

مكافحة الجريمة الالكترونية في التشريع الجزائري

الاستاذة بوعناد فاطمة زهرة

أستاذة مساعدة قسم "أ" كلية الحقوق والعلوم السياسية

جامعة الجيلالي ليابس - سيدي بلعباس

zladege@yahoo.frمقدمة:

يشهد العالم في الوقت الراهن تقدما هائلا تتجلى أبرز مظاهره في التكنولوجيا الجديدة للمعلومات والاتصالات، ولا شك أنّ هذه التكنولوجيا الحديثة تقدم للدول وأجهزتها الأمنية الكثير من الإمكانيات التي تسهم في رفع كفاءتها وتطوير قدرتها على التصدي للجريمة، إلا أنّ هذا التطور التكنولوجي أدى ويؤدي في الوقت نفسه إلى تطوير وتحديث الجريمة من حيث الأساليب والمضامين، فكل الوسائل التقنية الحديثة تثير مسألة الحماية القانونية لها. فظهور المعلوماتية أدى إلى بروز مشاكل قانونية جديدة، أي ظهور ما يسمى بأزمة القانون الجنائي، ولما كان القاضي الجنائي مقيدا بمبدأ شرعية الجرائم، فإنه لن يستطيع أن يجرّم أفعالا لم ينص عليها المشرع، حتى ولو كانت أفعالا مستهجنة، ومهما بالغ المشرع في الحماية الموضوعية للمصالح الاجتماعية في قانون العقوبات، فإنّ نجاحه يظلّ مرتهنا بمدى فاعلية التنظيم الإجرائي الذي يضمن تحقيق الهدف من العقاب.

أما بالنسبة للإشكالية الأساسية تتمحور حول إبراز المشاكل القانونية التي أفرزتها ظهور المعلوماتية وتطبيقاتها المتعددة في نطاق القانون الجنائي، وكذلك انعكاساتها على طبيعة الإجراءات الخاصة بملاحقة هؤلاء الجناة.

وتتطلب الحماية القانونية ضرورة اتخاذ آليات مواجهة في كافة الجوانب سواء تمثلت هذه الآليات في إصدار نصوص تشريعية لتجريم هذه الأفعال، أو من خلال الجهود الأمنية التي تباشر أجهزة إنفاذ القانون وهذا ما سنتطرق إليه في مبحثين على التوالي.

المبحث الأول: الحماية الموضوعية لمعطيات الحاسب الآلي.

كان على المشرع الجزائري وجوب إستحداث نظم قانونية جديدة لمواجهة التحديات التكنولوجية المعاصرة نظرا لعدم مواكبة هذه الأفعال للتشريعات التقليدية.

وسيتم التطرق من خلال هاللبحث للحماية التي كفلها المشرع الجزائري لمعطيات الحاسب الآلي من خلال قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها، وكذلك من خلال نصوص المعالجة الآلية للمعطيات وأيضا من خلال نصوص الملكية الفكرية، وقانون التوقيع الإلكتروني لسنة 2007 بالإضافة إلى القانون رقم (03-2000) الذي يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية.

المطلب الأول: الحماية في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها.

إنّ تفاقم الإعتداءات على معطيات الحاسب الآلي خاصة مع ضعف الحماية الفنية، استدعى تدخلا تشريعا صريحا، فقد استدرك المشرع الجزائري الفراغ القانوني من خلال هذا القانون¹، حيث أجاز المشرع مراقبة الإتصالات الإلكترونية² غير أنّه حدّد الحالات التي يسمح فيها بالهجوم إلى المراقبة الإلكترونية³ مع اشتراط الحصول على إذن مكتوب من السلطة القضائية المختصة، كما جاء في القانون جواز التفتيش ولو عن بعد⁴، بالإضافة إلى الإجراء المترتب عن التفتيش وهو الحجز⁵ وسيتم التطرق إلى هذه الإجراءات بنوع من التفصيل في المبحث الثاني المتعلق بالحماية الإجرائية.

المطلب الثاني: الحماية في قانون العقوبات.

