

مكافحة الجريمة الإلكترونية

أنيس العذار⁽¹⁾

المدرسة الوطنية للمهندسين صفاقس

الملخص:

أضحت الجريمة الإلكترونية اليوم واقعا مفرعا يهدّد الدول والأفراد. و يعود ذلك أساسا إلى الإمكانيات المتاحة للمجرم المعلوماتي الذي يستطيع تعطيل موقع الكتروني، يهّم الأمن الوطني أو يقرصن حساب أحد الشخصيات المعروفة، كما يمكنه اختراق البنوك و الاستيلاء على أرصدة عملائها أو بيع معطياتهم البنكية السرية على صفحات الشبكة العنكبوتية.

من جهة أخرى، فإنّ مكافحة الجريمة الإلكترونية ليست بالأمر الهين و ذلك لخصوصية مرتكب الجريمة الإلكترونية و طبيعة الجريمة الإلكترونية في حدّ ذاتها. يتميز المجرم المعلوماتي عادة بذكاء خارق، يجعل من الصعب كشفه باستعمال وسائل التفتيش التقليدية، كما أنّ إثبات الجريمة الإلكترونية من الأمور الصعبة نظرا لصبغتها اللامادية. وهو ما يتطلّب اعتماد أشخاص مدربين ومختصين في تعقّب الدليل الرقمي. ويزداد الأمر تعقيدا مع عدم قدرة نصوص التجريم التقليدية على مسايرة تطوّر الجريمة الإلكترونية.

الكلمات المفتاحية:

الجريمة الإلكترونية، المجرم المعلوماتي، الترشيح، الحجب، التشفير، مبدأ التأويل الضيق للقانون الجزائي، التعزير، اتفاقية بودابست لمكافحة الجرائم المعلوماتية.

تاريخ إرسال المقال: 2018/03/16، تاريخ قبول المقال: 2018/04/02، تاريخ نشر المقال: 2018/07/31

لتهميش المقال: أنيس العذار، "مكافحة الجريمة الإلكترونية"، المجلة الأكاديمية للبحث القانوني، المجلد 17، العدد 01، 2018، ص ص. 744-721.

<https://www.asjp.cerist.dz/en/PresentationRevue/72>

http://univ-bejaia.dz/Fac_Droit_Sciences_Politiques/revues-de-la-faculte

المقال متوفر على الروابط التالية:

(1) أستاذ مساعد، المدرسة الوطنية للمهندسين بصفاقس، جامعة صفاقس مُلحق بجامعة المجمع، المملكة العربية السعودية.

المؤلف المراسل: ladhar.anis@gmail.com

Combating cybercrime

Abstract:

Cybercrime has become an alarming reality today for both countries and individuals. This is mainly due to the opportunities available to cybercriminals who can hack into a website that affects national security, or usurp the identity of a famous personality. They can divert money from banks or sell confidential customer data over the internet.

The fight against cybercrime is not easy, because of the specificity of cybercrime. The cybercriminal is generally endowed with an extraordinary intelligence, which makes its capture extremely difficult with the traditional investigation techniques. The fight against the cybercrime is also difficult because of its specificity, which requires the use of qualified investigators. The difficulty is even greater with the ineffectiveness of current laws to adapt quickly to the fast evolution of cybercrime.

Key words

Cybercrime, cybercriminal, filtering, blocking, encryption, interpretation of criminal law, Budapest Convention.

La lutte contre la cybercriminalité

Résumé :

La cybercriminalité est devenue aujourd'hui une réalité alarmante, aussi bien pour les pays que pour les individus. Cela est dû principalement aux possibilités offertes aux cybercriminels. Ces derniers, peuvent pirater un site Internet touchant à la sécurité nationale, ou usurper l'identité d'une personnalité connue, comme ils peuvent détourner l'argent des banques ou vendre les données confidentielles de leurs clients sur Internet.

Par ailleurs, la lutte contre la cybercriminalité n'est pas aisée, en raison de la spécificité du cybercriminel et de la nature du crime cybernétique. Généralement, le cybercriminel est doté d'une intelligence qui sort de l'ordinaire, ce qui rend sa capture difficile avec les moyens d'investigation classiques. En plus, la preuve du crime cybernétique est difficile à apporter en raison de son caractère matériel, ce qui nécessite le recours à des personnes qualifiées en matière de preuve électronique. La difficulté est d'autant plus grande avec l'incapacité des textes d'incriminations ordinaires à s'adapter à l'évolution de la cybercriminalité.

Mots clés :

Cybercriminalité, cybercriminel, filtrage, blocage, chiffrement, interprétation étroite du droit pénal, Convention de Budapest.

مقدمة

تُعدّ الجريمة الإلكترونية من الجرائم المستحدثة¹، فقد تزامن ظهورها مع ظهور الحاسب الآلي و الإنترنت²، وهي إفراز لما نعيشه اليوم من ثورة معلوماتية³. رغم حداثة هذه الجريمة، إلا أنها أضحت تشكّل تهديدا حقيقيا للدول والأفراد⁴، يتجاوز أحيانا خطورة الجرائم التقليدية. ويزداد الأمر تعقيدا مع انتشار الجريمة الإلكترونية، إذ تُرتكب في العالم جريمة كل ثلاث دقائق عبر شبكة الأنترنت⁵. وقد ساهم انتشار الإنترنت في أنحاء العالم في تزايد عدد هذه الجرائم، حيث أنّ حوالي 10% مما يتم تداوله عبر الإنترنت مخالف للقوانين⁶. و قد وُصفت الجريمة الإلكترونية بأنها جريمة تقاوم التعريف، نتيجة اختلاف التعريفات و تفاوتها. ومن بين هذه المحاولات، التعريف الصادر عن منظمة التعاون الاقتصادي للتنمية (OCDE)، حين عرّفت الجريمة الإلكترونية بأنها "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية، يكون ناتجا بطريقة

¹ سُجّلت أول حالة اعتداء أمني على شبكة الإنترنت في عام 1988 م، حين قام "روبرت موريس" الطالب في جامعة "كورنل" بتطوير فيروس (عُرف لاحقا باسم فيروس موريس). وقد استغل هذا الفيروس ثغرة في نظام البريد الإلكتروني المستخدم آنذاك مكنته من استنساخ نفسه ونقل نسخة إلى عدد كبير من أجهزة الحاسب الآلي المرتبطة بالشبكة. أحدث هذا الفيروس شللا مؤقتا في جميع الأجهزة التي أصابها، والتي كانت تمثل حوالي 10 % من مجموع الأجهزة المرتبطة بالشبكة آنذاك وتسبب في خسارة قدرها 15 مليون دولار. (إلياس بن سمير الهاجري، "أمن المعلومات على شبكة الأنترنت"، ندوة حقوق الملكية الفكرية، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2004 م، ص 137).

² ظهرت الأنترنت في وزارة الدفاع الأمريكية وتم تطبيقها كتجربة داخل الولايات المتحدة بمعرفة الهيئات العلمية المتخصصة سنة 1969. وكانت الفكرة في البداية تقوم على ربط الحواسيب الآلية ببعضها البعض في مراكز البحث وفي كلّ منطقة في كل مدينة على حدة وقد رأى المشروع رأى النور أثناء الحرب الباردة وبالتحديد سنة 1969م، وسميت الشبكة آنذاك ARPANET.

³ حول الثورة المعلوماتية، انظر : سمير إبراهيم حسن، "الثورة المعلوماتية، عواقيها وآفاقها"، مجلة جامعة دمشق، المجلد 18، العدد الأول، 2002، ص 207. وهناك من يتحدث اليوم عن طوفان رقمي أو انفجار رقمي (انظر كتاب "الطوفان الرقمي"، هال أبلسون وهاري لويسوكين ليدين، ترجمة أشرف عامر، نشر إلكتروني لمؤسسة هنداوي).

⁴ في سنة 1434 هـ، تعرضت الشركة النفطية السعودية "أرامكو" إلى هجوم إلكتروني من طرف مجهولين ومن أربع قارات تسبب في إحداث أضرار بالشبكة الداخلية للشركة. كان الهدف من وراء هذا الاختراق هو وقف تدفق الزيت والغاز الى الاسواق المحلية والعالمية، بما يضر بشكل مباشر باقتصاد المملكة العربية السعودية و يحدث ارتباكا في أسواق النفط العالمية، وهو ما تمكّنت الشركة من تجنبه. وقد قال المتحدث الرسمي لوزارة الداخلية خلال المؤتمر الصحفي الذي عقده وزارة الداخلية وشركة "أرامكو" إثر الاعتداء الإلكتروني أنّ الوزارة بصدد إنشاء مركز وطني متخصص في محاربة الجرائم الإلكترونية وجميع ما يهدد أمن واستقرار الشركات السعودية المتخصصة في النفط والغاز والبتروكيماويات (انظر : جريدة الرياض، العدد 16240 الصادر في 26 محرم 1434 هـ).

⁵ انظر : ناصر بن محمد البقمي، "جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية"، الطبعة الأولى، الرياض، 1430 هجري - 2009 م، ص 23.

⁶ P. Sirinelli, « Conclusions » in, *La galaxie Internet, L'impératif de la conquête*, Edition Unicomm 1999, p. 220.

مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية⁷. من جهة أخرى، عرّف مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاينة المجرمين، المنعقد في فيينا سنة 2000 م، الجريمة المعلوماتية بأنها "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"⁸. هذا التعريف يقترب من التعريف الوارد بالمادة الأولى من نظام مكافحة جرائم المعلوماتية⁹ الذي يُعرّف الجريمة المعلوماتية بأنها "أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام". وقد جاء هذا النظام لمجابهة الجرائم الإلكترونية التي ازداد عددها و تفاقمت خطورتها، أمام غياب نظام خاص يردع مرتكبيها.

وتتميز الجريمة الإلكترونية بكلفتها الباهظة، فقد أشارت دراسة حديثة صادرة عن مركز الدراسات الاستراتيجية والدولية، CSIS، إلى أنّ جرائم الإنترنت تكلف الاقتصاد العالمي نحو 445 مليار دولار كل عام، وأنّ الأضرار التي لحقت بقطاع الأعمال نتيجة سرقة الملكية الفكرية تتسبب في خسارة للأفراد بحوالي 160 مليار دولار¹⁰. و المقلق في الأمر هو أنّه لا أحد في منأى عن الجريمة الإلكترونية، فعلى سبيل المثال تشهد منظومات وزارة الدفاع الأمريكية سنويا قرابة 250 ألف هجوم، و حسب تقارير مجلس الكونجرس الأمريكي فإنّ 162 ألفا منها تتجح في الدخول إلى المنظومات المعلوماتية للبنتاغون¹¹. ولم تسلم الشرطة الدولية "الإنتربول" من الهجمات الإلكترونية، فقد أقرّ المدير التنفيذي لخدمات الشرطة في الإنتربول "جون ميشال لوبوتين" تعرّض "الإنتربول" إلى عدة اختراقات، من ذلك هجمات من نوع "بوتنت" التي تسيطر على الأجهزة، كما تتعرّض حواسيبها لمئة ألف هجوم يوميا في مواقعها الإلكترونية حول العالم¹².

