ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2021 المجلد: الخامس العدد: الثاني ص.ص: 160-181

إساءة استخدام الأنترنت في القانون الجزائري

Misuse of the Internet in Algerian law

فاطمة الزهراء عكاكة*
جامعة عمار ثليجي - الأغواط
f. akaka@lagh-univ. dz

بهية بركات
جامعة عمار ثليجي - الأغواط
barkatbahia18@gmail. Com

تاريخ إرسال المقال: 2021/07/06. تاريخ قبول المقال: 2021/08/06 تاريخ نشر المقال01/09/2021

الملخص:

إن شبكة الأنترنت توفر طرقا حديثة للتواصل، لكنها توفر كذلك مجالا خصبا للجرائم الحديثة التي أصبحت تنخر المجتمع وتهدده في كيانه وفي كيان الأسرة بل ويتعداه إلى تهديد كيان الدول وتوتر العلاقات الدولية وتهديد أكبر الشركات الاقتصادية والتجارية العالمية بالإفلاس.

فتتعدد صور الأفعال المجرمة التي ترتكب بواسطة وسائل الأنترنت بحيث نجد الإختراق والدخول والبقاء بدون إذن وعدة أفعال أخرى تشكّل أركانا لجرائم معلوماتية الأمر الذي جعل التشريعات المختلفة ومنها المشرع الجزائري يسعون نحو ايجاد سياسة جزائية تسمح بردع المرتكبين والحد من توسع هذا النوع من الإجرام.

الكلمات المفتاحية: الإساءة، الجرائم، الأنترنت، الإختراق، القانون الجزائري.

Abstract:

Crime is an anti-social activity that has been known since the emergence of mankind, but it developed with its development, whether in the persons who committed it or in the method of its commission, so that criminals began to search for ways to develop means of committing crime by using the latest knowledge and adapting it to serve the crime.

The emergence of the computer and the innovations related to it that developed and expanded its uses, such as the information network and information systems, had a clear impact in the criminal field, so that the information system provided the opportunity to commit traditional crimes in unconventional ways, thus a new environment created for crime and criminal behavior was completely different. For the traditional environment.

*المؤلف المرسل.

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2021 المجلد: الخامس العدد: الثاني ص.ص: 160-181

An example of the topics raised by modern technologies is the issue of human rights and fundamental freedoms, which the technological stage allows its ill-intentioned users to violate and abuse.

It became imperative for the legal texts to be compatible with modern methods of committing the crime, which called for the legislator in the field of confronting electronic crime to issue special texts, whether in the field of criminalization or in the field of confrontation by means of criminal procedures, since the specificity of this technical crime requires, as well as legal expertise. The know-how to come up with proof.

Keywords: Abuse, crimes, internet, hacking, Algerian law.

المقدمة:

الجريمة نشاط معادي للمجتمع عرف منذ ظهور البشرية غير أنه تطوّر مع تطوّرها سواء في أشخاص مرتكبيها[1] أو في أسلوب ارتكابها، بحيث أصبح المجرمون يبحثون على طرق تطوير وسائل ارتكاب الجريمة باستعمال أحدث ما توصّل إليه العلم وتطويعه في خدمة الجريمة.[2]

فكان لظهور الحاسب الآلي[3] وما تلاه من مستحدثات متصلة به طوّرت من استعمالاته ووسعت رقعتها كالشبكة المعلوماتية ونظم المعلومات، الأثر الجلي في المجال الجنائي بحيث أصبح النظام المعلوماتي يتيح الفرصة لارتكاب الجرائم التقليدية بطرق غير تقليدية فظهرت بذلك بيئة جديدة مستحدثة للجريمة والسلوك الإجرامي مختلفة تمام الاختلاف عن البيئة التقليدية[4] و ذلك لمّا أصبح النظام المعلوماتي من ضروريات الحياة، غير أن كل تطور تقني له جانبه الإيجابي وجانبه السلبي، كما ينعكس هذا التطور التقني لا محالة على المستوى القانوني عامة وعلى القانون الجنائي على وجه خاص.

فكل الابتكارات تثير بعض المصالح والحقوق الجديرة بالحماية من الجانب الجزائي سواء في قانون العقوبات، باعتباره نص تقليدي، أو بسنّ قوانين ملائمة للوضع الجديد.

1) لا يعتبر المجرم في جرائم الحاسب الآلي والأنترنت مجرما عاديا بل هو من الخبراء في هذه التقنية أو النابغين فيها مهما كان سنّه، حجازي عبد الفتاح بيومي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي(دراسة قانونية معمقة في القانون المعلوماتي)، (د. ط)، دار الفكر الجامعي، الاسكندرية، مصر، 2006، ص 15.

2) الملط أحمد خليفة، الجرائم المعلوماتية (دراسة مقارنة)، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، مصر، 2006، ص 8.

3) يقصد به آلة الكترونية تستخدم وفق نظام معين لمعالجة وإدارة البيانات والمعلومات الرقمية المدخلة فيه وفق أوامر وتعليمات يختارها المشغل أو طالب الخدمة.

4) المناعسة أسامة أحمد، الزعبي جلال محمد، جرائم تقنية نظم المعلومات الالكترونية (دراسة مقارنة)، (د. ط)، دار الثقافة للنشر والتوزيع، 2014، ص15.

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2021 المجلد: الخامس العدد: الثاني ص.ص: 160-181

من أمثلة المواضيع التي تثيرها التقنيات الحديثة، موضوع حقوق الإنسان وحرياته الأساسية، التي بات الطور التكنولوجي يسمح لمستخدميها سيئ النية بخرقها والاعتداء عليها.

فبات لزاما على النصوص القانونية أن تتلاءم مع الأساليب الحديثة لارتكاب الجريمة مما دعى بالمشرع في مجال مواجهة الجريمة الالكترونية إلى إصدار نصوص خاصة سواء في مجال التجريم أو في مجال المواجهة بواسطة الإجراءات الجزائية، ذلك أن خصوصية هذه الجريمة التي تتسم بالفنية تستدعي، فضلا عن الدراية القانونية، دراية فنية للتوصل إلى إثباتها.

فالمشرع بوضعه النصوص يسعى إلى الحفاظ على التوازن بين مصلحة المجتمع في الاستفادة من التطور التكنولوجي والعلمي وبين حماية مصالحه وحقوقه.

من هذا المنطلق نطرح إشكالية هذا البحث التي تثير التساؤل التالي: **هل تواكب النصوص الحالية تطور الجريمة الناجمة عن سوء استخدام الانترنت ؟.**

في محاولة للإجابة على هذه الإشكالية إرتأينا تقسيم الموضوع إلى جزأين، الأول نتطرق من خلاله إلى الجوانب الموضوعية نستعرض فيه تركيبة الجريمة وأنواعها من أجل الوصول إلى معرفة مدى كفاية هذه النصوص أمام مواصلة التطور التكنولوجي. والجزء الثاني نضمّنه مختلف القواعد الإجرائية لإثبات هذه الجرائم. من هنا قسّمنا الموضوع إلى مبحثين وفق الخطة التالية:

- **المبحث الأول: مظاهر إساءة استخدام الانترنت في قانون العقوبات**
  - **المطلب الأول: تركيبة جريمة الأنترنت**
  - **المطلب الثاني: أنواع ومجالات جريمة الأنترنت**
- **المبحث الثاني: الإثبات الجنائي في جريمة الأنترنت**
  - **المطلب الأول: الدليل الإلكتروني**
  - **المطلب الثاني: مدى حجية الدليل الإلكتروني أمام القاضي الجزائي**
- **خاتمة تتضمن نتائج وتوصيات**

