الجرائم المستحدثة المرتكبة عبر وسائل التواصل الاجتماعي ومدى مكافحتها في لبنان

رسالة أُعدّت لنيل الماجستير في القانون الجزائي

إعداد الطالبة

مايا مصطفى الصبّاغ

لجنة المناقشة

- **الدكتور علي إبراهيم** **مشرفاً**
-
-

السنة 2020/ 2120

الإهداء

إلى مثلي الأعلى...

وقدوتي في الحياة

والدي العزيز

إلى ملاكي في الحياة..

إلى من كان دعاؤها سر نجاحي..

إلى أغلى الحبايب

والدتي الحبيبة

إلى من أظهروا لي ما هو أجمل من الحياة

أخوتي وأخواتي

إلى بناتي

أغلى ما في الحياة

إلى أستاذي الفاضل ومشرفي

المدّعي العام المالي القاضي الدكتور علي إبراهيم

إليهم جميعاً أُهدي هذا الجهد المتواضع

الجرائم المستحدثة المرتكبة عبر وسائل التواصل الاجتماعي ومدى مكافحتها في لبنان

الإطار النظري

المقدمة

القسم الأول
مفهوم الجرائم المرتكبة عبر وسائل التواصل الإجتماعي

المبحث الأول: ماهية الجرائم الإلكترونية

المطلب الأول: مفهوم الجرائم الإلكترونية، خصائصها، دوافعها

الفرع الأول: المفهوم اللغوي والفقهي للجريمة الإلكترونية

الفرع الثاني: التعريف الدولي لهذه الجريمة

الفرع الثالث: أسباب الجريمة الإلكترونية

الفرع الرابع: خصائص الجريمة الإلكترونية

الفرع الخامس: آثار الجريمة الإلكترونية

المطلب الثاني: صور الجرائم الإلكترونية وهي كثيرة منها:

الفرع الأول: القدح والذم والتشهير الإلكتروني

الفرع الثاني: الإبتزاز الإلكتروني

الفرع الثالث: الإتجار بالبشر الإلكتروني

الفرع الرابع: الإحتيال الإلكتروني

الفرع الخامس: جرائم الفكر والصحافة

المبحث الثاني: النظام القانوني للجرائم المرتكبة عبر وسائل التواصل الإجتماعي

المطلب الأول: التشريعات والقوانين المتعلقة بهذه الجرائم

الفرع الأول: في القانون اللبناني

الفرع الثاني: في القانون المصري

الفرع الثالث: في القانون الأردني

الفرع الرابع: في القانون الأوروبي

الفرع الخامس: في القانون الأميركي

المطلب الثاني: تصنيف مرتكبي الجرائم الإلكترونية

الفرع الأول: السمات الخاصة بالمجرم الإلكتروني

الفرع الثاني: أدوات الجرائم الإلكترونية وطرق تنفيذها

الفرع الثالث: الفئات التي تستهدفها هذه الجرائم

الفرع الرابع: طرق الوقاية من هذه الجرائم

الفرع الخامس: فئات مرتكبي هذه الجرائم

الإطار التطبيقي

القسم الثاني

مدى مكافحة الجرائم المستحدثة المرتكبة عبر وسائل التواصل الاجتماعي محلياً ودولياً

المبحث الأول: الأطر الدولية والمحلية لمكافحة هذه الجرائم

المطلب الأول: الأطر التشريعية

الفرع الأول: الإطار التشريعي المحلّي والدولي

الفرع الثاني: الإتفاقيات الدولية

الفرع الثالث: المؤتمرات الدولية

الفرع الرابع: التعاون الدولي في مكافحة هذه الجريمة

الفرع الخامس: التعاون القضائي في مكافحة هذه الجريمة

المطلب الثاني: الأُطر الأمنية

الفرع الأول: الإطار الأمني المحلّي

الفرع الثاني: الإطار الأمني الدولي

الفرع الثالث: دور الإنتربول في مكافحة الجريمة الإلكترونية

الفرع الرابع: المكافحة على صعيد سلطات إنفاذ القانون

الفرع الخامس: المكافحة على صعيد التوعية والتدريب

المبحث الثاني: الإطار الإجرائي فيما يختص بهذا النوع من الجرائم

المطلب الأول: دواعي الحماية الجنائية للمعلوماتية من الجرائم التي قد تقع عليها

الفرع الأول: تدريب القضاء والضابطة العدلية على التحقيق في هذه الجرائم المستحدثة

الفرع الثاني: تطوير الآليات التشريعية لتجريم الأفعال المستحدثة

الفرع الثالث: الحماية الإجرائية من خلال خصوصية الملاحقة والإثبات

الفرع الرابع: أهم الآليات الإجرائية التي أرساها المنتظم الدولي في هذه الجريمة

الفرع الخامس: مدى ملائمة القوانين المقارنة مع هذه الآليات الإجرائية

المطلب الثاني: المشكلات الإجرائية التي تثيرها الجريمة الإلكترونية

الفرع الأول: المشكلات المتعلقة بضبط الجريمة الإلكترونية وإثباتها

الفرع الثاني: الخبرة والمعاينة والتفتيش في الجرائم الإلكترونية

الفرع الثالث: المشكلات المتعلقة بسلطات التحري والملاحقة

الفرع الرابع: المشكلات المتعلقة بالاختصاص والقانون واجب التطبيق

الفرع الخامس: حلول مقترحة

خاتمة

الفهرس

الإطار التطبيقي

المقدمة

الجريمة وُجِدت منذ وجود الإنسان على الأرض وتنوّعت أشكالها. وقد تحوَّلت جريمة السطو والإحتيال والإبتزاز والسرقة والتخريب في شكلها التقليديّ إلى شكلٍ جديدٍ مع ثورة الإنترنت ألا وهو الجرائم السيبرانيَّة.[1]

إنَّ تكنولوجيا المعلومات والإتَّصالات أداةٌ أساسيةٌ في الحياة اليومية، وشاملةٌ لأغلب القطاعات والأنشطة الاقتصاديَّة، إضافة إلى فعَّاليتها في التنمية الاقتصاديَّة والاجتماعيَّة فهي تساهم في تحقيق التنمية الشاملة في الداخل وإقامة جسورٍ من التعاون بين الدول في الخارج، وتمكِّن من تبادل الآراء والخبرات التخصُّصيَّة في كافَّة المجالات.[2]

إلا أنَّ الإنفتاح الذي يميّز الفضاء السيبراني عموماً، جعله عرضةً للإنتهاكات والأنشطة الإجراميَّة والتّعدِّي على حقوق الناس، فقد تكون مواطناً صالحاً ولك مركزك في المجتمع وإذا بأحد المتطفلين يسرق صورتك الشخصية وينتحل صفتك ويقوم بإنشاء صفحة معيبة لك على فايسبوك لتشويه سمعتك وإذا بالصفحة المزوّرة باتت منتشرة بين الجميع وقد تستفيق صباحاً لتجد صوراً إباحية تظهر على صفحة الفايسبوك خاصتك ولا تدري من أين أتت.

وقد تقوم بتنزيل صور لك في فيديوهات أو أفكار خاصة بك على صفحات مواقع التواصل الإجتماعي فتجد أن غيرك يخزّنها أو يحوّر في مضمونها دون أن يستحصل على إذن منك فتجد مثلاً أن رأسك أصبح على جسدٍ عارٍ!![3].

فشيوع الإنترنت قد أنجب أنشطة إجرامية وأنشأ طرائق جديدة لجمع المعلومات، فاشتملت أنظمة التشغيل والبرمجيات على نقاط ضعف مما فتح الباب على مصراعيه أمام إمكانية القيام بأعمال تسهل التجسّس الأمني والإقتصادي وتؤثّر على أعمال السلطة، والتعدي على حقوق الناس يؤثر سلباً على جميع المستخدمين من أفراد وشركات ومنظمات.

تميّز القرن 21 باستخدام المعلومات، وعلى مدى السنوات القليلة الماضية توسّعت الإنترنت أضعافاً مضاعفة. حالياً، حوالي هناك 820 مليون شخص يستخدمون الإنترنت، بزيادة قدرها 126 في المئة من 2000 – 2005. لقد وفرت السهولة النسبية لاستخدام الإنترنت، والحصول على الإنترنت على نحو متزايد أكثر للإنترنت بأسعار معقولة والحصول على أجهزة الكمبيوتر مع أجهزة المودم فائقة السرعة، كل ذلك مكّن الناس من التواصل وتكوين الصداقات الجديدة، والتجارة،

---

[1] مجلة الامن، السنة الثانية عشر، العدد 140، ايلول 2003، ص 62

[2] مجلة الامن، المرجع نفسه، ص 62

[3] حماية الحق في الخصوصية المعلوماتية – د. هانيا فقيه، ص 2.

والترفيه، والتعلم، والقيام بأعمال تجارية، ودفع الفواتير عبر الإنترنت. وخلقت شبكة ويب العالمية ما يسمى العالم الافتراضي أو الفضاء الإلكتروني، والذي يعرف بأنه "مكان لأجل غير مسمى حيث يتفاعل الأفراد" (Britz, 2004, P2). ويتصف الفضاء الإلكتروني بأنه مكان بلا حدود مادية أو اجتماعية تحرم الأفراد من العيش فيه.

لقد تباينت الصّور الإجرامية لظاهرة الجريمة المعلوماتية وتشعّبت أنواعها فلم تعد تهدّد العديد من المصالح التقليدية التي تحميها القوانين والتشريعات فحسب بل أصبحت تهدّد أيضاً العديد من المصالح والمراكز القانونية التي استحدثتها التقنية المعلوماتية بعد اقترانها بثورتي الاتصالات والمعلومات. فالمصالح التقليدية بدأت تتعرض إلى أشكال مستحدَثة من الاعتداء بواسطة هذه التقنية الحديثة. فبعدما كان الاعتداء على الأموال يتم بواسطة السرقة التقليدية أو النصب، وكانت الثقة في المحررات الورقية يُعتدى عليها بواسطة التزوير، أصبحت هذه الأموال يُعتدى عليها عن طريق اختراق الشبكات المعلوماتية، وإجراء التحويلات الإلكترونية من أقصى مشارق الأرض إلى مغاربها في لحظات محدودة. كما أن الحقوق الثابتة في الأوعية الورقية صار يتم الاعتداء عليها في أوعيتها الإلكترونية المستحدثة عن طريق اختراق الشبكات والأنظمة المعلوماتية دون الحاجة إلى المساس بأي وثائق أو محرّرات ورقية.

وبعدما كانت حياة الإنسان الخاصة تواجه الاعتداء على شكل استراق السّمع، أصبحت هذه الخصوصية تُنتهك بواسطة اختراق البريد الإلكتروني.

ولهذا، فإن التقاعس في إنفاذ القوانين والتشريعات اللازمة في مواجهة هذه الظاهرة الإجرامية الجديدة من شأنه أن يضعنا في مواجهة العشوائية في الأمن السيبراني.

من هنا تبرز أهمية مضاعفة الجهود على كافة الأصعدة لضمان أمان الفضاء السيبراني والحدِّ من المخاطر الإلكترونيّة. وتكتسب الجهود المشتركة بين القطاعات والفرقاء المعنيّين، والتعاون الدوليِّ والإقليميِّ في مواجهة الانتهاكات على الفضاء السيبراني ومكافحتها، أهميّةً خاصّةً نظراً للطبيعة الشموليَّة للمخاطر السيبرانيّة. هذا الأمر الذي يدلُّ على مدى صعوبة متابعة ومكافحة مخاطر الفضاء السيبراني.

لذلك سوف أسلّط الضوء بالقدر المستطاع على موضوع جرائم الإنترنت الذي احتلّ حيّزاً مهماً لدى الرأي العام والباحثين على حدٍّ سواء، على المستوى المحليّ والعالميّ، وخاصّةً في الدول المتقدّمة.

كما سأسلّط الضوء على واقع الأمن السيبراني في لبنان والمشاكل التي يعاني منها بغية تعزيز وضعه في هذا المجال على كافّة الأصعدة مما له من أهميّة بالغة لارتباطه بالأمن القومي والاقتصادي والاجتماعي.

منهجية الدراسة:

تعدّ الجريمة المعلوماتيّة واحدة من أكبر التحدّيات التي نواجهها في عالمنا المعاصر، إن لم تكن أكبرها على الإطلاق. والحديث عن هذه التحدّيات يتطلّب أولاً إعطاء صورة عامّة عن ماهيّتها. ومن أجل ذلك لا بدّ من تعريفها وتصنيفها في **مبحث أوّل،** قبل التعرّض إلى بحث إشكاليات المسؤوليّة الجنائيّة وتحدّي المعلوماتيّة للقواعد العامة للمسؤولية الجنائية في **مبحث ثان.**

وقد تمّ تقسيم الرسالة إلى فصلين، وكلّ فصل إلى مبحثين. وتناول المبحث الأوّل مفهوم الجريمة الإلكترونية باعتبارها جريمة مستحدثة أثارت ضجّة كبيرة في الأوساط القانونية والتشريعية من حيث مفهومها والأفعال الإجرامية التي تدخل في نطاقها.

وقد عرّفنا الجريمة الإلكترونية بأنها كلّ سلوك غير مشروع أو غير أخلاقي أو غير مصرّح به يتعلّق بالمعالجة الآلية للبيانات أو نقلها.

وتناولنا الأسباب والدوافع لارتكاب الجرائم الإلكترونية. وهي كثيرة؛ وأهمّها أسباب على المستوى الفردي، والمستوى المجتمعي، والمستوى الكوني. كما أن هناك أسباباً تتعلق بخصائص الجريمة الإلكترونية، حيث إن سوق المعلومات والحاسوب الآلي والإنترنت يمثّل ثروة كبيرة للمجرمين، لذا يعدّ الأكثر جذباً لاستثمار الأموال، وغسيلها، وسرقة البنوك، واعتراض العمليات الماليّة وتحويل مسارها.. إلخ. وهنالك ثلاثة عوامل تحفز على ارتكاب الجريمة الإلكترونيّة؛ وهي الجاني المتحفّز، والهدف المناسب، وغياب الحراسة أو الرقابة.

وفي عصرنا الذي يشهد تطوّراً علمياً سريعاً أصبح كلّ اختراع واكتشاف في هذا المجال ينافس الآخر. وظهر الحاسوب الذي كان في بداية أمره متاحاً لعدد من الاستخدامات الشخصيّة فحسب. ورافقه بعد مدّة ظهور الشبكة العنكبوتية (الإنترنت) التي كانت لها محدوديّتها في البداية أيضاً؛ أي أنها كانت مقصورة على فئة معينة، فلم تكن آمنة في تصميمها وبنائها. على أنّ الوضع لم يبق على ما هو عليه. لقد أدّى التطور التاريخي للإنترنت إلى زيادة مستخدميها من جميع الفئات. وهو بذلك فتح أبواباً كانت مغلقة، ووسع حدوداً أضحت بلا حراسة. وهذا ما ساهم في ظهور الجرائم الإلكترونية التي دقّت ناقوس الخطر لتنبّه المجتمعات إلى مدى خطورتها. وظهر المجرم المعلوماتي المدفوع إلى ارتكاب الأفعال المجرمة في مجال التقانة كالجرائم الإلكترونية. وأثير الجدل، نتيجة توسع مجال الجريمة وتعدّد أشكالها، حول ماهيّة الجريمة الإلكترونية والغرض منها.. وحول السؤال الدقيق: ما هي صورها وما علاقتها بالحاسوب؟

فالجريمة الإلكترونية هي جريمة ذات طابع مادي، وتتمثّل في كلّ فعل أو سلوك غير مشروع مرتبط بأي وجهة أو بأي شكل بالحواسيب والشبكات الحاسوبية، يتسبّب في تحميل أو إمكان تحميل

المجني عليه خسارة، وحصول أو إمكان حصول مرتكبه على أي مكسب.. وغالباً ما تهدف هذه الجرائم إلى سرقة المعلومات الموجودة في الأجهزة الحاسوبية، أو تهدف على نحو غير مباشر إلى الأشخاص والجهات المعنية بتلك المعلومات. والجريمة من هذا النوع لها مسميات عدة منها: جرائم الحاسوب والإنترنت computer crime جرائم التقنية العالية hi-tech crime الجريمة الإلكترونية e-crime– الجريمة السايبِرية (Cyber crime) – جرائم أصحاب الياقات البيضاء (white collar).. وغالباً ما تكون الاعتداءات على الكيانات المعنوية المتعلقة بقيمتها الإستراتيجية، كمخازن المعلومات، وهذا أهمّ ما يميّز الجرائم الإلكترونية عن غيرها من الجرائم؛ فهي تتعلّق بالكيانات المعنويّة ذات القيمة المادية أو القيمة المعنوية البحتة أو كليهما معاً. وهذا هو أساسها الذي لا يمكن تصوّر وجود جريمة إلكترونية بدونه، فلولا هذا الأساس لكانت من الجرائم العادية التي تخضع للقانون الجنائي التقليدي. إضافة إلى هذا، فهي تتكون من أساسين هما عناصر الجريمة والسلوك ووصفه الإجرامي، والنصّ القانوني على تجريم السلوك وإيقاع العقوبة هو من أساسيات الجرائم العادية.

ونظراً إلى تطوّر الجرائم الإلكترونية وتعدد أشكالها وأنواعها، مع إمعان العالم في استخدام الحاسوب، وصعوبة حصرها ووضع نظام قانوني ذي أساس قوي ومتين يخضع له المجرم المعلوماتي باءت محاولات الباحثين بالإخفاق، حيث أنه يمكن ارتكاب الجريمة بكبسة زر. وصعوبة تحديد الفاعل أو تعذُّر معرفة مكانه أدّيا إلى إثارة الجدل حول هذه الجرائم الإلكترونية وصورها، وهل يمكن حصرها في أنواع معيّنة، فالجريمة الإلكترونية تبدأ من عمليات الاقتناص لأرقام الحسابات وبطاقات الائتمان، إلى التخريب في المواقع، ونشر الصور الإباحية، وإنشاء المواقع الكاذبة، وغسيل الأموال، والتجسس.. إلخ.

الأهميّة العلمية:

تكمن أهمية هذه الدراسة في تناولها ظاهرةً مستحدثة هي ظاهرة الجرائم الإلكترونية (السايبرية)، فالتطوّر التكنولوجي على الرغم من آثاره الإيجابية إلا أن له العديد من السلبيات التي تهدد أمن المجتمع واستقراره في العالم بأسره.

ومما لا شك فيه أن التطور التكنولوجي يؤدي إلى ظهور مهن ومهارات جديدة تؤدي بدورها إلى اضطرابات في أنساق العمل القديمة وتهديد للمهن القائمة، الأمر الذي يترتب عليه حدوث مشكلات اجتماعية جمّة.

الإشكاليّة:

نعم، هناك صعوبات جمّة وأخطار تحول دون كشف الجرائم الإلكترونية، وذلك لتعدد وسائل إخفائها عن الأنظار، وكذلك بسبب الخبرة المتراكمة لدى مرتكبيها.

وتصدر الأخطار والتهديدات السيبرانية عن أعمال قصدية كالاختراقات والاعتداءات، وعن أعمال غير قصدية كالإهمال وقلّة الوعي والإدراك.

ويمكن توزيع الأخطار في الفضاء السيبراني انطلاقاً من أهدافها على ما يطال الدول وما يطال الأشخاص. ويندرج في إطار الفئة الأولى كلّ ما يعرض الأمن القومي والعسكري، والاقتصادي، والاجتماعي، ويهدد البيئة التحتية والحرجة للدول ولأسواق المال والقطاعات المصرفية، والسلم الدولي والمنشآت النووية والمؤسسات الصحية وقطاعات النقل بكلّ أنواعه: البرّي والبحري والجوي، ورفاه الشعوب.

بينما يندرج في الفئة الثانية: سرقة البيانات الشخصية، وتسريبها، واستخدامها دون إذن ودون وجه حقّ، وسرقة الأموال، واختراق أنظمة المعلومات، والاعتداء على الملكية الفكرية والصناعية والعلامات التجارية.

وتشمل هذه الفئة أيضاً: الاحتيال، والبريد غير المرغوب فيه، والجرائم ضدّ الأطفال، والمحتوى غير المشروع، وغيرها الكثير مما يعتبر جرائم سيبرانية، ضدّ الأشخاص وضد الأموال.

تسعى الدراسة الحاليّة التي تعالج الجريمة الإلكترونية إلى فكّ طلاسم الجريمة الإلكترونية بتعقيداتها، والتي تربط بين التطور التكنولوجي والجريمة. ولتحقيق هذا الهدف سنحاول الإجابة عن التساؤلات التالية:

1- ما الدور المزدوج للتطوّر التكنولوجي؟
2- كيف يلعب التطور التكنولوجي دوراً في الجريمة المنظّمة عبر الحدود الوطنية؟
3- كيف نغيّر أدوات الجريمة وأساليبها؟
4- ما طبيعة التنافس في استخدام الأساليب التكنولوجية للجريمة وفي الوقاية منها؟
5- ما طبيعة جرائم الحاسوب الآلية وشبكة المعلومات الدولية؟
6- هل يكفي ما تقوم به الجهات الحكوميّة في مواجهة الجرائم الإلكترونية وتحديد حجمها؟

الخطة العامة للرسالة

سيتناول موضوع هذه الدراسة فصلين بالإضافة الى الخاتمة، اذ يتضمن **الفصل الأول** ماهية جرائم الإنترنت بالإضافة إلى مصادر الإعتداءات ودوافع إرتكابها، والذي سنتناوله على مدى مبحثين، نستعرض في **المبحث الأول** منه تعريف الجرائم الإلكترونية وبيان أركانها وتحديد أنواعها وآثارها، أما **المبحث الثاني** فسنخصصه لبيان النظام القانوني لهذه الجرائم.

أما **الفصل الثاني**، سنخصّصه لعرض المخاطر والتَّحدِّيات المحدقة بالجرائم السيبرانيَّة و أبرز طرق مكافحتها وذلك من خلال عرض التحديات والوسائل الوقائيَّة على صعيد التشريع **(مبحث أول)** وكيفية مكافحة الجرائم الإلكترونية على صعيد سلطات إنفاذ القانون ومن خلال التَّوعية والتَّدريب **(مبحث ثاني)**

وبسبب الأهمية المتزايدة لهذه الجريمة الحديثة في الوقت الحاضر، فقد آثرت الكتابة في هذه (الجرائم الإلكترونية) ودراستها بشكل مُعمَّق لغرض توضيحها والاطلاع على ما يجري بخصوصها، محاولاً الإدلاء ببعض ما أعانني الله عليه، لأنه يبقى في النهاية جهداً انسانياً يحتمل الخطأ والنسيان.

الإطار النظري

القسم الأول

مفهوم الجرائم المرتكبة عبر وسائل التواصل الإجتماعي

تمهيد

في ظلِّ الثَّورة المعلوماتية و"عصر الإنسان المعلوماتيّ" وبالرغم من التسهيلات العديدة التي تقدمها المعلوماتية فإنَّها تؤدّي إلى مخاطر عديدة وظهور أنواع جديدة من الجرائم التي تقترف من قبل أشخاص لديهم المهارات والمعرفة، ما يجعلهم يمثِّلون تهديداً حقيقيّاً على المجتمع. إنَّها جرائمٌ تطال المعرفة، الإستخدام، الثِّقة، الأمن، الرّبح ،المال، السمعة، الإعتبار...

إنَّ مفهوم جرائم الإنترنت مرَّ بتطوّر تاريخيٍّ تبعاً لتطوّر التقنيَّة واستخدامها. ففي المرحلة الأولى من شيوع إستخدام الكمبيوتر في الستينات ومن ثم السبعينات ظهرت أوَّلُ معالجات لما يسمّى جرائم الكمبيوتر. ترافقت هذه النقاشات مع التساؤل حول ما إذا كانت هذه الجرائم مجرد شيء عابر أم ظاهرة جرمية مستجدّة.

