بحث محكَّم

# مكافحة الجريمة الإلكترونية..
# الصعوبات والحلول

إعداد :

د. أنيس علي العذار

الأستاذ المساعد بكلية العلوم والدراسات الإنسانية بالغاط – جامعة المجمعة

## ملخص البحث

بيّن الباحث التالي:

مفهوم الجر يمة الإلكترونية والتعريفات المقترحة.

خطورة الجرائم الإلكترونية، حيث أضحت واقعا مفزعا يهدّد الدول والأفـراد، إذ يمكن للمجرم المعلوماتي أن يشل موقعا إلكترونيا يهم الأمن القومي، أو يقرصن حساب أحد الشخصيات المعروفة، كما يمكنه اختراق البنوك والاستيلاء على أرصدة عملائها أو بيع معطياتهم البنكية السرية على صفحات الشبكة العنكبوتية.

صعوبة مكافحة الجر يمة الإلكترونية الناتجة عن خصوصية مرتكب الجر يمة الإلكترونية وطبيعة الجر يمة الإلكترونية.

المجرم المعلوماتي شخص فائق الذكاء، ومن الصعب كشفه باستعمال وسائل التفتيش التقليدية.

إثبات الجر يمة الإلكترونية من الأمور الصعبة نظرا لصبغتها اللامادية مما يتطلّب اعتماد أشخاص مدرّبين ومختصّين في تعقّب الدليل الرقمي.

عدم قدرة نصوص التجريم التقليدية على مسايرة تطوّر الجر يمة الإلكترونية، ففي كل يوم تظهر تقنيات جديدة للقرصنة والتحايل والاختراق بشكل يصعب مجاراته من طرف الأنظمة.

النتائج الإيجابية لصدور نظام مكافحة جرائم المعلوماتية، بموجب قرار مجلس الوزراء رقم ٧٩ بتاريخ ١٤٢٧/٩/١٦ هجري،

القاضي بالموافقة على نظام مكافحة جرائم المعلوماتية والمتوّج بالمرسوم الملكي رقم (م ١٧) بتاريخ ١٤٢٨/٣/٨ هجري.

أهمية نظام مكافحة الجرائم المعلوماتية في مجال مكافحة الجر يمة الإلكترونية، نظرا للعقوبات الرادعة التي أقرّها. وقد سمح هذا النظام للقضاء السعودي بالتصدي لعديد الجرائم، وخاصة الأخلاقية منها، على غرار تخزين صور فاضحة في ذاكرة الهاتف النقّال والتشهير بالغير عن طريق الهاتف الجوال.

ضرورة تشديد العقاب بالنسبة لبعض الجرائم في نظام مكافحة الجرائم المعلوماتية (السرقة الإلكترونية والاتجار بالمخدرات عبر الإنترنت) بحيث يكون العقاب متقاربا مع العقاب المقرر لها في المملكة خارج المجال الإلكتروني.

ضرورة إحداث خليّة مختصة في متابعة المخاطر والجرائم الإلكترونية وإعداد النصوص النظامية الملائمة في وقت قياسي.

وقد اعتمد الكاتب المخطط التالي:

المبحث الأول: صعوبة مكافحة الجر يمة الإلكترونية.

المطلب الأول: الصعوبات المرتبطة بمرتكب الجر يمة الإلكترونية.

المطلب الثاني: الصعوبات المرتبطة بطبيعة الجر يمة الإلكترونية.

المبحث الثاني: طرق مكافحة الجر يمة الإلكترونية.

المطلب الأول: الطرق التقنية.

المطلب الثاني: الطرق القانونية.

# المقدمة

الحمد لله رب العالمين، والصلاة والسلام على سيد المرسلين، سيدنا محمد وعلى آله وصحبه أجمعين، و بعد:

تُعد الجريمة الإلكترونية من الجرائم المستحدثة[١]، فقد تزامن ظهورها مع ظهور الحاسب الآلي والإنترنت[٢]، وهي إفراز لما نعيشه اليوم من ثورة معلوماتية[٣]. ورغم حداثة هذه الجريمة، إلا أنها أضحت تشكّل تهديدا حقيقيا للدول والأفراد[٤] يتجاوز أحيانا خطورة الجرائم التقليدية، إذ تُرتكب في العالم

(١) سُجّلت أول حالة اعتداء أمني على شبكة الإنترنت في عام ١٩٨٨ 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 ١٠ ٪ من مجموع الأجهزة المرتبطة بالشبكة آنذاك وتسبب في خسارة قدرها ١٥ مليون دولار.
( إلياس بن سمير الهاجري،» أمن المعلومات على شبكة الإنترنت»، ندوة حقوق الملكية الفكرية، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، ٢٠٠٤ م ،ص ١٣٧ ).

(٢) ظهرت الإنترنت في وزارة الدفاع الأمريكية وتم تطبيقها كتجربة داخل الولايات المتحدة بمعرفة الهيئات العلمية المتخصصة سنة ١٩٦٩. وكانت الفكرة في البداية تقوم على ربط الحواسب الآلية ببعضها البعض في مراكز البحث وفي كلّ منطقة في كل مدينة على حدة وقد رأى المشروع النور أثناء الحرب الباردة وبالتحديد سنة ١٩٦٩م، وسميت الشبكة آنذاك ARPANET.

(٣) حول الثورة المعلوماتية، انظر : سمير إبراهيم حسن، «الثورة المعلوماتية، عواقبها وآفاقها»، مجلة جامعة دمشق، المجلد ١٨، العدد الأول، ٢٠٠٢، ص ٢٠٧. و يتحدّث البعض اليوم عن طوفان رقمي أو انفجار رقمي (انظر كتاب «الطوفان الرقمي»، هال أبلسون وهاري لويسوكين ليدين، ترجمة أشرف عامر ، نشر إلكتروني لمؤسسة هنداوي).

(٤) في سنة ١٤٣٤ 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 تمكنّت الشركة من تجنبّه. =

جريمة كل ثلاث دقائق عبر شبكة الإنترنت[٥]. وقد أسهم انتشار الإنترنت في أنحاء العالم في تزايد عدد هذه الجرائم، حيث إن حوالي ١٠٪ مما يتم تبادله عبر الإنترنت مخالف للقوانين[٦].

وُصفت الجريمة الإلكترونية بأنها جريمة تقاوم التعريف، نتيجة ما تناولته الكتابات عنها شرحا وتوضيحا. ومن بين التعريفات المُقترحة، التعريف الذي اعتمدته منظّمة التعاون الاقتصادي للتنمية(OCDE)، حين عرّفت الجريمة الإلكترونية بأنها «كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية، يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية».[٧] من جهة أخرى، عرّف مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين، المنعقد في فينّا سنة ٢٠٠٠ م، الجريمة الإلكترونية 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»[٨]. و لا يختلف هذا التعريف كثيرا عن التعريف

---

= و خلال المؤتمر الصحافي الذي عقدته وزارة الداخلية وشركة «أرامكو» إثر الاعتداء الإلكتروني، قال المتحدث الرسمي لوزارة الداخلية بأن الوزارة بصدد إنشاء مركز وطني متخصص في محاربة الجرائم الالكترونية وجميع ما يهدد أمن واستقرار الشركات السعودية المتخصصة في النفط والغاز والبتروكيماويات ( انظر : جريدة الرياض، العدد ١٦٢٤٠ الصادر في ٢٦ محرم ١٤٣٤ هـ).

(٥) انظر : ناصر بن محمد البقمي، «جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية»، الطبعة الأولى، الرياض، ١٤٣٠ هجري -٢٠٠٩ م، ص٢٣.

(٦) P. Sirinelli. Conclusions in « La galaxie Internet. L'impératif de la conquête ». Edition Unicom 1999. p. 220.

(٧) أنظر : أحمد خليفة الملط، «الجرائم المعلوماتية»، دار الفكر العربي، الاسكندرية، ٢٠٠٥ م، ص ٩٦.

(٨) أسامة أحمد المناعسة، «جرائم الحاسب الآلي والإنترنت»، دار وائل، عمان، الأردن، ط ١، ٢٠٠١ م، ص ٧٧.

الوارد بالمادة الأولى من نظام مكافحة جرائم المعلوماتية[٩] الذي يُعرّف الجريمة المعلوماتية بأنها «أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام».

و يتعيّن الإشارة إلى أن الحاسب الآلي لم يعد المستهدف الوحيد من طرف الجريمة الإلكترونية، فقد أضحت بطاقات الائتمان مجالا مغريا للإجرام الإلكتروني. كما تشكّل الهواتف الذكية هدفا محتملا للمجرم المعلوماتي، خاصة و أن معظمها لا تحتوي برامج حماية ضد الفيروسات الإلكترونية. و يزداد الأمر دقة مع الثورة التكنولوجية التي تشهدها الهواتف الذكية، حيث لم تعد مجرّد وسيلة لتبادل المكالمات، بل أصبحت في الآن ذاته حواسيب مصغّرة وآلات تسجيل صوتي و تصوير فائقة الدقة، مع كل ما يسمحه ذلك من تجاوزات محتملة ومن تعد على خصوصية الغير. فأصبحت الهواتف الذكية وسيلة فعّالة لارتكاب الجرائم الإلكترونية.

وعادة ما يُستعمل مصطلح الجريمة الإلكترونية كمرادف للجريمة المعلوماتية[١٠]، كما قد تتخذ الجريمة الإلكترونية تسميات أخرى مثل: «جرائم الكمبيوتر والإنترنت» و«الجرائم السيبرانية»[١١] و«جرائم الحاسب الآلي» و«جرائم التقنية

(٩) في ٩/١٦/ ١٤٢٧ هـ، صدر قرار مجلس الوزراء رقم ٧٩، القاضي بالموافقة على نظام مكافحة جرائم المعلوماتية و المتوّج بالمرسوم الملكي رقم (م ١٧) بتاريخ ١٤٢٨/٣/٨ هجري. وكان قد عُهد في البداية إلى لجنة النقل والاتصالات وتقنية المعلومات في مجلس الشورى بدراسة نظام مكافحة جرائم المعلوماتية، وأنهت تقريرها بشأنه معتبرة أن إصدار نظام مكافحة جرائم المعلوماتية يأتي لازدياد الجرائم ذات الصلة بالحاسب الآلي والإنترنت.

(١٠) انظر : ناصر بن محمد البقمي، «جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية»، الطبعة الأولى، الرياض، ١٤٣٠ هجري -٢٠٠٩ م، ص ١٥.

(١١) انظر : محمد قاسم أحمد الردفاني، «تحقيقات الشرطة في مواجهة تحديات الجرائم السيبرانية»، المجلة العربية للدراسات الأمنية و التدريب، المجلّد ٣٠، العدد ٦١، صفر ١٤٣٦ هـ، ص ١٥٧.

الحديثة» و«الجرائم الرقمية»[١٢].

قد تتخذ الجريمة الإلكترونية صورا متعددة، فقد تكون في شكل جريمة تقليدية مرتكبة باستعمال الحاسب الآلي والإنترنت، من قبيل جريمة القذف والسب أو السرقة أو تبييض الأموال أو ممارسة الإرهاب الفكري. و يمكن أن تأخذ الجريمة الإلكترونية شكلا تقنيا بحتا، من ذلك قرصنة برامج الحاسب أو التجسس على البيانات السرية للأفراد والشركات أو اختراق مواقع إنترنت محمية أو نشر فيروس إلكتروني. و يمكن أن ترتكب الجريمة الإلكترونية من طرف شخص محترف في المعلوماتية، كما يمكن أن يرتكبها شخص عادي. و يُعد تنزيل المؤلفات المحميّة بموجب حقوق التأليف، من الأعمال واسعة الانتشار على الإنترنت.

