جامعة عـــــــــــــمار ثليجي الأغواط
كلية الحقوق والعلوم السياسية
قسم الحقوق

الجريمة المعلوماتية وسبل الوقاية منها في التشريع الجزائري

مذكرة في إطار مقتضيات نيل شهادة الماستر في القانون الجنائي والعلوم الجنائية

إعداد الطلبة:
1/ قوجال أحمد
2/ بن حرمة ميهوب

إشراف الأستاذ:
بلحسن حسام الدين لحسن

لجنة المناقشة

الأستاذ: غريبي يحى	- رئيســــــــــا
الأستاذ: بلحسن حسام الدين لحسن	- مشرفا و مقررا
الأستاذ:غريبي محمد	- عضوا ومناقشا

السنة الجامعية: 2024-2025


بسم الله الرحمن الرحيم

ا لإ هـــــــد ا ء

الحمد الله الذي هدانا إلى هديه المستقيم ودربه المنير

الذي أشاع بنوره دربي وأنار بنور العلم عقلي

في سبيل طلب العلم والمعرفة

أهدي ثمرة عملي هذا إلى النور الذي يضيء حياتي

والدا يا رحمهم الله وعائلتي العزيزة

إلى كل من شاركني في التعب والجهد والعناء

وأصدقائي وزملائي

أحمد قوجال ***ميهوب بن حرمة***

تـشكـــــر ا ت

أتوجه إلى الله عز وجل بعظيم الشكر والعرفان

على توفيقه لي في إنجاز هذا العمل المتواضع

كما أتقدم بأسمى عبارة الشكر والتقدير إلى الأستاذ المشرف **الدكتور**

بلحسن حسام الدين لحسن

الذي لم يبخل علينا وعلى زملائي بالتوجيه والنصح.

كما أتقدم بجزيل الشكر إلي أسرة جامعة عمار ثليجي

كما لا يفوتني أن أقف وقفة إحترام وتقدير

أمام كل من ساهم في تلقيني العلم في جميع أطوار دراستي

وأشكر في الختــام كل من ساعدني من قـريب أو بعيــد

في إتمام عملي هذا.

أحمد قوجال ***ميهوب بن حرمة***

قائمة المختصرات

الرمز	الكلمة
ج ر	الجريدة الرسمية للجمهورية الجزائرية الديموقراطية الشعبية
ق ع	قانون العقوبات
ق إ ج ج	قانون الإجراءات الجزائية الجزائري
ص	صفحة
ط	طبعة
ج	جزء

مقدمة

منذ القدم عرف المجتمع البشري البسيط ظاهرة الجريمة، وتم إعتبار أن كل فعل يمس بأمن الجماعة أو الإعتداء على حياة الفرد أو ماله أو سلامته الجسدية، فهو فعل مجرم يستحق العقاب عليه. وفي العصر الحديث تطورت فكرة تجريم الأفعال والعقاب عليها من طرف الدولة بدلا من النظام القديم، إنطلاقا من رب الأسرة إلى شيخ القبيلة وفي العصر الحالي الدولة.

لذلك نجد أن الدولة أصدرت تشريعات بنصوص قانونية تجسدت في قانون العقوبات الذي يجرم الفعل ويحدد العقوبات الخاصة لكل واحد منها، والتي تحترم منظور الشريعة الإسلامية التي تسعى لتحقيق حفظ الدين، النفس، العقل، النسل، والمال وفي نفس الوقت تخضع للقانون الساري المفعول وكذا الإجراءات التي من الواجب إتباعها أمام الهيئات القضائية والضبطية القضائية.

ونتيجة للتطور الهائل في مجال التكنولوجيا والاتصالات وتقنية المعلومات، التي كان سببها إستعمال الأجهزة الذكية من حواسيب وبرامج مكان البشر، حتى حل الذكاء الاصطناعي محل الذكاء البشري، وعلى الرغم من أن هذه التكنولوجيا هي صناعة بشرية في الأساس، فلقد أصبحت الدول تقاس بمدى تقدمها بقدرتها على إمتلاك والتعامل مع هذه التكنولوجيا الحديثة في الحياة اليومية.

وكما هو معلوم لكل تكنولوجيا لها ميزات لها أيضا مساوئ وبذلك أصبحت نقمة عندما تم إستخدام هذه التكنولوجية بطريقة غير قانونية، وأصبحت هذه الطريقة معروفة بأصحاب الإجرام الناعم لأنه لا يستعمل فيها أي عنف أو إراقة دماء أو الظرب كما هو الحال في الجرائم التقليدية، والخطير في هذه الجرائم أنها تعتبر عابرة للحدود، لأنه يستخدم فيها شبكات المعلومات والتكنولوجيا الحديثة، وبذلك يسهل التهرب من العقاب، حيث ترتكب كثير من هذه الجرائم عن بعد، أي يمكن إرتكابها من خارج الحدود الدولية. وقد إنتشرت في الآونة الأخيرة وأصبحت ظاهرة جديدة من الجرائم المستحدثة، وتتم عن طريق هذه التكنولوجيا لهذه الجريمة المعلوماتية، والتي أصبحت ظاهرة تخترق المجتمع وتهدد دعائمه، ولعله السبب الرئيسي لتجريم هذه الجريمة التي تسمى بالجريمة الإلكترونية. وهو ما دفع المشرع الجزائري إلى سن تشريعات

تتماشى مع المستجدات على الساحة الاجرامية، ووضع نصوصا واضحة فيها عقوبة الجاني وإهتم مفسري القانون إلى شرح هذه التشريعات، وتبيان أركان الجريمة التي تقوم عليها.

ونتيجة إنتشار هذه التكنولوجيا لجميع مجالات وخاصة في مجال الحاسب الآلي والأنترنت والتي تسهل بنقل المعلومة صوتا وصورة، وكنتيجة سلبية لهذه التكنولوجيا التي يمكن لأي شخص إستغلال هذه الشبكة، يقوم بعض الأشخاص بإرتكاب جرائمهم الناعمة وفي نفس الوقت الخطيرة والتي تهدد الفرد والمجتمع والعالم بصفة عامة.

وهنا تظهر أهمية دراسة هذا الموضوع وذلك لإعتبارها ظاهرة جديدة عن المجتمع و غير معروفة في القانون الجنائي، لذلك كان إهتمامنا بالبحث في موضوع أركان هذه الجريمة و سبل الوقاية منها في التشريع الجزائري وكذا الحد من الجرائم المعلوماتية، وذلك من أجل شرح و تحليل المفاهيم القانونية المتعلقة بها.

والغاية من دراسة الموضوع هو إثراء المكتبة الجامعية في هذا المجال، ومحاولة دراسة هذه الظاهرة وتبيان دور كيفية مكافحتها في ضل القانون الجزائري.

غير أنه قد واجهنا بعض الصعوبات في إنجاز البحث، منها له علاقة بالجانب التقني والفني لتكنولوجيات الجديدة من الحاسوب والأنترنت، وهذا ما يستدعي الإلمام بها.

والإشكال الذي يطرح هو:

هل التدابير والإجراءات في القانون الجزائري كفيلة لمواجهة الجريمة المعلوماتية؟

وللإجابة عن هذه الإشكالية، يجب البحث في بعض التساؤلات التي تتفرع منها ومن بينها، ما يلي:

- ✓ الجريمة المعلوماتية أحد صور الجرائم التقليدية
- ✓ للجريمة المعلوماتية خصائص وأنواع
- ✓ للجريمة المعلوماتية نفس الأركان الجريمة التقليدية
- ✓ للجريمة المعلوماتية هيئات وآليات قانونية للكشف عنها في التشريع الجزائري.

أسباب اختيار الموضوع:

ومن الأسباب الشخصية التي دفعتنا للكتابة في هذا الموضوع، هو هذا الغموض الذي يحيط بهذه الجريمة وخاصة كيف يمكن التصدي لها وخاصة أن الفاعل يقوم بالفعل الإجرامي المتخفي وراء شاشة الحاسوب فلا يترك أي أثر وراءه على مسرح الجريمة كما هو الحال في الجريمة التقليدية، مما يجعلك تتخيل في عقلك مسرح الجريمة وكأنها في عالم إفتراضي، لكن في واقعها تمس الواقع للحياة اليومية، وهذه الجريمة تمس تقريبا كافة القطاعات وتعتبر أخطر جريمة وأكبر عقبة لكل دولة تريد إنشاء الحكومة الإلكترونية وبالتالي تضر بمصداقية هذه الحكومة الإفتراضية.

أهداف الدراسة:

تهدف هذه الدراسة إلى التعرف على العديد من النقاط منها:

- ✓ التعرف على الجريمة المعلوماتية.
- ✓ التعرف على دوافع التي أدت إلى إرتكاب الجريمة المعلوماتية.
- ✓ دراسة أركان الجريمة المعلوماتية في التشريع الجزائري.
- ✓ التعرف على الهيئات المختصة لمكافحة الجريمة المعلوماتية.

أهمية الدراسة

تظهر الأهمية العلمية للدراسة في تسليط الضوء على مرتكب الجريمة المعلوماتية في التشريع الجزائري، حيث أن تفشي هذه الجريمة أصبح يشكل خطر كبيراً لذا إرتأينا أن نقوم بدراسة الآليات والسبل للوقاية من الجريمة، ولعل في هذا العمل ما يكون نواة يستند إليها الباحثين ورواد القانون والعاملين في المجال القانوني، والتقليل من آثارها، وزيادة الوعي لدى مستخدمي الأجهزة الحديثة بمخاطر هذه الجريمة، وبأخذ الحذر والحيطة في الاستخدام.

الحدود الموضوعية :

نتناول في هذه الدراسة القانونية العلمية للجريمة المعلوماتية، وكذلك سبل الوقاية من هذا النوع من الإجرام، وتسليط الضوء على الدراسة بالنسبة للمنظور التشريع الجزائري، وحتى يتأتى ذلك نتعرض للجريمة المعلوماتية وأنواعها، وأركانها والعقوبات المقررة للقضاء عليها وسبل الوقاية منها.

منهج الدراسة:

وللإجابة على الإشكالية المطروحة، إعتمدنا في ذلك بعض المناهج الملائمة وطبيعة الموضوع، منها المنهج الإستقرائي في جمع المادة العلمية من مختلف المراجع، ثم المنهج التحليلي الوصفي إذ قمنا بوصف الظاهرة وبيان المفاهيم القانونية وتحليل المفاهيم وشرحها للتمييز بين الجريمة المعلوماتية والجريمة التقليدية.

الدراسات السابقة:

- عادل بغدادي و حمزة مكاس، الحماية القانونية لبرامج الحاسوب في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الإداري، جامعة محمد بشير الإبراهيمي، برج بوعريريج الجزائر، 2023.
- عائشة نايري، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، جامعة أحمد دراية، أدرار الجزائر،2017

صعوبات الدراسة:

أهم الصعوبات التي واجهتنا في إعداد هذا البحث والمتمثلة أساسا في:

- قصر الوقت المخصص لتحضير المذكرة.
- بسبب ارتباطات العمل والواجبات اليومية أثرت على الوقت المخصص للبحث.
- صعوبة التنقل بين مكان العمل والمؤسسة الخارجية وكذا مكتبة الجامعة.
- طبيعة الموضوع في حد ذاته وعدم معالجته من قبل بالتحديد وتداخل مفهومه وتعدد استعمالاته بين عدة تخصصات، علم الاقتصاد، القانون والإدارة ... إلخ.

وللإجابة على الإشكالية للموضوع، إتبعنا في ذلك خطة منهجية ثنائية الفصول، حيث خصصنا الفصل الأول إلى الأساس النظري والقانوني للجريمة المعلوماتية في التشريع الجزائري وأما الفصل الثاني تناولنا فيه آليات الوقاية من الجرائم المعلوماتية في التشريع الجزائري

الفصل الأول
الأساس النظري والقانوني للجريمة المعلوماتية
في التشريع الجزائري

نتيجة الإستعمال الواسع في جميع الميادين للحاسوب الآلي والأنترنت في منتصف القرن العشرين و أصبح من الإيديولوجيات الحديثة بأن تجعل فعل الإتصال هو الغاية الأساسية للمجتمع و جعلها تبدو أنها الملاذ الوحيد و البديل و ذلك بإستعمال الطرق المشروعة لإستعمال هذه التقنية الجديدة ومن الطبيعي ينجر عنها إستعمال الغير المشروع ومما يدفع إلى الأشخاص إلى إرتكاب جرائم مرتبطة بهذه التكنولوجيا الجديدة والتي يعرف عنها بالجريمة الإلكترونية، وبما أنها جريمة جديد فقد إختلف الفقهاء في وضع تعريف موحد لهذه الجريمة، لكنها إتسمت بمجموع من الخصائص، وعرفت نوع جديد من المجرمين ولكل مجرم له دوافعه لإرتكاب هذه الجريمة وسنحاول التطرق في هذا الفصل المتكون من مبحثين، في المبحث الأول نتطرق إلى الأسس النظرية والقانونية للجريمة المعلوماتية في التشريع الجزائري، في المبحث الثاني سنتطرق إلى الطبيعة القانونية للجريمة الإلكترونية في القانون الجزائري.

المبحث الأول: المفاهيم المرتبطة بالجريمة المعلوماتية

في هذا المبحث سنحاول التعرض لمختلف عناصر الجريمة الإلكترونية وأركانها التي ترتكز عليها وذلك نظرا لطبيعة البيئة التي تقع فيها من عالم إفتراضي، وذلك عكس الجريمة التقليدية التي تقع في الواقع، وذلك من خلال المطلبين التالين:

المطلب الأول: الإتجهات الفقهية في تعريف الجريمة المعلوماتية

إن الفقه الجنائي لم يعطي تسمية موحدة لجريمة [1] الإلكترونية، فهناك من يسميها الجريمة المعلوماتية وآخرون يسميها جرائم إساءة إستخدام تكنولوجيا المعلومات والإتصال، أو جرائم الكمبيوتر والأنترنت، الجرائم المستحدثة، بالجريمة الناعمة، إجرام ذوي الياقات البيضاء إلا أنه يجب الإشارة إلى أن هناك فرق بين جرائم الحاسب الآلي وجرائم الأنترنت، ففي الأولى تتحقق بالإعتداء على مجموعة الأدوات المكونة للحاسب الآلي وبرامجه والمعلومات المخزنة به، أما جرائم الأنترنت تتحقق بنقل المعلومات والبيانات بين أجهزة الحاسب الآلي عبر الألياف البصرية أو خطوط الهاتف أو الشبكات الفضائية إلا أن الواقع التقني أدى إلى اندماج الميدانين وقد انقسم الفقهاء إلى اتجاهين، المفهوم الضيق للجريمة الإلكترونية Cybercrime والإتصالات ومنهم من ينظر إليها بمفهوم واسع، كما أن للجريمة الإلكترونية أركان لا تقوم الجريمة إلا بتوافرها، وهذا ما سأتناوله في الفرعين المواليين.

الفرع الأول: تعريف الجريمة المعلوماتية

إن موضوع الجريمة الإلكترونية فيه إختلاف حول تحديد نطاق هذه الجريمة فبعض الفقهاء ينظر إليه بمفهوم ضيق، وبعض الآخر بمفهوم واسع، وسنحاول تعريفهما

أولا: تعريف الجريمة الإلكترونية من الإتجاه الضيق (موضوع الجريمة)

1- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ط 20 ، ج 1، دار هومة الجزائر، 2018. ص261

يراى أنصار هذا الإتجاه أن الجريمة الإلكترونية هي "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازم لإرتكابه من ناحية، لملاحقته وتحقيقه من ناحية أخرى" [1] ويعتبر هذا التعريف يضيق بدرجة كبيرة من الجريمة الإلكترونية، بمعنى يجب أن يتوافر قدر كبير من العلم في التكنولوجيا لدى الجناة حسب المعايير التالية. وبما أن الأداة الأساسية المستعملة في هذه الجريمة هو الحاسوب الآلي ولواحقها وأستعمل إحدي الوسائل التقنية الحديثة كالهواتف الذكية والألواح الرقمية وهذا ما ذهب إليه الأستاذ تريدمان TREDMANN أن الجريمة المعلوماتية تشمل أي جريمة ضد المال، مرتبطة باستخدام المعالجة الآلية للمعلومات "كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب بواسطة الحاسوب" [2]

ويرى الأستاذ روزنبلات ROSENBLATT أن " نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو التي تحول عن طريقه " [3] وحسب هذا التعريف فإن الأفعال غير المشروعة التي يستخدم فيها الحاسب الآلي كأداة لإرتكابها تخرج من نطاق التجريم .

أما الأستاذ MAWRE يرى أن " الجريمة الإلكترونية هي فعل غير مشروع الذي يتورط الحاسب الألي في إرتكابه " [4] أما الأستاذ دفيد تومسون عرفها انها " أي جريمة يكون متطلب لإقترافها أن تتوفر لدى فاعلها معرفة بتقنية الحاسب" [5] وهنا نجده انه قد أضاف الى هذه الجريمة بوجوب توفر معرفة كافية لدي الجاني عند إرتكابه لهذه الجريمة.

1- عائشة نايري، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الإداري، جامعة أحمد دراية أدرار، الجزائر، 2017، ص06

2- عائشة نايري، الجريمة الإلكترونية في التشريع الجزائري، ص06

3- عائشة نايري، المصدر السابق، ص06

4- عقباش بريزة مبارك حنان، آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، مذكرة مقدمة لإستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق، جامعة محمد بشير الإبراهيمي، برج بوعريريج الجزائر، 2022، ص 8

5- عقباش بريزة مبارك حنان، آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، ص 8

وكذلك أن جانبا من الفقه وضع عددا من التعريفات التي تقوم على أساس سمات شخصية لدى مرتكب الفعل فمثلا وزارة العدل الأمريكية تبنت في عام 1979 دراسة وضعها معهد ستانفورد للأبحاث حيث عرفت الجريمة المعلوماتية أي جريمة لفاعلها معرفة فنية بالحاسبات تمكن من ارتكابها.