لذلك فإنَّنا سوف نتطرق في هذا الفصل إلى تعريف ماهية جرائم الإنترنت وأنواعها وآثارها **(مبحث أوَّل)** ثم ننتقل إلى النظام القانوني للجرائم المرتكبة عبر وسائل التواصل الاجتماعي **(مبحث ثاني).**

المبحث الأوَّل

ماهية الجرائم الإلكترونية

إن جرائم الانترنت هي امتداد لما عرف بجرائم الحاسوب ، والمقصود بجرائم الحاسوب: "كل عمل إجرامي ـ غير قانوني ـ يرتكب باستخدام الحاسوب كأداة أساسية، ودور الحاسوب في تلك الجرائم قد يكون هدفا للجريمة أو أداة لها. "

وعندما ظهرت شبكة الانترنت ودخلت جميع المجالات كالحاسوب، بدءا من الاستعمال الحكومي ثم المؤسساتي والفردي، كوسيلة مساعدة في تسهيل حياة الناس اليومية ، انتقلت جرائم

الحاسوب لتدخل فضاء الانترنت كأداة أساسية ، وكما هو الحال في جرائم الحاسوب، كذلك جرائم الانترنت قد تكون الانترنت هدفا للجريمة أو أداة لها.

والمقصود بجرائم الإنترنت الجرائم السبرانية ، وهو " أي نشاط غير مشروع ناشئ في مُكوّن أو أكثر من مكونات الإنترنت، مثل مواقع الإنترنت، وغرف المحادثة، أو البريد الإلكتروني، ويمكن أن تشمل أيضاً أي أمر غير مشروع، بدءاً من عدم تسليم البضائع أو الخدمات، مروراً باقتحام الكمبيوتر، وصولاً إلى انتهاك حقوق الملكية الفكرية، والتجسس الاقتصادي ، والابتزاز على الإنترنت، وتبييض الأموال الدولي، وسرقة الهوية، وقائمة متنامية من الجرائم الأخرى التي يسهلها الإنترنت."

ويجب الإشارة الى أن جرائم الانترنت لا تقع على ماديات وإنما على معنويات الكمبيوتر وما يحتويه من معلومات ، وهذا ما استوجب معه على الدول ان تسن تشريعات تعرف من خلالها الأفعال المجرّمة وتحددها مقابل وضع العقاب المناسب لها. وقد عرفت جرائم الانترنت بحسب أشكالها ، فنجد أن لكل شكل تعريف خاص به، نظرا لطريقة ووسيلة ارتكابه، او الهدف منه أو محله، وهو ما سأتعرض له ضمن أنواع جرائم الانترنت.

المطلب الأول: مفهوم الجرائم الإلكترونية، خصائصها، دوافعها

إنّ الجريمة بشكلٍ عام عبارة عن سلوك إراديّ يُجرّمه القانون ويقرر لفاعله عقوبة، لكن مع العلم أن أي جريمة مهما كانت لا تعد مستوجبة العقوبة إلا إذا توفرت جميع أركانها، فلا تخضع جميع الجرائم إلى القواعد نفسها، بل إنّ لكل جريمة قواعد خاصة بها تختلف عن الأخرى، وتنقسم الجريمة إلى نوعين، النوع الأول الجرائم الواقعة على الأشخاص، كالاغتصاب والخطف والقتل والضرب المُفضي للموت، والنوع الثاني الجرائم الواقعة على الأموال، كالسرقة التامة والموصوفة وإساءة الإئتمان والغش والإحتيال، لذا سيتم توضيح أركان الجريمة، ومفهوم الجرائم الإلكترونية، وأهداف ارتكاب الجرائم الإلكترونية، وجرائم أنظمة المعلومات[1] وآثارها على المستوى الوطني والعالمي.

الفرع الأول: المفهوم اللغوي والفقهي للجريمة الإلكترونية

تتكون الجريمة الإلكترونية أو الافتراضية (cyber crimes) من مقطعين هما الجريمة (crime) والإلكترونية (cyber). ويستخدم مصطلح الإلكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات. أما الجريمة فهي السلوكيات والأفعال الخارجة على القانون. والجرائم الإلكترونية

[1] فرج القصير (2006)، القانون الجنائي العام، تونس: مركز النشر الجامعي، صفحة 37.

هي "المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي أو عقلي للضحية مباشر أو غير مباشر باستخدام شبكات الاتصالات مثل الإنترنت (مثل غرف الدردشة، والبريد الإلكتروني، والموبايل). ويمثل جوهر الجريمة الإلكترونية، أبعد من هذا الوصف، ومع ذلك فالأعمال ذات الصلة بالحاسوب لأغراض شخصية أو تحقيق مكاسب مالية أو ضرر، بما في ذلك أشكال الجرائم المتصلة بالهوية، والأفعال المتعلقة بمحتويات الكمبيوتر جميعها تقع ضمن معنى أوسع لمصطلح "الجريمة الإلكترونية.

وتعرف جرائم الإنترنت بأنها الجرائم التي تعرف الحدود الجغرافية والتي يتم ارتكابها بأداة هي الحاسب الآلي عن طريق شبكة الإنترنت وبواسطة شخص على دراسة فائقة لها[1].

ويتشابه تعريف الجريمة الإلكترونية مع تعريف الجريمة التقليدية، حيث تُعرف على أنها "إتيان فعل" معاقب عليه، أو ترك فعل مأمور به ومُعاقب على تركه، ويشمل المفهوم العام للجريمة كل معصية أوخطيئة مخالفة لأوامر الله أو نواهيه، سواء كانت هذه المعصية نتيجة سلوك، يمكننا أن نلمسه مادياً، أم كانت المعصية مستترة في النفس البشرية، وسواء كانت العقوبة المقررة لها دنيوية أم عقوبة أخروية. ويعرف الماوردي الجريمة بأنها "محظورات شرعية زجر الله تعالى عنها بحدّ أو تعزير". وقد عرّف الفقهاء الجريمة وفقاً لهذا المفهوم بأنها "فعل ما نهى الله، وترك ما أمر الله به".

كذلك يمكن تعريف جرائم الإنترنت أو الجرائم الإلكترونية بأنها "كل نشاط إجرامي تكون شبكة الإنترنت دوراً هاماً في إتمامه على أن يكون هذا الدور على قدر من الأهمية، ولا يختلف الأمر سواء تم النشاط عبر شبكة تضم عدة حسابات آلية أو كانت الشبكة وسيلة لارتكابه". الجريمة الإلكترونية تعدّ جريمة معلوماتية ولكن ليست كل جريمة معلوماتية جريمة إلكترونية، فالجريمة الإلكترونية لا بد وأن ترتكب في إطار شبكة تضم عدة حسابات آلية.

الفرع الثاني: التعريف الدولي لهذه الجريمة

إن جرائم الكمبيوتر والإنترنت، أو ما يسمى Cyber Crimes هي ظواهر إجرامية تقرع أجراس الخطر لتنبه مجتمعنا عن حجم المخاطر والخسائر التي يمكن أن تنجم عنها، خاصة أنها جرائم ذكية تنشأ وتحدث في بيئة إلكترونية أو بمعنى أدق رقمية، يقترفها أشخاص مرتفعي الذكاء ويمتلكون أدوات المعرفة التقنية، مما يسبب خسائر للمجتمع ككل على المستويات الاقتصادية والاجتماعية والثقافية والأمنية. إذا كانت مجتمعاتنا العربية لم تتأثر بشكل كبير من مثل هذه الظواهر الإجرامية، إلا أن هناك دولاً عربية كثيرة أضحت مهتمة بتلك الظواهر، ومفهومها القانوني، وسمات

[1] World Drug Report 2013 – United Nations Office on Drugs and Crime.

المجرم المعلوماتي، وهو ما سوف نحاول أن نتعرض له بشيء من التفصيل في هذا البحث محاولين أن نضع ولو لبنة صغيرة في الإطار التنظيمي والتشريعي في تلك المسألة.

لا يوجد إجماع على تعريف الجريمة الإلكترونية من حيث كيف تُعرف، أو ما هي الجرائم التي تتضمنها الجريمة الإلكترونية.

وكما يقول فان دير هلست و ونيف "هناك غياب لتعريف عام وإطار نظري متسق في هذا الحقل من الجريمة، وفي أغلب الأحيان تستخدم مصطلحات الافتراضية والحاسوب والإلكترونية والرقمية.

تعتمد "تعريفات" الجريمة الإلكترونية في الغالب على الغرض من استخدام المصطلح، إذ أن هناك عدد محدود من الأفعال ضد السرية والنزاهة وتوافر بيانات الكمبيوتر أو أنظمته تمثل جوهر الجريمة الإلكترونية وأعمال متعلقة بالكمبيوتر لتحقيق مكاسب شخصية أو مالية أو ضرر، بما في ذلك أشكال الأفعال المتصلة بجريمة الهوية وجرائم محتويات الكمبيوتر لا تصلح بسهولة إلى الجهود للوصول إلى التعاريف القانونية للمصطلح الكلي.

ومثل تلك الجرائم قد تهدد أمن الدولة وسلامتها المالية والقضايا المحيطة بهذا النوع من الجرائم كثيرة وأبرز أمثلتها الاختراق أو القرصنة وانتهاك حقوق التأليف ونشر الصور الإباحية للأطفال ومحاولات استمالتهم لاستغلالهم والتجارة غير القانونية (كتجارة المخدرات) كما تضم انتهاك خصوصية الآخرين عندما يتم استخدام معلومات سرية بشكل غير قانوني.

ولا تقتصر الجرائم الإلكترونية على أفراد أو مجموعات وإنما قد تمتد إلى مستوى الدول لتشمل التجسس الإلكتروني والسرقة المالية وغيرها من الجرائم العابرة للحدود.

وأحيانا توصف الأنشطة التي تتعلق بالدول وتُستهدف فيها دولة أخرى واحدة على الأقل بأنها تقع في إطار "الحرب الإلكترونية"، والنظام القانوني الدولي يحاول تحميل الفاعلين المسؤولية عن أفعالهم في مثل هذا النوع من الجرائم من خلال المحكمة الجنائية الدولية.

الفرع الثالث: أسباب الجريمة الإلكترونية

هناك عدد من الأسباب التي يمكن حصرها كأسباب للجريمة الإلكترونية، منها ما يقع على مستوى كوني، ومنها ما يقع على مستوى مجتمعي، ومنها ما يقع على مستوى فردي أو شخصي. كما أنّ أسباب الجريمة الإلكترونية تتفاوت وفق نوعها ونوع المستهدف ونوع الجاني ومستوى تنفيذه (فردي، مجتمعي، كوني). فجرائم الشباب والهواة والصغار تختلف عن أسباب جرائم المحترفين،

وتختلف وفق هدفها (سرقة أو معلومات أو تجارة بالمعلومات أو شخصية...)[1].

1- من أسباب الجريمة الإلكترونية على المستوى الفردي[2]:

الفرصة: لقد وفَّرت التقنيات الحديثة والإنترنت فرصاً غير مسبوقة لانتشار الجريمة الإلكترونية. إن الفرصة تنتج الجريمة[3]، وتلعب البيئة وترتيباتها دوراً كبيراً في إنتاج الجريمة، والخروج عن القواعد الاجتماعية، فوقت الانحراف عن قواعد الامتثال ليلاً ونهاراً وفي أي مكان، وعدم وجود رقابة، كلها عوامل تزيد من فرصة ارتكاب الجريمة الإلكترونية. وقد تشكّل المعلومات هدفاً سهل المنال، ويحقق المنفعة السريعة، وبالتالي يمكن سرقتها، أو سرقة محتوياتها، فهي فرصة مربحة، وقليلة المخاطر، واحتمالية كشف الفاعل فيها ضئيلة[4].

إن تكنولوجيا المعلومات والاتصالات والاستخدام المتزايد للإنترنت قد خلقت فرصاً جديدة للمجرمين وسهّلت نمو الجريمة.

إن جرائم الإنترنت تمثّل شكلاً جديداً ومميّزاً للجريمة، وقد خلقت تحديات لتوقُّع التطورات، والوقاية منها.

2- أمّا أسباب الجريمة على المستوى المجتمعي[5]:

الضغوط العامة: يتعرّض المجتمع لظروف اقتصادية صعبة، كالفقر والبطالة والأميّة، وهي عوامل ضاغطة على المجتمع عامّة وخاصّة على قطاع الشباب، مما يولد مشاعر سلبية عند شرائح كبيرة من الناس ضد الظروف وضد المجتمع، مما يدفعهم إلى أساليب تأقلم سلبية مع هذه الظروف منهها: الاتجار الإلكتروني بالبشر، والجنس، والجريمة الإلكترونية وغيرها..

وما يحفّز الجريمة الإلكترونية أيضاً، غياب التشريعات الجزائية والجنائية وضعف الممارسات العدلية والشرطية والقضائية في المحاكمة والتحقيق في الجرائم الإلكترونية. وغالباً ما تجد في دول كثيرة أن التقنيات المتوافرة متواضعة جداً، وكذلك الخبراء القادرون على متابعة ورصد وملاحقة الجريمة الإلكترونية داخل المجتمع والعابرة منها للحدود الوطنية.

---

[1] د. دياب موسى البداينة، الظواهر الإجرامية المستحدثة وسبل مواجهتها، 1999 جرائم الحاسوب والإنترنت، في مركز الدراسات والبحوث، الرياض.

[2] المرجع نفسه، ص9.

[3] المرجع نفسه، ص10.

[4] World Drug Report 2013 – United Nations Office on Drugs and Crime.

[5] المرجع نفسه، ص14.

ومن أسباب الجريمة على المستوى الكوني هو العولمة: إن ظهور "الفضاء الإلكتروني" يخلق ظواهر جديدة متميزة عن وجود أنظمة الكمبيوتر نفسها، والفرص المباشرة للجريمة والتي وفّرتها أجهزة الكمبيوتر الآن ضمن الفضاء الإلكتروني، قد يُظهر الفرق بين الأشخاص في الامتثال (القانوني) وعدم الامتثال (غير القانوني) مقارنة مع سلوكهم في العالم المادي. فالأشخاص على سبيل المثال، قد يرتكبون جرائم في الفضاء الإلكتروني لا يرتكبونها في الواقع المادي وعدم ظهور الهوية بسبب مكانتهم وموقعهم. بالإضافة إلى ذلك فمرونة الهوية (identity flexibility)، وضعف عوامل الردع تحفّز السلوك الإجرامي في العالم الافتراضي[1].

3- دوافع وطرق ارتكاب جرائم الإنترنت:

بالنسبة لهذا النوع من الجرائم فثمة دوافع عديدة تحرّك الجناة لارتكاب أفعال الاعتداء ومن هذه الدوافع:

أ- السعي إلى تحقيق الكسب المالي والسرقة والابتزاز:

يعد هذا الدافع (الذي يمثل في الحقيقة غاية الفاعل)، من بين أكثر الدوافع تحريكاً للجناة لاقتراف هذه الجرائم. ومنذ بدايات الظاهرة فإن الدراسات إشارة إلى أن المحرك الرئيسي لأنشطة احتيال المعلوماتية هو تحقيق الكسب المالي.

وهذا النوع من مجرمي الإنترنت خطير، وهذه الفئة عادة ما تكون عديمة الضمير وهم على استعداد لارتكاب أي نوع من الجرائم، طالما أنها تجلب لهم المال. حيث "بدأوا في إنتاج المواد الإباحية وغالباً ما تسمى السيبرانية للمواد الإباحية والتي تشمل الإباحية القانونية وغير القانونية على شبكة الإنترنت". هم عادة ما يكونون أذكياء جداً ومنظمون ويعرفون كيفية الهروب من وكالات إنفاذ القانون. ومجرمو الإنترنت هؤلاء يرتكبون الجرائم الخطيرة، وخاصة جرائم إباحية الأطفال والقمار الإلكتروني، وهذه تشكل تهديداً خطيراً للمجتمع.

ب- الرغبة في قهر النظام والتفوق على تعقيد الوسائل التقنية:

يرى البعض أن الدافع إلى ارتكاب هذا النوع من الجرائم يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح، حيث يميل مرتكبو هذه الجرائم إلى إظهار تفوقهم ومستوى ارتقاء براعتهم ولا بد من الإشارة إلى أنه يتزايد شيوع هذا الدافع لدى فئة صغار السن الذين يمضون وقت طويل أمام حواسيبهم.

[1] المرجع السابق، UNODC, 2013

ج- الانتقام من المؤسسة:

هناك عدد من موظفي تكنولوجيا المعلومات يحتفظ بكلمات المرور في بيته ليســـرقها منه قريب أو صـــديق أو جار له دائم التردد عليه، ثم يســـتثمرها بإجرام أو يعطيها لمن لديه القدرة على استخدامها بعد إبرام اتفاق على اقتسام الغنيمة.

الفرع الرابع: خصائص الجريمة الإلكترونية

يمكن تلخيص خصائص الجريمة الإلكترونية بما يلي:

1- الحاسوب الآلي هو أداة ارتكاب الجريمة: من المعلوم أن خاصية الحاسوب الآلي هو دائماً أداة للجريمة في الجرائم التي ترتكب على شبكة الإنترنت وهي خاصة تنفرد عن الجرائم الأخرى ذلك أن الحاسوب الآلي هي الأداة الوحيدة التي تمكن الشخص من الدخول على شبكة الإنترنت Internet وقيامه بتنفيذ جريمته أيّاً كان نوعها. وعليه فالحاسوب الآلي هو الأداة الوحيدة لارتكاب أي جريمة من الجرائم التي ترتكب على شبكة الإنترنت.

2- جرائم ترتكب عبر شبكة الإنترنت: تعدّ شبكة الإنترنت هي حلقة الوصل بين كافة الأهداف المحتملة وتلك الجرائم كالبنوك والشركات الصناعية وغيرها من الأهداف التي غالباً ما تكون ضحية لتلك الجرائم.

3- مرتكب الجريمة هو شخص ذو خبرة فائقة في مجال الحاسوب الآلي: لاستعمال الحاسوب الآلي من أجل تنفيذ جريمة ما على شبكة الإنترنت لا بد وأن يكون مستعمل هذا الحاسوب الآلي على دراية ومعرفة فائقة، وذا خبرة كبيرة في مجال استعماله، ولذلك نجد أنّ معظم من يرتكبون تلك الجرائم هم من الخبراء في مجال الحاسوب، وأن الشرطة تبحث أول ما تبحث عن خبراء الحاسوب عند ارتكاب الجرائم.

4- الجريمة لا حدود جغرافية لها: شبكة الإنترنت ألغت أي حدود جغرافية في ما بين الدول، إذ يمكن التحدث في ما بين أشخاص ليس في بلدان مختلفة فحسب، وإنما في قارات مختلفة في الوقت نفسه على شبكة الإنترنت من الدردشة. وعليه، فإنّ أي جرائم ترتكب عبر شبكة الإنترنت تتخطى حدود الدولة التي ارتكبت فيها لتتعدى آثارها البلدان كافة على مستوى العالم.

5- جرائم الحاسوب والإنترنت: هناك مجموعة من الجرائم تتّسم بسمات مخصوصة عن غيرها من الجرائم، فهي تستهدف معنويات وليست ماديات محسوسة، وتثير في هذا النطاق مشاكل الاعتراف بحماية المال المعلوماتي إن جاز التعبير.

6- كما أنها تتّسم بالخطورة البالغة نظراً إلى أغراضها المتعددة: ونظراً إلى حجم الخسائر الناجمة عنها، قياساً بالجرائم التقليدية، لارتكابها من عدة فئات تجعل من التنبؤ بالمشتبه بهم أمراً صعباً.

7- صعوبة التحقيق والتحرّي في جرائم الحاسوب والإنترنت والمقاضاة في نطاقها: حيث تنطوي على مشاكل وتحديات إدارية وقانونية تتصل ابتداء بمعوقات ومتطلبات عمليات ملاحقة الجناة، فإن تحققت إمكانية الملاحقة أصبحت الإدانة صعبة لسهولة إتلاف الأدلة من قبل الجناة، أو لصعوبة الوصول إلى الأدلة، أو لغياب الاعتراف القانوني بطبيعة الأدلة المتعلقة بهذه الجرائم. ونظراً إلى أنها جرائم لا تحدّها حدود، وتعدّ من الجرائم العابرة للحدود، فإنها تثير لذلك تحديات وعوائق كثيرة في حقل الاختصاص القضائي والقانون الواجب التطبيق ومتطلبات التحقيق والملاحقة والضبط والتفتيش.

إن جرائم الحاسوب الآلي قد ترتكب عن طريق حاسوب آلي في دولة ما، في حين يتحقق الفعل الإجرامي في دولة أخرى. فجرائم الحاسوب والإنترنت لا تحدّها حدود، ولا تعترف ابتداء في هذه المرحلة من تطوّرها بسبب شبكات المعلومات بعنصر المكان أو حدود الجغرافيا. وتتميّز بالتباعد الجغرافي بين الفاعل والمجني عليه. ومن الوجهة التقنية، بين الحاسوب أداة الجريمة وبين المعطيات أو البيانات محل الجريمة في نظام الحاسوب المستهدفة بالاعتداء. وهذا التباعد قد يكون ضمن دائرة الحدود الوطنية للدولة، لكنه وبفعل سيادة تقنيات شبكات النظم والمعلومات امتد خارج هذه الحدود – دون تغيير في الاحتياجات التقنية – ليطال دولة أخرى يوجد فيها نظام الحاسوب المخزّنة فيه المعطيات محل الاعتداء.

في الحقيقة، إن مسألة التباعد الجغرافي بين الفعل وتحقيق النتيجة من أكثر المسائل التي تثير إشكالات في مجال جرائم الحاسوب، وبشكل خاص الإجراءات والاختصاصات والقانون الواجب التطبيق. وهذا بدوره عامل رئيس في نمو دعوات تضافر الجهود الدولية لمكافحة هذه الجرائم الخطيرة التي باتت واحدة من أهم سمات عصرنا هذا، بل من أهمّ ظواهره.

ومن خصوصيّة الجريمة الإلكترونية أن بعض حالات ارتكابها يتعمّد مرتكبها التدخل في مجالات النظام المعلوماتي المختلفة؛ منها مجال المعالجة الإلكترونية للبيانات، ومجال المعالجة الإلكترونية للنصوص والكلمات الإلكترونية. في المجال الأول يتدخل الجاني من خلال ارتكاب الجريمة الإلكترونية في مجال المعالجة الإلكترونية (الآلية) للبيانات، سواء من حيث تجميعها أو تجهيزها حتى يمكن إدخالها إلى جهاز الحاسوب الآلي، وذلك بغرض الحصول على المعلومات. وفي المجال الثاني يتدخل الجاني في مجال المعالجة الإلكترونية للنصوص والكلمات، وهي طريقة

أوتوماتيكية تمكن مستخدم الحاسوب الآلي من كتابة الوثائق المطلوبة بدقة متناهية بفضل الأدوات الموجودة تحت يده، وبفضل إمكانيات الحاسوب الآلي تتاح إمكانية التصحيح والتعديل والحذف والتخزين والاسترجاع والطباعة، وهي بذلك علاقة وثيقة بارتكاب الجريمة.

الفرع الخامس: آثار الجريمة الإلكترونية

إن جريمة الحاسب الآلي من أعظم الجرائم وأخطرها على الفرد والمجتمع فهي تؤدي إلى انتهاك حقوق الإنسان وزعزعة الإستقرار الاجتماعي وتهديد سيادة الدول وتهديد حياة الأفراد.

وإنّ المحادثات الإلكترونية عبر شبكة الإنترنت أصبحت وسيلة تهدد سلامة المجتمع ونظامه الأخلاقي، فقد تسبّبت تلك المحادثات في ارتكاب جرائم أخلاقية ضدّ الأطفال على أيدي أشخاص عديمي الأخلاق والضمير.

كما أنّ لهذه الجرائم تأثيرها ومخاطرها الكبيرة على الإقتصاد نسبة إلى الكوارث المالية التي تنتج عنها حيث قُدِّرت الخسائر الناجمة عن الجرائم ذات العلاقة بالحاسب الآلي التي تُمنى بها الشركات الأمريكية أكثر من 5 مليارات دولار سنوياً.

نشير إلى أنّ إحصاء قامت به الجمعية الأمريكية للأمن الصناعي للتدليل على مدى تأثير هذه الجرائم على اقتصاد الدول ومخاطرها العظيمة، حيث تشير إحصاءات هذه الجمعية للآتي:

أ. تبلغ الخسائر المالية التي يمكن أن تسبّبها جرائم الحاسب الآلي للصناعات الأمريكية 63 بليون دولار أمريكي.

ب. يبلغ متوسط سرقات البنوك المرتكبة بواسطة الحاسب الآلي 1,5 مليون دولار في العالم علماً بأن المكتَشَف من تلك الجرائم لا يتجاوز الـ 1%.

