

تحديات الجريمة الإلكترونية في الجزائر The challenges of cybercrime in Algeria

تاريخ النشر: 2020/01/08	تاريخ القبول: 2019/09/23	تاريخ الارسال: 2019/08/18
-------------------------	--------------------------	---------------------------

د. خلوفي رشيد
جامعة الجزائر 1
rkhelloufi@yahoo.fr

*ط.د. بولحية شهرزاد
جامعة الجزائر 1
chahrazed.boulahia@yahoo.ca

ملخص :

إن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدى إلى بروز أشكال جديدة من الإجرام وهو ما يصطلح على تسميته بالجرائم الإلكترونية ومجالها جهاز الكمبيوتر المستخدم لاختراق شبكة الأنترنت لذلك يمكن القول أن كل تطور ايجابي لا يخلو من سلبيات والآثار السلبية للأنترنت كبيرة وخطيرة ذلك هو الأمر الذي ألقى رجال القانون مسؤولية تاريخية وإنسانية تجاه هذا الخطر الدائم إذ لا يخف على أحد بأن الجرائم الإلكترونية لم تعد تقتصر على القرصنة لسرقة المعلومات والسطو على أرقام بطاقات الائتمان لاستخدامها والاستغلال الجنسي للأطفال والإخلال بالآداب العامة ناهيك عن جرائم التجسس والإرهاب¹.

ثمة جهود كبيرة تُبذل لمحاربة الجريمة الإلكترونية بكافة أشكالها، لكن لتمييز هذه الجرائم من الصعب الكشف عنها وتحديد الدليل المادي الذي يدين مرتكبها. لذلك من المتوقع أن هذا النوع من الجرائم سيستمر ويطن على ساحة الاجرام بقدر كبير، وسيطور مع مرور الوقت إلى ما هو أخطر وأعقد. لذا فإن وجود استراتيجية فعالة لدى الدول تحارب هذه الجرائم هي الوسيلة الضامنة لتقليلها ومحاولة التحكم بها. ولا ننس دور الأفراد في محاربتها

*المؤلف المرسل : بولحية شهرزاد

عن طريق تبصيرهم بإيجابيات وسلبيات استخدام شبكة الإنترنت، وحث الشركات المتخصصة على إنتاج برامج حماية متخصصة تهدف إلى حماية البرامج الأخرى ومتصفحات الإنترنت .

الكلمات المفتاحية: الغش المعلوماتي، الاختلاس المعلوماتي؛ جريمة الحاسب؛ الاعتداء الإلكتروني؛ المساس بأنظمة المعالجة الآلية للمعطيات.

Abstract:

The technological progress has led to the appearance of new forms of criminality called Cyber-criminality. That is why the lawmen have assumed a historical, humanitarian responsibility for this constant threat. And it is not secret to anyone that cybercrimes are no longer restricted to piracy to steal information and credit card number, now it also includes the sexual exploitation of children and the violation of public decency, not to mention the crimes of espionage and terrorism in various fields.

There are efforts done for the sake of fighting the Electronic Crime. But, to distinguish these crimes, there is still some difficulty in revealing and precising its real evidence that proves the suspect guilty. This might be the reason why these crimes are expected to spread and cover a large part of the crimes scene that will be more dangerous and complicated. Therefore, having an effective strategy owned by the countries working against these specific crimes is the best way to reduce and control the Electronic crime. Not to mention the great role of individuals to protect themselves, and encourage the specialized companies to produce programs to protect the internet browsers.

Keywords: Information Fraud; Information embezzlement; Cyber Crime; Electronic Assault.

مقدمة:

أدى التطور الهائل في تكنولوجيا المعلومات والاتصال وزيادة الترابط الإلكتروني والاعتمادية المتزايدة على التقنية إلى ظهور نوع جديد من المعاملات تسمى بالمعاملات الإلكترونية تختلف عن المعاملات التقليدية؛ وبالمقابل أفرزت جرائم مستحدثة تعتمد على الوسائل التي أتاحتها تلك الثورة المعلوماتية خاصة الإنترنت والتي تدعى بجرائم الإنترنت أو جرائم استخدام الحاسوب التي تتمثل في كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية.

مرت الجريمة الإلكترونية بعدة مراحل تاريخية مختلفة فوصلت إلى درجة عالية من التطور، ونظرا لتطورها و تغيرها يصعب على التشريعات إيجاد مفهوم متفق عليه حيث تأرجحت تعاريفها بين التعريفات الواسعة والضيقة ولكنها لم تتخلف عن تصدي لها وكافحتها بأحدث الطرق، أما بالنسبة للمشروع الجزائري فقد تطرق إلى تعريف الجريمة الإلكترونية مسميا إياها بجريمة المساس بأنظمة المعالجة الآلية للمعطيات.

وتظهر مخاطر الجريمة المعلوماتية في التحديات التي تفرضها لمكافحتها في ظل طبيعتها التي تعتمد على الإنترنت، كالثقة المتزايدة في استعمال تكنولوجيا المعلومات والاتصال وزيادة عدد مستخدمي شبكة الانترنت، وظهور جرائم جدد، وإقامة إجراءات الإثبات الرقمية.

ولخطر هذا النوع من الجرائم والمحتمل أن يكون كبيرا في ظل ضعف الجاهزية التقنية والتشريعية، قامت العديد من الدول منها الجزائر بإصدار قوانين خاصة أو تعديل قوانينها الجزائية لمواجهة الآثار السلبية التي خلفتها هذه التقنية العالية إضافة إلى الوسائل الفنية وتأهيل كوادر قادرة على التتبع والتحقيق في هذه الظاهرة. ولم بكتف التشريع الجزائري بتجريم أعمال الإلكترونية وقوانين العقوبات وقانون الإجراءات والقوانين الخاصة والمتعلقة بها بل

أقرت أجهزة خاصة لمراقبة ومكافحة هذه الجريمة مجهزة بأحدث الطرق العلمية والمتطورة. ومهما تمت مكافحتها، تبقى الجريمة الإلكترونية في تطور بتطور وسائل التكنولوجيا. من أجل ذلك، تركز دراستنا على ستة محاور أساسية.

المحور الأول: تعريف الجريمة الإلكترونية أو الجريمة المعلوماتية

لم يتم الإجماع على تعريف عام وموحد للجريمة الإلكترونية كما تجنب غالبية المشرعين الخوض في مسألة وضع تعريف تشريعي لنظام المعالجة الآلية للمعطيات وأوكلوا مهمة ذلك إلى الفقه والقضاء. لهذا سنحاول في هذا المحور التطرق لمختلف التعاريف اللغوية منها والاصطلاحية وكذا تعريفها في الجزائر.

المحور الثاني: الطبيعة القانونية الخاصة للجريمة الإلكترونية

إن ارتباط الجرائم الإلكترونية بجهاز الحاسوب وشبكة الانترنت، أضفى عليها مجموعة من الخصائص المميزة لها عن باقي الجرائم التقليدية. لذا بات من الضروري إيجاد الوسائل المثالية للتوفيق بين التشريعات الخاصة بهذه الجرائم عن طريق إبرام الاتفاقات الدولية الخاصة بتسليم المجرمين والوسائل الكفيلة بمكافحة هذا النوع من الجرائم.

المحور الثالث: تجريم الأعمال الإلكترونية في القانون الجزائري

تأثر المشرع الجزائري بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل مما دفعه إلى تعديل قانون العقوبات وقانون الإجراءات الجزائية.

المحور الرابع: القوانين التي نصت على الجريمة الإلكترونية في الجزائر

رغبة من المشرع الجزائري في التصدي لظاهرة الإجرام الإلكتروني، وما يصاحبها من أضرار من جهة، ومحاولة منه تدارك الفراغ التشريعي القائم في هذا المجال من جهة أخرى، قام من خلال ذلك إلى إصدار قوانين عامة وخاصة.