قام المشرع الجزائري بتعديل قانون العقوبات، هذا التعديل الذي تمّم الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر رقم (156/66) المتضمن قانون العقوبات الجزائري بقسم سابع مكرّر عنوانه "المساس بأنظمة المعالجة الآلية للمعطيات"، ويشمل المواد من (394 مكرّر) إلى (394 مكرّر 7).

فمن خلال استقراء نصوص هذه المواد، يتبين أنّ المشرع الجزائري حاول حصر هذه الجرائم فيما يلي:
1. الحول منظومة معلوماتية عن طريق الغش: وفرّق المشرع في هذه الحالة بين ما إذا كانت الجريمة بسيطة أو ترتب على ذلك حذف أو تغيير لمعطيات المنظومة، وبين ما إذا ترتب على ذلك تخريب لنظام اشتغال المنظومة⁶.

2. الاعتداء العمدي على المعطيات: فالمشرع لم ينص على الإعتداء العمدي على سير نظام المعالجة الآلية للمعطيات، وإنما نص على الإعتداء العمدي على المعطيات⁷.

3. جرائم المعالجة الآلية للمعطيات الماسة بالدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام⁸.

4. جرائم الشخص المعنوي: تجدر الإشارة إلى أن مبدأ مسؤولية الشخص المعنوي لا ينفي مسؤولية الأشخاص الطبيعية في نفس الجريمة⁹.
5. المشاركة في مجموعة أو اتفاق بغرض الإعداد لجريمة أو أكثر من الجرائم الماسة بالأنظمة المعلوماتية: إنَّ الحكمة من هذا التجريم هو توسيع نطاق العقوبة وذلك بإخضاع الأعمال التحضيرية التي سبق البدء في التنفيذ للعقوبة إذا تمت في إطار اتفاق جنائي.
6. المشروع في الجريمة: أي أنَّ المشرِّع جعل المشروع في إحدى الجرائم الماسة بالأنظمة المعلوماتية معاقب عليه بنفس عقوبة الجريمة التامة.
- كما نص المشرِّع في هذا القانون على العقوبات التكميلية¹⁰.
- ومن خلال استقراء النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية يتبين وجود تدرج داخل النظام العقابي، هذا التدرج يحدّد الخطورة الإجرامية التي قدرَّها المشرِّع لهذه التصرفات.

المطلب الثالث: الحماية في قوانين خاصة.

وهذه القوانين الخاصة شملت الحماية في قانون التأمينات الإجتماعية، وكذلك الحماية من خلال نصوص الملكية الفكرية، وأيضاً الحماية في نصوص التوقيع الإلكتروني بالإضافة إلى الحماية المتعلقة بالمواصلات السلوكية واللاسلكية.

الفرع الأول: الحماية في قانون التأمينات الإجتماعية.

وما ينبغي الإشارة إليه إلى أنَّ المشرِّع الجزائري بمقتضى أحكام قانون التأمينات الإجتماعية الجديد لسنة 2008¹¹، شدّد العقوبة فيما يتعلق بالمساس الغير المشروع للبطاقة الإلكترونية للمؤمن له إجتماعياً.

وقد عاقب المشرِّع الجزائري، كلَّ من يسلم أو يستلم بهدف الإستعمال غير المشروع للبطاقة الإلكترونية للمؤمن له إجتماعياً، أو المفتاح الإلكتروني لهيكل العلاج أو المفتاح الإلكتروني لمهنيي الصحة¹²، كما يشمل العقاب أيضاً التعديل أو الحذف الكلي أو الجزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية¹³.

وقد أقرَّ المشرِّع أيضاً عقوبة للشخص المعنوي تتمثل في غرامة تساوي خمس مرات المبلغ الأقصى للغرامة المقرّرة للشخص الطبيعي¹⁴، كما يحكم بمصادرة الأجهزة والوسائل المستعملة وكذا غلق المحلات وأماكن الإستغلال التي تكون محل الجنح.

الفرع الثاني: الحماية في نصوص الملكية الفكرية.

تقسم حقوق الملكية الفكرية إلى قسمين: أحدهما حقوق الملكية الصناعية، والثاني هو الحقوق الأدبية والفنية.

أولاً: خضوع معطيات الحاسب الآلي لنصوص الملكية الصناعية.