**أهمية البحث:**

يتعرّض البحث لجريمة مستحدثة ارتبط وجودها بظهور المجتمع المعلوماتي. ويُبيّن البحث تزايد خطورة هذه الجريمة على مستوى الأضرار المادية التي تُسببها وعلى مستوى أمن الأفراد والدول. وتتأكد هذه الخطورة من خلال الدراسات الحديثة، من ذلك أن دراسة صادرة عن مركز الدراسات الاستراتيجية والدولية CSIS قدّرت أن جرائم الإنترنت تكلّف الاقتصاد العالمي نحو ٤٤٥ مليار دولار

(١٢) انظر : ابراهيم خالد ممدوح، «الجرائم المعلوماتية»، دار الفكر الجامعي، الإسكندرية، مصر، طبعة أولى، مصر، ٢٠٠٩ م، ص ٨٨، محمد الشوا، «ثورة المعلومات و انعكاساتها على قانون العقوبات»، دار النهضة العربية، القاهرة، ١٩٩٤ م، ص ٥، «دعاوى الجرائم الإلكترونية و أدلة اثباتها في التشريعات العربية بين الواقع والمأمول» بحث صادر عن إدارة الدراسات والبحوث، ١٤٣٣ هـ، ص ٣، بحث يمكن تحميله من موقع http://www.fichier-pdf.fr.

كل عام، وأن الأضرار التي لحقت بقطاع الأعمال نتيجة سرقة الملكية الفكرية تتسبب في خسارة للأفراد بحوالي ١٦٠ مليار دولار[١٣]. و مما يزيد في خطورة الأمر أنه لا أحد في منأى عن الجريمة الإلكترونية، فعلى سبيل المثال تشهد منظومات وزارة الدفاع الأمريكية سنويا قرابة ٢٥٠ ألف هجوم، وحسب تقارير مجلس الكونجرس الأمريكي فإن ١٦٢ ألفا منها تنجح في الدخول إلى المنظومات المعلوماتية للبنتاغون[١٤]. ولم تسلم الشرطة الدولية «الإنتربول» من الهجمات الإلكترونية، فقد أقرَّ المدير التنفيذي لخدمات الشرطة في الإنتربول «جون ميشال لوبوتين» تعرّض «الإنتربول» إلى عدة اختراقات، من بينها هجمات من نوع «بوتنت» التي تسيطر على الأجهزة، كما تتعرّض حواسبها لمئة ألف هجوم يوميا في مواقعها الإلكترونية حول العالم[١٥]. وقد اتّسع مجال الجرائم الإلكترونية ليشمل دول الشرق الأوسط التي أصبحت من أكبر المستهدفين بالجريمة الإلكترونيَّة في العالم. و أسهمت الطفرة التي تعرفها المملكة العربية السعودية في مجال الإنترنت والتجارة الإلكترونية في جعلها هدفا محتملا للمجرمين المعلوماتيين، خاصة وأن نصف سكان المملكة يستعملون الإنترنت[١٦].

---

(١٣) مقال بعنوان «الجريمة الإلكترونية تُكلّف الاقتصاد العالمي ٤٤٥ مليار دولار سنويًا»، مقال صادر عن البوابة العربية للأخبار التقنية http://aitnews.com.

(١٤) رضا مثناني، «مجتمع المعلومات والتنمية، أية علاقة؟»، مركز النشر الجامعي، الطبعة الثالثة، تونس، ٢٠٠٩، ص ٤٧١.

(١٥) انظر : مجلة الاتصالات والعالم الرقمي، العدد ٢٥٢، ١٤٢٩/٥/١٣هـ ( مرجع ذكره ناصر بن محمد البقمي، جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية، الطبعة الأولى، الرياض، ١٤٣٠ هجري -٢٠٠٩ م، ص٢٣).

(١٦) بلغ عدد مستعملي الإنترنت في المملكة في ٢٠١٤/١٢/٣١ م ، ١٨,٣ مليون شخص (المصدر : www.internetworldstats.com).

و تبيّن هذه الأمثلة الواقعية تفاقم ظاهرة الإجـرام الإلكتروني الناجمة بالأساس على صعوبة مكافحتها بواسطة الطرق التقليدية. ويسعى البحث إلى استعراض الحلول الكفيلة بالتصدّي للجرائم الإلكترونية.

**مشكلة البحث:**

تشكّل خصوصية الجرائم الإلكترونية، الراجعة إلى طابعها التقني والدولي، حاجزا يحول دون مكافحتها بطريقة ناجحة. وتستدعي هذه الخصوصية حلولا مستحدثة وعملية تعتمد التقنيات الحديثة في علوم الحاسب، كما تتطلّب إصدار نصوص قانونية حديثة ورادعة تواكب تطور الإجرام الإلكتروني وتحول دون إفلات الجناة من العقاب.

**منهج وخطة البحث:**

اتّبعت المنهج الوصفي الاستقرائي التحليلي النقدي. وقد اعتمدت في البحث على الأنظمة والقوانين العربية والغربية الخاصة بمكافحة الجرائم الإلكترونية لاستجلاء الحلول الكفيلة بالتصدّي للجريمة الإلكترونية. وقد تعرّضت في مرحلة أولى إلى الصعوبات التي تقف أمام مكافحة الجريمة الإلكترونية (المبحث الأول)، ثم تعرّضت في مرحلة ثانية إلى الطرق الممكنة لمكافحة الجريمة الإلكترونية (المبحث الثاني).

# المبحث الأول
# صعوبة مكافحة الجريمة الإلكترونية

تثير الجريمة الإلكترونية عدة صعوبات تحول دون مكافحتها بشكل ناجع. وعادة ما تكون هذه الصعوبات مرتبطة بأطراف الجريمة الإلكترونية (المطلب الأول) أو بطبيعة الجريمة الإلكترونية (المطلب الثاني).

## المطلب الأول: الصعوبات المرتبطة بأطراف الجريمة الإلكترونية

يُقصد بأطراف الجريمة الإلكترونية مرتكب الجريمة (أ) والمجني عليه (ب).

### الصعوبات المرتبطة بمرتكب الجريمة الإلكترونية

على خلاف الجرائم التقليدية التي لا يتطلب ارتكابها في الغالب مهارات من نوع خاص، فإن الجريمة الإلكترونية تعتبر من جرائم أصحاب الياقات البيضاء[١٧]. وعادة ما يكون مرتكب هذه الجريمة شخصا مختصا في مجال الحاسب الآلي والإنترنت ويمتلك قدرا من الفطنة والذكاء يسمح له بخرق قواعد السلامة المعلوماتية واختراق أنظمة الحماية المعقدة. ويمكن تقسيم المجرمين المعلوماتيين إلى ثلاثة أصناف رئيسية: المخترقين، والمحترفين والحاقدين[١٨].

(١٧) انظر يوسف حسن يوسف، «الجرائم الدولية للإنترنت»، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١١، ص٧.

(١٨) هذا التقسيم أورده الكُتاب ( David Icov، Karl Seger and William Vonstresh ) في كتابهم «جرائم الكمبيوتر» (Computer crimes، O'Reilly and Associates، Inc، ١٩٩٥). انظر حسين الغافري، «السياسة الجنائية في مواجهة جرائم الإنترنت، دراسة مقارنة»، دار النهضة العربية، ٢٠٠٩، ص ٦٧.

المخترقون: يمكن تقسيمهم إلى صنفين[١٩]: المتسللون [٢٠] وهم «أشخاص يصلون بطرق غير قانونية إلى المعلومات في نظام حاسوبي، كما أنهم قد يبادرون بتعديل هذه المعلومات»[٢١] دون أن يعلم هؤلاء في الغالب نتيجة ما قاموا به من أعمال. المخربون[٢٢] و لا يقتصر دورهم على اختراق إجراءات الحماية بل يقومون بالعبث بالبيانات والمعلومات المخزنة على تلك الحاسبات والشبكات»[٢٣].

وسواء تعلق الأمر بالمتسلّلين أو بالمخرّبين فإن الوصول إليهم يبقى أمرا صعبا، وأحيانا شبه مستحيل إذا ما تحصّن المجرم الإلكتروني وراء اسم مستعار أو اعتمد حاسبا آليا لشخص آخر، بحيث يعجز الأمن على تعقبه. وعادة 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 يدينه[٢٤].

---

(١٩) ناصر بن محمد البقمي، جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية، الطبعة الأولى، الرياض، ١٤٣٠ هجري -٢٠٠٩ م، ص ٥.

(٢٠) يُطلق عليهم بالإنجليزية ( Hackers ) و هناك من يصفهم ب«القراصنة الهواة» (انظر مذكرة صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مذكرة ماجستير في القانون، جامعة مولود معمري، تزي وزو، ٢٠١٣، ص. ٣٣).

(٢١) ناصر بن محمد البقمي، نفس المرجع.

(٢٢) يُطلق عليهم بالإنجليزية (Crackers ) وهناك من يصفهم بالقراصنة المحترفين.

(٢٣) ناصر بن محمد البقمي، المرجع نفسه.

(٢٤) محمد عبد الرحيم سلطان العلماء،» جرائم الإنترنت والاحتساب عليها»، مؤتمر القانون والكمبيوتر و الإنترنت، منعقد من ١ إلى ٣ ماي ٢٠٠٠ م بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثالث، الطبعة الثالثة، ٢٠٠٤ م، ص٨٧.

المحترفون: يتميزون بالمهارة التقنية والتنظيم والقدرة على التخطيط للجريمة. وهم يشكّلون مصدر خطر كبير للأفراد، وتستهدف اعتداءاتهم تحقيق الكسب المادي السريع وغير المشروع. وقد تكون الغاية من ذلك مادية بحتة، كما قد تكون وسيلة لتحقيق أغراض سياسية أو إيديولوجية. وعادة ما يتطلّب إيقاف المجرمين المحترفين مجهودا كبيرا. على سبيل المثال، تطلّب إيقاف الهاكر الجزائري «حمزة بن دلاج» المُتّهم باختراق ٢١٧ بنكا عبر العالم، ثلاث سنوات من التّعقب من طرف مكتب التحقيقات الفيدرالي الأمريكي وتنسيقا دوليا حتى تمكنت قوات الأمن ببانكوك من إيقافه.

الحاقدون: يهدف أفراد هذه الطائفة إلى الانتقام والثأر من الغير. من ذلك قيام أحد الطلبة المختصين في المعلوماتية بلبنان بالتشهير بصديقته التي هجرته، حيث نزّل على موقعها الشخصي بشبكة الإنترنت، ودون علمها، صورا لها ذات طابع إباحي، مصحوبة بتعليقات نابية عن أخلاقها. وقد يكون الدافع من الجريمة الإلكترونية شن حرب معلوماتية ضد دولة أو نظام سياسي معادي عن طريق تدمير المواقع الحساسة أو الحيوية للدولة[٢٥].

نستنتج مما سبق، أن للمجرم المعلوماتي خصائص تُميّزه عن المجرم التقليدي[٢٦]. ويرمز إليها الأستاذ Parker بمصطلح SKRAM، وهي كلمة مركّبة يعني بها المهارة Skills والمعرفة Knowledge والوسيلة Ressources والسلطة

(٢٥) انظر حسين الغافري، «السياسة الجنائية في مواجهة جرائم الإنترنت، دراسة مقارنة»، دار النهضة العربية، ٢٠٠٩، ص ٧١.

(٢٦) لمزيد التفاصيل حول خصائص المجرم المعلوماتي، انظر عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة مركز دراسات الكوفة، العدد السابع، ٢٠٠٨ م، ص ١١٧.