من جهة أخرى اتّسع مجال الجرائم الإلكترونية ليشمل دول الشرق الأوسط الذي أصبح أحد أكبر المستهدفين بالجريمة الإلكترونيّة في العالم. و قد صُنّفت المملكة العربية السعودية على أنّها أكبر مصدر

⁷ أنظر : أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر العربي، الاسكندرية، 2005 م، ص 96.

⁸ أسامة أحمد المناعسة، جرائم الحاسب الآلي والأنترنت، دار وائل، عمان، الأردن، ط 1، 2001 م، ص 77.

⁹ في 16/9/1427 هجري، صدر قرار مجلس الوزراء رقم 79، القاضي بالموافقة على نظام مكافحة جرائم المعلوماتية و المتّوج بالمرسوم الملكي رقم (م 17) بتاريخ 8/3/1428 هجري. وكان قد عُهد في البداية إلى لجنة النقل والاتصالات وتقنية المعلومات في مجلس الشورى بدراسة نظام مكافحة جرائم المعلوماتية، وأنهت تقريرها بشأنه معتبرة أنّ إصدار نظام مكافحة جرائم المعلوماتية يأتي لازدياد الجرائم ذات الصلة بالحاسب الآلي والأنترنت. (انظر ناصر بن محمد البقمي، جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية، الطبعة الأولى، الرياض، 1430 هجري -2009 م، ص 210).

¹⁰ مقال بعنوان "الجريمة الإلكترونية تُكلف الاقتصاد العالمي 445 مليار دولار سنوياً، مقال صادر عن البوابة العربية للأخبار التقنية <http://aitnews.com>.

¹¹ رضا مثناني، "مجتمع المعلومات والتنمية، أية علاقة؟"، مركز النشر الجامعي، الطبعة الثالثة، تونس 2009، ص 471.

¹² أنظر : مجلة الاتصالات والعالم الرقمي، العدد 252، 13/5/1429 (مرجع ذكره ناصر بن محمد البقمي، جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية، الطبعة الأولى، الرياض، 1430 هجري -2009 م، ص 23).

وهدف في نفس الوقت لأعمال إجرامية على الإنترنت بمنطقة الشرق الأوسط، محتلة بذلك الرقم 38 على مستوى الترتيب العالمي¹³. ويمكن تفسير استهداف المملكة بالجرائم المعلوماتية بما تعرفه من طفرة في مجال الإنترنت والتجارة الإلكترونية، حيث أن نصف سكان المملكة يستعملون الإنترنت¹⁴، بما يجعلها تحتل المرتبة الثانية في الشرق الأوسط على مستوى عدد السكان المستعملين للإنترنت¹⁵.

هذه الأمثلة الواقعية، تبين تنامي الجريمة الإلكترونية وتدفعنا إلى طرح السؤال التالي: إلى أي مدى يمكن إيجاد حلول عملية لمكافحة الجرائم الإلكترونية؟

على هذا السؤال سنتعرض في مرحلة أولى إلى الصعوبات التي تقف أمام مكافحة الجريمة الإلكترونية (المبحث الأول)، لننتعرض فيما بعد إلى الطرق الممكنة لمكافحة الجريمة الإلكترونية (المبحث الثاني).

المبحث الأول: صعوبة مكافحة الجريمة الإلكترونية

تشير الجريمة الإلكترونية عدة صعوبات تحول دون مكافحتها بشكل ناجح. ويمكن أن تكون هذه الصعوبات مرتبطة بمرتكب الجريمة الإلكترونية (المطلب الأول) أو بطبيعة الجريمة الإلكترونية (المطلب الثاني).

المطلب الأول: الصعوبات المرتبطة بمرتكب الجريمة الإلكترونية

على خلاف الجرائم التقليدية التي لا يتطلب ارتكابها في الغالب مهارات من نوع خاص، فإن الجريمة الإلكترونية تتطلب قدرا من الذكاء والمعرفة الدقيقة بالحاسب الآلي والشبكة المعلوماتية، لا يتوفر لدى الشخص العادي. وعادة ما يكون مرتكب هذه الجريمة شخصا متمكنا من مجال الحاسب الآلي والإنترنت، ويمتلك قدرا من الفطنة والذكاء يسمح له بخرق قواعد السلامة المعلوماتية واختراق أنظمة الحماية المعقدة. ويمكن تقسيم المخترقين إلى صنفين¹⁶ : المتسللون¹⁷ Hackers وهم "أشخاص يصلون بطرق غير قانونية إلى

¹³ محمد الجندي، "الجريمة الإلكترونية في الشرق الأوسط"، مقال منشور في <http://www.alukah.net/Sharia/0/2982>.

¹⁴ بلغ عدد مستعملي الأنترنت في المملكة في منتصف سنة 2012 م ثلاثة عشر مليون مستعمل.

(المصدر : www.internetworldstats.com).

¹⁵ انظر : www.internetworldstats.com.

¹⁶ ناصر بن محمد البقمي، جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية، الطبعة الأولى، الرياض، 1430 هجري - 2009 م، ص 5.

¹⁷ هناك من يصفهم ب"القرصنة الهواة" (انظر مذكرة صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة ماجستير في القانون، جامعة مولود معمري، تزي وزو، 2013، ص. 33).

المعلومات في نظام حاسوبي، كما أنهم قد يبادرون لتعديل هذه المعلومات¹⁸، دون أن يعلم هؤلاء في الغالب نتيجة ما قاموا به من أعمال، و المخربون¹⁹ Crackers ولا يقتصر دورهم على اختراق اجراءات الحماية ، بل يقومون بالعبث بالبيانات والمعلومات المخزنة على تلك الحاسبات والشبكات.

وسواء تعلق الأمر بالمتسللين أو بالمخربين فإن الوصول إليهم يبقى أمرا صعبا، و أحيانا شبه مستحيل، إذا ما تحصّن المجرم الإلكتروني وراء اسم مستعار أو اعتمد حاسبا آليا لشخص آخر بحيث يعجز الأمن على تعقبه. و عادة ما يعيق المجرم في جرائم الإنترنت سلطات التحقيق عن الوصول إلى الدليل بشتى الوسائل، كمسح برامج أو وضع كلمات سرية ورموز، وقد يلجأ لتشفير التعليمات لمنع إيجاد أي دليل يدينه²⁰. على سبيل المثال، تطلب إيقاف الهاكر الجزائري "حمزة بن دلاج"، المتهم باختراق 217 بنكاً عبر العالم، ثلاث سنوات من التعقب من طرف مكتب التحقيقات الفيدرالي الأمريكي و تنسيقا دوليا حتى تمكنت قوات الأمن ببانكوك من إيقافه²¹.

ويتميز المجرم المعلوماتي بخصائص تميزه عن المجرم التقليدي²²، ويرمز إليها الأستاذ Parker بكلمة SKRAM هي المهارة Skills والمعرفة Knowledge والوسيلة Ressources والسلطة Authority والباعث Motives²³. و يتمتع المجرم المعلوماتي بالمهارة والمعرفة الكافيتان لاختراق المواقع الالكترونية و كسر حواجز الشفرة. ويُعدّ المجرم المعلوماتي في نظر الكثير من الباحثين من نوابغ المجرمين، نظرا لما يمتلكه من قدرة على التعامل مع وسائل التقنية الحديثة ، و من إمكانية إخفاء الأدلة المادية للجريمة و التخفي وراء الأسماء المستعارة²⁴. و هناك من يعتبر بأنّ الجرائم الإلكترونية هي من أعراض "مرض النخبة"²⁵. وعادة ما يكون هؤلاء

¹⁸ ناصر بن محمد البقمي، نفس المرجع.

¹⁹ هناك من يصفهم بالقرصنة المحترفين.

²⁰ محمد عبد الرحيم سلطان العلماء، " جرائم الإنترنت والاحتماس عليها"، مؤتمر القانون والكمبيوتر و الأنترنت، منعقد من 1 إلى 3 ماي 2000 بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثالث، الطبعة الثالثة، 2004 م، ص 87.

²¹ انظر المقال الإلكتروني "بعد اختراقه عشرات البنوك الهاكر الجزائري حمزة بن دلاج في قبضة الـ FBI" المنشور في موقع : www.mbc.net

²² لمزيد التفاصيل حول خصائص المجرم المعلوماتي، انظر عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة مركز دراسات الكوفة، العدد السابع، 2008 م، ص 117.

²³ نائلة عادل قورة، "جرائم الحاسب الآلي الاقتصادية"، ص 56 (مرجع ذكره ناصر بن محمد البقمي، جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية، الطبعة الأولى، الرياض، 1430 هجري -2009 م، ص 44).

²⁴ عبد الفتاح بيومي حجازي، مبادئ الاجراءات الجنائية في جرائم الكمبيوتر والأنترنت، دار الفكر الجامعي، القاهرة، مصر، 2006، ص 14.

²⁵ انظر محمد رؤوف المراكشي، القانون الجنائي للإعلامية، محاضرة أُلقيت في إطار الجمعية التونسية للقانون الجنائي، مجلة القضاء والتشريع، عدد 3 لسنة 1985 م، ص. 40.

المجرمين من المتحصّلين على أعلى الشهادات العلمية²⁶. ومن الأمثلة على ذلك ما قام به الطالب الأمريكي Ian Murphy حين عمد سنة 1981، بمعية أصدقائه، إلى استعمال خط هاتفي للدخول إلى ملفات سرّية مخزّنة في حاسوب تابع للحكومة الفيدرالية الأمريكية²⁷. ورغم أنّ دوافع المجرم المعلوماتي لا تختلف عن دوافع المجرمين عامة، إلا أنّ مكنم الخطورة يتمثّل في أنّ المجرم المعلوماتي لا يرى عادة أنّ فعله يمثل فعلاً إجرامياً، وإنّما يُعدّ من قبيل إثبات الذات و تحدّي تقنية المعلومات²⁸.

المطلب الثاني: الصعوبات المرتبطة بطبيعة الجريمة الإلكترونية

من أهم الصعوبات التي تحول دون نجاعة مكافحة الجريمة الإلكترونية صبغتها العالمية (أ) إضافة إلى صعوبة إثباتها (ب) و عدم قدرة نصوص التجريم التقليدية على مسايرة تطورها (ج).