ترمز حقوق الملكية الصناعية إلى المبتكرات الجديدة كالاختراعات، وقد نضمها المشرع بقانون شهادات المخترعين وبراءات الاختراع.

ويرى القائلون بالحماية لقوانين براءة الاختراع أن برامج الحاسوب ولأنهم تستعمل للتعامل مع آلات الحاسوب وإدارتها، فهي بذلك تصبح جزءاً منها ولمّا كانت البرامج تتضمن استخدامات جديدة لأفكار أو مبادئ علمية لتشغيل الحاسب، فهي من هذه الزاوية تصبح قابلة للبراءة¹⁵.

غير أنه من الصعب توفير حماية ناجعة للمعطيات بالرجوع إلى قانون الملكية الصناعية، ويتعلق الأمر بتوافر شرطين هما: شرط الجدّة والقابلية للاستغلال الصناعي، فهذان الشرطان تتفق حولهما التشريعات المقارنة مع التشريع الجزائري، فيما يضيف هذا الأخير شرطاً آخر وهو أن يكون الاختراع نشاطاً خلافاً.

وتجدر الإشارة أنه يمكن استثناء الحصول على براءة الاختراع بخصوص برامج الإعلام الآلي في حالتين هما:

1. أن يكون البرنامج جزءاً من ذاكرة الحاسب نفسه مثال ذلك: البرنامج المبني.
2. أن يكون البرنامج جزءاً، أي أن طلب البراءة ينصب على وسيلة صناعية جديدة يستخدم البرنامج في تحقيق إحدى مراحلها، فالحماية تبقى رهينة توفر الشرطين المذكورين وقد ثبت صعوبة توفرها، وبالنتيجة ثبت تعذر الحماية¹⁶.

والمشرع الجزائري استبعد صراحة المعطيات من مجال الحماية بواسطة براءات الاختراع¹⁷.

ثانياً: خضوع معطيات الحاسب الآلي لنصوص الملكية الأدبية والفنية.

إنّ المشرع الجزائري لم ينص صراحة على حماية مصنّفات الحاسب الآلي من خلال حق المؤلف، إلاّ أنّ بعض المختصين يرون إمكانية الحماية بدليل الصياغة المرنة عند ذكر المصنّفات المشمولة بالحماية. من استقرء الأمر (10/97) المعدل والمتمم بالأمر (05/03) المتعلق بحق المؤلف والحقوق المجاورة يستخلص ما يلي:

1. أنّ المشرع وسع قائمة المؤلفات المحمية حيث أدمج تطبيقات الإعلام الآلي ضمن المصنّفات الأصلية والتي عبر عنها بمصنّفات قواعد البيانات وبرامج الإعلام الآلي.
2. تشديد العقوبات الناجمة عن المساس بحقوق المؤلفين لاسيما المصنّفات المعلوماتية¹⁸.

الفرع الثالث: الحماية في نصوص التوقيع الإلكتروني.

إنّ المشرع الجزائري من خلال المرسوم التنفيذي رقم (162/07) المؤرخ في 30 مايو 2007¹⁹، لم يكفل الحماية الشاملة للتوقيع الإلكتروني وإنّما جاء هذا المرسوم متضمناً لتعريفات فقط.

وقد عرف المشرع التوقيع الإلكتروني بأنه معطى ينجم عن استخدام أسلوب عمل يستجيب للشروط المحددة في المادتين (323 مكرر و323 مكرر1)²⁰.

كما عرف مؤدي خدمات التصديق الإلكتروني وتطرق للشهادات التي يسلمها هذا الأخير المقيم في بلد أجنبي واعترف لها بنفس قيمة الشهادات المسلمة بموجب أحكام هذا المرسوم²¹.

الفرع الرابع: الحماية المتعلقة بالمواصلات السلوكية واللاسلكية.

إن القانون رقم (2000-03) المتعلق بالبريد والمواصلات السلوكية واللاسلكية²² يحدد مفهوم المواصلات السلوكية واللاسلكية²³.