المبحث الأول: مظاهر إساءة استخدام الانترنت في قانون العقوبات

الإنترنت تلقب كذلك بشبكة المعلومات، الشبكة العالمية، الشبكة العنكبوتية وهي شبكة اتصالات عالمية تسمح بتبادل المعلومات بين شبكات أصغر تتصل من خلالها الحواسيب حول العالم. تعمل وفق

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2021 المجلد: الخامس العدد: الثاني ص.ص: 160-181

أنظمة محددة، وتشير كلمة «إنترنت» إلى جملة المعلومات المتداولة عبر الشبكة وأيضاً إلى البنية التحتية التي تنقل تلك المعلومات عبر القاراتأصبح استعمال الانترنت يعرف انتشارا واسعا بين الناس من مختلف الأعمار والأجناس بحيث لم يعد يخلو مكان عمومي أو خاص من هذه الخدمة التي ما بات يزيد من خطورتها توفرها بمقربة من الأفراد(على الهواتف الذكية مثلا).

ففضلا عن الإدمان الذي يحدثه استخدام الأنترنت والمشاكل الاجتماعية المترتبة على ذلك يمكن أن يصل الأمر ببعض الأشخاص إلى حدّ ارتكاب الجرائم بواسطة التكنولوجيا التي لم تبتكر لذلك لكن سوء استخدامها يمكن أن يتخذ صورا يجرّمها قانون العقوبات.

المطلب الأول: تركيبة الجريمة

تسمى جريمة الأنترنت بالجريمة المستحدثة نظرا للثورة التي أحدثها الأنترنت على نظم الجريمة المختلفة فمهما اتفقت مع الجريمة التقليدية من حيث اشتراط توفر أركانها العامة منها والخاصة فهي تختلف عنها من حيث صفات الفاعل وطبيعة السلوك الذي يتميز بخاصية المعنوية كما أن مسرح الجريمة معنوي كذلك فضلا عن تنوّع أصنافها.[1]

تعتبر جريمة الأنترنت ذات طابع مزدوج، الأول تقني والآخر قانوني، فأما الطابع التقني فيعود إلى وجود حاسب آلي وشبكة اتصالات يشكّل نطاق اتصال، فالحاسب الآلي قائم على نظام معالجة آلية للمعلومات، لعلّ أبرز ما يعزز هذا الجانب أنه أصبح يطلق على الفاعل فيها مصطلح المجرم المعلوماتي أو الإلكتروني[2] وكل الإجراءات المتعلقة بها يضاف لها مصطلح "الإلكتروني"، وأما الطابع القانوني فيرجع إلى نظرية الجريمة وتطبيق قواعدها من وجوب قيام أركانها وفق مبادئ القانون الجنائي لا سيما مبدأ الشرعية ومبدأ قرينة البراءة.

من هنا بات لزاما تسليط الضوء على خصوصية مرتكب الجريمة الذي يتميز عن المجرم في الجرائم التقليدية بجملة من الخصائص، لعلّ أهمها تمتّع الجاني بمهارة لتنفيذ النشاط الإجرامي وهذا لا يعني بالضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم [3]، لكن بالقدر الذي يكفيه للتعرف على الظروف المحيطة بالجريمة المراد تنفيذها وإمكانيات نجاحها واحتمالات فشلها بشكل يتلاءم مع الوسائل

1) المناعسة أسامة أحمد، الزعبي جلال محمد، جرائم تقنية نظم المعلومات الالكترونية (دراسة مقارنة)، مرجع سابق، ص 66.
2) هشام رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي التقني، مجلة الأمن والقانون، (د.ط)، كلية الشرطة دبي، 1999، ص 110.
3) القهوجي عبد القادر، الحماية الجنائية لبرامج الحاسب الآلي، الطبعة الأولى، الدار الجامعية للطباعة والنشر، 1999، ص 21.

المتاحة سواء كان الهدف من وراء ارتكاب الجريمة تحقيق الربح المادي بطريقة غير مشروعة، وهي الحالة الغالبة[1]، أو كان الهدف الانتقام أو رغبة في تحدي الذات.

أما عن السلوك الذي يعدّ قوام الركن المادي لجريمة الأنترنت فيتخذ صورا عديدة مثله مثل السلوك في الجرائم التقليدية لكن الأنظمة المعلوماتية تتيح الفرصة لارتكاب الجرائم التقليدية بطريقة غير تقليدية، فضلا عن اختصار الوقت والمسافات وبدون عناء مما يضفي على جريمة الأنترنت أنها جريمة عابرة للحدود.

فالسلوك المادي في جريمة الأنترنت، على اختلاف صوره، مرتبط بتقنية الحاسب الآلي وتفاعلية مع تقنية نظم المعلومات بشكل عام بما فيها شبكات الاتصال المعلوماتي يضاف لذلك نسبة ذكاء الفاعل التي تمكنه من الخروج عن تقليدية الفعل المادي في الجرائم التقليدية.

قد يحدث هذا السلوك أثرا ماديا وتكون الجريمة تامة وقد لا يحدث أثرا ونكون بصدد شروع في جريمة.

قامت الجزائر على غرار عديد من دول العالم بتجريم هذا النوع من الجرائم وذلك بتعديله لقانون العقوبات بموجب القانون 15/04 المؤرخ في 2004/11/10 والذي استحدث بموجبه القسم السابع مكرر اختار له عنوان " المساس بأنظمة المعالجة الآلية للمعطيات" والذي تضمّن المواد من 394 مكرر إلى 394 مكرر7، وكان هذا التعديل بداعي أن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدى إلى بروز أشكال جديدة للإجرام مما دفع بالكثير من الدول إلى النص على معاقبتها، وأن الجزائر تسعى إلى توفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات لمواجهة بعض أشكال الإجرام الجديد.[2]

أما على الصعيد الإجرائي فنص المشرع الجزائري على جملة من الإجراءات الوقائية بموجب القانون 04/09 المؤرخ في 2009/08/05 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ميّزه أمران أساسيان الأول على الصعيد الداخلي يتمثل في النص على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته بموجب المادة 13 منه تمّ تنصيبها فعلا عن طريق تشكيلها والنص على كيفية تسييرها بموجب مرسوم رئاسي مؤرخ في 2015/10/08، والأمر الثاني الذي ميّز القانون 04/09 حثّه على التعاون الدولي في مجال الوقاية من هاته الجرائم ومكافحتها نظرا لخاصية بارزة فيها وهي أنها عابرة للحدود.

1) مزيود سليم، الجرائم المعلوماتية واقعها في الجزائر وآليات مكافحتها، المجلة الجزائرية للإقتصاد والمالية، العدد 01 أفريل 2014، ص 98.
2) عرض أسباب تعديل قانون العقوبات بموجب الأمر 15/04 ص2.

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2021 المجلد: الخامس العدد: الثاني ص.ص: 160-181

المطلب الثاني: صور جرائم الأنترنت في التشريع الجزائري

تختلف أنواع جرائم الأنترنت باختلاف محل كل واحدة منها عن الأخرى، فمنها من تقع على النظام المعلوماتي بذاته بالاعتداء على المكونات المادية لهذا النظام ومنها ما يتمثل في الاعتداء على المكونات غير المادية للنظام مثل جرائم الاعتداء على البيانات المخزنة في ذاكرة الحاسوب والمنقولة عبر شبكات الاتصال المختلفة، وتلك التي يستخدم فيها النظام المعلوماتي وهي الجرائم التي يستخدم فيها الحاسب الآلي كأداة لتنفيذ الجريمة.