ثانيا :الإتجاه الموسع من تعريف الجريمة الإلكترونية (معالم الجريمة)

إبتداء من منطلق أن الوسيلة المستعملة في إرتكاب الجريمة لا تدخل في تعريف هذه الجريمة أو ما مدى تحكم الجاني في هذه الوسيلة وهذا هو الإنتقاد الذي وجه إلى أصحاب الإتجاه المضيق و من هنا ظهر مفهوم الإتجاه الموسع و الذي يدافع على الإتجاه منهم : [1]

حيث يرى هذا الفريق من الفقهاء ومن بينهم الفقيه باركر PARKER " كل فعل إجرامي معتمد أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه، او كسب يحققه" [2]

أما الفقيهان ميل سيردو فقد عرفها على أنها " تشمل إستخدام الحاسب كأداة لإرتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج كل المصرح به لحاسوب المجني عليه أو بياناته" [3]

وبالتالي هي كل جريمة تتم بوسيلة إلكترونية كالحاسوب مثلا، وذلك باستخدام شبكات الأنترنت من خلال غرف الدردشة، واختراق البريد الإلكتروني ومختلف وسائل التواصل الإجتماعية بغرض إلحاق الضرر لفرد أو مجموعة من الأفراد، وحتى لدولة من الدول تكون ضمن برنامج الإستهداف الحربي، أو الإقتصادي، أو الإضرار بسمعتها أو العكس، ويبقى الهدف واحد، وهو الكشف عن قضايا مستتر عليها، أو نشر معلومات لفائدة طرف أو أطراف

1-عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة مقدمة لإستكمال متطلبات شهادة الماستر المهني، جامعة قاصدي مرباح ورقلة، 2019، ص 04

2- عقباش بريزة و مبارك حنان، آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، مصدر سابق ، ص 9

3- عقباش بريزة مبارك حنان، مصدر سابق ، ص 9

أخرى من باب التسريب، على أنه لمن الضرورة التوسيع من مفهوم هذه الجريمة، ولذلك نجد أن هذا الإتجاه من الفقه أعطى للجريمة المعلوماتية معنى واسعا لتشمل كل أشكال السلوك أو الفعل غير المشروع والذي يرتكب بواسطة جهاز الحاسوب.

ويعتبر هذا الإعتداء على البيانات و البرامج فقد عرفته المنظمة الأوربية للتعاون و التنمية الاقتصادية على أنه عملا إجراميا : "كل عمل أو إمتناع يأتيه الإنسان إضرارا بمكونات الحاسب الآلي المادية و المعنوية وشبكات الإتصال الخاصة به، بإعتبارها من المصالح والقيم المتطورة التي تمتد تحت مظلة قانون العقوبات لحمايتها" [1]

وبصفة عامة ومن خلال هذه التعريفات يمكن القول أنه كل فعل ضار يكون فيه الجاني له معرفة جيدة وكافية بتقنية الحاسوب أو نظاما حاسوبيا، أو شبكة حاسوبية، للوصول إلى البيانات، والبرامج بغية نسخها، أو تغييرها، أو حذفها، أو تزويرها، أو توزيعها بصورة غير مشروعة، أو جعلها غير صالحة، أو حيازتها أو تخريبها.

تكون محل نشاط إجرامي تستخدم فيه هذه التقنية الإلكترونية الحاسوب الآلي أوشبكة الأنترنت بطريقة مباشرة أو غير مباشرة، كوسيلة لتنفيذ الفعل الإجرامي ومن خلال هذه التعاريف يتضح لنا صعوبة قبول هذا التوجه، لأن جهاز الحاسوب الآلي قد يكون محلا تقليديا في بعض الجرائم، كسرقة الحاسب الآلي بنفسه، أو الأقراص الممغنطة، أو الإسطوانات الممغنطة على سبيل المثال .ومن ثم لا يمكن إعطاء وصف الجريمة الإلكترونية إستنادا فقط على سلوك الفاعل وذلك كون الحاسب الآلي أو أي من مكوناته كانت محل للجريمة الإلكترونية. ومنه لا نكون أمام جريمة إلكترونية كما من قام بالإتصال بواسطة حاسب آلي بشركائه في ارتكاب جريمة السطو على بنك.

1- عقباش بريزة مبارك حنان، مصدر سابق ، ص 10

ثالثا: الإتجاه الموسع والضيق لتعريف الجريمة (المختلط)

من خلال التوفيق بين الإتجاه الضيق والموسع نجد أنه قد ظهر إتجاه ثالث ليجد أرضية مشتركة بين الإتجاهات الفقهية، وقد تبنه كذلك منظمة الأمم المتحدة في مؤتمرها العاشر لمنع الجريمة حول جرائم الحاسب الآلي وشبكاته الذي انعقد بفيينا بتاريخ 10 أفريل2000 ، يمكن اعتباره كخلاصة تعريفية لما سبق حيث عرفتها بأنه يقصد بالجريمة الإلكترونية أي جريمة يمكن إرتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام " حاسوب وتشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية "[1]

وهو نفس الإتجاه الذي تبناه المشرع الجزائري وأعطاها مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والإتصال وذلك لأن عملية معالجة المعطيات تحتاج إلى آلية منظمة تتولى عمليات جمع وتوفير المعلومات اللازمة ومعالجتها، وهو الأمر الذي ولد الحاجة إلى إجراءات ووسائل تساعد على القيام بذلك فظهر بالنتيجة مصطلح نظم المعلومات المبنية على الحاسبات الآلية، أو ما يسمى بنظام المعلومات المحوسبة، وهو نظام يعتمد على المكونات والأجهزة البرمجية للحاسوب في معالجة المعطيات واسترجاع المعلومات. فالتطور التقني الحاصل في عالم تكنولوجيا المعلومات وما يتطلبه من ضرورة القيام بمهام توفير وجمع ومعالجة وتبادل المعلومات في نفس الوقت أدى إلى ابتكار نظام المعالجة الآلية، والذي نشأ في الحقيقة بهدف وصف الحالة التي انبثقت عن اندماج تقنية نظم المعلومات وتقنية الاتصالات عن بعد.

ولقد حسن فعلا حين تبنى المشرع الجزائري بموجب أحكام القانون 09-04 المؤرخ في 05-08-2009 وعلى هذا ذهبت أيضا المجموعة الدولية في الإتفاقية الدولية الإجرامية لتقنيات [2] الرقمية بان مفهوم

1- عقباش بريزة مبارك حنان، مصدر سابق ، ص 10

2- أنظر المادة 02 القانون رقم 09-04 المؤرخ في 05 اوت 2009 ، يتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، عدد 47.

وأيضا كما ورد في قانون التجارة الإلكترونية في مادته الثانية تعريفا للنظام المعلومات باعتباره النظام الذي يستخدم لإنشاء رسائل البيانات وارسالها واستلامها أو تخزينها أو لتجهيزها على أي وجه اخر.

الجريمة المعلوماتية " أنه كل آلة بمفردها أو مع غيرها من الآلات المتصلة أو المرتبطة والتي يمكن أن تقوم سواء بمفردها أو مع مجموعة عناصر أخرى تنفيذا لبرنامج معين بأداء معالجة آلية للبيانات "

وعلى المستوى العربي نجد مشروع القانون النموذجي الموحد لمكافحة سوء استخدام تكنولوجيا المعلومات والاتصالات في صيغته المعادلة نجد في مادته الأولى تعريفا لنظام المعالجة الآلية للمعطيات على أنه كل مجموعة مركبة من وحدة أو عدة وحدات المعالجة سواء كانت متمثلة في ذاكرة الحاسوب وبرامجه أو وحدات الإدخال والإخراج والاتصال التي تساهم في الحصول على نتيجة معينة .[1]

وكمثال للجريمة الإلكترونية في الجزائر، سنة 2016 تسرب أسئلة البكالوريا، وقيام القرصان الجزائري حمزة بن دلاج بقرصنة حسابات بنكية عالمية الذي ألقي عليه القبض من طرف الشرطة الفيدرالية الأمريكية [2]

ثانيا: صور الجريمة المعلوماتية

1) الدخول غير المرخص به

هنا يكون الدخول باستعمال الوسائل الفنية والتقنية للنظام المعلوماتي، وبغض النظر إن كان الدخول إلى النظام بأكمله أو إلى جزء منه فقط.

والجزاء لهذه المخالفة يكون بمجرد تحقق الركن المادي للجريمة، والذي يكمن في فعل الدخول، وطبعا يوقع العقاب حتى على مجرد المحاولة أي الشروع في الجريمة بغض النظر عن تحقيق النتيجة الإجرامية، وهو ما أدى إلى الإقرار أن هذه الجرائم من الجرائم الشكلية، التي لا تشترط لقيامها تحقق النتيجة.

1- عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري ، مصدر سابق ، ص 25

2- المصدر السابق، 25

2) البقاء غير المرخص به

ويقصد به هنا الدخول إلى النظام والاستمرار في التواجد داخله وذلك دون إذن صاحبه، رغم علمه بأن بقاءه فيه غير مرخص ولقد سوى المشرع الجزائري بين كل من جريمة الدخول غير المرخص به والبقاء غير المرخص به، وهو ما تأكد بتطبيق الجزاء نفسه على السلوكين

المطلب الثاني: عناصر الجريمة المعلوماتية (أركان، خصائص، دافع)

الفرع الأول: أركان الجريمة المعلوماتية

إن البيئة التي تقع فيها الجريمة المعلوماتية تكون على مستوى الحاسب الآلي وشبكة الأنترنت مما يعطيها الفضاء الإفتراضي إلا ان تجسيد آثارها تلمس الواقع وهذا ما يجعلها تشترك مع الجريمة التقليدية في وجود الفعل الغير المشروع وتشترك أيضا بتوفر أركان أي جريمة، ونتطرق إلى إظهار أركان هذه الجريمة الجديدة

أولا: الركن الشرعي لجريمة المعلوماتية

إن المقصود بالركن الشرعي هو وجود نص يجرم هذا الفعل ويضع العقاب المخصص لها، وذلك لأنه لايجوز معاقبة أي شخص على فعل لم يتم إصدار نص قبل تجريمه، أو بعد إلغائه كما لايجوز قياس أفعال لم ينص المشرع على تجريمها وأفعال أخرى ورد نص التجريم عليها مهما يكن بينها من تشابه من حيث الدوافع أو الفاعلية أو النتائج أو العناصر، ذلك أنه لا يجوز أيضا التوسع في تفسير النصوص الجزائية، وعلى القضاة التقيد بمدلول النص والالتزام بمضامينه [1] ويترتب على إهمال هذه القاعدة الشرعية للجرائم والعقوبة النتيجة والتي تتمثل في عدم رجعية القاعدة الجنائية، أي بمفهوم المخالفة تنطبق القواعد الجنائية بأثر فوري ولا مجال لإهمالها بأثر رجعي، إلا إذا نص القانون على ذلك صراحة في النص القانوني أو إذا ما أعملت قاعدة تطبيق القانون الأصلح للمتهم ويعتمد الركن الشرعي للجريمة هو الصفة

1- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص ، مرجع سابق ، ص261

الغير مشروعة للفعل الذي يقوم به الجاني له ركنين أساسين:

- ألا يخضع الفعل المرتكب لسبب من أسباب الإباحة (أي أن يكون النص الواجب التطبيق يقرر نفس العقوبة.

- مطابقة الفعل لنص التجريم (أي تطابق الأفعال التي يجرمها القانون مع النصوص التشريعية الموجودة).

وهذا ما نص عليه المشرع على مكافحة لجرائم المعلوماتية من خلال تعديله لقانون العقوبات لسنة 2004 وأضافه إلى القسم 7 مكرر الموضوع تحت مسمى " **المساس بأنظمة المعالجة الآلية للمعطيات**"

Des atteintes aux systèmes de traitement automatisé des donnes

وإعتمادا على معيار نجد أن النظام المعلوماتي له دور في تحديد معالم الجريمة، فسمى المشرع الجزائري الجرائم الموجهة ضد النظام المعلوماتي بجرائم المساس بأنظمة المعالجة الألية للمعطيات، كما بينها في قانون العقوبات من المادة 394 مكرر إلى 394 مكرر 8 وبذلك ترك المجال واسع لأي جريمة أخرى ترتكب عن طريق منظومة معلوماتية أو نظام الإتصالات الإلكترونية.

ثانيا) الركن المادي والركن المعنوي للجريمة المعلوماتية

1- الركن المادي للجريمة المعلوماتية

هو كل فعل أو سلوك إجرامي صادر من إنسان عاقل سواء كان إيجابيا أو سلبيا، ينتج عنه توقيف نظام المعالجة الآلية للمعطيات، ويلزم تحققه حتى يمكن البحث في توافر أو عدم توافر أركان أي جريمة من جرائم الاعتداء على هذا النظام، فإن ثبت تخلف هذا الشرط، فلا يكون هناك مجال لهذا البحث إذ يعتبر هذا الشرط عنصر ضروري لكل منها. [1]

1- عقباش بريزة مبارك حنان، آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، مرجع سابق، ص 8

- توفر جهاز الحاسوب نفسه أو تمتد إلى شبكات الاتصال أو البرامج والمعطيات ويمثل نظام المعالجة الآلية للمعطيات
- الحماية التقنية للنظام المعلوماتي حتى يتمكن الإستفادة من الحماية الجزائية لنظام المعالجة الآلية للمعطيات يجب أن يكون متوفر على الحماية التقنية وهذا ما ذهب إليه أغلب الفقهاء، وحجتهم في ذلك أن الاعتداء على النظام الأمني شرط مفترض لقيام الجريمة المعلوماتية، وأن القضاء يقضي بعدم العقاب على فعل يعد اعتداء على حق لم يتحوط له صاحبه، بالإضافة إلى أن تغيب هذا الشرط يعد توسعا في التجريم فكل دخول

إذن غير مشروع يعد جريمة وهو أمر غير منطقي، وهذا الذي مجلس الشيوخ الفرنسي أن النظام لابد أن يكون محميا بجهاز للأمان وأن الأنظمة المحمية تقنيا هي وحدها التي تحضى بالحماية الجنائية.

إلا أنه على عكس ذلك ذهب فقهاء فرنسيين إلى عدم إشتراط الحماية التقنية للنظام المعلوماتي حتي تقوم الجريمة لأن سوء نية من قام بانتهاك النظام والدخول إليه بطريقة غير شرعية، ويدخل في عداد إثبات القصد الجنائي.

ولما كانت مكونات النظام المعلوماتي غير المادية لا تظهر على حالة واحدة إذ قد تكون مخزنة به أو منقولة منه أو عليه، فإن الأمر يتوجب التطرق لدراسة المقصود بنظام المعالجة الآلية للمعطيات.

وبذلك يتحقق الركن المادي [1] للجريمة المعلوماتية إذا تم الاعتداء على النظام المعالجة الآلية للمعلومات أو سلامته، كما نكون في حالة الدخول والبقاء غير المشروع في هذا النظام بالحذف أو التغيير أو في المعطيات، كما يمكن اعتبار التخريب أو أي إتلاف في نظام الاشتغال اعتداءات مادية (المادة 394 مكرر ق ع ج.) يؤدي إلى نتيجة تمس حقا من الحقوق، التي يكفلها الدستور والقانون وقد ذهب الدكتور

1-إيمان بغدادي، أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الإلكترونية، مجلة آفاق للبحوث والدراسات السياسية دولية محكمة، العدد 04، المركز الجامعي إليزي، الجزائر، 2019. ص 189

أحسن صقيعة إلى تقسيم الركن المادي في حد ذاته إلى ثلاث عناصر:

السلوك الإجرامي – النتيجة الإجرامية– العلاقة السببية بين الفعل والنتيجة.