ج. إن 25% من بين 500 شركة أمريكية تتضرر من جرائم الحاسب الآلي بخسائر تتراوح بين 2 و10 مليون دولار في العام[1].

نذكر مثلاً الاختراق الذي طال بيانات موقع آشلي ماديسون، حيث كُشفت مئات من رسائل البريد الإلكتروني التي تنتمي لمسؤولي حكومة الولايات المتحدة، واستخدمت هذه الرسائل التي كتبها هؤلاء المسؤولين للغش على أزواجهم. هؤلاء الناس يمثلون كل جزء من البيروقراطية الفيدرالية مثل الموظفين الفدراليين في البيت الأبيض، وموظفي الكونغرس، والوكالات الفيدرالية، بما في ذلك وزارة الأمن الداخلي.

[1] المجلة العربية للدراسات الأمنية والتدريب، **"التحقيق في جرائم الحاسب الآلي"**، المجلد 15، عدد 130، ت1، 2000، ص. 318.

موظفي البيروقراطية الفيدرالية من أقسام مختلفة مثل الخارجية والدفاع والعدل والطاقة والخزانة والنقل والأمن الداخلي كانوا بين أولئك الذين يتمتعون بكونهم جزءاً من شبكة الزنا هذه، بعض البيروقراطيين حتى كانوا يعملون مع البنتاغون. وقد كُشفت البيانات العائدة لهؤلاء المسؤولين بسبب استخدامهم عنوان البريد الإلكتروني الرسمي.

كان يمكن أن تمر الأمور دون أن يلاحظها أحد، ولكن عنوان بريد إلكتروني تم تعقّبه من قِبل صحفي محقق تبين أنه عائد لأحد الرسميين الذي اعترف بعضويته في الموقع.

وقد أعلن وزير الدفاع أشتون كارتر عن فتح تحقيق حول كل هؤلاء الأشخاص الذين لديهم حسابات في هذا الموقع. هذا الفعل يمكن أن يشكّل جريمة بموجب المحكمة العسكرية للعدالة في الولايات المتحدة. وقد كشف هذا الاختراق أن الموظفين الفدراليين لديهم الميل نحو استخدام عناوين بريد إلكتروني وهمية مع اسم مستعار مثل: Latinlovers, soontobesingle لجذب الجنس الآخر تجاههم. وقد بلغ مجموع عناوين البريد الإلكتروني 6788 وهي تعود للنطاق الإلكتروني us.army.mil و 1655 رسالة بريد إلكتروني للنطاق الإلكتروني navy.mil وكان الوضع أسوأ بالنسبة لأولئك المسؤولين الذين يعملون في مواقع حساسة، وكانوا قد أتاحوا استعمال مواقعهم الجغرافية على الموقع المذكور.

وقد صرح أحد المسؤولين الأميركيين بأن الولايات المتحدة تستحقُّ أفضل من هؤلاء الموظفين الفدراليين الذين يستخدمون أجهزة الكمبيوتر الحكومية الفاقدة للحماية لزيارة هذه المواقع. والسؤال الأكبر هو، هل ظنّوا في أي وقت مضى أن أي شخص قد يستخدم هذه البيانات لابتزازهم، وكيف تركت إدارة أوباما هؤلاء القراصنة الصينيين يمضون قدماً بمثل هذه البيانات الحساسة، وهو أمر محرج حقاً أن ما يفعله من هم في مناصب عليا، هو قضاء الوقت على مواقع الزنا[1].

وفي حزيران 2015، تم اختراق الخطوط الجوية البولندية حيث تم إلغاء عشر رحلات بسبب حصول خرق في نظام أجهزة الكمبيوتر الخاصة بالطائرات، هذا الاختراق أثّر على الكثير من المسافرين في الرحلات الدولية عبر بولندا، فقد حوصر نحو 1400 راكب بسبب هذا الاختراق لأجهزة الكمبيوتر[2].

[1] http://www.hackersnewsbulletin.com/2015/08/hack-revealed-big-names-white-house-security-staff-federal-employees-users-ashley-madison.html

[2] http://www.hackersnewsbulletin.com/2015/06/poland-international-flights-system-got-hacked-affecting-10-flights-1400-passengers.html

وبحسب صحيفة رويترز فقد بلغت تكاليف الجريمة السيبرانية للاقتصاد العالمي حوالي 445 بليون دولار سنوياً، مع الأضرار التي لحقت المؤسسة التجارية من سرقة للملكية الفكرية تتجاوز الـ 160 مليار دولار للأفراد من القرصنة، وفقاً لدراسة نشرت عام 2014[1].

إن التقرير الصادر عن مركز الدراسات الإستراتيجية والدولية (CSIS) قال أن الجريمة السيبرانية صناعة في طور النمو وقد أضرّت بالتجارة والمنافسة والابتكار.

وقالت الدراسة، التي ترعاها شركة أمن البرمجيات مكّافي أن تقدير الخسائر بحدّه الأدنى سوف يكون 375 بليون دولار، في حين أن الحد الأقصى يمكن أن يكون 575 بليون دولار، وبحسب المصدر فإن "الجريمة السيبرانية هي ضريبة على الابتكار وتبطئ وتيرة الابتكار العالمي عن طريق الحد من معدل العائد للمبتكرين والمستثمرين"، و"بالنسبة للبلدان المتقدمة فإن الجريمة السيبرانية لها تداعيات خطيرة على فرص العمل".

وتتحمل أكبر الاقتصادات في العالم وطأة الخسائر، بحسب الأبحاث. فالخسائر على الولايات المتحدة والصين واليابان وألمانيا تصل إلى 200 مليار دولار في السنة كمجموع، أما الخسائر المتصلة بالمعلومات الشخصية، مثل بيانات بطاقات الائتمان المسروقة، فقد وصلت إلى 150 مليار دولار.

وقال نحو 40 مليون شخص في الولايات المتحدة، أن حوالي 15 في المئة من السكان، تم سرقة معلوماتهم الشخصية من قبل القراصنة، في حين أن الانتهاكات رفيعة المستوى أثرت على 54 مليون شخص في تركيا، 16 مليون في ألمانيا، وأكثر من 20 مليون شخص في الصين.

وقالت McAfee المملوكة من قبل شركة "انتل كورب" أن تحسين التعاون الدولي قد بدأ يؤتي ثماره في الحد من الجرائم الإلكترونية، وخير مثل على ذلك توقيف عصابة إجرامية خرقت مئات الآلاف من أجهزة الكمبيوتر باسم برنامجها المشهور Gameover Zeus[2].

المطلب الثاني: صور الجرائم الإلكترونية وهي كثيرة منها:

الجرائم الإلكترونية هي كل محاولة لابتزاز أو إيقاع أو إجبار شخص ما على أن يقدم لك خدمة مقابل المفاوضة على صور أو مقاطع صوتية أو مرئية أو حتى محادثات ومعلومات شخصية من الممكن أن يؤدي انتشارها إلى إلحاق أذى مباشر لحياة الضحية أو لسمعته ونفسيته.

[1] http://www.reuters.com/article/2014/06/09/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609
[2] http://www.hackersnewsbulletin.com/2015/06/poland-international-flights-system-got-hacked-affecting-10-flights-1400-passengers.html

من الممكن أن تكون الجريمة الإلكترونية (المعلوماتية) تستهدف مؤسسة كاملة أو مجموعات كاملة وليس فقط الأفراد. أهدافها الأساسية هي حصول المبتز أو المجرم الإلكتروني على أهداف مادية مثل النقود أو على خدمات جنسية يقدمها الضحايا مقابل المحافظة على عدم نشر صورهم ومعلوماتهم.

ويكسب المبتزون مبالغ هائلة من المال في حال خضعت لهم الضحية وذلك ما سنحاول أن نعالجه في المطلب الثاني من خلال عرض أنواع الجرائم الإلكترونية التي من الممكن أن نواجهها في عالم وسائل التواصل الاجتماعي، لكي نبدأ بفهم كيفية التعامل مع مثل هذه الحالات ومثل هؤلاء المجرمين.

للجرائم الإلكترونية عدة أشكال وأنواع تُستخدم من قبل قراصنة المعلومات أو أشخاص آخرين سنعرض أهمها.

الفرع الأول: القدح والذم والتشهير الإلكتروني

تعد جرائم الذم والقدح والتشهير من أكثر الجرائم الإلكترونية شيوعًا، حيث يساعدها على التعبير عن الجريمة كتابةً أو صوتاً استغلال المعطيات الحاسوبية لإرسال هذه المواد إلى المعتدى عليه، لهدف النيل من شرفه وكرامته، أو تعريضه لبغض الناس وتشهيرهم دون الحاجة إلى مواجهته في مجلس مشهود في العالم الواقعي، ومع التمتع بالمجهولية التى تتيحها تلك الوسائط الإلكترونية الحديثة.

وقد أثار استغلال تقنية المعلومات لتنفيذ هذا النوع من الجرائم تحديات كبيرة بالنسبة لقانون العقوبات؛ ففي إطار مجتمع المعلومات الإلكترونية أدى الباعثون غرضهم في نشر رسائل وبثها، وهي تحتوي عبارات الذم والقدح لأشخاص مستهدفين بذاتهم أو مستهدفين لانتمائهم إلى مجموعات عرقية أو دينية أو سياسية معينة. سوف نقف على أساليب ارتكاب جريمة الذم والقدح والتشهير، وعلى وسائل العلنية عبر الشبكة الافتراضية (الإنترنت) وشبكة الهواتف النقالة.

إن جرائم الذم والقدح والتشهير هي إحدى أكثر الجرائم شيوعًا في العالم الافتراضي، فالبُعد الجغرافي بين المعتدي والمعتدى عليه، والمجهولية، وسرعة انتشار الأسانيد الجارحة عبر التقنية الرقمية، كل ذلك يشجع المعتدين على ارتكاب هذه الجرائم للنيل من شرف الغير وكرامته، وتتنوع أساليب الذم والقدح والتشهير بتنوع الغرض من استخدام شبكة الإنترنت وشبكة الهواتف النقالة، ويتم عادة من خلال المراسلات والنشر الإلكتروني. ويقع الذم والقدح وجاهيًا عبر خطوط الاتصال

المباشر، ويقع غيابيًا وقد يقع أيضاً بواسطة المطبوعات الإلكترونية إذا تجاوزت العبارات حدود النقد المباح.

من المتعارف عليه تقليدياً أن جرائم القدح والذم كانت ترتكب إما بالفعل أو بالقول أو الكتابة، غير أنه مع التطور الذي شهدته الإنسانية في تكنولوجيا الاتصال، ظهرت وسيلة جديدة وخطيرة لارتكاب جرائم القدح والذم في شبكات التواصل الإلكترونية.

4- هل تعتبر شبكة الإنترنت وسيلة نشر المنصوص عنها في المادة 209 عقوبات؟

نص المادة 209 عقوبات: تعد وسائل نشر الأعمال والحركات إذا حصلت في محل عام أو مكان مباح للجمهور أو معرض للأنظار أو شاهدها بسبب خطأ الفاعل من لا دخل له بالفعل. الكلام أو الصراخ سواء جهر بهما أو نقلاً بالوسائل الآلية بحيث يسمعها في كلا الحالين من لا دخل له بالفعل.

بمراجعة للمادة المذكورة، يتبين أن المشترع تكلم بشكل واضح عن الوسائل الآلية دون تحديدها وتالياً لا يجوز إخراج أي وسيلة آلية يمكن النشر من خلالها. وأن الاعتراف بشمول المادة 209 للإنترنت والحاسوب ووسائل التواصل الحديثة لا يعتبر على سبيل القياس الذي لا يجوز اللجوء إليه في قوانين العقوبات. مما ينطبق على جرائم القدح والذم المرتكبة بواسطة شبكة الإنترنت، غير أن المعول عليه هو ليس وسيلة النشر بل النشر بحد ذاته الذي يؤلف الجريمة، وتحديداً عندما يستطيع إنسان التأثير على عدة أشخاص.

كما عرّفتها المادة 3 من قانون المطبوعات بأنها وسيلة النشر على تدوين الكلمات والأشكال بالحروف والصور والرسوم، وعليه تعتبر محاكم المطبوعات اللبنانية أن النشر عبر شبكة الإنترنت وتحديداً في المواقع الإلكترونية هو من وسائل النشر المحددة بالمادة 3 من قانون المطبوعات خصوصاً متى كان الموقع يعود للصحف والمجلات المحددة هويتها والموجهة إلى القراء.

وعليه، فإن النيابة العامة في لبنان اعتادت أن تدّعي في جرائم القدح والذم المرتكبة من خلال مواقع الصحف أو المجلات الإلكترونية أمام محكمة المطبوعات حتى ولو لم يكن لهذه المواقع نسخة ورقية.

بيدَ أن لتحقق جرائم القدح والذم يجب توافر كل من الركن المادي والركن المعنوي، حيث أن الركن المادي يتمثل بمحتوى المنشور على شبكة الإنترنت والمتضمن القدح والذم وهو ما يعرف بموضوع الجريمة، والنشر الذي هو فعل الاعتداء ومن النتيجة الجرمية التي تتحقق بوصول المحتوى إلى العامة بالصورة العلنية بعد تعيين الشخص الموجّه له القدح والذم.

أما الركن المعنوي يتمثل بالقصد الجرمي، فالمشترع اللبناني لا يعاقب على القدح والذم، إلا إذا رافقتها النية الجرمية لدى صاحبها.

في الخلاصة، وبعد ملاحقة العديد من الأشخاص بسبب آرائهم وكتاباتهم في مواقع التواصل الاجتماعي، فإن شبكة الإنترنت تبقى متاحة للجميع والتشهير بسمعة الأشخاص لا يمكن التعويض عنه بحيث أنه يكفي بضع دقائق حتى ينتشر الخبر بين الملايين من البشر.

ليبقى السؤال، هل إن كرامات الناس مباحة لكل شخص تطاوله نفسه على التجريح بالآخر تحت راية الحريات المكرسة في الإعلان العالمي لحقوق الإنسان؟ أم إن حرية الصحافة جدار لا يمكن تجاوزه بخاصة متى تجاوز حدود الآخرين؟ وهل سيستدرك المشترع اللبناني الثورة التكنولوجية فينظمها ويحدّ من مخاطرها ونتائجها؟

الفرع الثاني: الابتزاز الإلكتروني

الابتزاز الإلكتروني من الناحية اللغوية هو محاولة الحصول على مكاسب مادية أو معنوية عن طريق الإكراه المعنوي للضحية، وذلك بالتهديد بكشف أسرار أو معلومات خاصة، والابتزاز بهذه الصورة يمتد ليشمل جميع القطاعات، فنجد ما يسمى بالابتزاز السياسي والابتزاز العاطفي والابتزاز الإلكتروني.

وتعدّ جريمة الابتزاز الإلكتروني من الجرائم المستحدثة بفعل التقدم الكبير في تكنولوجيا المعلومات، مما جعل من العالم قرية صغيرة، وسهل الكثير من أمور الحياة، ولا يخفى ما لهذا التطور من فوائد في النواحي الاقتصادية والسياسية والاجتماعية والعلمية إلا أنه لم يخلو من مواطن خلل، فقد سهلت لظهور نوع من المرجمين يستخدمون هذه التقنيات لتنفيذ جرائمهم بواسطتها، الابتزاز الإلكتروني هو الابتزاز الذي يتم باستخدام الإمكانيات التكنولوجية الحديثة ضد ضحايا أغلبهم من النساء لابتزازهم مادياً أو جنسياً.

يمكن تكييف جرائم الابتزاز قانونياً، وفقاً للمواد 469 من قانون العقوبات وما يليها، التي تتعلق بانتحال الهوية بهدف الاحتيال أو الإساءة إلى السمعة والتشهير، بالإضافة إلى المادة 650 المتعلقة بالتهديد والابتزاز مثل فضح معلومات تم الاستحصال عليها عبر الإنترنت وابتزاز الشخص المهدّد، وهناك أيضاً حماية الخصوصية المعلوماتية عبر قانون حماية الملكية الأدبية والفنية رقم 75، تاريخ: 1999/04/03.

يواجه العالم تحدياً خطيراً يعتبر أحد إفرازات ثورة التكنولوجيا الرقمية الآخذة في التطور يوماً تلو الآخر، ولعل الابتزاز الإلكتروني بات واحداً من إفرازات تلك الثورة، وربما يكون أكثرها

انتشاراً، لا سيما أنه لا يتطلب المزيد من الأدوات أو التخطيط الدقيق لاصطياد ضحاياه، حيث يحتاج المبتز غلى صورة أو مقطع مصور أو حتى معلومة في إحدى منصّات التواصل الإلكتروني لينسج بعد ذلك فصول جريمته التي يدر من خلالها أموالاً كثيرة عبر طرق وحيل الابتزاز الإلكتروني المتعارف عليها في عالم المبتزين.

ورغم أن الغرض من جرائم الابتزاز الإلكتروني هو الحصول على المال، إلا أن ضحايا تلك العمليات يتعرضون لظروف صعبة طوال فترة ابتزازهم بسبب خوفهم من الفضيحة أو التشهير بهم، وتؤدي تلك الظروف إلى تدهور الحالة النفسية للضحايا وترديها لدرجة تدفع البعض منهم إلى إنهاء حياته ما لم يتم التدخل في الوقت المناسب.

المختصون يرون أن الابتزاز الإلكتروني في تزايد، وأن التعامل غير الحذر مع منصات التواصل الإلكتروني والثقة في الآخرين هي أبرز أسباب الوقوع في فخ الابتزاز.

تطاول ظاهرة الابتزاز والتهديد عبر مواقع التواصل الرجال بنسبة 40% والنساء 60% من مختلف الفئات العمرية من عمر الخمس عشرة سنة حتى الخمسين، وفق ما كشفت عنه المديرية العامة لقوى الأمن الداخلي، في معلومات حصرية لـ"العربي الجديد". وكثرت الشكاوى الواردة من المواطنين إلى مكتب مكافحة جرائم المعلوماتية والملكية الفكرية (أُسس في مارس/آذار 2006)، وتحديداً ما يتعلق بجرم الابتزاز والتهديد عبر مواقع التواصل الاجتماعي في الآونة الأخيرة، نتيجة التطور الكبير في مجال المعلوماتية ووسائل التواصل الاجتماعي وارتفاع نسب الجرائم على الإنترنت، إذ بلغ عدد التحقيقات خلال عام 2017، 2175 تحقيقاً، وتم توقيف 237 شخصاً. اللافت أن عدد القضايا ارتفع بنسبة تصل إلى قرابة 100% من عام 2017، والذي تم التحقيق خلاله في 663 قضية وتوقيف 49 متهماً، فيما بلغ العدد 1229 قضية خلال عام 2018، الذي شهد توقيف 166 متهماً.

أما لناحية المبتزّ أو الشخص الذي يلجأ إلى التهديد، فهم في معظمهم من البالغين والشباب، ويتوزعون بين الجنسيات اللبنانية والسورية والمغربية والتونسية والمصرية. وبالنسبة إلى الضحايا، فهم بالنسبة الأكبر من الشباب والقصّار، في حين تعدّ النسبة الأقل من المسنّين، وهم في المجمل من الجنسيتين اللبنانية والسورية، وفق ما وثّقته المديرية العامة لقوى الأمن الداخلي.

وأدت الظاهرة إلى التأثير بشكل رئيسي على الحالات النفسية والاجتماعية للمواطنين، ما جعل نسبة كبيرة منهم يخشون تقديم الشكاوى مباشرة لدى القضاء المختص خشية نشر مقاطع الفيديو العائدة، أو خوفاً من نظرة المجتمع لهم فيعمدون إلى إرسال مبالغ مالية إلى المجرمين ومنهم من يعمد

إلى أذية نفسه، ووصلت في بعض الحالات إلى الانتحار وفق ما جاء في إفادة المديرية العامة لقوى الأمن الداخلي.

في بعض الحالات، لا يتم التوصل إلى معرفة الفاعل لوجود عدد كبير من مرتكبي الجرم خارج لبنان، وخاصة في قضايا الابتزاز الجنسي، وعدم وجود معلومات كافية عن الفاعلين، إذ يكونون في معظم الأوقات منتحلي صفة وبأسماء وهمية، وضياع الدليل الرقمي الذي من خلاله يتم تعقب الفاعل وتوقيفه، وعدم تزويد المكتب بمعلومات تنير التحقيق من قبل المدعين والتراجع عن الشكاوى المقدمة منهم، بحسب إفادة المديرية العامة التي لفتت إلى أن نتيجة التحقيقات في الشكاوى الواردة ليست بمعظمها إيجابية.

لكن المديرية العامة لقوى الأمن الداخلي تؤكد أن "أي تحقيق أو توقيف بهذه الجرائم يتم بناء على إشارة القضاء المختص وبالتنسيق معه، وذلك استناداً إلى القوانين اللبنانية المرعية الإجراء كقانون العقوبات وأصول المحاكمات الجزائية والقانون رقم 81/2018 المتعلق بالمعاملات الإلكترونية والبيانات ذات الطابع الشخصي وعند توقيف الفاعل أو المشتبه به يتم الاستماع إلى إفادته وتتم مواجهته بالأدلة والقرائن الموجودة لدى المكتب ومن بعدها سوقه إلى المرجع القضائي المختص لإصدار الحكم المناسب بحقه"[1].

الابتزاز الإلكتروني يرتفع بنسبة 184%: كما في كل شيء، كان لانتشار وباء كورونا تداعيات على مختلف جوانب الحياة، انتشار هذا الفيروس فضح معه أوبئة أخرى تعاني منها المجتمعات منذ فترات طويلة، إلا أن الحجر الصحي وإغلاق مرافق الحياة في كل العالم ضاعف من آثار مخاطر عديدة من شأنها أن تؤدي إلى عواقب كارثية.

الابتزاز الإلكتروني، واحدة من الجرائم الدولية التي تضاعفت بسبب أزمة الكورونا والحجر الصحي، الخوف الذي ينتج عن ابتزاز وتهديد أحدهم لك بفضح المحادثات والصور الخاصة لا يختلف عن الخوف من الإصابة بالفيروس. وما قام به العالم من تباعد اجتماعي حرصاً على عدم نقل المرض، لم يبعد البعض عن استغلال التقارب الإلكتروني لممارسة وحشيتهم.

في لبنان، توفر الوقت في فترة التعبئة العامة وانعدام المال بسبب الأوضاع الاقتصادية ووباء كورونا، عوامل تضافرت وأدت إلى ارتفاع نسبة الابتزاز الإلكتروني. يوصّف القانون اللبناني الابتزاز بالجريمة، حيث يتم من خلالها التهديد بنشر صور أو فيديوهات خاصة بالضحية بهدف

[1] www.alaraby.co.uk

الحصول على مبالغ مالية، أو دفع الضحية للقيام بأعمال غير مشروعة. وبحسب قوى الأمن الداخلي ارتفعت نسبة شكاوى جرائم الابتزاز والتحرش الجنسي بنسبة 184% خلال فترة التعبئة العامة.

هذا العام، حتى شهر آذار 2020 وصلت عدد الشكاوى إلى 315 شكوى، مسؤول في شعبة العلاقات العامة لقوى الأمن الداخلي يقول لـ"مهارات نيوز" أن النساء أكثر عرضة لخطر الابتزاز الإلكتروني، الذي ينتج عن تقارب إلكتروني معين يصل إلى حد إرسال صور شخصية بوضعيات غير لائقة، أو من خلال القرصنة. فئة الفتيات اللواتي تتراوح أعمارهن بين الـ12 أو الـ14 سنة هنّ ضحايا جريمة الابتزاز أكثر من غيرهن".

ملاحقة القوى الأمنية للمبتزين عادة ما تبوء بالنجاح عبر إلقاء القبض على المبتز، وتكاد نسبة النجاح في ملاحقة المبتزين في لبنان تصل إلى 100% بحسب ما أكده المسؤول في شعبة العلاقات العامة لـ"مهارات نيوز". أما الغايات خلف القيام بهذه العمليات الابتزازية، فهي مادية أو جنسية من أجل السيطرة على الضحية واستغلالها إلى حد الاستعباد وصولاً إلى تهديدها بالقتل أو الخطف". وبحسب المادة 650 من قانون العقوبات اللبناني:

"يُعاقب كل شخص يهدد شخص آخر بفضح أمر ينال من شرفه أو كرامته أو اعتباره بالسجن من شهرين إلى سنتين وبالغرامة المالية".