أ- الصبغة العالمية للجريمة الإلكترونية المرتكبة عبر الأنترنت

إنّ الصبغة العالمية للجريمة الإلكترونية المرتكبة عبر الأنترنت، تجعل من مكافحتها بطريقة ناجعة و فعّالة أمراً صعباً²⁹. فهي ليست مقصورة على منطقة أو دولة معينة ، وإنّما هي جريمة عابرة للحدود. وغالباً ما يستغل مرتكبو هذه الجرائم هذه الخاصية ، فيستهدفون مواطنين من دولة أجنبية ليجعلوا من تتابعهم ومحاكمتهم أمراً صعباً. ففي الجرائم المتعلقة بقرصنة البطاقات البنكية مثلاً، يعتمد القراصنة إلى قرصنة بطاقات لمواطني دولة أخرى ، ثم يبيعون هذه البطاقات عبر الأنترنت إلى أشخاص مقيمين في دولة ثالثة لا ينتمي إليها القراصنة أو ضحاياهم، مما يشنّت مجهودات وحدات الأمن داخل هذه الدول التي تضطر إلى التنسيق على مستوى ثلاثي. ولا تقتصر الصعوبة على هذا المجال، فحتى إذا ما تعهد القضاء بالجريمة المعلوماتية العابرة للحدود وأصدر حكماً بالإدانة ، فإنّه لا يمكن إجبار الدولة التي ارتكبت فيها الجريمة أو احتّمى بها المجرم على تنفيذ الحكم، و ذلك احتراماً لسيادة هذه الدولة³⁰، وبالأخص إذا كان قانون هذه الدولة لا يجرم الأفعال موضوع الإدانة. ويُطرح هنا مشكل تصادم الصبغة العالمية للأنترنت مع مبدأ إقليمية النص الجزائي الذي يُفيد بأنّ "قواعد

²⁶ انظر الهاشمي الكسراوي، "الجريمة المعلوماتية"، مجلة القضاء والتشريع، العدد 7 لسنة 2006، ص 27.

²⁷ Frédéric Jérôme Pansier et Emmanuel Jez, *La criminalité sur internet*, « Que sais-je ? », 2001, p. 100.

²⁸ انظر: ناصر بن محمد البقمي، جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية، الطبعة الأولى، الرياض، 1430 هجري - 2009 م، ص 46.

²⁹ حول الصبغة العالمية للجريمة الإلكترونية انظر : مذكرة صغير يوسف، "الجريمة المرتكبة عبر الأنترنت"، مذكرة ماجستير في القانون، جامعة مولود معمري، تيزي وزو، 2013، ص 16.

³⁰ أعلنت الجمعية العامة للأمم المتحدة منذ سنة 1965 في قرارها عدد 2131 مبدأ الاستقلالية الدستورية: "كل دولة لها الحق غير القابل للتصرف في اختيار نظامها السياسي (...). من دون أي شكل من أشكال التدخل من أي دولة".

القانون الجنائي لا تطبق إلا في حدود الإقليم الخاضع لسيادة الدولة³¹ و الذي يُعتبر نتيجة طبيعية لتطبيق مبدأ شرعية الجرائم والعقوبات³². وتكمن الصعوبة في أنّ القوانين الجزائية تختلف من بلد إلى آخر. ففي حين يسمح بلد مثل هولندا بتعاطي المخدرات فإنّ سائر بلدان العالم تجزّمه، وفي حين تُجيز عدة بلدان غربيّة القمار فإنّ دولا أخرى تمنعه، ونفس الأمر ينطبق على مواقع الإنترنت الإباحية³³.

وقد طرح اشكال اختلاف النصوص الجزائية بين الدول في القضية المتعلقة بمحرك البحث "ياهو" "Yahoo"³⁴. ففي 2000 / 11 / 21 أصدرت المحكمة الابتدائية بباريس قرارا يُلزم شركة "ياهو" بإيجاد حلول فنية تمنع مستعملي الإنترنت القاطنين بفرنسا من النفاذ إلى موقع البيع بالمزاد العلني ، الذي تُعرض فيه أغراض و بضائع ذات علاقة بالنازية و هو ما يُجرّمه القانون الفرنسي³⁵. وقد كان القرار مُرفقا بتقرير صادر عن هيئة من الخبراء يبيّن الطريقة الفنيّة التي يمكن اتباعها لتنفيذ هذا القرار. و رغم ذلك فقد رفض القضاء الأمريكي اعتماد هذا الحل لمخالفته للفصل الأول من الدستور الأمريكي الذي ينص على حرية التعبير³⁶. و قد طُرح نفس الإشكال بخصوص الفيلم الأمريكي "براءة المسلمين" الذي حاول تشويه صورة الرسول صلّى الله عليه وسلّم³⁷.

ب- صعوبة إثبات الجريمة الإلكترونية

صاحب ظهور الحاسوب وشبكة الإنترنت تحديات جديدة للقانون الجنائي بشقّيه الموضوعي والإجرائي، بما يُفقد قانون الإجراءات الجنائية أهميته وفعاليته³⁸. ومما يزيد الأمر صعوبة، جمع الجريمة الإلكترونية بين سرعة الانتشار وصعوبة الإثبات. فإذا كانت سرعة الانتشار تعود إلى الصبغة العالمية لهذه الجريمة، فإنّ صعوبة إثباتها راجع إلى صبغتها اللامادية التي تجعل من محو الأدلة الجزائية أمرا سهلا، إذ يمكن للمجرم الإلكتروني محو مئات الآلاف من البيانات من الحاسب الآلي في ضغطة زر. و بإمكانه عدم تخزينها أصلا

³¹ فرج القصير، القانون الجنائي العام، مركز النشر الجامعي، 2006، ص 49.

³² فرج القصير، المرجع السابق.

³³ انظر: عبد الفتاح بيومي حجازي، "الأحداث و الأنترنت"، 2002، ص 314.

³⁴ انظر: مقال الهاشمي الكسراوي، "الجريمة المعلوماتية"، مجلة القضاء والتشريع، العدد 7 لسنة 2006، ص 21.

³⁵ يجزّم الفصل 1-645 R من المجلة الجزائية الفرنسية مجرد عرض الأشياء المتعلقة بجرائم ضد الإنسانية.

³⁶ المحكمة الفدرالية بكاليفورنيا، 7 / 11 / 2001م.

³⁷ ألزم القضاء الأمريكي شركة Google بسحب الفيلم ولكن ليس على خلفية ما شكّله من إساءة إلى الإسلام وإنّما بناءً على طلب ممثلة في الفيلم تعرضت إلى تهديدات بالقتل مرتبطة بالفيلم.

³⁸ انظر محمد فتحي، "تفتيش شبكة الأنترنت لضبط جرائم الاعتداء على الآداب العامة"، المركز القومي للإصدارات القانونية، 2012 م، ص 504.

وعدم معالجتها على حاسبه الشخصي، خصوصا مع انتشار الحوسبة السحابية³⁹. وقد طُرح الإشكال أمام القضاء الفرنسي بالنسبة للملفات الوقتية temporary files المخزنة في الحاسب الآلي. وقد اعتبرت محكمة التعقيب الفرنسية أنها لا تشكل دليلا كافيا على ارتكاب الجريمة، طالما أن تسجيل هذه الملفات يتم تلقائيا ولا يُعبّر عن رغبة واضحة في تنزيل الملفات المحمية بحقوق التأليف⁴⁰. وبذلك تشكل خصوصية الدليل الرقمي تحديا إضافيا أمام الباحث الجنائي⁴¹.

وقد يعمد بعض الجناة إلى تشفير المعطيات المجرّمة، بحيث يستحيل فك رموزها من طرف السلطات الأمنية. ويمكن أن يكون ذلك على مستوى التخزين أو على مستوى تبادل المعلومات بين مجرمي الإنترنت على الشبكة العنكبوتية. وقد تطوّرت تقنيات التشفير بشكل يسمح بتشفير رسائل إلكترونية ثم بتبادلها في شكل صور فوتوغرافية عادية، وهي تقنية تحمل اسم « steganography »⁴². وتشكل الفضاءات العامة والمقاهي التي يمكن فيها استغلال خدمة الإنترنت بدون تحديد مسبق لهوية المستفيد من الخدمة، صعوبة إضافية تقف أمام تحديد الجاني في صورة ارتكابه لجريمة عن طريق الإنترنت المخصصة للعموم. في هذه الحالة يصعب كثيرا إثبات أنه ارتكب الجريمة.

من جهة أخرى فإنّ الضحية لا تلجأ في عديد الحالات إلى تتبع المجرم، إما لعدم تقطنها إلى حدوث الجريمة⁴³، أو لاقتراعها بعدم جدوى التتبع⁴⁴، أو خوفا على سمعتها إذا تعلق الأمر بجرائم ابتزاز أو جرائم

³⁹ الحوسبة السحابية (بالإنجليزية: Cloud computing) هي مصطلح يشير الي المصادر والأنظمة الحاسوبية المتوفرة تحت الطلب عبر الشبكة، والتي تستطيع توفير عدد من الخدمات الحاسوبية المتكاملة دون التقيد بالموارد المحلية بهدف التيسير على المستخدم، وتشمل تلك الموارد مساحة لتخزين البيانات والنسخ الاحتياطي والمزامنة الذاتية، كما تشمل قدرات معالجة برمجية وجدولة للمهام ودفع البريد الإلكتروني والطباعة عن بعد، ويستطيع المستخدم عند اتصاله بالشبكة التحكم في هذه الموارد عن طريق واجهة برمجية بسيطة تُبَسِّطُ وتتجاهل الكثير من التفاصيل والعمليات الداخلية.

⁴⁰ Christiane Féral-Schuhl, Cyberdroit, le droit l'épreuve d'internet, Dalloz, 2008, p. 906.

⁴¹ انظر محمد فتحي، "تفتيش شبكة الأنترنت لضبط جرائم الاعتداء على الآداب العامة"، المركز القومي للإصدارات القانونية، 2012 م، ص 407.

⁴² Voir, « Comprendre la cybercriminalité : guide pour les pays en développement », 2009, p. 91. (Rapport téléchargeable sur internet).