Authority والباعث Motives[٢٧] . وبالفعل، فإن المجرم المعلوماتي يتمتّع بالمهارة والمعرفة الكافيتان لاختراق المواقع الإلكترونية وكسر حواجز الشفرة. ويُعد المجرم المعلوماتي في نظر الكثير من الباحثين من نوابغ المجرمين[٢٨]، نظرا لما يمتلكه من قدرة على التعامل مع وسائل التقنية الحديثة ومن إمكانية إخفاء الأدلة المادية للجريمة والتخفي وراء الأسماء المستعارة[٢٩]. وهو ما يجعل البعض يعتبر ما يقوم به المجرمون المعلوماتيون من أعراض «مرض النخبة»[٣٠]. وعادة ما يكون هؤلاء المجرمون من المتحصّلين على أعلى الشهادات العلمية، فهم إما طلبة أو بصدد إعداد أطروحات دكتوراه في علوم الحاسب[٣١]. ومن الأمثلة على ذلك ما قام به الطالب الأمريكي Murphy Ian حين عمد سنة ١٩٨١ م، بمعيّة أصدقائه، إلى استعمال خط هاتفي للدخول إلى ملفات سرّية مخزّنة في حاسوب تابع للحكومة الفيدرالية الأمريكية[٣٢].

---

(٢٧) نائلة عادل قورة، «جرائم الحاسب الآلي الاقتصادية»، ص ٥٦ ( مرجع ذكره ناصر بن محمد البقمي، جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية، الطبعة الأولى، الرياض، ١٤٣٠ هجري -٢٠٠٩ م، ص ٤٤).

(٢٨) انظر محمد قاسم أسعد الردفاني، .«تحقيقات الشرطة في مواجهة تحديات الجرائم السيبرانية»، المجلة العربية للدراسات الأمنية و التدريب، المجلد ٣٠، العدد ٦١، صفر ١٤٣٦ هـ، ص ١٦٦.

(٢٩) عبد الفتاح بيومي حجازي، «مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت»، دار الفكر الجامعي، القاهرة، مصر، ٢٠٠٦، ص ١٤.

(٣٠) انظر محمد رؤوف المراكشي، «القانون الجنائي للإعلامية»، محاضرة ألقيت في إطار الجمعية التونسية للقانون الجنائي، مجلة القضاء والتشريع، عدد ٣ لسنة ١٩٨٥ م، ص ٤٠.

(٣١) انظر الهاشمي الكسراوي، «الجريمة المعلوماتية»، مجلة القضاء والتشريع، العدد ٧ لسنة ٢٠٠٦، ص ٢٧، انظر كذلك عادل يوسف عبد النبي الشكري، «الجريمة المعلوماتية و أزمة الشرعية الجزائية»، مركز دراسات الكوفة، ٢٠٠٨ م، ص ١١٦.

(٣٢) Frédéric Jérôme Pansier et Emmanuel Jez. « La criminalité sur internet ». « Que sais-je ? ». 2001. p. 100.

ورغم أن دوافع المجرم المعلوماتي لا تختلف عن دوافع المجرمين عامة، إلا أن مكمن الخطورة يتمثّل أحيانا في أن المجرم المعلوماتي لا يرى أن فعله يمثّل فعلا إجراميا، وإنما يُعد من قبيل إثبات الذات وتحدّي تقنية المعلومات(٣٣).

## الصعوبات المرتبطة بضحايا الجر يمة الإلكترونية

تتميّز الجريمة الإلكترونية بطابعها السرّي، إذ لا تلجأ الضحية في عديد الحالات إلى تتبع المجرم إما لعدم تفطنها إلى حدوث الجريمة أو لاقتناعها بعدم جدوى التتبع لصعوبة ضبط الجاني أو خوفا على سمعتها إذا تعلق الأمر بجرائم ابتزاز أو جرائم تستهدف مؤسسة أمنية أو بنكية. وتتكتّم البنوك في الغالب على هذه الجرائم رغم ما تسببه لها من خسائر فادحة، خوفا من زعزعة ثقة عملائها فيها وخشية من سحبهم لأرصدتهم البنكية، فلا أحد يرغب في إيداع أمواله في بنك يتعرض للسرقة. وقد يُفسّر هذا التكتم كذلك بخوف المؤسسات الأمنية والبنكية من إمكانية المساءلة القانونية من أجل التقصير في حماية المعطيات السرية التي تعرّضت للسرقة أو التخريب. ويذهب البعض إلى الحديث عن وجود «قانون الصمت» في مجال الجريمة الإلكترونية، ذلك أن الشكاوى التي تقدّم إلى المحاكم بخصوص الجرائم المعلوماتية لا تتعدّى نسبة ١٠ ٪ من جملة الجرائم المقترفة والتي تفطّنت إليها المؤسسات المعتدى عليها. ويجعل هذا التكتم تقدير الأضرار الناجمة عن الجريمة الإلكترونية أمرا صعبا.

(٣٣) انظر: ناصر بن محمد البقمي، جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية، الطبعة الأولى، الرياض، ١٤٣٠ هجري-٢٠٠٩ م، ص ٤٦).

## 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) وعدم قدرة نصوص التجريم التقليدية على مسايرة تطورها (ج).

### أ–الصبغة العالمية للجر يمة الإلكترونية المرتكبة عبر الإنترنت

إن الصبغة العالمية للجريمة الإلكترونية المرتكبة عبر الإنترنت، تجعل من مكافحتها بطريقة ناجعة وفعّالة أمرا صعبا[٣٤]، فهي ليست مقصورة على منطقة أو دولة معينة وإنما هي جريمة عابرة للحدود[٣٥]، أدت إلى ما يمكن تسميته بعولمة الجريمة[٣٦]. وغالبا ما يستغل مرتكبو الجرائم الإلكترونية هذه الخاصية فيستهدفون مواطنين من دولة أجنبية ليجعلوا من تتبعهم ومحاكمتهم أمرا صعبا. ففي الجرائم المتعلقة بقرصنة البطاقات البنكية مثلا يعمد القراصنة إلى قرصنة بطاقات مواطني دولة أخرى ثم يقومون ببيع هذه البطاقات عبر الإنترنت إلى أشخاص مقيمين في دولة ثالثة لا ينتمي إليها القراصنة أو ضحاياهم، مما يشتت مجهودات وحدات الأمن داخل هذه الدول التي يتعين عليها التنسيق على مستوى ثلاثي. ولا تقتصر

(٣٤) حول الصبغة العالمية للجريمة الإلكترونية انظر : مذكرة صغير يوسف، «الجريمة المرتكبة عبر الإنترنت»، مذكرة ماجستير في القانون، جامعة مولود معمري، تزي وزو، ٢٠١٣، ص١٦.

(٣٥) انظر محمد علي سالم و حسون عبيد هجيج، «الجريمة المعلوماتية»، مجلة جامعة بابل، العلوم الإنسانية، المجلد ١٤، العدد ، ٢٠٠٧، ص ٩٢. .

(٣٦) انظر محمد قاسم أحمد الردفاني، «تحقيقات الشرطة في مواجهة تحديات الجرائم السيبرانية»، المجلة العربية للدراسات الأمنية و التدريب، المجلّد ٣٠، العدد ٦١، صفر ١٤٣٦ هـ، ص ١٧١.

الصعوبة على هذا المجال فحسب، فحتى إذا ما تعهد القضاء بالجريمة المعلوماتية العابرة للحدود وأصدر حكما بالإدانة، فإنه لا يمكن إجبار الدولة التي ارتكبت فيها الجريمة أو احتمى بها المجرم على تنفيذ الحكم، احتراما لسيادة هذه الدولة(٣٧)، وبالأخص إذا كان قانون هذه الدولة لا يجرّم الفعل موضوع الإدانة. ويُطرح هنا مشكل تصادم الصبغة العالمية للإنترنت مع مبدأ إقليمية النص الجزائي. وينص هذا المبدأ على أن قواعد القانون الجنائي لا تطبّق إلا في حدود الإقليم الخاضع لسيادة الدولة(٣٨)». وهو يُعتبر نتيجة طبيعية لتطبيق مبدأ شرعية الجرائم والعقوبات(٣٩). ويكمن الإشكال في أن القوانين الجزائية تختلف من بلد إلى آخر بشكل كبير، ففي حين يسمح بلد مثل هولندا بتعاطي المخدرات فإن سائر بلدان العالم تجرّمه، وفي حين تُجيز عدة بلدان غربيّة القمار فإن دولا أخرى تمنعه، وينطبق نفس الأمر على مواقع الإنترنت الإباحية(٤٠).

وقد طرح إشكال اختلاف النصوص التجريمية بين الدول في القضية المتعلقة بمحرك البحث «Yahoo»(٤١)، ففي ٢١ / ١١ / ٢٠٠٠م أصدرت المحكمة الابتدائية بباريس قرارا يلزم شركة «ياهو» بإيجاد حلول فنية تمنع

(٣٧) أعلنت الجمعية العامة للأمم المتحدة منذ سنة ١٩٦٥ في قرارها عدد ٢١٣١ مبدأ الاستقلالية الدستورية: «كل دولة لها الحق غير القابل للتصرف في اختيار نظامها السياسي (...) من دون أي شكل من أشكال التدخل من أي دولة «.

(٣٨) فرج القصيّر، القانون الجنائي العام، مركز النشر الجامعي، ٢٠٠٦، ص ٤٩.

(٣٩) فرج القصّير، المرجع السابق.

(٤٠) انظر: عبد الفتاح بيومي حجازي، «الأحداث و الإنترنت»، ٢٠٠٢، ص ٣١٤.

(٤١) انظر: مقال الهاشمي الكسراوي، «الجريمة المعلوماتية»، مجلة القضاء والتشريع، العدد ٧ لسنة ٢٠٠٦، ص ٢١.

مستعملي الإنترنت بفرنسا من النفاذ إلى موقع البيع بالمزاد العلني الذي تعرض فيه أغراض وبضائع لها علاقة بالنازية وهو أمر يجرّمه القانون الفرنسي[٤٢]. وقد كان القرار مُرفقا بتقرير صادر عن هيئة خبراء يبيّن الطريقة الفنيّة التي يمكن بها تنفيذ هذا القرار. رغم ذلك فقد رفض القضاء الأمريكي قبول هذا القرار لمخالفته للفصل الأول من الدستور الأمريكي الذي ينص على حرية التعبير[٤٣]. نفس الإشكال طرح بخصوص الفيلم الأمريكي «براءة المسلمين» الذي حاول تشويه صورة الرسول صلّى الله عليه وسلّم[٤٤] والذي أدّى إلى تظاهر آلاف المسلمين حول العالم احتجاجا على ما ورد به من إساءة للإسلام.

### ب- صعوبة إثبات الجريمة الإلكترونية

صاحب ظهور الحاسوب وشبكة الإنترنت تحديات جديدة للقانون الجنائي بشقّيه الموضوعي والإجرائي مما يُفقد قانون الإجراءات الجنائية أهميته وفعاليته[٤٥]. ويزداد الأمر صعوبة مع جمع الجريمة الإلكترونية بين سرعة الانتشار وصعوبة الإثبات. فإذا كانت سرعة الانتشار تعود إلى الصبغة العالمية للجريمة الإلكترونية، فإن صعوبة إثباتها راجع إلى صبغتها اللامادية التي تجعل من محو الأدلة الجزائية أمرا سهلا. يُمكن للمجرم الإلكتروني في ضغطة زر محو مئات الآلاف من البيانات من الحاسب الآلي، كما أن بإمكانه

(٤٢) يجرّم الفصل R ٦٤٥-١ من المجلة الجزائية الفرنسية مجرد عرض الأشياء المتعلقة بجرائم ضد الإنسانية.

