، لأنه من الطبيعي في نظرهم، أن من يقوم باستغلال نظام المعالجة الآلية للمعطيات، ويحقق ربحا من هذا الاستغلال، يضع الوسائل الفنية اللازمة لمنع الغش، وأن القانون الجنائي لا يحمي إلا الأشخاص الذين لديهم حرص على أموالهم، وليس من يهمل منهم في توفير الحد الأدنى لحماية أمواله[61].

وبالرجوع إلى النصوص المتعلقة بجرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات نجدها لا تتضمن شرط الحماية الفنية،وجاءت تلك النصوص خالية منه تماما.

ومن المبادئ العامة المستقرة في تفسير القانون الجنائي أنه لا يجوز تقييد النص المطلق، أو تخصيص النص العام، إلا إذا وجد نص يجيز ذلك. ولا يوجد في حالتنا نص خاص يقيد إطلاق النص أو يخصص عمومه، ولذلك فإن عدم ذكر المشرع لشرط الحماية الفنية يعني أن المشرع أراد استبعاده. هذا بالإضافة إلى أن الحماية الجزائية يجب أن تمتد لتغطي كل أنظمة المعالجة الآلية للمعطيات سواء كانت تتمتع بحماية فنية أم لا[62].

وتطبيقا لذلك، فإنه لا يشترط لوجود الجريمة أن يكون الدخول إلى النظام مقيدا بوجود حماية فنية ولكن إذا نظرنا للواقع، نلاحظ أن غالبية أنظمة المعالجة الآلية للمعطيات تتمتع بنظام حماية فنية، بالإضافة إلى أن وجود مثل تلك الحماية يساعد على إثبات أركان الجريمة وبصفة خاصة الركن المعنوي[63].

---

[60] علي عبد القادر القهوجي، مرجع سابق، ص 122.

[61] نفس المرجع، ص 123.

[62] أمال قارة، مرجع سابق، ص 105.

[63]– علي عبد القادر القهوجي، مرجع سابق، ص 123.

الفرع الثاني: أشكال الاعتداء على نظم المعالجة الآلية للمعطيات

لقد نص المشرع الجزائري على مجموعة من الافعال المجرمة من خلال المواد 394 مكرر، 394 مكرر 7 من ق.ع والتي يمكن تلخيصها كما يلي:

- الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات.
- الاعتداءات العمدية على نظام المعالجة الآلية للمعطيات.
- الاعتداءات العمدية على سلامة المعطيات الموجودة داخل النظام.

وسوف نتعرض لهذه الاعتداءات بالتفصيل فيما يلي:

أولا: جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات

نصت عليه المادة 394 مكرر من قانون العقوبات كما يلي:"يعاقب بالحبس من ثلاثة أشهر إلى سنة 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 عن ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج".

يقصد بفعل الدخول هنا وهو الركن المادي لجريمة الاعتداء على نظام المعالجة الالية للمعطيات، ذلك الدخول المعنوي أو الالكتروني باستعمال الوسائل الفنية والتقنية إلى النظام المعلوماتي، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات، فلا يقصد هنا بالدخول الدخول بالمعنى المادي.

ولم يحدد المشرع وسيلة الدخول أو الطريقة التي يتم الدخول بها إلى النظام، ولذلك تقع الجريمة بأية وسيلة أو طريقة. ويستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر، كما هو الحال في الدخول عن بعد من خلال شبكات الاتصال الهاتفية[64].

[64]علي عبد القادر القهوجي، مرجع سابق، ص 121.

ومن خلال المادة المذكورة اعلاه، نستشف أنه لا يعد فعل الدخول بحد ذاته سلوكا غير مشروع، وإنما يتخذ وصفه الاجرامي انطلاقا من كونه قد تم دون وجه حق أو غير مشروع أو دون ترخيص.

كما اعتبر المشرع من خلال ذات المادة جريمة الدخول دون وجه حق بمثابة جريمة سلوك التي لا يشترط لقيام الركن المادي فيها تحقق النتيجة الاجرامية، أي أنه جرم مجرد الدخول إلى نظام المعالجة الآلية للمعطيات بأكمله أو إلى جزء منه فقط، بشرط أن يكون فعل الدخول غير مشروع أي مقصودا وليس صدفة أو خطأ أو سهوا. فلم يتطلب فيها المشرع أية نتيجة اجرامية. وحسنا فعل المشرع عندما جرم مجرد الدخول إلى نظام المعالجة الآلية للمعطيات عن طريق الغش وبغض النظر عن ما إذا كان النظام المتعدى عليه محاطا بحماية فنية أم لا، وبهذا يكون قد جعل من هذا التدبير بمثابة تدبير وقائي سيساهم في التصدي لظاهرة الاجرام المعلوماتي.

أما فيما يخص فعل البقاء داخل النظام فيقصد به استمرارية التواجد داخل نظام المعالجة دون إذن من صاحبه أو من له السيطرة عليه، بمعنى آخر هو بقاء شخص داخل نظام المعالجة ملك الغير بعد الدخول إليه خطأ أو صدفة، رغم علمه بأن بقاءه فيه غير مرخص[65].

فقد اعتبر المشرع الجزائري من خلال المادة 394 مكرر من ق.ع فعل البقاء غير المرخص به داخل النظام جريمة مثلها مثل جريمة الدخول غير المشروع، وحدد لهما نفس العقوبة.

كما نصت المادة 394 مكرر الفقرة 2، 3 من قانون العقوبات على ظرفين تشدد بهما عقوبة جريمة الدخول والبقاء داخل النظام، ويتحقق هذان الظرفان عندما ينتج عن الدخول أو البقاء إما محو أو تعديل البيانات التي يحتويها النظام، وإما عدم صلاحية النظام لأداء وظائفه.ويكفي لتوفر هذا الظرف وجود علاقة سببية بين فعل الدخول غير المشروع أو البقاء غير المشروع وتلك النتيجة الضارة التي حددتها المادة في محو أو تعديل بيانات النظام أو تخريب تشغيل النظام ذاته[66].

---

[65] قارة أمال، مرجع سابق، ص 44.

[66] خثير مسعود، الحماية الجنائية لبرامج الكومبيوتر في التشريع الجزائري، دار الهدى، الجزائر، 2010، ص 119.

ثانيا: جريمة الاعتداء على سير نظام المعالجة الآلية للمعطيات

لم يورد المشرع الجزائري نصا خاصا بالاعتداء على سير النظام واكتفى بالنص على الاعتداء على المعطيات الموجودة بداخل النظام، وربما يجد ذلك تفسيره في أن الاعتداء على المعطيات قد يؤثر على صلاحية النظام للقيام بوظائفه. غير أنه يمكن استخلاص ذلك من خلال النصوص التي استحدثها بخصوص تجريم الاعتداءات الواقعة على أنظمة المعالجة أو على معطيات هذه الانظمة سواء كانت معطيات داخلية أم خارجية.

فالاعتداء على النظام بتخريبه كما نصت المادة 394 مكرر من ق.ع من شأنه أن يعيب سير النظام، والاعتداء على المعطيات الداخلية للنظام باستعمال برامج الفيروسات وبرامج القنابل المعلوماتية من شأنه كذلك التأثير في سير أو حسن سير النظام المعلوماتي[67].

ويمكن أن تتخذ الافعال الماسة بسير النظام عدة صور نذكر منها:

-**التعطيل أو التوقيف:** إن التعطيل قد يقع بأي وسيلة، فالمشرع لم يشترط طريقة معينة لحصول الإعاقة، فقد تكون بطريقة مادية أو معنوية. فالتعطيل يمكن أن يصيب الاجهزة المادية للنظام كتحطيم الاسطوانات أو قطع شبكة الاتصال أو يصيب الكيانات المنطقية للنظام كالبرامج أو المعطيات باستخدام برنامج فيروسي مما يؤدي إلى عرقلة سير النظام.

- **الإفساد أو التعييب:** ويقصد به كل فعل وإن كان لا يؤدي إلى التعطيل لكنه يؤدي إلى جعل نظام المعالجة الآلية للمعطيات غير صالح للاستعمال السليم، وذلك بأن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها[68].

ثالثا: جريمة الاعتداء على معطيات المعالجة الآلية

يقصد بالاعتداء هنا ذلك الاعتداء الذي يهدف إلى الاضرار بمعلومات الكومبيوتر أو وظائفه سواء بالمساس بسريتها أو المساس بسلامة محتوياتها، تكاملها أو بتعطيل قدرة وكفاءة

[67] ونوغي نبيل، زيوش عبد الرؤوف، الجريمة المعلوماتية في التشريع الجزائري، مجلة العلوم القانونية والاجتماعية، المجلد الرابع، العدد الثالث، جامعة زيان عاشور بالجلفة-الجزائر،سبتمبر 2019، ص 136.