⁴³ في بعض الجرائم الإلكترونية مثل جرائم الاختراق لا تتقطن الضحية عادة إلى الأفعال المرتكبة من طرف المجرم المعلوماتي. ومن الأمثلة التي يتم فيها إخفاء الجريمة بصورة شبه كاملة ما وقع في الولايات المتحدة الأمريكية حين قام مبرمج بأحد البنوك بإجراء تعديلات على أحد البرامج، بحيث يتم إضافة عشرة سننات إلى خدمة تقل قيمتها عن عشرة دولارات ودولار واحد إلى الخدمات التي تزيد عن هذا المقدار، ومن ثم يتم تحويل المبالغ الزائدة إلى حساب قام الجاني بفتحه تحت اسم وهمي و هو "ZZWICKE"، بحيث يضمن أن يكون هذا الحساب هو الحساب الأخير طبق الترتيب الأبجدي لتسهيل عملية التحويل. وقد تمكّن الفاعل بهذه الطريقة من تحويل مئات الدولارات شهريا دون أن يقع اكتشاف أمره، إلى أن قام البنك في إطار عملية دعائية

تستهدف مؤسسة أمنية أو بنكية. وعادة ما تتكتم البنوك على هذه الجرائم رغم ما تسببه لها من خسائر فادحة، خوفا من زعزعة ثقة حلفائها فيها و خشية من سحبهم لأرصدهم البنكية، فلا أحد يرغب في إيداع أمواله في بنك يتعرض للسرقة. ويذهب البعض إلى الحديث عن وجود "قانون الصمت" في مجال الجريمة الإلكترونية، "ذلك أنّ الشكاوى التي تقدّم إلى المحاكم بخصوص الجرائم المعلوماتية لا تتعدّى نسبة 10 % من جملة الجرائم المقترفة والتي تفتّنت إليها المؤسسات المعتبرة عليها"⁴⁵. هذا التكتّم يجعل من تقدير الأضرار الناجمة عن الجريمة الإلكترونية أمرا صعبا.

و قد تعرّض أحد البنوك في تونس إلى القرصنة، من خلال تكليف مدير البنك لأحد مبرمجي الحاسوب بتزوير البيانات الشهرية و الأسبوعية الخاصة بالبنك و معطيات أخرى مرتبطة بالوضعية المالية للبنك، بحيث تُعطي انطباعا خاطئا عند انعقاد الجلسة العامة لمجلس إدارة البنك و إظهار موازنة السداسية بأنّ البنك في وضعية مالية ممتازة، و الحال أنّه يتكبد خسائر فادحة. و قد أدى ذلك إلى مغالطة مجلس الإدارة إلى أن انكشف الأمر بعد فوات الأوان⁴⁶.

ج-عدم قدرة نصوص التجريم التقليدية على مسايرة تطوّر الجريمة الإلكترونية

يُعدّ التطور السريع في الميدان المعلوماتي من أهمّ العوائق التي تحول دون مكافحة الجريمة الإلكترونية بطريقة ناجعة. ففي كل يوم تظهر تقنيات جديدة للقرصنة و التحايل والاختراق بشكل يصعب مجارته من طرف السلط التشريعية⁴⁷، بحيث أصبحنا نعيش فيما يمكن أن نسمّيه بالطوفان الرقمي⁴⁸. وفي المقابل، فإنّ أكثر دول

باختيار العميل الأول والعميل الأخير للبنك لتكريمهم كنوع من الدعاية، عندها اكتشف البنك أنّ العميل الأخير لا يوجد أصلا، (مثال أورده نائلة عادل محمد فريد قورة، "جرائم الحاسب الآلي الاقتصادية" منشورات الحلبي الحقوقية، 2004).

⁴⁴ العديد من الجرائم المعلوماتية تتم دون أن يشعر بها المتضررون ، من ذلك جرائم التجسس التي تتم عن طريق اعتراض النبضات الإلكترونية و جرائم الاختلاس التي تتم عبر تعديل البرامج والتلاعب بالأنظمة المعلوماتية وجرائم القرصنة و نشر الفيروسات (انظر غازي عبد الرحمان هيان الرشيد، الحماية القانونية من جرائم المعلوماتية (الحاسب والأترنت) أطروحة دكتوراه في القانون، الجامعة الإسلامية في لبنان، كلية الحقوق، 2010، ص 539).

⁴⁵ تقرير صادر عن دائرة مستديرة حول الجريمة الإلكترونية انعقدت بفرنسا في 1999/12/2 م،

(انظر الموقع الإلكتروني www.finance.gouv.fr).

⁴⁶ انظر قرار تعقيبي جزائي عدد 47396 مؤرخ في 1993/6/23، غير منشور.

(انظر الموقع الإلكتروني www.finance.gouv.fr).

⁴⁷ عادة ما يتطلب إصدار النصوص القانونية في مجال الجريمة الإلكترونية المرور بثلاثة مراحل:

المرحلة الأولى: تحديد مجال التجاوزات المحتملة في المجال المعلوماتي

المرحلة الثانية: تحديد الثغرة القانونية في القانون الجزائي

المرحلة الثالثة: صياغة النصوص القانونية الملائمة لمكافحة الجريمة.

العالم "تعتمد في مواجهة جرائم المعلوماتية على التشريعات العقابية التي وجدت لمواجهة الجرائم التقليدية المتعارف عليها، وهو ما أدى إلى قصور في الحماية الجنائية لعدم قدرتها على استيعاب هذه الجرائم ضمن النصوص القائمة"⁴⁹. وقد حاولت الدول العربية التصدي للجريمة الإلكترونية منذ سنة 1999، تاريخ صدور أول قانون عربي يتطرق إلى الجريمة الإلكترونية، وهو القانون التونسي المؤرخ في 2 / 8 / 1999⁵⁰ الذي أضاف إلى المجلة الجزائية التونسية فصولاً خاصة بالجريمة الإلكترونية، تلاه القانون العماني⁵¹ والإماراتي⁵² والسعودي⁵³. رغم ذلك فإن هذه النصوص، على أهميتها، تحمل في طياتها ثغرات ناجمة عن التطور السريع للجريمة المعلوماتية.

وفي المقابل، تعجز السلطات القضائية أحياناً، عند تعهدها ببعض القضايا المرتبطة بالجريمة الإلكترونية، على ردع المتهمين احتراماً لمبدأ الشرعية⁵⁴. و يحول هذا المبدأ دون محاكمة الشخص طالما لم يكن هناك نص صريح يجرم الفعل الذي ارتكبه، وهو ما يسمح لبعض مرتكبي الجريمة الإلكترونية بالإفلات من العقاب. وقد طُرح هذا الإشكال في بعض الدول العربية، على غرار ما حصل في دولة الإمارات العربية المتحدة في منتصف سنة 2000، حين تمكّن شاب بريطاني من اختراق شبكة اتصالات إماراتية و تخريب الإنترنت بها. وعندما أُلقي القبض عليه والتحقيق معه تبين عدم تجريم النصوص الجزائية في ذلك الوقت لهذه الأفعال، باستثناء بعض الفصول الموجودة في قانون الاتصالات و التي تضمنت عقوبات بسيطة غير رادعة⁵⁵.

و قد طُرح نفس الإشكال في القضية الصادرة عن محكمة التعقيب التونسية بتاريخ 24 أفريل 2002⁵⁶. تتمثل وقائع القضية في قيام المتهم بفتح رموز سرية لبطاقات رقمية أصلية معدة لقراءة قنوات تلفزيونية مشفرة، ثم

أنظر التقرير الصادر عن الاتحاد الدولي للاتصالات :

Comprendre la cybercriminalité : guide pour les pays en développement, 2009, p. 93. (Rapport téléchargeable sur internet).

⁴⁸ انظر كتاب "الطوفان الرقمي"، هال أبلسون وهاري لويسوكين ليدين، ترجمة أشرف عامر، نشر إلكتروني لمؤسسة هنداوي.

⁴⁹ ناصر بن محمد البقمي، جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية، الطبعة الأولى، الرياض، 1430 هـ - 2009 م، ص 32.

⁵⁰ القانون عدد 98 لسنة 1999 المؤرخ في 2 / 8 / 1999 م.

⁵¹ المرسوم السلطاني رقم 2001/72 م.

⁵² القانون الاتحادي رقم 2 لسنة 2006 م.

⁵³ صدر المرسوم الملكي رقم م/17 في 8 / 3 / 1428 هجري.

⁵⁴ حول مبدأ الشرعية، انظر : د. خالد بن عبد الله الشافي، مبادئ النظام الدستوري في المملكة العربية السعودية، 2012 م، ص 183، انظر كذلك : عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة مركز دراسات الكوفة، العدد السابع، 2008 م، ص 118.

⁵⁵ انظر عبد الفتاح بيومي حجازي، "الأحداث و الأنترنت"، 2002، ص 299.

⁵⁶ قرار تعقيبي عدد 16065 بتاريخ 24 / 4 / 2004 منشور بمجلة القضاء والتشريع، ديسمبر 2004، ص 165.

قام بشحن بطاقات رقمية عذراء بتلك الرموز السرية المستنسخة ، وبعد ذلك قام ببيعها بواسطة متهّم ثاني. قامت النيابة العمومية بإحالة على المحكمة الجزائية بناءً على الفصل 199 من المجلة الجزائية بتهمة "افتعال وثيقة معلوماتية ومسك واستعمال تلك الوثيقة". رغم ذلك فقد قضت محكمة البداية في شأنه بعدم سماع الدعوى ، لأنّ الفصل المذكور لم يجرّم فعل الصنع والافتعال، كما تأيّد هذا الحكم لدى محكمة الاستئناف ببزرت، فتعقيبته النيابة العمومية لدى محكمة التعقيب طالبة النقض والإحالة. لكن محكمة التعقيب رفضت مطلب التعقيب أصلاً معتبرة أنّ " المشرع لم يجرّم افتعال مثل هذه البطاقات وبالتالي لم يحدّد أية عقوبة على كل من يعتمد إلى تقليد أو افتعال أية بطاقة إلكترونية أو معلوماتية ... ومن البديهي الوقوف عند عبارات النص الجزائي وعدم التوسّع فيه، عملاً بالمبدأ القائل بأنّ تأويل النص الجزائي يكون ضيقاً وإن حصل يكون لصالح المتهّم".