لقد نص المشرع الجزائري على مجموعة من الأفعال المادية التي تشكل جريمة المساس بالمعالجة الآلية للمعطيات نذكر من بينها الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك وجعل لها عقوبة حبس من 3 أشهر إلى سنة وغرامة من 50.000 دج إلى 100.000 دج على أن تضاعف العقوبة في حالة وقوع نتيجة تتمثل في حذف أو تغيير لمعطيات المنظومة، كما تصبح العقوبة الحبس من 6 أشهر إلى سنتين إذا وقع نتج عن الأفعال المذكورة سالفا تخريب نظام اشتغال المنظومة. [1]

كما عاقب المشرع الجزائري بموجب المادة 394 مكرر 1 من قانون العقوبات على فعل الادخال بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها وجعل لها عقوبة الحبس من 6 أشهر إلى 3 سنوات والغرامة.

أما المادة 394 مكرر 2 فنصت على مجموعة أفعال مادية عمدية أو عن طريق الغش وجعلت لها عقوبة الحبس من شهرين إلى 3 سنوات والغرامة، من بين هذه الأفعال تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية وكذا حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم.

إن الصورة الغالبة لتحقيق غاية المجرم المعلوماتي في نطاق الشبكة تتمثل في فعل الدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه بدون إذن، ومن ثم قيام الجاني بارتكاب فعله الذي قد يكون مجرّم فيشكل أحد أنواع جرائم الأنترنت، أو لا يكون كذلك، وتنصب هذه الجرائم على المعلومة، باعتبارها العنصر الأساسي المكوّن للبرامج والبيانات والمعلومات الموجودة بالحاسب الآلي، ويشترط أن تكون المعلومة

1) المادة 394 مكرر من قانون العقوبات المعدل والمتمم.

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2021 المجلد: الخامس العدد: الثاني ص.ص: 160-181

خاصة قاصرة على فرد أو افراد دون غيرهم، تبلغ حدّا من الأهمية يستأثرون بها وتشكل لديهم عامل مهم، في أدائهم يميزهم عن غيرهم، وتحمل ابتكارا أو إضافة يكونوا هم مصدرها.

و بالرجوع للمشرع الجزائري نجد أنه، وعلى غرار بقية التشريعات لا سيما التشريع الفرنسي والأمريكي والإنجليزي عاقب على جرائم أدرجها في القسم السابع مكرر من قانون العقوبات المعدل بالقانون15/04 المؤرخ في نوفمبر 2004 المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات بالمواد 394مكررالى 394 مكرر 7 مثلما سبق ذكره مجرّما من خلالها:

- فعل الدخول أو البقاء عن طريق الغش في كلّ أو جزء من منظومة المعالجة الآلية للمعلومات أو محاولة ذلك، أو متى ترتب عنه تغيير معطيات المنظومة أو حذف نظام التشغيل أو تخريبه.
- الإدخال أو الإزالة بطريقة الغش لمعطيات في نظام المعالجة الآلية للمعلومات.
- القيام عمدا وعن طريق الغش بتصميم أو بحث أو بتوفير، نشر، أو الاتجار بمعطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم الخاصة بأنظمة المعالجة الآلية للمعطيات.
- المشاركة في مجموعة أو اتفاق بغرض الإعداد لجريمة من الجرائم المنصوص عليها الخاصة بأنظمة المعالجة الآلية للمعطيات.

ورغم ذلك أشارت إحصائيات الى وقوع بين 200 الى 250 اعتداء يوميا على الأنظمة المعلوماتية بالجزائر وهو ما يستدعى التطبيق الفعلي لهذه النصوص.

ونلاحظ بالقراءة لما سبق أن الجريمة تتحقق بتوفر الركن المادي الذي تمثل في أحد أشكال الاعتداء على نظام المعالجة الآلية للمعطيات والذي يكمن في أحد الصور التالية:

1- الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات.

2- الاعتداءات العمدية على نظام المعالجة الآلية للمعطيات والتي تشترط وجود نظام معالجة للمعطيات كشرط مسبق.

3- الاعتداءات العمدية على سلامة المعطيات الموجودة داخل النظام (تخريب، اتلاف، الاتجار...).

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2021 المجلد: الخامس العدد: الثاني ص.ص: 160-181

بينما تمثل الركن المعنوي في صورة القصد الجنائي الذي يتمثل في العلم والإرادة، إضافة إلى نية الغش، فيجب أن تتجه إرادة الجاني إلى فعل الدخول أو البقاء وهو يعلم أن ليس له الحق في ذلك حتى لو كان بهدف الفضول وإثبات القدرة على المهارة.

وتبدو نية الغش من خلال الأسلوب الذي تم به الدخول من خرق الجهاز الرقابي الذي يحمي النظام، وبالنسبة للبقاء فيستنتج من العمليات التي تمت داخل النظام.

ونجد أن كل التشريعات السالف ذكرها (الأمريكي، الإنجليزي، الفرنسي والجزائري) قد فرّقت بين فعل الدخول والبقاء، فقد يكون فعل البقاء المجرم نتيجة دخول مشروع، بينما الدخول المجرّم هنا هو فعل غير مشروع، ويعدّ من الجرائم المؤقتة والشكلية، التي تكتمل بمجرد تحقيق السلوك الإجرامي دون تطلّب ركن مادي للجريمة، في حين يعتبر البقاء من الجرائم المستمرة فمجرد التواجد المعنوي للجاني داخل نظام للمعالجة الآلية للمعلومات واستغراقه لحيز وقتى بداخله تحقق الجريمة.

وتتحقق الجريمة متى كان الدخول أو البقاء مسموح ومشروع ولكن تجاوز الفاعل الوقت المحدد والمسموح به أو الغرض المصرح له بالدخول خلافا لإرادة صاحب الشأن المسيطر على النظام، وينتفي القصد الجنائي إذا دخل المستخدم إلى النظام بطريق الخطأ، لأن ذلك يعد جهلا بالوقائع ولكن يسأل جنائيا إذا دخل بطريق الخطأ إلى نظام معلوماتي، وظل متجولا فيه مع علمه بذلك.

من هذا المنطلق يمكن اعتماد تقسيم جرائم الأنترنت حسب التصنيف التقليدي للجرائم إلى جرائم تقع على الأموال وجرائم تقع على الأشخاص.

اولا / جرائم الأنترنيت الواقعة على الأموال:

1- جريمة إساءة استعمال بطاقة الإئتمان:

و هي من الجرائم الآلية الواقعة على الأموال كأن يلج الفاعل في الأنظمة المعلوماتية ويستولي على المعلومات المخزنة عن طريق قراءتها على شاشة الحاسوب أو نسخها مثلا وفي حالة سرقتها من صاحبها، ومن الصور أيضا القرصنة عن طريق اعتراض المعلومات أثناء حركتها.[1]

يعتمد نظام بطاقة الدفع الإلكتروني على عمليات التحويل الإلكتروني من حساب بطاقة العميل بالبنك المصدر للبطاقة إلى رصيد التاجر أو الدائن الذي يوجد به حسابه وذلك من خلال شبكة التسوية الالكترونية

1 الملط احمد خليفة، الجرائم المعلوماتية (دراسة مقارنة)، مرجع سابق، ص 196.