ما تقوم به القوى الأمنية من جهود توعوية وقانونية لملاحقة المبتزين يعوّل عليه، لكن العمل الحقيقي يتبلور من خلال إقرار قانون خاص بالعنف الإلكتروني بما له من خصوصية وجوانب مختلفة، لأنها جريمة تستحق تشريع قانون خاص فيها، تطلب مرشاد.

حماية أنفسنا على وسائل التواصل الاجتماعي ضرورة قصوى اليوم، ويمكن تفادي أي خطأ يمكن وقوعه علينا من خلال "البلوك أو الحظر". إلا أن هناك ما هو أبعد من الحظر.

أغلب جرائم الابتزاز تحصل من قِبل أشخاص كنا نعرفهم مسبقاً، وأولينا بهم الثقة، كصديق أو زوج أو حبيب، هؤلاء هم من يمكن أن يحولونا إلى ضحاياهم بعد تهديدنا بنشر كل ما يملكونه عنا، الذنب لا يقع دوماً على الضحية ولا تُلام وحدها على فعل قامت به مرة، والحملات الإعلامية لا يجب أن تخاطبها وحدها. هي الضحية هنا، الحملة الإعلامية يجب أن تكون في وجه المجرم أيضاً، أي المبتز.

الفرع الثالث: الإتجار بالبشر

إن التاريخ المعروف للبشرية يشير إلى أن الرق أو الإستعباد أو العبودية قد برزت منذ آلاف السنين، وبعد أن استطاعت المجتمعات نزع فكرة السيّد والعبد وانقضى زمن العبودية. عاد هذا الأخير بشكل حديث وأصبح يعرف بالإتجار بالبشر أو الإتجار بالأشخاص، متخذاً من الإنسان سلعة للإتجار بها مستخدماً وسائل إجرامية حديثة لا تقتصر على حدود معينة أو وسيلة واحدة، كما لا تعرف هوية التاجر بسهولة إذ أصبحت الشبكات الإجرامية المنظمة في عصرنا هذا جرائم عابرة للحدود، يعمل أفرادها في صفحات سوداء من مواقع التواصل الإجتماعي والإنترنت أدائها التكنولوجيا وهدفها الثراء والكسب السريع للمال من دون أدنى اعتبار لحقوق الإنسان أو للإنسانية.

جريمة الإتجار بالبشر لا تقتصر على جنس معين أو فئة معينة أو مجتمع معيّن، ففاعلوها أناسٌ يستغلون الأزمات والصراعات والنكبات، كما وأن أعمالهم تمتد إلى الولوج في تجارة أعضاء البشر فيقتلون ويسرقون الجثث ويبيعون قطع غيار بشرية وكأنهم يتاجرون بأشياء مادية، ويتاجرون بالنساء والأطفال ويستغلون ضعفهم.

حظي موضوع مكافحة الإتجار بالبشر باهتمام كافة الدول، والعديد من المنظمات الدولية والإقليمية، باعتبار أن هذه الجريمة من أخطر الظواهر الإجرامية على المستوى الدولي، وتعبيراً قانونياً عن صورة العبودية المُستحدثة.

وقد عنيت المنظمات الدولية والإقليمية وخاصة منظمة الأمم المتحدة بدعوة المجتمع الدولي لمواجهة هذه الجريمة من خلال إبرام بروتوكول لمنع ومعاقبة الاتجار بالبشر (بروتوكول باليرمو) وهو بروتوكول مكمّل لاتفاقية الأمم المتحدة لمنع ومكافحة الجريمة المنظمة عبر الوطنية (لإتفاقية باليرمو)، بالإضافة إلى اتجاه غالبية الدول إلى تصديق الإتفاقية والبروتوكول المذكورين، والعمل على إصدار تشريعات وطنية.

حيث وبموجب القانون رقم 682 تاريخ 2005/8/24 أُجيز للحكومة اللبنانية الانضمام إلى بروتوكول منع وقمع ومعاقبة الإتجار بالأشخاص وبخاصة النساء والأطفال، الموقّع في نيويورك بتاريخ 2002/12/9، وقد أصدر أيضاً المشترع اللبناني القانون رقم 2011/64 تاريخ 2011/8/24 المضاف إلى قانون العقوبات اللبناني لمعاقبة الإتجار بالأشخاص. وذلك بغية مكافحة هذه الجريمة وصدّ مرتكبيها من الإستفادة من الأسباب الجذرية للإتجار التي هي ذات طبيعة إقتصادية، وثقافية، وإجتماعية، وقانونية، وسياسية.

إن مصطلح الإتجار بالبشر أو الإتجار بالأشخاص هو مصطلح حديث نسبياً، وهو ما يعرف بالعبودية الحديثة أو تجارة الرقيق المعاصر، وقد عرّفه بروتوكول الأمم المتحدة الخاص لمنع وقمع ومعاقبة الاتجار بالأشخاص، المكمّل لإتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام 2000، بأنه: "تجنيد أشخاص أو نقلهم أو تنقيلهم أو إيوائهم أو استقبالهم بواسطة التهديد بالقوة واستعمالها أو غير ذلك من أشكال القسر أو الاختطاف أو الاحتيال أو الخداع أو استغلال السلطة أو استغلال حالة استضعاف أو بإعطاء أو تلقي مبالغ مالية أو مزايا لنيل موافقة شخص ما له سيطرة على شخص آخر لغرض الاستغلال".

الاتجار بالبشر جريمة جنائية في القانون الدولي، وعلى الدول الأطراف التزام أساسي في التصدي للاتجار بطريقة تحترم وتحمي وتكفل حقوق الإنسان، ولا سيّما حقوق الفئات المهمّشة على النحو المنصوص عليه في ميثاق الأمم المتحدة الأساسي، والمستمدّة من الإعلان العالمي لحقوق الإنسان.

والاتجار بالبشر يشمل تجنيد الأشخاص أو نقلهم أو إيوائهم أو استقبالهم، عن طريق التهديد أو استخدام القوة أو غير ذلك من أشكال الإكراه، أو الاختطاف أو الاحتيال أو الخداع أو إساءة استخدام السلطة، أو منح أو تلقي مدفوعات أو مزايا للحصول على موافقة شخص له سيطرة على شخص آخر لغرض الاستغلال.

ويشمل الاستغلال أيضاً كحدّ أدنى استغلالاً من أجل بغاء الآخرين أو غير ذلك من أشكال الاستغلال الجنسي أو السخرة أو الإجبار على العمل أو الاستعباد أو الممارسات الشبيهة بالرق والعبودية، أو المتاجرة بالأعضاء.

وحث الخبراء في سيداو الحكومات على معالجة الأسباب الجذرية التي تدفع بالنساء والفتيات إلى أوضاع هشّة. وتتركز هذه المشاكل في التمييز على أساس النوع الاجتماعي، بما في ذلك الظلم الاقتصادي والاجتماعي في بلد المنشأ، وسياسة الهجرة المتحيّزة ضد النوع الاجتماعي وأنظمة اللجوء في البلدان الأجنبية فضلاً عن النزاعات وحالات الطوارئ الإنسانية.

"الاتجار بالبشر هو جريمة جنسانية ترتبط بالاستغلال الجنسي، يجب على الدول الأطراف تهيئة الظروف المناسبة لضمان أن تكون النساء في مأمن من مخاطر الاتجار"[1].

ودعت لجنة "سيداو" إلى وضع سياسات عامة لتوفير الاستقلال الذاتي للمرأة والمساواة في الوصول إلى التعليم وفرص العمل. كما حثّت على وضع إطار للهجرة الآمنة يراعي المنظور

[1] داليا لينارت من سيداو، **"الاتجار بالبشر هو جريمة جنسانية ترتبط بالاستغلال الجنسي"**.

الجنساني لحماية النساء والفتيات المهاجرات، وشددت على أهمية نظم الحماية والمساعدة الشاملة لمساعدة النساء والفتيات المشرّدات في النزاعات وحالات الطوارئ.

كما شدّدت اللجنة في التوصيات العامة على أن **"الاتجار بالنساء والفتيات واستغلالهن جنسياً هو انتهاك لحقوق الإنسان، ويمكن أن يشكل تهديداً للسلم والأمن الدوليين"**.

دعت لجنة أممية تُعنى بحقوق المرأة الحكومات لاتباع جميع الوسائل المناسبة للقضاء على الاتجار بالنساء والفتيات، وسلّطت الضوء على الاستخدام المتزايد لوسائل التواصل الاجتماعي في تجنيد ضحايا الاتجار بالبشر أثناء جائحة كوفيد-19.

وفي توصيات عامة، أشارت لجنة القضاء على التمييز ضد المرأة (سيداو) إلى أن النساء والفتيات لا يزلن ضحايا رئيسيات للاتجار بالبشر في جميع أنحاء العالم، على الرغم من الأطر القانونية والسياساتية الحالية لمكافحة الاتجار بالبشر على المستويين الوطني والدولي.

ولفتت اللجنة الانتباه إلى الاتجاهات الأخيرة للاتجار عبر الفضاء الإلكتروني، وخاصة عبر وسائل التواصل الاجتماعي وتطبيقات الدردشة والتي تسهّل الوصول إلى الضحايا المحتملات عندما لا يتمكن المتاجرون بالبشر من استخدام طرق أكثر تقليدية لتجنيد النساء والفتيات للاستغلال الجنسي، لا سيما خلال أوقات الإغلاق التي فرضتها جائحة كوفيد -19.

تجنيد الضحايا عبر الإنترنت: رغم أن التقنيات الرقمية أتاحت إمكانيات جديدة لإحداث تأثير إيجابي داخل المجتمعات، إلا أنها تشكل تحديات أمنية جديدة على المستويين الفردي والوطني. وبحسب سيداو، يوفر استخدام العملات الإلكترونية أدوات لإخفاء المعلومات الشخصية مثل تحديد هوية الأطراف المعنية ومواقع الأشخاص، كما يسمح الفضاء الإلكتروني بإجراء مدفوعات مجهولة المصدر ودون الكشف عن الغرض من المعاملة[1].

ودعت سيداو في توصياتها وسائل التواصل الاجتماعي وشركات المراسَلة إلى وضع ضوابط مناسبة لتقليص مخاطر تعريض النساء والفتيات للاتجار والاستغلال الجنسي. كما طلبت من هذه الشركات استخدام بياناتها لتحديد المتاجرين بالبشر والأطراف التي تقوم بالطلب.

وقالت داليا لينارت التي قادت صياغة التوصيات في سيداو: **"إن مكافحة الاتجار تستلزم أيضاً تثبيط الطلب"**.

[1] داليا لينارت من سيداو، **"كشفت الجائحة العالمية الحاجة الملحّة للتصدي لاستخدام التكنولوجيا الرقمية في الاتجار بالبشر ولمكافحته بها"**.

ويطرح استخدام التكنولوجيا الرقمية في الاتجار بالبشر مشاكل كبيرة، خاصة اثناء جائحة كوفيد-19، إذ تواجه الدول الأطراف نمواً في الاتجار بالفضاء الإلكتروني عبر زيادة التجنيد للاستغلال الجنسي عبر الإنترنت، كما تسهّل التكنولوجيا الاتجار بالأطفال لأغراض جنسية.

وقالت لينارت: **"كشفت الجائحة العالمية الحاجة الملحّة للتصدي لاستخدام التكنولوجيا الرقمية في الاتجار بالبشر ولمكافحته بها"**[1].

أقرّت الجمعية العامة للأمم المتحدة اعتبار يوم 30 تموز/يوليه اليوم العالمي لمكافحة الاتجار بالأشخاص في قرارها 192/68.

ويتأثر كل بلد في العالم بالاتجار بالبشر، سواء أكانت من بلدان المنشأ أو من بلدان العبور أو من بلدان المقصد، ويواصل المتاجرون بالبشر في جميع أنحاء العالم استهداف النساء والفتيات. وظهر أن الغالبية العظمى من ضحايا الاتجار بالبشر الذين كُشف عنهم في إطار مكافحة الاستغلال الجنسي هم من النساء، كما ظهر أن 35 % من ضحايا السُخرة (العمل الجبري/القسري) هنّ من الإناث. ويزيد النزاع من تفاقم أوجه الضعف، حيث تستغل الجماعات المسلحة المدنيين في حين يستهدف المتاجرون بالأشخاص النازحين قسراً.

تشير البيانات كذلك إلى أن الاتجار بالبشر يحدث في كل مكان حولنا حيث تضاعفت نسبة الأشخاص المُتّجر بهم داخل بلادهم في السنوات الأخيرة إلى 58% من جميع الضحايا الذين كُشف عنهم، بحسب ما ذكر تقرير مكتب الأمم المتحدة المعني بالمخدرات والجريمة العالمي بشأن الاتجار بالأشخاص لعام 2018.

تأتي ضحايا هذا الشكل الواسع الانتشار من الاتجار في المقام الأول من البلدان النامية، يتم استقدامهم والاتجار بهم باستخدام الخداع والإكراه ويجدون أنفسهم محتجزين في ظروف العبودية للقيام بمجموعة متنوعة من الأشغال.

ويمكن أن تشارك الضحايا في أعمال زراعية أوتعدين أو صيد الأسماك أو في أعمال البناء، إلى جانب عبودية منزلية وغيرها من الوظائف الكثيفة العمالة.

يؤثر هذا الشكل السائد للاتجار في كل منطقة في العالم، إما كبلد مصدر أو بلد عبور أو بلد مقصد. إن النساء والأطفال في البلدان النامية، ومن القطاعات الضعيفة من المجتمع في البلدان المتقدمة، تغريهم الوعود بالعمل اللائق ومغادرة منازلهم والسفر إلى ما يعتبروه حياة أفضل، وكثيراً

[1] www.news.un.org

ما يتم تزويد الضحايا بوثائق سفر مزورة وتستخدم شبكة منظمة لنقلهم إلى بلد المقصد، حيث يجدون أنفسهم مجبرين بالاستغلال الجنسي ومحتجزين في ظروف غير إنسانية ورعب مستمر.

في العديد من البلدان، تكون قوائم الانتظار لعمليات الزرع طويلة جداً، وقد انتهز المجرمون هذه الفرصة لاستغلال يأس المرضى والجهات المانحة المحتملة. إن صحة الضحايا، وحتى حياتهم، معرضة للخطر حيث يمكن إجراء العمليات في ظروف سرية دون متابعة طبية.

من المرجح أن شيخوخة السكان وزيادة حالات الإصابة بمرض السكري في العديد من البلدان المتقدمة قد تزيد متطلبات زرع الأعضاء وتجعل هذه الجريمة أكثر ربحية[1].

هناك العديد من أشكال الاتجار، لكن أحد الجوانب الثابتة هو استغلال ضعف الضحايا المتأصّل.

الفرع الرابع: الإحتيال الإلكتروني

يشير مصطلح احتيال الإنترنت إلى أي نوع من أنواع الخدع أو الحيل التي تستخدم خدمة أو أكثر من خدمات الشابكة (الإنترنت)، كغرف المحادثة أو البريد الإلكتروني أو منتديات الإنترنت أو مواقع الوب من أجل توجيه نداءات خادعة إلى ضحايا محتملين على الشابكة (الإنترنت) .

يهدف احتيال الإنترنت في العادة إلى الاحتيال على المستخدمين عن طريق سلب أموالهم (إما بسرقة أرقام بطاقات ائتمانهم أو بجعلهم يرسلون حوالات مالية أو شيكات) أو دفعهم إلى الكشف عن معلومات شخصية (بغرض التجسس أو انتحال الشخصية أو الحصول على معلومات حسابهم في مركز حساس)[2].

تستهدف عمليات الاحتيال الناس من كل الخلفيات والأعمار، كل شخص معرّض لعمليات الاحتيال، لذا يحتاج الجميع إلى معلومات عن كيفية التعرف عليها وتفاديها. المحتالون أذكياء، وإذا لم تعرفوا ما الذي يجب أن تنتبهوا له، يمكن لأي شخص أن يقع ضحية عملية احتيال.

تنجح عمليات الاحتيال لأنها تبدو مثل الشيء الحقيقي وتأتي على غفلة في وقت لا تتوقعونها. يمكنها أن تشمل عرضاً مغرياً جداً ليكون صحيحاً، أو اتصالاً هاتفياً للمساعدة في تصليح الكمبيوتر الخاص بك، أو تهديداً لدفع مال لست مديناً به، أو تحذيراً من مصرفك أو مزوّدك بخدمة الاتصالات حول مشكلة في حسابك، أو حتى دعوة لتكون "صديق" شخص ما على الإنترنت.

[1] www.interpol.int
[2] www.ar.m.wikipedia.org

يستغل المحتالون التكنولوجيا الحديثة، المنتجات أو الخدمات الجديدة والمناسبات الكبرى لخلق قصص يمكن تصديقها من شأنها إقناعك بتقديم مالك أو تفاصيلك الشخصية. حتى أن المحتالين ينتحلون صفة موظفين حكوميين ويطلقون ادعاءات كاذبة أو يستخدمون تهديدات بفرض غرامات مثلاً والاعتقال والترحيل عن البلاد لإخافتكم وحملكم على دفع المال. قد يحصل هؤلاء المحتالون على بعض معلوماتك الشخصية من مواقع التواصل الاجتماعي ليجعلوا مطالبهم تبدو مشروعة أكثر[1].

1- احتيال الاستيلاء على الحساب (ATO):

تحدث هجمات ATO عندما تستخدم الجهات المخادعة الهويات المسروقة وهجمات الروبوتات والتصيد الاحتيالي والبرامج الضارة وغيرها من الأدوات للحصول على بيانات اعتماد المستخدم والتحكم في حساب التجارة الإلكترونية. بعد اختراق الحساب، يمكن للمجرم تحويل الأموال أو إجراء عمليات شراء الحساب أو تعديله أو حتى استهداف حسابات أخرى للضحية. يمكن أن تشير الزيادة المفاجئة في عمليات تسجيل الدخول وعمليات الإغلاق والتغييرات في ملفات تعريف الحساب إلى هجمات ATO المحتملة.

2- سوء استخدام الطرف الأول

غالباً ما يشار إليه باسم "الاحتيال الودّي"، ويكون لهذا النوع من الاحتيال تأثير مالي على التجار على الرغم من أنه غالباً ليس ضاراً. يحدث ذلك عندما يتم الشراء عبر الإنترنت بواسطة حامل البطاقة أو أحد أفراد العائلة، مثل طفل. بعد ذلك، ينسى حامل البطاقة أنه قد أجرى عملية الشراء، أو لا يكون على علم بعملية الشراء التي قام بها أحد أفراد الأسرة، ويبلغ البنك الذي يتعامل معه بأنه احتيال يؤدي إلى ردّ المبالغ المدفوعة.

3- احتيال اختبار البطاقة

في هذا النوع الشائع من الاحتيال على بطاقة الائتمان، عندما يحصل الخبثاء على أرقام حسابات بطاقات الائتمان المسروقة، فغالباً ما يستخدمون البرامج النصية أو الروبوتات لإجراء عمليات شراء متعددة عبر الإنترنت بسرعة للتحقق أن الحسابات لا تزال صالحة والتأكد من حدود الائتمان المرتبطة. قبل أن يتم الكشف عن عمليات الشراء التجريبية الصغيرة، يقوم المجرمون بإجراء العديد من عمليات الشراء الكبيرة، وعادة ما تصل إلى الرصيد المتاح في الحسابات.

[1] www.scamwatch.gov.au

4- احتيال الطرف الثالث

يُشار إليه أيضاً بإساءة استخدام طرف ثالث، وهو أحد أكثر أنواع الاحتيال في التجارة الإلكترونية شيوعاً، يحدث ذلك عندما يتمكن فاعل سيء من الوصول إلى معلومات الدفع المسروقة، مثل رقم بطاقة الائتمان، ويستخدمها لإجراء عملية شراء عبر الإنترنت. عندما يعلم حامل البطاقة الفعلي بعملية الشراء غير المصرح بها، فإنه يقوم بإبلاغ البنك بذلك مما يؤدي إلى رد المبالغ المدفوعة إلى التاجر.

يمكن تقليل الأنشطة الاحتيالية مثل هذه بشكل كبير باستخدام حل منع الاحتيال المناسب. على سبيل المثال، أولئك الذين يستخدمون تقنيات الذكاء الاصطناعي المتقدمة ويتعلمون من شبكة واسعة من البيانات قادرون على مراجعة عمليات الشراء عبر الإنترنت واكتشاف الأنماط التي تشير إلى ما إذا كان النشاط حقيقياً أم احتيالياً.

تعمل هذه الحلول على النحو التالي:

5- عند بدء عملية شراء عبر الإنترنت، فإنها تحلّل العديد من جوانب المعاملة مثل من بدأ الشراء، والجهاز الذي يتم استخدامه، والمنتج الذي يتم شراؤه، والبطاقة المستخدمة. بعد ذلك، عندما يكتشف النظام أنماطاً مشبوهة، فإنه ينبهك إلى أنه تم وضع علامة على عملية الشراء على أنها احتيال محتمل في بطاقة الائتمان حتى تتمكن من منع استمرار المعاملة.

عندما يحدث الاحتيال في التجارة الإلكترونية، يعاني عملك أكثر من خسائر الإيرادات. ويكون عليك أيضاً أن تتعامل مع الضرر الذي يلحق بسمعة شركتك وكذلك فقدان ثقة العملاء.

كل من هذه الآثار السلبية – الخسائر المالية، وتضرر السمعة، وتراجع الثقة – تهدد صحة عملك على المدى الطويل. وبغض النظر عن حجم شركتك، فإن مخاطر هذه الأنواع من الاحتيال في التجارة الإلكترونية حقيقية[1].

6- الاحتيال الإلكتروني أوهام بالثراء السريع.. والوعي سلاح الحماية:

في ظل التطور التكنولوجي الذي نعيشه وتطور المعاملات المالية، انتشر في الآونة الأخيرة وقوع الكثير من الأفراد ضحايا عمليات نصب واحتيال إلكتروني، تتاجر بآمال وأحلام الناس عن طريق منحهم وعوداً بالثراء السريع، إلا أنه للأسف يكتشف مثل هؤلاء متأخرين أنهم وقعوا ضحية

[1] www.mics.microsoft.com

لاحتيال، من قبل أناس لا يعرف عنهم أكثر من كبسة زر، من خلال لوحة المفاتيح لمواقع التواصل الاجتماعي.

شدّد مسؤولون وقانونيون على خطورة الانجرار خلف المجرمين الذين يترصدون ضحاياهم عبر وسائل الاتصال والتواصل الحديثة، لتحقيق مآربهم بوسائل منمّقة تخبرهم بالفوز بجائزة مالية، أو التبرع لمشروع خيري، مؤكدين أن الجهات الحكومية تبذل جهوداً متواصلة للحدّ من عمليات النصب والاحتيال على مواقع التواصل الاجتماعي والإنترنت أو من خلال رسائل مضلّلة عبر الهواتف، مشيرين إلى أن الجهات الأمنية المختصة تقوم بتتبع مصدر الرسائل والإيقاع بمرتكبيها وتقديمهم للعدالة، وفقاً للقانون الاتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات ومواده القانونية التي تتضمن الغرامات المالية والحبس.

وأشاروا إلى أن الطمع، وقلة الوعي، من أهم أسباب وقوع الضحايا في براثن المحتالين، داعين الجمهور إلى الحذر وعدم تقديم أية معلومات مالية أو شخصية إلا من خلال الطرق الصحيحة والمعروفة، مؤكدين أهمية التركيز على الوعي الاجتماعي لدى الأفراد ونقاط التنوير لديهم عبر توعيتهم بالعقوبات التي تقع على مثل هؤلاء المحتالين، بالإضافة إلى ضرورة استحداث أساليب وقائية مبتكرة لحماية الضحايا قبل وقوعهم في شرك الاحتيال[1].

الفرع الخامس: جرائم الفكر والصحافة

في أعقاب الربيع العربي، ارتفع عدد الانتهاكات لحريّة التعبير في البلدان العربيّة، ويذهب لبنان حالياً في الاتجاه نفسه، على الرغم من أن الحكومة اللبنانية لطالما أعربت عن التزامها باحترام هذا الحق الأساسي على الصعيدين الدولي والمحلّي. لا سيما أن المادة 13 من الدستور[2] تكفل ممارسة هذا الحق، وكذلك الإعلان العالمي لحقوق الإنسان المندرج ضمن الدستور[3]، والذي يحمي حرية التعبير ويضمنها طالما هي "ضمن الحدود التي يحددها القانون"، وأيضاً الاتفاقية الدولية للحقوق المدنية والسياسية[4]، التي وقّع عليها لبنان عام 1972، وتؤكد على أهمية حرية التعبير.