وبذلك يُمثّل مبدأ التأويل الضيق للقانون الجزائي عائقاً إضافياً أمام اعتماد النصوص المنطبقة على الجرائم التقليدية في مكافحة الجريمة الإلكترونية. رغم ذلك، يجب الإشارة إلى أنّ الشريعة الإسلامية، التي تُعدّ دستور البلاد في المملكة العربية السعودية⁵⁷، تسمح للقاضي بسلطة واسعة في تقدير العقوبة، حتى في غياب نص تجريمي صريح، وذلك عن طريق التعزير. والتعزير⁵⁸ هو "تأديب عن ذنوب لم تشرّع فيها الحدود"⁵⁹. وبناءً على ذلك "لا يُشترط في جرائم التعزير أن يكون لكل جريمة عقوبة معيّنة محددة يتقيّد بها القاضي كما هو الحال في جرائم الحدود أو جرائم القصاص والدية، فللقاضي أن يختار لكل جريمة ولكل مجرم العقوبة الملائمة من مجموعة من العقوبات شرّعت لعقاب الجرائم التعزيرية كلّها، وللقاضي أن يخفّف العقوبة أو يغلّظها"⁶⁰. ويمكن القول بأنّ التعزير يسمح بتجاوز الثغرات التي قد تنشأ نتيجة التطبيق الصارم لمبدأ التأويل الضيق للنص الجزائي. ولكن ذلك لا يعني عدم خضوعه إلى ضوابط موضوعية⁶¹ تضمن العدل في تطبيق العقوبة التعزيرية⁶². وقد لجأ القضاء السعودي بالفعل، قبل صدور نظام مكافحة جرائم المعلوماتية، إلى اعتماد التعزير

⁵⁷ جاء بالمادة الأولى من النظام الأساسي للحكم : "المملكة العربية السعودية، دولة إسلامية، ذات سيادة تامة، دينها الإسلام، ودستورها كتاب الله تعالى وسنة رسوله ﷺ. ولغتها هي اللغة العربية، وعاصمتها مدينة الرياض".

⁵⁸ حول التعزير، انظر : سليم محمد النجار، سلطة القاضي في تقدير العقوبات التعزيرية، ماجستير في القضاء الشرعي، كلية الشريعة والقانون بالجامعة الإسلامية بغزة، 1428 هجري، 2007 م، انظر كذلك : صباح بنت صالح فلمبان، التعزير بأخذ المال، مجلة العدل، صادرة عن وزارة العدل السعودية، العدد 61، محرم 135 هجري، ص 77.

⁵⁹ الأحكام السلطانية، ص 205، بدائع الصنائع ج 7، ص 63، أسنى المطالب، ج 7، ص 161.

⁶⁰ عبد القادر عودة، التشريع الجنائي الإسلامي مقارناً بالقانون الوضعي، الجزء الأول، دار الحديث، القاهرة، ص 102.

⁶¹ ذكر الشيخ عبد الله بن محمد آل خنين 13 ضابطاً يتعيّن احترامه عند تقدير العقوبة التعزيرية. انظر بحثه "ضوابط تقدير العقوبة التعزيرية"، مجلة القضائية، العدد الأول، محرم 1432 هجري، ص 56.

⁶² انظر : عبد الله بن محمد آل خنين، "ضوابط تقدير العقوبة التعزيرية"، مجلة القضائية، العدد الأول، محرم 1432 هجري، ص 56.

في القضية الجزائية رقم 16/9 الصادرة عن المحكمة المستعجلة بالرياض في 1/5 / 1423 هـ⁶³، حيث قضى بجلد شاب مئة وخمسين جلدة تعزيراً إضافة إلى سجنه إحدى عشر شهراً والحكم بإبعاده لبلده، من أجل إخفائه فتاةً برضاها في منزله واستخدامه الإنترنت لاستدراج الفتيات والإيقاع بهن.

من جهة أخرى، لم يمنع صدور نظام مكافحة جرائم المعلوماتية من اعتماد القضاء السعودي التعزير في الجرائم المعلوماتية، من ذلك القرار الصادر عن المحكمة العامة بالغايط في 24 / 4 / 1435 هـ⁶⁴. و تتمثل وقائع القضية في ضبط شاب بأحد المكتبات العامة، التي تُوفّر خدمة الإنترنت للعموم مجاناً، بصدد تنزيل صور ومقاطع إباحية على حاسبه الآلي المحمول، عن طريق الإنترنت اللاسلكي. ورغم أنّ المتهم تمت إحالته من طرف الادعاء العام بناءً على المادة السادسة من نظام مكافحة جرائم المعلوماتية⁶⁵، إلا أنّ القاضي المتعهد بالقضية اعتبر أنّ الجريمة المرتكبة ليست جريمة معلوماتية. رغم ذلك، تمت إدانة المتهم. وقد استند القاضي لأحكام الشريعة معتبراً أنّ "ما قام به المدعى عليه أمر محرّم وحيث أنّ الشرع أمر بغض البصر ونظراً لكون تخزين مثل هذه المقاطع وسيلة إلى انتشار الرذيلة، ولما لها من التأثير السلبي على الفرد والمجتمع، ونظراً لكون هذه الجريمة تستدعي الردع والزجر لمرتكبها"⁶⁶، فقد قرّر القاضي إدانة المتهم بتخزين المقاطع الإباحية بجهاز الحاسب الآلي الخاص به وسجنه مدة شهر و جلده ثلاثين جلدة في مكان عام و إشهار اسمه و جريمته. وقد يكون استبعاد القاضي لأحكام المادة السادسة، التي كان من الممكن اعتمادها في قضية الحال، يجد تبريره في صرامة العقاب المقرر فيها، والذي يصل إلى خمس سنوات سجنًا.

⁶³ انظر : مدونة الأحكام القضائية ، الإصدار الثالث، سنة 1429 هـ (2008) ، ص 156. قرار رقم 35221481 صادر بتاريخ 24 / 4 / 1435 هـ عن المحكمة العامة بمحافظة الغاط، قرار غير منشور.

⁶⁴ قرار رقم 35221481 صادر بتاريخ 24 / 4 / 1435 هـ عن المحكمة العامة بمحافظة الغاط، قرار غير منشور.

⁶⁵ جاء بالمادة السادسة من نظام مكافحة جرائم المعلوماتية: "يعاقب بالسجن مدة لا تزيد عن خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية: 1. إنتاج ما من شأنه المساس بالنظام العام، أو القيم الدينية أو الآداب العامة، وحرمة الحياة الخاصة، أو إعداده، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي..."

⁶⁶ انظر القرار رقم 35221481 الصادر بتاريخ 24 / 4 / 1435 هـ عن المحكمة العامة بمحافظة الغاط، قرار غير منشور.

المبحث الثاني: طرق مكافحة الجريمة الإلكترونية

الأصل أن تكون مكافحة الجريمة عن طريق النصوص القانونية (المطلب الثاني) ، لكن خصوصية الجريمة الإلكترونية، المتمثلة أساساً في صبغتها العالمية و في قدرة مرتكبها على التخفي والإفلات من العقاب، تستدعي اعتماد طرق مكافحة تقنية (المطلب الأول).

المطلب الأول: الطرق التقنية

تتقسم الطرق التقنية لمكافحة الجريمة الإلكترونية إلى طرق تقنية ذات صبغة عامة تعتمدها الدولة (أ) و طرق تقنية خاصة يعتمدها الخواص (ب).

أ-الحماية التقنية العامة

تتمثل الحماية التقنية العامة أساساً في اعتماد نظام الترشيح والحجب (1) إضافة إلى اعتماد تقنية التشفير (2) و إحداث هيئة تابعة للدعاء العام مختصة في الجرائم المعلوماتية (3).

1- اعتماد نظام الترشيح والحجب

نظام الترشيح والحجب هو "أسلوب لحجب صفحات معينة يمكن أن تكون مؤذية أو عدوانية أو إباحية بالنسبة لمستخدم الأنترنت، فإذا حاول المستخدم الوصول إلى صفحة محجوبة ظهرت له رسالة تبليغه أن الوصول إلى هذه الصفحة غير مسموح به"⁶⁷. هذا النظام معمول به في المملكة العربية السعودية وقد تم إعداده من طرف "وحدة خدمات الأنترنت" التابعة إلى مدينة الملك عبد العزيز التابعة بدورها للعلوم والتقنية⁶⁸. ومنذ سنة 2006، أوكلت مهمة الإشراف على الترشيح إلى "هيئة الاتصالات وتقنية المعلومات"⁶⁹. ويتم الترشيح من قبل

⁶⁷ ناصر بن محمد البقمي، جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية، الطبعة الأولى، الرياض، 1430 هجري- 2009 م، ص 177.

⁶⁸ ناصر بن محمد البقمي، نفس المرجع.

⁶⁹ يوضح موقع الأنترنت الخاص بهيئة الاتصالات وتقنية المعلومات كيف تتم خدمة الترشيح : " تقوم هيئة الاتصالات وتقنية المعلومات بتقديم خدمة ترشيح محتوى الأنترنت في المملكة، وذلك من خلال وضع الضوابط والمتطلبات الخاصة بترشيح خدمات الأنترنت بالتنسيق مع اللجنة الأمنية الدائمة للأنترنت، كما تقوم بتوفير القوائم الخاصة بالمواقع المحجوبة يومياً لمزودي خدمة المعطيات، في حين يتولى مزودو خدمة المعطيات مسؤولية توفير الحلول التقنية بما يتوافق مع متطلبات الهيئة وسياساتها. ويتم حجب المواقع والمواد التي تتنافى مع الدين الحنيف والأنظمة الوطنية بناءً على توجيهات اللجنة الأمنية الدائمة. وقد أوكلت اللجنة مهمة حجب المواقع التي تروج للإباحية وتوفر وسائل لتجاوز الحجب إلى هيئة الاتصالات وتقنية المعلومات. وتتم عملية الترشيح من خلال قائمتين إحداها تجارية تضم أكثر من 90 تصنيفاً، ويتم حجب التصنيفات المتعلقة بالمواد الإباحية والقمار والمخدرات. هذه القائمة يتم تحديثها يومياً، ومن ثم توفيرها لمزودي خدمة المعطيات بعد دمجها مع القائمة المحلية لتطبيقها على أجهزة

مزوّدي خدمات المعطيات على أجهزة الخوادم لديهم. ورغم فعالية نظام الترشيح والحجب في منع النفاذ إلى المواقع الإباحية⁷⁰ ومواقع المخدرات والميسر، إلا أنّ كفاءتها تبقى محدودة بالنسبة للمواقع السياسية و الدينية⁷¹. من جهة أخرى، فإنّه بإمكان الأشخاص المتمكّنين من التقنيات المعلوماتية التخفي والنفاذ إلى المواقع المعنية بالحجب عن طريق البروكسي⁷². وعلى هذا الأساس، يعتبر البعض أنّ التوفيق بين الرقابة وسرعة تدفق المعلومات يغدو مهمة "سيزيفية" اليوم⁷³. وقد كتب "بيل غيتس" سنة 1995، "لكي تحقق الوصول الكامل إلى الإنترنت وتحافظ في الوقت ذاته على الرقابة، فسيتمّ عليك في أغلب الأحوال أن تعيّن لكل مستخدم شخصاً يُطل عليه"⁷⁴.