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2021 المجلد: الخامس العدد: الثاني ص.ص: 160-181

للهيئات الدولية " هيئة الفيزا كاردvisa card، هيئة الماستر كاردmaster card وتعطي بطاقة الدفع الإلكتروني الحق للعميل بالحصول على السلع والخدمات عبر الشبكة عن طريق تصريح كتابي أو تليفوني، بخصم القيمة على حساب بطاقة الدفع الإلكتروني الخاصة به، وتتم العملية بدخول العميل أو الزبون إلى موقع التاجر على الشبكة ويختار السلع المراد شراءها ويتم التعاقد بملأ النموذج الإلكتروني ببيانات بطاقة الائتمان الخاصة بالمشترى وعنوانه فيقوم محاسب المتجر بخصم قيمه السلع من بطاقة الدفع الإلكتروني وإرسالها إلى المشترى.

وأمام التطور التكنولوجي أصبحت إمكانية خلق مفاتيح البطاقات والحسابات البنكية بالطرق الغير المشروعة ممكنة عبر قنوات شبكة الانترنت.

2- جريمة الاحتيال باستخدام بطاقة الإئتمان:

و يكون ذلك من قبل صاحب البطاقة الشرعي وذلك بإساءته لاستخدام بيانات البطاقة الائتمانية أثناء مدة صلاحيتها، بدفع ثمن السلع والخدمات عن طريق الشبكة بملأ الإستمارة رغم علمه أنّ رصيده غير كافي لتغطية هذه المبالغ، أو أن يقوم بتحويل رصيده من بنك لأخر وهو يعلم أنه تجاوز رصيده الحقيقي، وفي صورة أخرى يتم الغش باستخدام بيانات البطاقة الائتمانية بعد مدة صلاحيتها أو إلغاؤها، فقد يكون البنك مصدر البطاقة قد ألغاها أثناء مدة صلاحيتها بسبب سوء استخدامها من العميل الذي يتعين عليه إعادتها للبنك، والذي قد يمتنع عن ذلك ويستمر في استعمالها باستخدام بياناتها في تعاملاته عبر الشبكة، وهو ما يشكل جريمة النصب بمجرد ملأ البيانات لإقناع الغير بوجود ائتمان وهمي، لأن البطاقة قد خلعت عنها قيمتها كأداة ائتمان خاصة بتحقق تسليم البضاعة أو السلع المشترات أو تمكينه من الاستفادة بالخدمات.

3- جريمة الغش في استخدام البطاقة من قبل الغير:

و ذلك في حالة التقاطها عبر الشبكة واستعمالها بطريقة غير مشروعة في سحب النقود الرقمية أو الوفاء بها، وبذلك تكون بياناتها محلا للسرقة من خلال تداولها عبر شبكة الانترنت بين العميل والتاجر بواسطة التجسس أو الخداع أو الحصول عليها باستخدام تقنية التفجير " إغراق الموقع"، وقد ذهبت المحاكم الفرنسية إلى أن سرقة بيانات بطاقة الائتمان واستخدامها بصورة غير شرعية، يشكل جريمة النصب على أساس انتحال الغير لاسم كاذب في حين يرى جانب من الفقه أنّ هذا الفعل شكل جريمة السرقة باستعمال مفتاح مصطنع باعتبار أنّ بطاقة الائتمان تعد مفتاح مصطنع لأنّ النصوص القانونية لم تحدّد بدقة ما هي المفاتيح المصطنعة.

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2021 المجلد: الخامس العدد: الثاني ص.ص: 160-181

4- جريمة تزوير بطاقات الإئتمان:

وقد تكون بطاقات الائتمان محلا للتزوير وذلك بتخليق أرقام بطاقات ائتمان خاصة ببنك ولهذه الأحداث أثر بالغ على المواطن الجزائري الذى نراه متخوف جدا من بطاقات الدفع الإلكتروني التي بدأت توزّع عبر نقاط البريد وطنيا ويحبّذ بقاء التعامل بالشيك، لأنّ هذه البطاقات ستكون محلا للاحتيال أو السرقة الالكترونية.

ثانيا / جرائم الأنترنيت الواقعة على الأشخاص:

1- جرائم إفشاء الأسرار العامة منها والخاصة:

أ / جرائم إفشاء الأسرار العامة:

وهي التي يتعلق الأمر فيها بأسرار تخص الدولة ونظام الدفاع عنها وهي الحالة التي نص عليها المشرع الجزائري في المادة 394 مكرر 3 من قانون العقوبات التي نصت على مضاعفة العقوبات المنصوص عليها إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد.

وقد تتخذ صورا خطيرة تصل حد الإرهاب وذلك بعد ظهور ما أصبح يسمى بالإرهاب الإلكتروني والذي يتخذ شكل التهديد والقصف الذي يعد أسلوبا للهجوم قد يؤدي إلى تعطيل مواقع، تدمير أنظمة المعلومات، التجسس الإلكتروني، الإختراق الإلكتروني، الإرهاب النووي والكيماوي، المعلوماتي لأغراض التخويف وبث الرعب والجسدي الذي يستهدف أشخاصا معينة بالذات أو غير معينين فضلا عن الإرهاب الإقتصادي الممارس للسيطرة الطبقية (اللوبيات)، الإرهاب الفكري والعقائدي وغيره.[1]

ب/ جرائم إفشاء الأسرار الخاصة:

وهي التي يقصد من ورائها التشهير بالشخص أو جماعة معينة أو الابتزاز أو طلب الرشوة مثلا وهذا النوع الأخير أصبح في تزايد مستمر عن طريق مواقع التواصل المختلفة بحيث وقع أن أخذت صور لأشخاص وتم بثها للعامة أو التهديد ببثها سواء ألتقطت بعلم الضحية ورضاه أو كان ذلك نتيجة قرصنة أو سرقة هاتف نقال أو غيرها من الحالات.

1) جندل جاسم محمد، الإرهاب الإلكتروني، الطبعة الأولى، دار البداية، 2014، ص 111.

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2021 المجلد: الخامس العدد: الثاني ص.ص: 160-181

2- المضايقة والملاحقة:

تتخذ جرائم الأنترنت صورا أخرى بحيث بعضها يتم بالملاحقة والمضايقة على شبكة الإنترنت غالباً باستخدام البريد الإلكتروني أو وسائل الحوارات الآنية المختلفة على الشبكة، تشمل الملاحقة رسائل تخويف ومضايقة، تتفق جرائم الملاحقة على شبكة الإنترنت مع مثيلاتها خارج الشبكة في الأهداف والتي تتمثل في الرغبة في التحكم في الضحية، و تتميز عنها بسهولة إمكانية إخفاء هوية المجرم علاوة على تعدد وسهولة وسائل الاتصال عبر الشبكة، الأمر الذي ساعد في تفشي هذه الجريمة، من المهم الإشارة إلى أن كون طبيعة جريمة الملاحقة على شبكة الإنترنت لا تتطلب اتصال مادي بين المجرم والضحية، لا يعني بأي حال من الأحوال قلة خطورتها، فقدرة المجرم على إخفاء هويته تساعده على التمادي في جريمته والتي قد تفضي به إلى تصرفات عنف مادية علاوة على الآثار السلبية النفسية على الضحية، فالقصد من المضايقة هو خلق نوع من التذمر أو الملل في نفس المجني عليه مما يؤدي به للانصياع لطلبات الجاني أو لمجرد المضايقة فقط[1].