أ–**السلوك الإجرامي** :هذا السلوك يوجد بصورتين فقد يكون بفعل إيجابي، إذ يفترض في هذه الصورة قيام الجاني بفعل إرادي بغية إحداث نتيجة معينة، كما يمكن أن يكون بفعل سلبي يأخذ وصف الامتناع عن إتيان أمر يوجبه المشرع، وفي الجريمة المعلوماتية نجده بنوعيه السلوك الإيجابي او السلبي. وذلك نتيجة التطور الكبير في محتوى وطبيعة هذا السلوك الإجرامي الذي تطور بتطور الوسائل التي وجدت بين يدي الفاعل، وهذا السلوك الذي طورته أيضا عقلية الفاعل الذكية، والتي استطاعت أن تخرج من تقليدية السلوك الجرمي إلى مساحات أكثر تعقيدا أوجدت بلا شك صعوبات كثيرة

ب –النتيجة الإجرامية: يقصد بها السلوك الذي قد يحدث تغييرات ملموسة، وهو يقوم على أساس ما يعتد به المشرع وما يترتب عليه من نتائج، بغض النظر عما يمكن أن يحدثه السلوك الإجرامي [1]من نتائج أخرى

ج –العلاقة السببية بين الفعل والنتيجة :تتمثل العلاقة السببية في الصلة التي تربط بين الفعل والنتيجة، وتثبت أن ارتكاب الفعل هو الذي أدى إلى حدوث النتيجة وأهمية الرابطة السببية ترجح إلى إسناد النتيجة الى الفعل هو شرط أساسي لتقرير مسؤولية مرتكب الفعل عن النتيجة، وتحقق الرابطة السببية تلازما ماديا بين الفعل والنتيجة يؤدي إلى وقوف مسؤولية الجاني عند حد الشروع، إذ لا يعد مسؤولا عن النتيجة التي تحققت، أما إذا كانت غير عمدية فإن نفي الرابطة السببية يؤدي إلى انتفاء المسؤولية كلية عنها ذلك أنه لا شروع في الجرائم غير العمدية

ثانيا: الركن المعنوي

يقوم الركن المعنوي للجريمة الإلكترونية على أساس مجسد في توافر الإرادة الجرمية لدى الفاعل، لذلك انه

1–عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مصدر سابق ، ص 14

يقوم الركن المعنوي للجريمة الإلكترونية على أساس مجسد في توافر الإرادة الجرمية لدى الفاعل، لذلك انه يوجد اتجاه من الفقه أن القضاء الأمريكي لم يستقر على حال بالنسبة لبعض الجرائم التي ترتكب باستخدام الانترنت ، من حيث مدى تحديد إذا كانت تتطلب قصدا عاما أم خاصا ، فالقصد الخاص يتوافر في بعض الجرائم المعلوماتية ، خاصة وأن الجرائم المعلوماتية تقوم بتوافر القصد العام ، أي علم الجاني بمضمون فعله أنه يقوم بعمل غير مشروع ، وارتباط هذا العلم بالإ رادة ، ومثال عنها ما حكمت به محكمة النقض الفرنسية بتوافر نية التملك الوقتي في جريمة سرقة المعلومات من جهاز الحاسوب ، ويكفي ليقام تحقق هذه النية هو سلب وحيازة المستندات خلال وقت معين بدون إرادة صاحبها الشرعي أو الحائز عليها بصفة دائمة أو مؤقتة ، أي توفر نية المشاركة في الانتفاع بها كذلك الحال بالنسبة لجريمة التزوير المعلوماتي ، بتوفر نية إضافية لدى الجاني ترمي إلى استعمال المستند المزور، ولم يستعمل من الناحية الفعلية ، فنكون في الحالة الأخيرة أمام قصد احتمالي عند بإمكانية إحداث ضرر

وكل ذلك يجعلنا أمام حالة صعوبة إثبات القصد الجنائي الخاص، وبالتالي صعوبة إثبات الركن المعنوي للجريمة المعلوماتية، وتوجيه هذه الإرادة إلى القيام بعمل غير مشروع جرمه القانون كانتحال شخصية المزود عبر الانترنت. وسرقة أرقام البطاقات الائتمانية، كما يجب أن تتوفر النتيجة الجريمة المترتبة على الأفعال السابقة، فتكتسب إ رادة الجاني الصفة المجرمة من العمل غير المشروع الذي يبين الشبه في ارتكابه وهو عالم بالآثار الضارة الناشئة عنه

ويختلف الركن المعنوي [1] في الجرائم المعلوماتية من جريمة إلى أخرى، فجريمة الدخول غير المصرح به إلى نظام الحاسب الآلي تتطلب قصدا جنائيا عاما يتمثل في علم الجاني بعناصر الركن المادي للجريمة أي العلم بأن الولوج إلى داخل النظام المعلوماتي بشكل غير مصرح به يعد جريمة باعتبار حماية المشرع

1- عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مصدر سابق، ص 15

لمحل الحق وهو جهاز الحاسب الآلي لما يتضمنه من معلومات وبرامج، وعلى هذا النحو فدخوله إلى نظام الحاسب الآلي خطأ أو سهوا ينفي عنه شرط القصد الجنائي بشرط المغادرة فور علمه بدخوله غير الشرعي وفي جريمة الاحتيال الإلكتروني التي بدورها جريمة عمدية، يتطلب المشرع قصدا جنائيا لقيام مسؤولية الجاني، والقصد الجنائي المشترط هو القصد الجنائي بنوعية العام والخاص، فالمجرم يعلم أنه يخالف القانون بسلوكه مع اتجاه نيته إلى تحقيق ربح غير مشروع له أو للغير أو تجريد شخص أخر من ممتلكاته على نحو غير مشروع.

الفرع الثاني: خصائص الجريمة المعلوماتية

أولا: خصائص متعلقة بالجريمة المعلوماتية

تعتبر أهم خصائص التي تميز الجرائم المعلوماتية عن غيرها من الجرائم التقليدية وهي كالآتي:

- جريمة عابرة للأوطان

إن أطراف الشبكة العنكبوتية المتشعبة في جميع أنحاء العالم ولا ترتبط بإقليم جغرافي معين، بل يكفي توفير جهاز حاسوب. [1]

ويكون مزودا بالشبكة المعلوماتية لارتكاب جريمة معلوماتية في أي مكان في الكرة الأرضية.

وبذلك أصبحت هذه الجريمة تخص كل سكان العالم دون إستثناء، مما أدى إلى حتمية التعاون والتنسيق الدوليين من أجل مكافحة هذه الجرائم بكافة الوسائل المتاحة بداية من خلال إبرام اتفاقيات ومعاهدات دولية ، وفتح المجال واسعا للقيام بإجراءات التحري والتدقيق اللازمين لكشف مرتكبي هذه الجرائم من خلال تحديد القانون الواجب التطبيق في هذه الحالات، وتحديد الدولة صاحبة الاختصاص القضائي

1- علي إبراهيم بن دراح، محاضرات في الجرائم المعلوماتية، مطبوعة بيداغوجية المركز الجامعي آفلو جامعة عمار ثليجي الأغواط الجزائر، 2021.ص 07

02: صعوبة اكتشاف الجريمة المعلوماتية

في أغلب الأحيان الضحية لا يلاحظها وذلك بسبب أن الجاني يمتلك قدرات فنية تمكنه من ارتكاب جريمته بدقة عند إرسال الفيروسات وسرقة الأموال والبيانات الخاصة أو إتلافها والتجسس وسرقة المكالمات وغيرها من الجرائم. [1]

كما أن وسيلة تنفيذها تتميز في أغلب الأحيان بالطابع التقني الذي يضفي عليها الكثير من التعقيد بالإضافة إلى حجم التبليغ عن هذه الجرائم في حالة اكتشافها لخشية المجني عليهم فقدان عملائهم فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل إثبات.

03: صعوبة إثبات الجريمة المعلوماتية

نظرا أن هذه الجريمة تقع في بيئة إفتراضية غير تقليدية بواسطة الحاسوب ومنه لا يمكن لسلطات الأمن وأجهزة التحقيق والملاحقة، وذلك ما تتطلبه هذه الجرائم من أسلوب خاص في التحقيق والتعامل، الأمر الذي لم يتحقق في الجهات الأمنية والقضائية، وذلك لنقص وتخصص في التقنية لتحصين الجهاز الأمني والقضائي ضد هذه

الظاهرة، حيث لم تعد القوانين التقليدية قادرة على مواجهة تطور الجريمة المعلوماتية في ظل التطور السريع للتكنولوجيا.

04 :أسلوب ارتكاب الجريمة المعلوماتية

الجريمة المعلوماتية هي جريمة ناعمة خالية من العنف أو صور الكسر أو الخلع كما هو الأمر في الجريمة الكلاسيكية، فالمجرم يوظف خبراته النظرية والإطار المنهجي للدراسة أو اختراق لخصوصيات الغير و التعامل مع الشبكة للقيام بجرائم المختلفة كالتجسس على القاصرين و دون الحاجة لسفك الدماء.

1- هاشم بشير، الآليات الدولية لمكافحة الجريمة الإلكترونية، المركز الدولي للدراسات المستقبلية والإستراتيجية، القاهرة مصر، 2012 ، ص8

05: الأشخاص المشاركين في الجريمة المعلوماتية

تتم هذه الجريمة إلا بتعاون وبساعدة أحد من محيط المؤسسة المستهدفة بهذه الجريمة، فمن جهة يقوم المجرم المتخصص في الحاسوب والأنترنت وطرق الإختراق الإلكتروني بالعميل من داخل المؤسسة [1] لتغطية التلاعب و تحويل الأموال إلى المجرمين، وهذا على عكس المجرم التقليدي الذي لايحتاج إلى معرفة أو مستوى دراسي

ثانيا: خصائص متعلقة بالجاني

1: المجرم الإلكتروني: كما أن للجريمة الإلكترونية كغيرها من الجرائم أطراف تتمثل في الجاني وهو يكون شخصا طبيعيا ذا أهلية وقدرة على تحمل العقوبة أو شخص معنوي.

- ✓ **سمات المجرم الإلكتروني**

المهارة والذكاء: يقوم المجرم بالتعرف على كافة الظروف المحيطة بالجريمة ومعرفة كل نقاط القوة و الضعف و يقال عن هذه الجريمة بأنها جريمة الأذكياء بالنسبة للجريمة التقليدية التي يكون العنف أساسها في حين المجرم الإلكتروني يستعمل مهاراته في مجال تكنولوجيا المعلومات من أجل إختراق الحواجز الأمنية من أجل تحقيق غرضه من هذه الجريمة يدعي المجرم الإلكتروني بأن ما يقوم به ليس موجود في قائمة الجرائم وخاصة أنه لا يريد الإضرار بالأشخاص بل هو يريد إظهار تفوقه على الحاجز الأمني الخوف من الكشف عنه مما لها من تابعات من فقدان وظيفته أو الأموال التي تحصل عليها بطريقة غير مشروعة ومما يترتب عليها من متابعة جزائية

تقليد الآخرين حيث يميل بعض المجرمين إلى تقليد الآخرين وإتباع خطواتهم في الإختراق والتخطي للحواجز الأمنية.

1-إيمان بغدادي، أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الإلكترونية، مصدر سابق، ص 187

- ✓ التخطيط المسبق للجريمة حيث يقوم بالتخطيط والتنظيم في داخل الشبكة العنكبوتية مثلها مثل الجريمة التقليدية، حيث يقوم مجموعة بالتعاون داخل هذا التنظيم للقيام بالجريمة كل حسب دوره
- ✓ التكيف الاجتماعي يظهر هذا النوع عند وجود مجموعة مثلا من صغار النوابغ للمعلوماتية، وتنتج منها علاقات وروابط صداقة ومنها ما يكون حتي علاقات دولية، وهذا مما يدع مجال كبير للوقوع في تحديات فيما بينهم، تكون نتيجتها الوقوع في جرائم حسب تأثير دافع كل مجرم منهم فمنها الدوافع الشخصية أو الموضوعية.

02 - طوائف المجرم الإلكتروني

المخترقون (المتطفلون)

الهاكرز (صغار النوابغ): هو الشخص البالغ المقترن الحواسيب الآلية والذي بقوم بإنشاء أو تعديل البرمجيات، وأغلبهم يكونون طلبة لهم معارف كبيرة في مجال التقنية المعلوماتية ويكون الدافع الأكبر لهم الإستمتاع واللعب والمزاح من أجل إثبات مهاراتهم دون قصد إلحاق الضرر وذلك بإكتشاف مواطن الضعف في أنظمة الحماية وهناك أنواع للهاكرز[1]

- ✓ الهاكر الأخلاقي (ذو القبعة البيضاء) هو الهاكر الذي يقوم بإصلاح الأخطاء
- ✓ الهاكر المفسد (ذو القبعة السوداء) يكون دوره في الإفساد و التخريب
- ✓ الهاكر المترنح (ذو القبعة الرمادية) يقوم بأعمال الإصلاح و أحيانا بالعبث
- ✓ الكراكز: هو المقتحم ويكون من ذوي المكانة الاجتماعية العالية ويكون متخصص في هذا المجال ويمكنهم التحكم الكامل في بيئة المعالجة الآلية للمعلومات

1- نهلا عبد القادر المومني، الجرائم المعلوماتية، ط 2 ، دار الثقافة للنشر و التوزيع، عمان الأردن، 2010، ص 79

- ✓ **مجرم الحاسب الآلي المحترف:** يخضع ما تعلمه من تنفيذ جريمته بكل إحترافية من أجل سحب الأموال من أرصدة ضحاياه لحسابه او لحساب من جنده لتحقيق أغراض سياسية أو فكرية أو إجتماعية. وتعتبر هذه الفئة الأخطر في عالم الإجرام الإفتراضي
- ✓ **الحاقدون:** يعتبر أهم دافع لهذه الفئة هو الإنتقام من رب العمل ويكونوا مقسمين إلى ثلاثة أقسام إما مستخدم للنظام بصفته موظف في هذه المؤسسة أو مشترك بالنظام محل الجريمة او غريب عن المؤسسة يتعاون مع من هم بداخلها لتغطية اللأعيب
- ✓ **مجرم ذوي دافع سياسي:** من أجل الحصول على المعلومات السياسية والبيانات الغاية السرية المتعلقة بالدفاع والأمن للدولة فهنا المجرم يوظف ذكائه ومهاراته لإكتشاف الثغرات وإختراق البرامج المحصنة للحصول على مبتغاه من معلومات سرية تؤدي بضرر خطير جدا قد تؤدي إلى إنهيار تام لهذا الكيان.
- ✓ **صغار السن:** هم النوابغ المعلوماتية التي تكون دون سن الأهلية وتكون الحواسيب شغفهم الدائم وحبهم لإثبات مهاراتهم لتحدي أنظمة الحماية وكسرها ورغم الخطر التي تمثله ظهر راي آخر يقول أن هذه الفئة من النوابغ المعلوماتية قد أثارة جدلا كبير بين الفقهاء و طلبوا بإخراجهم من دائرة التجريم إلى دائرة العبث أو البطولة ومن بين المؤلفات التي تدعوا إلى ذلك كتاب " خارج نطاق الدائرة الداخلية كيف تعلمها؟" للمؤلف لبيب لاندريد الأمريكي، وكتاب " المتعلثمين أبطال ثورة الحاسوب" جهاز حاسوب [1]

أما المجني عليه فيكون في أغلب الأحيان شخص معنوي، كالبنوك والشركات وغيرها من المنظمات أو الهيئات التي تعتمد في إنجاز أعمالها على الحاسب الآلي، وعلما أن محل الجريمة الإلكترونية يتمثل في المعلومات، الأجهزة، الأشخاص أو الجهات

1- عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري ، مصدر سابق، ص 9

ثالثا – دافع لإرتكاب الجريمة

إن أول إهتمام للمجرم هو الوصول إلى المعلومات بشكل غير شرعي كسرقة المعلومات أو الإطلاع عليها أو حذفها أو تغييرها وذلك عن طريق الشبكة العنكبوتية وصولا إلى أجهزة الخادمة الموفرة للمعلومات وتعطيلها أوالتلاعب بمعطياته، لذلك تختلف أسباب الدوافع فمنها شخصية، ذهنية أو موضوعية

أ: الدوافع الشخصية:

تكون هذه الأهداف عادة إلى أهداف مادية أو ذهنية

الدوافع المادية

تصنف كأكبر دافع للجاني لإقتراف الجريمة الإلكترونية وذلك لإنها تعتبر أكبر وأسرع طريقة لتحقيق الربح السريع و السهل وفي نفس الوقت تجعل الجاني من تطوير نفسه لمواكبة التطور السريع للتكنولوجيا و الكشف عن الثغرات التي تمكنه المرور منها للوصول إلى أنظمة المعالجة الآلية لتحويل مبالغ مالية لحسابه أو لحساب شركائه، كما يتم الحصول على هذه المعلومات السرية للجهات المستخدمة للتكنولوجيا كالمؤسسات والبنوك والجهات الحكومية والأفراد أو إبتزازهم من خلالها دافع مادي أو سياسي، وتحقق الكسب المادي أو المعنوي أو السياسي غير المشروع عن طريق تقنية المعلومات مثل عمليات اختراق وهدم المواقع على الشبكة العنكبوتية وتزوير وسرقة الحسابات المصرفية [1]

– الدوافع الذهنية

تقوم على شغف الجاني وحبه للمتعة والتحدي أنظمة الحواسيب الآلية وأنظمتها المعقدة للحماية وان الجاني لا يمكن قهره وانه يمكنه تخطي كل الحواجز الأمنية وهذه العملية تعطي للجاني متعة كبيرة وشعور بقوته على التفوق على التكنولوجيا الحديثة وغالبا ما يكون هذا الهدف ليس بنية التخريب أو دوافع

عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري ، مصدر سابق، ص 9

حقد أو غيرها بل هي من دافع التحدي، وتعطي للجاني متعة كبيرة وشعور بقوته على التفوق على التكنولوجيا الحديثة وغالبا ما يكون هذا

الهدف ليس بنية التخريب أو دوافع حقد أو غيرها بل هي من دافع التحدي.

ب: الدوافع الموضوعية لإرتكاب الجريمة الإلكترونية

نتيجة لبعض المواقف التي يتعرض لها الجاني لإرتكاب الجريمة الإلكترونية وهنا لاتكون من باب التسلية أو المتعة ومن هذه المواقف هي:

- دافع الإنتقام وإلحاق الضرر برب العمل

ينتج هذا الهدف عندما يتعرض الجاني للفصل من عمله أو عدم الإستفادة من الترقية أو الحوافز ونتيجة لمعرفته الكبيرة للمعلومات عن المؤسسة أو الشركة فيدفعه إلى الإنتقام من رب العمل [1]

- هدف التعاون والتواطؤ

يحدث هذا النوع من الجرائم عندما يتعاون في المشروع الإجرامي بأحد من المؤسسة أو من محيطها مع أحد آخر يكون متخصص في الأنظمة المعلوماتية للقيام بتغطية عمليات التحويلات المالية أو تبادل المعلومات حول نشاط هذه المؤسسة. لذلك نجد أن الدوافع هنا تكون مركبة منها المتعة أو التسلية وقد تتطور إلى الحيازة والإبتزاز والحصول على الأموال ومنه نجد أن الجريمة الواحد لها دوافع متعددة نتيجة لعدد المشاركين فيها وكل شخص يريد تحقيق أهدافه الخاصة.