المحور الخامس: الأجهزة المختصة في متابعة الجريمة الإلكترونية في التشريع الجزائري

نظرا للطابع الخاص للجريمة الإلكترونية ومختلف النصوص القانونية التي تم وضعها، تم إنشاء عدة أجهزة من أجل مكافحة هذا النوع من الجرائم، ألا وهي: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الهيئات القضائية الجزائية المتخصصة: الأقطاب القضائية الجزائية المتخصصة والمعهد الوطني للأدلة الجنائية وعلم الجرائم.

المحور السادس: الصعوبات التي تعترض مكافحة هذه الجريمة

تتميز جرائم الإنترنت بمجموعة من الخصائص التي تؤدي إلى صعوبة التعامل معها وضبطها، حيث تواجه الأجهزة الأمنية عند مواجهتها لهذه الجرائم على المستوى الوطني العديد من الصعوبات. كما تعد جرائم الإنترنت صورا إجرامية مستحدثة من الجرائم العابرة للحدود الوطنية في عالم ذابت فيه الفواصل وتلاشت الحدود، مما جعل من السهولة ارتكاب الجرائم عبر الشبكة الإنترنتية ليس فقط على المستوى الوطني، بل وعلى المستوى الدولي وهو ما يصعب أكثر التعامل معها.

المحور الأول: تعريف الجريمة الإلكترونية أو الجريمة المعلوماتية

لا يوجد إجماع على تعريف الجريمة الإلكترونية من حيث كيف تُعرف أو ما هي الجرائم التي تتضمنها الجريمة الإلكترونية. وكما يقول فان دير هيلست وونيف "هناك غياب لتعريف عام وإطار نظري متسق في هذا الحقل من الجريمة... وفي أغلب الأحيان تستخدم مصطلحات الافتراضية والحاسوب والإلكترونية والرقمية وكلها تعكس فجوات مهمة في التعريف².

1. التعريف اللغوي

يقصد بالمعلوماتية المعالجة الآلية وهي ترجمة للمصطلح الفرنسي informatique وتعني تكنولوجيا تجميع للمعلومات ومعالجة وإرسال المعلومات بواسطة الكمبيوتر، وقد استعمل

مصطلح traitement automatique des données ويعني المعالجة الآلية للبيانات ومصطلح télématique أي اتصالات، وهي تعادل مصطلح telematic في اللغة الإنجليزية وإن كان ليس لها أصل في القاموس الإنجليزي، مستمدة من اللغة الفرنسية³.

2. التعريف الاصطلاحي

سيشمل هذا التعريف، التعريف الفقهي والتعريف القانوني.

أولاً: التعريف الفقهي: يلاحظ عدم وجود اتفاق على مصطلح معين للدلالة على هذه الظاهرة المستحدثة، فهناك من يطلق عليها ظاهرة الغش المعلوماتي، أو الاختلاس المعلوماتي، أو الجريمة المعلوماتية، فهذا نجد بعض الفقهاء وضعوا تعريف الجريمة المعلوماتية في مجالين: مجال واسع ومجال ضيق⁴.

أ. التعريف الواسع: هناك تعريفات حاولت التوسع في مفهوم الجريمة المعلوماتية فعرفوها كالاتي: كّل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الاعتداء على الأموال والأشياء المعنوية. وقد أعطى الخبير الأمريكي Parker مفهومًا واسعًا للجريمة المعلوماتية أنها: كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل⁵.

يعرف الأستاذ Hestanc و Vivant الجريمة المعلوماتية أنها: مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب⁶.

أما جرائم الكمبيوتر فهو مصطلح شامل أشمل من المصطلح السابق ويقصد فيه كل الجرائم التي يستخدم فيها الكمبيوتر فهو سواء أداة الجريمة أو كان هدف الجريمة ويدخل من ضمنها جرائم معلوماتية وجرائم الإنترنت، كما يدخل من ضمنها الاعتداء على الشبكات المحلية خاصة بالهياكل والمنشآت الخاصة والعامة.

وجاء في تعريف آخر أن الجريمة الإلكترونية هي ببساطة استخدام التقنيات الرقمية لإخافة الآخرين⁷.

ب. التعريف الضيق: تعرف الجريمة المعلوماتية على أنها: "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكاب من ناحية لملاحقته وتحقيقه من ناحية أخرى".

يرى الأستاذ Mass أن المقصود بالجريمة المعلوماتية "الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح"⁸.

أما الفقيه الألماني Tiedemann فعرفها بأنها "كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب. فهو يركز في تعريفه على وسيلة ارتكاب الجريمة. يعرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية من خلال تعريف جريمة الحاسب أنها: الجرائم التي تلعب فيها البيانات الكمبيوتر والبرامج المعلوماتية دورا رئيسيا. وارتكز كذلك في تعريفه على الوسيلة المرتكبة بها الجريمة.

وجاء تعريف David Thompson لجريمة الحاسب بأنها: أي جريمة يكون متطلبا لاقتوافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب وهذا الفقيه ارتكز في تعريفه على توافر المعرفة بتقنية المعلومات⁹.

أما بالنسبة للفقه المصري، فهي تنشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال أو الأشياء المعنوية. وهناك فريق آخر يرى أن الجريمة المعلوماتية هي "عمل أو امتناع يأتيه إضرارا بمكونات الحاسب، وشبكات الاتصال الخاصة به، التي يحميها قانون العقوبات ويفرض له عقابا". وقد عرفها محمد علي العريان بأنها "كل فعل إيجابي أو سلبي عمدي يهدف إلى الاعتداء على تقنية المعلوماتية أية كان غرض الجاني"¹⁰.

يعتبر الاقتراح المقدم من قبل مجلس الشيوخ الفرنسي بشأن نظام المعالجة الآلية عند تبنيه للقانون 88-19 المتعلق بالغش المعلوماتي مؤرخ في 05 جانفي 1988 والذي تم إدماجه في القانون العقوبات الفرنسي، أهم تعريف يمكن الاعتماد عليه في تحديد مفهوم المعالجة الآلية للمعطيات، بحيث اقترح هذا المجلس التعريف التالي: نظام المعالجة تتكون كل منها ذاكرة، برامج، معطيات، أجهزة إدخال وإخراج، أجهزة ربط، يربط بينهما مجموعة من العلاقات

تتحقق عن طريق نتيجة معينة وهي معالجة المعطيات ، مع ضرورة أن يكون هذا المجموع أو المركب محميا بأجهزة أمان¹¹

ورغم شيوع هذا التعريف فيما بعد في أوساط الفقه إلا أن الجمعية الوطنية الفرنسية لم تحتفظ به عند الصياغة النهائية لنص القانون 88-19، وذلك لأسباب منهجية بحثة لا علاقة لها بمضمون هذا التعريف، الذي يبقى في كل الأحوال وسيلة لتفسير النص.

ويلاحظ على هذا التعريف أنه اشترط على نظام المعالجة الآلية للمعطيات أن تتوافر على شرطين لا قائمة له ولا حماية قانونية بدونهما هما: ضرورة وجود علاقات تربط ما بين العناصر الداخلة في تكوين النظام ، وتوحيدهما نحو تحقيق هدف واحد محدد هو المعالجة الآلية للمعطيات هذا مع الملاحظة أن العناصر الأدبية والمعنوية التي يتكون منها المركب والتي وردت في تعريف مجلس الشيوخ ، إنما وردت على سبيل المثال وهنا يفتح المجال أمام إضافة عناصر جديدة أو حذف بعضها حسب ما يفرزه التطور التقني في هذا المجال مستقبلا ضرورة توافر النظام على أجهزة أمان تحقق له حماية فنية كشرط للتمتع بالحماية الجنائية .