3- إنتحال الشخصية:

هناك صورة أخرى لجرائم الأنترنت تتمثل في انتحال الشخصية وهي جريمة الألفية الجديدة كما سماها بعض المختصين في أمن المعلومات وذلك نظراً لسرعة انتشار ارتكابها خاصة في الأوساط التجارية، تتمثل هذه الجريمة في استخدام هوية شخصية أخرى بطريقة غير شرعية، وتهدف إما لغرض الاستفادة من مكانة تلك الهوية (أي هوية الضحية) أو لإخفاء هوية شخص المجرم، لتسهيل ارتكابه جرائم أخرى، إن ارتكاب هذه الجريمة على شبكة الإنترنت أمر سهل وهذه من أكبر سلبيات الإنترنت الأمنية، وللتغلب على هذه المشكلة، فقد بدأت كثير من المعاملات الحساسة على شبكة الإنترنت، كالتجارية في الاعتماد على وسائل متينة لتوثيق الهوية كالتوقيع الرقمي والتي تجعل من الصعب ارتكاب هذه الجريمة.

4- التغرير والإستدراج:

كما قد يعمد بعض مستعملي الأنترنت إلى أسلوب التغرير والاستدراج، فغالب ضحايا هذا النوع من الجرائم هم صغار السن من مستخدمي الشبكة، حيث يقوم المجرمون بإيهام ضحاياهم برغبتهم في تكوين علاقة صداقة على الأنترنت، والتي قد تتطور إلى اللقاء المادي بين الطرفين، والقصد من ذلك هو ربط علاقات غير مشروعة أو استخدام الأطفال في أغراض أخرى لا أخلاقية.

1) R.Merle et A.Vitu, Traité de droit criminel, 5eme edition tome 2 cujas 2001 p 42.

إنّ مجرمي التغرير والاستدراج على شبكة الإنترنت يمكن لهم أن يتجاوزوا الحدود السياسية فقد يكون المجرم في بلد والضحية في بلد آخر، وكون معظم الضحايا هم من صغار السن، فإن كثير من الحوادث لا يتم الإبلاغ عنها، حيث لا يدرك كثير من الضحايا أنهم قدُ غرّر بهم.

5- التشهير وتشويه السمعة:

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

6- صناعة ونشر الإباحة:

من بين الصور أيضا صناعة ونشر الإباحية، حيث قد وفرت شبكة الإنترنت أكثر الوسائل فعالية وجاذبية لصناعة ونشر الإباحية وقد شجعتها بشتى وسائل عرضها من صور وفيديو وحوارات بوضعها في متناول الجميع، ولعل هذا يعد أكبر الجوانب السلبية للإنترنت خاصة في مجتمع محافظ على دينه وتقاليده كمجتمعنا الإسلامي.

ولعل الكثير منا تفاجأ بصور خليعة تظهر على شاشة الكمبيوتر، وهي نوع من الدعاية المجانية لهذه المواقع التي تبيع الرذيلة وتحقق ملايين الدولارات ومختلف العملات من الأرباح وتستهدف نشر البغاء في المجتمعات.

7- جرائم القذف والسب:

تعد هذه الجرائم الأكثر انتشارا في هذا المجال جرائم القذف والسب، بحيث تعد جرائم السب والقذف الأكثر شيوعا في نطاق الشبكة، فتستعمل للمساس بشرف الغير أو كرامته واعتباره، ويتم السب والقذف وجاهيا عبر خطوط الإتصال المباشر أو يكون كتابيا، أو عن طريق المطبوعات وذلك عبر المبادلات الالكترونية.

1) D. Thomas , le concept de proces penal, melangésp. couvrat PUF 2001 p 401.

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2021 المجلد: الخامس العدد: الثاني ص.ص: 160-181

فحسب القواعد العامة لجرائم القذف والسب يستعمل الجاني عبارات بذيئة تمس وتخدش شرف المجني عليه، ومهما كانت الوسيلة المعتمدة، مع علمه أن ما يقوم به يعد مساسا بسمعة الغير بل أن إرادته اتجهت لذلك بالذات، وبالتطور أصبحت الأنترنت إحدى هذه الوسائل إن لم نقل أكثرها رواجا، فعادة ما ترسل عبارات السب أو القذف عبر البريد الصوتي أو ترسم أو تكتب على صفحات الويب مما يؤدي بكل من يدخل هذا الموقع لمشاهدتها أو الاستماع إليها ويتحقق بذلك ركن العلنية الذي تتطلبه الكثير من التشريعات في السب العلني، وإذا لم يطّلع عليها أحد، فانه يمكن تطبيق مواد السب أو القذف غير العلني.

و يرى جانب من الفقه انطباق النصوص التقليدية على جرائم السب والقذف المرتكبة بواسطة الأنترنت، وذلك باعتبار صفحات الأنترنت نشرة إعلامية فتأخذ حكم السب والقذف عبر الإعلام[1].

تجدر الإشارة إلى أنه راعى المشرع الجزائري في القانون 15/04 السالف الذكر إمكانية ارتكاب الجرائم الماسة بالمعالجة الآلية للمعطيات في جميع صورها من طرف شخص معنوي ورصد له عقوبة الغرامة تساوي 5 مرات الحد الأقصى المقرر للشخص الطبيعي. [2]

المطلب الثالث : الوسائل الحديثة لإرتكاب جرائم الأنترنت

لقد أصبحت الانترنت الوسيلة الحديثة لارتكاب جرائم التهديد، والتي في حد ذاتها تحتوي عدة وسائل لإيصال التهديد للمجني عليه لما تتضمنه من نوافذ وجدت للمعرفة وللأسف استعملت للجريمة فأصبحت المنابر الإلكترونية تمكّن المجرم من الوصول إلى ضحاياه بسرعة وبدقة دون عناء كما مكّنت من تواصل المجرمين مع بعضهم وحشد موالين لهم والمتعاطفين معهم (في مجال الإضرابات مثلا أو أخطر من ذلك الإرهاب).[3] وهي:

1- البريد الالكتروني:

الذي هو عبارة عن خط مفتوح على كل أنحاء العالم يستطيع الفرد من خلاله إرسال واستقبال كل ما يريده من رسائل سواء كتابه او صوتا وصورة وتعد الخدمة الأكثر استعمالا من قبل مستخدمي الشبكة، فتسمح لتبادل الرسائل بين مستخدمي الشبكة، سواء بين طرفين أو أكثر في نفس الوقت . القوائم البريدية . أين توزع رسالة الكترونية على ألاف الأشخاص في وقت واحد، كل على عنوانه البريدي.

1) S. Guinchard et J. Buisson ,procedure penale, 8eme editionlitec 2012 p 06.

2) المادة 394 مكرر 4 من قانون العقوبات معدل ومتمم.

3) جندل جاسم محمد، الإرهاب الإلكتروني، مرجع سابق، ص 105.

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2021 المجلد: الخامس العدد: الثاني ص.ص: 160-181

وكثيرة هي رسائل المرسلة عن طريق البريد الإلكتروني إلى المجني عليهم، المتضمنة تهديد بارتكاب جناية ضد نفسه أو ماله أو ضد الغير في نفسه أو ماله، وبإسناد إليه أمور ماسة بالشرف أو إفشاء الأسرار الخاصة به سواء كان مصحوبا بأمر أو طلب أو لمجرد الانتقام أو التسلية بمشاعر الاخرين، وكثيرا ما يقع التهديد بتدمير أو إغراق الموقع الإلكتروني أو جهاز المرسل إليه، وينطبق النص التقليدي لجريمة التهديد في أغلب التشريعات على التهديد المرتكب عبر الشبكة، نظرا لعدم اهتمام المشرع بوسيلة التهديد بقدر اهتمامه بمحتوى التهديد وجسامته.