---

[1] www.albayan.ae

[2] تنص المادة 13 من الدستور اللبناني على أن: "حرية الفرد بالتعبير عن آرائه شفوياً أو كتابياً، وحرية الصحافة، وحرية التجمع، وحرية تكوين الجمعيات مكفولة في الحدود التي يحددها القانون".

[3] ينص الدستور اللبناني في الجزء الأول، الأحكام الأساسية، الديباجة، ب) على أن: "لبنان عضو مؤسّس ونشط في الأمم المتحدة، وهو يلتزم بعهوده وبالإعلان العالمي لحقوق الإنسان. وعلى الحكومة أن تؤسس هذه المبادئ في جميع المجالات والمناطق من دون استثناء". إلى ذلك، تم تحديد حرية التعبير في المادة 19 من الإعلان، على أنه "لكل شخص الحق في حرية الرأي والتعبير، ويشمل هذا الحق حرية الآراء من دون تدخل والسعي إلى المعلومات والأفكار وتلقيها ونقلها عبر أي وسائط وبغض النظر عن الحدود".

[4] تنص المادة 19,2 من الاتفاقية على أن: "لكل شخص الحق في حرية التعبير ويشمل هذا الحق حرية البحث عن المعلومات والأفكار بجميع أنواعها وتلقيها ونقلها، بغض النظر عن الحدود، شفهياً أو كتابياً أو مطبوعاً أو في شكل فني أو من خلال أي وسائط أخرى يختارها".

تزايدت حالات استدعاء الأفراد لاستجوابهم حول قضايا متعلقة بحرية التعبير منذ عام 2017، وكان أغلبها من قبل النيابات العامة ومكتب الجرائم المعلوماتية والقوى الأمنية، وقد تقدمت بها شخصيات سياسية ودينية مما يظهر أن السلطة لا ترحب بالانتقاد. وتشكل هذه الظاهرة انتهاكاً صارخاً لحقوق الإنسان وتهديداً كبيراً لمساحة الحوار الديموقراطي.

تقوم منظمات المجتمع المدني بتوثيق الحالات التي تمّ خلالها استخدام التشريعات لمعاقبة الصحافيين والناشطين والمواطنين من قبل السلطة، وذلك للمطالبة بتعديل القوانين وتحسين مستوى حرية التعبير في لبنان.

اللافت أن هذه الأحكام تتعارض مع المادة 13 من الدستور التي تحفظ حرية التعبير، إلا أنه يتم استخدامها في كثير من الأحيان لقمع أي نقد عبر تشجيع الاحتجاز والاعتقال. وعلى الرغم من أن المادة 47 من قانون أصول المحاكمات الجزائية[1] تنصّ على حقوق المعتقلين ومسؤوليات الشرطة القضائية خلال فترة الاحتجاز، لكنها غالباً لا تطبق أو لا يؤخذ بها.

تبرز هيئة أخرى معنية بحرية التعبير، وهي محكمة المطبوعات التي تأسست في العام 1962 من خلال قانون المطبوعات الذي يتناول جرائم متعلقة بما يتم نشره عبر وسائل الإعلام المكتوبة والمسموعة والمرئية. ولا يشمل هذا القانون المنصّات الرقمية، بالرغم من وجود محاولات حثيثة لتعديل وإعادة هيكلة القانون لتشمل صلاحياته هذه المنصّات باعتبارها وسيلة رسمية للنشر، إلا أن هذه التعديلات لا تزال عالقة في مجلس النواب (حلاوي، 2018). إضافةً إلى هذا النقص الفادح في الوضوح حيال هذه القوانين، تبرز المادة 209 من قانون العقوبات التي تحدد وسائل نشر المعلومات ولا تذكر المنصات الرقمية أيضاً. بالإضافة إلى ذلك عدم تدريب القضاة على التعامل مع القضايا التي تتناول المساحات الرقمية ووسائل التواصل الاجتماعي، يزيد من قلّة كفاءة النظام القضائي في التعاطي مع حرية التعبير.

وبالنسبة إلى هيئات المراقبة والمساءلة، تبرز اللجنة الوطنية لمكافحة الفساد التي لم يتم تشكيلها بعد، ولكن يُفترض أن تكون كياناً حكومياً، مهمته مساءلة المسؤولين الفاسدين وتنفيذ قوانين مكافحة الفساد التي أقرها البرلمان ومن ضمنها قانون حق الوصول إلى المعلومات، الذي يُلزم الحكومة بتزويد المواطنين والمواطنات بالمعلومات المتعلقة بكل القرارات التي تتخذها .

"جريمة الشير" لم تكن هذه الجريمة الأولى من نوعها، إذ لطالما نصّب المكتب التابع للشرطة القضائية نفسه رقيباً على نشاط الصحافيين والناشطين الإلكترونيين، بدءاً بالمقالات، وصولاً

[1] تنص المادة 47 من قانون أصول المحاكمات الجزائية: يتولى الضباط العدليون، بوصفهم مساعدي النيابة العامة، المهام التي تكلفهم النيابة العامة فيها استقصاء الجرائم غير المشهودة وجمع المعلومات عنها والقيام بالتحريات الرامية إلى كشف فاعليها...

إلى البوستات والتغريدات وحتى الـshares هكذا، راح يستدعيهم الواحد تلو الآخر للتحقيق معهم في شكاوى قدّمها أطراف عدّة، بينهم سياسيون و"عرّافون"، كما حدث مع الصحافي ربيع فرّان.

على سبيل المثال، قال ميشال قنبور، وهو صحفي لبناني ومؤسس صحيفة "ليبانون ديبايت" الإلكترونية، لـ"هيومن رايتس ووتش" إن المسؤولين الحكوميين رفعوا عليه دعاوى قدح وذم حوالي 20 مرة منذ 2015، وأغلبها نتيجة لنشره تقارير عن الفساد وسوء السلوك من قبل المسؤولين. في مارس/آذار 2018، حكمت محكمة المطبوعات غيابياً بحبس قنبور ستة أشهر وتغريمه عشرة ملايين ليرة لبنانية (6,667 دولار أمريكي) لاتهامه مدير عام مؤسسة حكومية بالفساد. قال قنبور: "في 2019، من العار أن يصدر قضاتنا أحكاماً بحبس الصحفيين. السبب الوحيد الذي يبرر حبس الصحفي هو التحريض على العنف. الإهانة المفترضة لشخص ما ليست مبرراً".

في قضية أخرى شهيرة، في 10 يناير/كانون الثاني 2018، حكمت المحكمة العسكرية على الصحفية والباحثة اللبنانية غدار غيابياً بالحبس ستة أشهر لانتقادها الجيش اللبناني في تعليقات أدلت بها خلال مؤتمر في واشنطن. على الرغم من أن المحكمة العسكرية أسقطت حكمها ضد غدار وأحالت قضيتها إلى محكمة المطبوعات في 10 أبريل/نيسان 2018، معللة ذلك بعدم اختصاصها، قالت غدار إن الرسالة كانت واضحة: "انتهى زمن حرية التعبير التي تمتّعنا بها لفترة، والآن عدنا إلى ما قبل 2005، لكن، بدلاً من الجيش السوري، لدينا الدولة اللبنانية"[1].

ففي أيلول (سبتمبر) عام 2013، استدعي الأخير بناءً على شكوى رفعتها ليلى عبد اللطيف على خلفية مقال نشره على موقع "مختار" الإلكتروني، قبل أن يوقّع تعهداً بعدم التعرض لها. وهناك أيضاً حادثة التحقيق مع الصحافي مهند الحاج على أثر شكوى "قدح وذم وإثارة نعرات" ضد مجهول رفعها رئيس حزب "القوات اللبنانية" سمير جعجع على خلفية مقال نشرته مدونة "المحاسبة" بعنوان "رسالة من قدامى القوات إلى سمير جعجع". يومها، ظن الجميع أن "مكتب الجرائم الإلكترونية" لن يتعرض للصحافيين والناشطين اللبنانيين بعد الضربة التي تعرض لها (الأخبار 2013/9/18).

المطلوب اليوم هو "قوننة هذا المكتب"، لكن إلى حين أن يصبح هذا ممكناً يجب أن تبتعد حالات الاستنكار عن "الفردية، ونشكّل تحركاً ممنهجاً، كمكتب متابعة مؤلف من محامين وصحافيين ومؤسسات صحافية وغيرهم. وقل كل ذلك، علينا إرشاد الناس إلى حقوقهم وواجباتهم أثناء التحقيق معهم". لكن ألا يُعتبر الأمل في تحقيق هذا الأمر والوصول إلى "قوننة المكتب" ضرباً من الخيال

[1] www.hrw.org

في ظل الواقع اللبناني، وخصوصاً اليوم؟ الجواب بالنسبة إلى نادين فرغل بسيط: "علينا أن نطلب الحد الأقصى لنتمكن من إحداث تغيير ما. فلو كانت كل مطالب الناس معقولة، لما تحقق أي شيء!".

المبحث الثاني

النظام القانوني للجرائم المرتكبة عبر وسائل التواصل الإجتماعي

تميّز القرن الواحد والعشرين بانتشار المعلوماتية والتي ازدهرت بشكل سريع مما أصبح معه سمت هذا القرن، وتعددت نواحي استعمال المعلوماتية حيث أضحت تمسّ مختلف الميادين التجارية والإدارية والثقافية لما لها من إيجابيات في التنظيم واقتصاد الوقت والتكلفة، إلا أن لها مساوئ بدأت تتجلى مع تفشّي الجريمة الإلكترونية.

لقد تأخر المشرّعون في إصدار قوانين منظمة للمجال المعلوماتي، خاصة منها المتعلقة بمكافحة الجريمة الإلكترونية، ورغم أن بعض الدول كانت سبّاقة لسنّ قوانين للوقاية من مخاطر الجريمة الإلكترونية، إلا أن معظم الدول لم تستشعر خطورة هذه الجريمة لتعمل على تحصين قوانينها، ولذلك تعتبر أغلب التشريعات المقارنة المتعلقة بمكافحة الإجرام الإلكتروني حديثة نسبياً، حيث تعمل جلّ الدول على ملائمة قوانينها بما يتناسب مع هذا النوع من الإجرام وسداً للقصور الذي كان يعانيه القضاء في مكافحة الجريمة الإلكترونية بالنصوص القانونية التقليدية والذي كان يخالف مبدأ الشرعية، باعتباره مبدأ يحقّق الحماية لحقوق المتهم من تجريمه على أفعال وعقابه بعقوبات لم ينصّ عليها القانون، كما يطرح جدوى هذا الموضوع في الاقتداء بتطور القوانين لدى التشريعات المقارنة في ملاحقتها للأنماط المستحدثة من الجريمة الإلكترونية والذي قد يتأخر المشرّع الجنائي الوطني في مواكبته لأسباب تقنية.

إن تاريخ التشريعات المتعلقة بمكافحة الجريمة الإلكترونية حديثة نسبياً، فهي لم تتعدى السبعينات من القرن الماضي لدى الدول السباقة لسنّ تشريعات خاصة بهذا المجال مثل القانون الفرنسي رقم 78-17 بشأن الحريات والمعلوماتية الصادر في 6 يناير عام 1978. وقانون جرائم الحاسوب الصادر عام 1978 بولاية فلوريدا أول قانون في الولايات المتحدة الأمريكية. كما أصدر المشرع الإنجليزي قانون حماية البيانات الصادر في 12 يوليوز 1984. كانت هذه الدول سباقة لإقرار تشريعات تأطر الحماية من إساءة استخدام الحاسوب. كما أن التأطير القانوني للجريمة الإلكترونية يجد أهميته في الدور الذي أصبحت المعلوماتية تلعبه في الحياة اليومية ومدى الخطورة

التي يمكن أن تنتج عن إساءة استخدامها وأبرز الجهود التي تلعبها كل الدول لتجويد وتوحيد تشريعات مكافحة الجريمة الإلكترونية نظراً لطابعها العابر للحدود الوطنية.

المطلب الأول: التشريعات والقوانين المتعلقة بهذه الجرائم

(عرض مفصّل لعدد من القوانين والتشريعات العربية والأوروبية بخصوص الجرائم الإلكترونية) ومنها:

الفرع الأول: في القانون اللبناني

لقد شهدت السنوات الأخيرة إقرار عدد لا بأس به من التشريعات السيبرانيّة وآخرها في لبنان، قانون رقم 81 الصادر في 2018/10/10 المعاملات الإلكترونية والبيانات ذات الطابع الشخصي.

حيث كانت المعاملات الإلكترونية في لبنان تتم في ظل فراغ تشريعي إذ إن القوانين اللبنانية كانت عاجزة عن مجاراة التطور الحاصل وإيجاد الحلول القانونية الملائمة.

وكانت تُطبّق مواد قانون العقوبات اللبناني الذي جرى وضعه في الأربعينيات من القرن الماضي.

إنّ نصّ المادة 281 عقوبات يعاقب بالحبس من دخل أو حاول الدخول إلى مكان محظور بقصد الحصول على أشياء أو وثائق أو معلومات يجب أن تبقى مكتومةً حرصاً على سلامة الدولة.

كذلك فإن نصّ المادتين 282 و283 عقوبات يعاقب بالحبس من يُقدِم على سرقة أو حيازة وثائق أو معلومات كالتي ذُكرت في المادة 281 بقصد إفشائها.

وهنا يمكن أن تكون هذه المعلومات أو الوثائق المذكورة أعلاه مسجّلة على أشرطة إلكترونية أو أسطوانات مدمجة تستعمل في الحاسب الآلي، ويمكن بالتالي أن تكون مواد جرمية.

يمكن أيضاً ومن خلال نصوص قانون العقوبات معاقبة العديد من الجرائم المعلوماتية التي تحصل بواسطة نشر مواد أو صور أو توجيه رسائل إلكترونية على شبكة الإنترنت من شأنها مثلاً إضعاف الشعور القومي أو إثارة النعرات العنصرية أو المذهبية في زمن الحرب أو عند توقّع نشوبها (مادة 295 عقوبات وما يليها) أو تحتوي على قدح وذمّ أو تحقير لأحد رجال السلطة العامة (المواد 383 لغاية 389) أو لأحد الأفراد (المواد 582 لغاية 589 عقوبات)، أو تهديد بجناية أو بجنحة

(المواد 574 لغاية 578 عقوبات) أو تعتبر إفشاء لأسرار (المواد 579 عقوبات[1] وما يليها) أو تشكل مساساً بالشعور الديني (المادتين 473 و474 عقوبات) أو تشكل تعرضاً للآداب أو الأخلاق العامة (المواد 531 و532 و533 عقوبات)، مع العلم أن شبكة الإنترنت أضحت شبكة عامة ومباحة للجمهور وعلنية، ويمكن اعتبارها من الوسائل الآلية المحدّدة في المادة 209 عقوبات.

إضافة إلى ذلك يمكن تطبيق نصّ المادة 635 عقوبات وما يليها التي تجرّم أعمال السرقة على أنواعها على سرقة أجهزة الحاسب الآلي المادية وتوابعها ولا تطال البرامج أو المعلومات التي هي أشياء غير ملموسة "Hardware".

يمكن أيضاً تطبيق نصّ المادة 650 عقوبات الذي يعاقب كلّ من هدّد شخصاً بفضح أمر أو إفشائه أو الإخبار عنه، وكان من شأنه أن ينال من قدْرِ هذا الشخص أو شرفه لكي يحمله على جلب منفعة له أو لغيره غير مشروعة، في حال استعمال معلومات أمكن الحصول عليها عبر الأنظمة المعلوماتية لأن النص لا يشير إلى مصدر المعلومات التي تستعمل في التهديد أو الابتزاز.

ويمكن أيضاً معاقبة تزوير بطاقات الاعتماد المصرفية الإلكترونية واستعمالها سنداً للمادتين 471 و454 عقوبات.

إضافة إلى ذلك يمكن سنداً للمادة 655 عقوبات معاقبة جرائم الاحتيال إذا حصلت المناورات الاحتيالية بواسطة وسائل إلكترونية[2].

كذلك فإن نصّ المادة 733 عقوبات الذي يعاقب من أقدم على تخريب الأشياء في حال إقدام أحدهم على تخريب أجهزة الكمبيوتر وتوابعها.

فأتى القانون الراهن في ثمانية أبواب غطّت مجمل المواضيع المنوّه عنها سابقاً.

يتضمن الباب الأول من القانون الأحكام القانونية المتعلقة بالكتابة والإثبات بالوسائل الإلكترونية. تعترف القواعد القانونية الواردة في هذا الباب بالإسناد الإلكتروني والتواقيع الإلكترونية، وتعطي للسند الخطي على دعامة إلكترونية ذات القوة الثبوتية للسند على دعامة ورقية، ضمن شروط معينة. كما تتيح إمكانية إقرار الأسناد الرسمية الإلكترونية بموجب مرسوم يتخذ في مجلس الوزراء، ما يتيح تحضير الإدارة لهذا الأمر ووضع الضوابط والضمانات اللازمة.

كما يتطرق هذا الباب لمسائل متنوعة وهي:

[1] القاضي خميس فوزي، **"جرائم المعلوماتية وبنوك وقواعد المعلومات"**، العدل 1999، ص. 2.
[2] خميس، فوزي: مرجع سابق، ص. 3.

1- حفظ البيانات الإلكترونية.

2- النزاعات حول الإثبات الخطي.

3- قاعدة تعدد النسخ بالنسبة للسند العادي.

4- إنكار أو ادعاء تزوير الأسناد والتواقيع الإلكترونية.

5- وسائل حماية الكتابة الإلكترونية .

6- دور مقدمي خدمات المصادقة الإلكترونية واعتمادهم من قبل المجلس اللبناني للاعتماد وشروط ذلك...

يتعرض الباب الثاني للتجارة الإلكترونية، حيث ينص على موجبات كل من يمارس التجارة الإلكترونية، كما يضع تنظيماً لآلية العرض بوسيلة إلكترونية وأحكاماً خاصة بخصوص القبول الصادر بوسيلة الكترونية والتدوين بالصيغة الإلكترونية عوضاً عن خط يد الملتزم ورسائل التسويق والترويج غير المستدرجة.

أما فيما يتعلق بالخدمات المصرفية الإلكترونية، فيضع هذا الباب تنظيماً لأوامر الدفع الإلكترونية وللتحاويل الإلكترونية وللبطاقات المصرفية وللنقود الإلكترونية وللشيك الإلكترونية ولموجبات المصارف والمؤسسات المالية في هذا الموضوع ولموجبات العميل ومسؤولياته ولمضمون الاتفاقات المبرمة في هذا الموضوع مع العملاء، وأخيراً لصلاحيات مصرف لبنان في هذا المجال.

أما الباب الثالث من القانون يتضمن الأحكام القانونية المتعلقة بالنقل إلى الجمهور بوسيلة إلكترونية. فهذا الباب ينصّ على موجبات مقدمي الخدمات التقنية (مقدّم خدمة الاتصال أو مستضيف البيانات) ومسؤولياتهم وينظم عمليات نشر المعلومات للجمهور من خلال خدمة اتصال مباشر دون إفضاء الهوية.

يتناول الباب الرابع أسماء المواقع على شبكة الإنترنت، وهو ينظم كيفية منح وإدارة أسماء المواقع المتعلقة بالنطاق lb، ولبنان والشروط القانونية الوطنية الإدارية والتقنية المفروضة، بالإضافة إلى الشروط والموافقات المفروضة من الجهات الدولية المعنية بتسجيل مواقع الإنترنت، كما يتطرق إلى دور المؤسسة المرخّص لها بمنح وإدارة أسماء المواقع وحقوقها ومسؤولياتها عن العبارات المستخدمة كأسماء مواقع، وإلى حالات إلغاء اسم الموقع الممنوح، وإلى تسوية النزاعات المتعلقة بأسماء المواقع بطرق غير قضائية وعبر المحاكم المختصة في هذا المجال.

أما الباب الخامس يضع تنظيماً قانونياً متكاملاً لموضوع حماية البيانات ذات الطابع الشخصي، فهو يحدد أهداف معالجة المعلومات ذات الطابع الشخصي وضوابطها والمعالجات الممنوعة قانوناً وكيفية جمع المعلومات ذات الطابع الشخصي وموجبات المسؤول عن المعالجة ومسؤولياته. كما يورد هذا الباب لائحة طويلة من المعالجات المعفية من التصريح أو طلب الترخيص لوضعها قيد التنفيذ.

وينظم بالمقابل أصول التصريح عن المعالجات غير المعفية أو طلب الترخيص بخصوص بعضها من المرجع الرسمي المختص. كما ينص هذا الباب على حقوق قانونية للشخص الذي يتعلق به البيانات موضوع المعالجات:

1- حقه في الاعتراض على هذه المعالجات.

2- حقه في الاستعمال عن هذه المعالجات، وطلب معلومات بشأنها.

3- حقه في طلب تصحيح المعلومات المتعلقة به أو تحديثها أو إكمالها أو محوها...

يتناول الباب السادس الجرائم المتعلقة بالأنظمة والبيانات المعلوماتية وبطاقات الإيفاء بالإضافة إلى بعض التعديلات على قانون العقوبات (مرسوم اشتراعي رقم 340 تاريخ 1943/3/1). ويتضمن الباب نصوص جزائية حول الجرائم المتعلقة بالأنظمة والبيانات المعلوماتية، وحول تقليد بطاقات الإيفاء أو السحب أو تزويرها، وحول عدم مراعاة القواعد المطبقة على التجارة الإلكترونية. كما تتضمن التعديلات على قانون العقوبات تعديلاً للمادة 209 التي تعرف وسائل النشر وللمادة 453 التي تعرف التزوير.

أما بالنسبة للباب السابع فهو يتضمن تعديلات على بعض مواد قانون حماية المستهلك رقم 659 تاريخ 2005/2/4 لضمان تناسق هذا القانون مع أحكام التجارة الإلكترونية.

أخيراً ينصّ الباب الثامن على بعض الأحكام الختامية والانتقالية المتعلقة بهذا القانون، لا سيما لجهة مراعاة قانون السرية المصرفية وبعض القوانين الأخرى، ولجهة تحديد صلاحيات مصرف لبنان في مجال التراخيص والمصادقات العائدة للتواقيع الإلكترونية المستخدمة في القطاع المالي والمصرفي.

الفرع الثاني: في القانون المصري

في ظل الانتشار السريع للتكنولوجيا خاصة في زمن الكورونا أصبحت معظم التعاملات الاجتماعية والتجارية والسياسية، تتم عن طريق الشبكة المعلوماتية (الإنترنت)، وأصبح الإنسان أكثر عرضة للوقوع كضحية لتلك الجرائم الإلكترونية أو المعلوماتية.

تتمثل الجريمة الإلكترونية في اعتداء معلوماتي يقوم فيه الجاني باستخدام وسائل اتصال حديثة بهدف ابتزاز الضحية أو تشويه سمعتها وما إلى ذلك، سواء بغرض تحقيق مكاسب مادية أو أهداف سياسية.

على الصعيد الآخر، يتحمل المستخدمون من المواطنون، بل الشركات والحكومات أنفسهم كل تلك المخاطر، وذلك نظراً إلى أن الإنترنت أصبح بلا منافس في شتى التعاملات، وبات من الصعب على مستخدميه تجنّبه، وذلك لأنه أكثر الوسائل سرعة وتوفيراً للوقت والجهد، خاصة في ظل تحديد الحركة وفي ظل "المنافسة" التي تجيد استخدامه في شتى بقاع الأرض.

ولما اختلفت التعاملات من تعاملات "عادية" إلى تعاملات "إلكترونية"، احتاج الإنسان إلى قانون أكثر تحديداً لينظم تلك التعاملات، قانون يتعامل معها ومع ما تفرضه من تحديدات ومستجدات. لذلك كان لظهور قانون مصري يحمي تلك المعاملات أهمية قصوى، قانون يضع حد للجرائم والانتهاكات التي تتم بشكل متكرر، ويفعل المادة 95 من الدستور المصري الحالي الصادر في عام 2014، والتي جرى نصها على أن "الجرائم الإلكترونية بالنسبة للقضاء والمحامين والمشرّع المصري تعتبر من أكثر الجرائم التي تمثل صعوبة في تطبيقها، وذلك لأنه من الصعب مثلاً:

1- تحديد هوية الجاني
2- تحديد ميكانيكية الآلة الإلكترونية المستخدمة.
3- الوقف على معايير إثبات عادلة.
4- التساؤل عن أخلاقية الفعل المرتكب.