ولقد تضمن الفصل الثاني من الباب الرابع من هذا القانون الأحكام الجزائية المترتبة في حالة مخالفة النظام القانوني، فالأشخاص المرخص لهم بتقديم خدمة المواصلات السلوكية واللاسلكية والعمّال لدى متعاملي الشبكات العمومية الذين ينتهكون سرية المراسلات الصادرة أو المرسلّة أو المستقبلّة عن طريق المواصلات السلوكية واللاسلكية أو الذين يأمرّون أو يساعدون في ارتكاب هذه الأفعال فيعاقبون طبقاً لما يقضي به نص المادة (137) من قانون العقوبات. وما عدا هؤلاء الأشخاص المذكورين فكل شخص يرتكب هذه الأفعال يعاقب بالحبس والغرامة²⁴.

كما أنّ نفس العقوبات المنصوص عليها في المادة (137) من قانون العقوبات تطبق على من ينتهك مضمون المراسلات المرسلّة عن طريق اللاسلكي الكهربائي أو يخبر بوجودها دون ترخيص²⁵.

المبحث الثاني: الحماية الإجرائية لمعطيات الحاسب الآلي.

تبدأ المشكلات الإجرائية بتعلّقها في كثير من الأحيان بمعطيات معالجة إلكترونية وكيانات منطقية غير مادية، وبالتالي يصعب كشف هذه الجرائم ويستحيل أحياناً جمع الأدلة بشأنها.

المطلب الأول: الإجراءات العامة لحماية معطيات الحاسب الآلي.

لقد ارتأينا تقسيم الإجراءات العامة إلى إجراءات مادية وأخرى شخصية وذلك على النحو التالي:

الفرع الأول: الإجراءات المادية.

أولاً: المعاينة.

عرف جانب من الفقه المعاينة بأنها "رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة"، والأصل في المعاينة أنّها إجراء من إجراءات التحقيق²⁷.

وينبغي التعامل مع مسرح الجريمة الإلكترونية على أنه مسرحان هما:

1. **مسرح تقليدي:** ويقع خارج بيئة الحاسوب والانترنت، ويتكون من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة وهو أقرب ما يكون إلى مسرح أية جريمة تقليدية، يترك فيها الجاني آثار كالبصمات، أو وسائط تخزين رقمية.

2. **مسرح افتراضي:** ويقع داخل البيئة الإلكترونية، ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب، في ذاكرة الأقراص الصلبة الموجودة بداخله²⁸.

ومن الإجراءات التي يتم اتباعها عند إجراء المعاينة ما يلي:

- القيام بتصوير جهاز الحاسب الآلي وما قد يتصل به من أجهزة طرفية ومحتوياته.
- عدم التسرع في نقل أي مادة معلوماتية للتيقن من عدم وجود أي مجالات مغناطيسية في العالم الخارجي.
- القيام بحذف المستندات الخاصة بالإدخال وكذلك مخرجات الحاسوب الورقية.
- ربط الأقراص الكمبيوترية التي ربما تحمل أدلة مع جهاز يمنع الكتابة عليها مما يتيح للمحققين قراءة بياناتها من دون تغييرها²⁹.

ثانيا: **التفتيش في البيئة الإلكترونية.**

التفتيش إجراء من إجراءات التحقيق يستهدف البحث عن الحقيقة في مستودع السر، لذلك يعتبر من أهم إجراءات التحقيق لأنه غالبا ما يسفر عن أدلة مادية تؤيد نسبة الجريمة للمتهم.

- **مدى قابلية مكونات وشبكات الحاسوب للتفتيش:**

تتكون نظم الحاسوب من مكونات مادية ومكونات منطقية.

1- **تفتيش مكونات الحاسوب المادية:**

الواقع أن تفتيش المكونات المادية للحاسوب بحثا عن شيء يتصل بجريمة إلكترونية وقعت، ويفيد في كشف حقيقة عنها وعن مرتكبيها، يدخل في نطاق التفتيش طالما تمّ وفقا للإجراءات القانونية المقررة، بمعنى أن حكم تلك المكونات يتوقف على طبيعة المكان الموجودة فيه، سواء من الأماكن العامة أو الأماكن الخاصة³⁰.

2- **مدى خضوع مكونات الحاسوب المعنوية للتفتيش:**

لقد ثار خلاف تشريعي وفقهي بشأن مدى جواز تفتيش المكونات المعنوية للحاسوب تمهيدا لضبط الأدلة

الإلكترونية.