ثانيا: التعريف القانوني: إن غالبية المشرعين تجنبوا الخوض في مسألة وضع تعريف تشريعي لنظام المعالجة الآلية للمعطيات وأوكلوا مهمة ذلك إلى الفقه والقضاء، إلا أن بعضهم من جهة أخرى اتجهوا إلى وضع تعاريف لنظام المعلومات وليس لنظام المعالجة الآلية للمعلومات، ومن بين التشريعات التي عرفت النظام المعلوماتي نذكر:

أ. قانون Uncitral النموذجي بشأن التجارة الإلكترونية لسنة 1996 ، حيث عرف هذا القانون من خلال نص المادة 2 الفقرة و ، نظام المعلومات على أنه: "النظام الذي يستخدم لإنشاء رسائل البيانات أو إرسالها أو استلامها أو تخزينها لتجهيزها على أي وجه آخر"¹²

ب. قانون المعاملات الإلكترونية الأردني رقم 85 لسنة 2001 ، حيث عرف هذا القانون بدوره من خلال نص المادة 2 الفقرة 10 أيضا نظام معالجة المعلومات على أنه " :النظام الإلكتروني المستخدم لإنشاء رسائل المعلومات أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو تجهيزها على أي وجه آخر "¹³

ج. قانون إمارة دبي الخاص بالمعاملات والتجارة الإلكترونية رقم 02 لسنة 2002 ، حيث عرف هذا القانون هو الآخر من خلال نص المادة 2 الفقرة 6 ، بصدد تعريف المصطلحات أيضا نظام المعلومات الإلكترونية على أنه " : نظام إلكتروني لإنشاء أو استخراج أو إرسال أو استلام أو تخزين أو عرض أو معالجة المعلومات أو الرسائل إلكترونيا¹⁴ " .

الملاحظ على التعريفات الثلاثة المتقدمة أنها تنطبق على نظام المعالجة الآلية للمعطيات أكثر من على نظام المعلومات ككل ، كذلك أنها انصبت في مجرى واحد معتمد في تعريف نظام المعلومات على تعداد الوظائف التي يقوم بها أو ينجزها هذا النظام والتي تمثل طرق المعالجة المعلوماتية ومعبرة " المعالجة الآلية " مجرد وظيفة من تلك الوظائف¹⁵ .

على رغم من أن فكرة المعالجة الآلية أوسع من فكرة المعالجة المعلوماتية، أضف إلى ذلك خلوها من الإشارة إلى الشرطين اللذين أشار مجلس الشيوخ الفرنسي إلى ضرورة توافرها في النظام.

د. المشرع السعودي بحيث عرف المشرع السعودي من خلال نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية بموجب نص المادة 1 النظام المعلوماتي بأنه " : مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها ، وتشمل الحاسبات الآلية " ، وينطبق على تعريف المشرع السعودي¹⁶ ما تقدم من انتقادات بشأن تعريفات التشريعات الثلاث أعلاه، لكن يحسب له اشتراطه اشتمال النظام على حاسبات آلية ، إذ توجد في هذه الأخيرة على اختلاف أنواعها وإن صح التعبير غرفة عمليات المعالجة الآلية للمعطيات ، يتميز الحاسب الآلي بقدرته الهائلة على معالجة أحجام ضخمة من البيانات والمعطيات وبسرعة عالية جدا ودقة متناهية دون تعب أو ملل¹⁷ .

3. تعريف الجريمة الإلكترونية في الجزائر

أولاً: التعريف الفقهي: إن الجريمة الإلكترونية تتمتع بخطورة إجرامية لم يشهد لها العالم مثيلاً في الجرائم التقليدية، فلهذا ظهر اختلاف في تعريف قائماً من هذه التعاريف ما يلي "بأنها الجريمة التي تتم باستخدام جهاز الكمبيوتر من خلال الاتصال".

وهناك من يعرفها على أنها "كل عمل أو امتناع عن عمل يقوم به شخص إضراراً بمكونات الحاسب المادية والمعنوية، وشبكات الاتصال الخاصة به، باعتبارها من المصالح والقيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها". أو أنها "استخدام الأجهزة التقنية الحديثة مثل الحاسب الآلي والهاتف النقال، أو أحد ملحقاتها أو برامجها في تنفيذ أغراض مشبوهة وأمور غير أخلاقية لا يرتضيها المجتمع"¹⁸. ومن خلال هذه التعاريف تبني الفقه الجزائري تعريف المؤتمر العاشر للأمم المتحدة لمنع الجريمة حول جرائم الحاسب الآلي وشبكاته إذ عرف الجريمة المعلوماتية بأنها جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب وتتمثل من ناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية¹⁹.

ثانياً: التعريف الأكاديمي: كل فعل إجرامي متعمد أي كانت صلته بالمعلوماتية، ترتبت عنه خسارة تلتحق بالصحة أو مكسب يحققه الجاني، كما يمكن الاعتماد في التعريف الواسع للجريمة المعلوماتية على:

1- عندما ما تكون المعلوماتية موضوعاً للاعتداء (عندما تقع الجريمة على المكونات المادية للأجهزة والمعدات المعلوماتية).

2- عندما تكون المعلوماتية أداة ووسيلة للاعتداء (عندما يستخدم الجاني أو جهاز معلوماتي لتنفيذ جريمته)²⁰.

ثالثاً: التعريف القانوني: تبني المشرع الجزائري للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبراً أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلاً للجريمة ويمثل نظام المعالجة الآلية للمعطيات المسألة الأولية الشرط الأولي الذي

لا بد من تحقيقه حتى يمكن البحث في توافر أو عدم توافر أركان الجريمة من جرائم الاعتداء على هذا النظام فإن ثبت تخلف هذا الشرط الأولي فلا يكون هناك مجال لهذا البحث²¹.

لم يتخلف المشرع الجزائري بدوره عن ركب التشريعات التي وضعت تعريفا لنظام المعلومات، حيث أنه عرف من خلال نص المادة 2 من الفقرة من القانون رقم 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها مسميا إياه "المنظومة المعلوماتية" وهي أي نظام منفصل أو مجموعة من الأنظمة المتصلة مع بعضها البعض أو مترابطة، يقوم واحد منها أو أكثر معالجة الآلية للمعطيات تنفيذا لبرنامج معين²² "

جرم المشرع الجزائري الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثر الجزائر بالثورة المعلوماتية إذ تعد أشكالاً جديدة من الإجرام التي لم تشهدها البشرية من قبل وهذا دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في العاشر من نوفمبر 2004 المتمم للأمر رقم 66-156 المتضمن قانون العقوبات والذي أفرد القسم السابع مكرر منه تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات والذي تضمن 08 مواد من المادة 394 مكرر وحتى المادة 394 مكرر²⁴ 07.

وفقا للمشرع الجزائري في تعريفه لنظام المعالجة الآلية للمعطيات مقارنة مع التشريعات الأخرى اشترط ضرورة الترابط بين مكونات أو أجهزة النظام أو بين الأنظمة فيما بينها، وركز على وظيفة المعالجة الآلية للمعطيات موسعا بذلك المجال ليشمل كلا من المعالجة الآلية للمعطيات²⁵.

أما فيما ينص الشرط الثاني لمجلس الشيوخ الفرنسي والمتعلق بضرورة توافر النظام على حماية فنية فيبدو ان النظام المشرع قد حسم موقفه إلى جانب الفقه الذي لا يشترط هذا الشرط لحماية نظام المعالجة الآلية للمعطيات الجنائية²⁶.

المحور الثاني: الطبيعة القانونية الخاصة للجريمة الإلكترونية وخصائصها

لبيان الطبيعة القانونية للجريمة الإلكترونية لابد من تقسيم هذا المحور إلى فرعين نتطرق في الفرع الأول إلى الطبيعة القانونية وفي الفرع الثاني إلى خصائص الجريمة الإلكترونية.

1. الطبيعة القانونية الخاصة للجريمة الإلكترونية

إن دراسة الجريمة الإلكترونية بشكل خاص تدخل ضمن قسم من أقسام قانون العقوبات وهو قسم الخاص وهو ذلك الفرع الذي يدرس كل جريمة على حده متناولا كل عناصرها الأساسية والعقوبة المقررة لها ، فالجريمة تتعلق بالقانون المعلوماتي لأنها ظاهرة إجرامية ذات طبيعة خاصة²⁷

"إن هذا النوع من الجرائم يرتكب ضمن نطاق المعالجة الإلكترونية للبيانات سواء أكان في تجميعها أو تجهيزها أم في إدخالها إلى الحاسب المرتبط بشبكة المعلومات ولغرض الحصول على معلومات معينة ، كما قد ترتكب هذه الجرائم في مجال الكلمات أو معالجة النصوص وهذا النوع الأخير من الجرائم لا يعد أن يكون طريقة أوتوماتيكية المستخدم من تحرير الوثائق والنصوص على الحاسب مع توفير إمكانيات التصحيح والمسح والتخزين والاسترجاع والطباعة"²⁸

فهذه العمليات كلها هي وثيقة الصلة بالجرائم محل البحث وعليه لابد للجاني من فهمها فضلا عن أن الجاني قد يتعامل مع مفردات جديدة كالبرامج والمعطيات التي تشكل محل الاعتداء أو تستخدم وسيلة له²⁹.