رغم الانتقادات التي يمكن أن توجّه لنظام الترشيح والحجب، و المتمثلة أساساً في تقييده حرية الإبحار عبر الإنترنت و محدودية نجاعته بالنسبة لبعض المواقع، إلا أنّه يبقى ضرورياً لحماية الشباب وخاصة القصر من مواقع المخدرات والإرهاب وخاصة المواقع الإباحية. وتشير دراسات أمريكية إلى أنّ المدمنين على المواقع الإباحية تتغير لديهم المفاهيم حول ما يعتبرونه مقبولا اجتماعيا. كما تبين الإحصائيات أنّ 50% من المغتصبين قد اطلعوا على مواد خليعة لتنشيط أنفسهم جنسياً قبل مباشرة جرائمهم الجنسية. وقد قام عدد من

الترشيح لديهم. كما يتوفر لدى الهيئة قائمة أخرى محلية، وهي عبارة عن قائمة داخلية يتم إعدادها من قبل هيئة الاتصالات وتقنية المعلومات وذلك من خلال إضافة المواقع الواردة إلى الهيئة من قبل عموم المستخدمين أو التوجيهات الواردة من الجهات المختصة. (انظر : موقع هيئة الاتصالات وتقنية المعلومات www.citc.gov.sa)

⁷⁰ حسب موقع هيئة الاتصالات وتقنية المعلومات، تشكّل المواقع الإباحية أكثر من 92 % من القائمة الخاصة بالترشيح والحجب. ⁷¹ قامت أربع جامعات أجنبية (جامعة هارفارد و كامبريدج و تورنتو و أكسفورد) بدراسة نظام الترشيح السعودي و بيّنت نتائجها كفاءة ترشيح المواقع الإباحية بنسبة 98 % و مواقع المخدرات بنسبة 68 % و مواقع الميسر بنسبة 93 % و المواقع السياسية بنسبة 3 % و المواقع الخاصة بالكيان الصهيوني بنسبة 2 % و المواقع الدينية بنسبة 1 % . (انظر: ناصر من محمد البقمي، "جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية"، المرجع السابق، ص 178).

⁷² "البروكسي" هو خادم يعمل كوسيط للطلبات بين العميل الذي يطلب مصادر من خوادم أخرى. هو جهاز كومبيوتر آخر يعمل كموزع تتم معالجة الطلبات من خلاله. عند الاتصال بأحد هذه الخوادم، فإنّ جهاز الكومبيوتر الخاص بالمستخدم يقوم بإرسال طلباته إلى خادم البروكسي الذي يقوم بدوره بمعالجة هذه الطلبات ثم يعيد إلي المستخدم ما طلبه. وبهذه الطريقة يعمل كوسيط بين الجهاز الشخصي وباقي أجهزة الكومبيوتر على شبكة الإنترنت. ويوجد نوع خاص من وحدات خدمة بروكسي يسمى "بروكسي CGI". وهي عبارة عن مواقع ويب تتيح للمستخدم فرصة الدخول من خلالها على أي موقع محجوب. وتقوم هذه المواقع عموماً باستخدام PHP أو CGI لتتمكن من العمل كوحدة خدمة بروكسي. وتستخدم هذه الأنواع من البروكسي عادةً للدخول على مواقع الويب التي يتم حجبها.

⁷³ انظر : سمير إبراهيم حسن، "الثورة المعلوماتية، عواقبها وآفاقها"، مجلة جامعة دمشق، المجلد 18، العدد الأول، 2002، ص 220.

⁷⁴ بيل غيتس، "المعلوماتية بعد الأنترنت (طريق المستقبل)"، ترجمة عبد السلام رضوان، سلسلة عالم المعرفة، الكويت، آذار 1998، ص 376.

ضباط الشرطة الأمريكيين بدراسة ظواهر الاغتصاب والقتل الجماعي، فوجدوا أنّ تداول المواد الإباحية سمة معروفة وموحدة لدى العديد من القتلة والمغتصبين. وقد قام مكتب التحقيقات الفيدرالي الأمريكي باستجواب 24 مجرماً في السجون، أدينوا من أجل جرائم اغتصاب وقتل، فتبين أن 81 % منهم كانوا مدمنين على المواد الإباحية وكانت جرائمهم تطبيقاً لما شاهدوه من إباحية⁷⁵. وقد كان من بين هؤلاء المجرمين "أرتور جاري بيشوب" Arthur Gary Bishop الذي أدين من أجل الاعتداء على خمسة أطفال وتشويههم وقتلهم، والذي صرح قبل إعدامه بأنه "لو أنّ مواد الدعارة والإباحية قد منعت مني في صباي، لم يكن شغفي بالجنس والشذوذ والإجرام ليتحقق"⁷⁶.

وتجدر الإشارة إلى قيام استراليا منذ سنة 1999 بتكليف هيئة مستقلة⁷⁷ بمراقبة الأنترنت. وقد اعتمدت هذه الهيئة قائمة سوداء في المواقع الاسترالية المخالفة للقانون، والتي يتعين على مزودي الاستضافة إغلاقها مثل المواقع الإباحية التي تستهدف الأطفال و المواقع العنصرية، إضافة إلى المواقع التي تخرق قواعد الملكية الفكرية. وفي نفس السياق، صدر سنة 2000 في الولايات المتحدة الأمريكية قانون لحماية الأطفال « Children's Internet Protection Act » يفرض على المكتبات العامة استخدام مرشحات تحجب المواقع الإباحية حتى تكون مستحقة للدعم الفيدرالي⁷⁸. من جهة أخرى، التزمت عدة محرّكات بحث ألمانية منذ بداية سنة 2005، وبصفة تلقائية، باعتماد قائمة سوداء تشمل المواقع المخالفة للقانون الألماني⁷⁹.

2- اعتماد تقنية التشفير

التشفير هو "استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تمريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومة بدونها"⁸⁰. وتعتبر تقنية التشفير من أنجع الوسائل للحفاظ على سرّية المعلومات المتبادلة إلكترونياً وعلى سلامتها من التغير. وهي "تقنية تستخدم لحماية سرّية الوثائق الإلكترونية استناداً إلى نظام العد العشري الذي يسمح بجعل

⁷⁵ انظر : محمد فتحي، "تفتيش شبكة الأنترنت لضبط جرائم الاعتداء على الآداب العامة"، المركز القومي للإصدارات القانونية، القاهرة، 2012 م، ص 78.

⁷⁶ انظر : محمد فتحي، نفس المرجع.

⁷⁷ Australian Broadcasting Authority

⁷⁸ انظر : محمد فتحي، "تفتيش شبكة الأنترنت لضبط جرائم الاعتداء على الآداب العامة"، المركز القومي للإصدارات القانونية، القاهرة، 2012 م، ص 173.

⁷⁹ Wiem YAAKOUB, *La cybercriminalité, Mémoire pour l'obtention du DEA en droit privé*, Sfax, 2009, p. 99.

⁸⁰ هذا التعريف اعتمدته التشريع التونسي في الفصل 2 من القانون عدد 83 لسنة 2000 المؤرخ في 2000/08/09 المتعلق بالمبادلات والتجارة الإلكترونية.

البيانات غير مفهومة بالنسبة لمن لا يملك المفتاح اللازم لفك الرموز⁸¹. وبذلك يمكن القول بأنّ "التشفير لا يخرج عن كونه كتابة بالرموز"⁸². وكلّما كانت هذه الرموز معقّدة كلما كان اختراقها أصعب. ولا يخفى ما تضمنه تقنية التشفير من أمن على مستوى مواقع الإنترنت الحساسة، كتلك التي تمسّ الأمن القومي أو تلك المختصة في التجارة والمبادلات المالية الإلكترونية. وقد أثبت الواقع العملي أنّ تقنية التشفير تكفل درجة عالية من تحقيق السلامة المعلوماتية، بما جعلها الحل الأمثل لقطع الطريق أمام القرصنة المعلوماتية⁸³.

رغم ذلك، يجب التأكيد على أنّ التشفير يمكن أن يقع استعماله لغايات منافية للغايات التي جُعل من أجلها، كأن يقع تبادل معلومات مشفرة بين قراصنة معلوماتيين. وبناءً على ذلك فقد قيّدت عدّة دول استعمال خدمات التشفير عبر شبكات الاتصالات بشروط وإجراءات مضبوطة⁸⁴. فقد نصّت المادة 9 من مجلة الاتصالات التونسية على أن "تُضبط بأمر شروط وإجراءات استعمال وسائل أو خدمات التشفير عبر شبكات الاتصالات وكذلك شروط تعاطي الأنشطة ذات العلاقة". و قد اشترط القانون الفرنسي من جهته أن يخضع التشفير إلى رخصة إدارية أو القيام بتصريح إداري، بما يسمح بعدم استعمال تقنية التشفير في أغراض إجرامية⁸⁵.

3- إحداث هيئة تابعة للدعاء العام مختصة في الجرائم المعلوماتية

تتطلب مكافحة الجريمة الإلكترونية إحداث هيئة مختصة في الأمن والسلامة المعلوماتية، على غرار ما هو معمول به في المملكة العربية السعودية. وقد نصّت المادة 14 من نظام مكافحة الجرائم المعلوماتية على ما يلي: "تتولّى هيئة الاتصالات وتقنية المعلومات وفقاً لاختصاصها تقديم الدعم والمساعدة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة". ويُعدّ اعتماد هيئة مختصة في دعم و مساندة الجهات الأمنية عند مكافحتهم للجريمة الإلكترونية أمراً ضرورياً، نظراً لصعوبة إثبات الجريمة المعلوماتية. وقد أنشأت عدة دول في العالم وحدات متخصصة في مكافحة جرائم الإنترنت من ذلك الصين والولايات المتحدة و بريطانيا⁸⁶. وفي فرنسا، اقترح وزير الداخلية السابق "ميشال دي فيلبان" مشروع قانون يهدف إلى مكافحة الجريمة الإلكترونية. ومن بين الحلول الواردة في مشروع القانون الترفيع في قوات الشرطة والدرك

⁸¹ هذا التعريف اعتمده التشريع التونسي في القانون النموذجي المتعلق بتبادل الوثائق الإلكترونية.

⁸² المنصف زغاب، "الوثيقة الإلكترونية"، مجلة القضاء والتشريع، ديسمبر 2005، ص 139.

⁸³ المنصف زغاب، المرجع السابق، ص 140.

⁸⁴ انظر محمد العسكري، "خصوصيات الإثبات في الجرائم المعلوماتية"، مجلة القضاء والتشريع، 2005م، العدد 7، ص 179.

⁸⁵ Loi française n° 96-659 du 26 juillet 1996 relative à la réglementation des télécommunications.

⁸⁶ انظر نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، 2013، ص

المتخصصين في المعلوماتية. وقد ذهب وزير الداخلية الفرنسي إلى حد اقتراح "البحث عن وسائل خاصة للتحقيق تمكّن من اكتشاف الجرائم الخطيرة في الوقت المناسب فلا يمكن مثلا للمحققين أن يشاركوا تحت اسم مستعار في المحادثات الالكترونية بدون أن يكونوا مسؤولين جزائيا"⁸⁷.