(٤٣) المحكمة الفدرالية بكاليفورنيا، ٧ / ١١/ ٢٠٠١م.

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

(٤٥) انظر محمد فتحي، «تفتيش شبكة الإنترنت لضبط جرائم الاعتداء على الآداب العامة»، المركز القومي للإصدارات القانونية، ٢٠١٢ م، ص ٥٠٤.

عدم تخزينها وعدم معالجتها على حاسبه الشخصي، خصوصا مع انتشار الحوسبة السحابية(٤٦). وقد طُرح الإشكال أمام القضاء الفرنسي بالنسبة إلى الملفات الوقتية Temporary files المخزّنة في الحاسب الآلي. وقد اعتبرت محكمة النقض الفرنسية أنها لا تشكّل دليلا كافيا على ارتكاب الجريمة طالما أن تسجيل هذه الملفات يتم تلقائيا ولا يُعبّر عن رغبة واضحة في تنزيل الملفات المحمية بحقوق التأليف(٤٧). وبذلك تُشكّل خصوصية الدليل الرقمي تحدّيا إضافيا أمام الباحث الجنائي يجعل من إثبات الجريمة المعلوماتية أمرا صعبا(٤٨).

وقد يعمد بعض الجناة إلى تشفير المعطيات المجرّمة فيستحيل 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 وتبادلها في شكل صور فوتوغرافية عادية، وهي تقنية تحمل اسم « steganography »(٤٩).

---

(٤٦) الحوسبة السحابية (بالإنجليزية: Cloud computing) هي مصطلح يشير الي المصادر والأنظمة الحاسوبية المتوافرة 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 تُبَسّطُ وتتجاهل الكثير من التفاصيل والعمليات الداخلية.

(٤٧) Christiane Féral-Schuhl. Cyberdroit. le droit l'épreuve d'internet. Dalloz. 2008. p. 906.

(٤٨) انظر محمد فتحي، «تفتيش شبكة الإنترنت لضبط جرائم الاعتداء على الآداب العامة»، المركز القومي للإصدارات القانونية، ٢٠١٢ م، ص ٤٠٧.

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

وتمثّل الفضاءات العامة والمقاهي التي يمكن فيها استغلال خدمة الإنترنت بدون تحديد مسبق لهوية المستفيد صعوبة إضافية تقف أمام تحديد الجاني في صورة ارتكابه لجريمة عن طريق الإنترنت المخصصة للعموم.

### ج–عدم قدرة نصوص التجريم التقليدية على مسايرة تطوّر الجر يمة الإلكترونية

يُعد التطور السريع في الميدان المعلوماتي من أهم العوائق التي تحول دون مكافحة الجريمة الإلكترونية بطريقة ناجعة، ففي كل يوم تظهر تقنيات جديدة للقرصنة والتحايل والاختراق بشكل يصعب مجاراته من طرف السلطة التشريعية(٥٠)، جعلنا نعيش فيما يمكن أن نسمّيه بالطوفان الرقمي(٥١). وفي المقابل فإن أكثر دول العالم «تعتمد في مواجهة جرائم المعلوماتية على التشريعات العقابية التي وجدت لمواجهة الجرائم التقليدية المتعارف عليها، وهو ما أدّى إلى قصور في الحماية الجنائية لعدم قدرتها على استيعاب هذه الجرائم ضمن النصوص القائمة»(٥٢). وقد حاولت

---

(٥٠) 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.
أنظر التقرير الصادر عن الاتحاد الدولي للاتصالات :
Comprendre la cybercriminalité : guide pour les pays en développement. 2009. p. 93. Rapport téléchargeable sur internet)).

(٥١) انظر كتاب «الطوفان الرقمي»، هال أبلسون وهاري لويسوكين ليدين، ترجمة أشرف عامر ، نشر إلكتروني لمؤسسة هنداوي.

(٥٢) ناصر بن محمد البقمي، جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية، الطبعة الأولى، الرياض، ١٤٣٠ هـ-٢٠٠٩ م، ص٣٢.

الدول العربية التصدي للجريمة الإلكترونية منذ سنة ١٩٩٩م، تاريخ صدور أول قانون عربي يتطرّق إلى الجريمة الإلكترونية، وهو القانون التونسي المؤرخ في ٢ / ٨/ ١٩٩٩ م(٥٣) الذي أضاف إلى المجلة الجزائية التونسية فصولا خاصة بالجريمة الإلكترونية، تلاه القانون العماني(٥٤) والإماراتي(٥٥) والسعودي(٥٦). غير أن هذه النصوص، على أهميتها، تحمل في طيّاتها ثغرات ناجمة عن التطوّر السريع للجريمة المعلوماتية.

وتعجز السلطات القضائية أحيانا عن ردع المتهمين، عند تعهدها ببعض القضايا المرتبطة بالجريمة الإلكترونية، احتراما لمبدأ الشرعية(٥٧). ويحول هذا المبدأ دون محاكمة الشخص في غياب نص صريح يجرّم الفعل الذي ارتكبه، وهو ما يسمح لبعض مرتكبي الجريمة الإلكترونية من الإفلات من العقاب. وقد طرح هذا الإشكال في بعض الدول العربية، على غرار ما حصل في دولة الإمارات العربية المتحدة في منتصف سنة ٢٠٠٠ م، حين تمكّن شاب بريطاني من اختراق شبكة اتصالات إماراتية والإضرار بشبكة الإنترنت. و تبيّن عند التحقيق معه عدم تجريم النصوص الجزائية في ذلك الوقت لهذه الأفعال باستثناء بعض الفصول الموجودة في قانون الاتصالات

(٥٣) القانون عدد ٩٨ لسنة ١٩٩٩ المؤرخ في ٢/ ٨ / ١٩٩٩م.

(٥٤) المرسوم السلطاني رقم ٢٠٠١/٧٢ م.

(٥٥) القانون الاتحادي رقم ٢ لسنة ٢٠٠٦م.

(٥٦) صدر المرسوم الملكي رقم م/١٧ في ٨/ ٣/ ١٤٢٨هجري.

(٥٧) حول مبدأ الشرعية، انظر : د. خالد بن عبد الله الشافي، مبادئ النظام الدستوري في المملكة العربية السعودية، ٢٠١٢ م، ص ١٨٣، انظر كذلك : عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة مركز دراسات الكوفة، العدد السابع، ٢٠٠٨ م، ص ١١٨.

والتي تضمّنت عقوبات بسيطة غير رادعة[٥٨].

وقد وُجد الإشكال نفسه في القضية الصادرة عن محكمة التعقيب التونسية بتاريخ ٢٤ / ٤ / ٢٠٠٢ [٥٩]. وتتمثل وقائع القضية في قيام المتهم بفتح رموز سرية لبطاقات رقمية أصلية معدّة لقراءة قنوات تلفزيّة مشفّرة قام بعدها بشحن بطاقات رقمية عذراء بتلك الرموز السرية المستنسخة. وبعد ذلك باعها بواسطة متّهم ثانٍ. قامت النيابة العمومية بإحالته على المحكمة الجزائية بموجب الفصل ١٩٩ من المجلة الجزائية بتهمة «افتعال وثيقة معلوماتية ومسك واستعمال تلك الوثيقة» إلا أن محكمة البداية قضت في شأنه بعدم سماع الدعوى لأن الفصل المذكور لم يجرّم فعل الصنع والافتعال، كما تأيّد هذا الحكم لدى محكمة الاستئناف ببنزرت، فتعقبته النيابة العمومية لدى محكمة التعقيب طالبة النقض والإحالة. لكن محكمة التعقيب رفضت مطلب التعقيب أصلا معتبرة أن «المشرّع لم يجرّم افتعال مثل هذه البطاقات وبالتالي لم يحدّد أية عقوبة على كل من يعمد إلى تقليد أو افتعال أية بطاقة إلكترونية أو معلوماتية... ومن البديهي الوقوف عند عبارات النص الجزائي وعدم التوسّع فيه عملا بالمبدأ القائل بأن تأويل النص الجزائي يكون ضيقا وإن حصل يكون لصالح المتّهم».

وبذلك يُمثّل مبدأ التأويل الضيق للقانون الجزائي عائقا إضافيا أمام اعتماد النصوص المنطبقة على الجرائم التقليدية في مكافحة الجريمة الإلكترونية.

---

(٥٨) انظر عبد الفتاح بيومي حجازي، «الأحداث و الإنترنت»، ٢٠٠٢، ص ٢٩٩.

(٥٩) قرار تعقيبي عدد ١٦٠٦٥ بتاريخ ٢٤/٤/ ٢٠٠٤ منشور بمجلة القضاء والتشريع، ديسمبر ٢٠٠٤، ص ١٦٥.

ورغم ذلك نشير إلى أن الشريعة الإسلامية، التي تُعدُّ دستور البلاد في المملكة العربية السعودية[٦٠]، تسمح للقاضي بسلطة واسعة في تقدير العقوبة، حتى في غياب نص تجريمي صريح، وذلك عن طريق التعزير. والتعزير[٦١] هو «تأديب عن ذنوب لم تشرّع فيها الحدود»[٦٢]. 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»[٦٣]. ويمكن القول بأن التعزير يسمح بتجاوز الثغرات التي قد تنشأ نتيجة التطبيق الصارم لمبدأ التأويل الضيق للنص الجزائي. ولكن ذلك لا يعني عدم خضوعه إلى ضوابط موضوعية[٦٤] تضمن تحقيق العدل في تطبيق العقوبة التعزيرية[٦٥]. وقد لجأ القضاء

(٦٠) جاء بالمادة الأولى من النظام الأساسي للحكم «المملكة العربية السعودية، دولة إسلامية، ذات سيادة تامة، دينها الإسلام، ودستورها كتاب الله تعالى وسنة رسوله صلى الله عليه وسلم. ولغتها هي اللغة العربية، وعاصمتها مدينة الرياض».

(٦١) حول التعزير، انظر : سليم محمد النجار، سلطة القاضي في تقدير العقوبات التعزيرية، ماجستير في القضاء الشرعي، كلية الشريعة والقانون بالجامعة الإسلامية بغزة، ١٤٢٨ هـ، ٢٠٠٧ م، انظر كذلك : صباح بنت صالح فلمبان، التعزير بأخذ المال، مجلة العدل، صادرة عن وزارة العدل السعودية، العدد ٦١، محرم ١٣٥ هـ، ص ٧٧.

(٦٢) الأحكام السلطانية، ص ٢٠٥، بدائع الصنائع ج ٧، ص ٦٣، أسنى المطالب، ج ٧، ص ١٦١.

(٦٣) عبد القادر عودة، «التشريع الجنائي الإسلامي مقارنا بالقانون الوضعي»، الجزء الأول، دار الحديث، القاهرة، ص ١٠٢.

(٦٤) ذكر الشيخ عبد الله بن محمد آل خنين ١٣ ضابطا يتعيّن احترامه عند تقدير العقوبة التعزيرية. انظر بحثه «ضوابط تقدير العقوبة التعزيرية»، مجلة القضائية، العدد الأول، محرم ١٤٣٢ هجري، ص ٥٦.

(٦٥) انظر : عبد الله بن محمد آل خنين، «ضوابط تقدير العقوبة التعزيرية»، مجلة القضائية، العدد الأول، محرم ١٤٣٢ هجري، ص ٥٦.