في إطار السياق الجديد، وأهدافه، ومن أجل تحديد عقوبة تتناسب مع هذه الجريمة المستحدثة.

تصدّى القانون رقم 175 لسنة 2018 بإصدار قانون مكافحة جرائم تقنية المعلومات، المعروف إعلامياً بـ"مكافحة الجرائم الإلكترونية"، للمخالفات التي قد يرتكبها مقدمو الخدمة في ضوء التزاماته الواردة بالقانون تفصيلاً، وفي مقدمتها الإخلال بالحفاظ على سرية البيانات التي تم حفظها وعدم إفشائها.

وفي هذا الصدد، جاء القانون في مادته (31) ليقضي بعقوبة الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن 5 آلاف جنيه، ولا يتجاوز 20 ألف جنيه، أو بإحدى هاتين العقوبتين، كل مقدم خدمة خالف الأحكام الواردة بالبند 2 من الفقرة أولاً من المادة 2 من هذا القانون، وتتعدد عقوبة الغرامة بتعدد المجني عليهم من مستخدمي الخدمة.

ويقضي البند 2 من الفقرة أولاً من المادة الثانية، بالتزام مقدّم الخدمة بالمحافظة على سرية البيانات التي تم حفظها وتخزينها وعدم إفشائها أو الإفصاح عنها بغير أمر مسبّب من إحدى الجهات القضائية المختصة. ويشمل ذلك البيانات الشخصية لأيٍّ من مستخدمي خدمته، أو أي بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التي يدخل عليها هؤلاء المستخدمين أو الأشخاص والجهات التي يتواصلون معها. ويعمل القانون على تحقيق التوازن بين مكافحة الاستخدام غير المشروع للحاسبات وشبكات المعلومات، وحماية البيانات والمعلومات الحكومية والأنظمة والشبكات المعلوماتية الخاصة بالدولة أو أحد الأشخاص الاعتبارية العامة، من الاعتراض أو الاختراق أو العبث بها أو إتلافها أو تعطيلها بأي صورة، والحماية الجنائية لحرمة الحياة الخاصة التي كفلها الدستور للمراسلات الإلكترونية، وعدم إفشائها أو التنصت عليها إلا بأمر قضائي مسبّب، بالإضافة لضبط الأحكام الخاصة بجمع الأدلة الإلكترونية.

لا يسعنا إلا حمد الجهد المبذول من قِبل المشرّع المصري، وإن كان بطيئاً بعض الشيء في مواجهة تطورات المجتمع، ولكن على كل حال، قد أنتج قانوناً لمكافحة جرائم تقنية المعلومات وبذلك خرجت رسالته إلى النور والتطبيق والنفاذ، وأُرسيت نصوصه تجريمات وعقوبات تبدو متوازنة، تجمع بين الخطوط العامة للمسؤولية عن الجرائم بصفة عامة والسياق الذي تفرضه تلك الجرائم.

وأخيراً، يُشكر المشرّع المصري على جمعه وتفنيده وتضمينه للنصوص والأحكام القضائية المتناثرة في القانون المصري، خاصةً تركيزه على الأحكام الموضوعية والإجرائية التي تتناول المسؤولية الجنائية للجرائم الإلكترونية، يبقى الدور على القضاة والمحامين والباحثين في تطبيق وتمحيص وتطوير هذا القانون، ودمجه في القانون المصري بشكل ممنهج سليم[1].

الفرع الثالث: في القانون الأردني

يعتبر قانون الجرائم الإلكترونية الذي صدر سنة 2015، نسخة محدّثة من قانون "جرائم أنظمة المعلومات" الذي مرّرته الحكومة الأردنية، سنة 2010، والذي شهد استهجاناً كبيراً من مختلف الفئات المجتمعية عامةً والقانونيين خاصة، إذ تم تمرير هذا القانون في ذلك الوقت في ظل غياب

[1] www.thelegalist.net

مجلس النواب. وبذلك فإن التعديل الذي تم إدخاله على المشروع في عام 2018 والذي من المتوقع أن يتم التصويت عليه في البرلمان الأردني خلال فترة قريبة، سيمثل التعديل للمرة الثانية على التوالي.

وفي ذات السياق، أثارت التعديلات التي قُدمت إلى البرلمان للنظر فيها في وقت مبكر من عام 2018، الكثير من المخاوف بالنسبة لمنظمات المجتمع المدني والناشطين حول القيود المحتملة على حرية التعبير على الإنترنت. فقد أدخلت التعديلات على سبيل المثال، تعريفاً غامضاً وفضفاضاً لخطاب الكراهية، حيث عرّف على أنه "كل قول أو فعل من شأنه إثارة الفتنة أو النعرات الدينية أو الطائفية أو العرقية أو الإقليمية أو التمييز بين الأفراد أو الجماعات"، والذي يمكن تفسيره على أنه ينطبق على محتوى معين معبّر على الإنترنت بغض النظر عما إذا كان المقصود منه التحريض على الكراهية أو الأذى، أو حتى في حال كان يشكل تهديداً.

كما اقترحت التعديلات عقوبات جنائية على خطاب الكراهية، وأكثر من ذلك، فإن هذا التعديل يساوي بين خطاب الكراهية وانتقاد شخصيات عامة أو شركات على وسائل التواصل الاجتماعي، وهو ما سيسمح للسلطات باحتجاز أي شخص يشتبه في نشر خطاب الكراهية لمدة 24 ساعة إلى سبعة أيام قابلة للتمديد لمدة شهر واحد. وبالتالي من الممكن استخدام هذا الإجراء لاستهداف معارضي الحكومة والناشطين والمدافعين عن حقوق الإنسان.

بالإضافة إلى ذلك، تم تعديل المادة 9 لتجرّم إرسال أو نشر أي معلومات قد تتضمن محتوى جنسي بغض النظر عن نيّة المرسل.

فعلى سبيل المثال، في حال تمكّن أحد أفراد جهاز الأمن من ضبط محادثة جماعية، على أحد مواقع التواصل الاجتماعي، قد تحتوي على مواد إباحية، سواءاً كانت من قبيل المزاح، أو حتى إذا كانت تتعلق بمناقشة حالات صحية أو طبية جنسية، فيمكن ملاحقة أولئك الأشخاص دون الحاجة إلى تقديم شكوى من شخص قد تضرّر من مشاركة مثل هذه المواد.

كما تمّ رفع عقوبة التعامل بالمواد الإباحية من ثلاثة أشهر إلى ستة، ورفع الحد الأدنى والأقصى للغرامة، أي تغليظ العقوبة.

إلى جانب ذلك، تمّ تعديل المادة 2 بإضافة عبارة "التطبيقات" إلى تعريف نظام المعلومات، الأمر الذي يعني إدراج جميع تطبيقات الهواتف الذكية مثل (الواتساب وخلافه) وإخضاعها للرقابة، وبالنتيجة تقييد حرية التعبير وخرق الحياة الخاصة للأفراد. كما أن القانون في المادة 11 و13 يعاقب على التشهير الإلكتروني، ويسمح للحكومة بمصادرة الأجهزة الشخصية، ونظم المعلومات وتعليقها وتفتيشها، مما ينتهك حق الأفراد في الخصوصية.

شَهِدت العاصمة عمّان مؤخراً احتجاجات واسعة، ورفضاً شعبياً لسياسات قمع حرية التعبير عن الرأي لتطبيق قانون الجرائم الإلكترونية بصورته المعمول بها حتى هذا الوقت.

بناءً على ذلك، في 9 كانون الأول 2018، أعلنت الحكومة الأردنية أنها ستقوم بسحب مشروع القانون المعدّل لسنة 2015 المتعلق بمكافحة الجرائم الإلكترونية والذي سبق أن تمّ إحالته إلى مجلس النواب بناءً على طلب من رئيس مجلس النواب في الأردن، عاطف الطراونة، وذلك بحجة دراسته تمهيداً لإعادة صياغته بما يتماشى مع التشريعات الجزائية النافذة في الأردن. إلاّ أنه وبعد مرور 48 ساعة على سحب المشروع، وفي 11 كانون الأول تحديداً، أجرت الحكومة في جلستها بعض التعديلات الجديدة على مشروع القانون قبل أن ترسله مجدداً إلى مجلس النواب، الأمر الذي اعتُبر من قبيل "الالتفاف على المطالب الشعبية لتلطيف تعدّيها الصارخ على الحقوق والحريات التي كفلها الدستور". وبالتالي رفض خوض حوار وطني حول أي نص تشريعي يتماشى مع التطورات التقنية والتكنولوجية في العالم مع مختلف الجهات المجتمعية خاصة تلك التي لديها تحفظات على التعديلات الجديدة[1].

في 19 شباط 2019، ناقش مجلس النواب الأردني في جلسته الثانية والعشرين مشروع القانون المتعلق بمكافحة الجرائم الإلكترونية، واختتمت الجلسة بالتصويت بالأغلبية على مقترح النائب عبد الكريم الدغمي بردّ مشروع القانون إلى الحكومة لإدخال التعديلات اللازمة على بعض النصوص القانونية، أهمها ما يتعلق بتعريف خطاب الكراهية والمعاقبة على الأخبار الكاذبة والإشاعات إلى جانب عدم الخلط ما بين مشروع القانون وقانون العقوبات الأردني.

الفرع الرابع: في القانون الأوروبي

لا نبالغ إذا قلنا إن التجربة الأوروبية في حقل أمن المعلومات والخصوصية هي التجربة الأكثر نضجاً في العالم، فعلى المستوى الوطني كانت الدول الأوروبية من أوائل الدول التي تعاملت مع الظاهرة تعاملاً واقعياً عبر دراسات معمّقة للواقع ولطبيعة المشكلات وللحلول والتدابير الأفضل. لم تكن تجربة متسرّعة، لكنها لم تكن أيضاً بطيئة من حيث الاستجابات، بل على العكس كانت استجابات مبكرة في حدود متطلّبات الواقع. ولأن فهم الظاهرة أساساً، وأخذ التدابير على ضوء هذا الفهم المعمّق هما أهم ضمانات النجاح فإن الدول الأوروبية بإدراكها لظاهرة جرائم الحاسوب توقف فعالية المكافحة على انسجام التدابير التشريعيّة الأوروبية. وعلى مدى الخمسة عشر عاماً الماضية

[1] www.accessnow.org

جاءت الاتجاهات التشريعية الأوروبية متماثلة تقريباً أو متقاربة بشأن التعامل مع ظاهرة جرائم الحاسوب والإنترنت[1].

ومع تطور الظاهرة، ومع الشعور بأن ما أنجز – وهو كثير – لم يعد كافياً بسبب الحاجة إلى مزيد من التوحّد ومزيد من الانسجام[2]. والأهم من ذلك، عملت هذه الجهود والتعاون بين دول أوروبا في حقل المكافحة إلى جعلها مؤسسات حكومية. وعليه جاءت مبادرة المجلس الأوروبي المتمثّل بوضع مشروع اتفاقية عالمية لجرائم الحاسوب. ونركّز أدناه على معالجة هذه الاتفاقية باعتبارها الرؤية الأوسع والأحدث للإطار القانوني للحماية من جرائم الحاسوب في بيئة أوروبية، بل في العالم أجمع دون إغفال ما سبقها من أنشطة على المستوى الوطني لكلّ دولة مكتفين بإيراد نماذج من الجهود الوطنية:

1- فرنسا:

سنّ المشرّع الفرنسي القانون رقم 19 – 88 بتاريخ 5 كانون الثاني/ يناير 1988 الخاص ببعض جرائم المعلوماتية، وضمنه قانون العقوبات الفرنسي في المادة (462) وجرم فيه مجرد الولوج إلى نظام المعالجة الآلية أو البقاء فيه بطريق غير مشروع (2/462). وشدد العقوبة في الأحوال التي ينجم فيها عن هذا الولوج محو أو تعديل في المعطيات المعالجة آلياً. ونصّ القانون على تجريم إتلاف المعطيات وتزوير المستندات المعالجة آلياً، واستعمال هذه المستندات. وعاقب على هذه الجرائم بعقوبة الحبس أو الغرامة. وقد خضع هذا القانون لتعديلات في العام 1993 وسّعت من نطاق السلوكيات محلّ التجريم إضافة إلى تعديل بعض العقوبات لتحقيق مزيد من الأبعاد الردعيّة.

2- **بريطانيا:**

سنّ المشرّع البريطاني قانون إساءة استخدام الحاسوب لسنة 1990 (Computer Misuse Act) وبدأ سريانه بتاريخ 29 آب/أغسطس 1990. وقد خلق هذا القانون ثلاث جرائم جديدة لمواجهة جرائم الاختراق والتوصّل غير المصرح به لتعديل معطيات الحاسوب وإتلافها بشكل عام وجرائم إدخال الفيروس بشكل خاص. هذه الجرائم هي:

أ. الدخول غير المصرح به لنظام الحاسوب (النشاط الرئيسي للعب أو التطفّل).

ب. نفس الفعل السابق، ولكن بقصد ارتكاب أو تسهيل ارتكاب فعل آخر.

[1] د. جورج لبكي – المعاهدات الدولية للإنترنت، نقل بتصرف، مصدر سابق.

[2] القمة العالمية لمجتمع المعلومات، جنيف 2003 وتونس 2005م، 2017/1/29، متاح على الرابط:
http://www.itu.int/net/wsis/index-ar.html

ج. التعديل أو التحوير غير المصرّح به لنظام الحاسوب بقصد إضعاف أو تعطيل النظام.

وبالرغم من أن الاستجابة البريطانية للتدابير التشريعيّة الجديدة في حقل تقنية المعلومات وصفت بأنها متأخرة عن غيرها من الدول الأوروبية، ومتأخرة بالتأكيد عن الاستجابة الأمريكية إلا أن السنوات الأخيرة، وتحديداً الأعوام من 1998 وحتى الآن، تشهد تميزاً في التجربة البريطانية سواء من حيث محتوى التنظيم أو الحلول التشريعية المقرّرة، ليس في نطاق أمن المعلومات فحسب، بل في نطاق حماية البيانات الشخصية والخصوصية وتنظيم حرية البيانات والمعلومات وفي مختلف الفروع الأخرى لقانون تقنية المعلومات.

3- ألمانيا الإتحادية:

صدر بتاريخ 15 أيار/مايو 1986 (قبل اتحاد الألمانيتين) القانون الثاني لمكافحة الجريمة الاقتصادية، وسرى مفعوله في الأول من آب/أغسطس 1986. وقد جرّم هذا القانون إتلاف أو محو أو تغيير أو تزوير البيانات المعالجة آليّاً، وشدّد العقوبة بالنسبة إلى البيانات ذات الأهمية الأساسية لقطاع الأعمال أو السلطة الإدارية لتصل إلى حدّ السجن لمدة خمس سنوات والغرامة. وكذلك جرّم هذا القانون غش الحاسوب أو الاحتيال بواسطة الحاسوب وعاقب عليه بالعقوبة المذكورة ذاتها، كما عاقب على الحصول دون تصريح من قِبل الفاعل لنفسه أو غيره على بيانات غير معدّة أو مخصّصة له ومحمية بوجه خاص ضد الوصول غير المصرّح به.

4- الدانمارك:

سنّ المشرّع بتاريخ 6 حزيران/يونيو 1985 القانون الخاص بجريمة الحاسوب، وضمنه المواد 193 و263 من قانون العقوبات، وعاقب فيه على مجرد الوصول إلى معلومات أو برامج الغير. وشدّد العقوبة في حال ارتكاب فعل التوصل بغرض الإطلاع على الأسرار التجارية (م2/263) وجرم إتلاف وتعطيل أنظمة المعالجة الآلية وتخزين البيانات (م 193).

5- النرويج:

عدّل المشرّع قانون العقوبات عام 1985 وجرّم الوصول غير المصرّح به عن طريق تخطّي الحماية إلى البيانات المخزّنة أو المنقولة بالوسائل الإلكترونية أو الفنية الأخرى، وجرّم إتلاف وتعطيل البيانات والاستخدام غير المصرّح به لوقت وخدمات الحاسوب.

6- سويسرا:

تضمّن القانون السويسري بشأن جرائم المعلوماتيّة نصوصاً تعاقب على الحصول دون تصريح على بيانات مخزّنة إلكترونياً أو على البرامج بقصد الإثراء على نحو غير مشروع وعلى التواصل مع نظم الحاسوب وإتلاف المعطيات.

7- فنلندا:

في أواخر الثمانينيات اقترح فريق العمل المكلّف بدراسة جرائم الحاسوب تجريم كل صور الوصول إلى نظم البيانات المرتكبة باستخدام غير مأذون لكلمة السرّ، أو تخطّي الرقابة أيّاً كانت وسائلها.

الفرع الخامس: في القانون الأميركي

إن الولايات المتحدة الأمريكية لا تتميز بأسبقية سنّ التشريعات القانونية فحسب، بل تتميز بسن تشريعات خاصة بكافة مسائل تقنية المعلومات، وفي قطاعات الحوسبة والاتصالات والإنترنت التي ترتبط أو تتعلق بجرائم الحاسوب والإنترنت مباشرة أو على نحو غير مباشر، كما أنها تشريعات تراعي خصائصها المميزة، وتتطور تبعاً لتطور قطاع التقنية ذاته. وتتميز الولايات المتحدة الأمريكية أيضاً بوضع عدة تشريعات على المستوى الفدرالي وحزمة معتبرة من التشريعات على مستوى الولايات.

فعلى المستوى الفدرالي، تبلور نشاط لجنة الكونغرس الخاصة بحماية استخدام الحاسوب بتقديم مشروع (قانون حماية الحاسوب سنة 1984) غير أن هذا المشروع، لدى عرضه ودراسته من قبل الكونغرس ولجانه المختصة، خضع للتعديل في أحكامه بشكل جوهري، وتمّ إقراره بعد سلسلة من التعديلات والإضافات، ولم يصدر باسمه المشار إليه، بل صدر قانون (غشّ الحاسوب وإساءة استخدامه لعام 1984) أو كما يترجم اسمه البعض (قانون الاحتيال وإساءة استخدام الحاسوب – Computer Fraud and abuse Act) وأضيف إلى القانون مدونة القانون الأمريكي تحت قسم الجرائم. واعتبر أول قانون أمريكي يجرم مرتكبي الجرائم الإلكترونية في الولايات المتحدة الأمريكية آنذاك.

وقد نصّ القانون المذكور على تجريم مجرد الاتصال دون تصريح بنظام حاسوب، وعلى الاتصال المصرح به الذي يستخدم فيه الفاعل الحاسوب لأغراض غير مصرح بها كتعديل أو إتلاف أو تدمير أو إفشاء المعلومات المخزنة في الحاسوب، كما نصّ على عقاب من يرتكب فعلاً من شأنه منع الاستخدام المصرح به للحاسوب"، وخضع لاحقاً لتعديلات واكبت التطورات التقنية. وصدر أيضاً في الولايات المتحدة على المستوى الفدرالي (قانون أمن الحاسوب لسنة 1987) والذي يقضي

باتخاذ الوكالات الفدرالية خطوات ملائمة لتأمين وحماية أنظمة حواسيبها، وينظّم هذا القانون مستويات الحماية والرقابة عليها والمسؤولية عن إغفالها. وتوالت بعد ذلك في التسعينيات التعديلات والتشريعات الفرعية والقطاعية ذات العلاقة بأمن المعلومات.

أما على مستوى الولايات، فقد سنّت جميع الولايات – عدا واحدة – قوانين خاصة، أو عدّلت قوانين العقوبات لديها بما يكفل النصّ على تجريم أنشطة جرائم الحاسوب مع تباين في ما بينها سواء من حيث صور النشاط المجرم، أو من حيث آلية التعامل مع محل الاعتداء. فقد نصّت قوانين بعض الولايات على المساواة بين معطيات الحاسوب والأموال المادية من حيث الحكم القانوني، ما يتيح انطباق نصوص التجريم التقليدية على جرائم الحاسوب باعتبارها تستهدف المعطيات المتخذة حكم الأموال المادية بنص القانون الصريح. من هذه الولايات مثلاً، ولاية آلاسكا، التي أدخل قانونها الجديد الإتلاف المعلوماتي ضمن الأموال التي تخضع لنصوص الإضرار بالمال، وكذلك ساوى قانونها بين غشّ الإنسان وغشّ الآلة، وكذلك ولاية فرجينيا التي نصّ قانونها على اعتبار وقت أو خدمات الحاسوب، أو خدمات المعالجة الآلية للبيانات أو المعلومات أو البيانات المخزّنة ذات الصلة بذلك ماليّاً، وبهذا الحكم يتحقق انطباق نصوص التجريم التقليدية فيما يتصل بالاعتداء على المال.

على أن غالبية الولايات سنّت نصوصاً تشريعية صريحة في تجريم أنشطة إساءة استخدام الحاسوب، فنصّت قوانين كل من أريزونا، وكاليفورنيا، وكولورادو، وديلاوار، وفلوريدا، وجورجيا، وإلينوي، وميتشيغان، وميسوري، ومونتانا، ونيومكسيكو، ورود أيسلاند، وتينسي، وأوتاوا، وسكونسين، على تجريم إتلاف القيم المعلوماتية غير المادية، وغش الحاسوب، والاستخدام غير المصرّح به للحاسوب، وسرقة وقت أو خدمات الحاسوب، وإعاقة استخدامه، والتوصل غير المصرح به لتعديل أو تغيير أو إنشاء أو استخدام البيانات المخزنة في نظام الحاسوب. ونحاول هنا رصد الإطار القانوني لجرائم الحاسوب والإنترنت من خلال تحليل قوانين الولايات الأمريكية (49 ولاية).

إن الولايات المتحدة الأمريكية لا تتميز بأسبقية سن التشريعات لمكافحة هذه الجرائم فحسب، بل إنها تتميز بسن تشريعات خاصة بكافة مسائل تقنية المعلومات، وفي قطاعات الحوسبة والاتصالات والإنترنت التي ترتبط أو تتعلق بجرائم الحاسوب والإنترنت مباشرة أو على نحو غير مباشر. وهي تشريعات تراعي خصائصها المميزة، وتتطور تبعاً لتطور قطاع التقنية ذاته. وتتميز الولايات المتحدة الأمريكية أيضاً بوضع عدة تشريعات على المستوى الفدرالي، وحزمة معتبرة من التشريعات على مستوى الولايات. فعلى المستوى الفدرالي، تبلور نشاط لجنة الكونغرس الخاصة بحماية استخدام الحاسوب بتقديم مشروع (قانون حماية الحاسوب سنة 1984) غير أن هذا المشروع لدى عرضه ودراسته من قبل الكونغرس ولجانه المختصة، جرى التعديل على أحكامه بشكل

جوهري، وجرى إقراره بعد سلسلة من التعديلات والإضافات. ولم يصدر باسمه المشار إليه وإنما بعنوان قانون (غش الحاسوب وإساءة استخدامه لعام 1984) أو كما يترجمه بعضهم (قانون الاحتيال وإساءة استخدام الحاسوب computer fraud and abuse Act) وأضيف إلى القانون مدونة القانون الأمريكي تحت قسم الجرائم. واعتبر أول قانون أمريكي يجرم مرتكبي الجرائم الإلكترونية في الولايات المتحدة الأمريكية آنذاك.

لقد كان للولايات المتحدة الأمريكية دور أساسي في التصدي للجريمة الإلكترونية، حيث تصدى قانون العقوبات للظواهر الإجرامية فحدّد الأفعال الجرمية، ووضع العقوبات الرادعة لكل منها بهدف إنزال العقاب بالمجرمين، وحماية المجتمع من شرورهم، وردع غيرهم عن الاقتداء بهم. وهذا يمثّل الشق الأول من المعادلة التشريعية الجزائية. أمّا الشق الثاني فيتمثل في قانون أصول المحاكمات الجزائية الذي يحدد القواعد الإجرائية والضمانات التي ينبغي أن تسير على هديها الجهات المعنية بإنفاذ القانون في مراحلها المختلفة بدءاً بمرحلة الاستدلال وانتهاءً بالمحاكمة، فالقانونان إذن يكمّل بعضهما الاخر.