من صورها أيضا جرائم إرسال تهديدات إلى الآخرين عبر البريد الإلكتروني ومثالها قيام شابين أمريكيين بإرسال تهديداً عبر البريد الالكتروني لجمعية إسلامية في إحدى الولايات الأمريكية وقامت الجمعية بتحويل التهديد إلى الشرطة التي لاحقت الرسالة الالكترونية وتوصلت إلى عنوان مرسلها وقامت باعتقاله وتم تحويل الشابين إلى المحكمة.

وقد قدمت وزارة العدل الأمريكية اتهاما رسميا ضد مواطنين أمريكيين من ولاية نيويورك بتوجيه تهديدات بالقتل لمواطنين مسلمين مقيمين في ولاية ديترويت ويفيد محضر الاتهام أن مايكل براتيساكس وجون بارنيت وجّها رسائل إلكترونية إلى المركز الإسلامي الأمريكي عدة مرات من منزلهما في ولاية نيويورك وهدّدا بقتل مسلمين يمارسون شعائرهم الدينية الإسلامية بحرية في الولايات المتحدة انتقاما لما يجري في منطقة الشرق الأوسط وأوضحت الوزارة في بيانها أنه يجب على هيئة الاتهام إثبات خطورة هذه الرسائل الإلكترونية.

2. منتديات المناقشة والمجموعات الإخبارية وغرف المحادثات والدردشة:

هي ساحات افتراضية للقاء والتحدث بين مستخدمي شبكة الانترنت، من ذوي الاهتمامات المشتركة الذين يؤلفون فيما بينهم مجموعات نقاش وتبادل البيانات والمعلومات والأفكار حول موضوع او قضية معينة، وذلك من خلال الرسائل المكتوبة عبر لوحة المفاتيح، و التي يراها الآخرين على الشاشة ليتم الرد عليها بنفس الشكل، ويتم اختيار الموضوع بكل حرية مهما كان نوعه في حدود ما توفره الانترنت من تقنية، ويمكن لأي شخص خلالها أن يقدم على تهديد الغير او ان يكون هو محلا للتهديد على اعتبار ان المشرع لم يحصر وسيلة التهديد.

3. صفحات الويب:

وهي النظام الأكثر شهرة في شبكة الأنترنت، للبحث عن المعلومات والاتصال والتبادل عبر الشبكة فهو أساس نمو الشبكة الهائل، تتم جريمة التهديد هنا بقيام شخص بإنشاء موقع ويب خاص به وينشر عليه تهديد لشخص آخر أو يتوعّد بإتلاف موقع آخر خاص بشخص أو شركة.

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2021 المجلد: الخامس العدد: الثاني ص.ص: 160-181

وفي إحدى الدول الأوروبية تم ضبط أحد الأشخاص أثناء قيامه بتهديد إحدى شركات المياه الغازية، طالبا منها مبلغ من المال حتى لا يقوم بوضع صورة زجاجة المياه المنتجة من الشركة وبداخلها حشرة على موقع الانترنت، ويطلق على الشخص الذي يقوم بإرسال عشرات الرسائل دفعة واحدة عبر الأنترنت إلى أشخاص لا يعرفهم ولم يطلبوا منه هذه الرسائل والتي تكون – في الغالب– بيانات أو إعلانات أو شتائم وتهديدات بمجرمSPAM .

المبحث الثاني: الإثبات الجنائي في جرائم الأنترنت

يقصد بالإثبات الجنائي إقامة الحجة والدليل من طرف السلطة القضائية المنوط بها ذلك وفق الإجراءات الجزائية للبحث عن قيام الجريمة بطرق مشروعة في مختلف مراحل الدعوى ابتداء من مرحلة جمع الاستدلالات إلى مرحلة المحاكمة مرورا بمرحلة التحقيق القضائي، وذلك حتى يمكن تطبيق النص القانوني الذي يتضمنه قانون العقوبات على الوقائع المنسوبة لشخص مرتكبها.

المطلب الأول: الدليل الالكتروني

احتراما لمبدأ قرينة البراءة التي تقضي بأن الأصل في الإنسان البراءة وجب عند إسناد واقعة قانونية مجرّمة مواجهة المتهم بارتكابها بالدليل الكفيل بإسقاط براءته وتأسيس العقوبة التي تفرض عليه بموجب قانون العقوبات احتراما هذه المرة لمبدأ الشرعية.

إن القاعدة في عبء الإثبات أنه يقع على سلطة الاتهام ممثلة في النيابة العامة بحيث يقع عليها إثبات قيام عناصر الجرم عن طريق التحقق من وقوعه ونسبته لفاعله بالدليل المادي أو المعنوي أو القولي.

يختلف الدليل الإلكتروني عن الدليل التقليدي لاختلاف محل الجريمة أو أداتها وهذا يعتبر نتيجة حتمية للأثر الذي أحدثته الثورة العلمية في نوعية الجرائم ونوعية الجناة، ويكمن هذا الإختلاف أساسا في عدم نجاعة الدليل التقليدي أو عدم كفايته في إثبات الجريمة المعلوماتية. [1]

للدليل الإلكتروني عدة خصائص، منها أنه دليل علمي وتقني ذو هيئة إلكترونية غير ملموس ولإدراكه يجب الاستعانة بأجهزة ومعدات واستخدام نظم وبرامج معلوماتية فهو كدليل يحتاج إلى بيئته الرقمية، [2]كما

1) قنديل أشرف عبد القادر، الاثبات الجنائي في الجريمة الالكترونية، (د. ط)، دار الجامعة الجديدة، الاسكندرية، مصر 2015، ص107.

2) نفس المرجع، ص 126.

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2021 المجلد: الخامس العدد: الثاني ص.ص: 160-181

أنه كذلك دليل يصعب التخلص منه عكس الدليل التقليدي الذي يكون ملموسا يمكن تمزيقه أو حرقه أو مسحه (مسح البصمات أو الآثار مثلا).

إن خصوصية الجريمة الناتجة عن سوء استخدام الأنترنت تقود إلى ضرورة إيجاد أدلة غير تقليدية لإثباتها أو تطبيق الطرق التقليدية بصورة غير عادية لتتلاءم وخصوصية الجريمة.

لقد نظم المشرع كيفية استنباط الدليل بواسطة إجراءات يتم إتباعها لوصول إلى الغاية، لعلّ أهم هذه الإجراءات المعاينة، التفتيش، ضبط الأشياء، سماع الشهود وندب الخبراء.

أولا: المعاينة

يقصد بها " رؤية بالعين لمكان أو شخص أو شيْ لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة"[1]، فهي إجراء من إجراءات التحقيق خاصة في مرحلة التحقيق الابتدائي بواسطة الضبطية القضائية، غير أنه يمكن أن يقوم بها قاضي التحقيق في مرحلة التحقيق القضائي.

غير أنه نظرا لخصائص جريمة الأنترنت يمكن لضابط الشرطة القضائية وكذا القاضي المكلف بالتحقيق الاستعانة بذوي الخبرة الفنية في الأمور التي يستعصى عليهم فهمها.