تكمن الطبيعة الخاصة لهذه الجرائم في قدرة شبكة المعلومات على نقل وتبادل معلومات ذات طابع شخصي وعام في آن واحد مما يؤدي إلى الاعتداء على الخصوصية والسبب في ذلك توسع بنوك المعلومات بأنواعها علاوة على رغبة الأفراد وسعيهم إلى ربط حواسيبهم بالشبكة.

وبالتالي هذه الطبيعة الخاصة للأفعال المجرمة هل تدخل ضمن أحكام خدمات البريد أم التخابر الخاص أم يكون الهدف الأساسي للتحري عن نظام القانوني المناسب لطبيعة الجرائم المعلوماتية هو معرفة النصوص القانونية الوضعية التي يجب تطبيقها على خدمات نشر

المواقع والمعلومات فيها ؟ ومن هذا النظام القانوني تتحدد المسؤولية التي يفترض تطبيقها على الأشخاص المسؤولين عن هذا النشر، ومن خلال المجال التي ترتكب فيه الجريمة المعلوماتية والمحل الاعتداء عليها تظهر لنا الطبيعة القانونية الخاصة للجريمة³⁰.

إن التطور المعلوماتي يفتح المجال لاقتناء وسائل الكترونية تمكن المتجاوزين لاستخدامها في ارتكاب جرائم مختلفة لأن الإجرام المعلوماتي يتعلق بكل سلوك غير مشروع فيها يتعلق بالمعالجة الآلية لبيانات وإدخال المعلومات ونقلها ومن ثم يتحتم ضمه إلى نطاق القانون الجنائي على الرغم من أن معظم نصوصه المقارنة عاجزة عن مواكبة التطور المعلوماتي أو بما يحتويه من فراغ تشريعي في هذا المجال.

أما من حيث تكييف القانوني فتتخذ هذه الجرائم طبيعة خاصة إذا لم تكن القواعد التقليدية مخصصة لهذه الظواهر الإجرامية المستحدثة، إن تطبيق النصوص التقليدية على الجرائم المعلوماتية يثير مشاكل عديدة في مقدمتها مسألة الإثبات وصعوبة إيجاد دليل مادي يدين مرتكب الجريمة لأنه من السهل على الجاني محو أدلة الإدانة في وقت قصير لا يتجاوز لحظات وخاصة في حالة تفتيش الشبكات أو عمليات اعتراض الاتصال قد تكون البيانات التي تجري البحث عنها مشفرة ولا يعرف شفرة الدخول إلا أحد العاملين على الشبكة و من هنا تثار مسألة مدى مشروعية إجباره على فك الشفرة³¹.

ومن صعوبة ملاحقة مرتكبي الجرائم المعلوماتية الذين يقيمون في دولة أخرى دون أن ترتبط هذه الدولة باتفاقية مع الدولة التي تحقق فيها السلوك الإجرامي أو جزء منه وفي ضوء الاعتبارات السابقة يمكن القول بأن هذه الجرائم تتمتع بطبيعة قانونية خاصة.

2. خصائص الجريمة الإلكترونية

إن للجريمة الإلكترونية خصائص كثيرة سنحاول حصرها وإبرازها في ما يلي:

أولا الجرائم الإلكترونية من الجرائم العابرة للحدود: وسعت شبكات المعلومات عملية الاتصال وتبادل معلومات بين الدول والأنظمة التي يفصل بينها آلاف الأميال، ومع القدرة التي يتمتع بها الحاسب أدى ذلك إلى إمكانية ارتكاب الجريمة الإلكترونية في أماكن متعددة من العالم وفي وقت واحد، كما يمكن أن يكون المجني عليه في غير الدولة التي يقيم فيها الجاني³².

إن الجريمة المعلوماتية هي شكل من أشكال الجرائم العابرة للحدود، فمسرح الجريمة لم يعد محليا بل أصبح عالميا إذ أن الفاعل لا يتواجد ماديا على مسرح الجريمة وهذا التباعد في المسافات بين الفعل المرتكب من خلال الحاسوب والفاعل وبين المعلومات التي كانت محل الاعتداء، فالجاني يستطيع القيام بجريمته بالدخول إلى ذاكرة الحاسوب الآلي الموجود في بلد آخر وهذا الفعل قد يضر شخصا ثالثا في بلد آخر.

ومن خلال هذه الخاصية الدولية يثار إشكال حول الاختصاص القضائي في محاكمة المجني عليه بمعنى آخر ما هي الدولة المختصة بمحاكمة الجاني؟ هل هي الدولة التي ارتكب على إقليمها النشاط إجرامي أم التي يوجد فيها المجني عليه؟

وبمعنى آخر أن هذه الجريمة لا تقع في دولة واحدة ولا تعترف هذه الجريمة بالحدود الجغرافية للدول إذ غالبا ما يكون الجاني في بلد والمجني عليه في بلد آخر وقد يكون الضرر المحتمل في بلد ثالث.

ثانيا صعوبة اكتشاف وإثبات الجرائم الإلكترونية : تمتاز الجرائم المعلوماتية بصعوبة الاكتشاف والإثبات وذلك نظرا لعدم ترك الجاني آثار تدل على إجرامه، فالجرائم التي تتم بواسطة إدخال الرموز والأرقام، هي رموز دقيقة ويصعب اكتشافها وإثباتها لهذا عادة ما يتم اكتشافها بالصدفة وغالبا ما يتم معاقبة مجرمين وذلك لعدم وجود أدلة قائمة في حقه³³.

فالجريمة المعلوماتية لا تترك أثارا ملموسة وبذلك لا تترك شهودا يمكن الاستدلال بأقوالهم ولا أدلة مادية يمكن فحصها لأنها تقع في بيئة افتراضية يتم فيها نقل المعلومات وتناولها بواسطة نبضات الكترونية غير مرئية.

وصعوبة اكتشاف وإثبات الجرائم المعلوماتية راجع لعدة أسباب منها وسيلة التنفيذ التي تتسم في أغلب الحالات بالطابع التقني الذي يضيف عليها الكثير من التعقيد ومن ثم فإنها تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها، لأنها تتطلب إلماما خاصا بتقنيات الكمبيوتر ونظم المعلومات.

ويصعب في جرائم المعلوماتية العثور على دليل مادي للجريمة وذلك راجع إلى استخدام الجاني وسائل فنية وتقنية معقدة في كثير من الأحيان، وهذا السلوك المادي في ارتكابها لا يستغرق إلا ثواني معدودة يتم فيها محو الدليل والتلاعب به³⁴.

ثالثا: تتطلب وسائل خاصة في الحاسب الآلي وشبكة الأنترنت: إن الجريمة المعلوماتية تستلزم لقيامها توفر الحاسب الآلي وكذلك شبكة الانترنت وسيلة ارتكاب الجريمة وأدواتها الرئيسية أماكن المعرفة التقنية فتكون ضرورية بحسب درجة خطورة الجريمة المعلوماتية³⁵.

رابعا: تتطلب خبرة وتحكما في تكنولوجيا المعلوماتية عند متابعتها: إن جريمة المعلوماتية لها طبيعة تقنية وبذلك لا يستطيع رجال الضبطية القضائية التعامل باحترافية ومهارة أثناء البحث والتحري، لذلك لابد أن يكون المحقق متخصص في جريمة المعلوماتية حتى لا يتسبب في إتلاف الدليل الإلكتروني³⁶.