[68] بدري فيصل، مرجع سابق، ص 171.

الانظمة بشكل يمنعها من أداء وظيفتها بشكل سليم[69]، يتحقق الاعتداء على معطيات المعالجة الآلية عادة بعد مرحلة الدخول والبقاء في النظام، ويتخذ أحد الشكلين التاليين:

✓ **الاعتداء على المعطيات الداخلية للنظام:**

لقد جرم المشرع الجزائري في المادة 394 مكرر 1 من ق.ع[70] أي إعتداء على المعطيات الموجودة داخل نظام المعالجة الآلية، وحدد من خلال ذات المادة صور الاعتداء على معطيات النظام الداخلية على سبيل الحصر، ما يعني أن أي اعتداء لا يحمل إحدى هذه الصور، الادخال، المحو أو التعديل لا يخضع لاحكام المادة 394 مكرر 1.

فالبنسبة للإدخال: يقصد بفعل الإدخال إضافة معطيات جديدة غير صحيحة إلى المعطيات الموجودة داخل النظام والتي تمت معالجتها آليا[71].

أما المحو: يقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة موجودة داخل النظام أو تحطيم تلك الدعامة، أو نقلوتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة[72].

أما التعديل: يقصد به تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى.

ولا يشترط اجتماع هذه الصور، بل يكفي أن يصدر عن الجاني إحداها فقــط لكي يتوافر الركــن المــادي لجريمة الاعتداء على معطيات نظام المعالجة.

✓ **الاعتداء على المعطيات الخارجية للنظام:**

يقصد بالمعطيات الخارجية لنظام المعالجة تلك المعطيات التي لها دور في تحقيق نتيجة معينة تتمثل في المعالجة الآلية للمعطيات.

---

[69] ونوغي نبيل، زيوش عبد الرؤوف، مرجع سابق، ص 134.

[70] تنص المادة 394 مكرر 1 من ق.ع على أنه:" يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريقة الغش معطيات في نظام المعالجة الآلية أو أزال أو عدّل بطريق الغش المعطيات التي يتضمنها".

[71] ونوغي نبيل، زيوش عبد الرؤوف، مرجع سابق، ص 135.

[72] بدري فيصل، مرجع سابق، ص 176.

وقد نص عليها المشرع الجزائري في المادة 394 مكرر2من قانون العقوبات كما يلي:" يعاقب بالحبس من شهرين إلى 3 سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج كل من يقوم عمدا أو عن طريق الغش بما يأتي:

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

2-حيازة أو إفشاء أو نشر أو إستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

الفرع الثالث: عقوبات جرائم الاعتداء على نظم المعالجة الآلية للمعطيات

سنتناول في هذا الفرعالجزاءات التي قررها المشرع الجزائري لهذا النوع من الإجرام الحديث، والتي تتمثل في عقوبات أصلية وعقوبات تكميلية تطبق على الشخص الطبيعي، كما توجد عقوبات تطبق على الشخص المعنوي، وأيضا عقوبة المساهم والشريك في الجريمة كما يلي:

أولا: العقوبات الأصلية:

أ- العقوبات المقررة للشخص الطبيعي:

من خلال استقراء النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية يتبين لنا وجود تدرج داخل النظام العقابي. هذا التدرج في العقوبات يحدد الخطورة الإجرامية التي قدرها المشرع لهذه التصرفات،إذ نجد سلم خطورة يتضمن ثلاث درجات،جريمة الدخول أو البقاء بالغش في الدرجة الأولى وبعدها في الدرجة الثانية جريمة الدخول والبقاء المشددة،أما الدرجة الثالثة فتحتلها الجريمة الخاصة بالاعتداءالعمدي على المعطيات.

- ✓ **عقوبة الدخول أوالبقاء بالغش داخل النظام (الصورة البسيطة للجريمة):**

حدد المشرع عقوبة هذه الجريمة بالحبس من 3 أشهر إلى سنة والغرامة من 50.000 دج إلى 100.000 دج غرامة (المادة 394 مكرر من ق.ع).

✓ **الدخول أوالبقاء بالغش داخل النظام (الصورة المشددة للجريمة):**

تضاعف العقوبة إذا ترتب عن هذه الأفعال حذف أو تغيير معطيات النظام،وتكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج إذا ترتب عن الدخول أو البقاء غير المشروع تخريب لنظام اشتغال المنظومة (المادة 394 مكرر فقرة 2 و3 من ق.ع).

✓ **الاعتداء العمدي على المعطيات:**

حدد المشرع عقوبة الاعتداء على المعطيات الموجودة داخل النظام في المادة 394 مكرر 1من ق.ع، بالحبس من ستة أشهر إلى ثلاث سنوات وغرامة من 500.000 دج إلى 2.000.000 دج.

كما عمل على حماية خصوصية الافراد، حيث أقر عقوبة لاستخدام المعطيات في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية، وكذا حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية، طبقا للمادة 394 مكرر 2 من ق.عهي الحبس من شهرين إلى ثلاث سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج.

ب- **العقوبات المقررة الشخص المعنوي:**

أقر المشرع الجزائري مبدأ مساءلة الشخص المعنوي في القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 وذلك بموجب المادة 51 مكرر منه، كما حدد ثلاثة شروط لإمكان مساءلة الشخص المعنوي جنائيا تتمثل في:

- أن ترتكب إحدى الجرائم المنصوص عليها قانونا.
- أن تكون بواسطة أحد أعضاء أو ممثلي الشخص المعنوي.
- أن ترتكب الجريمة لحساب الشخص المعنوي.

كما نص في المادة 18 مكرر من نفس القانون على:" العقوبات التي تطبق على الشخص المعنوي في مواد الجنايات هي:

– الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.

– واحدة أو أكثر من العقوبات التكميلية الآتية:

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

من هذا المنطلق، أقر المشرع عقوبة على الشخص المعنوي عند ارتكابه أحد جرائم الاعتداء على نظام المعالجة الآلية للبيانات في المادة 394 مكرر 4 من قانون العقوبات، حيث جاء فيها مايلي:" يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي".

ج: عقوبة الاشتراك والشروع في الجريمة

ج.أ– عقوبة الاشتراك:

أقر المشرع الجزائري المعاقبة على الاتفاق الجنائي بنص المادة 394 مكرر 5 من ق.ع، بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية، والتي تنص على أنه:" كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل اوبعدة أفعال مادية،يعاقب بالعقوبات المقررة بالجريمة ذاتها ".

فالمشرع الجزائري يعاقب على الاشتراك في الاتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها، فإذا تعددت الجرائم التي يتم التحضير لها تكون العقوبة هي عقوبة الجريمة الأشد[73].

وشروط المعاقبة على الاتفاق الجنائي بمكن استخلاصها من نص المادة 394 مكرر 5 من قانون العقوبات، والتي هي:

- مجموعة أو اتفاق.
- بهدف تحضير جريمة من الجرائم الماسة بالأنظمة المعلوماتية.
- تجسيد هذا التحضير بفعل مادي.
- فعل المشاركة في هذا الاتفاق.
- القصد الجنائي.

ج.ب- عقوبة الشروع في الجريمة:

نص عليه المشرع الجزائري في المادة 394 مكرر 7 من قانون العقوبات. فالجرائم الماسة

بالأنظمة المعلوماتية لها وصف جنحي ولا عقاب على الشروع في الجنح إلا بنص[74].

وتنص المادة 394 مكرر 7 على ما يلي:" يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها ".

والملاحظ أن المشرع وسع في نطاق العقوبة لتشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية بجعل الشروع في إحدى الجرائم الماسة بالأنظمة المعلوماتية معاقب عليه بنفس عقوبة الجريمة التامة من أجل مكافحة هذه الجريمة المستحدثة، والتي تمس بأمن الدولة والأفراد على حد السواء.

[73] أمال قارة، مرجع سابق، ص 131.

[74] بدري فيصل، مرجع سابق، ص182.

.

ثانيا: العقوبات التكميلية

نصت المادة 394 مكرر 3 من قانون العقوبات على العقوبات التكميلية إلى جانب العقوبات الأصلية والمتمثلة في:

أ/ المصادرة: وهي عقوبة تكميلية تشمل الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالأنظمة المعلوماتية، مع مراعاة حقوق الغير حسن النية.

ب/ إغلاق المواقع: والأمر يتعلق بالمواقع التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية.

ج/ إغلاق المحل أو مكان الاستغلال: إذا كانت الجريمة قد ارتكبت بعلم مالكها ومثال ذلك إغلاق المقهى الالكتروني الذي ترتكب منه مثل هذه الجرائم شرط توفر عنصر العلم لدى مالكها.