1- عائشة نايري، الجريمة الإلكترونية في التشريع الجزائري، مصدر سابق ، ص 11

المبحث الثاني: الطبيعة القانونية للجريمة المعلوماتية في القانون الجزائري

جريمة الدخول في كل أو جزء من منظومة للمعالجة الآلية لمعطيات، ونجد أن المشرع قد جرم فعل الدخول بطريق غير شرعية إلى أي منظومة معلوماتية دخولا غير شرعي ، وذلك حين عبر عنه بطريق الغش

المطلب الأول: الأساس القانوني (394 مكرر وما بعدها) تحليل للنصوص القانونية

الفرع الأول: الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

أولا: جريمة الدخول والبقاء عن طريق الغش إلى نظام المعلوماتية

كما أن المشرع لم يفرق بين الدخول إلى جزء من المنظومة أوكله ونفهم من ذلك أن المشرع الجزائري قد أخذ بشكل الجريمة عندما أخذ بتسليم بمجرد الدخول إلى النظام معلوماتي عن طريق الغش يتوفر هنا مباشرة القصد الجنائي حتى ولو لم يسبب ذلك أي تخريب أو ضرر بالبيانات لكونها جريمة وقتية، ولكن المشرع لم يتوقف عند هذا الحد بل جرم حتى المحاولة وإعتبرها جريمة لها نفس العقوبة المقررة في المادة **تنص المادة 394 مكرر** [1] من ق ع ج ، للمعطيات أو يحاول ذلك أي بمعنى كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية سيتعرض للجزاء.

- **جريمة البقاء**

إن بقاء الجاني داخل النظام المعلوماتي بعد الدخول عن طريق الغش ماهو إلا تفسير واضح مما لا يدع الشك في توفر القصد الجنائي و بذلك يصبح الجاني مرتكبا لجريمة مستمرة وهذا ما أدى إلى المشرع إلى عدم التفريق بين الدخول و أو البقاء في نظام المعلوماتية و من أجل توفير حماية أكبر فقد جرم أيضا حتى المحاولة جرمها و ذلك لإعطاء أهمية لهذه الجريمة الخطيرة التي تهدد المجتمع بصفة عامة، وهذا هو الذي

1- علي إبراهيم بن دراح، محاضرات في الجرائم المعلوماتية، مصدر سابق ، ص 47

نلاحظه عندما وضح المشرع ذلك في الفقرة الثانية من نص المادة 394 مكرر من ق ع ج.

- **جريمة حذف أو تغيير في معطيات المنظوم كنتيجة الدخول الغير شرعي أو البقاء**

إن الفعل الإجرامي الذي يقوم به الجاني بحذف البيانات من نظام المعلومات او تغيير للمعلومات، فرغم من إختلاف الفعلين إلا أنه المشرع الجزائري إعتبرهما جريمتين خطيرتين و لذلك فقد ضاعف العقوبة وهذا نتيجة لخطورتهما وخطورة النتائج المترتبة عليهما. [1] و هذا الأمر نلاحظه في نص الفقرة الثانية من نص المادة 394 مكرر فقرة الثانية

-جريمة تخريب نظام الاشتغال نتيجة دخول الغير الشرعي أو البقاء

لم يعتبر المشرع الجزائري جريمة تخريب نظام جريمة مستقلة بذاتها عن جريمة الدخول الغير الشرعي أو البقاء بل باعتبارها نتيجة للجرائم السابقة، وذلك يرجع إلى أنه من الممكن حدوث تخريب لهذا النظام[1] ابتداء دون توفر القصد الجنائي إلا عندما يكون كنتيجة لجريمة سابقة وهذا ما أشار إليه المشرع الجزائري في نص المادة 394 مكرر فقرة 3

ثانيا: جريمة إدخال معطيات في نظام المعالجة الآلية أو إزالتها أو تعديلها عن طريق الغش

اعتبر المشرع أن إدخال معطيات المغشوشة في نظام المعالجة الآلية جريمة معلوماتية تستوجب عقوبة ، والتي ضاعفها إذا ما قورنت بالعقوبات السابقة ، وذا كان قد ربط فعل الحذف بالنتيجة المترتبة عن الدخول غير الشرعي أو البقاء ، فقد اعتبر جريمة الإزالة جريمة مستقلة في حد ذاتها تستوجب نفس العقوبة السابقة بالرغم من اتفاقية بودابست وكذا المشرع الفرنسي استعمل مصطلح الحذف لإستخدامه ضمن نفس المعنى وهو الإسقاط بينما يعني مصطلح الإزالة هو الإبعاد من المكان ، ومنه فان المشرع قد يكون فرق في الآثار بين الفعلين ، فحذف بيانات إلكترونية محددة وإسقاطها من موقعها في النظام المستهدف ولوكان بصفة مؤقتة، وبذلك تكون قابلة للاسترجاع عن طريق برامج خاصة لإسترجاع هذا النوع من المعلومات، ولكن

1- علي إبراهيم بن دراح، محاضرات في الجرائم المعلوماتية، مصدر سابق ، ص 47

إزالة البرامج تهدف إلى التخلص نهائيا منها وبشكل كامل ، لذلك يكون المشرع قد فرق بين الفعلين الإجراميين واعتبر الفعل الأخير أشد خطورة ، لذا فرق بين العقوبة المقررة لكل فعل مجرم منهما، وهذا ما أشار إليه المشرع الجزائري في نص المادة 394 مكرر 1

ثالثا: جريمة تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في المعطيات عمدا وعن طريق الغش من الملاحظ هنا أن المشرع الجزائري قد من توفر عدة شروط لقيام هذه الجريمة:

توفر القصد الجنائي لدى الجاني في هذه الحالة علمية تصميم برنامج معين أو بحث في برنامج معين آخر أو نشره وحتى الاتجار فيه لا يعتبر جرما في حد ذاته إذا سبقها توفر نية مسبقة لارتكاب جريمة معلوماتية تعتمد بالأساس على توفر علم مسبق لدى الجاني بان هذا البرنامج مغشوش.

يكون هذا الجرم مرتبطا بأفعال محددة وهي تصميم أو بحث أو تجميع أو توفير أو نشر أ والاتجار في المعطيات ، وعليه فان أي فعل آخر يمس هذه المعطيات لا يندرج ضمن هذا الإطار.

تكون المعطيات محل الجرم مخزنة أو معالجة أو مرسلة عن طريق منظومة [1] معلوماتية وهنا نجد المشرع قد إعترف ضمنا بضرورة أن تكون المعطيات تتوفر على قدر كاف من الحماية، لأن المساس بالمعطيات المتاحة والمتوفرة للجمهور لا يمكن أن تكون محل متابعة جزائية ، وبذلك يكون المشرع قد تأثر بالاتفاقيات والقانون المقارن الذي سعى إلى هذا الاتجاه لاسيما اتفاقية بودابست. كما يمكن إن يكون هذه الجرائم سببا غير مباشر في إرتكاب الجرائم المعلوماتية السابقة، وعليه فان المشرع قد قرر لها نفس العقوبة في نص المادة 394 مكرر2 ، جريمة حيازة أو إفشاء أو نشر أو استعمال معطيات المتحصل عليها من الجرائم سابقا عمدا وعن طريق الغش، وهنا نجد أن حتى الحيازة للمعطيات أو إفشائها جريمة يعاقب عليها القانون وهذا ما أشار إليه المشرع الجزائري في نص المادة 394 مكرر 2 فقرة 2

1- علي إبراهيم بن دراح، محاضرات في الجرائم المعلوماتية، مصدر سابق ، ص 47

الفرع الثاني: الجرائم الواقعة على الأشخاص والأموال

هي الجرائم التي تكون بالاعتداء أو تهدد بالخطر الحقوق ذات الطابع الشخصي، أي الحقوق اللصيقة بالشخص والتي تعتبر من بين المقومات الشخصية وتخرج عن دائرة التعامل الاقتصادي، ومن أهم هذه الحقوق الحق في الحياة والحق في سلامة الجسم وفي الحرية والحق في صيانة الشرف.

أولا: الجرائم الواقعة على الأشخاص

جريمة انتحال الشخصية : هي جريمة قديمة جدا تتمثل صورها في الكثير من الجرائم التي ترتكب بالطرق التقليدية، إلا أنه ومع انتشار شبكة الانترنت فقد أخذ هذا النوع شكلا جديدا وهي إنتحال شخصية الفرد على الشبكة الالكترونية واستغلالها أسوء استغلال ، وذلك بأخذ البيانات الشخصية كالعنوان وتاريخ الميلاد ورقم الضمان الاجتماعي وما شابهها من أجل الحصول على بطاقات ائتمانية وغيره، ومن خلال هذه المعلومات يستطيع المجرم إخفاء شخصيته الحقيقية والتصرف بحرية تحت اسم مستعار ، وغالبا ما يتحصل المنتحل على تلك المعلومات عن طريق الكم الهائل من الإعلانات التي تزدحم بها شبكة الانترنت.

جريمة المضايقة والملاحقة :

وهي عبارة عن مساحات معروفة في الفضاء الالكتروني تمكن لمستخدميها المشاركة في محادثات بين بعضهم البعض هو نوع حديث من الجرائم يقصد بها إرسال رسائل تهديد وتخويف ومضايقة وقد تم تشبيهه من طرف القضاة لهذه الجريمة كالتهديد العلني ولها نفس التأثيرات السلبية على النفسية الضحية [1]

جرائم التغرير والاستدراج :

تعتبر من أشهر وأكثرها إنتشارا حيث يقع ضحيتها من مستخدمين حسن النية وخاصة من أواسط صغار السن من مستخدمي الشبكة، وهي تقوم على عنصر الإمام حيث يوهم المجرمون ضحاياهم برغبتهم من

1-عقباش بريزة مبارك حنان، آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، مصدر سابق ، ص 26

اجل تكوين علاقة صداقة أو زواج على الانترنت ومن الممكن أن تتطور إلى لقاء مادي بين الطرفين، وهذه الجرائم لا تعرف الحدود ولا يمكن حصرها، وليس لها حدود سياسية أو اجتماعية اذ يستطيع كل متصل عبر الشبكة ارتكابها بكل سهولة [1]

جرائم التشهير وتشويه السمعة:

مع إنتشار الشائعات والدعاية الكاذبة التي تمس رموز جميع طبقات المجتمع سواء كانت تلك فكرية أو سياسية أو حتى دينية، وقد ظهرت على شبكة الانترنت بعض المواقع التي جندت نفسها لخدمة هذه الشائعات بهدف تشهير وتشويه السمعة، وتسميم أفكار الناس أو إبتزاز الأشخاص بنشر الشائعات عنهم، كإرسال الصور الغير اللائقة أو معلومات الكاذبة.

الجرائم المخلة بالأخلاق والآداب العامة:

إن طبيعة شبكة الانترنت هي العالمية يمكن لأي مستخدم أن بتفاعل معها، فإنه يمكن أن يعرض فيها كل ما يشاء من محتوى مها كان، فقد يكون هذا محتوى مخلا بالآداب والأخلاق العامة في بلد معين جريمة يعاقب عليها القانون في حين أنها لا تكون كذلك في بلد آخر [1] وتشمل هذه المحتويات كأعمال الإباحية وتعتبر من أشهرها والأكثر رواجا خاصة في الدول العربية وأوروبا والدول الآسيوية، وتشمل كافة الإشكال سواء كانت الصور أو الفيديو أو حوارات أو أرقام هاتفية مما خول هذه الشبكة أن تكون في متناول أيدي الجميع ودون أي حواجز أو رقابة.

وهنا يجب التفريق بين موضوع الاعتداء على الأموال ينصب على الحاسب الآلي ذاته وما يرتبط به، وسيتم تطبيق النصوص الجزائية التقليدية لأن الأمر يتعلق بمال عادي منقول، أما إذا وقع الاعتداء على نظام الحاسب الآلي من برمجة، فإن النصوص التشريعية التقليدية عاجزة عن حمايتها هذا المجال وهنا يبرز دور التشريع الجديد لحماية هذه الحقوق.

1- عقباش بريزة مبارك حنان، آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، مصدر سابق، ص 26

جرائم صناعة ونشر الفيروسات :

يعتبر الفيروس برنامج مثل أي برنامج آخر موجود على جهاز الحاسب الآلي، ولكنه صمم بطريقة ما، يمكنه التأثير على كافة البرامج الموجودة على الجهاز وتجعله غير قادرة على العمل بصقة عادية أو ممكن تؤدي الى تعطلها عن العمل بصفة جزئية أو نهائية، وذلك نتيجة لطبيعة عملها وحسب تصميمها فهنا من الفيروسات من تبدأ بالعمل بمجرد فتحها للرسالة وتعتبر هذه الطريقة الأكثر إنتشارا من بينها فيروس رسائل الحب، و الدودة الحمراء، حيث أدت إلى تعطل لأكثر من 250 ألف جهاز كمبيوتر في مدة 9 ساعات في سنة 2001

جرائم الاختراقات:

هو عبارة عن عملية دخول غير مصرح به إلى أجهزة الغير او لشبكات الالكترونية، ويتم بواسطة برامج متطورة يستخدمها أصحاب الخبرة والقدرة على تخطي أنظمة الحماية الموضوعة لحماية هذه الحاسبات أو الشبكات .وتختلف أهداف وأسباب الاختراق فمنهم من يخترق لمجرد الفضول والبعض الأخر لسرقتها، وهذا هو السبب الأبرز الذي يدفع المخترقين إلى الدخول إلى مواقع الحواسيب الأخرى لسرقة معلوماتهم التي قد يكونون قد عرضوها مقابل مبلغ مالي للاطلاع عليها.[1] وقد يكون السبب تبديل أو تحريف أو تعطيل المعلومات في أجهزة الغير وتسمى تغيير وجه الموقع، وهو أخطر أنواع الاختراق، ومن أبرز الضحايا هي مواقع الانترنت بتحريف تصاميمها ومعلوماتها .

1-جريمة تعطيل الأجهزة والشبكات:

عن طريق إرسال عدد هائل من الرسائل بطرق فنية معينة إلى الأجهزة أو الشبكات المراد تعطلها وهو الأمر الذي يعيقها عن تأدية عملها، مما يؤدي تعطيل البرامج إلى أعطال فنية

1- عقباش بريزة مبارك حنان، آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، مصدر سابق، ص 29

2-جريمة النصب والاحتيال:

إن طبيعة هذه الجريمة أن الجاني لا يمكن التعرف عليه في الجهة المقابلة من الطرف الآخر للشبكة مما أثرت هذه الحالة على التعاقدات الناتجة عن الأنترنت وأثرت بالسلب

على مصداقيتها وذلك بإستعمال طرق إحتيال جديدة ومبتكرة حيث تظهر وكأنها مواقع حقيقية وبذلك يقع الكثير من مستخدمي الأنترنت ولعل أهم وأبرزها هو سرقة معلومات البطاقات الائتمانية لسرقة المبالغ النقدية الموجودة داخل حسابات الضحايا [1]

ثانيا: الجرائم التي تقع على الأموال

وهي التي تهدد الأموال أي الحقوق ذات القيمة المالية ويدخل في نطاقها الحق ذو قيمة الإقتصادية.

1-جريمة التحويل الإلكتروني للأموال : من أهم نشاطات البنوك الإلكترونية عمليات تحويل ونقل الأموال للزبائن من حساب بنكي الى حساب آخر عن طريق المقاصة الإلكترونية بدلا من التحويلات التقليدية من طرف بنك مؤهل ومرخص له، ويتم ذلك بواسطة أجهزة الحاسوب فالجريمة تكون عندما يكون هذا التحويل غير قانوني وذلك بالتلاعب ببرامج التحويل الخاصة.

2-جريمة القمار عبر الأنترنت : ظهرت النوادي والكازينوهات الافتراضية عبر المواقع الإلكترونية .والخاصة بألعاب القمار لكن غير مسموح لهذه المواقع بممارسة نشاطها حيث اصبحت فيما بعد وكرا لجريمة غسيل الأموال.[2]

3- **جريمة غسيل الأموال:** هي جريمة تقليدية تطورت عن طريق التطور التكنولوجي حيث يتم ارتكابها عن طريق تطهير الأموال والتي يكون مصدرها غير مشروع ويتم إستثمارها بطريقة شرعية عن طريق

1-عقباش بريزة مبارك حنان، آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، مصدر سابق، ص 29

2- علي إبراهيم بن دراح، محاضرات في الجرائم المعلوماتية، مصدر سابق ، ص 55

البنوك، عن طريق نقلها بعملية اقتصادية ومالية للأموال من مصدر غير مشروع الى دائرة الاقتصاد الشرعي.

4-تجارة المخدرات عبر الانترنت

حيث هناك مواقع تروج لاستهلاك المخدرات وكيفية إنتاجها وتعليم تصنيعها و طرق تسويقها وانتاجها.

5- **السطو والسرقة الإلكترونية** : قرصنة أرقام بطاقات الإئتمان البنكية.