خامسا: تعدد الجرائم المعلوماتية أقل عنفا من الجرائم التقليدية: إن هذه الجريمة تعتمد على الدراية الذهنية والتفكير العلمي المدروس القائم على معرفة بتقنيات الحاسب الآلي، وفي الواقع ليس هناك شعور بعدم أمان تجاه المجرمين في مجال المعرفة المعلوماتية لأن مرتكبها ليسوا محترفي الإجرام³⁷.

سادسا: دافع ارتكاب الجريمة المعلوماتية: إن باعث الدافع الجريمة المعلوماتية قد يختلف عن دافع الجريمة التقليدية فقد يكون الدافع مخالفة النظام العام والخروج على القوانين وقد يكون ماديا يراد به اكتساب مبالغ طائلة أو الإهانة والتشهير... إلخ يكن دون الاحتكاك المباشر بالمجني عليه³⁸.

المحور الثالث: تجريم الأعمال الإلكترونية في القانون الجزائري

1. تجريم الأعمال الإلكترونية في قانون العقوبات الجزائري

لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل مما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 15-04 المؤرخ في 10 نوفمبر 2004 المتمم لأمر 156-66 المذكور سابقا، حيث أضيف قسم بعنوان المساس بأنظمة المعالجة الآلية للمعطيات " ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى 394 مكرر ونصت هذه المواد على ما يلي :

نصت المادة 394 مكرر على جريمة الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات محاولة ذلك بنصها " يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50000 دج إلى 100000 دج كل من يدخل أو يبقى عن طريق الغش في كل جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك .

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير معطيات المنظومة. وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج ."

نصت المادة 394 مكرر 1 على إدخال أو إزالة أو تعديل بطريق الغش معطيات في نظام المعالجة الآلية بنصها " يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500.000 دج إلى 2000.000 دج ، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل الغش المعطيات التي يتضمنها".

نصت المادة 394 مكرر 2 على أن " يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1000.0000 دج إلى 5000.0000 دج كل من يقوم عمدا وعن طريق الغش بما يأتي :

1. تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلّة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.
 2. حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.
- نصت المادة 394 مكرر 3 على أنه " : تضاعف العقوبة المنصوص عليها في هذا القسم ، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام ، دون الإخلال بتطبيق عقوبات أشد".
- نصت المادة 394 مكرر 4 على أنه " يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات بالحد الأقصى للغرامة المقررة للشخص الطبيعي 1".
- نصت المادة 394 مكرر 5 على فعل اشتراك في جريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم فإنه يعاقب بنفس عقوبة المقررة للجريمة في حد ذاتها وذلك بنصها " كل من شارك في مجموعة أو في اتفاق بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها".
- نصت المادة 394 مكرر 6 على " مع الاحتفاظ بحقوق الغير حسن النية، بحكم مصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكيها".
- نصت المادة 394 مكرر 7 على أنه " يعاقب على الشروع في ارتكاب الجناح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنة ذاتها".

في عام 2006 أدخل المشرع الجزائري تعديلا آخر على قانون العقوبات بموجب قانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 حيث مس ذلك التعديل القسم السابع مكرر والخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وقد تم تشديد العقوبة المقررة لهذه الأفعال فقط دون المساس بالنصوص التجريبية الواردة في هذا القسم من القانون 04-15 وربما يرجع سبب هذا التعديل إلى ازدياد الوعي بخطورة هذا النوع المستحدث عن الإجرام باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى وشيوع ارتكابه ليس فقط من الطبقة المثقفة بل من قبل الجميع بمختلف الأعمار ومستويات التعليم نتيجة تبسيط وسائل التكنولوجيا المعلومات وانتشار الأنترنت كوسيلة لنقل المعلومات.

2. تجريم الأعمال الإلكترونية في قانون الإجراءات الجزائية الجزائري

نجد أن المشرع نص على تمديد الاختصاص المحلي لوكيل الجمهورية في جرائم الإلكترونية في المادة 37 قانون الإجراءات الجزائية. ونص على التفتيش في المادة 45 الفقرة 7 وعلى توقيف النظر في جريمة المساس بأنظمة المعالجة في المادة 51 الفقرة 6 وعلى تراض المراسلات وتسجيل الأصوات والتقاط الصور من المادة 65 مكرر 5 إلى 65 مكرر 10.

أما بالنسبة لنصوص إجراءات التحقيق والمحاكمة تطبق عليه نفس إجراءات الجريمة التقليدية⁴⁰.

المحور الرابع: القوانين التي نصت على الجريمة الإلكترونية في الجزائر

1. الدستور الجزائري

بعد تعديل 2016، نصت المادة 44 منه أن "حقوق المؤلف يحميها القانون. لا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا بمقتضى أمر قضائي". كما نصت المادة 46 منه "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميها القانون. سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة. لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية. ويعاقب القانون على انتهاك هذا

الحكم. حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه".

2. قانون رقم 03-2000⁴¹ المؤرخ في والذي 5 أوت 2000 يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلوكية واللاسلكية

تسارع هذا القانون إلى مواكبة التطور الذي شهدته التشريعات العالمية مسايرة التطور التكنولوجي لذلك بات من السهولة بمكان اجراء التحويلات المالية عن الطريق الإلكتروني ذلك ما نصت عليه المادة 87 من هذا القانون بالقول " يمكن أن ترسل الأموال ضمن النظام الداخلي بواسطة الحوالات الصادرة عن المتعامل والمحولة بالبريد أو البرق أو عن الطريق الإلكتروني ".

نصت المادة 84 الفقرة 2 منه " تطبق أحكام المادة 89 من هذا القانون عن استعمال جوالات دفع عادية أو الكترونية أو برقية ".

نصت المادة 105 الفقرة الأخيرة على أنه " لا يمكن بأي حال من الأحوال انتهاك حرمة المراسلات ".

رتبت المادة 127 منه جزاء كل من تسول له نفسه ويحكم مهنته أن يفتح أو يحول أو يخرب البريد أو ينتهك حرية المراسلات بنصها " :كل موظف أو عون من أعوان الدولة أو مستخدم أو مندوب عن مصلحة البريد يقوم اختلاس أو إتلاف رسائل مسلمة إلى البريد أو يسهل فضها أو اختلاسها أو إتلافها يعاقب بالحبس من ثلاثة أشهر إلى خمس سنوات وبغرامة من 30.000 دج إلى 500.000 دج .ويعاقب بالعقوبة نفسها كل مستخدم أو مندوب في مصلحة البرق أو يختلس أو يتلف برقية أو يذيع محتواها. ويعاقب الجاني فضلا عن ذلك بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس إلى عشر سنوات.

3. قانون رقم 01-08⁴² المؤرخ في 2 جاتفي 2008 والمتمم للقانون رقم 83-01 المتعلق بالتأمينات الاجتماعية

نصت المادة 6 مكرر 1 على أنه البطاقة الالكترونية تسلم للمؤمن له اجتماعيا مجانا من طرف هيئات الضمان الاجتماعي وهي صالحة في كل التراب الوطني وهي تقدم لكل مقدم علاج أو مقدم خدمات مرتبطة بالعلاج وهذا الأخير يزود الكترونيا يسمى " المفتاح الالكتروني لهيكل العلاج " حسب نص المادة 65 مكرر⁴³.

نصت المادة 93 مكرر 2 منه على معاقبة كل من يسلم أو يستلم البطاقة الالكترونية بغرض استعمالها بطريقة غير مشروعة وجاءت كما يلي: "دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به ، يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 100.000 دج إلى 200.000 دج.

كل من يسلم أو يستلم بهدف الاستعمال غير المشروع البطاقة الالكترونية للمؤمن له اجتماعيا أو المفتاح الالكتروني لهيكل العلاج أو المفتاح الالكتروني لمهن الصحة"

نصت المادة 93 مكرر 3 على أنه من يقوم عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا أو في المفتاح الالكتروني لهيكل العلاج أو في المفتاح الالكتروني لمهن الصحة وهي نفس العقوبة التي تطلق كذلك على كل من قام بتعديل أو نسخ وبطريقة غير مشروعة البرمجيات التي تسمح بالوصول أو باستعمال المعطيات المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا أو في المفتاح الالكتروني لهيكل العلاج أو مهن الصحة.