وتجدر الاشارة إلى ان الحماية الجنائية للمعلوماتية من خلال المواد المذكورة اعلاه من القانون رقم 15/04 المتضمن قانون العقوبات، تعتبر فعالة لشمولها أغلب الجرائم التي قد تمس نظام المعالجة الآلية للمعطيات، وكذا الجرائم التي قد تمس البيانات والمعطيات المكونة لهذا النظام.

المطلب الثاني:
المواجهة التشريعية في إطار نصوص خاصة

بالرغم من تبني المشرع نصوصا تشريعية حديثة لحماية المكونات المعنوية للنظام المعلوماتي إلا أنه لم يوفق بالاحاطة الشاملة لكل الجرائم المعلوماتية مثل جريمة التزوير المعلوماتي التي تكتسي أهمية خاصة مع انتشار ثقافة استخدام الكومبيوتر فيما بين الأفراد، بالاضافة إلى هذا يعاب كذلك على المشرع أنه بالرغم من وضعه لنصوص عقابية رادعة ووقائية إلا أنها تبقى غير قابلة للتطبيق كونها تحتاج إلى نصوص إجرائية تلازمها نظرا لما تمتاز به الجريمة المعلوماتية من خصوصية تختلف عن باقي الجرائم، وهو ما دفع المشرع إلى إصدار مجموعة من القوانين الخاصة لمواجهة الجريمة المعلوماتية على اختلافها منها المباشرة وغير المباشرة، نذكر منها:

الفرع الأول: القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها

تضمنها القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتهاحيث تدارك المشرع الفراغ التشريعي في مجال مكافحة الجريمة المعلوماتية من خلال هذا القانون المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

وقد أورد المشرع في المادة 2 من القانون رقم 09-04 أنه يقصد بالجرائم المتصلة بتكنولوجيات الاعلام والاتصال، جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية.

كما تضمن القانون المذكور في الفصل الرابع منه القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، في المادتين 10 و11، على أنه من بين التزامات مقدمي الخدمات مساعدة السلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبحفظ المعطيات المتعلقة بحركة السير ووضعها تحت تصرف السلطات المذكورة.

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحقيقين، وكذا المعلومات المتصلة بها تحت طائلة العقوبات المقررة لإغشاء أسرار التحري والتحقيق، بينما فصلت المادة 11 في إجراء حفظ المعطيات المتعلقة بخط السير، مع الاشارة الى قيام المسؤولية الجزائية للاشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من 6 أشهر إلى 5 سنوات وبغرامة من 50.000 دج إلى 500.000 دج، ويعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات.

الفرع الثاني: القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية

حددها القانون رقم 2000-03 المؤرخ في 5 أوت 2000 [75]، وقد تناول المشرع في الفصل الثاني من القانون تعريفات تتعلق بالمواصلات السلكية واللاسلكية منها الامواج اللاسلكية واللاسلكية الشبكة الخاصة والشبكة العامة وخدمة الهاتف وخدمة التلكس والخدمات البريدية وأطرافها من مرسل ومرسل إليه وغيرها من المصطلحات التي تم استخدامها في هذا القانون، وهذا لمنع أي لبس حول مفهومها، كما تضمن الجرائم المعلوماتية والعقوبات، وتتمثل في:

- فتح أو تحويل أو تخريب البريد أو إنتهاك سرية المراسلات أو المساعدة على ارتكاب هذه الأفعال من قبل كل شخص يقوم بتقديم خدمة البريد السريع الدولي أو كل عون يعمل لديه وفي إطار ممارستهم لمهامهم، كل شخص مرخص له بتقديم خدمة مواصلات سلكية ولاسلكية، وكل عامل لدى متعاملي الشبكات العمومية للمواصلات السلكية واللاسلكية وأثناء ممارستهم لمهامهم وغيرهم (المادة 127 من القانون).

- إنشاء أو استغلال شبكة عمومية للمواصلات السلكية واللاسلكية دون رخصة أو مواصلة ممارسة النشاط خرقا لقرار التعليق أو سحب هذه الرخصة (المادة 131 من القانون).

- إنشاء أو العمل على إنشاء شبكة مستقلة دون ترخيص (المادة 132 من القانون).

- إشهار بغرض بيع تجهيزات أو معدات للمواصلات السلكية واللاسلكية دون الحصول على الاعتماد المسبق (المادة 133 من القانون).

- تحويل أو العمل على تحويل أو إستغلال خطوط المواصلات السلكية واللاسلكية المحولة (المادة 135 من القانون).

الفرع الثالث:القواعد العامة المتعلقة بحقوق المؤلف والحقوق المجاورة

أدت القفزة الرقمية التي حدثت في العالم إلى إحداث أثر بالغ على كافة جوانب الحياة وكان لها أثر بالغ على الملكية الفكرية خاصة في مجال حقوق المؤلف حيث أصبح نشر

[75] قانون رقم 2000-03 المؤرخ في 5 أوت 2000 يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، العدد 48، الصادرة في 06 أوت 2000.

وتوزيع وعرض المصنفات غاية في السهولة والإتقان وبأقل التكاليف بظهور الحاسبات الآلية، مما أدى إلى مسايرة هذه التطورات لظهور ما يسمى بالملكية الرقمية والتي تشمل حقوق الملكية الفكرية على الانترنت والتي مضمونها يشمل كل مصنف ابداعي ينتمي الى بيئة تقنية المعلومات يعد مصنفا رقميا[76].

ولهذا سارع المشرع الجزائري على غرار التشريعات الأخرى إلى حماية هذه المصنفات بتطويع النصوص التقليدية الخاصة بحماية الملكية الفكرية الذي قام بإخضاع حماية المال المعلوماتي (برامج الحاسب الآلية) لقوانين الملكية الفكرية[77] حيث اعتبر برنامج الحاسوب الآلي ضمن المصنفات الأدبية والفنية بموجب المادة الرابعة من الأمر رقم 05/03 المؤرخ في 2003/07/19المتعلق بحقوق المؤلف والحقوق المجاورة[78] والتي تنص على أنه:" تعتبر على الخصوص كمصنفات أدبية أو فنية محمية ما يأتي:

أ- المصنفات الأدبية المكتوبة مثل: المحاولات الأدبية والبحوث العلمية والتقنية، والروايات والقصص، والقصائد الشعرية، وبرامج الحاسوب، ...".

وهو محمي بالأمر 05/03 ذاته فالحقوق المالية أو المادية هي الإطار الذي يمكن صاحب البرنامج من استغلاله بأي طريقة دون غيره، أو لمن يخوله هو نفسه هذا الحق وله في ذلك وفقا لأحكام المادة 27 من الأمرالمشار له إبلاغه للجمهور بأية منظومة معالجة معلوماتية ويترتب عن ذلك حقوق مادية للمؤلف صاحب البرنامج بالاستغلال التجاري له ولورثته بمختلف الطرق وهذا ما يستخلص من نص المادة 3 من نفس الأمر[79].

وقد بسط المشرع الجزائري حمايته على برامج الحاسبات الآلية مدرجا إياها تحت نطاق حقوق المؤلف تماشيا مع إتفاقية "برن" الدولية التي صادقت عليها الجزائر بموجب المرسوم الرئاسي 341/97 المؤرخ في 1997/09/13 حيث بموجب هذه الاتفاقية تبسط الحماية على حقوق المؤلف وبالتالي عللا البرامج مدة 50 سنة ابتداء من مطلع السنة الميلادية التي تلي نشر

---

[76] طرشي نورة، مرجع سابق، ص 49.

[77] نفس المرجع.

[78] ج ر ج ج، العدد 44، الصادرة في 23 يوليو 2003.

[79] زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار هومة، الجزائر، 2011، ص 88.

المصنف (المادة 1/58 من الامر 05/03 السالف الذكر) ومدة 50 سنة ابتداء من مطلع السنة الميلادية التي تلي تاريخ وفاة المؤلف تماشيا مع نص المادة السابعة من اتفاقية "برن"[80].

كما أن المشرع وسع قائمة المؤلفات المحمية حيث أدمج تطبيقات الإعلام الآلي ضمن المصنفات الأصلية، حيث عبر عنها بمصنفات قواعد البيانات وبرامج الإعلام الآلي، والتي تمكن من القيام بنشاط علمي أو أي نشاط من نوع آخر أو الحصول على نتيجة خاصة من المعلومات التي تقرأ بآلة وتترجم باندفاعات إلكترونية بالحاسوب[81].