فذهب الرأي الأول إلى جواز تفتيش نظم الحاسوب لتشمل المكونات المادية وغير المادية، وعلى النقيض من

ذلك هناك رأي آخر يرى أنه إذا كانت الغاية من التفتيش كشف الحقيقة فإنّ هذا المفهوم المادي لا ينطبق على الجرائم

الإلكترونية وقد جرّم المشرّع الجزائري أفعال المساس بأنظمة المعالجة الآلية للمعطيات³¹.

3- **مدى خضوع شبكات الحاسوب للتفتيش "التفتيش عن بعد":**

في هذه الصورة يمكن التفرقة بين الفرضين التاليين:

الفرض الأول: اتصال حاسب المتهم بحاسب موجود في مكان آخر داخل الدولة.

لقد أجاز المشرع الجزائري بموجب قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال التفتيش، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى فيجوز تمديد التفتيش بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

الفرض الثاني: اتصال حاسب المتهم بحاسب موجود في مكان آخر خارج الدولة.

من المشاكل التي تواجه سلطات التحقيق قيام مرتكبي الجريمة بتخزين بياناتهم في أنظمة تقنية خارج الدولة، غير أن المشرع بموجب القانون السالف الذكر نص على ضرورة المساعدة من قبل السلطات الأجنبية المختصة وفقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

ثالثا: الضبط

يختلف الضبط في الجريمة الالكترونية عن الضبط في غير ذلك من الجرائم من حيث المحل وذلك بسبب أن الأول يرد على أشياء ذات طبيعة معنوية وفي البيانات، المراسلات والاتصالات الالكترونية، أما الثاني فيرد على أشياء مادية.

وتجدر الإشارة إلى أن الضبط قد يرد على عناصر معلوماتية منفصلة مثل الاسطوانات المغنطة، وهنا لا تشور أي مشكلة قانونية عند القيام بالضبط، ولكن الصعوبة تثار عندما يلزم ضبط النظام كله أو الشبكة كلها، ذلك لأنها تحتوي على عناصر لا يمكن فصلها ومع ذلك يتعين ضبطها لأنها تتضمن عناصر مهمة للإثبات.

أما بالنسبة للمكونات المادية للحاسوب فلا يثير ضبطها أي مشكلات، فيمكن ضبط الوحدات المعلوماتية الآتية: وحدة المدخلات بما تشمله من مفردات كلوحة المفاتيح، نظام الفأرة، نظام القلم الضوئي، وضبط وحدة المخرجات وما تشمل عليه من وسائل كالشاشة، الطابعة، الرسم والمصغرات الفيلمية.

والمعروف أن ما يتم ضبطه من بيانات الكترونية يتعين تحريزها وتأمينها فنيا خاصة أمام غياب الثقافة المعلوماتية عن المحقق الجنائي مما يجعل تلك الأدلة عرضة للإتلاف والإفساد³².

الفرع الثاني: الإجراءات الشخصية.

أولا: التسرب.

استحدث المشرع الجزائري في مجال مكافحته جرائم المساس بأنظمة الحاسب الآلي عدة إجراءات ويرجع ذلك لعجز الأساليب التقليدية.

ولقد أدرج المشرع عملية التسرب بموجب القانون رقم (06-22) المؤرخ في ديسمبر 2006 المتضمن قانون الإجراءات الجزائية، والذي أفرد الفصل الخامس منه تحت عنوان: "في التسرب" والذي تضمن 8 مواد (من المواد 65 مكرر 11 حتى المادة 65 مكرر 18). وتناول من خلالها تحديد مفهوم هذه العملية، وشروط إجرائها، العمليات المبررة، وأخيرا الحماية الجنائية للقائم بعملية التسرب.

1. مفهوم عملية التسرب :

قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك. ويمكن تجسيد عملية التسرب في الجرائم الالكترونية كاشتراك ضابط أو عون الشرطة في محادثات غرف الدردشة أو حلقات النقاش حول دعارة الأطفال، أو كلام يدور حول قيام أحدهم باختراق شبكات أو بث فيروسات، فيتخذ المتسرب أسماء مستعارة ويحاول الاستفادة حول كيفية اقتحام الهاكر لموقع ما حتى يتمكنوا من اكتشاف وضبط الجرائم³³.