ومن الأمثلة على أشهر الجرائم الإلكترونية في الولايات المتحدة الأمريكية:

1- **اختراق وكالة ناسا**:

تمكن عمر جوناثان جيمس، المعروف بإسم "Comerade"، وهو في السادسة عشرة من عمره، من الدخول على منظومة بيانات مركز "مارشال لرحلات الفضاء" في "هانتسفيل" بولاية آلاباما الأمريكية، وبدأ تحميل الوثائق والبرمجيات الخاصة بمحطة الفضاء الدولية "ناسا" عام 1999.

وقدر المسؤولون في "ناسا" قيمة الوثائق التي سرقها "جيمس" بنحو 7.1 ملايين دولار، وأجبرت هذه الحادثة الوكالة على إغلاق شبكاتها لمدة 3 أسابيع لإصلاح الأضرار الجسيمة بتكلفة 41 ألف دولار.

2- **فضيحة ووترجيت**:

تجسس عدد من العاملين بصحيفة "نيوز أوف ذا وورلد" البريطانية، على المكالمات الهاتفية للسياسيين والمشاهير، وفي تحقيق يعود تاريخه إلى عام 2002، استعانت الصحيفة بمحققين مأجورين للتنصت والدخول على حسابات البريد الصوتي الخاصة بمشاهير من ضمنهم عارضة الأزياء ايل ماكفرسون، والممثلة سيينا ميلر، فضلاً عن شخصيات من العائلة الملكية البريطانية، وأغلقت الصحيفة في أعقاب هذه الفضيحة التي عرفت بفضيحة "ووترجيت".

3- **اختراق سوني**:

اخترقت مجموعة من القراصنة في يونيو 2011، يطلقون على أنفسهم اسم "لولزيك" شركة "سوني بيكتشرز"، وسرقوا بيانات تضمنت أسماء وكلمات سرية وعناوين الآلاف من عملاء الشركة، وقالت المجموعة إن هذا الهجوم كان انتقاماً من "سوني" لأنها تخذت إجراء قانوني ضد جورج هوتز، الذي اخترق نظام تشغيل منصة الألعاب "بلاي ستيشن 3" في وقت سابق.

المطلب الثاني: تصنيف مرتكبي الجرائم الإلكترونية

"المجرم الإلكتروني" أو "مخترقو أمن الشبكات" أو "المجرم الرقمي"، هو المجرم الذي له القدرة على تحويل لغته إلى لغة رقمية وتخزينها واسترجاعها باستخدام الحاسوب الإلكتروني الرقمي وملحقاته ووسائل الاتصال الرقمية، وذلك بأداء فعل أو الامتناع عنه، مما يحدث اضطرابات في المجتمع الدولي أو المحلي نتيجة لمخالفة قواعد الضبط الاجتماعي محلياً أو دولياً، باعتباره مرتكب جرائم الأذكياء، فهو نتاج التقدم التكنولوجي في مجال المعلومات والاتصالات. هذا التقدم الذي قدم للدول وأجهزتها الأمنية الكثير من التسهيلات والإمكانيات التي تسهم في رفع كفاءتها وتطوير قدرتها على التصدي للجريمة الإلكترونية إلا أنه في المقابل أدى ويؤدي في الوقت ذاته إلى تطوير وتحديث الجريمة من حيث الأساليب والمضامين، خاصة في ظل اتجاه التنظيمات أو العناصر الإجرامية إلى توظيف بعض مخرجات التكنولوجيا المعلوماتية في أنشطتها وممارستها، فتجاوز بذلك هذا التقدم بقدراته وإمكانياته أجهزة الدولة الرقابية، وأصبح يهدد أمنها وأمن مواطنيها.

الفرع الأول: السمات الخاصة بالمجرم الإلكتروني

هناك تفرقة تقليدية في دراسات علم الإجرام، تقوم على التمييز بين الإجرام الطبيعي والإجرام الاصطناعي "المكتسب"، ونادى بهذه التفرقة عالم الإجرام الإيطالي "جارفالو"، ولقد ثار جدال فقهي يدور حول النوع الذي ينتمي إليه المجرم الإلكتروني[1]، وما يمكن القول في هذا الصدد أن المجرم الإلكتروني يمثل بالنسبة للمجموعات التقليدية أي (الإجرام الطبيعي) شخصية مستقلة قائمة بذاتها، فهو من جهة مثال منفرد "للمجرم الذكي" ومن جهة إنسان اجتماعي بطبعه[2].

ولذلك فإن العقوبة لكي تحقق هدفها في مجال الردع العام أو الخاص، وإذا كنا في مجال الإجرام الإلكتروني، فيجب علينا أن ننظر إلى المجرم الإلكتروني من حيث الظروف التي دفعته

[1] عبد الفتاح بيومي حجازي، **"نحو صياغة نظرية عامة في الجريمة والمجرم الإلكتروني"**، ص. 95.
[2] محمد سامي الشوا، **"ثورة المعلومات وانعكاساتها على قانون العقوبات"**، الطبعة الثانية، دار النهضة العربية، مصر، 1998، ص. 24.

لارتكاب جريمته وأسبابها، وصفاته، وذلك حتى يمكن إعادة تأهيله اجتماعياً، ويعود إلى حظيرة المجتمع كمواطن صالح ينفع المجتمع ولا يضرّه.

ونظراً لازدياد عدد الجرائم الإلكترونية سواءً على الصعيد العالمي أو الوطني، فقد حظيت أبحاث علم الإجرام في هذا المجال بالعديد من الدراسات القانونية والتي تحاول كشف النقاب عن فكرة المجرم الإلكتروني.

ما من شكّ أن تطور العلوم الجنائية، وما نتج في نطاقها من دراسات وتحديداً في ميدان علم الإجرام، أدى إلى تحديد سمات عامة للمجرمين عموماً، وسمات خاصة يمكن استظهارها لطائفة معينة من المجرمين تبعاً للجرائم التي يرتكبونها، فكان من الطبيعي أن يؤدي ارتكاب الجرائم الإلكترونية إلى ظهور وولادة طائفة جديدة من المجرمين، أطلق عليهم جانب من الفقه تسمية "المجرم الإلكتروني".

ولا شك أن الفاعل في الجريمة الإلكترونية يرتكب فعلاً غير مشروع ويعتدي فيه على حق من حقوق الغير، يعدّ في نظر القانون مجرماً ويتعرض للعقاب المناسب إذا ما اقترف جريمته.

إذ يقول الخبير الأمريكي "دون باركر" أن المجرم الإلكتروني وإن كان يتميز ببعض السمات الخاصة، إلا أنه لا يخرج في النهاية، عن كونه مرتكباً لفعل إجرامي يتطلب توقيع العقاب عليه، فكل ما في الأمر، أنه ينتمي إلى طائفة خاصة من المجرمين تقترب في سماتها من جرائم ذوي الياقات البيضاء "الإجرام المكتسب"، من حيث انتماء المجرم في أكثر الحالات إلى وسط اجتماعي، وتميّزه بدرجة من العلم والمعرفة، وليس معنى ذلك أنهم أقلّ خطورة من الناحية الإجرامية من المجرمين ذوي الياقات الزرقاء "المجرم بطبيعته".

باعتبار أن الجريمة الإلكترونية كأي عمل إجرامي آخر، قد تُرتكب في شكل اشتراك في جماعة إجرامية، فإن هذه الأخيرة تتميز ببعض الخصائص المختلفة عن سمات الفاعل الفرد المستقل في ارتكاب الجريمة الإلكترونية، لذلك سنحاول استعراض السمات المشتركة بين مرتكبي الجريمة الإلكترونية والسمات التي تنفرد بها الجماعات الإجرامية في الجرائم الإلكترونية.

1- السمات المشتركة بين جميع فئات مرتكبي الإجرام الإلكتروني:

باعتبار أن الفاعل في الجريمة الإلكترونية شخص طبيعي كأصل عام[1] يرتكب أفعاله غير المشروعة تعبيراً عن إرادته الخاصة المستقلة، ووفقاً لعلم الإجرام الإلكتروني فإن الفاعل الفرد في

[1] خالد عياد الحلبي، ص. 32.

الجريمة الإلكترونية يتمتع بقدر كبير من الذكاء، ويتميز عن غيره من المجرمين، واتصافه بسمات معينة جعلت منه محلاً للعديد من الأبحاث والدراسات، إذ يتميز المجرم الإلكتروني بعدة سمات أهمها:

أ- الذكاء

يعتبر الذكاء من أهم صفات مرتكبي الجرائم الإلكترونية، إذ يقال عادة أن الإجرام الإلكتروني هو إجرام الأذكياء، بالمقارنة مع الإجرام التقليدي الذي يميل إلى العنف[1]، فإذا كان من السهل تصور العنف في الإجرام الموجه ضد مكونات النظام المادي للمعلومات والذي يحدث غالباً في إطار العمليات الإرهابية، فإنه لا يمكن أن يتصور أي عنف في الإجرام الموجه ضد المكونات المنطقية والبيانات، وبالتالي يجب أن يكون المجرم على دراية كافية بأنماط الجريمة. فهناك أنماط مختلفة يمكن استخدامها في التلاعب بهذه البيانات تتمثل في "القنابل المنطقية"[2]، كما أن هناك أنماط أخرى تعرف بالفيروسات الإلكترونية[3].

وتأكيداً على ذلك فقد أجريت دراسة من طرف وزارة الداخلية البريطانية أن الأطفال الذين يقضون وقت أطول أمام ألعاب الكمبيوتر يكونون أكثر ذكاءً مقارنة بغيرهم ممن لا يمارسون ألعاب الكمبيوتر، إذ يتوقع دخولهم مجالات الاستخدامات الغير مشروعة لجهاز الكمبيوتر.

ولقد أجريت الدراسة على مائة وسبعة وعشرون شخصاً من بينهم ثلاثة وستون طفلاً، بمقارنتهم مع صغار آخرين وجد أن هواة الكمبيوتر يعتبرون أشخاص أذكياء للغاية ومتحمسين وساعين للإنجاز، كما أفادت المتابعة لمدة خمسة أعوام على هؤلاء الأطفال أنهم تفوقوا دراسياً والتحقوا بالجامعة، وبوظائف مرموقة[4].

ب- الخبرة والمهارة

يرى الخبير "دون باركر" أن المهارة هي أبرز خصائص المجرم الإلكتروني، فتنفيذ الجريمة التقنية يتطلب قدراً من المهارة يتمتع بها الفاعل والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في المجال الإلكتروني الحديث أو مجرد التفاعل الاجتماعي مع الآخرين.

---

[1] محمد سامي الشوا، مرجع سابق، ص. 35.

[2] القنابل المنطقية: يمكن للجاني زرع تعليمات في برنامج مزود بعداد والذي عندما يصل إلى بداية معينة تنطلق هذه التعليمات لتمحوا البرنامج.

[3] الفيروسات: هي عبارة عن برامج من الحجم الصغير الذي يصعب اكتشافه ويوضع في الأسطوانة ثم يقوم بنسخ نفسه بداخل النظام لتدميره في فترة وجيزة. انظر: محمد سامي الشوا، مرجع سابق، ص. 35

[4] خالد ممدوح إبراهيم، **"الجرائم الإلكترونية"**، ص. 134.

إلا أن ذلك لا يعني بالضرورة أن يكون مرتكب جريمة إلكترونية حديثة على قدر كبير من العلم في هذا المجال، أو أن تكون لديه خبرة كبيرة، بل إن الواقع العملي قد أثبت أن بعض أنجح مجرمي الإلكترونية الحديثة لم يتلقوا المهارة اللازمة لارتكاب الجريمة عنطريق التعليم أو الخبرة المكتسبة من العمل في المجال التقني، كما أننا نرى أن عدداً لا بأس به من صور الجرائم الإلكترونية التي ترتكب عبر وسيلة تقنية، أي عندما لا يكون نظام الإلكتروني هو هدف الجريمة، لا يتطلب سوى الحد الأدنى من المعرفة والمهارة لظهور الجريمة أو إمكانية ظهورها.

2- <u>المجرم الإلكتروني عائد للإجرام</u>

يعود الكثير من مجرمي الإلكترونية إلى ارتكاب جرائم أخرى في مجال الكمبيوتر، انطلاقاً من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم، وأدت إلى تقديمهم إلى المحاكمة في المرة الأولى، ويؤدي ذلك إلى العودة إلى الإجرام، وقد ينتهي بهم الأمر كذلك في المرة الثانية إلى تقديمهم للمحاكمة[1].

تتكون هذه النزعة الإجرامية المتوفرة في المجرم الإلكتروني لتأثره بعوامل عضوية ونفسية صاحبت نشأته، ومع اقتران تلك العوامل بعنصر آخر جديد يساعد على استثارة الحالة الإجرامية ويزيد من قدرة ضغوط عوامل الإجرام وتفوقها على موانع الإقدام، وهذا العنصر الجديد هو الذي أكسب الشخص للمهارة العلمية والتكنولوجية.

3- <u>الميل إلى التقليد</u>

يبلغ الميل إلى التقليد منتهاه حينما يوجد الفرد وسط الجماعة إذ يكون عندئذ أسهل وأسرع انسياقاً لتأثير الغير عليه، ويظهر ذلك في الجريمة المرتكبة عبر الإنترنت، لأن أغلب الجرائم تتم من خلال محاولة الفرد تقليد غيره بالمهارات الفنية، مما يؤدي به الأمر إلى ارتكاب الجرائم.

لا شك أن ذلك نتيجة لعدم الاستواء في شخصية الفاعل الفرد الذي يتأثر بخاصية الميل إلى التقليد بسبب عدم وجود ضوابط يؤصلها الفرد في ذاته مما يحجم لديه غريزة التفاعل مع الوسط المحيط، وينتهي به الأمر إلى ارتكاب الجريمة.

الفرع الثاني: أدوات الجرائم الإلكترونية وطرق تنفيذها

تشهد التقنية والتكنولوجيا تطورات كثيرة واستحداث لأمور جديدة، هذا الأمر ينذر بتطور أدوات وسبل الجريمة الإلكترونية بشكل أكثر تعقيداً أو أشد ضرراً من قبل، الأمر الذي يلزم الدول

[1] عبد الفتاح بيومي حجازي، **"التزوير في جرائم الكمبيوتر والإنترنت"**، دار الكتب القانونية، مصر، 2007، ص. 107.

لتطوير آليات مكافحة هذه الجرائم، واستحداث خطوط دفاع، وسن قوانين وتوعية الناس بمستحدثات هذه الجرائم وتشجيعهم للإبلاغ عنها.

1- **أدوات الجريمة الإلكترونية:**

أ. برامج نسخ المعلومات المخزنة في أجهزة الحاسب الآلي.

ب. الإنترنت كوسيط لتنفيذ الجريمة.

ج. خطوط الاتصال الهاتفي التي تستخدم لربط الكاميرات ووسائل التجسس.

د. أدوات مسح الترميز الرقمي (البار كود).

ه. الطابعات.

و. أجهزة الهاتف النقال والهواتف الرقمية الثابتة.

ز. برامج مدمرة: مثل برنامج حصان طروادة Trojan horse بحيث يقوم بخداع المستخدم لتشغيله، حيث يظهر على شكل برنامج مفيد وآمن ويؤدي تشغيله إلى تعطيل الحاسب المصاب وبرنامج الدودة الذي يشبه الفيروس، ولكنه يصيب أجهزة الحاسب دون الحاجة إلى أي فعل، وغالباً يحدث عندما ترسل بريد إلكتروني إلى كل الأسماء الموجودة في سجل الأسماء.

2- **أهم طرق الجريمة الإلكترونية** وتشمل وليس حصراً على:

أ. تخريب المعلومات وإساءة استخدامها : ويشمل ذلك قواعد المعلومات، المكتبات، تمزيق الكتب، تحريف المعلومات، تحريف السجلات الرسمية، الخ.

ب. سرقة المعلومات: بيع المعلومات كالبحوث أو الدراسات الهامة أو ذات العلاقة بالتطوير التقني أو الصناعي أو العسكري أو تخريبها أو تدميرها.. إلخ.

ج. تزوير المعلومات: الدخول لقواعد في النظام التعليمي وتغيير المعلومات وتحريفها، مثل تغيير علامات الطلاب.

د. تزييف المعلومات: تغيير في المعلومات على وضع غير حقيقي مثل: وضع سجلات شهادات لم تصدر عن النظام التعليمي وإصدارها.

ه. انتهاك الخصوصية: نشر معلومات ذات طبيعة خاصة عن الأفراد، أو الدخول لحسابات الأفراد الإلكترونية ونشر معلومات عنهم أو وضع معلومات تخص تاريخ الأفراد ونشرها.

و. التصنت: الدخول لقواعد المعلومات وسرقة المحادثات عبر الهاتف.

ز. التجسس: اعتراض المعلومات ومحاولة معرفة ما يقوم به الأفراد.

ح. التشهير: استخدام المعلومات الخاصة أو ذات الصلة بالانحراف أو الجريمة ونشرها بشكل القصد منه اغتيال شخصية الأفراد أو الإساءة.

ط. السرقة العلمية: الكتب والبحوث العلمية الأكاديمية وخاصة ذات الطبيعة التجريبية والتطبيقية.

ي. سرقة الاختراعات: وخاصة في المجالات العلمية لاستخدامها أو بيعها.

ك. الدخول غير القانوني للشبكات: بقصد إساءة الاستخدام أو الحصول على منافع من خلال تخريب المعلومات أو التجسس أو سرقة المعلومات.

ل. قرصنة البرمجيات: النسخ غير القانوني للبرمجيات واستخدامها أو بيعها مرة أخرى.

م. قرصنة البيانات والمعلومات: اعتراض البيانات وخطفها بقصد الاستفادة منها، وبخاصة أرقام البطاقة الائتمانية، وأرقام الحسابات، وكلمات الدخول، وكلمات السر.

ن. خلاعة الأطفال: نشر صور خاصة للأطفال "الجنس السياحي" للأطفال خاصة وللإناث على الشبكات بشكل عام ونشر الجنس التخيلي.

س. القنابل البريدية: إرسال فيروسات لتدمير البيانات من خلال رسالة إلكترونية.

ع. إفشاء الأسرار: الحصول على معلومات خاصة جداً ونشرها على الشبكة.

ف. الاحتيال المالي بالبطاقات: هذا ناتج عن استخدام غير شرعي لبطاقات التسوق أو المالية أو الهاتف الخ.

ص. سرقة الأرقام والمتاجرة بها: خاصة أرقام الهواتف السرية واستخدامها في الاتصالات الدولية أو أرقام بطاقات الائتمان.

ق. التحرش الجنسي: ويقصد به المضايقة من الذكور للإناث أو العكس من خلال المراسلة أو المهاتفة، أو المحادثة أو الملامسة.

ر. المطاردة والملاحقة والابتزاز: ملاحقة الذكور للإناث أو العكس، والتتبع بقصد فرض إقامة علاقة ما، وذلك من خلال استخدام البريد الإلكتروني وإرسال الرسائل.

ش. الإرهاب الإلكتروني: يشمل جميع المكونات السالفة الذكر في بيئة تقنية متغيرة والتي تؤثر على فرص الإرهاب ومصادرة هذه التغيرات تؤثر على تكتيكات الإرهاب وأسلحته وأهدافه، ومن التكتيكات الإرهابية ما يعرف بالإرهاب الإلكتروني[1].

الفرع الثالث: الفئات التي تستهدفها هذه الجرائم

تقع الجرائم الإلكترونية ضمن ثلاث فئات رئيسية هي: الأفراد، والممتلكات، والحكومات. فيما تختلف أنواع الهجمات والأساليب المستخدمة ودرجات الصعوبة بحسب كل فئة.

1- الأفراد:

تشمل هذه الفئة من الجرائم الإلكترونية كل الأفراد الذين يقومون بتوزيع معلومات ضارة أو غير قانونية عبر شبكة الإنترنت، مثل مطاردة الضحايا عبر المواقع أو منصات وسائل التواصل الاجتماعي، وتوزيع المواد الإباحية والاتجار وغيره.

2- الممتلكات:

ضمن هذه الفئة، تقع كل الهجمات التي تحاول الوصول بشكل غير قانوني إلى ممتلكات الأشخاص، مثل تفاصيل البنك أو بطاقة الائتمان وغيره. عادة ما يقوم المتسلل بسرقة التفاصيل المصرفية بهدف الوصول إلى الأموال أو إجراء عمليات شراء عبر الإنترنت أو تنفيذ عمليات التصيد الاحتيالي المخادعة لحمل الضحايا على الكشف عن معلوماتهم الشخصية. كما يمكنه أيضاً استخدام برامج ضارة للوصول إلى صفحة ويب معينة تحتوي على معلومات سرية.

3- الحكومات:

هذه الفئة هي الأقل شيوعاً حول العالم، ولكنها من أخطر الجرائم الإلكترونية. تُعرف الجريمة ضد الحكومات والمؤسسات الرسمية أيضاً باسم الإرهاب السيبراني، وتشمل اختراق المواقع الحكومية أو المواقع العسكرية أو توزيع الدعاية السيئة أو التلاعب بعمليات التصويت في الانتخابات وغيره. هؤلاء المجرمون هم عادة إرهابيون أو تابعون لحكومات معادية للدولة.

[1] www.democraticac.de

رصدت مؤخراً تغيراً في أنماط الجريمة الإلكترونية خلال عام 2020، حيث صارت تستهدف بشكل أكبر الشركات والمؤسسات بدلاً من التركيز على الأفراد.

ووجدت الدراسة التي أجراها مركز موارد سرقة الهوية (أي. تي. أر. سي)، وهو مؤسسة غير ربحية، تهدف لمتابعة الجرائم الإلكترونية، أن عدد جرائم سرقة البيانات في الولايات المتحدة تراجع في 2020 بنسبة 19% إلى 1108 جرائم، في حين أن الجرائم الإلكترونية، التي تستهدف الأفراد تراجعت 66% خلال الفترة نفسها مقارنة بالعام السابق. وأشار إلى أن جرائم الاحتيال وطلبات الفدية أصبحت الآن هي النمط المفضل لمجرمي الإنترنت[1].

ولا تقتصر الجرائم الإلكترونية على أفراد أو مجموعات، وإنما قد تمتد إلى مستوى الدول فتهدد أمنها القومي وسلامتها المالية، ويشمل ذلك التجسس الإلكتروني (وأبرز أمثلته ما كشفته تسريبات الأمريكي إدوارد سنودن بشأن مخططات الإدارة الأمريكية للتجسس على اتصالات الأفراد والدول الأخرى)، والسرقة المالية، وغيرها من الجرائم العابرة للحدود.

وأحياناً توصف الأنشطة الموجهة لدولة واحدة على الأقل بأنها تقع في إطار "الحرب الإلكترونية"، والنظام القانوني الدولي يحاول تحميل الفاعلين المسؤولية عن أفعالهم في مثل هذا النوع من الجرائم من خلال المحكمة الجنائية الدولية.

وتتطلب الهجمات الإلكترونية التي يرتكبها أفراد أومجموعات معرفة تقنية عالية، وهي تحمل أشكالاً عديدة ترتكب يومياً على الإنترنت.

وأبرز الجرائم التي تستهدف بشكل رئيسي "شبكات الحاسوب أو الأجهزة تتضمن فيروسات الحاسوب، وهجمات الحرمان من الخدمة، والبرمجيات الخبيثة".

وأمثال هذه الجرائم يرتكبها قراصنة مجرمون يوصفون بـ"أصحاب القبعات السوداء"، وعلى النقيض منهم هناك "قراصنة أخلاقيون" أو "اصحاب القبعات البيض" (يعود أصل التسمية إلى أفلام رعاة البقر الأميركية القديمة عندما كان "البطل" يرتدي قبعة بيضاء و"الشرير" يرتدي قبعة سوداء) الذين يستغلون مهاراتهم لاكتشاف الثغرات والتنبيه إليها، أو حتى اكتشاف القراصنة المجرمين والإبلاغ عنهم.

وعندما يكون الأفراد هم الهدف الرئيسي للهجوم الإلكتروني، فإن الحاسوب يعتبر حينئذ أداة بدلاً من كونه هدفاً، ومثل هذه الهجمات لا تتطلب عادة خبرات تقنية عالية، وتعتمد على الخطأ البشري

[1] www.gans9ans.tn

كي تنجح، وأبرز أمثلتها: الاحتيال وسرقة الهوية، وحرب المعلومات، والتصيد، والبريد المزعج، ونشر المحتوى الفاحش أو المسيء مثل المضايقات والتهديدات، وكذلك تجارة المخدرات[1].