وفي سبيل تقرير حماية جنائية فعالة في هذا المجال عدد المشرع مجموعة من الأفعال الماسة بالمصنفات وبحقوق مؤلفيها وجرمها، وجعل مرتكبيها يشكلون خرقا لحقوق المؤلف تجب معاقبته من اقترافها. ومن الجرائم المعلوماتية التي جاء بها الأمر رقم 05/03 المتعلق بحقوق المؤلف والحقوق المجاورة ما يلي:

– ارتكاب جنحة التقليد عن طريق: الكشف غير المشروع للمصنف أو المساس بسلامة مصنف أو أدء لفنان مؤد أو عازف، استنساخ مصنف أو أداء بأي أسلوب من الأساليب في شكل نسخ مقلدة، استيرد أو تصدير نسخ مقلدة من مصنف أو أداء، بيع نسخ مقلدة لمصنف أو أداء، تأجير أو وضع رهن التداول لنسخ مقلدة لمصنف أو أداء (المادة 151 من الامر 05/03).

– ارتكاب جنحة التقليد عن طريق: انتهاك الحقوق المحمية بموجب هذا الأمر فيبلغ المصنف أو الأداء عن طريق أي منظومة معالجة معلوماتية (المادة 152 من نفس الأمر).

– الإشتراك بالعمل أو بالوسائل الحائز عليها للمساس بحقوق المؤلف أو أي مالك للحقوق المجاورة (المادة 154 من نفس الأمر).

أما بالنسبة للعقوبات المقررة على مختلف هذه الاعتداءات فقد تضمنتها المواد 153، 156، 157، 158، 159 من الأمر السالف الذكر. وتتمثل العقوبة لمرتكب جنحة التقليد لمصنف أو أداء فني كما هو وارد في المادتين 151 و152 من ذات الأمر بالحبس من 6 أشهر إلى ثلاثة سنوات، وبغرامة من خمسة مئة ألف (500.000 دج) إلى مليون دينار جزائري

[80] طرشي نورة، مرجع سابق، ص 50.

[81] بدري فيصل، مرجع سابق، ص140.

(1.000.000 دج)، سواء كان النشر قد حصل في الجزائر أو خارجها طبقا للمادة 153 من نفس الامر.

كما نص في المادة 154 من نفس الامر على معاقبة الشريك في ارتكاب جريمة التقليد سواء بأعماله أم بالوسائل التي يحوزها للمساس بحقوق المؤلف بنفس العقوبات المقررة في المادة 153 من الامر السالف الذكر. ونفس الشيء بالنسبة لكل من يمتنع عن دفع المكافأة المستحقة للمؤلف (المادة 155 من ذات الأمر).

وقد شدد المشرع العقوبة في حالة العود إلى ضعف العقوبة المقدرة في المادة 153 من الامر 05/03 المشار اليه سابقا طبقا للمادة 156 من نفس الأمر.

بالاضافة الى هذه العقوبات الأصلية قرر المشرع كذلك لهذه الجرائم العقوبات التكميلية التي تتمثل في الغلق المؤقت لمؤسسة يستغلها المقلد أو شريكه، والمصادرة سواء مصادرة المبالغ التي تمثل الايرادات الناتجة عن الاستغلال غير الشرعي لمصنف أو أداء محمي طلقا للمادة 157 من الأمر 05/03، وكذلك نشر حكم الإدانة وفقا لأحكام المادة 158 من نفس الأمر.

المبحث الثاني:

المواجهة الاجرائية للجريمة المعلوماتية في التشريع الجزائري

وضعت الجرائم المعلوماتية نظرا لطبيعتها الخاصة كونها غير مادية، عقبات شديدة أمام القائمين على التحريات والتحقيقات الجنائية لجمع الأدلة الناتجة عن هذه الجرائم، إذ يصعب على المحقيقين إجراء تحقيق وجمع الادلة الرقمية، بإتباع الاجراءات التقليدية للتحقيق، كالمعاينة، التفتيش، الضبط...إلخ. الامر الذي استلزم على بعض الدول النص على إجراءات خاصة في جمع الأدلة عن جرائم الحاسوب تختلف عن تلك المتبعة في الجرائم التقليدية، وعلى التكوين الفني والتقني للمتخصصين في مجال التحريات والتحقيقات.

وفي هذا السياق ورغبة منها في مكافحة فعالة للجريمة المعلوماتية، تبنت كذلك الجزائر أساليب جديدة للتحري من خلال تعديل قانون الاجراءات الجزائية بموجب القانون رقم

06-22 بتاريخ 20 ديسمبر 2006، عن طريق إضافة إجراءات جديدة تطبق على جرائم المساس بأنظمة المعالجة الآلية للمعطيات (المطلب الأول).

وكذا القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، من خلاله خلق المشرع آليات جديدة خاصة للتحري محاولة منه تطويقها والقضاء عليها أو على الأقل الحد من انتشارها (المطلب الثاني).

المطلب الأول:
المكافحة الإجرائية في ظل قانون الاجراءات الجزائية

تماشيا مع التطور المعلوماتي الذي لحق بالجريمة نص قانون الاجراءات الجزائية على مجموعة من إجراءات التحري والتحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ووضع قواعد وأحكام خاصة لسلطة المتابعة والاختصاص قصد مواجهة الجريمة.

وعليه، سنتناول في هذا المطلب توسيع الاجراءات الخاصة بالاختصاص في هذه الجريمة، التفتيش، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، التسرب، في الفروع التالية:

الفرع الأول: توسيع الاجراءات الخاصة بالاختصاص في الجرائم المعلوماتية

نصت المادة 329 من قانون الاجراءات الجزائية في فقرتها الاخيرة على جواز تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعلومات.

كما أنشئت الأقطاب الجزائية المتخصصة[82] بموجب القانون رقم 14/04 المؤرخ في 10 نوفمبر 2004 المعدل لقانون الاجراءات الجزائية، من بين الجرائـــم التي تختص بها الجرائم

[82] يعني إنشاء جهات متخصصة داخل نطاق التنظيم القضائي الساري المفعول، تطبق الاجراءات القانونية المنصوص عليها في القانون العام، فهي جهات قضائية متخصصة وليست جهات قضائية خاصة تنشط بإجراءات قانونية خاصة. راجع: كور طارق، آليات مكافحة جريمة الصرف، مذكرة لنيل شهادة ماجستير، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي- أم البواقي، الجزائر، جوان 2012، ص 137.

الماسة بأنظمة المعالجة الآلية للمعطيات (طبقا للمواد 37 و40 و329 من ق.إ.ج).

كذلك نظم المشرع الجزائري في القانون 04/09 المؤرخ في 5 أوت 2009 أحكاما جديدة خاصة بالاختصاص في مجال الجريمة المعلوماتية تتماشى والتطور الذي لحق الجريمة، حيث جاء في المادة 15 منه أنه:" زيادة على قواعد الاختصاص المنصوص عليها في قانون الاجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية والدفاع الوطني أو المصالح الاستراتيجية للإقتصاد الوطني".

كما وسع مجال إختصاص النيابة العامة، وذلك بموجب المادة 37 من ق.إ.ج ليشمل نطاقات أخرى لم يكن مرخصا لها بها من قبل، حيث نصت هذه المادة على تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

كذلك سحب نظام الملاءمة من النيابة العامة في مجال متابعة بعض الجرائم، إذ يلتزم وكيل الجمهورية بتحريك الدعوى العمومية بقوة القانون بحيث لا يتمتع بشأنها بسلطة الملاءمة بين تحريك الدعوى العمومية وعدم تحريكها مثلما فعل في الجرائم المنصوص عليها في المواد 144 مكرر و144 مكرر 1 و144 مكرر 2 من قانون العقوبات المعدل والمتمم بالقانون 09/01 المؤرخ في 26 يونيو 2001[83].

الفرع الثاني: التفتيش

يكتسي التفتيش أهمية بالغة في البحث عن الأدلة والكشف عن الحقيقة لكنه بالمقابل اجراء خطير نظرا لمساسه بحريات الاشخاص وكرامتهم وممتلكاتهم لذلك فقد أحاطه المشرع بتنظيم خاص.

[83] طرشي نورة، مرجع سابق، ص 134.

يختلف التفتيش في الجريمة المعلوماتية عن التفتيش المتعارف عليه في الجرائم العادية، فهذا الاخير ينصب على الاشخاص والممتلكات أما التفتيش في الجريمة المعلوماتية فيتعدى الاشخاص والممتلكات إلى المنظومة المعلوماتية في حد ذاتها.

أ- تفتيش وضبط الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في حالات التلبس بالجريمة[84]:

ويكون ذلك وفقا للقواعد التالية:

- الحصول على إذن مسبق من قبل السلطة القضائية المختصة:

نصت المادة 44 من ق.إ.ج على أنه:" لا يجوز لضابط الشرطة القضائية الانتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية أو أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء تفتيش إلا بإذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب الاستظهار بهذا الأمر قبل الدخول إلى المنزل والشروع في التفتيش.

ويكون الأمر كذلك في حالة التحري في الجنحة المتلبس بها أو التحقيق في إحدى الجرائم المذكورة في المادتين 37 و40 من هذا القانون.