6-التزوير الإلكتروني : من بين الجرائم الإلكترونية جريمة التزوير ويعتبر من بين أخطر ما يقوم به المجرم المعلوماتي لأنه يمكن بواسطة الضوئي و الوسائل المتطورة العملة بجودة عالية مما تؤثر على الإقتصاد الوطني

المطلب الثاني: الجرائم الواقعة على المؤسسات العمومية

وتتمثل اساسا في المساس بأمن المؤسسات العمومية والبنوك والمؤسسات الحساسة للدولة وكذلك الجيش الوطني ويدرج هذا النوع من الاعتداءات على أنه من الإرهاب ضد الوطن [1]

الفرع الاول: الإرهاب الإلكتروني

من أخطر الجرائم الإلكترونية جريمة الإرهاب المعلوماتي لكونها تقع هذه الجرائم في عالم إفتراضي لا يمكن معرفة من المتصل في الطرف الآخر من الشبكة العنكبوتية ولا يمكن معرفة المقاصد المراد تحقيقها من التدخل في هذه الجريمة المعلوماتية. لأنه أصبحت هذه البيئة الإفتراضية الجديدة على المجتمعات مكانا لترويج الأفكار المنظمات الارهابية والتعبير عن معتقداتها، وذلك بمحاولة التأثير على المعتقدات الدينية لأفراد المجتمع وتقاليده مما يؤدي إلى خلق الفوضى وبالتالي يمس بأمن الدولة وإستقرارها، وفي بعض الأحيان نجد أن هناك من ضعاف النفس من أفراد المجتمع من تسول له نفسه بالتعاون مع القوى الأجنبية قصد

1- عقباش بريزة مبارك حنان، آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، مصدر سابق، ص 29

الإضرار بالبلد وهنالك أشخاصا آخرون قد تكون لهم فائدة بنشر الفوضى عن طريق الإشادة بالأفعال الإرهابية ضد الدولة بحجة أنهم فئة مضطهدة ولها الحق في الدفاع عن نفسها و الانتفاضة على المؤسسة العسكرية و المطالبة بالإنفصال للحصول على حريتها، ومن أجل تحقيق هدفها عن طريق زرع الفيروسات المخربة او تعطيل الأنظمة بالتنويه والإشادة بالإرهاب ضد دولة وذلك بإستغلال المؤيدين لهذا الفكر المتطرف .

الفرع الثاني: جريمة التجسس على الدولة

تقوم به الدول المعادية وذلك بتجميع الأسرار عن الدولة والحصول على الأخبار فيكون التجسس خاصة على الأسرار العسكرية، ويكون في المجال الأمني والاقتصادي من طرف تمس بأمن الدولة وتتم عن طريق اختراق المواقع الحكومية والرئاسية او قرصنتها ليتمكن بذلك من الاطلاع على أسرار الدولة العسكرية والاقتصادية [1] .

حيث أن إستهداف الدفاع الوطني للدولة والهيئات الهامة في الدولة يتم بواسطة أشخاص أو منظمات تتواجد داخل أو خارج البلاد والتجسس يكون على المواقع والمنظمات والشخصيات عسكرية.

أما الشخصيات الاقتصادية فيتم التجسس على إقتصاد المؤسسات الاقتصادية التابعة للدولة من قبل عملاء من دولة معادية او حتى صديقة لكشف الأسرار الاقتصادية، أو من شركة منافسة في نفس المجال فهي معلومات سرية مؤمنة لا يسمح بالاطلاع عليها لأنها مدرجة على أنها أسرار دولة، لكن الاختراق يكشف عن الحماية وخاصة إذا كان نظام الحماية نظام التأمين ضعيفا يسهل إختراقه.

1- عقباش بريزة مبارك حنان، آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، مصدر سابق، ص 29

ملخص الفصل الأول

في هذا الفصل تم تناول تعريف الجريمة المعلوماتية وذلك حسب الإتجاهات القانونية و الآراء الفقهية للجريمة المعلوماتية جريمة جديدة والناتجة عن التطور السريع للتكنولوجيا و بما لها من خصائص وميزات حسنة لها في نفس الوقت صفات سيئة، كإستهداف الأشخاص و المؤسسات العامة و الخاصة على حد سواء و بغض النظر عن الهدف من هذا الإعتداء سواء كان على المعطيات بدلالتها التقنية الواسعة أو الاستعانة بها لإرتكاب جرائم لها آثار كالجرائم التقليدية، لكنها ترتكب داخل الحاسب الآلي في عالمها الإفتراضي والشبكات العنكبوتية، ثم بعد ذلك تم تحديد الطبيعة القانونية لها ثم إظهار خصائصها، بالإضافة إلى موقف المشرع الجزائري من هذه الجريمة المعلوماتية الجديدة وذلك من خلال النصوص القانونية لمواجهة هذه الجريمة، والصور التي جاءت بها هذه النصوص القانونية

الفصل الثاني
آليات الوقاية من الجرائم المعلوماتية في التشريع الجزائري

أحسن مثل يقال منذ قدم الزمان هو ان الوقاية خير من العلاج وهذا ما تحاول معظم الأمم والمجتمعات و التشريعات الوضعية و المنزلة **من الله تعالى (يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ قُوٓاْ أَنفُسَكُمۡ وَأَهۡلِيكُمۡ نَارٗا وَقُودُهَا ٱلنَّاسُ وَٱلۡحِجَارَةُ عَلَيۡهَا مَلَٰٓئِكَةٌ غِلَاظٞ شِدَادٞ لَّا يَعۡصُونَ ٱللَّهَ مَآ أَمَرَهُمۡ وَيَفۡعَلُونَ مَا يُؤۡمَرُونَ)** [1] الآية 06 سورة التحريم

فالمفهوم من هذا الأمر أن معظم المشرعين قد إستبق بوضع قوانين وقائية مسبقة للحماية من الوقوع في هذه الجرائم الجديدة على المجتمع ومما تسببه من أضرار جسيمة على الأموال والأشخاص والمؤسسات بصفة عامة

وهذه الجريمة المستحدثة التي تستعمل الفضاء الإفتراضي بإستعمال الشبكات العنكبوتية وفي نفس الوقت تستعمل جهاز الكمبيوتر وملحقاته للولوج إلى الطرف الآخر من نقطة الإتصال دون معرفة من هو المتصل أو هويته او ماهي خلفيته السياسية أو الاقتصادية أو العسكرية.

وسنحاول التطرق في هذا الفصل إلى السياسة الوقاية من الجرائم المعلوماتية، ففي المبحث الأول نتناول الآلية القانونية للحد من الجريمة المعلوماتية، وفي المبحث الثاني نتطرق إلى الهيئات المختصة في الكشف المسبق عن الجرائم المعلوماتية.

1-قرآن الكريم، سورة التحريم ، الآية 06

المبحث الأول :الوقاية القانونية من الجريمة المعلوماتية

مع التطور التكنولوجي الهائل وانتشار الإنترنت بشكل واسع، شهد العالم ظهور نوع جديد من الجرائم يُعرف بالجرائم المعلوماتية. هذه الجرائم تستهدف الأفراد والمؤسسات والحكومات عبر استخدام تقنيات المعلومات والاتصالات بطرق غير مشروعة ولمكافحة الجريمة الإلكترونية في الجزائر ومواجهة التحديات التي تطرأ نتيجة التقدم التكنولوجي، قام المشرع الجزائري بتعديل قانون العقوبات لتجريم الأفعال المرتبطة بأنظمة الحاسوب. يأتي هذا التعديل نتيجة تأثر المشرع بالتطورات التكنولوجية والتحولات الجديدة في مجال الجريمة الإلكترونية التي نشأت نتيجة الثورة المعلوماتية وقد تم إدخال التعديلات في قانون العقوبات. [1]

وقد فتح المشرع الجزائري الباب واسعا لهذا المجال تمثلت في صور وأنواع هذه الجريمة الالكترونية بنظرة عامة، الجريمة الإلكترونية التي ترتكبها الأفراد الطبيعيون والأشخاص المعنويون وفقًا للقانون العقوبات

المطلب الأول: التشريعات الخاصة (ق 09-04، 15-04، 18-04) تحليل النصوص القانونية

جاءت هذه القوانين إستجابة لضرور تكنولوجية ومواكبة للتطور السريع للمجتمع و للحفاض على خصوصية و سرية المعلومات فقد تم إصدار

الفرع الأول: القانون يتعلق بالحماية و السرية

القانون المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال رقم 04/09 و يشمل عدة نقاط منها:

حماية الخصوصية والسرية :يعزز القانون حماية الخصوصية والسرية في استخدام تكنولوجيا المعلومات

1-الأمر رقم 66-156 المؤرخ في 08 جوان 1966، معدل ومتمم بالقانون 24-06 المؤرخ في 28 جوان 2024، والمتضمن قانون العقوبات، ج ر عدد 30

والاتصالات. يتطلب من الأفراد والمؤسسات احترام خصوصية البيانات وعدم الاعتداء عليها أو استخدامها

1- **مكافحة الجرائم الإلكترونية** :يهدف القانون إلى توفير إطار قانوني لمكافحة الجرائم الإلكترونية. ينص على الإجراءات اللازمة للتحقيق في الجرائم الإلكترونية[1] وتقديم العقوبات المناسبة للمتورطين.

2- **التعاون الدولي** :يؤكد القانون على أهمية التعاون الدولي في مجال مكافحة الجرائم الإلكترونية. يشجع على تبادل المعلومات والتعاون بين الجهات القضائية والأمنية في الدول المختلفة لمواجهة التهديدات الرقمية عبر الحدود .

3- **التحقيقات القضائية** :يحدد القانون إجراءات التحقيق القضائي في الجرائم الإلكترونية. يتطلب من الجهات القضائية القدرة على جمع الأدلة الرقمية واستخدام التقنيات المتقدمة للتحقيق والكشف عن الجرائم الإلكترونية.

4- **المسؤولية القانونية** :يحدد القانون المسؤولية القانونية للأفراد والمؤسسات في حالة ارتكاب جرائم إلكترونية. يتضمن ضوابط وقواعد للحماية القانونية وتقديم العقوبات المناسبة للمتسببين في الجرائم.

5- **الوقاية والتوعية** :يشجع القانون على تعزيز الوعي والتوعية بأمن المعلومات والجرائم الإلكترونية. يلزم المؤسسات والجهات الحكومية بتبني سياسات وإجراءات لتعزيز الوعي والحماية وتثقيف الجمهور حول مخاطر الجرائم الإلكترونية.

الفرع الثاني: قانون يتعلق بالتوقيع والتصديق الإلكترونيين (القانون رقم 15-04)

يتعلق بالتوقيع والتصديق الإلكترونيين، ويهدف إلى تنظيم استخدام التوقيع الإلكتروني وتأكيد صحته وقانونيته. ينص القانون على جرم إفشاء البيانات الشخصية أو اساءة استعمالها، وجرم الإخلال بسرية

1-القانون رقم 09-04 المؤرخ في 05 اوت 2009 ، يتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر عدد 47.

البيانات، وينص على العقوبات المناسبة لكل من يرتكب هذه الجرائم. ويتضمن عدة نقاط هامة، وفيما يلي أبرز هذه النقاط:

التوقيع الإلكتروني :يعترف القانون بصحة التوقيع الإلكتروني ويجعله معادلاً للتوقيع الورقي التقليدي، ويتطلب أن يتوفر في التوقيع الإلكتروني عناصر محددة للتأكد من هوية الموقع وسلامة البيانات.[1]

- **حماية البيانات الشخصية** :ينص القانون على ضرورة حماية البيانات الشخصية وعدم الاعتداء عليها أو استخدامها بطرق غير قانونية. يعاقب أي شخص يقوم بإفشاء البيانات الشخصية أو اساءة استعمالها بالحبس والغرامة.
- **الحماية القانونية للتوقيع الإلكتروني** :يحدد القانون العقوبات القانونية لأي شخص يقوم بالتزوير أو التلاعب بالتوقيع الإلكتروني. يهدف إلى ضمان صحة وأمان التوقيعات الإلكترونية ومنع أي تلاعب
- **سرية البيانات والمعلومات** :يلتزم القانون بحماية سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكترونية. يجب على مقدمي خدمات التصديق الإلكتروني الحفاظ على سرية هذه المعلومات وفي حالة انتهاك ذلك يتعرض المخالف للعقوبات القانونية.
- **التعاون الدولي** :يشجع القانون على التعاون الدولي في مجال التوقيع والتصديق الإلكتروني. يتطلب تعاون الدول في تطوير القوانين والممارسات القانونية لتعزيز استخدام التوقيع الإلكتروني وتبادل المعلومات ذات الصلة.
- **التوقيع الرقمي الموثوق** :يعطي القانون أهمية كبيرة للتوقيع الرقمي الموثوق، الذي يستخدم تقنيات

متقدمة لضمان صحة التوقيعات الإلكترونية. يعمل على تعزيز الثقة في البيئة الإلكترونية وتسهيل العمليات

1-القانون 15-04 المؤرخ في 01 فيفري 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني

التجارية والمعاملات الرقمية.

01- قانون يتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية (القانون رقم 18-04)

يهدف هذا القانون إلى تنظيم وتوفير الأطر القانونية اللازمة لتطوير واستخدام التوقيع والتصديق الإلكتروني في الجزائر، مما يعزز الثقة والأمان في البيئة الرقمية ويسهم في تسهيل العمليات والمعاملات الإلكترونية ويشمل عدة نقاط رئيسية، وفيما يلي أبرز هذه النقاط:

-**حماية سرية المراسلات الإلكترونية** :يؤكد القانون على ضرورة حماية سرية المراسلات الإلكترونية التي تتم عبر البريد الإلكتروني أو وسائل الاتصالات الإلكترونية[1] الأخرى. يُعاقب أي شخص ينتهك سرية المراسلات أو يفشي مضمونها أو يستخدمها بدون ترخيص بالحبس والغرامة.

- **عدم تحويل المراسلات الصادرة** :ينص القانون على منع تحويل المراسلات الصادرة عبر البريد الإلكتروني أو وسائل الاتصالات الإلكترونية الأخرى. يُعاقب أي متعامل للاتصالات الإلكترونية يقوم بتحويل المراسلات بالحبس والغرامة.

-**حماية الحياة الخاصة للأفراد** :يحث القانون على عدم مساس واستخدام شبكات وخدمات الاتصال الإلكترونية بالحياة الخاصة للأفراد. يُعاقب أي شخص ينتهك هذا الحق بالحبس والغرامة.

-**التعاون الدولي وتطوير القوانين** :يشجع القانون على التعاون الدولي في مجال البريد والاتصالات الإلكترونية، وذلك من خلال تبادل المعلومات وتطوير القوانين والسياسات المتعلقة بالمجال. والبيانات التي تنتقل عبر البريد ووسائل الاتصال الإلكترونية.

1- القانون 18-04 المؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية،

المطلب الثاني: العقوبات والإجراءات التحفظية والردعية

الفرع الأول: العقوبات الأصلية

نص المشرع الجزائري في القانون 24-06 ، على عقوبات أصلية لجريمتي الدخول و البقاء الغير مشروعان أي عن طريق الغش للنظام المعلوماتي، وقد حدد الجزاء لكل جريمة منها وهي كاتالي:

تنص المادة 394 مكرر من قانون العقوبات الجزائري ق 24-06 أنه : [1]

" يعاقب بالحبس من ستة أشهر إلى سنتين وبغرامة من60.000 دج إلى 200.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك "

-عقوبات التشديد على الاعتداء في نظام المعالجة الآلية للمعطيات

يشدد المشرع الجزائري من عقوبة الدخول والبقاء بدون ترخيص في نظام المعالجة الآلية، إذا ترتب في تخريب نظام إشتغال المنظومة وذلك بموجب الفقرة الثانية من المادة 394 مكرر تضاعف العقوبة.

يعاقب بالحبس من سنة إلى ثلاث سنوات وبغرامة من100.000 دج إلى 300.000 دج

-جريمة إستهداف الجيش الوطني أو الهيئات العمومية

في هذه الجريمة لما الجاني يعتدي على مؤسسة من مؤسسات الجيش الوطني أو المؤسسات العمومية فإن العقوبة تشدد لأنه لا تسامح مع مثل هذه الجرائم و التي تعد من جرائم الإرهاب ضد الدولة [1] وقد نصت المادة 394 مكرر3 بأن يعاقب الجاني بالحبس من سنتين(2) إلى عشر (10) سنوات وبغرامة من700.000 دج إلى 2.000.000 دج .

1- الأمر رقم 66-156 المؤرخ في 08 جوان 1966، معدل ومتمم بالقانون 24-06 المؤرخ في 28 جوان 2024، والمتضمن قانون العقوبات، ج ر عدد 30

-عقوبات الأخرى لاعتداء على نظام المعالجة الآلية للمعطيات

لقد جرم المشرع فعل الدخول بطريق غير شرعية إلى أي منظومة معلوماتية دخولا غير شرعي، وذلك حين عبر عنه بطريق الغش، كما أن المشرع لم يفرق بين الدخول إلى جزء من المنظومة أو كلها، وهنا سيتخلص منها ما يلي:

-التسليم بتوفير القصد الجنائي بمجرد الدخول إلى نظام معلوماتي عن طريق الغش.

-عدم الاعتداد بنتائج هذا الدخول حتى ولو يسبب أي تخريب أو إضرار بالبيانات، وذلك لكونها جريمة وقتية. لذلك نجد أنه في إطار أحكام القسم السابع مكرر المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات، صور قد تم تحديدها في المواد من 394 مكرر إلى 394 مكرر 8 والمتمثلة في الجرائم التالية:

1-جريمة إدخال أو إزالة أو تعديل بطريق الغش معطيات في نظام المعالجة الآلية وقد عاقب عليها المشرع في نص المادة **394 مكرر 1** بالحبس من سنة إلى ثلاث سنوات وبغرامة من500.000 دج إلى 2.000.000 دج

2-جريمة القيام **عمدا** وعن طريق الغش **بالتصميم – بحث –تجميع – توفير – نشر – الإتجار في المعطيات المخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية والحيازة –إفشاء نشر أو إستعمالها لأي غرض كان** يعاقب عنها بالحبس من سنة إلى ثلاث سنوات وبغرامة من1.000.000 دج إلى 5.000.000 دج وهذا الذي نجده قد أشارت له المادة 394 مكرر 2 ق ع ج .