السعودي قبل صدور نظام مكافحة جرائم المعلوماتية إلى اعتماد التعزير في القضية الجزائية رقم ٩ / ١٦الصادرة عن المحكمة المستعجلة بالرياض في ٥ / ١ / ١٤٢٣هجري[٦٦]، حيث قضى بجلد شاب مئة وخمسين جلدة تعزيرا إضافة إلى سجنه أحد عشر شهرا 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 بالغاط في ٢٤ / ٤ / ١٤٣٥هجري[٦٧]. وتتمثل وقائع القضية في ضبط شاب بأحد المكتبات العامة، التي تُوفّر خدمة الإنترنت للعموم مجّانا بصدد تنزيل صور ومقاطع إباحية على حاسبه الآلي المحمول عن طريق الإنترنت اللاسلكي. ورغم أن المتهم تمت إحالته من طرف الادعاء العام بناءً على المادة السادسة من نظام مكافحة جرائم المعلوماتية [٦٨] إلا أن القاضي المتعهّد بالقضية اعتبر أن الجريمة المرتكبة ليست جريمة معلوماتية. وقد أُدين المتهم بالاستناد لأحكام الشريعة، حيث اعتبر القاضي أن «ما قام به المدعى

(٦٦) انظر : مدوّنة الأحكام القضائية ، الإصدار الثالث، سنة ١٤٢٩ هجري (٢٠٠٨ م) ، ص ١٥٦. قرار رقم ٣٥٢٢١٤٨١ صادر بتاريخ ٢٤/ ٤/ ١٤٣٥ هجري عن المحكمة العامة بمحافظة الغاط، قرار غير منشور.

(٦٧) قرار رقم ٣٥٢٢١٤٨١ صادر بتاريخ ٢٤/ ٤/ ١٤٣٥ هجري عن المحكمة العامة بمحافظة الغاط، قرار غير منشور.

(٦٨) 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 أيا من الجرائم المعلوماتية الآتية : ١. 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...»

عليه أمر محرّم وحيث إن الشرع أمر بغض البصر ونظرا لكون تخزين مثل هذه المقاطع وسيلة إلى انتشار الرذيلة ولما لها من التأثير السلبي على الفرد والمجتمع ونظرا لكون هذه الجريمة تستدعي الردع والزجر لمرتكبها»[٦٩] فقد أدين المتهم من أجل تخزين المقاطع الإباحية بجهاز الحاسب الآلي الخاص به وسجنه مدة شهر وجلده ثلاثين جلدة في مكان عام وإشهار اسمه و جريمته. وقد يكون استبعاد القاضي لأحكام المادة السادسة، التي كان بالإمكان اعتمادها في هذه القضية، يجد تبريره في صرامة العقاب المقرر فيها، والذي يصل إلى خمس سنوات سجنا.

(٦٩) انظر القرار القضائي رقم ٣٥٢٢١٤٨١ صادر بتاريخ ٢٤/ ٤/ ١٤٣٥ هجري عن المحكمة العامة بمحافظة الغاط، قرار غير منشور.

# المبحث الثاني:
# طرق مكافحة الجريمة الإلكترونية

الأصل أن تكون مكافحة الجريمة باعتماد الطرق القانونية (المطلب الثاني)، لكن خصوصية الجريمة الإلكترونية، المتمثّلة أساسا في صبغتها العالمية وقدرة مرتكبها على التخفّي والإفلات من العقاب، تستدعي اعتماد طرق مكافحة تقنية (المطلب الأول).

## المطلب الأول: الطرق التقنية

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

### أ–الطرق التقنية العامة

تتمثّل الحماية التقنية العامة أساسا في اعتماد نظام الترشيح والحجب (١) إضافة إلى اعتماد تقنية التشفير (٢).

**اعتماد نظام الترشيح والحجب**

نظام الترشيح والحجب هو «أسلوب لحجب صفحات معينة يمكن أن تكون مؤذية أو عدوانية أو إباحية بالنسبة إلى مستخدم الإنترنت، فإذا حاول المستخدم الوصول إلى صفحة محجوبة ظهرت له رسالة تبلغه أن الوصول إلى هذه الصفحة غير مسموح به»[٧٠]. هذا النظام معمول به في المملكة

(٧٠) ناصر بن محمد البقمي، «جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية»، الطبعة الأولى، الرياض، ١٤٣٠ هجري-٢٠٠٩ م، ص ١٧٧.

العربية السعودية وقد تم إعداده من قبل «وحدة خدمات الإنترنت» التابعة إلى مدينة الملك عبد العزيز الخاصة بالعلوم والتقنية[٧١]. وقد أوكلت منذ سنة ٢٠٠٦م مهمة الإشراف على الترشيح إلى «هيئة الاتصالات وتقنية المعلومات»[٧٢]. ويتم الترشيح من قبل مزوّدي خدمات المعطيات على أجهزة الخوادم لديهم. ورغم فعالية نظام الترشيح والحجب في منع النفاذ إلى المواقع الإباحية[٧٣] ومواقع المخدرات والميسر إلا أن كفاءتها تبقى محدودة بالنسبة إلى المواقع السياسية والدينية[٧٤]. من جهة أخرى، فإنه

(٧١) ناصر بن محمد البقمي، المرجع نفسه.

(٧٢) يوضّح موقع الإنترنت الخاص بهيئة الاتصالات وتقنية المعلومات كيف تتم خدمة الترشيح : « تقوم هيئة الاتصالات وتقنية المعلومات بتقديم خدمة ترشيح محتوى الإنترنت في المملكة، وذلك من خلال وضع الضوابط والمتطلبات الخاصة بترشيح خدمات الإنترنت بالتنسيق مع اللجنة الأمنية الدائمة للإنترنت، كما تقوم بتوفير القوائم الخاصة بالمواقع المحجوبة يومياً لمزودي خدمة المعطيات، في حين يتولى مزودو خدمة المعطيات مسئولية 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 إحداهما تجارية تضم أكثر من ٩٠ 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 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)

(٧٣) حسب موقع هيئة الاتصالات وتقنية المعلومات، تشكّل المواقع الإباحية أكثر من ٩٢ ٪ من القائمة الخاصة بالترشيح والحجب.

(٧٤) قامت أربع جامعات أجنبية (جامعة هارفارد و كامبريدج و تورنتو و أكسفورد) بدراسة نظام الترشيح السعودي و بيّنت نتائجها كفاءة ترشيح المواقع الإباحية بنسبة ٩٨ ٪ و مواقع المخدرات بنسبة ٦٨ ٪و مواقع اليسر بنسبة ٩٣ ٪ و المواقع السياسية بنسبة ٣ ٪و المواقع الخاصة بالكيان الصهيوني بنسبة ٢ ٪ و المواقع الدينية بنسبة ١ ٪. (انظر: ناصر من محمد البقمي، «جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية»، المرجع السابق، ص ١٧٨).

بإمكان الأشخاص المتمكّنين من التقنيات المعلوماتية التخفي والنفاذ إلى المواقع المعنية بالحجب عن طريق «البروكسي»[٧٥]. وعلى هذا الأساس، يعتبر البعض أن التوفيق بين الرقابة وسرعة تدفق المعلومات يغدو اليوم مهمة عبثية[٧٦]. وقد كتب «بيل غيتس» سنة ١٩٩٥م: «لكي تحقق الوصول الكامل إلى الإنترنت وتحافظ في الوقت ذاته على الرقابة، يتعيّن عليك في أغلب الأحوال أن تعيّن لكل مستخدم شخصا يُطل عليه»[٧٧].

ورغم الانتقادات التي يمكن أن توّجه لنظام الترشيح والحجب والمتمثّلة أساسا في تقييده لحرية الإبحار عبر الإنترنت ومحدودية نجاعته بالنسبة لبعض المواقع، إلا أنه يبقى ضروريا لحماية الشباب وخاصة القصر من المواقع الإباحية ومواقع المخدرات والإرهاب. وتشير دراسات أمريكية إلى أن المدمنين على المواقع الإباحية تتغير لديهم المفاهيم حول ما يعتبرونه مقبولا اجتماعيا. وقد انتهت دراسة لضباط الشرطة الأمريكيين حول ظواهر الاغتصاب والقتل الجماعي إلى أن تداول

---

(٧٥) «البروكسي» Proxy 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، فإن 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 عمومًا باستخدام PHP أو CGI لتتمكن من العمل كوحدة خدمة بروكسي. وتُستخدم هذه الأنواع من البروكسي عادةً للدخول على مواقع الويب التي يتم حجبها.

(٧٦) انظر : سمير إبراهيم حسن، «الثورة المعلوماتية، عواقبها وآفاقها»، مجلة جامعة دمشق، المجلد ١٨، العدد الأول، ٢٠٠٢، ص ٢٢٠.

(٧٧) بيل غيتس، «المعلوماتية بعد الإنترنت (طريق المستقبل)»، ترجمة عبد السلام رضوان، سلسلة عالم المعرفة، الكويت، آذار ١٩٩٨، ص ٣٧٦.

المواد الإباحية سمة معروفة وموحّدة لدى العديد من القتلة والمغتصبين. وقد بيّن استجواب قام به مكتب التحقيقات الفيدرالي الأمريكي لأربعة وعشرين مجرما في السجون الأمريكية، أدينوا من أجل جرائم اغتصاب وقتل، أن ٨١٪ منهم كانوا مدمنين على المواد الإباحية وكانت جرائمهم تطبيقا لما شاهدوه من إباحية(٧٨). وقد كان من بين هؤلاء المجرمين السفّاح «أرتور جاري بيشوب» Arthur Gary Bishop الذي أدين من أجل الاعتداء على خمسة أطفال وتشويههم وقتلهم، والذي صرّح قبل إعدامه بأنه «لو أن مواد الدعارة والإباحية قد منعت مني في صباي، لم يكن شغفي بالجنس والشذوذ والإجرام ليتحقق»(٧٩).

وتجدر الإشارة إلى قيام أستراليا منذ سنة ١٩٩٩م بتكليف هيئة مستقلة(٨٠) بمراقبة الإنترنت. وقد اعتمدت هذه الهيئة قائمة سوداء في المواقع الأسترالية المخالفة للقانون التي يتعيّن على مزوّدي الاستضافة إغلاقها مثل المواقع الإباحية التي تستهدف الأطفال والمواقع العنصرية، إضافة إلى المواقع التي تخرق قواعد الملكية الفكرية. وفي السياق نفسه صدر سنة ٢٠٠٠م في الولايات المتحدة الأمريكية قانون حماية الأطفال « Children's Internet Protection Act » يفرض على المكتبات العامة استخدام مرشّحات تحجب المواقع الإباحية حتى تكون مستحقة للدعم الفيدرالي(٨١) كما التزمت عدة

(٧٨) انظر : محمد فتحي، «تفتيش شبكة الإنترنت لضبط جرائم الاعتداء على الآداب العامة»، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١٢ م، ص ٧٨.

(٧٩) انظر : محمد فتحي، نفس المرجع.

(٨٠) Australian Broadcasting Autority

(٨١) انظر : محمد فتحي، «تفتيش شبكة الإنترنت لضبط جرائم الاعتداء على الآداب العامة»، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١٢ م، ص ١٧٣.

محرّكات بحث ألمانية منذ بداية سنة ٢٠٠٥ م، طوعا بقائمة سوداء تشمل المواقع المخافة للقانون الألماني[٨٢].