2. شروط صحة عملية التسرب:

- أ. صدور إذن من وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية.
- ب. أن يكون الإذن مكتوبا ومسببا.
- ج. يذكر في الإذن، الجريمة التي تبرر اللجوء إلى هذا الإجراء، وهوية ضابط الشرطة.
- ح. يحدد مدة عملية التسرب التي لا يمكن أن تتجاوز 4 أشهر، غير أنه يمكن أن تجدد .

ثانيا: الشهادة في الجريمة الالكترونية.

الشاهد في الجريمة الالكترونية هو الفني صاحب الخبرة والتخصص في تقنية الحاسب وشبكات الاتصال الذي تكون لديه معلومات جوهرية لولوج نظام المعالجة الآلية للمعطيات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله³⁴.

وتجدر الإشارة أنه نتيجة قصور أحكام الشهادة في الحصول على الدليل الالكتروني يرى بعض الفقهاء ضرورة البحث عن وسيلة قانونية جديدة ما لم تستطع فكرة الالتزام بالشهادة أن تؤديه، وهذه الوسيلة هي "الالتزام بالإعلام في الجريمة المعلوماتية". وذلك من خلال النص الصريح في القانون الذي يفرض عليه واجبا بتقديم أية معلومات ضرورية ولازمة من أجل إعانة سلطات التحقيق والاستدلال في الحصول على أدلة إثبات عن الجريمة الالكترونية الواقعة، كما أن فرض مثل هذا الالتزام من شأنه أن يلعب دورا وقائيا في حفظ النظام المعلوماتي.

ثالثا: الخبرة التقنية

الخبرة القضائية عموما هي الاستشارة الفنية التي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقديرها إلى معرفة أو دراية علمية خاصة لا تتوفر لديه فهي وسيلة من وسائل الإثبات التي

تهدف إلى كشف بعض الدلائل أو الأدلة أو تحديد مدلولها بالاستعانة بالمعلومات العلمية والفنية والتي لا تتوفر سواء لدى المحقق أو القاضي.

غير أنه قد تواجه سلطات الاستدلال والتحقيق بعض المشاكل الفنية والتقنية والتي تستلزم معالجتها بالاستعانة بخبير معلوماتي ذو تخصص خاص ودقيق، وقد لا تتوفر مثل هذه النوعية من الخبرة في من يحملون جنسية الدولة، وهنا يثور التساؤل عن مدى إمكانية الاستعانة بخبير معلوماتي؟ لقد اختلفت الدول في معالجتها لهذه المسألة، فبعض الدول تجد في الاستعانة بالخبير الأجنبي مصدر تهديد وخطر على سيادتها وأمنها، ويلاحظ أن المشرع المصري قد اشترك صراحة أن يكون الشخص متمتعاً بالجنسية الوطنية لكي يكون بمقدوره تسجيل اسمه في جدول الخبراء، فيما لم يأخذ المشرع الفرنسي بهذا الشرط، من ثم فإن ذلك يدل على إجازته لانتداب خبير معلوماتي أجنبي³⁵.

المطلب الثاني: الإجراءات الخاصة لحماية معطيات الحاسب الآلي.

من الضروري أن تواكب التشريعات هذا التطور الملحوظ وذلك من خلال خلق قواعد قانونية إجرائية غير تقليدية.

الفرع الأول: الإجراءات المتعلقة بالبيانات الساكنة.

إن الإجراءات الخاصة بالبيانات الساكنة كلها مستقاة من اتفاقية بودابست³⁶ وهي أولى المعاهدات التي تكافح تلك الجرائم الالكترونية .

وتتمثل الإجراءات المتعلقة بالبيانات الساكنة فيما يلي:

أولاً: التحفظ المعجل على البيانات المخزنة:

إن هذا الإجراء يعد للجزائر سلطة قانونية جديدة، فهو أداة تحقيق مستحدثة ويقصد به توجيه السلطة المختصة لمزودي الخدمات الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزتها وتحت سيطرته في انتظار اتخاذ إجراءات قانونية أخرى كالتفتيش أو الأمر بتقديم بيانات معلوماتية³⁷.