ب- الحماية التقنية الخاصة

هي الوسائل التقنية الحمائية التي يمكن للخواص اللجوء إليها من أجل التقليل من مخاطر الاختراق، من ذلك اقتناء برمجيات الوقاية من الفيروسات الإلكترونية و اعتماد جدار حماية ناري⁸⁸ Firewall. كما يتعيّن على مستخدم الحاسب الآلي تحديث جهازه بصفة دورية ، و عدم فتح رسائل البريد المشكوك فيها وتقادي نزيل الملفات من المواقع المريبة. ولم يعد مجال الحماية يقتصر حاليا على الحاسب الآلي، بل أصبح يشمل كذلك الهواتف الذكية، التي يمكن أن تكون هدفا سهلا للمجرم المعلوماتي نتيجة ما قد تحتويه من بيانات شخصية حساسة مخزنة في ذاكرتها.

من جهة أخرى، تتطلب مكافحة الجريمة الإلكترونية تثقيف مستخدمي الإنترنت و توعيتهم في مجال السلامة المعلوماتية، لكي يتجنبوا المخاطر التي تترصدهم. ويكون ذلك خاصة عن طريق تنبيههم في مواقع الإنترنت المهددة بالاختراق الإلكتروني، وإعلامهم بالطرق الاحتياطية التي قد يعتمدها المجرم المعلوماتي و طرق الوقاية منها. ويمكن لمتصفح الإنترنت غير المتمرس تقادي عديد الاختراقات والفيروسات الإلكترونية بتحبّ فتح رسائل البريد الإلكتروني المريبة وبتوخي الحذر عند اقبال النوافذ المنبثقة⁸⁹.

⁸⁷ انظر نبيلة هبة هروال، المرجع السابق، ص 115.

⁸⁸ جدار النار هو نظام أمني مخصص لحماية شبكة مؤسسة ما من الأخطار الخارجية، كالمطّفلين النافذين من شبكات أخرى للأنترنت. يقوم جدار النار بمنع حواسيب المؤسسة من الاتصال المباشر بأي حاسوب خارجي، سواء كانت طالبة أو مطلوبة، ويقوم جدار النار بتسيير جميع الاتصالات إلى مخدّم وكيل خارج شبكة المؤسسة، لكي يفحص الرسائل الواردة ويقرر تمريرها إلى شبكة المؤسسة أو صدّها (رضا مثنائي، "مجتمع المعلومات والتنمية، أية علاقة"، مركز النشر الجامعي، الطبعة الثالثة، تونس 2009، ص 651).

⁸⁹ النوافذ المنبثقة هي النوافذ التي تقفز على شاشة الكمبيوتر عند الولوج إلى بعض المواقع الإلكترونية. وتحاول هذه المواقع الإلكترونية خداع المستخدم من أجل تنزيل برامج تجسس أو دعاية في الحاسب الآلي، من خلال الضغط على كلمة "OK" أو "Accept" الموجودة في النافذة المنبثقة. لذا يتعيّن على المستخدم اتباع وسيلة آمنة، وهي الإقفال من مربع العنوان (X) الموجود في أعلى النافذة.

المطلب الثاني: الطرق القانونية

نظرا للصبغة العالمية للجريمة الإلكترونية ، فإنّ مكافحتها تستدعي تضافر جهود الدول المهددة بها ، قصد اعتماد اتفاقيات دولية توحد الحلول و الإجراءات لمجابهتها وحتى لا يكون المجرم المعلوماتي في مأمن من التتبع والعقاب أينما وُجد في العالم (أ). رغم ذلك، تبقى النصوص القانونية الداخلية الرادع الأساسي لمثل هذه الجرائم (ب).

أ- على المستوى الدولي

أثبت الواقع العملي عدم قدرة أي دولة على مكافحة الجريمة الإلكترونية لوحدها. ونظرا لصبغتها العالمية، ولكونها عابرة للحدود، فإنّ مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي الجنائي⁹⁰. وفي هذا الإطار، لعبت منظمة الأمم المتحدة دورا فعّالا في مكافحة الجريمة الإلكترونية (1)، كما ساهمت اتفاقية بودابست في وضع اللبّات الأولى للتصدي لهذه الجريمة (2)، وقد حاولت الدول العربية من جهتها إيجاد حلول مشتركة لمقاومة الجريمة الإلكترونية (3).

1- جهود الأمم المتحدة

بذلت منظمة الأمم المتحدة جهودا كبيرة من أجل مكافحة جرائم الأنترنت. وقد توصلت المنظمة في مؤتمرها الثامن⁹¹ حول منع الجريمة ومعاملة المجرمين، إلى إصدار قرار خاص بالجرائم المعلوماتية وقع التتبع فيه على الإجراءات التي يتعيّن اتخاذها من طرف الدول الأعضاء لمكافحة الجرائم الإلكترونية. وفي سنة 2000، تبنّت منظمة الأمم المتحدة الاتفاقية الخاصة بمكافحة إساءة استعمال التكنولوجيا لأغراض إجرامية. وقد أكّدت هذه الاتفاقية على ضرورة التنسيق بين الدول على مستوى تتبّع الجرائم المعلوماتية، و شددت على ضرورة تكوين الأشخاص المعنيين بالتتبع وتمكينهم من الوسائل الضرورية لذلك⁹²، كما عقدت منظمة الأمم المتحدة سنة 2010 المؤتمر الثاني عشر لمنع الجريمة و العدالة الجنائية. وقد ناقشت الدول الأعضاء آخر التطورات في استخدام التكنولوجيا الحديثة من طرف المجرمين، بما في ذلك الجرائم الإلكترونية. و احتلّت الجريمة المعلوماتية موقعا بارزا في جدول أعمال المؤتمر⁹³.

⁹⁰ انظر : حسين بن سعيد الغافري، "الجهود الدولية في مواجهة جرائم الأنترنت"، ص 5، مقال منشور في موقع المنشاوي للدراسات والبحوث، www.mishawi.com.

⁹¹ انعقد هذا المؤتمر بهافانا (كوبا) من 1990/8/27 م إلى 1990/9/7 م.

⁹² انعقد المؤتمر الثاني عشر لمنظمة الأمم المتحدة لمنع الجريمة والعدالة الجنائية بالبرازيل من 12 إلى 19 أبريل 2010.

⁹³ انظر مذكرة صغير يوسف، "الجريمة المرتكبة عبر الأنترنت"، مذكرة ماجستير في القانون، جامعة مولود معمري، تزي وزو، 2013، ص 93.

2- اتفاقية بودابست لمكافحة الجرائم المعلوماتية لسنة 2001

جاءت اتفاقية بودابست تنويعا للجهود التي بذلها الاتحاد الأوروبي و المجلس الأوروبي من أجل إيجاد صيغة قانونية لمكافحة الجريمة الإلكترونية، و هي تُعدّ حاليا الإطار المرجعي لمكافحة الجرائم المعلوماتية. وُضعت هذه الاتفاقية من قبل مجلس أوروبا بالتعاون مع كندا واليابان و جنوب إفريقيا والولايات المتحدة الأمريكية. وقد دخلت حيز التنفيذ في سنة 2004⁹⁴ ويمكن لأي دولة الانضمام إليها. أبرزت هذه الاتفاقية في صلب توطئتها مدى اقتناع الدول المصادقة عليها بخطورة الجريمة المعلوماتية ، وبضرورة تضافر الجهود الدولية لمواجهتها. وقد تعرّضت إلى بعض المفاهيم، مثل مفهوم النفاذ غير الشرعي و مفهوم الجريمة المعلوماتية و غيرها من المفاهيم التي تستدعي اعتماد مفهوم موحد لتسهيل تطبيق الاتفاقية⁹⁵. كما تضمنت قواعد متعلّقة بالتعاون في ميدان مواجهة الجريمة الإلكترونية، كالقواعد الخاصة بالاختصاص الترابي للمحاكم (المادة 22) وتسليم المجرمين (المادة 24) واعتماد شبكة مفتوحة كامل الأسبوع مخصصة لبقية الدول الأعضاء لتوفير المساعدة في الأبحاث المرتبطة بالجرائم المعلوماتية (المادة 35).

3- على مستوى الدول العربية

تبدو جهود الدول العربية في مكافحة الجرائم الإلكترونية ، من خلال اجتماع ممثلي الدول العربية في المؤتمر العربي للتحضير لمؤتمر القمة العالمية لمجتمع المعلومات في الفترة الممتدة من 16 إلى 18 يونيو 2003. وقد حضر المؤتمر ممثلو 19 دولة عربية إضافة إلى مندوبي 9 دول إفريقية كمراقبين و عدّة شخصيات مرموقة عالميا في مجال الاتصالات والمعلوماتية. و أوصى المشاركون في المؤتمر بإنشاء فريق عمل تحت مظلة جامعة الدول العربية لتأمين شبكة المعلومات العربية و حماية المستهلك العربي من جرائم الإنترنت⁹⁶. وقد سعى مجلس التعاون لدول الخليج العربي كذلك إلى مكافحة الجريمة الإلكترونية، حيث أوصى منذ سنة 2007 بأن ينخرط أعضاؤه في المنظومة العالمية لمكافحة الجريمة الإلكترونية وفق المعايير الدولية⁹⁷.

⁹⁴ انظر مذكرة صغير يوسف، "الجريمة المرتكبة عبر الأنترنت"، المرجع السابق، ص 100.

⁹⁵ الهاشمي الكسراوي، "الجريمة المعلوماتية"، مجلة القضاء والتشريع، العدد 7 لسنة 2006، ص 40.

⁹⁶ ناصر بن محمد البقمي، "جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية"، الطبعة الأولى، الرياض، 1430 هجري- 2009 م، ص 100.

⁹⁷ Voir, « Comprendre la cybercriminalité : guide pour les pays en développement », 2009, p. 122. (Rapport collectif téléchargeable sur internet).

ب- على المستوى الداخلي

رغم أهمية التعاون الدولي في مكافحة الجريمة الإلكترونية ،إلا أنه يصطدم في عديد الحالات بصعوبات ناتجة عن التباين الكبير للأنظمة القانونية للدول و الراجع أساسا إلى خصوصياتها الثقافية والدينية. و يوجد اختلاف بين الدول في تعريف الأنشطة التي تدخل في مفهوم الجريمة المعلوماتية، مع عدم الاتفاق على النماذج التي تشكّل البناء القانوني لهذه الجريمة، إضافة إلى التباين في التعامل الإجرائي معها⁹⁸. وعلى أساس ذلك يتعيّن على الدول صياغة الأنظمة الملائمة لمكافحة الجريمة الإلكترونية ،مع الأخذ بعين الاعتبار بخصوصياتها الاجتماعية والدينية.