### ٢–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[٨٣]». وتعتبر تقنية التشفير من أنجع الوسائل للحفاظ على سرّية المعلومات المتبادلة إلكترونيا وعلى سلامتها من التغيير. وهي «تقنية تستخدم لحماية سرّية الوثائق الإلكترونية استنادا إلى نظام العد العشري الذي يسمح بجعل البيانات غير مفهومة بالنسبة لمن لا يملك المفتاح اللازم لفك الرموز[٨٤]». وبذلك يمكن القول بأن «التشفير لا يخرج عن كونه كتابة بالرموز[٨٥]». وكلّما كانت هذه الرموز معقّدة كلما صعب اختراقها. وتضمن تقنية التشفير أمن مواقع الإنترنت الحسّاسة كتلك التي تمسّ الأمن القومي أو التجارة والمبادلات المالية الإلكترونية. وقد أثبت الواقع العملي أن تقنية التشفير تكفل درجة عالية من تحقيق السلامة المعلوماتية بما جعلها الحل الأمثل لقطع الطريق أمام القرصنة المعلوماتية[٨٦].

---

(٨٢) انظر: Wiem YAAKOUB. La cybercriminalité. mémoire pour l'obtention du DEA en droit privé. Sfax. 2009. p. 99.

(٨٣) هذا التعريف اعتمده التشريع التونسي في الفصل ٢ من القانون عدد ٨٣ لسنة ٢٠٠٠ المؤرخ في ٢٠٠٠/٠٨/٩ المتعلق بالمبادلات والتجارة الإلكترونية.

(٨٤) هذا التعريف اعتمده التشريع التونسي في القانون النموذجي المتعلق بتبادل الوثائق الإلكترونية.

(٨٥) المنصف زغاب، «الوثيقة الإلكترونية»، مجلة القضاء والتشريع، ديسمبر ٢٠٠٥، ص ١٣٩.

(٨٦) المنصف زغاب، المرجع السابق، ص ١٤٠.

ويجب التأكيد على أن التشفير قد يُستعمل لغايات منافية للتي جُعل من أجلها، كأن يتبادل قراصنة معلوماتيون معطيات مشفّرة فيما بينهم لتفادي تعقّبهم من طرف السلطات الأمنية. وقد يجعل نظام التشفير إقامة الدليل على ارتكاب الجريمة أمرا مستحيلا. وهذا ما حدث في قضية «fawrisson» حيث نشرت على صفحات الإنترنت رسائل عنصرية ومضادة لليهودية تحمل اسم Robert Fawrisson . ورغم أن الموقع الإلكتروني الذي صدرت منه الرسائل قد تم إيواؤه في الولايات المتحدة الأمريكية، إلا أن المحكمة الأمريكية المتعهدة بالقضية لم تتمكّن من إقامة الدليل على أن المتهم هو صاحب الرسالة المجرّمة(٨٧).

وخوفا من استعمال التشفير لتبادل المعلومات بين المجرمين على الإنترنت، فقد قيّدت عدّة دول استعمال خدمات التشفير عبر شبكات الاتصالات بشروط وإجراءات مضبوطة(٨٨)، فقد نصّت المادة (٩) من مجلة الاتصالات التونسية على أن «تُضبط بأمر شروط وإجراءات استعمال وسائل أو خدمات التشفير عبر شبكات الاتصالات وكذلك شروط تعاطي الأنشطة ذات العلاقة». وقد اشترط القانون الفرنسي من جهته أن يخضع التشفير إلى رخصة إدارية أو القيام بتصريح إداري، بما يسمح بعدم استعمال تقنية التشفير في أغراض إجرامية(٨٩).

---

(٨٧) انظر محمد فتحي، « تفتيش شبكة الإنترنت لضبط جرائم الاعتداء على الآداب العامة»، ٢٠١٢المصدر القومي للإصدارات القانونية، القاهرة، ٢٠١٢، ص ١٧٨.

(٨٨) انظر محمد العسكري، «خصوصيات الإثبات في الجرائم المعلوماتية»، مجلة القضاء والتشريع، ٢٠٠٥م، العدد ٧، ص١٧٩.

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

### ب–الحماية التقنية الخاصة

الحماية التقنية الخاصة هي الوسائل التقنية الحمائية التي يمكن للخواص اللجوء إليها من أجل التقليل من مخاطر الاختراق كاقتناء برمجيات الوقاية من الفيروسات الإلكترونية واعتماد جدار حماية ناريFirewall [٩٠]. وعلى مستخدم الحاسب الآلي تحديث جهازه بصفة دورية وعدم فتح رسائل البريد المشكوك فيها وتفادي تنزيل الملفات من المواقع المريبة. ولم يعد مجال الحماية يقتصر 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 مخزّنة في ذاكرتها.

وتتطلّب مكافحة الجريمة الإلكترونية تثقيف مستخدمي الإنترنت وتوعيتهم في مجال السلامة المعلوماتية لكي يتجنبوا المخاطر التي تترصّدهم. ويكون ذلك خاصة عن طريق تنبيههم في مواقع الإنترنت المهددة بالاختراق الإلكتروني، وإعلامهم بالطرق الاحتيالية التي قد يعتمدها المجرم المعلوماتي وطرق الوقاية منها. ويمكن لمتصفّح الإنترنت غير المتمرّس تفادي عديد الاختراقات والفيروسات الإلكترونية بتجنّب فتح رسائل البريد الإلكتروني المُريبة والحذر عند إقفال النوافذ المنبثقة[٩١].

---

(٩٠) «جدار النار» هو نظام أمني مخصص لحماية شبكة مؤسسة ما من الأخطار الخارجية، كالمتطفّلين النافذين من شبكات أخرى للإنترنت. و 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 مثناني، «مجتمع المعلومات والتنمية، أية علاقة»، مركز النشر الجامعي، الطبعة الثالثة، تونس ٢٠٠٩، ص ٦٥١).

(٩١) 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 فإن مكافحتها تستدعي تضافر جهود الدول المهددة بها واعتماد اتفاقيات دولية توحّد الحلول والإجراءات لمجابهتها وحتى لا يكون المجرم المعلوماتي في مأمن من التتبع والعقاب أينما وُجد في العالم (أ). ورغم ذلك، تظل 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، كما أن أي جهود أحادية الجانب تقوم بها الدول على مستوى العالم لن تأتي بأية نتائج ملموسة. ونظرا لصبغتها العالمية، ولكونها عابرة للحدود، فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي الجنائي[٩٢]. وفي هذا الإطار، لعبت منظمة الأمم المتحدة (١) والإنتربول (٢) ومنظمة التجارة الدولية (٣) دورا فعالا في مكافحة الجريمة الإلكترونية، كما ساهمت اتفاقية بودابست في وضع اللّبنات الأولى لمكافحة هذه الجريمة (٤)، وقد حاولت الدول العربية من جهتها إيجاد حلول مشتركة لمقاومة الجريمة الإلكترونية (٥).

**جهود الأمم المتحدة**

بذلت منظمة الأمم المتحدة جهودا كبيرة من أجل مكافحة جرائم

(٩٢) انظر : محمد فتحي، «تفتيش شبكة الإنترنت لضبط جرائم الاعتداء على الآداب العامة»، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١٢، ص ٥٣١.

الإنترنت. وقد توصلت المنظمة في مؤتمرها الثامن لمنع الجريمة ومعاملة السجناء (هافانا ) [٩٣] إلى إصدار قرار خاص بالجرائم المعلوماتية وقع

(٩٣) انعقد هذا المؤتمر بهافانا (كوبا) من ١٩٩٠/٨/٢٧ م إلى ٧ /٩/ ١٩٩٠م. و فيما يلي نص القرار الصادر عنه : « إن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء، إذ يسلم بضرورة تطوير سبل ووسائل التعاون في المسائل الجنائية، ورغبة منه في استكمال العمل الذي أنجز في ميدان معايير الأمم المتحدة وقواعدها في ميدان العدالة الجنائية. وإذ يضع في اعتباره ان نظم الكمبيوتر كثيرا ما تستعمل لتخزين بيانات سياسة واقتصادية وطبية واجتماعية وشخصية تتسم بحساسية بالغة، وإن هذه النظم قد تستخدم لأداء ومراقبة مهام معقدة كثيرا ما تنطوي على حالات قد تعرض للخطر الحياة وحقوق الانسان والحريات الأساسية. وإذ يدرك أن زيادة استخدام تكنولوجيا الكمبيوتر وشبكات الاتصالات السلكية واللاسلكية على نطاق العالم عن طريق الكمبيوتر بوصفها جزءا لا يتجزأ من العمليات المالية والمصرفية الدولية قد تهيء ظروفا تيسر الى حد كبير من ارتكاب العمليات الاجرامية داخل البلدان وفيما بينها. وإذ يساوره القلق لازدياد اساءة استعمال الكمبيوتر كإحدى طرق الجريمة الاقتصادية وصعوبة الكشف عن الجرائم ذات الصلة بالكمبيوتر، وخصوصا بسبب السرعة التي يمكن أن ترتكب بها هذه الجرائم. وإذ يساوره القلق ايضا لزيادة النفاذ غير المصرح به الى نظم الكمبيوتر وبياناته وبرامجه والاقدام دون إذن على استعمالها أو مراقبتها ، أو التدخل فيها، أو ارتكاب أفعال ضارة أخرى ذات صلة بنظمه وبياناته وبرامحه. وإذ يلاحظ امكانية الربط بين الجريمة المنظمة وما يتصل بها من إساءة استعمال الكمبيوتر وأن الكمبيوتر كثيرا ما قد تستخدمه الجريمة المنظمة لأغراض من قبيل غسل الاموال أو في إدارة الأصول المتحصلة بطريقة غير مشروعة . وإذ يأخذ في اعتباره أيضا أعمال منظمة التعاون الاقتصادي والتنمية ولا سيما تقريرها الصادر عام ١٩٨٦ وتوصية وتقرير مجلس أوروبا بشأن الجرائم المتعلقة بالكمبيوتر والمبادئ التوجيهية التشريعية التي اعتمدتها اللجنة الوزارية لمجلس أوروبا في ١٣ ايلول / سبتمبر ١٩٨٩ . وإذ يأخذ في اعتباره كذلك مشروع المبادئ التوجيهية المتعلقة باستعمال ملفات البيانات الشخصية في نظم الكمبيوتر المعد من قبل اللجنة الفرعية لمنع التمييز وحماية الأقليات . وإذ يضع في اعتباره أن عددا من الدول الأعضاء تضطلع منذ مدة بشأن المسائل المتعلقة بالجرائم المتصلة بالكمبيوتر بما في ذلك إعداد دراسات وبحوث وسن تشريعات . وإذ يسلم بضرورة مواصلة العمل من أجل التوصل الى توافق دولي في الآراء بشان أنماط إساءة استخدام الكمبيوتر التي يتعين اعتبارها سلوكا اجراميا.

واقتناعا منه بأن منع هذه الجرائم ومكافحتها يتطلبان استجابة دولية ديناميكية في ضوء الطابع الدولي والأبعاد الدولية لإساءة استخدام الكمبيوتر والجرائم المتعلقة به. فإنه:

- يؤكد أن وضع إجراء دولي ملائم يتطلب بذل جميع الدول الأعضاء جهدا جماعيا.
- يهيب بالدول الأعضاء، في ضوء الأعمال المطلع بها فعلا في مجال الجرائم ذات الصلة بالكمبيوتر أن تكثف جهودها كي تكافح بمزيد من الفعالية عمليات إساءة استعمال الكمبيوتر التي تستدعي تطبيق جزاءات جنائية على الصعيد الوطني بما في ذلك النظر ، إذا دعت الضرورة إلى ذلك ، في التدابير التالية:

أ - تحديث القوانين وأغراضها الجنائية بما في ذلك التدابير المتخذة من أجل: =

التنصيص فيه على الإجراءات المتعيّن اتخاذها من الدول الأعضاء لمكافحة الجرائم الإلكترونية. ومن بين التوصيات التي وردت بالقرار: تحسين تدابير الأمن والوقاية المتعلقة بالحاسوب مع مراعاة الخصوصية واحترام حقوق الإنسان، تدريب القضاة والمسؤولين عن مكافحة الجرائم الإلكترونية، التعاون مع المنظمات المهتمة بهذا الموضوع في وضع قواعد آداب خاصة بالإنترنت، اعتماد سياسات خاصة بضحايا الجرائم المعلوماتية.