ويتضح أن التحفظ العاجل هو إجراء أولي تمهيدي الهدف منه هو محاولة الاحتفاظ بالبيانات قبل فقدانها.

ثانياً: الأمر بتقديم بيانات معلوماتية متعلقة بالمشارك.

الأصل أن البيانات الشخصية المتعلقة بمستخدمي الشبكة تدخل في إطار الحق في الخصوصية، غير أنه يسمح لرجال الضبط القضائي أن يأمروا الأشخاص بتسليم ما تحت أيديهم من موضوعات والتي يطلب تقديمها كدليل، ومن بينها البيانات المتعلقة بالمشارك التي يجوزها مزودوا الخدمات³⁸.

الفرع الثاني: اعتراض المراسلات الإلكترونية.

يقصد بهذا الإجراء مراقبة الإتصالات الإلكترونية أثناء بثّها وليس الحصول على اتصالات إلكترونية مخزنة. وقد استحدثت المشرّع الجزائري هذا الأمر عن طريق قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال، مراقبة الإتصالات الإلكترونية، غير أنّه حدد الحالات التي يسمح فيها باللجوء إلى المراقبة الإلكترونية كالأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، أو في حالة توفر معلومات عن احتمال إعتداء على منظومة معلوماتية على نحو يهدّد النظام العام أو مؤسسات الدولة أو في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة³⁹.

وتترتب على المراقبة السرية للاتصالات عموما ومن ضمنها الاتصالات الالكترونية في الغالب، تسجيل محتوى تلك الاتصالات وتخزينها على وسائط مادية قابلة للنقل، بغية استخدامها فيما بعد لإثبات الجريمة الواقعة، ولطكن تختلف نوعية التسجيل هنا بحسب ما إذا كانت المحادثة الالكترونية المراقبة هي عبارة عن اتصال صوتي فقط، أو أنّها اتصال صوتي مرئي، ففي الأول يكون التسجيل صوتي فقط، في حين أنه يكون في الثاني تسجيل صوتي مرئي. وما ينبغي الإشارة إليه أن المراقبة السرية للاتصالات الالكترونية، ومن ضمنها المحادثات الهاتفية، لا يمكن اعتبارها نوعا من أنواع التفتيش، وذلك لأن المراقبة الالكترونية ترد عن البيانات الالكترونية المتحركة والتي تتجسد هنا بالاتصالات الالكترونية حال إجرائها، دون تلك التي انتهت وخزنت، في حين التفتيش إنما يرد فقط على البيانات الالكترونية الساكنة أو المخزنة والتي تتجسد هنا بالاتصالات الالكترونية التي تمت وخزنت⁴⁰.

خاتمة:

تعتبر جرائم الحاسب الآلي جرائم حديثة، غيرت في النظرية التقليدية للجريمة بوجه عام، بما تتصف به من امتداد عبر الدول، فهذه الطبيعة الخاصة، أوجدت في الواقع الكثير من المشاكل العملية في التحقيق والإثبات، منها مشاكل تتعلق بجمع الأدلة، ومشاكل تتعلق بالقانون، وقد انتهينا من هذا البحث على ضرورة التأكيد على بعض النقاط من خلال عدة توصيات:

1. ضرورة وضع تشريع جزائري يتسق مع الأحكام القانونية الدولية في مجال مواجهة هذه الجرائم، وتنظيم الأحكام الإجرائية الخاصة بمواجهة هذه الجرائم.
2. إعداد برنامج أمن المعلومات من خلال إعداد خطط التدريب المختلفة مع تعيين المتخصصين في كل جهة لتتولى مسؤولية الأمن المعلوماتي.
3. وضع ضوابط لمقاهي الانترنت وحصر المترددين عليها وعمل قاعدة بيانات لهم حتى يسهل متابعتهم.
4. منح سلطات التحقيق الصلاحية القانونية والتدريب العملي اللازم لاختراق نظام الحاسوب وضبط ما يحتويه من بيانات مخزنة.

5. ضرورة التعاون الدولي لمواجهة مشاكل صور السلوك المنحرف المتمثل في جرائم الكمبيوتر والانترنت، وذلك بعقد المزيد من الإتفاقيات الثنائية والجماعية.