تتخذ المعاينة في هذه الجرائم صور عديدة منها النسخ أو الطباعة أو التصوير في مسرحان للجريمة بدلا من واحد في الجرائم التقليدية، المسرح الأول تقليدي يتمثل في الأماكن التي تقع خارج بيئة الحاسب الآلي التي يمكن أن تشتمل على آثار للجريمة، والمسرح الثاني افتراضي يقع داخل البيئة الالكترونية يتكون من البيانات الرقمية الموجودة داخل الحاسب وشبكة الأنترنت مما يستوجب تعاملا خاصا وقواعد فنية أهمها إعداد مختصين في التفتيش الالكتروني مثلا.

يتبع في معاينة في جرائم الأنترنت مجموعة من الأفعال منها تصوير جهاز الحاسب الذي يستعمل في ارتكاب الجرائم، العناية بطريقة الارتكاب عن طريق ملاحظة إعداد النظام والآثار الالكترونية التي يتركها الدخول أو التردد على الموقع وكذا السجلات الالكترونية التي تمكّن من معرفة موقع الاتصال ونوع الجهاز المستعمل، كما ينبغي عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة لتجنب إحداث أي إتلاف للبيانات المخزنة. [2]

1) أبو عامر محمد زكي، الإجراءات الجنائية، الطبعة السابعة، دار الجامعة الجديدة، الإسكندرية، مصر، 2002، ص 233.

2) سليمان أحمد فاضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، (د. ط)، دار النهضة العربية، القاهرة، مصر، 2007، ص 290.

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2021 المجلد: الخامس العدد: الثاني ص.ص: 160-181

ثانيا: التفتيش في البيئة الالكترونية

يعتمد على التفتيش لإظهار الحقيقة في غالبية التحقيقات لأنه في جل الحالات ينتج عنه أدلة مادية من شأنها التدليل على مرتكب الجريمة، فهو وسيلة من شأنها الإيصال إلى أدلة مادية تسهم في بيان الحقيقة.[1]

ففي المجال المعلوماتي ينبغي الأخذ بعين الاعتبار وجود مكونات مادية وأخرى منطقية فضلا عن وجود شبكات اتصال بعدية داخليا ودوليا تربط الحواسيب.

فأما تفتيش المكونات المادية فيخضع للقواعد العامة للتفتيش، أما تفتيش المكونات المنطقية (المعنوية) فيقصد بها تفتيش نظام تشغيل الحاسب الآلي ولو عن بعد بالدخول بغرض التفتيش إلى منظومة معلوماتية والمعطيات المخزنة بها ومنظومة التخزين في حد ذاتها أو منظومة أخرى يعتقد وجود المعطيات المبحوث عنها بها ولو كانت في الخارج وفي الحالة الأخيرة ينبغي للحصول عليها مساعدة السلطات الأجنبية، مع إمكانية تسخير كل من له دراية بعمل المنظومة لمد يد العون للمكلفين بالتحقيق للوصول إلى أحسن نتيجة.[2]

ثالثا: الحـــجز

يمكن حجز المعطيات المخزنة في منظومة معلوماتية وتكون مفيدة في التحقيق عن طريق نسخها ووضعها على دعامة تخزين إلكترونية قابلة للحجز مع الحرص على سلامة المعطيات التي تجري عليها السلطات المختصة التفتيش، كما يجوز لهته الأخيرة استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل المعطيات لاستغلالها دون المساس بمحتواها. [3]

تجدر الإشارة أن المشرع الجزائري نص في المادة 47 فقرة 4 من قانون الإجراءات الجزائية على إمكانية التفتيش والضبط على المكونات المعنوية للحاسوب وذلك من طرف قاضي التحقيق أو الضبطية القضائية.

رابعا: المراقبة الالكترونية

تتم عن طريق مراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها وقت حدوثها مع الأخذ بعين الاعتبار الأحكام القانونية التي تضمن سرية المراسلات والاتصالات والحق في الخصوصية.

1) المرصفاوي حسن صادق، أصول الإجراءات الجنائية في القانون المقارن، (د. ط)، منشأة المعارف، الإسكندرية، مصر 1982، ص375
2) المادة 5 من القانون 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها ج ر رقم 47.
3) المادة 6، نفس المرجع.

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2021 المجلد: الخامس العدد: الثاني ص.ص: 160-181

لقد نص المشرع على هذا الإجراء في قانون الإجراءات الجزائية لا سيما المواد 65 مكرر5 وما بعدها التي تسمح بالتحري عن طريق اعتراض المراسلات، التي يضمن الدستور سريتها لعلاقتها بالحرية الشخصية، وذلك بواسطة وسائل الاتصال السلكية واللاسلكية وتسجيل الأصوات بوضع ترتيبات تقنية دون موافقة المعنيين من أجل التقاط وتسجيل الكلام وكذا وضع رقابة على الهواتف والتقاط الصور لشخص أو أكثر يتواجدون في مكان خاص.

وضع المشرع لهذه الطرق ضوابط تتمثل في الإذن المسبق من وكيل الجمهورية المختص والتزام ضباط الشرطة القضائية القائمين بالإجراء بالسر المهني لكون هذه الطرق تمس بحرمة الحياة الخاصة للمواطنين.

خامسا: الإختراق

يسمى في التشريع الجزائري بالتسرب وذلك بموجب تعديل قانون الإجراءات الجزائية سنة 2006 بحيث استحدث المادة 65 مكرر5 وهو إجراء خطير يقوم به عون أو ضابط الشرطة القضائية بإذن مكتوب من وكيل الجمهورية وتحت إشرافه يوهم من خلاله أفراد العصابة أنه منهم وشريك لهم قصد التوغل داخل الجماعة الإجرامية يسمح للضابط خلال العملية استعمال هوية مستعارة وأن يرتكب عند الضرورة بعض الجرائم.

المطلب الثاني: حجية الدليل الرقمي أمام القاضي الجزائي

إن الدليل الرقمي شأنه شأن بقية الأدلة الأخرى يخضع للسلطة التقديرية للقاضي سواء في قبول الدليل أو في تقديره.

أقر المشرع الجزائري مبدأ حرية الإثبات الجنائي في المادة 212 من قانون الإجراءات الجزائية للوصول إلى إقناع القاضي الذي يستوجب عليه بناء حكمه على تلك القناعة.

للقاضي الجنائي دور إيجابي في توفير الدليل الإلكتروني ذلك أنه لا يلتزم بما يقدمه له أطراف الدعوى بل يبادر من تلقاء نفسه إلى اتخاذ كل الإجراءات للتحقيق في الدعوى، مع الإشارة إلى أن " القاضي" لا يقصد به قاضي الحكم فقط بل أيضا قضاء التحقيق.[1]

1) محمود محمد مصطفى، شرح قانون الإجراءات الجنائية، الطبعة الثانية، مطبعة دار النشر والثقافة، القاهرة، مصر، 1953، ص 360.

ردمد ورقي: 9971 - 2571 المجلة الأكاديمية للبحوث القانونية والسياسية ردمد إلكتروني: 2661-7404
السنة: 2021 المجلد: الخامس العدد: الثاني ص.ص: 160-181

من مظاهر الدور الإيجابي للقاضي الجنائي في البحث عن الدليل الإلكتروني أنه يمكن له الأمر للقائم بتشغيل النظام بتقديم المعلومات اللازمة لاختراق النظام والدخول إليه كالإفصاح عن كلمة المرور أو كلمة السر، كما للقاضي أن يأمر بتفتيش نظام الحاسب الآلي بكل مكوناته وكذا شبكات الاتصال.