الفرع الثاني: العقوبات المقررة للشخص المعنوي

إن من شروط هذه الجريمة أنه إذا قام الشخص المعنوي بهذه الجرائم وذلك أن ترتكب إحدى الجرائم المنصوص عليها قانونا تكون بواسطة أحد أعضاء أو ممثلي الشخص[1] المعنوي أي ترتكب الجريمة

1-عائشة نايري، الجريمة الإلكترونية في التشريع الجزائري، مصدر سابق ، ص 38

لحساب الشخص المعنوي فإنه يعاقب بغرامة (5) خمس مرات للحد الأقصى للغرامة المقررة للشخص الطبيعي كما تنص عليه المادة 394 مكرر4 ق ع ج

أما عقوبة الإشتراك و الشروع

أ – عقوبة الإشتراك:

أن كل من شارك في مجموعة أو في إتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المعلوماتية فإنه يعاقب بنفس العقوبة المقررة للجريم وذلك نجده في نص المادة 394 مكرر 5 ق ع ج.

فالملاحظ أن المشرع الجزائري قد أعطى نفس الجزاء لهذه الجريمة ولم يفرق بينهما

ب- عقوبة الشروع

بأن المشرع الجزائري يعاقب على جريمة الشروع في إر تكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها وهذا ما نصت عليه المادة 394 مكرر 6 من ق ع ج ، لكن في نفس الوقت مع الإحتفاظ بحقوق الغير حسن النية، في حالة مصادرة الأجهزة المستخدمة وإغلاق الموقع الإلكتروني وكذلك المحل المستغل في الجريمة إذا كان الجريمة أرتكبت دون علمه وذلك حسب المادة 394 مكرر 7 من ق ع ج كل من قام بالشروع للقيام بالجريمة الإلكترونية " يعاقب بالعقوبات المقررة لجنحة ذاتها، والجدير بالذكر أنه المشرع قد أضاف مقدموا الأنترنت حسب المادة 394 مكرر 8 ، بأنهم عندما يخضعوا لجزاء عند مخالفتهم التنظيم الخاص بالتدخل الفوري لسحب أو تخزين المحتويات التي تتيح ّالإطلاع عليها أو جعل الدخول إليها ممكنا عندما تتظمن محتويات تشكل جرائم منصوص عليها قانونا بعقوبات التالية: "يعاقب بالحبس من سنة إلى ثلاث سنوات وبغرامة من2.000.000 دج إلى 10.000.000 دج أو بإحدى هاتين العقوبتين فقط " [1]

1- عائشة نايري، الجريمة الإلكترونية في التشريع الجزائري، مصدر سابق ، ص 38

الفرع الثالث: العقوبات التكميلية

نصت المادة 394 مكرر 06 من نفس القانون على مجموعة من العقوبات التكميلية، إلى جانب العقوبات الأصلية وهي كالتالي:

-**المصادرة:** وهي التحفظ على الأجهزة والبرامج والوسائل المستخدمة لارتكاب الجرائم الماسة بالنظام

-**إغلاق المواقع** :إغلاق المواقع الإلكترونية بصفة عامة، والتي كانت وسيلة لإرتكاب هذه الجرائم أو ساهمت في إرتكابها.

-**إغلاق المقهى الإلكتروني** يكون في الحالة عندما يكون صاحب المحل مشاركا في الجريمة أو لم يتصدى لها بالإخبار عنها، أو بمنع مرتكبيها من القيام بهذه الجريمة في محله أو سمح بإرتكاب مثل هذه الجرائم.

ومن هنا نلاحظ أن هذه العقوبات جاءت رادعة حيث تتضاعف عند الضرورة، كما اشتملت على عقوبات تكميلية، وحتى عقوبات الشخص المعنوي. [1]

المبحث الثاني: الوقاية المؤسسية والعملية من الجريمة المعلوماتية

وللقيام بالتدخل في هذه الجريمة يجب أن تحترم الإجراءات وإلا ستكون تحت طائلة البطلان القانوني ومن هذه الإجراءات منها الإجراءات التقليدية للكشف على الجرائم الإلكترونية وهناك إجراءات مستحدثة تم إنشاءاها نتيجة التطور المستمر والسريع للتكنولوجيا في مجال الإتصالات الإلكترونية والجرائم المتصلة بها.

1-نهلا عبد القادر المومني، الجرائم المعلوماتية، ط 2 ، مصدر سابق ، ص 24

المطلب الأول: دور الشرطة القضائية وقاضي التحقيق في الوقاية من الجريمة

الفرع الأول: الإجراءات التقليدية للكشف عن الجريمة المعلوماتية

أولا: معاينة موقع الجريمة المعلوماتية

إن معظم التشريعات وكذلك المشرع الجزائري إعتمد إجراء التحري والذي نصت عليه المادة 61 من ق إ ج ج ، من أجل الكشف الحقيقة يجب تنقل ضابط الشرطة القضائية إلى عين المكان لمعاينة موقع الجريمة بالعين المجردة وضبط كل ما يلزم لكشف الحقيقة.

ويعد التنقل وجوبي في الجنيات وجوازا في الجنح فعندما يكون الجريمة في مكان عام فضابط الشرطة القضائية لا

يحتاج إلى إذن من النيابة العامة بإجرائها، أما إذا كانت بمكان خاص؛ فلابد لصحتها من رضا صاحب المكان أو وجود إذن مسبق من سلطة التحقيق وفي هذه الجريمة الحديثة يجب التفرقة بين حالتين:

1- الجرائم الواقعة على المكونات المادية للحاسوب Hardwar [1]

ويقصد به هنا مكونات الحاسوب ذات الطابع المادي المحسوس (شاشة العرض، الوحدة المركزية، لوحة المفاتيح، والأقراص الصلبة، وذاكرات التخزين المحمولة...) وتمكن لضابط الشرطة القضائية التحفظ عليها وتعد كأدلة مادية للكشف عن الجريمة

2- الجرائم الواقعة على المكونات غير المادية للحاسوب Software

التي تقع على برامج الحاسوب والبينات المخزنة فيه وبطبيعتها أنها إفتراضية فيصعب الحصول على الآثار المادية للجريمة وكذلك يصعب تحديد المجرم الذي قام بالإعتداء الإجرامي وذلك نتيج للعدد الكبير الذين يستعملون هذا الحاسوب وطول المدة عن إكتشاف الجريمة.

1-نهلا عبد القادر المومني، الجرائم المعلوماتية، ط 2 ، مصدر سابق ، ص 24

لذلك يجب على ضابط الشرطة القضائية أن يقوم بجميع الإحتياطات الآزمة من أجل المحافظة على الأدلة، مثل عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة، وذلك قبل إجراء الاختبارات اللازمة للتأكد من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي حتى لا يحدث أي إتلاف للبيانات المخزنة ومحو للبيانات المسجلة، ووضع مخطط تفصيلي للموقع الجريمة ودور كل كشف تفصيلي بالمسؤولين ودور كل واحد منهم، و التحفظ على ما تحتويه سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة، و الأشرطة، و الأقراص الممغنطة المحطمة أو السليمة، والمستندات ورفع البصمات التي تكون في مسرح الجريمة، و القيام بتصوير الحاسوب وخاصة أجزائه الخلفية و ملحقاته، والتوصيلات التي تكون متصلة بأي نظام وتسجيل التاريخ والمكان ووقت التصوير من أجل عرضها على المحكمة.

ثانيا: ضبط وتفتيش النظام المعلوماتي

من أجل الكشف والحصول على أدلة يجب على ضابط الشرطة القضائية إجراء التحقيق في الجرائم المعلوماتية؛ وذلك بوضع اليد على الشيء وحبسه والمحافظة عليه للحصول على دليل لمصلحة التحقيق عن طريق إثبات واقعة معينة. [1]

وهذا ما نصت عليه المادة 47 –4 من ق إ ج ج ، وذلك إذا تعلق الأمر بجريمة ماسة بأنظمة المعالجة الآلية للمعطيات يمكن لقاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية للقيام بذلك

1- تفتيش المكونات المادية للحاسوب

هناك حالات خاصة للتفتيش في هذه المكونات الحاسوب هي:

1- محمد نجيب دبابلو، الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، ط1 ، المركز المغاربي ، شرق أدنى للدراسات الإستراتيجية بريطانيا، 2024، ص 77

– إذا كانت هذه المكونات موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته، فإنها تأخذ نفس الأحكام المقررة لتفتيش المسكن وبنفس الضمانات المقررة قانونا في مختلف التشريعات

– إذا كانت مكونات الحاسوب المادية منعزلة عن غيرها من أجهزة الكمبيوتر أم أنها متصلة بجهاز أو نهاية طرفية في مكان آخر كمسكن غير مسكن المتهم، بحيث إذا كانت هناك بيانات مخزنة في أوعية هذا النظام الآخر، فإن عملية الكشف قد تصبح صعبة جدا، وفي بعض الأحيان تكون مستحيلة لذلك نجد المشرع الجزائري قد قرر المادة 65 مكرر 5 وما يليها من قانون الإجراءات الجزائية التي تسمح إذا إقتضت ضرورات التحري أو التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بإعتراض المراسلات وتسجيل الأصوات والتقاط الصور[1]

– إذا وجدت مكونات الحاسوب المادية في الأماكن العامة كالمطاعم وسيارات الأجرة... الخ، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص، وبنفس الضمانات والقيود المنصوص عليها في هذه الحالات

ثانيا: تفتيش المكونات غير المادية للحاسوب

يقصد بها هنا مجموعة البرامج والأساليب والقواعد وعند الاقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات

ثالثا: قواعد التفتيش

أ- إجراء التفتيش بحضور أشخاص معينين بالقانون

وفق المادة 45 من قانون الإجراءات الجزائية أن التفتيش يتم بحضور المتهم أو من يجوز أن يمثله وضابط الشرطة القضائية القائم بالتفتيش واذا تعذر حضور المتهم أو من يجوز أن يمثله يتم التفتيش بحضور شاهدين من غير الموظفين الخاضعين لسلطته

1- محمد نجيب دبابلو، الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، مصدر سابق، ص 78

ب- **إعداد محضر خاص بالتفتيش:** ويكون بتكليف القائم بالتفتيش باصطحاب كاتب يحرر محضر خاص بالتفتيش والضبط، تسجل فيه جميع وقائع التحقيق بالتفصيل، وذكر البيانات والأشياء والوثائق التي يتم ضبطها بكل أمانة ودقة. [1]

وللقيام بهذا العمل يجب أن يكون القائم بالتفتيش على علم بقدر كبير بعلوم الإعلام الآلي حتى يتسنى له معرفة نظم الحاسوب المراد تفتيشها، والاستعانة بخبراء النظام بالحصول على كلمة السر والدخول للنظام ومعرفة مكان القيام بتحليل نظم الحاسوب الآلي وكذلك تحديد هوية أعضاء فريق التفتيش مع تخاذ الخطوات التالية:

- تأمين حماية مسرح الجريمة، بضمان فصل القوة الكهربائية عن موقع المعاينة وأجهزة خادمة شبكة الانترنت، لشل فاعلية الجاني في القيام بأي فعل من شأنه التأثير على أثار الجريمة
- إبعاد المتهم عن مكان النظام إن كان قريبا منه
- أخذ الحيطة لمنع تمكن المتهم من الدخول عن بعد للنظام المعلوماتي
- الدخول إلى الموقع ببطء، لكي لا يتم إتلاف الدليل أو تشوهه
- عدم لمس لوحة المفاتيح، لأن ذلك قد يستلزم استخدام برامج أخرى احتيالية أو صعبة
- يجب العناية بالملاحظات وكلمات السر ورموز الشفرة إلى غيرها من العمليات والإجراءات الفنية التي تساعد على الكشف عن الجريمة

وفي هذا نطاق نجد أن المشرع الجزائري لم يحدد مدة معينة لتنفيذ تفتيش نظم وذلك بعدم تقييد المحقق بمدة زمنية معينة، بل يجب تركها للسلطة التقديرية له، لأن الوقت الذي تكثر فيه الجرائم المعلوماتية هو ليلا، لسهولة الاتصال وأيضا لسهولة الدخول إلى المواقع المستهدفة لقلة المستخدمين في هذا الوقت.

1- محمد نجيب دبابلو، الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، مصدر سابق، ص 79

الفرع الثاني :الآليات الحديثة للكشف عن الجريمة المعلوماتية

إن إجراءات المستحدثة للكشف عن للجرائم الماسة بأنظمة المعالجة للمعطيات بعد التعديل قانون الإجراءات الجزائية 06-22 المؤرخ في 20-12-2006 وهي:

أولا- آلية إعتراض المراسلات وتسجيل الأصوات والتقاط الصور

أعطى المشرع الجزائري في نص المادة 03 من القانون 09-04 المؤرخ في 05أوت 2009 مع مراعاة الأحكام القانونية التي تخص سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية "[1] ووفقا لنص هذه المادة أصبح لضابط الشرطة القضائية صلاحية اعتراض المراسلات وتسجيل الأصوات عن طريق وضع رقابة على الهواتف وتسجيل الأحاديث التي تتم عن طريقها، كما يتم أيضا عن طريق وضع ميكروفونات حساسة تستطيع إلتقاط الأصوات وتسجيلها على أجهزة خاصة وأيضا عن طريق التقاط إشارات لاسلكية أو إذاعية، لأنه يجب التفريق بين مصطلح إعتراض المكالمات الهاتفية وبين مصطلح وضع الخط الهاتفي تحت المراقبة، فبينما يكون الأول دون رضا المعني، ومن الممكن أيضا أن الإجراء لا يمس فقط المتهم فقط بل تمس أيضا بالأشخاص المحيطين به أو أقاربه أثناء التسجيل، وفي حالة أخرى قد تكون برضاه أو بطلب من صاحب الشأن، لتقدير الهيئة القضائية بعد تسخير مصالح البريد والمواصلات لذلك.

ويخضع التقاط الصور في المحلات السكنية والأماكن العامة والخاصة من أجل الكشف عن جرائم المعلوماتية، وهي إجراءات تباشر بشكل خفي، على الرغم من تناقضها مع النصوص المقررة لحماية الحق في الحياة الخاصة وهي حق دستوري.

1- عقباش بريزة مبارك حنان، آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، سابق، ص39

لهذا نجد أن المادة 65 من ق إ ج ج ، تباشره الجهة القضائية في بعض الجنايات والجنح التي وقعت أو التي قد تقع في القريب العاجل للتحري والتحقيق، وكل ما يتمخض عنها كدليل ضد كل شخص قامت تحريات جدية على أنه ضالع في ارتكاب هذه الجريمة أو لديه أدلة تتعلق بها، وأن في مراقبة أحاديثه الهاتفية ما يفيد في إظهار الحقيقة، بعد أن صعب الوصول إليها بوسائل البحث العادية.

لكن مع ذلك، نجد المشرع حاول أن يوفق بين هذه المتعارضات، بأن أجاز هذه الأساليب وهي مباشرة التحري بإذن من وكيل الجمهورية المختص، والتزام أعوان وضباط الشرطة القضائية القائمين بإجراء السر المهني، وفيما يلي نتولى شرح كلا الضابطين، فالمشرع على الرغم من إقراره أساليب تحري خاصة قد تمس بحرمة الحياة الخاصة إلا أنه يعاقب على اللجوء لاستعمالها بطرق غير مشروعة وهو ما سنشير إليه في مايلي:

أولا: **مباشرة التحري بإذن من وكيل الجمهورية**

إلا بإذن من وكيل الجمهورية المختص سمح المشرع بإجرء إعتارض المراسلات وتسجيل الأصوات والتقاط الصور بقصد التحري والتحقيق عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وهذا ما قررته المادة 65 مكرر5 من ق إ ج ج التي جاء فيها أنه يجوز لوكيل الجمهورية المختص أن يأذن بما يلي:

إعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية و اللآسلكية ...) وعند مباشرة التحريات والتحقيقات، يحرر ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص، محضر عن كل عملية اعتراض للمراسلات وتسجيل الأصوات والتقاط للصور، وحتى عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتسجيل الصوتي أو السمعي البصري، كما يذكر في المحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها ، بحيث يشتمل المحضر على كل البيانات المذكورة سابقا وتكون

1- عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري مرجع سابق، ص 53

محددة تحديدا نافيا للجهالة، ويجب أن يكون في المحضر توقيع محرره في نهايته، بعد أن يصنف أو ينسخ ضابط الشرطة القضائية المأذون له أو المناب، المراسلات أو الصور أو المحادثات المسجلة أو المفيدة في إظهار الحقيقة في محضر يودع بملف المتهم، وتنسخ وتترجم المكالمات التي تتم باللغات الأجنبية عند الاقتضاء، بمساعدة مترجم لهذا الغرض.

ثانيا :إلتزام السر المهني

تكون إجراءات التحري والتحقيق سرية، ومن ثم فإن بحثها ضمن الضمانات الممنوحة للمتهم، والسرية تعني القيام قدر الإمكان ممن هو قائم بالتحري أو كلف بإجراء أو ساهم فيه بالمحافظة على السر المهني، وبالتالي صارت السرية ليس هدفها كما كان عليه من قبل هو تسهيل قمع المتهم، [1] بل صارت وسيلة لضمان الحريات الشخصية

وفقد نص المشرع صراحة على أن هذه العمليات تتم بمراعاة السر المهني ودون المساس به، فالضابط المأذون له باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، ملزم قانونا بكتمان السر المهني ويجب أن يتخذ مقدما التدابير اللازمة لضمان احترام هذا السر، وقد نص قانون الإجراءات الجزائية على أن تكون إجراءات التحري والتحقيق سرية، ما لم ينص القانون على خلاف ذلك، ودون إضرار بحقوق الدفاع، وكل شخص يساهم في هذه الإجراءات ملزم بكتمان السر المهني بالشروط المبينة في قانون العقوبات وتحت طائلة العقوبات المنصوص عليها لذلك فعملية التحري عن جرائم المساس بأنظمة المعالجة الألية للمعطيات تتم بسرية مطلقة، فيمنع منعا باتا أن يخبر المشتبه فيه بهذه التحريات أو أي شخص آخر، كذلك يمنع على ضابط الشرطة المأذون له أو المناب أن يفصح عن مضمون محضر التحريات لأي شخص كان، والا وقع تحت طائلة الجزاء الجنائي بتهمة إفشاء السر المهني، فيجب على ضباط الشرطة القضائية ومرؤوسيهم عدم إفشاء الأسرار التي جمعوها أثناء التحريات، لأن سمعة المواطنين

1- عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري مرجع سابق، ص 57

لا يجوز أن تظل مهددة ببيانات غير مؤكدة.