4. قانون 04-09⁴⁴ مؤرخ في 14 شعبان 1430 الموافق ل 09 ل 5 أوت 2009 للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

إن إصدار المشرع الجزائري لقانون 09/04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها قام بإرساء قواعد إجرائية جديدة تضمن تحكما جيدا في أساليب مكافحة هذا النوع الجديد من الإجرام وبما يتوافق

وخصائصه، فقد شملت مواده الكثير من الآليات المستحدثة بنصه على إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، كذلك القواعد المتعلقة بالاختصاص الإقليمي للقانون الجزائري حيث تم التوسع في الاختصاص الإقليمي للسلطة القضائية في متابعة جرائم تمس مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني نظرا لما يمكن لهذه التكنولوجيات الحديثة من القيام به في حالة استغلالها ضد مصالح الدولة ولو في أقاليم دول أخرى من طرف جزائريين أو أجانب، أيضا فإن عالمية استغلال تكنولوجيات الإعلام والاتصال وخاصة الانترنت أدت إلى حذف الحدود الإقليمية وأصبحت الجرائم تمتد عبر عدة أقاليم وتكون من اختصاص القانون الجزائري لأكثر من دولة مما قد ينجر عنه تنازع في الاختصاص أو رفض له، مما قد ينشأ للمجرمين أماكن لا قانون فيها فكان التعاون الدولي في هذا النوع من الجرائم مفيدا وفعال جدا ولا يتأتى ذلك إلا باستعمال الطرق الحديثة للتواصل ما بين السلطات القضائية دون المرور بالطرق الدبلوماسية المعقدة وهو ما تم تشريعه فعلا ضمن هذا القانون، كذلك الأمر بالنسبة لتنسيق القوانين الجزائية العالمية سيؤدي بالتأكيد لإحكام قبضة العدالة على المجرمين في أي دولة يكونون فيها. أيضا فإن لطرق التحري في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ميزاتها والتي تبناها المشرع في القانون 09/04، فالمراقبة الإلكترونية للاتصالات وتفتيش نظم المعلوماتية أعطى لها القانون صفة الشرعية القانونية بتقنياتها وإدخالها ضمن الترسنة الإجرائية الجزائية في القانون الجزائري، تسمح للمتحرين عن الجرائم والمحققين فيها فسحة قانونية لتقديم الأدلة اللازمة لإدانة المتهم أو تبرئته. كما يلعب مقدمو الخدمات بما لديهم من تقنيات متماشية مع تطور التكنولوجيات الحديثة للإعلام والاتصال دورا مهما في مكافحة هذا النوع من الإجرام وتقديم المساعدة التقنية للسلطات المكلفة بالبحث والتحري عن الجرائم المرتكبة بواسطة أو ضد هذه التكنولوجيات، وأيضا الالتزام بما قرره المشرع بحفظ للمعطيات المعلوماتية يسمح للمتحرين تتبع الجريمة وحركة المجرمين.

المحور الخامس: الأجهزة المختصة في متابعة الجريمة الإلكترونية في التشريع الجزائري

سننتقل إلى ثلاث أجهزة لمتابعة هذه الجريمة والمتمثل في:

1. الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

يقصد بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال جرائم المساس بأنظمة المعالجة الآلية للمعطيات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية.

وأنشئت بموجب القانون رقم 04-09 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها⁴⁵.

تعد سلطة إدارية مستقلة لدى وزير العدل تعمل تحت إشراف ومراقبة لجنة مديرة يرأسها وزير العدل وتضم أساسا أعضاء من الحكومة معنيين بالموضوع ومسؤولي مصالح الأمن وقاضيين اثنين من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

وتضم الهيئة قضاة وضباط وأعوان من الشرطة القضائية تابعين لمصالح الاستعلام العسكرية والدرك الوطني والأمن الوطني وفقا لأحكام قانون الإجراءات الجزائية.

وتكلف الهيئة بتنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. كما تعنى بمساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال وضمان مراقبة الاتصالات الإلكترونية للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم التي تمس بأمن الدولة وذلك تحت سلطة القاضي المختص وباستثناء أي هيئة وطنية أخرى.

ومن مهام الهيئة الوطنية أيضا تفعيل التعاون القضائي والأمني الدولي وإدارة وتنسيق عمليات الوقاية ولمساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية.

وهناك الحالات التي تسمح بمراقبة الاتصالات الالكترونية لأغراض وقائية كالوقائية من جرائم الإرهاب والجرائم الماسة بأمن الدولة بإذن من النائب العام لدى مجلس قضاء الجزائر لمدة ستة أشهر قابلة للتجديد. والوقاية من اعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني بإذن من السلطة القضائية المتخصصة.

2. الهيئات القضائية الجزائية المتخصصة: الأقطاب القضائية الجزائية المتخصصة

أولاً: إنشاؤها : أنشئت بموجب القانون 14-04⁴⁶ المؤرخ في 10 نوفمبر 2004 المعدل للقانون الإجراءات الجزائية. تختص الجهات القضائية المتخصصة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقاً للمواد 37 ، 40 و 329 من قانون إجراءات الجزائية. تتمتع باختصاص إقليمي موسع طبقاً للمرسوم التنفيذي رقم 06-348 المؤرخ في 5 جانفي 2006. ويمكن قيام اختصاص المحاكم الجزائية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة في الخارج حتى ولو كان مرتكبها أجنبياً إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني المادة 15 من القانون رقم 04-09.

ثانياً: توسيع صلاحية الضبطية القضائية: عند معاينة الجرائم الماسة بأنظمة المعالجة الآلية كما يمكن تمديد الاختصاص المحلي على كامل الإقليم الوطني المادة 16 قانون إجراءات جزائية. كما يمكن تفتيش المحلات السكنية وغير السكنية في كل ساعة من ساعات الليل والنهار بإذن من وكيل الجمهورية حسب المادة 47 قانون الإجراءات الجزائية.

ثالثاً: أساليب التحري الخاصة : تتمتع الأقطاب بالصلاحيات التالية:

- اعتراض المراسلات الالكترونية وفقاً للمادة 65 مكرر من 5 قانون إجراءات الجزائية المدرجة بموجب القانون 06-22 المؤرخ في 20 ديسمبر 2006.
- التسرب المادة 65 مكرر 11 من قانون الإجراءات الجزائية .
- تفتيش المنظومة المعلوماتية المادة 5 من القانون رقم 04-09.

- حجز المعطيات المعلوماتية المادة 6 رقم 09-04.
- نسخ المعطيات على دعامة تخزين الكترونية.
- إمكانية منع الوصول إلى معطيات تحتويها المنظومة.
- منع الاطلاع على المعطيات التي يشكل محتواها جريمة.

3. المعهد الوطني للأدلة الجنائية وعلم الجرائم

يتكون المعهد الوطني للأدلة الجنائية وعلم الإجرام من إحدى عشرة دائرة متخصصة في مجالات مختلفة، جميعها تضمن إنجازها الخبرة، التكوين والتعليم تقديم المساعدات التقنية، البحوث، الدراسات والتحليل في علم الجريمة. تكلف دائرة الإعلام الآلي والالكتروني بمعالجة، تحليل وتقديم كل دليل رقمي وتمائلي للعدالة كما تقدم مساعدة تقنية للمحققين في التحقيقات المعقدة.

يسهر أفراد الدائرة على تأمين اليقظة التكنولوجية من أجل تحسين المعارف، التقنيات والطرق المستعملة في مختلف الخبرات العلمية، لإنجاز المهام المنوطة بها، تنقسم الدائرة إلى ثلاث مخابر وذلك حسب نوع المعلومات (سمعية، بصرية، والإعلام الآلي). كل مخبر مزود بقضية مهمتها إنشاء المعطيات من حوامل المعلومات وضمان نزاهة وشرعية الدليل وهذه المخابر هي: مخبر الإعلام الآلي، مخبر الفيديو ومخبر الصوت⁴⁷.