يجب أن يتضمن هذا الإذن المسبق بيان وصف الجرم موضوع البحث عن الدليل وعنوان الأماكن التي سيتم زيارتها وتفتيشها وإجراء الحجز فيها، وذلك تحت طائلة البطلان. تنجز هذه العمليات تحت الإشراف المباشر للقاضي الذي أذن بها والذي يمكنه عند الاقتضاء أن ينتقل إلى عين المكان للسهر على إحترام أحكام القانون.

إذا اكتشفت أثناء هذه العمليات جرائم أخرى غير تلك التي ورد ذكرها في إذن القاضي فإن ذلك لا يكون سببا لبطلان الإجراءات العارضة".

---

[84]تنص المادة 41 من ق,إ.ج على مايلي:" توصف الجناية أو الجنحة بأنها في حالة تلبس إذا كانت مرتكبة في الحال أو عقب ارتكابها.

كما تعتبر الجناية أو الجنحة متلبسا بها إذا كان الشخص المشتبه في ارتكابه إياها في وقت قريب جدا من وقت وقوع الجريمة قد تبعه العامة بصياح أو وجدت في حيازته أشياء أو وجدت آثار أو دلائل تدعو إلى إفتراض مساهمته في الجناية أو الجنحة.

وتتسم بصفة التلبس كل جناية أو جنحة وقعت ولو في غير الظروف المنصوص عليها في الفقرتين السابقتين، إذا كانت قد ارتكبت في منزل وكشف صاحب المنزل عنها عقب وقوعها وبادر في الحال باستدعاء أحد ضباط الشرطة القضائية لإثباتها".

– حضور صاحب المسكن أثناء عملية التفتيش والضبط في الجرائم الماسة بأنظمة المعالجة الآلية للمعلومات:

يخضع التفتيش والضبط في هذه الجرائم وبعض الجرائم المنصوص عليها على سبيل الحصر في المادة 3/47 من ق.إ.ج، لقواعد خاصة تختلف عن القواعد العامة المقررة في الفقرتين 1 و2 من المادة 45 من نفس القانون[85]، وتختلف هذه القواعد حسب حالتين:

الأولى: إذا تعلق الأمر بالتحقيق التمهيدي في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، فإن ضابط الشرطة القضائية بموجب الفقرة الأخيرة من المادة 45 من ق.إ.ج لم يعد القائم بالتفتيش مقيدا عند إجراء تفتيش المساكن والمحلات بالشرط المتعلق بضرورة حضور المشتبه فيه أو من ينوبه أو شاهدين إذا جرى التفتيش في مسكنه، أو حصل في مسكن شخص آخر يشتبه بأنه يحوز أوراقا أو أشياء لها علاقة بالجريمة، حيث تنص المادة المذكورة على أنه:" لا تطبق هذه الأحكام إذا تعلق الأمر ... والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات...".

الثانية: أصبح لضابط الشرطة القضائية بموجب المادة 47 مكرر المستحدثة في ق.إ.ج إذا تعلق التحقيق التمهيدي الذي يجريه بجريمة متلبس بها أو تحقيق متعلق بإحدى أنواع الجرائم السابقة الذكر، أن يجري التفتيش بعد الموافقة المسبقة من وكيل الجمهورية أو قاضي التحقيق بحضور شاهدين مسخرين من غير الموظفين الخاضعين لسلطته أو بحضور ممثل يعينه صاحب المسكن محل التفتيش، إذا كان الشخص الذي يتم تفتيش مسكنه موقوفا للنظر أو محبوسا في مكان آخر وأن الحال يقتضي عدم نقله إلى ذلك المكان بسبب مخاطر جسيمة قد تمس بالنظام العام أو لاحتمال فراره أو اختفاء الأدلة خلال المدة اللازمة لنقله.

---

[85]تنص المادة 45 على أنه:" تتم عملية التفتيش التي تجري طبقا للمادة 44 أعلاه على الوجه الآتي:
1- إذا وقع التفتيش في مسكن شخص يشتبه في أنه ساهم في ارتكاب الجناية فإنه يجب أن يحصل التفتيش بحضوره، فإذا تعذر عليه الحضور وقت إجراء التفتيش فإن ضابط الشرطة القضائية ملزم بأن يكلفه بتعيين ممثل له. وإذا إمتنع عن ذلك أو كان هاربا استدعى ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته.
2- إذا جرى التفتيش في مسكن شخص آخر يشتبه بأنه يحوز أوراقا أو أشياء لها علاقة بالأفعال الاجرامية فإنه يتعين حضوره وقت إجراء التفتيش، وان تعذر ذلك اتبع الإجراء المنصوص عليه في الفقرة السابقة.
ولضابط الشرطة القضائية وحده مع الاشخاص السابق ذكرهم في الفقرة الاولى اعلاه الحق في الإطلاع على الأوراق أو المستندات قبل حجزها".

أما فيما يخص المواعيد فقد استثنى المشرع الجزائري إخضاع التفتيش في الجريمة المعلوماتية وتقييده بحدود زمنية وخول للمكلف بهذا الإجراء القيام به في أي وقت من أوقات الليل أو النهار طبقا للمادة 3/47 من ق.إ.ج.

ب- التفتيش والضبط في الجرائم المعلوماتية في مرحلة التحقيق الابتدائي

نصت المادة 64 من ق.إ.ج أنهلا يجوز تفتيش المساكن ومعاينتها وضبط الاشياء المثبتة للتهمة إلا برضا صريح ومكتوب بخط اليد من الشخص الذي ستتخذ لديه هذه الاجراءات، فان كان لا يعرف الكتابة بإمكانه الاستعانة بشخص يختاره بنفسه، ويذكر ذلك في المحضر، مع ضرورة التقيد بالاحكام المنصوص عليها في المواد من 44 إلى 47 من ق.إ.ج. أما عندما يتعلق الأمر بالتحقيق في إحدى الجرائم المنصوص عليها في المادة 3/47 من نفس القانون فإنه تطبق الأحكام الواردة في تلك المادة وكذا أحكام المادة 47 مكرر من هذا القانون.

ج- **التفتيش والضبط في الجرائم المعلوماتية في مرحلة التحقيق القضائي**

تضمنت المادة 79 من ق.إ.ج على أنه يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، مع الاستعانة بكاتب التحقيق ويحرر محضرا بما يقوم به من إجراءات، على أن يباشر التفتيش وفقا للمادة 81 من نفس القانون في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة.

أما بخصوص مواعيد التفتيش فيكون لقاضي التحقيق دخول المساكن وتفتيشها في أي وقت خارج المواعيد الزمنية المقررة في المادة 1/47 من ق.إ.ج متى تعلق الأمر بالجرائم المذكورة، كما له أن يأمر ضابط الشرطة القضائية المختص القيام بذلك (المادة 3/47 و4 من نفس القانون)، وهو ما يستشف من المادتين 82 و83 من ق.إ.ج.ج.

أما بالنسبة لأدلة ضبط الجريمة فقد نصت المادة 84 من ق.إ.ج.ج على أنه إذا اقتضى الأمر أثناء إجراء تحقيق وجوب البحث عن مستندات فإن لقاضي التحقيق أو ضابط الشرطة القضائية المنوب عنه أن يتخذ مقدما جميع الإجراءات اللازمة لضمان إحترام كتمان سر المهنة، وحقوق الدفاع، ويجب على الفور إحصاء الأشياء والوثائق المضبوطة ووضعها في

أحراز مختومة. ولا يجوز فتحها إلا بحضور المتهم مصحوبا بمحاميه أو بعد استدعائهما قانونا، كما يستدعى أيضا كل من ضبطت لديه هذه الأشياء لحضور هذا الإجراء.

الفرع الثالث: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

وهي من بين الاجراءات الجديدة التي استحدثها المشرع الجزائري في قانون الإجراءات الجزائية لمكافحة الجريمة، حيث تمم هذا القانون بالباب الثاني من الكتاب الأول بالقانون رقم 22/06 المؤرخ في 20 ديسمبر 2006 بفصل رابع تحت عنوان " في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور"، وتناوله في المواد من 65 مكرر 5 إلى 65 مكرر 10 منه التي تجيز لضباط الشرطة القضائية وأعوانهم القيام بهذه الأعمال.

وقد عرف البعض **اعتراض المراسلات** أنها "عملية مراقبة سرية المراسلات السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة أو المعلومات حول الأشخاص المشتبه فيهم في ارتكابهم أو في مشاركتهم في ارتكاب الجريمة"[86].

أما المقصود **بالمراسلات** التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة عن طريق الأسلاك أو البصريات أو اللاسلكي الكهربائي أو أجهزة أخرى كهربائية مغناطسية حسب المادة 21/8 من القانون رقم 03/2000 المؤرخ في 5 أوت 2000 المحدد للقواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية[87].