و تبنّت منظمة الأمم المتحدة، في سنة ٢٠٠٠ م، الاتفاقية الخاصة بمكافحة إساءة استعمال التكنولوجيا لأغراض إجرامية. وقد أكّدت هذه الاتفاقية على ضرورة التنسيق بين الدول على مستوى تتبّع الجرائم المعلوماتية وشدّدت

---

= ١. ضمان أن تطبق الجزاءات والقوانين الراهنة، بشأن سلطات التحقيق وقبول الأدلة في الإجراءات القضائية على نحو ملائم وادخال تغييرات مناسبة اذا دعت الضرورة الى ذلك.
٢. وضع أحكام وإجراءات تتعلق بالتحقيق والأدلة للتصدي الى هذا الشكل الجديد والمعقد من أشكال النشاط الاجرامي.
٣. مصادرة أو رد الأصول بصورة غير مشروعة والناجمة عن ارتكاب جرائم ذات صلة بالحاسوب.
ب- تحسين تدابير الأمن والوقاية المتعلقة بالحاسوب مع مراعاة حماية الخصوصية واحترام حقوق الانسان وحرياته الأساسية.
ج- اعتماد تدابير لزيادة وعي الجماهير والعاملين في الأجهزة القضائية وأجهزة انفاذ القوانين بالمشكلة وبأهمية مكافحة الجرائم ذات الصلة بالحواسيب.
د- اعتماد تدابير مناسبة لتدريب القضاة والمسؤولين والأجهزة المسؤولة عن منع الجرائم الاقتصادية والجرائم ذات الصلة بأجهزة الحاسوب والتحقيق فيها ومحاكمة مرتكبيها وإصدار الأحكام المتعلقة بها.
هـ- التعاون مع المنظمات المهتمة بهذا الموضوع في وضع قواعد للآداب المتبعة في استخدام أجهزة الحاسوب وتدريس هذه الآداب ضمن المناهج الدراسية.
و- اعتماد سياسات بشأن ضحايا الجرائم المتعلقة بالكمبيوتر تنسجم مع إعلان الامم المتحدة بشان مبادئ العدل المتعلقة بضحايا الإجرام والتعسف في استعمال السلطة ، وتتضمن إعادة الممتلكات التي يتم الحصول عليها بطرق غير مشروعة ، وتدابير لتشجيع الضحايا على ابلاغ السلطات المختصة بهذه الجرائم.

على ضرورة تكوين الأشخاص المعنيين بالتتبّع وتمكينهم من الوسائل الضرورية لذلك[٩٤]. كما عقدت منظمة الأمم المتحدة في سنة ٢٠١٠م المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية، وقد ناقشت الدول الأعضاء آخر التطورات في استخدام التكنولوجيا الحديثة من طرف المجرمين بما في ذلك الجرائم الإلكترونية. واحتلّت الجريمة المعلوماتية موقعا بارزا في جدول أعمال المؤتمر[٩٥].

من جهة أخرى، أسهمت منظمة الأمم المتحدة بواسطة المنظمة العالمية للملكية الفكرية، وهي إحدى الوكالات المتخصصة التابعة لها، في مكافحة الجرائم الإلكترونية، وخصوصا الجرائم التي تنتهك حقوق التأليف في مجال برامج الحاسب الآلي. وقد أعدّت نصوصا قانونية نموذجية بواسطة خبراء في مجال الملكية الفكرية من أجل مساعدة الدول على استكمال تشريعاتها في مجال حماية البرامج. وكان الهدف من هذه النصوص التي تم وضعها عام ١٩٧٨م، هو اعتمادهما في التشريعات الوطنية للدول الأعضاء أو الاستئناس بها في صورة القيام بمراجعة تشريعية، مثل تشريعات حقوق التأليف والتشريعات الأخرى التي تكفل حماية أسرار التجارة وتحظر المنافسة غير المشروعة[٩٦].

---

(٩٤) انعقد المؤتمر الثاني عشر لمنظمة الأمم المتحدة لمنع الجريمة والعدالة الجنائية بالبرازيل من ١٢ إلى ١٩ /٤/ ٢٠١٠ م.

(٩٥) انظر مذكرة صغير يوسف، «الجريمة المرتكبة عبر الإنترنت»، مذكرة ماجستير في القانون، جامعة مولود معمري، تزي وزو، ٢٠١٣، ص٩٣.

(٩٦) انظر: موقع http://www.startimes.com.

**جهود المنظمة الدولية للشرطة الجنائية (الإنتربول)**

تُعتبر الجرائم الإلكترونية المرتكبة عبر الإنترنت من الجرائم العابرة للدول، إذ غالبا ما يكون الجاني في بلد والمجني عليه في بلد أخر، كما قد يكون الضرر في بلد ثالث في ذات الوقت. ونظرا لهذه الخصوصية، فقد أصبح التعاون الدولي أمرا ضروريا. ويتعيّن الإشادة بجهود «الإنتربول» في هذا المجال، من خلال ضباط الارتباط المتواجدين في معظم دول العالم، والمكلّفين بتوفير قاعدة بيانات ضخمة يمكن أن تشكّل نقطة انطلاق لمكافحة الجرائم الإلكترونية(٩٧). أُنشئت منظمة «الإنتربول» في عام ١٩٢٣م، وتتكون حاليا من ١٩٠ عضوا ومقرها الرئيسي بفرنسا. وتهدف هذه المنظمة إلى التنسيق بين أجهزة الشرطة في الدول الأعضاء من خلال جمع للبيانات والمعلومات المتعلقة بالمجرمين عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول الأعضاء بالمنظمة. و تسعى منظمة الشرطة الدولية إلى الحصول على المعلومات من الدول المنخرطة فيها وخاصة تلك المتعلقة بالجرائم العابرة للدول التي تُعتبر جرائم الإنترنت من أهمها. ومن الأمثلة الواقعية على دور الإنتربول في مكافحة الجريمة الإلكترونية، مساعدته للسلطات اللبنانية في القبض على طالب قام بتنزيل صور إباحية على الإنترنت لقاصرة سنها أقل من عشرة أعوام وذلك إثر تلقي النيابة اللبنانية لبرقية من الإنتربول في ألمانيا بهذا الخصوص(٩٨).

(٩٧) انظر جلال محمد الزعبي و أسامة أحمد المناعسة، «جرائم تقنية المعلومات الإلكترونية»، دراسة مقارنة، دار الثقافة، عمان، ٢٠١٠ م، ص ٩٣.

(٩٨) انظر جريدة النهار اللبنانية، عددها الصادر في ٢٠٠١/٧/١٩ م (ذكره حسين الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت دراسة مقارنة»، دار النهضة العربية، ٢٠٠٩، ص ٦٤٠).

**جهود منظمة التجارة العالمية:**

رغم حداثة منظمة التجارة العالمية[٩٩]، إلا أنها تلعب دورا مهما في مكافحة صنف واسع الانتشار من الجرائم الإلكترونية وهو نسخ وتقليد البرامج المعلوماتية. وقد كان للبدء في تطبيقها منذ بداية عام ١٩٩٥ م أثرا مهما في مجال حماية حقوق الملكية الفكرية، وذلك باعتماد اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (تربس). وقد نصّت المادة (١٠ / ١) من هذه الاتفاقية على أن برامج الكمبيوتر تتمتع بالحماية باعتبارها مصنفات فنية بموجب اتفاقية «برن» (١٩٧١). ويؤكد نص هذه المادة على وجوب حماية برامج الحاسب الآلي باعتبارها من حقوق المؤلف[١٠٠].

و قد خصّت الاتفاقية حق المؤلف بمجموعة من الأحكام، كما أقرّت لمنتجي البرامج حقوقا يتعيّن على الدول الأعضاء حمايتها، ومن بينها حق المؤلف في تأجير برنامجه. وتعتبر اتفاقية (تربس) أول اتفاقية أوردت نصا خاصا لحماية حق المؤلف و ذلك بالمادة (١٠ / ١)، والتي تنطبق على برامج الحاسب الآلي.

**اتفاقية بودابست لمكافحة الجرائم المعلوماتية لسنة ٢٠٠٢ م**

جاءت اتفاقية بودابست[١٠١] تتويجا للجهود التي بذلها الاتحاد الأوربي والمجلس الأوربي من أجل إيجاد صيغة قانونية لمكافحة الجريمة الإلكترونية،

---

(٩٩) يعود توقيع اتفاقية إنشاء منظمة التجارة العالمية إلى ١٩٩٤/٤/١٥ م.

(١٠٠) حول الحماية الجنائية لبرامج الحاسب الآلي، انظر: محمد نصر محمد، « مشكلات الحماية الجنائية لبرامج الحاسب الآلي، دراسة مقارنة»، مجلة القضائية، العدد الثامن، محرم، ١٤٣٥ هـ، ص ١٧٦.

(١٠١) انظر هلالي عبد اللاه أحمد، «اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها»، دار النهضة العربية، القاهرة، ٢٠١١، الطبعة الأولى.

وتُعد الإطار المرجعي لمكافحة الجرائم المعلوماتية في الوقت الحالي. وُضعت هذه الاتفاقية من قبل مجلس أوربا بالتعاون مع كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية. وقد دخلت حيّز التنفيذ سنة ٢٠٠٤ م[١٠٢]، ويمكن لأي دولة الانضمام إليها. أبرزت هذه الاتفاقية مدى اقتناع الدول المصادقة عليها بخطورة الجريمة المعلوماتية وبضرورة تظافر الجهود الدولية لمواجهتها. وقد تعرّضت إلى بعض المفاهيم، مثل مفهوم النفاذ غير الشرعي ومفهوم الجريمة المعلوماتية وغيرها من المفاهيم التي تستدعي اعتماد مفهوم موحّد لتسهيل تطبيق الاتفاقية[١٠٣]، كما تضمّنت قواعد متعلّقة بالتعاون في ميدان مواجهة الجريمة الإلكترونية، كالقواعد الخاصة بالاختصاص الإقليمي للمحاكم (المادة ٢٢) وتسليم المجرمين (المادة ٢٤) واعتماد شبكة مفتوحة طوال الأسبوع مخصّصة لبقية الدول الأعضاء لتوفير المساعدة في الأبحاث المرتبطة بالجرائم المعلوماتية ( المادة ٣٥).

### ٥- على مستوى الدول العربية

اجتمع ممثّلو الدول العربية في المؤتمر العربي للتحضير لمؤتمر القمة العالمية لمجتمع المعلومات في الفترة الممتدّة من ١٦ إلى ١٨ يونيو ٢٠٠٣. وحضر المؤتمر ممثّلو ١٩ دولة عربية إضافة إلى مندوبي ٩ دول إفريقية باعتبارهم مراقبين وعدّة شخصيات مرموقة عالميا في مجال الاتصالات والمعلوماتية. وقد تم التنصيص على انشاء فريق عمل تحت مظلة جامعة الدول العربية لتأمين شبكة المعلومات

(١٠٢) انظر مذكرة صغير يوسف، «الجريمة المرتكبة عبر الإنترنت»، المرجع السابق، ص ١٠٠.
(١٠٣) الهاشمي الكسراوي، «الجريمة المعلوماتية»، مجلة القضاء والتشريع، العدد ٧ لسنة ٢٠٠٦، ص ٤٠.