ثالثا : آلية الإختراق والتسرب

يعتبر التسرب تقنية جديدة أدرجها المشرع في تعديل قانون الإجراءات الجزائية سنة 2006 ،[1] عندما تقتضي ضرورات التحري والتحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر5 ، كما يجوز لوكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن شروط محددة ويشترط حصول الضابط المكلف بالتسرب على الإذن من وكيل الجمهورية المختص، ويجب أن تتم العملية تحت أشرافه ومراقبته، فإن قرر ضابط الشرطة القضائية مباشرة هذا الإجراء وجب عليه أولا إخطار وكيل الجمهورية بذلك، ثم يقوم بمنح الإذن مكتوب لضابط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته، على أن يتم ذكر هويته فيه ، وهذا تحت طائلة البطلان المطلق، فيجب أن يكون الإذن مكتوبا يتضمن كل ما يتعلق بعملية التسرب وكذلك هوية ضباط وأعوان الشرطة المأذون لهم بالتسرب. وبمعنى آخر هو قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه فيهم، بإيهامهم أنه فاعل معهم أو شريك لهم.

فالتسرب إذن هو قيام المأذون له بالتحقيق في الجريمة بمراقبة الأشخاص المشتبه في ارتكابهم جريمة، أو التوغل داخل جماعة إجرامية بإيهامهم أنه شريك لهم، ويسمح لضباط وأعوان الشرطة القضائية بأن يستعملوا لهذا الغرض هوية مستعارة وأن يرتكب عند الضرورة بعض الجرائم، دون أن يكون مسؤولا جزائيا، وذلك بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية، بإخفاء الهوية الحقيقية.

ولهذا يجوز لضابط أو عون الشرطة القضائية المرخص له بإجراء عملية التسرب والأشخاص الذين يسخرون لهذا الغرض، دون أن يكونوا مسؤولين جزائيا القيام بما يلي:

- اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتجات أو وثائق أو معلومات

1- عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري مرجع سابق، ص 58

متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها

- استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم، الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخريب أو الإيواء أو الحفظ أو الاتصال. [1]

ويحظر على المتسرب إظهار الهوية الحقيقية في أي مرحلة من مراحل الإجراءات مهما كانت الأسباب إلا لرؤسائهم السلميين، لأن هذا سيؤدي إلى إفشال الخطة المتبعة في القبض على المشتبه فيهم وتعريض العضو المكشوف عن هويته للخطر، وهو ما أكده المشرع بموجب المادة 65 مكرر 16 بأن نصت صراحة أنه " لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشروا التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات " كما عاقب المشرع كل من يكشف هوية ضباط أو أعوان الشرطة القضائية بالحبس من سنتين إلى خمس سنوات وبغرامة من 50000 دج إلى 2000000دج، واذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب وجرح أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين، فتكون العقوبة الحبس من خمس سنوات إلى 10 سنوات والغ ا رمة من 200000 دج إلى 500000 دج، واذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص فتكون العقوبة الحبس من 10 إلى 20 سنة والغرامة من500000 إلى 1000000 دج ، رغم أن المشرع أجاز مثل هذه الأفعال التي تعتبر في حقيقة الأمر جرائم من أجل خلق الثقة وتعزيزها في ضباط الشرطة القضائية وأعوانهم المرخص لهم بإجراء عملية التسرب من قبل المشتبه فيهم والنجاح في إيهامهم بأنهم شركاء أو فاعلون، مع ذلك منع المشرع هؤلاء الضباط أو الأعوان من أن يحرّضوا المشتبه فيهم على ارتكاب الجريمة، بمعنى أنه يمنع على الضباط والأعوان المتسربين أن يخلقوا الفكرة الإجرامية للشخص الموضوع تحت المراقبة ودفعه لارتكاب الجريمة، فهذا الفعل ممنوع تحت طائلة بطلان الإجراء

1- عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري مرجع سابق، ص 58

المطلب الثاني: دور الهيئات الوطنية ومؤسسات الرقابة السيبيرانية في الوقاية من الجريمة المعلوماتية

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال

تم إنشاء أجهزة متخصصة على المستوى الدولي مهمتها البحث والتحري في العالم الافتراضي مثل هيئة الإنتربول واليوروبول والأفريبول، أما في الجزائر فقد أنشأت هيئات ووحدات متخصصة أبرزها وفي الجزائر فلقد تم إنشاءها بموجب المادة 13 من القانون 09 -04 ، و بموجب المرسوم الرئاسي 21- 439 مؤرخ في 7 نوفمبر سنة2021 تم تحديد تشكيلة هذه الهيئة وكيفيات[1] سيرها. فهي تعتبر "هيئة لسلطة ادارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع لدى رئيس الجمهورية **ويقصد بالسلطة الإدارية** : أسلوب جديدا لممارسة السلطة العامة تجمع بين سلطتي التسيير والرقابة كونها مزودة بسلطة حقيقية ومستقلة في اتخاذ القرار وقد وجدت أساسا لضبط المجالين الاقتصادي والمالي، ومقر الهيئة بالجزائر ويمكن نقلوه الى اي مكان آخر من التراب الوطني بموجب مرسوم رئاسي بناء على نص المادة3

تتكون الهيئة من مديرية عامة ومجلس توجيه ويكونوا تحت السلطة المباشرة لرئيس الجمهورية ويقدمان له عرضا عن نشاطاتهما حسب نصت عليه المادة 5

1- عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري مرجع سابق، ص 59

أولا: تعريف الهيئة وخصائصها

تتشكل الهيئة من جهازين اداري وبشري

أ – **الجهاز الإداري:** تتكون الهيئة من مجلس توجيه ومديرية عامة يوضعان تحت السلطة المباشرة لرئيس الجمهورية ويقدمان له عرضا عف نشاطاتهما وفي ما نصت عليه المادة 5 من هذا القانون: [1]

01- **مجلس التوجيه :** نصت عليه المادة 6 التي جاء فيها المدير العام للهيئة، يعينه رئيس الجمهورية ويتولى امانة مجلس التوجيه الذي يتشكل من الأعضاء التالية:

–الأمين العام لوزارة الشؤون الخارجية والجالية الوطنية بالخارج

– الأمين العام لوزارة الداخلية والجماعات المحلية والتهيئة العمرانية

– الأمين العام لوزارة العدل

– الأمين العام لوزارة البريد والمواصلات السلكية واللاسلكية

– قائد الدرك الوطني

–المدير العام للأمن الداخلي

– المدير المركزي للأمن الجيش بأركان الجيش الوطني الشعبي

– المدير العام للأمن الوطني

– رئيس مصلحة الدفاع السيبيراني ومراقبة أمن الأنظمة لأركان الجيش الوطني الشعبي

المديرية العامة : بناء على نص المادة 9 يدير المديرية العامة مدير عام ويعين بموجب مرسوم رئاسي وتنهى مهامه حسب الأشكال نفسها كما تعد وظيفة المدير العام وظيفة عليا في الدولة وتظم المديرية

1– عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري مرجع سابق، ص 59

العامة مديريات ومصالح وملاحق حسب نص المادة 11 وفقا لما يلي:

- مديرية المراقبة الوقائية واليقظة الالكترونية
- مديرية الإدارة والوسائل
- مصلحة الدراسات والتلخيص
- مصلحة التعاون واليقظة التكنولوجية
- ملحقات جهوية.

ويحدد التنظيم الداخلي لهياكل الهيئة[1] بموجب قرار من الأمين العام لرئاسة الجمهورية بناء على اقتراح من المدير العام للهيئة كما جاء في نص المادة13

ب :الجهاز البشري.

بالإضافة الى موظفي الدولة العاملون في وظائف عليا في الهيئة والموظفين يوجد مستخدمين وافراد آخرين نصت عليهم المواد 20 و 21 منهم:

- قضاة وفقا للشروط والكيفيات المنصوص عليها بموجب التشريع الساري المفعول
- ضباط وأعوان الشرطة القضائية مؤهلون من المصالح العسكرية للأمن والدرك الوطني والأمن الوطني

التي تحدد بموجب قرارات مشتركة بين وزير الدفاع الوطني والوزير المكلف بالداخلية والأمين العام لرئاسة الجمهورية

- مستخدمو الدعم التقني والإداري للمصالح العسكرية للأمن المختصة والدرك الوطني والأمن الوطني.

1-عقباش بريزة مبارك حنان، آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، مرجع سابق، ص45

- كما ان المادة 21 من نفس المرسوم رخصت للهيئة بتوظيف فئات أخرى من المستخدمين حسب حاجتها
- و كما نصت المادة 32 على إمكانية الاستعانة بموظفين مختصين من الوزارات المعنية بمجال تكنولوجيات ٱلإعلام والاتصال أو أي شخص اخر سواء خبير أو شخص عادي قادر على المساعدة في عمل.

ثانيا: مهام الهيئة.

اولا : على المستوى الوطني.

تمارس الهيئة المهام المنصوص عليها في نص المادة 14 من القانون 09 -04 تحت السلطة القضائية طبقا لأحكا التشريع الساري المفعول لا سيما منها قانون الاجراءات الجزائية والقانون المذكور اعلاه تكلف الهيئة بما يأتي

1-مهام عامة للهيئة:

لهذه الهيئة العديد من المهام أهمها :

– تنسيق وتنشيط الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها [1]

– مساعدة السلطة القضائية ومصالح الشرطة القضائية وذلك بجمع المعلومات وتزويدهم به وذلك حسب نص المادة 14 فقرة ب من قانون 09-04.

– تقوم الهيئة بإذن من السلطات القضائية بتنفيذ عمليات المراقبة الوقائية للاتصالات الالكترونية من أجل الكشف عن الجرائم المتصلة بتكنولوجيات الاعلام والاتصال

– جمع واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم الالكترونية ومكافحتها وحفظها

1-عقباش بريزة مبارك حنان، آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، مرجع سابق، ص45

– تزويد بالمعلومات والمعطيات المتعلقة بالجرائم الإلكترونية السلطات القضائية ومصالح الشرطة القضائية تلقائيا او بناء على طلبها

–القيام بالتدقيق والتفتيش في أي مكان او هيكل او جهاز يحوز او يستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات الالكترونية باستثناء ذلك التابعة لوزارة الدفاع الوطني

–تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية

–تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية في المجال نفسه

ثانيا : على المستوى الدولي.

تنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة وجمع المعطيات المفيدة في تحديد مكان تواجد مرتكبي الجرائم المتصلة بتكنولوجيات الإعلا م والاتصال[1] والتعرف عليهم وتبادل المعلومات واتخاذ الإجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة او الاتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل

الفرع الثاني: هيئة الضبط الإداري والاجهزة الأمنية

هي مجموعة القواعد التي تعرضها السلطة العامة على مواطنين أي دولة وذلك بقصد تحقيق الأمن والنظام العام والسهر على سيادة وإحترام القانون، وللضبط الإداري وظيفتين وظيفة الظبط القضائي ووظيفة الضبط الإداري أو البوليسي وهو يهدف إلى المحافظة على النظام العام في الأماكن العامة والصحة العامة والسكينة العامة عن طريق إصدار القرارات واللاوائح وإستخدام القوة المادية مما قد ينتج عنه من فرض القيود على الحريات الفردية حسب ما يستلزمه ضروريات الحياة في المجتمع ومن أهم دور للضبط الإداري هو مكافحة جرائم المعلوماتية وكذلك له صلاحيات الوقاية منها وذلك بإتخاذ كافة الإجراءات والوسائل لمنع وقوع هذه الجرائم المعلوماتية.

1–عقباش بريزة مبارك حنان، آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، مرجع سابق، ص45

أولا: هيئة الضبط الإداري

01-سلطة الضبط

نتيجة التطور السريع لتكنولوجيا والميزة التي تجمع بين المال والاقتصاد في سلطة الضبط كان من الضروري تنظيم عمل هذه السلطة و لذلك تم إستحداثها عن طريق نص المادة 13 من القانون 18-04 المؤرخ في 10 ماي 2018 ج ر عدد 27 والذي يحدد القواعد العامة المتعلقة بالبريد و الاتصالات الإلكترونية، وضمان ضبط أسواق البريد والإتصال الإلكترونية لحساب الدولة و أهم مهام هذه السلطة

- السهر على وجود منافسة فعلية ومشروعة في سوق وترقته
- السهر على تقاسم منشآت الاتصالات الإلكترونية في ظل إحترام حق الملكية
- تخصيص ذبذبات لكل متعاملي شبكات الإتصال الإلكترونية وعدم التمييز بينهم
- تحيين وإعداد وضعيات الذبذبات المخصصة لكل متعامل وتبليغها إلى الوكالة الوطنية للذبذبات [1]
- إعداد مخطط وطني للترقيم ودراسة طلبات الأرقام الجديدة للمتعاملين
- منح التراخيص العامة لإنشاء أو إستغلال شبكات الإتصال الإلكترونية
- المصادقة على تجهيزات البريد والاتصالات الإلكترونية طبقا للمعايير المحدد عبر التنظيم
- الفصل في النزاعات بين المتعاملين وتسويتها
- الحصول من المتعاملين على جميع المعلومات الضرورية للقيام بمهامها.
- التعاون في إطار مهامها مع السلطات الأخرى أو الهيئات الوطنية أو الأجنبية ذات الهدف المشترك
- إعداد ونشر التقارير والإحصائيات السنوية مع إحترام واجب التحفظ حماية لخصوصية وسرية الأعمال الموجهة للجمهور، وإرسالها إلى الوزارة الأولى والوزارة المكلفة بالبريد والإتصال الإلكتروني وكذلك إلى البرلمان بغرفتيه.

1-عقباش بريزة مبارك حنان، آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، مرجع سابق، ص48

- السهر على إحترام الأحكام القانونية والتنظيمية المتعلقة بالأمن السيبيراني
- السهر على حماية حقوق المشتركين في الخدمات الاتصالات الإلكترونية ومعالجة شكاوهم
- نشر كل معلومة مفيدة لحماية حقوق المشتركين والقيام بحملات تحسيسية وتوعوية
- تمثيل الجزائر في المنظمات الدولية المختصة وتسديد المساهمات ونفقات المختلفة التي تستحقها المنظمات الإقليمية والدولية في مجال البريد والاتصالات الإلكترونية

02- المتدخلين في بيئة الأنترنت

في بعض الأحيان ونتيجة لعمل بعض العاملين في بيئة الأنترنت يصبح لهم صفة الضبطية الإدارية [1] مثلا على ذلك كمزودي الخدمات ومزودي الدخول إلى الأنترنت وذلك وفقا للقانون الذي يمنحهم صلاحية المراقبة في سير العمل ومدى الخضوع المتعاملين للنظام والقانون، لأنه إن تم من طرفهم الكشف عن وجود جريمة، وتقديم جميع المعلومات الضرورية للقيام سلطة الضبط بهامها

03: صعوبات مكافحة الجريمة الإلكترونية

يعترف المهتمون بشؤون تكنولوجيا المعلومات بصعوبة اكتشاف الجريمة الإلكترونية، وذلك للأسباب التالية:

- يمكن أن تنقضي عدة أشهر أو سنوات قبل اكتشاف الجريمة.

- صعوبة التوصل إلى الجاني، فكثيرا ما يقوم الجاني بالدخول إلى شبكة الأنترنت بإستخدام إسم مستعار، وغالبا ما يقوم بالدخول للأنترنت عن طريق مقاهي الأنترنت، فيصعب معرفة الجاني وتحديد موقع اتصاله.

-تنازع القوانين الجنائية من حيث المكان، إذ أن هناك مبادئ تحكم تطبيق القانون الجنائي منها مبدأ إقليمية القانون الجنائي، وتثور المشكلة في حالة ارتكاب الفعل الإجرامي في الخارج فأي من القوانين سوف يخضع لها الجاني. حيث تكمن صعوبة تحديد المسؤول جنائيا عن الفعل الإجرامي، كأن يدخل

1-عقباش بريزة مبارك حنان، آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، مرجع سابق، ص48

المستخدم للشبكة على موقع فيجد به أفعال إباحية، فهل يسأل عن هذه الجريمة عامل الإتصال، أم مورد المنافذ، أو مورد المعلومات، أو غيرهم من العاملين في مجال الأنترنت.

-إفتراض العلم بقانون جميع الدول، ففي حالة ارتكاب الجريمة في بلد ما، وتحقق النتيجة في بلد آخر يجد الجاني

صعوبة المطالبة بالتعويض المدني، حيث يرجع في ذلك لأحكام القانون الدولي الخاص.

- جهل الناس بثقافة الأنترنت يجعلهم يقومون بأفعال لا يعرفون بأنها تشكل جريمة يعاقب عليها القانون

-عدم ظهور الدليل المادي للجريمة الإلكترونية أو آثار مادية ملموسة .[1]

-عجز الوسائل التقليدية عن ضبط آثار الجريمة الإلكترونية .