الهوامش:

- ¹ قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق ل 5 غشت سنة 2009، يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- ² المادة 03 من القانون السالف الذكر.
- ³ المادة 04 من القانون السالف الذكر.
- ⁴ المادة 05 من القانون السالف الذكر.
- ⁵ المادة 06 من القانون السالف الذكر.
- ⁶ المادة (394 مكرر) من القانون (15/04) المتضمن قانون العقوبات الجزائري.
- ⁷ المادة (394 مكرر 2) من القانون السالف الذكر.
- ⁸ المادة (394 مكرر 3) من القانون السالف الذكر.
- ⁹ المادة (394 مكرر 4) من القانون السالف الذكر.
- ¹⁰ المادة (394 مكرر 6) من القانون السالف الذكر.
- ¹¹ قانون رقم 1/08 المؤرخ في 23 يناير سنة 2008، يتمم القانون رقم 11/83 المؤرخ في 2 يوليو سنة 1983 والمتعلق بالتأمينات الاجتماعية.
- ¹² المادة 93 مكرر 2 من القانون المذكور.

- 13 المادة 93 مكرر 3 من القانون المذكور.
- 14 المادة 93 مكرر 5 من القانون المذكور.
- 15 د. عبد الفتاح بيومي حجازي، مقدمة في حقوق الملكية الفكرية وحماية المستهلك في عقود التجارة الإلكترونية، دار الفكر (الإسكندرية)، سنة 2005، ص 14.
- 16 د. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، دار الثقافة للطباعة والنشر، القاهرة، سنة 1999، ص 45.
- 17 أ. أمال قارة، الحماية الجزائرية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، ط1، سنة 2006، ص 15.
- 18 أ. محمد الألفي، تأملات حول التصدي للجرائم المعلوماتية، بتاريخ 3 تشرين الأول 2007، ص 1 على الموقع: www.arabalawinfo.com
- 19 المرسوم التنفيذي رقم (07-162) مؤرخ في 30 مايو 2007 يعدّل ويتمم المرسوم التنفيذي رقم (01-123) المؤرخ في 09 مايو 2001 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية.
- 20 المادة رقم 323 مكرر والمادة 323 مكرر 1 من القانون (05-10) المتضمن القانون المدني.
- 21 المادة (3 مكرر ف 2) من المرسوم التنفيذي السالف الذكر.
- 22 القانون رقم (03-2000) مؤرخ في 5 غشت 2000 يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية.
- 23 المادة (8 ف 21) من القانون السالف الذكر.
- 24 المادة (127 ف 03) من القانون السالف الذكر.
- 25 المادة 130 من ذات القانون.
- 26 د. جميل عبد الباقي الصغير، الجوانب الإجرائية للانترنت، دار الفكر العربي، القاهرة، 2001، ص 27.
- 27 المادة 79 من قانون الإجراءات الجزائية الجزائري.
- 28 د. جميل عبد الباقي الصغير، المرجع السابق، ص 28.
- 29 أ. عائشة بن قارة، حجية الدليل الإلكتروني، دار الجامعة الجديدة، الأزاريطة، سنة 2010، ص 80.
- 30 أ. عائشة بن قارة، المرجع السابق، ص 91.
- 31 القانون رقم (04-15) المؤرخ في 10 نوفمبر سنة 2004 المتضمن قانون العقوبات الجزائري.
- 32 أ. عائشة بن قارة، المرجع السابق، ص 93.
- 33 د. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، سنة 2010، ص 191.
- 34 د. خالد ممدوح إبراهيم، المرجع السابق، ص 193.
- 35 أ. رشاد خالد عمر، المشاكل القانونية والفنية لتحقيق في الجرائم المعلوماتية (دراسة مقارنة)، المكتب الجامعي الحديث، الإسكندرية، سنة 2013، ص 123.
- 36 للإطلاع على النص الكامل لاتفاقية بودابست، مراجعة الموقع الخاص بالمجلس الأوروبي.
- 37 د. خالد ممدوح إبراهيم، المرجع السابق، ص 197.
- 38 أ. عائشة بن قارة، المرجع السابق، ص 158.
- 39 المادة 04 من القانون رقم 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- 40 أ. رشاد خالد عمر، المرجع السابق، ص 192.