كما أن اللجوء إلى طلب القيام بخبرة تقنية يعبّر على أقوى مظاهر التعامل القانوني والقضائي مع ظاهرة تكنولوجيا المعلومات وذلك لكون الخبرة التقنية تؤدي دورا بارزا أمام نقص المعرفة القضائية الشخصية لظاهرة الحاسب الآلي والأنترنت. [1]

غير أن طبيعة الدليل الرقمي تثير مشكلات عديدة تؤثر في الوصول إلى اقتناع القاضي نختصرها في مشكلات موضوعية وأخرى إجرائية.

أوّلا: المشكلات الموضوعية

يقصد بها تلك المتعلقة بطبيعة الدليل ذاته بسبب خصائصه الفيزيائية فهو دليل غير مرئي مخزن في نظام مزدوج يمزج بين ما هو جائز وما هو مجرم وقد يختلط الاثنان، أو بسبب مشكلة الأصالة في الدليل الإلكتروني كونها ذات الطابع الافتراضي عكس الدليل المادي أو بسبب ديناميكيته بحيث ينتقل عبر شبكات الاتصال بسرعة فائقة مما يعني إمكانية تخزين المعلومات أو البيانات في الخارج بواسطة شبكة الاتصال عن بعد، مما ينجر عنه صعوبة تعقب الأدلة الرقمية وضبطها واصطدام بمشاكل الحدود وسيادة الدول.

ثانيا: المشكلات الإجرائية

تتلخص المشكلات الإجرائية التي يثيرها الدليل الإلكتروني في ارتفاع تكاليف الحصول عليه ونقص المعرفة التقنية لدى رجال القانون، فعن ارتفاع التكاليف فالخبرة الفنية غالبا ما تكلف العدالة الجنائية مصاريف ضخمة يتم إنفاقها في سبيل الحصول على الدليل الرقمي التي تحتاج أحيانا إلى اللجوء إلى شركات أو منظمات أجنبية في الخارج، وأما عن المشكل الثاني المتمثل في نقص المعرفة التقنية لدى رجال القانون الأمر الذي استدعى إنشاء شرطة متخصصة لمكافحة هذا النوع المستحدث من الإجرام في عديد الدول غير أن الجزائر لم تنشئ إدارة متخصصة في مكافحة الجرائم الالكترونية بل اكتفت بوجود فرق ضمن الضبطية القضائية تتكفل بهذه المهمة، لكن ومع ارتفاع معدل هذا النوع من الجرائم تم استحداث بالجزائر شبكة إتصالات وطنية موحدة لجمع البيانات تربط بين مختلف مكاتب الدرك الوطني تزودهم بقاعدة البيانات المتعلقة بشبكات الجريمة المنظمة.

1) أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الالكترونية، مرجع سابق، ص200.

الخاتمة:

من خلال ما سبق عرضه تبين أن التطور الهائل في تكنولوجيا المعلومات والاتصال أدى إلى ظهور نوع جديد من المعاملات أفرزت جرائم مستحدثة تعتمد على الوسائل التي أتاحتها تلك الثورة المعلوماتية خاصة الأنترنت والتي تسمى جرائم الأنترنت أو جرائم استخدام الحاسوب.

أمام مواصلة التطور التكنولوجي يحتمل أن يتضاعف خطر هذه الجرائم بسبب ضعف الجاهزية التقنية والتشريعية لذلك وكذا صعوبة إقامة الدليل عليها لذلك وجب:

- إعطاء جرائم التقنية حقها من الأهمية بإدراج نصوص في التشريعات الداخلية والانخراط في الاتفاقيات الدولية بسبب البعد الدولي العابر للحدود لهذه الجرائم.
- تعديل التشريعات الحالية سواء الموضوعية أو الإجرائية على نحو يتلاءم مع طبيعة جرائم الأنترنت.
- تثقيف العاملين في مجال إثبات هذه الجرائم وحتى القضاة بعقد دورات تكوينية مكثفة مع إدراج مواد في طور التكوين في الكليات والمعاهد.
- إنشاء مركز معلومات عربي وعالمي لرصد جرائم الأنترنت ومرتكبيها.
- مواكبة التشريع للتطور الذي تعرفه التكنولوجيا وبالتبعية الظاهرة الإجرامية بواسطة هاته التكنولوجيا.
- إيجاد الوسائل الناجعة للتعاون الدولي من الناحية الإجرائية كتبادل المعلومات وتسليم المجرمين.
- إنشاء وحدات متخصصة في مكافحة هذا النوع من الجرائم.
- تعزيز دور الإعلام والمجتمع المدني في الوقاية منها.
- تعزيز دور الوقاية من هاته الجرائم بنشر الوعي الرقمي بين المستخدمين لمنع التعدي على بياناتهم الشخصية عن طريق بعض الأعمال البسيطة.

المراجع:

القوانين:

- قانون العقوبات المعدل والمتمم بالقانون 15/04 المؤرخ في 2004/11/10 المتعلق. بالمساس بأنظمة المعالجة الآلية للمعطيات ج ر 71

- القانون 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها ج ر رقم 47.

المراجع باللغة العربية

- حجازي عبد الفتاح بيومي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي (دراسة قانونية معمقة في القانون المعلوماتي)، (د. ط)، دار الفكر الجامعي، الاسكندرية، مصر، 2006.
- الملط أحمد خليفة، الجرائم المعلوماتية (دراسة مقارنة)، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، مصر، 2006.
- المناعسة أسامة أحمد، الزعبي جلال محمد، جرائم تقنية نظم المعلومات الالكترونية (دراسة مقارنة)، (د. ط)، دار الثقافة للنشر والتوزيع، 2014.
- القهوجي عبد القادر، الحماية الجنائية لبرامج الحاسب الآلي، الطبعة الأولى، الدار الجامعية للطباعة والنشر، 1999.
- جندل جاسم محمد، الإرهاب الإلكتروني، الطبعة الأولى، دار البداية، 2014.
- قنديل أشرف عبد القادر، الاثبات الجنائي في الجريمة الالكترونية، (د. ط)، دار الجامعة الجديدة، الاسكندرية، مصر، 2015.
- أبو عامر محمد زكي، الإجراءات الجنائية، الطبعة السابعة، دار الجامعة الجديدة، الإسكندرية، مصر، 2002.
- سليمان أحمد فاضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، (د. ط)، دار النهضة العربية، القاهرة، مصر، 2007.
- المرصفاوي حسن صادق، أصول الإجراءات الجنائية في القانون المقارن، (د. ط)، منشأة المعارف، الاسكندرية، مصر، 1982.
- محمود محمد مصطفى، شرح قانون الإجراءات الجنائية، الطبعة الثانية، مطبعة دار النشر والثقافة، القاهرة، مصر، 1953.
- عرض أسباب تعديل قانون العقوبات بموجب الأمر 15/04.

المقالات:

- هشام رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي التقني، مجلة الأمن والقانون، (د. ط)، كلية الشرطة دبي، 1999.
- مزيود سليم، الجرائم المعلوماتية واقعها في الجزائر وآليات مكافحتها، المجلة الجزائرية للاقتصاد والمالية، العدد 01 أفريل، الجزائر 2014.

المراجع بالفرنسية:

- D. Thomas- le concept de proces penal – melangésp. couvrat PUF 2001
- S. Guinchard et J. Buisson – procedure penale- 8eme editionlitec 2012
- R. Merle et A. Vitu- Traité de droit criminel- 5eme edition tome 2 cujas 2001