في إطار التصديّ للجريمة الإلكترونية في المملكة، صدر نظام مكافحة جرائم المعلوماتية السعودي و المتوجّ بالمرسوم الملكي رقم (م 17) بتاريخ 1428/3/8 هجري⁹⁹. أقرّ هذا النظام عقوبات ضد من يعتمد إلى التنصت على ما هو مرسل داخل الشبكة المعلوماتية ، أو أحد أجهزة الحاسب أو الالتقاط أو الاعتراض، كما جرّم المساس بالحياة الخاصة عن طريق استخدام الهواتف النقالة أو ما في حكمها، إضافة إلى التشهير بالغير وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات. المادة الرابعة من النظام تجرّم التحايل والتجسس على البيانات البنكية أو الائتمانية للأفراد. من جهة أخرى يجرم النظام المساس بالنظام العام أو القيم الدينية أو الآداب العامة، و يُفرد الجريمة الإلكترونية ذات الطابع الإرهابي بعقاب صارم يصل إلى عشر سنوات سجنا نظرا لما تشكّله من تهديد لأمن المجتمع.

يعتبر نظام مكافحة الجرائم المعلوماتية وسيلة قانونية ناجعة و فعّالة في مكافحة الجريمة الإلكترونية، حيث أقر عقوبات رادعة للجرائم الإلكترونية. وقد سمح هذا النظام للقضاء السعودي بالتصدي لعدد الجرائم، وخاصة الأخلاقية منها، على غرار تخزين صور فاضحة في ذاكرة الهاتف النقال¹⁰⁰ و التشهير بالغير عن طريق الهاتف الجوال¹⁰¹. رغم ذلك، فإنّ بعض العقوبات الواردة بهذا النظام تتسم باللين¹⁰²، حسب اعتقادنا، بالنظر إلى خطورة بعض الجرائم. من ذلك أنّ أقصى العقاب المقرر للاستيلاء على المال المنقول أو على سند أو توقيع هذا السند وعن طريق الاحتيال ،أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة لا يتجاوز ثلاث سنوات، في حين أنّ الأضرار التي يمكن أن تلحق بالغير في حالة الاستيلاء الإلكتروني على أموال مودعة

⁹⁸ ناصر بن محمد البقي، المرجع السابق، ص102.

⁹⁹ انظر : ناصر بن محمد البقي، المرجع السابق، ص 210.

¹⁰⁰ انظر القرار الصادر عن المحكمة العامة بالجبيل، بتاريخ 18 / 1 / 1433 هجري، غير منشور.

¹⁰¹ انظر القرار الصادر عن المحكمة العامة بالجبيل، بتاريخ 02 / 3 / 1433 هجري، غير منشور.

¹⁰² تمّت صياغة نظام مكافحة جرائم المعلوماتية السعودي على خلاف الأنظمة الجنائية الحديثة، حيث بدأ المنظم بتحديد العقوبات أولا، ثم تحديد الجرائم التي تنطبق عليها العقوبات، في حين أنّ الشائع في النصوص التجريبية أن يتم تحديد الجرائم أولا، ثم العقوبات في مرحلة لاحقة (انظر ناصر بن محمد البقي، المرجع السابق، ص 211).

بالبنوك تكون عادة فادحة، على غرار ما قام به الهاكر الجزائري حمزة بن دلاج¹⁰³. من جهة أخرى فإن أقصى العقاب المقرر لجريمة الإتجار بالمخدرات أو المؤثرات العقلية عبر الإنترنت هو خمس سنوات ، و هو عقاب يبدو بسيطاً مقارنة مع العقاب المقرر للإتجار بالمخدرات بالطرق التقليدية والذي يصل في المملكة إلى الإعدام¹⁰⁴. وقد تدفع قلة التناغم على مستوى التجريم بين الجرائم التقليدية والجرائم المعلوماتية بعض المجرمين إلى اعتماد الجريمة الإلكترونية وسيلة لتحقيق أهدافهم الإجرامية. ومن بين النقائص التي يمكن أن تُنسب إلى نظام مكافحة الجرائم المعلوماتية، عدم إلزام مزودي الخدمات بحفظ البيانات المخزنة في أنظمتهم لمدة زمنية محددة بما يسمح بالتعرف على مستعمل الخدمة و على حركة الاتصال، و هي وسائل تسمح بضبط المجرم المعلوماتي بشكل أسرع.

تُشكل الجريمة الإلكترونية تحدياً للدول التي يتعين عليها تحيين أنظمتها وملاءمتها مع تطور الجريمة الإلكترونية. هذا التحدي يزداد صعوبة في المملكة التي تخضع الأنظمة فيها لأحكام الشريعة الإسلامية، إذ ينص النظام الأساسي للحكم في مادته السابعة على أن "يستمد الحكم في المملكة العربية سلطته من كتاب الله تعالى وسنة رسوله، وهما الحاكمان على هذا النظام و جميع أنظمة الدولة". وقد أثبت نظام مكافحة الجرائم المعلوماتية قدرة الشريعة الإسلامية على مواكبة تطورات العصر، حيث "تركزت مجالا واسعا للعلماء و أولي الأمر لمعالجة أمور المعاملات في جوانبها المختلفة من مدنية وجنائية ودستورية و نحوها في ضوء التوجيهات القرآنية والنبوية العامة... أما الفروع والتفاصيل المتعلقة بكيفية إعمال هذه الأسس العامة والقواعد الكلية وتطبيقها وإجراءات ذلك، فهي تنسم في أغلبها بالمرونة والتجدد"¹⁰⁵. بهذه المرونة والتجدد تمكنت الشريعة الإسلامية الغراء من مسايرة متطلبات العصر و مواكبة الجرائم المستحدثة، لتكون بالفعل صالحة لكل زمان ومكان.

¹⁰³ انظر المقال الإلكتروني "بعد اختراقه عشرات البنوك الهاكر الجزائري حمزة بن دلاج في قبضة الـ FBI" المنشور في موقع :

www.mbc.net

¹⁰⁴ انظر نظام مكافحة الاتجار بالمواد المخدرة في المملكة العربية السعودية الصادر بموجب الأمر السامي رقم 4/ب/966 وتاريخ

10 / 7 / 1407 هـ المتضمن قرار هيئة كبار العلماء رقم 138 وتاريخ 20 / 6 / 1407 هـ، وكذلك قرار مجلس الوزراء رقم 11 لسنة 1374 هـ.

¹⁰⁵ محمد عبد الظاهر حسين، "الفقه الإسلامي المصدر الرئيس للتشريع"، دار النهضة العربية، القاهرة، مصر، 1999 م، ص 127 (مرجع ذكره ناصر بن محمد البقمي، "جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية"، الطبعة الأولى، الرياض، 1430 هجري - 2009 م، ص 194).

خاتمة

في الختام، وعلى ضوء ما تم استعراضه حول مكافحة الجرائم الإلكترونية، يمكن القول بأن الجريمة الإلكترونية جريمة من نوع خاص تستدعي إجراءات من نوع خاص. كما أنّ مكافحتها تتطلب تنسيقاً دولياً و اهتماماً أكثر بالجانب التقني. وعلى ضوء ما تم ذكره، أمكن التوصل إلى النتائج و التوصيات التالية:

أولاً: النتائج

- 1- خصوصية الجريمة الإلكترونية و خصوصية مرتكبها.
- 2- صعوبة مكافحة الجريمة الإلكترونية باعتماد وسائل المكافحة التقليدية.
- 3- أهمية الجانب التقني في مكافحة الجريمة الإلكترونية.
- 4- التباين الكبير بين دول العالم في مكافحة الجريمة الإلكترونية و ضعف التعاون الدولي.
- 5- تميّز المملكة من الناحية النظامية على مستوى مكافحة الجريمة الإلكترونية.
- 6- صعوبة مسايرة النصوص القانونية لتطور الجريمة الإلكترونية.

ثانياً: التوصيات

أ-على المستوى التقني:

1. إيلاء الجانب التقني أهمية كبرى على مستوى مكافحة الجريمة الإلكترونية
2. اعتماد نظام ترشيح وحجب أكثر فاعلية بالنسبة للمواقع السياسية والدينية و المواقع الخاصة بالكيان الصهيوني أسوة بفاعلية نظام الحجب بالنسبة للمواقع الإباحية و مواقع الميسر ومواقع الاتجار بالمخدرات.
3. اعتماد تقنية التشفير بشكل أوسع في المعاملات الإلكترونية و في المواقع الإلكترونية التي لها علاقة بالأمن الوطني.
4. إحداث هيئة خاصة لمكافحة الجرائم الإلكترونية تتكون من مهندسين مختصين في مجال المعلوماتية ، مع السماح لهم قانونياً باعتماد وسائل استقصاء و تعقب خاصة مثل استعمال أسماء مستعارة في منتديات الأنترنت قصد تحديد هوية المجرمين دون أن يكونوا مسؤولين جزائياً.
5. نشر ثقافة السلامة المعلوماتية من خلال حملات توعية للعموم على مستوى وسائل الإعلام ، وإعلام مستخدمي الإنترنت صلب المواقع الإلكترونية المهددة بالاختراق الإلكتروني بالمخاطر التي تهددهم وبسبل الوقاية منها.

ب-على المستوى القانوني:

1. تشديد العقاب بالنسبة لبعض الجرائم (السرقة الإلكترونية والإتجار بالمخدرات عبر الأنترنت) بحيث يكون العقاب متقاربا مع العقاب المقرر لها في المملكة خارج المجال الإلكتروني.
2. التنصيص صلب نظام مكافحة الجرائم المعلوماتية على مسؤولية مزودي خدمات الاتصال في حفظ البيانات مدة زمنية محددة ، بما يُسهّل من التصديّ للجريمة والتعرّف على مرتكبها.
3. التنصيص صلب نظام مكافحة جرائم المعلوماتية على الاختصاص الحكمي للمحاكم السعودية في مجال الجرائم الإلكترونية وفق معايير متعدّدة ، مثل معيار جنسية المجرم و معيار جنسية المتضرر من الجريمة و معيار مقر المجرم بشكل يسمح بمتابعة لمجرّد توقّر أحد هذه المعايير وهو ما يحول دون إفلاته من العقاب.
4. إحداث خلية قانونية مختصة في متابعة المخاطر والجرائم الإلكترونية وإعداد النصوص القانونية الملائمة في وقت قياسي.
5. التنسيق مع مختلف دول العالم من أجل التصديّ للجريمة الإلكترونية.