أما **تسجيل الأصوات وإلتقاط الصور** فالمقصود بها "تسجيل المحادثات الشفوية التي يتحدث بها الأشخاص بصفة سرية أو خاصة وفي مكان عام أو خاص وكذلك التقاط صورة لشخص أو عدة أشخاص يتواجدون في مكان خاص"[88].

---

[86] عبد الرحمان خلفي، محاضرات في قانون الإجراءات الجزائية، دار الهدى، الجزائر، 2010، ص 72.

[87] شرف الدين وردة، مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية في التشريع الجزائري، مجلة المفكر، العدد الخامس عشر، ص 542. منشورة على الموقع:
https://www.asjp.ceriste.dz/en/article.

[88] عبد الرحمان خلفي، مرجع سابق، ص 73.

أجاز المشرع الجزائري لضباط الشرطة القضائية القيام بإعتراض المراسلات وتسجيل والتقاط الصور للكشف عن الجريمة المعلوماتية، وهي إجراءات تباشر بشكل خفي، على الرغم من تناقضها مع النصوص المقررة لحماية الحق في الحياة الخاصة[89].

لكن مع ذلك، نجد أن المشرع قيدهم بضوابط أو شروط حتى تكون الاجراءات صحيحة ومنتجة لآثارها وهي:

– قيام الضباط بهذه الأعمال إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم حددها المشرع على سبيل الحصر في المادة 65 مكرر 5 من ق.إ.ج، وهي جرائم المخدرات والجريمة المنظمة العابرة للحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، وكذا جرائم الفساد. أما إذا كانت هذه الأعمال في غير هذه الجرائم فإجراؤها باطل[90].

– أن يصدر الإذن إلى ضباط الشرطة القضائية للقيام بالأعمال المحددة في المادة 65 مكرر 5 من ق.إ.ج مكتوبا من وكيل الجمهورية أو قاضي التحقيق المختصين[91]، بأن يأذنوا بما يلي:

– اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

– وضع الترتيبات التقنية، دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو إلتقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

يسمح الاذن المسلم بغرض وضع الترتيبات التقنية بالدخول الى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من هذا القانون وبغير علم أو رضا الأشخاص الذين لهم

---

[89] نفس المرجع.

[90] شرف الدين وردة، مرجع سابق، ص 543.

[91] كانت القاعدة العامة في قانون الاجراءات الجزائية الجزائري قبل 2006/12/20 أن اعتراض المراسلات وتسجيل الأصوات والتقاط الصور من الاجراءات القضائية التي لا يجوز اتخاذها إلا على مستوى التحقيق القضائي بموجب أمر من قاضي التحقيق ولا يمكن اللجوء إليها خلال مرحلة التحريات الأولية حتى ولو تعلق الامر بحالة تلبس، ثم استحدث المشرع اللجوء إلى هذه الأسايب بموجب القانون رقم 22/06 المؤرخ في 2006/12/20 من خلال استحداث المواد 65 مكرر 5 إلى 65 مكرر 10 منه. نفس المرجع، أشارت إليه في الهامش رقم 17، ص 588.

حق على تلك الأماكن، ويجب أن يتضمن هذا الاذن تحديد الاتصالات المطلوب المطلوب اعتراضها وتسجيلها أو الأماكن المقصودة بالتصوير سكنية أو غير سكنية، كما يجب ذكر الجريمة التي تبرر اللجوء إلى هذه الإجراءات ومدتها طبقا للمادة 65 مكرر 7 من ق.إ.ج. غير أن هذه الأخيرة اقتصرت على وجوب ذكر الجريمة دون ذكر القرائن والأدلة التي استندت عليها الجهات القضائية المختصة لإصدار أمر اعتراض المراسلات وتسجيل الأصوات.

– يجب أن تتم هذه الترتيبات تحت إشراف السلطة التي منحت الاذن بوضعها سواء وكيل الجمهورية أو قاضي التحقيق. ويقيد ضابط الشرطة القضائية أثناء قيامه بالعمليات المحددة في المادة 65 مكرر 5 بالحفاظ على السر المهني.

كما نصت الفقرة الثانية من المادة 65 مكرر 7 من ق.إ.ج على أن الإذن بعملية وضع الترتيبات يكون لمدة أقصاها أربعة أشهر قابلة للتجديد حسب ما تمليه ضرورة التحري والتحقيق ضمن نفس الشروط.

–يجوز للسلطة المكلفة بالتحري والتحقيق الاستعانة بأعوان مؤهلين لدى مؤسسات عمومية أو خاصة في هذا المجال وتسخيرهم من أجل التكفل بالجوانب التقنية لهذه العمليات طبقا للمادة 65 مكرر 8 من نفس القانون.

– يحرر ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص أن يحرر محضرا عن كل عملية اعتراض أو تنصت أو تصوير أو أي ترتيبات في هذا الشأن، ويذكر بالمحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها طبقا للمادة 65 مكرر 9 من ق.إ.ج، وكذلك يجب عليه أيضا أن يصف أو ينسخ المراسلات أو الأصوات أو الصور السجلة في محضر يودع بالملف طبقا للمادة 65 مكرر 10 من نفس القانون.

الفرع الرابع: التســـرب

يعتبر التسرب تقنية جديدة أدرجها المشرع في تعديل قانون الاجراءات الجزائية سنة 2006، عندما تقضي ضرورات التحري والتحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر 5 منه. وقد عرفته المادة 65 مكرر 12 من نفس القانون على أنه:" يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق

العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف".

أي أنه عملية دس عون أو ضابط الشرطة القضائية وسط شبكة إجرامية أو أشخاص متهمين بإرتكاب جريمة من أجل جمع أكبر قدر ممكن من الأدلة والمعطيات حول الجريمة موضوع التحري والتحقيق، وكذا إفادة المصالح الأمنية بحجم الإمكانات المادية والبشرية ووسائل الإتصال والتنقل المستعملة في ارتكاب الجرائم، وأساليب ارتكابها[92].

ويخضع القيام بعملية التسرب للشروط التالية:

– أن تقتضي ضرورات التحري أو التحقيق في إحدى الجرائم السبعة المنصوص عليها في المادة 65 مكرر 5 من ق.إ.ج ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

– يجب أن يتم الإذن بعملية التسرب بموجب إذن مكتوب ومسبب تحت طائلة البطلان صادر عن وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية، مع ذكر الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته.

كما يجب أن يذكر في الاذن مدة التسرب والتي يجب أن لا تتجاوز أربعة أشهر قابلة للتجديد ضمن نفس الشروط، غير أنه يجوز للقاضي الذي رخص بإجرائها أن يأمر في أي وقت بوقف العملية، ويودع الاذن في ملف الاجراءات بعد الإنتهاء من عملية التسري طبقا للمادة 65 مكرر 15 من ق.إ.ج.

ونظرا لخطورة عملية التسرب على حياة وسلامة الشخص المتسرب وعائلته في حالة كشفه فقد حاول المشرع ضمان حمايته بمعاقبة كل من يكشف عن هويته بالحبس من سنتين إلى خمس سنوات وبغرامة من 50.000 دج إلى 200.000 دج طبقا للمادة 65 مكرر 16 من ق.إ.ج.

[92] بدري فيصل، مرجع سابق، ص 216.

المطلب الثاني:

المكافحة الاجرائية في ظل قانون الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال

تضمن أيضا القانون رقم 04/09 المؤرخ في 5 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جملة من الإجراءات المستحدثة والخاصة بالتحري والتحقيق عن الجرائم المتصلة بتكنولوجيات الإعلام والإتصال كان من اللازم أن تلد مع التطور الحاصل في حقل الجريمة المعلوماتية كظاهرة حديثة، ومنها ما نصت عليه المادة الثالثة من هذا القانون:" مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية".

وعليه يمكن تقسيم إجراءات التحري في هذا المجال حسب ما نص عليه القانون إلى مراقبة الإتصالات الالكترونية، تفتيش المنظومة المعلوماتية، حجز المعطيات المعلوماتية، حفظ البيانات المعلوماتية المخزنة، وسنتكلم بمزيد من التفصيل عن كل إجراء في الفروع التالية:

الفرع الأول: مراقبة الإتصالات الالكترونية

يقصد بالاتصالات الإلكترونية حسب المادة 2 من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.

وقد حدد القانون مراقبة الاتصالات الالكترونية على سبيل الاستثناء وفي حالات محددة حصريا في المادة 4 من ذات القانون المذكور، أي أن هذه الأخيرة نصت على الحالات التي تسمح باللجوء إلى هذا الإجراء وهي:

1- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

2- حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

3- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية.

4- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

ولا يجوز إجراء عمليات المراقبة في الحالات المذكورة اعلاه إلا بإذن مكتوب من السلطات القضائية المختصة. إلا أن الأمر عندما يتعلق بالحالة الأولى يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والإتصال ومكافحته المنصوص عليها في المادة 13 من نفس القانون إذنا لمدة 6 أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

الفرع الثاني: تفتيش المنظومة المعلوماتية

بينت المادة 5 من القانون رقم 04/09 إجراءات التفتيش للمنظومة المعلوماتية، حيث تنص على أنه:" يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول، بغرض التفتيش، ولو عن بعد، إلى:

أ- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.
ب- منظومة تخزين معلوماتية".

كما أن القانون أشار إلى أنه في حالة ما إذا كانت المعطيات المبحوث عنها يمكن الدخول إليها إنطلاقا من منظومة معلوماتية تقع خارج الإقليم الوطني، يكون الحصول عليها بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل، كما أنه أجاز تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها وهذا للسلطات المكلفة بالتفتيش.

الفرع الثالث: حجز المعطيات المعلوماتية

تناوله المشرع في المادتين 6 و7 من القانون رقم 04/09 السابق الذكر، وتتمثل شروط إجراء الحجز فيما يلي[93]:

– عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكيبها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ كل المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

– يجب 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.

– إذا استحال إجراء الحجز وفقا لما هو منصوص عليه فيما سبق لأسباب تقنية، لذا يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

– على السلطة التي تباشر التفتيش أن تأمر بإتخاذ الإجراءات اللازمة لمنع الإطلاع على المعطيات التي يشكل محتواها جريمة، لا سيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك.

– تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية.

---

[93] المادة 21 من المرسوم الرئاسي رقم 261/15 المؤرخ في 8 أكتوبر 2015، المحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، ج ر، العدد 53، الصادرة في 8 أكتوبر 2015.

كما نظم القانون رقم 04/09 السالف الذكر إجراء جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها في المادة 10 منه، وجعله من التزامات مقدمي الخدمات في مساعدة السلطات المكلفة بالتحريات القضائية والتفتيش وحفظ المعلومات طبقا للمادة 11 من نفس القانون التي من شأنها تمكين سلطات التحقيق من التعرف على مستعملي الخدمة.

وأضافت المادة 12 من ذات القانون أنه:" زيادة على الالتزامات المنصوص عليها في المادة 11 من قانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، يتعين على مقدمي خدمات "الانترنت" مايأتي:

أ- التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن،

ب- وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها".

الفرع الرابع: الحفظ السريع للبيانات المعلوماتية المخزنة

عالج المشرع الجزائريإجراء التحفظ العاجل للبيانات المعلوماتية المخزنة في القانون رقم 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها كإلتزام من إلتزامات مقدمي خدمة الانترنت، وكذلك تناوله ضمن المرسوم الرئاسي رقم 261/15 المحدد لتشكيلة وتنظيم كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وذلك بجعل القيام بهذا الاجراء من المهام الموكلة إلى الهيئة.

أولا: الحفظ السريع للبيانات المعلوماتية المخزنة ضمن القانون 04/09

رتب القانون 04/09 على عاتق مقدمي الخدمات إلتزاما منصوص عليه في المادتين 10 و 11 منه وهو حفظ المعلومات أو المعطيات الذي من شأنه مساعدة السلطات المكلفة بالتحقيق.

حيث نصت المادة 10 على أنه:" في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة

بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11، تحت تصرف السلطات المذكورة.

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق".

أما المادة 11 فصلت في إجراء حفظ المعطيات المتعلقة بخط السير حيث نصت على ما يلي:" مع مراعاة طبيعة ونوعية الخدمات، يلتزمزامقدموا الخدمات بحفظ:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة،
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال،
- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال،
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها،
- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ" من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه.
تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل".

وفضلا عن العقوبات التي سلطها المشرع الجزائري على مقدمي الخدمة وفقا للمادة 394 مكرر 6 من ق.ع من مصادرة للأجهزة والوسائل وإغلاق المحلات فقد نص كذلك في القانون 04/09 بمعاقبتهم بـــالحبس من 6 أشهر إلى 5 سنوات وبغرامة من 50.000 دج إلى 500.000 دج ومعاقبة الشخص المعنوي وفقا للقواعد المقررة في قانون العقوبات. ويستخلص من نص المادة 11 من القانون 04/09 أنه وحتى في حالة استعمال الهاتف فإن المتعاملين في هذا الشأن ملزمون كذلك بما هو محدد في الفقرة "أ" من ذات المادة أي القيام بحفظ المعطيات التي تسمح بالتعرف على مصدر الإتصال وتحديد مكانه.

ثانيا: الحفظ السريع للبيانات المعلوماتية المخزنة ضمن المرسوم الرئاسي رقم 261/15

جاء في المادة 4 من المرسوم الرئاسي رقم 261/15 المحدد لتشكيلة وتنظيم كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أن من بين المهام المكلفة إلى الهيئة: حفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية. إلا أنه لم يحدد المدة القصوى التي تلتزم بها الهيئة لحفظ المعطيات المتعلقة بخط السير على مستوى مقدمي خدمات الانترنت بمقتضى المادة 11 من القانون 04/09.

ختاما لهذا الفصل نرى أنه يحسب على المشرع الجزائري تداركه لخطورة هذا النوع من الجرائم، من خلال توفير مجموعة من النصوص العقابية في قانون العقوبات، بالاضافة الى اجراءات استباقية وتدابير أمنية نص عليها في قانون الاجراءات الجزائية. كما نص على قانون يعمل على مكافحة الجرائم المتصلة بتكنولوجيات الاتصال والاعلام ومكافحتها.

فالمشرع الجزائري قد عمل جاهدا على سن نصوص قانونية عقابية موضوعية وإجرائية لمكافحة الجريمة المعلوماتية، مواكبا بذلك التشريعات العقابية المتطورة في هذا المجال، فاستحدث أحكاما قانونية لحماية البرامج وهذا ضمن الأمر 05/03 المؤرخ في 2003/07/19 المتعلق بحقوق المؤلف والحقوق المجاورة، وكذا تعديل قانون العقوبات 15/04 المؤرخ 2004/11/10 ، الذي عالج فيه المساس بأنظمة المعالجة الآلية للبيانات، إلا أن ما يعاب على المشرع أنه بالرغم من وضعه لنصوص عقابية رادعة إلا أنها تبقى غير قابلة التطبيق، ذلك أنها تحتاج إلى نصوص إجرائية تلازمها نظرا لما تمتاز به الجريمة المعلوماتية عن الجرائم الأخرى.

خـــاتمة:

تعد ظاهرة الجرائم المعلوماتية من المستجدات الاجرامية الحديثة نسبيا، وتستهدف الاعتداء على البيانات والمعلومات والبرامج بكافة أنواعها، فهي جريمة يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية أو الفنية، وتوجه للنيل من أجهزة الحواسب وشبكات الاتصال وقواعد البيانات والبرمجيات ونظم التشغيل، مما يظهر مدى خطورتها فهي تمس الحياة الخاصة للأفراد وتهدد الأعمال التجارية بخسائر فادحة كما قد تنال من الأمن القومي والسيادة الوطنية للدول، وتشيع فقدان الثقة في التعاملات الالكترونية.

ونظرا لارتباطها بتكنولوجيا متطورة أدى إلى تميزها عن الجرائم التقليدية بدءا بتسميتها وصولا إلى الافعال التي تدخل ضمن دائرتها، ما دفع بالعديد من الدول الى مواكبة هذا التطور التكنولوجي ووجدت نفسها مضطرة لايجاد حلول لمواجهتها، وهذه الحلول كانت بتعديل النصوص التقليدية وتطويرها وتشريع نصوص جديدة حتى لا تترك سلوكات مستهجنة ومجرمة دون عقاب.

والجزائر ليست بمعزل عن بقية الدول، حيث عملتعلى تطوير المنظومة القانونية وتكييفها مع المعطيات الدولية من خلال اصدار تشريعات تواكب التطور الحاصل في المجال المعلوماتي، وقد اتبع المشرع الجزائري سياسة مزدوجة للتصدي لظاهرة الاجرام المعلوماتي، فمن جهة قام بتعديل الجوانب الموضوعية، بالاضافة الى النصوص الخاصة التي تبناها المشرع في تعديله الاخير للقانون 15/04 المؤرخ في 2004/11/10 المعدل والمتمم للامر 155/66 المؤرخ في 1966/6/8 المتضمن قانون العقوبات، ويشمل المواد من 394 الى 394 مكرر 7، ومن ابرز تلك التعديلات كذلك ما أورده في الامر 05/03 الصادر في 2003/7/19 والمتعلق بحقوق المؤلف والحقوق المجاورة والتي ادرجت برنامج الحاسوب ضمن المؤلفات مضمونة الحماية، وكذلك تعديل الجوانب الاجرائية، حيث قام بتعديل قانون الاجراءات الجزائية عن طريق إضافة إجراءات جديدة تطبق على جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وقام من جهة ثانية باستحداث قوانين اخرى خاصة اكثر تجاوبا مع الطبيعة الخاصة للجرائم المعلوماتية، القانون رقم 04/09 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها.