أولاً: مخبر الإعلام الآلي: من مهامه تحليل ومعالجة حوامل المعطيات الرقمية (الهاتف، الشريحة، القرص الصلب، ذاكرة الفلاش)، تحديد التزوير الرقمي للبطاقات البنكية. ومن تجهيزاته: محطة ترميم وتصلح الأجهزة والحوامل المعطلة، الشبكات الإعلامية (خبرات الإعلام الآلي والتجهيزات البيانية)، محطة ثابتة ومحمولة لإجراء خبرات الإعلام الآلي وجهاز اقتناء معلومات الهواتف والحواسب.

أما القاعات التي يحتوي عليها: تتمثل في 7 قاعات (مكتب التوجيه، فصيلة الأنظمة المشحونة، فصيلة تحليل المعطيات، فصيلة الهواتف، فصيلة اقتناء المعطيات، قاعة موزع وقاعات تخزين)⁴⁸.

ثانيا: مخبر الفيديو: يختص مخبر الفيديو بمقارنة الأوجه وشرعية الصورة والفيديو وإعادة بناء مسرح الجريمة بالتشكيل ثلاثي الأبعاد وتحسين نوعية الصورة (فيديو - صورة) بمختلف التقنيات. ومن تجهيزاته: جهاز فيديو بوكس وحوامل الفيديو الرقمية والممغنطة وحبكات إعلامية (كونيتك ستوديو، ماكس ثلاثة أبعاد) وموزع لحفظ شرائح الفيديو. أما بالنسبة للقاعات يحتوي مخبر الفيديو على 4 قاعات (قاعتان للتحليل، قاعة التخزين وقاعة الموزع)⁴⁹.

ثالثا: مخبر الصوت

ومن مهامه التي يؤديها: تحسين نوعية إشارة الصوت بنزع التشويش وتعديل السرعة ومعرفة وتحديد المتكلم وتحديد شرعية التسجيلات الصوتية. ومن أجهزته: أجهزة الازدواجية والسماع وحبكات إعلامية، معالجة وتحسين التسجيلات الصوتية، نسخ الأقراص المضغوطة وأجهزة التصليح والتعبير.

أما بالنسبة للقاعات فإنه يحتوي على 5 قاعات: 3 قاعات للتحليل، قاعة تخزين وقاعة موزع⁵⁰.

4. المديرية العامة للأمن الوطني

تصدت هذه المديرية للجريمة الإلكترونية من مختلف الجوانب منها:

أولاً: الجانب القانوني: والمتمثل في النصوص القانونية كقانون 22-06 المؤرخ في 10 ديسمبر 2006، القانون 03-05، القانون المدني، القانون 04-09 المؤرخ في 5 أوت 2009 وقانون العقوبات في المواد من 394 مكرر إلى 394 مكرر⁷.

ثانياً: الجانب التنظيمي: ويتمثل في التكوين المتواصل والتخصيص والتكوين الأولي وتدعيم مخابر الشرطة العلمية، المصالح الولائية للشرطة القضائية وهيكله مصالح الشرطة القضائية للتصدي للجريمة.

ثالثاً: الجانب التوعوي: لم تغفل المديرية العامة للأمن الوطني عن الجانب الوقائي التوعوي يظهر ذلك من خلال برمجتها المديرية العامة لخطوات استباقية للتصدي للجريمة

الالكترونية للتصدي للجريمة الالكترونية عن طريق تنظيم دروس توعوية في مختلف الأطوار الدراسية وكذا المشاركة في الملتقيات والندوات الوطنية وجميع التظاهرات التي من شأنها توعية المواطن حول خطورة الجرائم الالكترونية.

أما في إطار سياسة الشرطة الجوية التي تنتجها قيادة المديرية، قام الأمن الوطني بفتح موقع الكتروني خاص بالشرطة الجزائرية على الانترنت يستطيع من خلاله أي مواطن مهما كان مستواه العلمي أو الاجتماعي طرح انشغاله والتبليغ عن أي شيء يثير الشبهة⁵¹

رابعاً: الجانب الدولي: في إطار مكافحة الجريمة الالكترونية ونظراً للبعد الدولي الذي عادة ما يتخذه هذا النوع من الجرائم، لم تغفل المديرية العامة للأمن الوطني استغلال عضويتها الفعالة في هاته الأخيرة تتيح مجالات للتبادل INTERPOL المنظمة الدولية للشرطة الجنائية المعلوماتي الدولي وتسهل الإجراءات القضائية المتعلقة بتسليم المجرمين، وكذا مباشرة الانابات القضائية الدولية ونشر أوامر القبض للمبحوث عنهم دولياً.

المحور السادس: الصعوبات التي تعترض مكافحة هذه الجريمة

- عملية تحصيل المعطيات خاصة المتعلقة بالارتباط لمزودي الخدمة تتطلب وقت كبير نظراً لتمرکزها بالجزائر العاصمة فقط.
- جهل الضحايا بالقانون، بمعنى أن الضحية لا يعتقد أنه يوجد أن هناك قانون يجرم تلك الأفعال فيعدلون عن التبليغ عن هاته الجرائم، كما لا تغفل طبيعة المجتمع الجزائري الذي يخشى نظرة المجتمع للضحية الذي يقع في مثل هاته الجرائم.
- صعوبة تحصيل الأدلة خاصة ما يتعلق منها بالجرائم التي ترتكب من الجزائر ومن طرف جزائريين ولكن أثارها خارج الوطن فتعتمد مصالح الأمن تحصيل الأدلة من محيط المشتبه فيه نظراً لصعوبة تحصيلها من موقع ظهور الجريمة بالخارج⁵².

الخاتمة :

بالنظر لحدثة هذا السلوك الإجرامي والذي يتجسد في الجريمة الإلكترونية، أوضحت هذه الدراسة النتائج الآتية:

أن الجريمة المعلوماتية لم تحظ بالدراسة والتحليل في الفقه الجنائي الا حديثا لذا فإنها لم تكن محلا لتنظيم تشريعي خاص إلا في بعض القوانين الغربية المقارنة وبهذه الصورة تتميز بخصوصية ذاتية من حيث صيغ هذه الحماية ومن حيث طبيعة الأحكام التي يجب أن تخضع لها واختلاف آثارها. ورغم تدارك المشرع الجزائري الفراغ القانوني في مجال الإجرام المعلوماتي وذلك بتجريم الاعتداءات الواردة على منتوجات الإعلام الآلي إلا أنه لم يستحدث نصا خاصا بالتزوير المعلوماتي. فقد عدل المشرع الجزائري قانون العقوبات في عام 2006 وذلك لازدياد الوعي بالخطورة هذا النوع المستحدث عن الإجرام باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى وشيوع ارتكابه ليس فقط من الطبقة المثقفة بل من قبل الجميع بمختلف الأعمار ومستويات التعليم نتيجة تبسيط وسائل التكنولوجيا المعلومات وانتشار الإنترنت كوسيلة لنقل المعلومات

أن الفكر القانوني المعاصر لم يستقر على رأي واحد يوضح تعريف الجريمة الإلكترونية او بيان خصائصها فضلا عن أن التشريعات المختلفة لا تحتو حاليا على نص يحدد مفهومها ويمكن الرجوع اليه وعليه فهي أفكار لا حدود لها وتستلزم تنظيما قانونيا خاصا بها.

أن الاجرام المعلوماتي الذي يقع عن طريق الشبكة العالمية (الانترنت) له طبيعة من نوع خاص على خلاف الجرائم الاخرى التقليدية وقد تستمد هذه الطبيعة الخاصة من المجال الذي يمكن أن ترتكب فيه أو من المحل الذي يقع عليه الاعتداء.

في ضوء النتائج السابقة التي أظهرتها الدراسة تخلص إلى بعض التوصيات والاقتراحات تتمثل في:

- ضرورة إعطاء تعريف موحد وشامل للجريمة الإلكترونية، يشمل فيه كل السلوكيات المجرمة.