-عولمة هذه الجريمة تؤدي إلى تشتيت جهود التحري والتنسيق الدولي، لتعقب مثل هذه الجرائم، وهي بمثابة صورة صادقة من صور العولمة.

-صعوبة تقدير حجم الجريمة الإلكترونية، فالإحصائيات الجنائية لا تعبر عن الإجرام الحقيقي، إذ منها ما يصل إلى علم السلطات المختصة بصورة دائمة، ومنها ما لا يصل إلى علمها إلا نادرا، كالجرائم الماسة بالعرض، وهنا يظهر الفارق بين الحجم الحقيقي للجريمة الإلكترونية، وبين ما هو مسجل بالإحصائيات. من خلال التطرق لمكافحة الجريمة الإلكترونية في التشريع الجزائري استنتج أنه لا بد من الوقاية من هذا النوع من الجرائم قبل انتشارها، واللجوء إلى مكافحتها، وذلك بتربية النشأ على الوازع الديني والأخلاق الفاضلة، اللذان هما بمثابة واقي للفرد يحول دون ارتكاب أي نوع من الجرائم، و يجعلان الفرد يعي مدى خطورة التعدي على حقوق الغير، علاوة على ذلك توعية الأفراد بأخطار وسلبيات الأنترنت، من خلال عقد ندوات ودراسات حول مخاطر الأنترنت في الجامعات والثانويات، وجميع الأنشطة من جمعيات وغيرها.

1-عقباش بريزة مبارك حنان، آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، مرجع سابق، ص48

ثانيا: الأجهزة الأمنية

01: الوحدات التابعة لسلك الأمن الوطني

أ-على مستوى المركزي

قامت المديرية العامة للشرطة القضائية بإستحداث مصلحة مختصة في لمكافحة الجريمة المعلوماتية تحت إسم نيابة مديرية مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وبالإضافة الى مديرية الشرطة العلمية والتقنية، (هي المخبر المركزي للشرطة العلمية) من أجل خدمة المصالح العملية المختصة بذلك، وتتولى أعمال البحث والتحري والتحقيق بشأن الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وهذه الوحدة والكائن مقرها بالجزائر العاصمة

2-**على المستوى الجهوي:**

تم إنشاء مخابر جهوية للشرطة العلمية في كل من:قسنطينة – وهران – ورقلة – بشار – تمنراست

وكل مخبر به مصلحة تسمى دائرة الأدلة الرقمية والآثار التكنولوجية التابعة لمخبر الأدلة الجنائية ، و تتولي هذه المصلحة أعمال البحث والتحقيق القائمة بشأن الجرائم المعلوماتية، وذلك تحت تسمية دائرة الأدلة الرقمية والأثار التكنولوجي [1] وتضم ثلاث 03 أقسام فرعية هي:

- قسم إستغلال الأدلة الرقمية الناتجة عن الحواسيب والشبكات.
- قسم إستغلال الأدلة الناتجة عن الهواتف النقالة.
- قسم تحليل الأصوات

وتضم كل دائرة في صفوفها ثمانية 08 أعضاء محققين أربع 04 منهم عناصر شرطيون رسميون

1- عمار حشمان ، الجريمة المعلوماتية في التشريع الجزائري مصدر سابق، ص 38

يتمتعون بصفة ضابط شرطة قضائية، والبقية هم أعوان شبيهون يحمل كل منهم شهادة جامعية في تخصص الإعلام الآلي إضافة إلى إلمامهم بالجانب القانوني

-**على المستوى المحلي:** ولتدعيم المصالح الولائية للشرطة القضائية في مجال مكافحة الجرائم المعلوماتية، أنشأت المديرية العامة للأمن الوطني سنة 2016 ما يقارب 48 فرقة لمكافحة الجرئام المعلوماتية.

ب: الوحدات التابعة للدرك الوطني

من أجل الحفاظ على الأمن والنظام العام ومحاربة الجريمة بكافة أنواعها

1-على المستوى المركزي: الهيئات لمكافحة الجرائم المعلوماتية ودعم أعمال البحث والتحقيق

- **مديرية الأمن العمومي والإستغلال:** وهي الهيئة التي تعمل على التنسيق بين مختلف الوحدات الإقليمية والمركز التقني العلمي، في مجال أعمال البحث والتحري في الجرائم المعلوماتية.

- المصلحة المركزية للتحريات الجنائية: وهي هيئة ذات إختصاص وطني من بين مهامها مكافحة الجريمة المرتبطة بتكنولوجيا الإعلام والإتصال.

- المعهد الوطني للأدلة الجنائية وعلم الإجرام وهو مؤسسة عمومية ذات طابع إداري، تم إنشاءه بمرسوم رئاسي رقم 04 - 183 بتاريخ 26 :جوان 2004 ، في إطار عصرنة قطاع الدرك الوطني مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية :أنشأ هذا المركز حديثا ويعتبر بمثابة نقطة وصل وطنية في مجال دعم أعمال البحث والتحقيق في الجرائم المعلوماتية إذ يوفر المساعدة التقنية للمحققين ويساهم في توجيه التحقيقات المرتبطة بتكنولوجيا الإعلام والإتصال ، فهو هيئة تقنية تعمل تحت وصاية مديرية الأمن العمومي والإستغلال لقيادة الدرك الوطني [1]

2-على المستوى الجهوي: تقوم بتنسيق النشاطات بين مختلف الوحدات التابعة للشرطة القضائية

1- عمار حشمان ، الجريمة المعلوماتية في التشريع الجزائري مصدر سابق، ص 44

وكذلك دعمها بالوسائل الخاصة للتحريات والأبحاث المعقدة كالجرائم المعلوماتية.

3-على المستوى المحلي : تم إنشاء خلية متخصصة لمكافحة الجرائم المتعلقة بتكنولوجيا الإعلام والإتصال في كل مجموعة ولائية، وهو ما يسمح بضم فصائل للأبحاث التي تتكون من أفراد لديهم خبرة وإختصاص في ميدان الشرطة القضائية، و هذه الفصائل مكلفة خصوصا بمكافحة الأشكال الخطيرة للإجرام المنظم كالجرائم المعلوماتية.

ملخص الفصل الثاني

في هذا الفصل تم تناول آليات الوقاية من الجرائم المعلوماتية في التشريع الجزائري وذلك حسب المؤسسات الجديد و المستحدثة لمكافحة الجريمة المعلوماتية كفكرة جديدة وناتجة عن التطور السريع للتكنولوجيا و بما لها من خطر على الأموال و الأشخاص و المؤسسات العامة و الخاصة على حد سواء و بغض النظر هذا الإعتداء سواء كان على المعطيات بدلالتها التقنية الواسعة أو الاستعانة بها لإرتكاب جرائم لها آثار كالجرائم التقليدية، لكنها ترتكب داخل الحاسب الآلي في عالمها الإفتراضي والشبكات العنكبوتية، وهذا مايسعى المشرع الجزائري من العمل المتواصل للحد من آثار هذه الجريمة المعلوماتية الجديدة وذلك من خلال الكشف المبكر لها و ووضع هيئات تحمل على عاتقها الكشف المبكر للجرائم المعلوماتية و ذلك بإستعمال أحدث الوسائل و طرق البرمجة و الأجهزة المتطورة الحديثة و النصوص القانونية لمواجهة هذه الجريمة، والصور التي جاءت بها هذه النصوص القانونية .

الخاتمة

مع التطور السريع للتكنولوجيا وانتشار استخدام الإنترنت، أصبحت الجريمة الإلكترونية واحدة من التحديات الأمنية الرئيسية التي تواجه المجتمعات في العصر الحديث يمكننا أن نستنتج أن إصدار القوانين الخاصة بمكافحة الجرائم الإلكترونية يعكس تطور التكنولوجيا وتزايد استخدام الإنترنت ووسائل الاتصال الإلكترونية في حياتنا اليومية. تعد هذه القوانين أدوات قانونية ضرورية للتصدي للتحديات القانونية والأمنية الناشئة عن الجرائم الإلكترونية.

وتأتي هذه التشريعات كخطوة هامة في تعزيز الأمن الرقمي وحماية المعلومات الشخصية في الجزائر. تم وضع هذه القوانين والقواعد الواضحة وعقوبات رادعة للتصدي للجرائم الإلكترونية والمخاطر الأمنية المرتبطة بها.

إن حماية الخصوصية وسرية المعلومات الشخصية تعد أولوية للمجتمع الرقمي، ويجب على الأفراد والمؤسسات الالتزام بالقوانين والتشريعات المتعلقة بالجرائم الإلكترونية.

من المهم أيضًا لزيادة الوعي وتعزيز التعليم في مجال الأمن الرقمي والجرائم الإلكترونية، حيث يلعب الأفراد دورًا حاسمًا في حماية أنفسهم ومنع الاعتداءات على خصوصيتهم. يجب أن يكون هناك تعاون وتنسيق بين الجهات المعنية، بما في ذلك القطاع الحكومي والخاص والمجتمع المدني، لضمان فعالية التشريعات وتطبيقها بشكل صحيح.

الا أنه نجد أن هناك تحديات التي تواجه مكافحة الجريمة الالكترونية وأهمها:

- **تطور التكنولوجيا** :يعد التقدم التكنولوجي السريع والمستمر تحديًا رئيسيًا. فمع كل تقدم جديد في التكنولوجيا، تظهر أساليب جديدة لارتكاب الجرائم الإلكترونية، مما يتطلب من القانون أن يتعاقب بشكل سريع وفعال.

- **الحدود القانونية** :قد تواجه القوانين الحالية صعوبة في مواجهة الجرائم الإلكترونية، بسبب عدم مواكبتها للتطور التكنولوجي السريع. قد يحتاج القانون إلى تحديث وتعديل لمواجهة هذه التحديات الجديدة.
- **التعاون الدولي** :الجريمة الإلكترونية لا تعترف بالحدود الجغرافية، ويمكن أن تتم بسهولة من قبل أفراد ومجموعات في مختلف أنحاء العالم. لذلك، يصبح التعاون الدولي في مكافحة الجريمة الإلكترونية ضرورة حتمية، ولكن هناك تحديات في تنسيق الجهود ومشاركة المعلومات بين الدول المختلفة.
- **الخصوصية وحقوق الفرد** :يجب أن يكون هناك توازن بين حماية المجتمع من الجرائم الإلكترونية وحماية خصوصية الأفراد وحقوقهم. ينبغي أن تضمن التدابير القانونية الفعالة القدرة على ملاحقة المجرمين دون المساس بالحقوق الأساسية للأفراد.
- **التحديات القضائية** :يمكن أن تواجه الأجهزة القضائية صعوبة في التعامل مع الجرائم الإلكترونية بسبب التعقيدات التقنية المرتبطة بها. قد يحتاج القضاة والمحققون إلى التدريب المستمر والتحديث القانوني لفهم ومواجهة التحديات الجديدة المرتبطة بالجرائم الإلكترونية.

لذلك يتعين على الأفراد والمؤسسات الالتزام بأحكام القانون رقم 09/04 واتخاذ التدابير اللازمة لحماية أنفسهم ومواجهة التهديدات الرقمية. يعد هذا القانون خطوة مهمة في توفير بيئة آمنة للاستخدام الآمن لتكنولوجيا المعلومات والاتصالات في الجزائر، يجب أن تظل التشريعات الجزائرية متجددة ومتوافقة مع التحديات الجديدة التي تطرأ في مجال الجرائم الإلكترونية.

ويجب أن يكون هناك التزام مستمر بتعزيز الحماية القانونية للأفراد والمؤسسات، وتطوير السياسات والإجراءات التي تعزز الأمان الرقمي وتحد من التهديدات الرقمية المستمرة.

قائمة المصادر و المراجع

I –المصادر

- **القرآن الكريم.**

II – الكتب

– أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ط 20 ، ج 1، دار هومة الجزائر، 2018.

– هاشم بشير، الآليات الدولية لمكافحة الجريمة الإلكترونية، المركز الدولي للدراسات المستقبلية والإستراتيجية، القاهرة مصر، 2012.

– نهلا عبد القادر المومني، الجرائم المعلوماتية، ط 2 ، دار الثقافة للنشر و التوزيع، عمان الأردن، 2010.

– فليب بروتون سيرج برو، ثورة الإتصال نشأة أيدويولوجية جديدة، ترجمة هالة عبد الرؤوف مراد، دار المستقبل العربي، القاهرة مصر، 1993.

– محمد نجيب دبابلو، الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، ط1 ، المركز المغاربي شرق أدنى للدراسات الإستراتيجية بريطانيا، 2024.

III – المذكرات

- عائشة نايري، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الإداري، جامعة أحمد دراية أدرار، الجزائر، 2017.
- عقباش بريزة مبارك حنان، آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، مذكرة مقدمة لإستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق، جامعة محمد بشير الإبراهيمي، برج بوعريريج الجزائر، 2022.
- عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة مقدمة لإستكمال متطلبات شهادة الماستر المهني، جامعة قاصدي مرباح ورقلة، 2019.

IV – المحاضرات البيداغوجية

- علي إبراهيم بن دراح، محاضرات في الجرائم المعلوماتية، مطبوعة بيداغوجية المركز الجامعي آفلو جامعة عمار ثليجي الأغواط الجزائر، 2021.

V – المجلات

- إيمان بغدادي، أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الإلكترونية، مجلة آفاق للبحوث والدراسات السياسية دولية محكمة، العدد 04، المركز الجامعي إليزي، الجزائر، 2019.

VI – الأوامر والنصوص القانونية

الأوامر

- الأمر رقم 66–156 المؤرخ في 08 جوان 1966، معدل ومتمم بالقانون 24–06 المؤرخ في 28 جوان 2024، والمتضمن قانون العقوبات، ج ر عدد 30

النصوص القانونية

- القانون رقم 09–04 المؤرخ في 05 اوت 2009 ، يتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر عدد 47.
- القانون 15–04 المؤرخ في 01 فيفري 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني، ج ر عدد 06
- القانون 18–04 المؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية، ج رعدد 27
- القانون 21–439 المؤرخ في 7نوفمبر 2021 ، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر عدد 86.

VII – المرسوم الرئاسي

- المرسوم الرئاسي 15-261 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 53.

VIII – موقع الأنترنت

- https://www.arpce.dz/fr/org-func (موقع سلطة الضبط)
- https://www.joradp.dz/HFR/Index.htm (موقع الجريدة الرسمية للدولة الجزائرية)

الفهرس

الإهداء	**I**
شكر و عرفان	**II**
قائمة المختصرات	**III**
مقدمة	أ
الفصل الأول: الأساس النظري والقانوني للجريمة المعلوماتية في التشريع الجزائري	
تمهيد	**13**
المبحث الأول: المفاهيم المرتبطة بالجريمة المعلوماتية	**14**
المطلب الأول: الإتجهات الفقهية في تعريف الجريمة المعلوماتية	**14**
أولا: تعريف الجريمة الإلكترونية من الإتجاه الضيق	**14**
ثانيا :الإتجاه الموسع من تعريف الجريمة الإلكترونية	**16**
ثاثا: الإتجاه الموسع والضيق لتعريف الجريمة (المختلط)	**18**
ثانيا: صور الجريمة المعلوماتية	**19**
المطلب الثاني: عناصر الجريمة المعلوماتية (أركان، خصائص، دافع)	**20**
الفرع الأول: أركان الجريمة المعلوماتية	**20**
الفرع الثاني: خصائص الجريمة المعلوماتية	**25**
المبحث الثاني: الطبيعة القانونية للجريمة المعلوماتية في القانون الجزائري	**32**
المطلب الأول: الأساس القانوني (394 مكرر وما بعدها) تحليل للنصوص القانونية	**32**
الفرع الأول: الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات	**32**
الفرع الثاني: الجرائم الواقعة على الأشخاص و الأموال	**35**
المطلب الثاني: الجرائم الواقعة على المؤسسات العمومية	**39**
الفرع الأول: الإرهاب الإلكتروني	**39**
الفرع الثاني: جريمة التجسس على الدولة	**40**
ملخص الفصل الأول	**41**
الفصل الثاني: آليات الوقاية من الجرائم المعلوماتية في التشريع الجزائري	
تمهيد	**43**
المبحث الأول : الوقاية القانونية من الجريمة المعلوماتية	**44**
المطلب الأول: التشريعات الخاصة (ق 09-04، 15-04، 18-04) تحليل النصوص القانونية	**44**
الفرع الأول: القانون يتعلق بالحماية و السرية	44

الفرع الأول: القانون يتعلق بالتوقيع و التصديق الإلكتروني	44
المطلب الثاني: العقوبات والإجراءات التحفظية والردعية	45
الفرع الأول: العقوبات الأصلية	48
الفرع الثاني: العقوبات المقررة للشخص المعنوي	49
الفرع الثالث: العقوبات التكميلية	51
المبحث الثاني: الوقاية المؤسسية والعملية من الجريمة المعلوماتية	51
المطلب الأول: دور الشرطة القضائية وقاضي التحقيق في الوقاية من الجريمة	52
الفرع الأول: الإجراءات التقليدية للكشف عن الجريمة المعلوماتية	52
الفرع الثاني :الآليات الحديثة للكشف عن الجريمة المعلوماتية	56
المطلب الثاني: دور الهيئات الوطنية ومؤسسات الرقابة السيبيرانية في الوقاية من الجريمة المعلوماتية	61
الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال	61
الفرع الثاني: هيئة الضبط الإداري و الأجهزة الأمنية	65
ملخص الفصل الثاني	72
الخاتمة	74
قائمة المصادر و المراجع	77
الفهرس	81