فتعتبر بذلك مكافحة فعالة نظرا لما تمتاز به من شمولية، بحيث جاءت لتشمل اغلب الجرائم التي قد تمس نظام المعالجة الالية للمعطيات بصفة عامة، وكذا تضمنت اغلب الجرائم التي قد تمس البيانات والمعطيات المكونة لهذا النظام، غير انها تحتاج الى نصوص اجرائية تلازمها نظرا لما تمتاز به الجريمة المعلوماتية من خصوصية تختلف عن باقي الجرائم.

وبذلك يكون المشرع قد تدارك النقص الذي كان موجود في التشريع العقابي الجزائري، فهو يعد قفزة في المجال التشريعي مواكبا للتشريعات المقارنة من خلال تجريمه للافعال التي يرتكبها الشخص الطبيعي، وتحميل الشخص المعنوي المسؤولية الجزائية وتوسيع نطاق العقوبة بتجريم الشروع في هذه الجرائم بتجريمه حتى الاعمال التحضيرية في إطار الاتفاق الجنائي.

رغم جهود المشرع الجزائري لسد الفراغ التشريعي لمواجهة هذه الجرائم إلا أن نصوصه لا تزال ناقصة لذلك نقترح بعض التوصيات وهي:

-لا يكفي مواكبة المشرع العقابي الجزائري لنصوص التشريعات المقارنة بدون تجسيدها من الناحية التطبيقية والاستعانة بمختصين وخبراء قاديرين على تشخيص الجريمة، والعمل على تكوين فرق من الضبطية القضائية لكي تختص بهذا النوع من الجرائم وتكوين قضاة مختصين في هذا النوع من الجرائم، مع توفير كافة الوسائل المادية والتقنية اللازمة لأداء عملها ومهامها على أحسن صورة.

- ضرورة تشديد الوصف الجنائي والعقوبات المقررة للانماط الاجرامية للجريمة المعلوماتية، بغية تحقيق الردع والقضاء على الاجرام المعلوماتي.

- ضرورة تكثيف الجهود الوطنية لنشر المعرفة وزيادة الوعي بالجرائم الالكترونية ومدى خطورتها ووسائل الوقاية منها وسبل مواجهتها.
- من الأفضل أن يسن المشرع قانون موحد لمكافحة الجرائم المعلوماتية، يلم بكل النصوص الموضوعية والإجرائية والتنظيمية، وهو ما يسهل عمل ضباط الشرطة القضائية ووكلاء الجمهورية وقضاة التحقيق والحكم، ويساعد رجال القانون من الإلمام بكل ما يخص هذا النوع المستحدث من الجرائم.

وفي الأخير نقول أنهأوضحت الدراسة أن الجرائم المعلوماتية أقل عنفا من الجرائم التقليدية أي انها لا تحتاج أدنى مجهود عضلي بل تعتمد على الدراسة الذهنية والتفكير العلمي المدروس القائم على معرفة بتقنيات الحاسوب.

قـــائـــمة المـــراجـــع

أولا : المـــــؤلـــفـــات

أ-المـــؤلفـــات العـــامة:

01- خثير مسعود، الحماية الجنائية لبرامج الكومبيوتر في التشريع الجزائري، دار الهدى، الجزائر، 2010.

02- عبد الرحمان خلفي، محاضرات في قانون الإجراءات الجزائية، دار الهدى، الجزائر، 2010.

03- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، بيروت، 1999.

04- محمد أبو بكر بن يونس، الأحكام الموضوعية والجوانب الإجرائية – الجرائم الناتجة عن استخدام الأنترنت، دار النهضة العربية، مصر، 2004، ص 60.

05- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، 1994.

06- نائلة عادل محمد فريد قورة، جرائم الحاسب الالي الاقتصادية دراسة نظرية وتطبيقية، ط1، منشورات الحلبي الحقوقية،بيروت- لبنان، 2005.

ب-المؤلفـــات المتخصصة:

1-أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2006.

2-أيمن عبد الحفيظ، الإتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دون دار وبلد النشر، 2005.

3-أحمد خليفة الملط، الجرائم المعلوماتية، ط 2، دار الفكر الجامعي، الإسكندرية، 2006.

4-زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار هومة، الجزائر، 2011.

5-نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعرف، الإسكندرية، 2008.

6-نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الاردن، 2010.

ثانيا : المقـــالات

1-بردال سمير، الجريمة المعلوماتية في التشريع الجزائري، مجلة القانون، العدد الثاني، جويلية 2010. منشورة على الموقع:

https://www.asjp.ceriste.dz/en/article

2-حوالف عبد الصمد، رحمان يوسف، الآليات القانونية لتلافي الجريمة المعلوماتية والحد من انتشارها وفقا للتشريع الجزائري، مجلة الفكر القانوني والسياسي، العدد الرابع، منشورة على الموقع:

https://www.asjp.ceriste.dz/en/article.

3-شرف الدين وردة، مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية في التشريع الجزائري، مجلة المفكر، العدد الخامس عشر. منشورة على الموقع:

https://www.asjp.ceriste.dz/en/article.

4-ونوغي نبيل، زيوش عبد الرؤوف، الجريمة المعلوماتية في التشريع الجزائري، مجلة العلوم القانونية والاجتماعية، المجلد الرابع، العدد الثالث،جامعة زيان عاشور بالجلفة-الجزائر،سبتمبر 2019.

ثالثا: الرسائل والمذكرات العلمية:

1- بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الولي والداخلي، أطروحة لنيل شهادة دكتوراه علوم في القانون تخصص قانون عام، كلية الحقوق، جامعة الجزائر 1، 2018/2017.

2- حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، مذكرة ماجستير في العلوم القانونية تخصص عللمالغجرام وعلم العقاب، كلية الحقوق والعلوم السياسية،جامعة الحاج لخضر باتنة، 2011-2012.

3- سعيداني نعيم، أليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، شهادة الماجستير في العلوم القانونية تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، الجزائر، 2013.

4- سوير سفيان، جرائم المعلوماتية، مذكرة الماجستير في العلوم الجنائية وعلوم الإجرام، كلية الحقوق والعلوم السياسية،جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2010-2011.

5- صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة الماجستير في القانون، تخصص القانون الدولي للاعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري-تيزي وزو، الجزائر، سنة 2013.

6- عبد القادر نشادي، الجرائم المعلوماتية في وسائل الاتصال الحديثة – دراسة وصفية تحليلية لمجموعة من الجرائم المرتكبة عبر الوسائط الاتصالية الحديثة في الجزائر، أطروحة لنيل شهادة الدكتوراه في علوم الإعلام والإتصال، كلية علوم الإعلام والإتصال، قسم الإتصال، جامعة الجزائر 3، 2016-2017.

7- بوخبزة عائشة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، الجزائر، 2012-2013.

8- كور طارق، آليات مكافحة جريمة الصرف، مذكرة لنيل شهادة ماجستير، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي-أم البواقي، الجزائر، جوان 2012.

رابعا: النصوص القانونية:

1-أمر رقم 97-10 المؤرخ في 1997/03/06، المتعلق بحق المؤلف والحقوق المجاورة، ج ر، العدد 13، المؤرخة في 1997/03/12.

2-قانون رقم 2000-03 المؤرخ في 5 أوت 2000، يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، العدد 48، المؤرخة في 06 أوت، 2000.

3-الامر رقم 03-05 المؤرخ في 2003/07/19، المتعلق بحق المؤلف والحقوق المجاورة، ج ر، العدد 44، المؤرخة في 2003/07/23.

4-القانون رقم 04-15 المؤرخ في 2004/11/10 المعدل والمتمم للامر رقم 156/66 المؤرخ في 1966/06/08، المتضمن قانون العقوبات، ج ر، العدد 71، المؤرخة في 2004/11/10.

5-القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، جر، العدد 47، المؤرخة في 16 أوت 2009.

6-المرسوم الرئاسي رقم 261/15 المؤرخ في 8 أكتوبر 2015، المحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، ج ر، العدد 53، المؤرخة في 8 أكتوبر 2015.

7-القانون رقم 01/16 مؤرخ ففي 6 مارس 2016، يتضمن التعديل الدستوري، ج ر، العدد 14، مؤرخة في 7 مارس 2016.

الفهـرس