- ضرورة تدريب وتأهيل أفراد الضبطية القضائية وكذا النيابة العامة على كيفية التعامل مع هذا النوع من الجرائم وتحقيق التعاون مع التقنيين من أصحاب الخبرة.
- وضع إجراءات كالتحقيق والمحاكمة للجريمة الإلكترونية تختلف عن الجريمة التقليدية.
- توعية المجتمع وخلق ثقافة اجتماعية جديدة عن هذه الجرائم بأنها أعمال غير مشروعة ويتعرض صاحبها لعقوبات جزائية.
- تدريس مواد الأنظمة المعلوماتية والجرائم التي قد تنشأ عنها في المدارس، بشكل مبسط، وفي الكليات الحقوق والمعاهد القضائية.

الهوامش :

- ¹ زبيخة زيدان: الجريمة المعلوماتية في التشريع الجزائري و الدولي ، دار الهدى ، عين مليلة ، الجزائر، 2011 ، ص 42.
- ² R. C van der Hulst, R. J. M Neve: *High-tech crime, soorten criminaliteit en hun daders : Een literatuurinventarisatie*, Boom juridische uitgevers, Den Haag, Netherlands, 2008,p18.
- ³ خالد ممدوح إبراهيم: أمن الجريمة الإلكترونية، دار الجامعية، الإسكندرية، مصر، 2008، ص 43.
- ⁴ محمد العريان: الجرائم المعلوماتية، كلية الحقوق جامعة الإسكندرية، دار الجامعة الجديد للنشر، الإسكندرية، مصر، 2004، ص 43.
- ⁵ نهلا عبد القادر المومني: الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2008، ص 49.
- ⁶ نهلا عبد القادر المومني ، المرجع السابق ، ص 49 .
- ⁷ أمير فرج يوسف: الجرائم المعلوماتية على شبكة الأنترنت، دار المطبوعات الجامعية، الإسكندرية، مصر، 2009، ص 106، 107.
- ⁸ نهلا عبد القادر المومني، المرجع السابق، ص 48.
- ⁹ سامي على حامد عياد: الجريمة المعلوماتية وإجرام الأنترنت، دار الفكر الجامعي، الإسكندرية، مصر، 2008، ص 38، 40.
- ¹⁰ محمد علي العريان ، المرجع السابق ، ص 45 .
- ¹¹ نشناش منية: مداخل حول الركن المفترض في الجريمة المعلوماتية ، جامعة بسكرة، الجزائر، 2015-2016، ص 3، 2.
- ¹² نشناش منية، المرجع السابق، ص 3.
- ¹³ قانون رقم 85 لسنة 2001 ، الجريدة الرسمية للمملكة الأردنية الهاشمية رقم 4524 الصادر بتاريخ 31 ديسمبر 2001، ص 6010.
- ¹⁴ قانون إمارة دبي رقم 02 لسنة 2002 متعلق بالمعاملات والتجارة الإلكترونية، صادر بتاريخ 12 فبراير 2002 .
- ¹⁵ نشناش منية، المرجع السابق ، ص 3 .
- ¹⁶ نشناش منية ، المرجع السابق ، ص 3 .
- ¹⁷ عمر محمد أبو بكر بن يونس: الجرائم الناشئة عن استخدام الأنترنت، دار النهضة العربية، القاهرة، مصر ، 2004، ص 6.
- ¹⁸ زبيخة زيدان: المرجع السابق، ص 43.
- ¹⁹ زبيخة زيدان: المرجع السابق، ص 44.
- ²⁰ المقدم عز الدين عز الدين : الاطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها ، ملتقى حول الجرائم المعلوماتية 16/ 11/ 2015، بسكرة، الجزائر، 2015.
- ²¹ قانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق لـ 16 أوت 2009 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 47، 2009.
- ²² نشناش منية: المرجع السابق، ص 4.
- ²³ قانون رقم 15-04 المؤرخ في 27 رمضان 1425 الموافق لـ 10 نوفمبر 2004 المعدل والمتمم للأمر 155-66 المتضمن قانون العقوبات، الجريدة الرسمية العدد 71، 2004.
- ²⁴ عائشة بن قارة مصطفى: حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن، دار الجامعة الجديدة، كلية الحقوق جامعة الإسكندرية، مصر، 2006، ص 27 .
- ²⁵ نشناش منية: المرجع السابق، ص 4 .
- ²⁶ نشناش منية: المرجع السابق، ص 4 .
- ²⁷ محمد زكي أبو عامر وعلي عبد القادر القهوجي: قانون العقوبات القسم الخاص، دار النهضة العربية القاهرة، مصر، 1993، ص 9.
- ²⁸ أحمد السمدان: النظام القانوني لحماية برامج الكمبيوتر، مجلة الحقوق، الكويت، 1987، ص 164.
- ²⁹ جميل عبد الباقي: الجوانب الإجرائية للجرائم المتعلقة بالأنترنت ، دار النهضة العربية ، القاهرة ، 2001 ، ص 92.

- ³⁰ طوبي ميشال عيسى: التنظيم القانوني لشبكة الإنترنت، دار صادر للمنشورات بيروت، 2000، ص383.
- ³¹ محمد علي سالم: الجريمة المعلوماتية، مجلة جامعة بابل للعلوم الإنسانية، المجلد 14، العدد 2، 2007، العراق، ص 91.
- ³² خالد ممدوح إبراهيم: أمن الجريمة الإلكترونية، دار الجامعة، الإسكندرية، مصر، 2008، ص82.
- ³³ معتوق عبد اللطيف: الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة مكملة لنيل شهادة الماجستير، 2011، 2012، ص 24.
- ³⁴ هشام محمد فريد: الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسبوط، 1994، ص82.
- ³⁵ معتوق عبد اللطيف: المرجع السابق، ص 15.
- ³⁶ معتوق عبد اللطيف: المرجع السابق، ص 15.
- ³⁷ معتوق عبد اللطيف: المرجع السابق، ص 15.
- ³⁸ جميل عبد الباقي الصغير: القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 1992، ص62.
- ³⁹ قانون 23-06 مؤرخ في 20 ديسمبر 2006 يعدل ويتمم الأمر 156-66 المؤرخ في 8 يونيو 1966 والمتضمن قانون العقوبات، الجريدة الرسمية العدد 84، 2006.
- ⁴⁰ مولود ديدان: قانون الإجراءات الجزائية، الأمر 02-11، دار بلقيس، الجزائر، ص 18، 22، 31، 32، 33.
- ⁴¹ قانون رقم 03-2000 المؤرخ في والذي 5 أوت 2000 يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، الجريدة الرسمية العدد 48، 2000.
- ⁴² قانون رقم 01-08 المؤرخ في 2 جاتفي 2008 والمتمم للقانون رقم 01-83 المتعلق بالتأمينات الاجتماعية، الجريدة الرسمية العدد 04، 2008.
- ⁴³ زبيحة زيدان: المرجع السابق، ص 77، 78.
- ⁴⁴ قانون 04-09 مؤرخ في 14 شعبان 1430 الموافق ل 5 أوت 2009 للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 47، 2009.
- ⁴⁵ سالم عبد الرزاق: ملتقى حول المنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية، بمحكمة سيدي محمد، ص 11.
- ⁴⁶ قانون رقم 22-06 مؤرخ في 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 155-66 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية العدد 84، 2006.
- ⁴⁷ هوارى عياش: مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، المعهد الوطني للأدلة الجنائية وعلم الإجرام، جامعة بسكرة كلية الحقوق، 2016، ص 3.
- ⁴⁸ سالم عبد الرزاق: المرجع السابق، ص 4.
- ⁴⁹ سالم عبد الرزاق: المرجع السابق، ص 7.
- ⁵⁰ سالم عبد الرزاق: المرجع السابق، ص 8.
- ⁵¹ حملاوي عبد الرحمان: مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية، جامعة محمد خيضر بسكرة كلية الحقوق، 2016، ص 5، 6.
- 52 حملاوي عبد الرحمان: المرجع السابق، ص 7.