العربية وحماية المستهلك العربي من جرائم الإنترنت[١٠٤]. وسعى مجلس التعاون لدول الخليج العربي من جهته إلى مكافحة الجريمة الإلكترونية، حيث أوصى منذ سنة ٢٠٠٧ م بأن ينخرط أعضاؤه في المنظومة العالمية لمكافحة الجريمة الإلكترونية وفق المعايير الدولية[١٠٥].

### 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 بين دولة وأخرى والراجع أساسا إلى الخصوصيات الثقافية والدينيّة. ويوجد اختلاف بين الدول في تعريف الأنشطة التي تدخل في مفهوم الجريمة الإلكترونية، بالإضافة إلى عدم الاتفاق على النماذج التي تشكّل البناء القانوني لهذه الجريمة و التباين في التعامل الإجرائي معها[١٠٦]. وعلى أساس ذلك يتعيّن على الدول صياغة الأنظمة الملائمة لمكافحة الجريمة الإلكترونية مع الأخذ بعين الاعتبار بخصوصياتها الاجتماعية والدينية.

و في إطار التصدّي للجريمة الإلكترونية في المملكة، صدر قرار مجلس الوزراء رقم ٧٩ بتاريخ ١٦ / ٩ / ١٤٢٧ هجري، القاضي بالموافقة على نظام مكافحة جرائم المعلوماتية و المتوّج بالمرسوم الملكي رقم (م ١٧) بتاريخ

---

(١٠٤) ناصر بن محمد البقمي، «جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية»، الطبعة الأولى، الرياض، ١٤٣٠ هجري–٢٠٠٩ م، ص١٠٠.

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

(١٠٦) ناصر بن محمد البقمي، المرجع السابق، ص١٠٢.

٨ / ٣ / ١٤٢٨هجري[١٠٧]. وقد أقر هذا النظام عقوبات ضد من يعمد 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. و تجرّم المادة الرابعة من النظام التحيل والتجسّس على البيانات البنكية أو الائتمانية للأفراد، كما يُجرّم النظام المساس بالنظام العام أو القيم الدينية أو الآداب العامة ويُفرد الجريمة الإلكترونية ذات الطابع الإرهابي بعقاب صارم يصل إلى عشر سنوات سجنا نظرا لما تشكله من تهديد لأمن المجتمع .

ولمساعدة الجهات الأمنية في تجاوز الصعوبات التقنية المرتبطة بالجرائم المعلوماتية، نصّت المادة ١٤ من نظام مكافحة الجرائم المعلوماتية على ما يلي: «تتولّى هيئة الاتصالات وتقنية المعلومات وفقا لاختصاصها تقديم الدعم والمساعدة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة». ويُعد اعتماد هيئة مختصة في دعم ومساندة الجهات الأمنية عند مكافحتهم للجريمة الإلكترونية أمرا ضروريا وعمليا، نظرا للصبغة التقنية للجريمة المعلوماتية. وهذا ما يُفسّر إنشاء عدة دول في العالم وحدات متخصصة في مكافحة جرائم الإنترنت كالصين والولايات المتحدة وبريطانيا[١٠٨]. وفي فرنسا، اقترح وزير الداخلية السابق «ميشال دي فيلبان»

(١٠٧) انظر : ناصر بن محمد البقمي، المرجع السابق، ص ٢١٠.

(١٠٨) انظر نبيلة هبة هروال، «الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات»، دار الفكر الجامعي، ٢٠١٣، ص ١٠٧.

مشروع قانون يهدف إلى مكافحة الجريمة الإلكترونية. ومن بين الحلول الواردة في مشروع القانون الفرنسي الترفيع في قوات الشرطة والدرك المتخصصين في المعلوماتية. وقد ذهب وزير الداخلية الفرنسي إلى حد اقتراح «البحث عن وسائل خاصة للتحقيق تمكّن من اكتشاف الجرائم الخطيرة في الوقت المناسب كأن يكون للمحققين الحق في أن يشاركوا تحت اسم مستعار في المحادثات الإلكترونية بدون أن يكونوا مسؤولين جزائيا»[١٠٩].

يعتبر نظام مكافحة الجرائم المعلوماتية وسيلة قانونية ناجعة وفعّالة في مكافحة الجريمة الإلكترونية، حيث أقر عقوبات رادعة للجرائم الإلكترونية. وقد سمح هذا النظام للقضاء السعودي بالتصدي للعديد من الجرائم المعلوماتية، وخاصة الأخلاقية منها، على غرار تخزين صور فاضحة في ذاكرة الهاتف النقال والتشهير بالغير بواسطة الهاتف الجوال. رغم ذلك، فإن بعض العقوبات الواردة بهذا النظام قد لا تحقّق الردع الكافي[١١٠]، حسب اعتقادنا، بالنظر إلى خطورة بعض الجرائم. من ذلك أن 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 أن الأضرار التي يمكن أن تلحق بالغير في حالة الاستيلاء الإلكتروني على

(١٠٩) انظر نبيلة هبة هروال، المرجع السابق، ص ١١٥. انظر نبيلة هبة هروال، «الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات»، دار الفكر الجامعي، ٢٠١٣، ص ١٠٧.

(١١٠) تمّت صياغة نظام مكافحة جرائم المعلوماتية السعودي على خلاف الأنظمة الجنائية الحديثة، حيث بدأ المنظّم بتحديد العقوبات أولا، ثم تحديد الجرائم التي تنطبق عليها العقوبات، في حين أن الشائع في النصوص التجريمية أن يتم تحديد الجرائم أولا، ثم العقوبات في مرحلة لاحقة (انظر ناصر بن محمد البقمي، المرجع السابق، ص ٢١١).

أموال مودعة بالبنوك تكون عادة فادحة، على غرار ما قام به الهاكر الجزائري حمزة بن دلاّج[١١١]. من جهة أخرى، فإن أقصى العقاب المقرر لجريمة الاتجار بالمخدرات أو المؤثرات العقلية عبر الإنترنت هو خمس سنوات. وهو عقاب أقل ردعا من العقاب المقرر للاتجار بالمخدرات بالطرق التقليدية، والذي يصل في المملكة إلى الإعـدام[١١٢]. 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 مزوّدي الخدمات بحفظ البيانات المخزّنة في أنظمتهم لمدة زمنية محددة بما يسمح بالتعرّف على مستعمل الخدمة وعلى حركة الاتصال، وهي وسائل تسمح بضبط المجرم المعلوماتي بشكل أسرع.

تُشكل الجريمة الإلكترونية تحدّيا للدول التي يتعيّن عليها تحديث أنظمتها وجعلها مُواكبة لتطور الجريمة الإلكترونية. هذا التحدي يزداد صعوبة في المملكة، نظرا لخضوع الأنظمة فيها لأحكام الشريعة الإسلامية[١١٣]. ويتعيّن على الأنظمة أن تستلهم من القرآن والسنة الحلول الكفيلة بمكافحة الجرائم

(١١١) انظر المقال الإلكتروني «بعد اختراقه عشرات البنوك الهاكر الجزائري حمزة بن دلاّج في قبضة الـ FBI» المنشور في موقع : www.mbc.net

(١١٢) انظر نظام مكافحة الاتجار بالمواد المخدرة في المملكة العربية السعودية الصادر بموجب الأمر السامي رقم ٤/ب/٩٦٦ وتاريخ ١٠ / ٧ / ١٤٠٧ هـ المتضمن قرار هيئة كبار العلماء رقم ١٣٨ وتاريخ ٢٠ / ٦ / ١٤٠٧ هـ، وكذلك قرار مجلس الوزراء رقم ١١ لسنة ١٣٧٤ هـ.

(١١٣) 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».

الإلكترونية. وقد أثبت نظام مكافحة الجرائم المعلوماتية قدرة الشريعة الإسلامية على مواكبة تطورات العصر. وبالفعل، فقد «تركت الشريعة مجالا واسعا للعلماء وأولي الأمر لمعالجة أمور المعاملات في جوانبها المختلفة من مدنية وجنائية ودستورية ونحوها في ضوء التوجيهات القرآنية والنبوية العامة... أما الفروع والتفاصيل المتعلقة بكيفية إعمال هذه الأسس العامة والقواعد الكلية وتطبيقها وإجراءات ذلك، فهي تتسم في أغلبها بالمرونة والتجدّد»[١١٤]. بهذه المرونة والتجدّد تمكنت الشريعة الإسلامية الغرّاء من مسايرة متطلبات العصر ومواكبة الجرائم المستحدثة؛ لتكون بالفعل صالحة لكل زمان ومكان.

(١١٤) محمد عبد الظاهر حسين، «الفقه الإسلامي المصدر الرئيس للتشريع»، دار النهضة العربية، القاهرة، مصر، ١٩٩٩ م، ص ١٢٧ (مرجع ذكره ناصر بن محمد البقمي، «جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية»، الطبعة الأولى، الرياض، ١٤٣٠ هـ - ٢٠٠٩ م، ص ١٩٤).

# الخاتمة

في الختام، وعلى ضوء ما تم استعراضه حول مكافحة الجرائم الإلكترونية، يمكن القول بأن الجريمة الإلكترونية تعتبر جريمة من نوع خاص تستدعي إجراءات من نوع خاص. كما أن مكافحتها تتطلّب تنسيقا دوليا واهتماما أكثر بالجانب التقني. وقد أمكن التوصّل إلى النتائج والتوصيات التالية:

## أولا: النتائج

- خطورة الجريمة الإلكترونية بالنسبة للدول والأفراد.
- خصوصية الجريمة الإلكترونية وخصوصية مرتكبها.
- صعوبة مكافحة الجريمة الإلكترونية باعتماد وسائل المكافحة التقليدية وأهمية الجانب التقني في مكافحتها.
- التباين الكبير بين دول العالم في مكافحة الجريمة الإلكترونية وضعف التعاون الدولي.
- عدم مواكبة أجهزة البحث الجنائي في معظم الدول العربية لظاهرة الإجرام الإلكتروني.
- صعوبة مسايرة النصوص القانونية لتطور الجريمة الإلكترونية.
- تميّز المملكة العربية السعودية من الناحية النظامية على مستوى مكافحة الجريمة الإلكترونية.

## ثانيا: التوصيات

**أ–على المستوى التقني:**

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

**على المستوى القانوني:**

- تشديد العقاب بالنسبة لبعض الجرائم (السرقة الإلكترونية والاتجار بالمخدرات عبر الإنترنت) بحيث يكون العقاب متقاربا مع العقاب المقرر لها في المملكة خارج المجال الإلكتروني.

- النص في صلب نظام مكافحة الجرائم المعلوماتية على مسؤولية مزودي خدمات الاتصال في حفظ البيانات مدة زمنية محددة مما يُسهّل من التصدّي للجريمة والتعرّف على مرتكبها.
- النص في صلب نظام مكافحة جرائم المعلوماتية على الاختصاص الحكمي للمحاكم السعودية في مجال الجرائم الإلكترونية وفق معايير متعدّدة مثل جنسية المجرم وجنسية المتضرر من الجريمة ومقر المجرم بشكل يسمح بتتبعه لمجرّد توفّر أحد هذه المعايير وهو ما يحول دون إفلاته من العقاب.
- إحداث خليّة قانونية مختصة في متابعة المخاطر والجرائم الإلكترونية وإعداد النصوص القانونية الملائمة في وقت قياسي.
- التنسيق مع مختلف دول العالم من أجل التصدّي للجريمة الإلكترونية.