الفرع الرابع: طرق الوقاية من هذه الجرائم

على الرغم من أن الجرائم الإلكترونية تشكل خطراً على مختلف المناطق في العالم، إلا أن هناك عدة خطوات وطرق تمكنك من حماية نفسك وحماية عائلتك من مثل هذه الجرائم. وهي تندرج تحت أقسام متعددة كالتالي:

أ- حماية نفسك ضد مرتكبي الجرائم الإلكترونية:

1- استخدم التحديثات المعتادة لبرامج مضادات الفيروسات ومضادات التجسس على جميع أجهزتك الإلكترونية.

2- احرص على تحديث متصفحك الخاص بالإنترنت بشكل مستمر.

3- لا تتواصل إلا مع الجهات والمواقع الإلكترونية ذات الأمان العالي والتي تقوم بحماية معلومات وبيانات المرور الخاصة بك.

4- لا تضغط على أي روابط أو إعلانات أو ملحقات، ولا تقم بالرد على أي رسائل الكترونية من مصادر غير معروفة لديك.

5- اكتب الرابط الذي تود استعراضه بيدك دائماً بدلاً من النقر على روابط جاهزة، وخاصة إذا لم تكن تعرف المرسل.

6- لا تقم بالرد على أي رسالة يتم فيها سؤالك عن بياناتك الشخصية، أو معلوماتك الأمنية مثل معلوماتك البنكية مثلاً. لا تجعل بياناتك منتشرة عبر الإنترنت بشكل يسهل أن تصبح ضحية في المستقبل.

7- حدّد أولئك الذين يمكنك مشاركة معلوماتك معهم عن طريق إعدادات الخصوصية والأمان على حساباتك في شبكات التواصل الاجتماعي المختلفة.

8- صدق إحساسك، فإذا شعرت أن هناك عرضاً جيداً لدرجة أن يصعب عليك تصديق صحته، فقد يكون إحساسك صحيحاً، ثق به.

[1] www.aljazeera.net

9- استخدم كلمة مرور قوية يصعب اكتشافها، استخدم الحروف والأرقام والرموز التي يمكنك تذكرها بسهولة ولكن يصعب على غيرك اكتشافها أيضاً.

10- لا تستخدم كلمة المرور ذاتها مرتين، وقم بتغييرها بشكل دوري.

11- إذا شعرت بأمر غير طبيعي، قم بإبلاغ السلطات المسؤولة.

ب- حماية نفسك ضد اللصوص الإلكترونيين**:**

1. لا تتشارك بياناتك الشخصية مع أي شخص لا تعرفه.
2. لا تنشر أي معلومات شخصية تخصّك مثل رقم هاتفك أو عنوان بريدك الإلكتروني على شبكات التواصل الاجتماعية أو غيرها من المواقع الإلكترونية.
3. لا تلتق شخصياً بالأشخاص الذين تعرفت إليهم عن طريق الشبكات الإلكترونية.
4. تجنب أي شكل من أشكال المحادثات الجنسية عبر الإنترنت.
5. استخدم إعدادات الخصوصية والأمان لتحديد من يمكنهم مشاهدة نشاطك الإلكتروني عبر شبكات التواصل الاجتماعية والمواقع الأخرى.

ج- حماية نفسك ضد (البلطجية) الإلكترونية:

1) إذا تم ابتزاز عن طريق الإنترنت أو عن طريق هاتفك، تجاهل الأمر، فالمبتزين عادة ينتظرون رداً، وتجاهلهم سيساعدك في إيقافهم.

2) قم بحظر أي شخص يحاول ابتزازك عن طريق ملفك الشخصي على مواقع التواصل الاجتماعي.

3) ساعد هؤلاء الآخرين الذين تم ابتزازهم من قبل، فالمبتزون عادة ما يتوقفون عن ابتزازهم إذا ما كان هناك شخص آخر يعمل على وقف نشاطهم.

4) إذا كنت أحد الوالدين، تحدث مع أطفالك حول هؤلاء اللصوص والمبتزين وحول خطرهم وتأثيرهم. علم أطفالك آداب استخدام الإنترنت، وكن أنت نفسك خير قدوة لهم في ذلك[1].

[1] www.assawsana.com

الفرع الخامس: فئات مرتكبي هذه الجرائم

يرتبط الإجرام الإلكتروني ارتباطاً وثيقاً بشخصية المجرم ودوافعه، فهو لا يتميز بالضرورة بالميول الإجرامية، فقد يكون شخصاً حسن النية ولا يقصد ارتكاب عمل إجرامي، ولكنه يتميز بالتقدم في مجال استخدام الحاسوب، فهو مجرم ذو مهارات تقنية عالية وذكاء غير عادي يمكنه من الدخول إلى أنظمة الحاسب الآلي والقدرة على تعديل البرامج وارتكاب الجرائم، والخبرة والمهارة في استخدام التقنية المعلوماتية، فالمجرم المعلوماتي أو "الهاكر" يقصد به مخترق شبكات الحاسوب.

1- القراصنة الهواة: ويقصد بهم الأشخاص الذين يستهدفون المعلومات والحسابات الآلية ويكونون من فئة الشباب البالغين ومعظمهم يكون من الطلبة. وبالتالي يقومون هؤلاء الأشخاص بالدخول إلى أنظمة الحاسب الآلي بطرق غير مصرّح لهم الدخول إليها، فهم بذلك يكسرون الحواجز الأمنية لأغراض عدة منها الخبرة أو حتى الفضول.

2- القراصنة المحترفين: ويقصد بهم الأشخاص التي تكون أعمارهم محصورة ما بين 25-45 سنة، بحيث يحتلون مكانة في المجتمع الجرائمي بالإضافة إلى اختصاصهم في مجال التقنية الإلكترونية، بحيث يتّسمون بالخطورة وتكرارهم للجرائم مرة أخرى.

3- طائفة الحاقدين: ويقصد بهم الأشخاص المنتقمون فمعظمهم يكونون ضد أصحاب العمل والمنشآت التي عملوا بها فهم يسعون إلى الانتقام من المدراء في العمل، بالإضافة إلى أن هذه الطائفة تكون أقل خطورة مقارنة بغيرها من الطوائف، ويكمن الهدف وراء هذه الطائفة هو التعمّد في إخفاء وإنكار الأفعال والأنشطة التي يقومون بها، مستخدمين بذلك تقنيات متخصصة في زراعة الفيروسات والبرامج المضرّة، بهدف تخريب الأنظمة المعلوماتية، حيث أن هذه الطائفة لا تهدف إلى إثبات قدراتهم ومهاراتهم الفنية، ولا أيضاً يهدفون إلى تحقيق مكاسب مادية، أو حتى سياسية.

4- طائفة المتطرفين.

5- طائفة الفكريين: فهم عبارة عن أشخاص يستعملون شبكة الإنترنت في نشر، بث، استقبال إنشاء المواقع التي من شأنها تسهّل عملية الانتقال والترويج لكافة المواد الفكرية التي تساهم في تغذية الطرف الفكري. وقد يقوم المفكرين باستعمال الشبكات الإعلامية الإخبارية وكافة المواقع الإلكترونية؛ بهدف تحقيق أغراض دعائية تحقق مصالحهم.

6- طائفة المتجسسين: ويقصد بهم الأشخاص الذين يسعون إلى العبث أو إتلاف المحتويات الشبكية، التي تشكل خطراً كبيراً، من مثل إرسال أسرار العمل في إحدى الشركات عبر

الإنترنت ومواقع التواصل الاجتماعي إلى الشركات المنافسة، فهي تهدف في المقام الأول على الحصول على قاعدة بيانات معلوماتية عن الأعداء والأصدقاء.

7- طائفة مخترقي الأنظمة: حيث يكون هؤلاء الأشخاص يقومون بتبادل المعلومات فيما بينهم، بهدف معرفة نقاط الضعف في الأنظمة المعلوماتية مستعملين بذلك النشرات الإعلامية الإلكترونية، من مثل مجموعات الأخبار. وبالتالي يقومون هؤلاء الأشخاص بعقد وتولي المؤتمرات لجميع مخترقي الأنظمة الإلكترونية، مع أهمية وجود خبراء، وذلك بهدف المشاركة والتشاور حول وسائل الاختراق وآلياتها.

الإطار التطبيقي

القسم الثاني
مدى مكافحة الجرائم المستحدثة المرتكبة عبر وسائل التواصل الاجتماعي محلياً ودولياً

تمهيد

إنّ جرائم الإنترنت قد تُرتكب عن طريق حاسب آلي في دولة ما، في حين يتحقق الفعل الإجرامي في دولة أخرى، لذلك هي جرائم لا تحدُّها حدود وتتميز بالتباعد الجغرافي بين الفاعل والمجني عليه، وبين الحاسوب أداة الجريمة والمعطيات أو البيانات محل الجريمة.

هذه السمة دفعت الجهود لمكافحة جرائم الإلكترونية لتتمدد من النطاق الوطني إلى النطاق الإقليمي والدولي الذي برز على نحو متزايد لدى المنظمات الدولية والإقليمية خاصة العاملة في مجال منع الجريمة ومكافحتها، ذلك أن الإشكالات التي تثيرها مميزات هذه الجرائم عديدة، وبشكل خاص الإجراءات الجنائية والاختصاص والقانون الواجب التطبيق والسلطات الملاحقة في ظل التطور التكنولوجي الضخم. فإن جرائم المعلوماتية لا تزال ترزح في جو من الفوضى القانونية لجهة الملاحقة وفرض العقوبات وتنفيذها، لذلك فإننا سنعمد في هذا الفصل إلى تحديد التحديات، المخاطر والوسائل الوقائية على صعيد التشريع **(المبحث الأول)**، ومن ثم ننتقل إلى طرق المكافحة المعتمدة على صعيد سلطات إنفاذ القانون والتوعية والتدريب **(المبحث الثاني)**.

المبحث الأول

الأطر الدولية والمحلية لمكافحة هذه الجرائم

أدت عولمة الأنشطة الإجرامية إلى ظهور الحاجة إلى تعزيز أشكال التعاون الدولي وآلياته، وقد أدّى إدراك أن التحقيقات والملاحقة القضائية ومكافحة الجريمة لم يعد من الممكن حصرها داخل الحدود الوطنية إلى صقل أشكال وآليات التعاون الدولي القائمة وتحسينها وتبسيطها على نحو متواصل، من أجل مواكبة أشكال الجريمة المعاصرة، بما في ذلك الجرائم الواقعة على التجارة الإلكترونية.

لذا يعد التعاون الدولي دعامة أساسية من دعائم واستقرار النظام الدولي، إذ بدونه لا يتصور تحقيق انتظام في سير العلاقات الدولية ولا تنشيط لمجالات التنمية الاجتماعية والاقتصادية والثقافية، ولن تصل الجهود الدولية نحو تعزيز هذه العلاقات في مختلف المجالات إلى أهدافها، فلا بد أن التعاون الدولي هو الأساس لقيام التنظيمات الدولية في صورتها الحديثة، بل إن من عناصر تعريف المنظمة الدولية بأنها هيئة أنشئت على أسس من التعاون الاختياري بين الدول من أجل تحقيق مصالح مشتركة.

المطلب الأول: الأطر التشريعية

ينبغي على كل دولة من دول المنطقة العمل على تحديث تشريعاتها، وسنّ قوانين لتجريم الجرائم السيبرانية، فقوانين العقوبات التقليدية ليست صالحة على الدوام لحكم هذه الأفعال الجرمية الجديدة، على الأقل في حالة الأفعال التي تكون فيها المعلوماتية محل الاعتداء. وكذلك ينبغي العمل باستمرار على تحديث التشريعات لمواكبة التطور التقني والأساليب المبتكرة التي يعتمدها المجرمون وإعادة النظر في العقوبات وفي ظروف تشديدها وفق ما يظهر من ممارسات إجرامية.

الفرع الأول: الإطار التشريعي المحلّي والدولي

إن تحقيق وتحرّي الجرائم الإلكترونية والمقاضاة في نطاقها ينطوي على مشكلات وتحدياتٍ إدارية وقانونية تتّصل ابتداءً بمعوقات ومتطلبات عمليات ملاحقة الجناة، فإن تحقّقت مكنة الملاحقة أصبحت الإدانة صعبة لسهولة إتلاف الأدلة من قبل الجناة أو لصعوبة الوصول إلى الأدلّة أو لغياب الاعتراف القانوني بطبيعة الأدلة المتعلقة بهذه الجرائم[1].

حرص مجلس أوروبا على التصدي للاستخدام غير المشروع للحاسبات وشبكات المعلومات، وتجلى ذلك في اتفاقية بودابست في 23 نوفمبر 2001 المتعلقة بالإجرام الكوني بمعنى الإجرام الإلكتروني أو الجرائم الإلكترونية، إيماناً من الدول الأعضاء في هذا المجلس والدول الأخرى الموقعة على هذه الاتفاقية بالتغيرات العميقة التي حدثت بسبب الرقمية والتقارب والعولمة المستمرة وتتكون هذه الاتفاقية من ثماني وأربعين مادة.

[1] د. عيسى ميشال طوني، **"التنظيم القانوني لشبكة الإنترنت"** صادر، ط1، 2001، القسم الثالث، ص. 388.

تشمل جوانب عديدة من جرائم الإنترنت بينها الإرهاب وعمليات تزوير بطاقات الائتمان ودعارة الأطفال. لكن مراسل BBC قال إن هناك قلقاً من أن تؤدي زيادة الرقابة إلى انتهاك حقوق مستخدمي الإنترنت[1].

أدرجت اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا) موضوع التشريعات السيبرانية في قائمة اهتماماتها منذ عام 2007، ونظمت في هذا الإطار عدداً من الأنشطة لعلّ أهمها مشروع "تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية"، الذي يموّله صندوق التنمية في الأمم المتحدة والذي بدأت الإسكوا بتنفيذه عام 2009. وقد أعدّت الإسكوا في إطار هذا المشروع إرشادات الإسكوا للتشريعات السيبرانية "التي تغطّي ستة محاور أساسية هي:

أ. الاتصالات الإلكترونية وحرية التعبير

ب. المعاملات الإلكترونية والتوقيع الإلكتروني

ج. التجارة الإلكترونية وحماية المستهلك

د. معالجة البيانات ذات الطابع الشخصي

ه. الملكية الفكرية في المجال المعلوماتي والسيبراني والجرائم السيبرانية.

وقد أعدّت الإسكوا هذه الإرشادات ليستعين بها المشرّعون عند صياغة التشريعات السيبرانية، وليستفيد منها أصحاب القرار في الوزارات والمؤسسات الحكومية من أجل وضع قوانين جديدة أو تعديل القوانين النافذة، وليعتمد عليها القضاة والمحامون في معالجة المسائل القانونية المتعلقة بالفضاء السيبراني[2].

لقد دخلت الدول العربية إلى عالم تشريع الفضاء السيبراني متأخرة بعض الشيء عن الدول الغربية، لذا فإنّ المشرع في الدول العربية وجد أن توفّر القوانين المنظمة لموضوع الفضاء السيبراني يشكل ضرورة من الناحية القانونية بالنسبة للتعاملات بين الأفراد والمؤسسات، ومثال على ذلك الإثبات الإلكتروني والتعاقد والمراسلات والحدّ من الجرائم السيبرانية. وتضاف إلى ذلك العوائق أمام التعاملات بين أفراد ومؤسسات عربية ونظيرتها في الدول الغربية حيث يتطلب مثل هذا التعاون وجود قواعد قانونية متوافقة بالحد الأدنى.

أمام هذا الغياب في التشريع السيبراني في الدول العربية، قامت بعض الدول في بداية الأمر باقتباس قوانين بعض الدول الأوروبية ومحاولة ملاءمتها مع الواقع القائم في الدول العربية المعنية

[1] هلاكي عبد اللاه أحمد، 2010، www.neelwafurat.com

[2] إرشادات الإسكوا للتشريعات السيبرانية، **مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية**، ص. أ.

لإقرار هذه القوانين، وقد تمّ أيضاً الاسترشاد بالمعاهدات والاتفاقيات الدولية والنماذج القانونية لمنظمات دولية مثل "الأونسيترال Uncitral" في ورشة التشريع العربية. وتختلف المقاربات التشريعية في الدول العربية لناحية تقنين مواضيع الفضاء السيبراني.

يعود اهتمام اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا) بتطوير التشريعات السيبرانية Cyber laws إلى أنها تشكل عنصراً أساسياً من عناصر البيئة التمكينية لمجتمع المعلومات، ولبناء الاقتصاد المبني على المعرفة.

لذلك قامت منظمة الإسكوا منذ عام 2007 بإعداد عدة دراسات حول وضع التشريعات السيبرانية في الدول العربية.

كما أوضحت الدراسات واجتماعات الخبراء أهمية تنسيق التشريعات السيبرانية فيما بين بلدان المنطقة العربية، من أجل تحسين التجارة الإلكترونية البينية ومواجهة الجرائم السيبرانية وبناء اقتصاد إقليمي مبني على المعرفة. وبناء على ذلك باشرت الإسكوا عام 2009 بإعداد وتنفيذ مشروع "تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية" للاستجابة لاحتياجات المنطقة العربية في مجال التشريعات السيبرانية[1].

وبهدف ضمان استمرارية العمل على تطوير التشريعات السيبرانية في المنطقة، تضمّن مشروع الإسكوا إنشاء شبكة افتراضية للنقاش والحوار، بحيث تشكّل هذه الشبكة اللُّبنة الأساسية لتبادل المعرفة وأداة لاستدامة المشروع.

الفرع الثاني: الإتفاقيات الدولية

تعتبر الاتفاقية الدولية الأكثر أهمية في هذا المجال هي اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية التي اعتمدت في عام 2001[2]. وفي بحثنا هذا حرصنا على استعراض هذه الاتفاقية كونها نموذجاً مقبولاً للجهود الدولية لمعالجة هذه الجرائم والتصدي لها، ومن ثم نستعرض أهم الاتفاقيات الدولية في هذا الجانب وتم تناول البحث وفق السياق الآتي:

1- <u>"الاتفاقية الأوروبية لمكافحة الإجرام المعلوماتي والمسماة (بودابست) لعام 2001:</u>

هو التزام دولي ملزم بشأن هذه المسألة وهو بمثابة المبدأ التوجيهي لأي بلد لوضع تشريع وطني شامل لمكافحة جرائم الإنترنت وكإطار للتعاون الدولي بين الدول الأطراف في هذه المعاهدة"[3].

---

[1] إرشادات الإسكوا للتشريعات السيبرانية، مرجع سابق، ص. ج 25.

[2] Understanding Cybercrime: A guide for Developing Countries.

[3] د. وليد طه، **"التنظيم التشريعي للجرائم الإلكترونية في اتفاقية بودابست"**، بحث إلكتروني، 2017، ص. 16.

ونظراً إلى ازدياد الجرائم المتعلقة بالحاسوب شرعت الدول المتحضرة بوضع تشريعات خاصة لمكافحة جرائم الحاسوب التي تعتبر ظاهرة مستحدثة على علم الإجرام. ومن هذه الدول الولايات المتحدة وفرنسا وباقي دول الاتحاد الأوروبي الذي وضع اتفاقية حول جرائم الحاسوب سنة 2001، والتي أوصت فيها الدول الأعضاء باتخاذ كافة الإجراءات التشريعية وغيرها حسب الضرورة لجعل الدخول إلى جميع نظم الحاسوب أو أي من أجزائه بدون وجه حق جريمة جنائية بحسب القانون المحلي، كما أوصت هذه الاتفاقية بمجموعة من المبادئ العامة المتعلقة بالتعاون الدولي، في مجال الشؤون الجنائية. وحدّدت كذلك الإجراءات المتعلقة بطلبات المساعدة المتبادلة بين الدول في غياب الاتفاقيات الدولية[1]. وقد اعتمد الاتحاد الأوروبي التشريع على غرار اتفاقية بودابست[2]. ويهدف واضعو هذه الاتفاقية إلى حث الدول الأعضاء على التوأمة بين القوانين الوطنية ونصوص الاتفاقية علاوة على ضرورة استكمال الأدوات القانونية لهذه الدول في المسائل الإجرائية، وذلك بغية تحسين الاتفاقية لقدرات النيابات العامة على إجراء التحقيقات وجمع الأدلة[3]. وقد وقعت على هذه الاتفاقية 30 دولة.

ولأهمية هذه الاتفاقية انضم إليها العديد من الدول من خارج المجلس الأوروبي، وأبرز هذه الدول الولايات المتحدة الأمريكية التي صادقت عليها في 22 أيلول/سبتمبر 2006، ودخلت حيّز النفاذ في الأول من كانون الثاني/يناير 2007[4].

أما جمهورية ألمانيا الفيدرالية فقد صادقت على الاتفاقية عام 2009، وصادقت فرنسا على الاتفاقية في 10 كانون الثاني/يناير 2006، أما مملكة النرويج فقد صادقت على هذه الاتفاقية سنة 2006.

واشتملت الاتفاقية على عدة جوانب من جرائم الإنترنت، بينها الإرهاب وعمليات تزوير بطاقات الائتمان ودعارة الأطفال[5]. وتهدف الاتفاقية إلى:

1. توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية.

---

[1] Cybercrime. EU Regulatory Framework on Cybercrime.norway.university of Oslo. 2017. Available at: http://www.jus.uio.no/ifp/english/research/projects/nrccl/signal/research-prongs/cybercrime

[2] د. عبد العال الديربي، الأستاذ محمد صادق إسماعيل. **"كتاب الجرائم الإلكترونية"**، مصدر سابق، ص. 8.

[3] أ. وسيم حرب **"كتاب برنامج تعزيز حكم القانون في بعض الدول العربية"**، مصدر سابق، ص. 7.

[4] **"دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول"**، ضمن فعاليات المؤتمر الالث لرؤساء المحاكم العليا (النقض، التمييز، التعقيب) في الدول العربية المنعقد في جمهورية السودان خلال الفترة 9/23.25/م الموافق 7-1433/11/9هـ. ص.10.

[5] **"دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول"**، مصدر سابق، ص. 10.

2. توفير الإجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة إلكترونياً بواسطة الحاسوب.
3. تعيين نظام سريع وفعال للتعاون الدولي.
4. الحفاظ بشكل سريع على البيانات المخزّنة على أجهزة الحاسوب وحفظها والإفصاح الجزئي عن حركة هذه البيانات المخزنة على الحاسوب.
5. جمع معلومات عن حركة البيانات وعن إمكانية وجود تدخل في محتواها[1].

واستناداً إلى المواد المشار إليها (2-13) فإن الاتفاقية تلزم الدول الأعضاء فيها (دول الاتحاد الأوروبي وأي دولة توقع عليها أو تريد أن تنضم إليها) باتخاذ الإجراءات والتدابير التشريعية الملائمة لتجريم تسع جرائم في ميدان الجرائم الإلكترونية وهي:

1- الدخول غير القانوني المتعمد Illegal Access.
2- الاعتراض غير القانوني Illegal Interception.
3- التدخل المتعمد أو الإرادي في المعطيات Data Interference بالتدمير Damaging أو الحذف Deletion أو التشويه والإفساد Deterioration أو تبديلها أو تغييرها أو تعديلها Alteration أوتعطيلها أو كبتها أو إخمادها Supperession.
4- التدخل المتعمد في الأنظمة system interference.
5- التزوير المتعمد باستخدام جهاز الحاسوب computer-related forgery
6- إساءة استخدام الأجهزة misuse of devices.
7- الاحتيال المتعمد باستخدام الحاسوب computer-related fraud
8- الجرائم المرتبطة بدعارة الأطفال offences related to child pornography.
9- الجرائم المرتبطة بحق المؤلف copyright and related offences.

وتناولت المادة 11 من الاتفاقية القواعد العامة المتعلقة بالمساهمة الجنائية والعقوبة بشأن الجرائم المشار إليها في المواد من 2 – 10. وقد ألزمت الاتفاقية الدول الأعضاء باتخاذ تدابير تشريعية للنص على المسؤولية عن الشروع والتدخل والتحريض في ارتكاب هذه الجرائم أو ما تختاره الدولة منها، وذلك بغرض وجود رادع عام لما لهذه الجرائم من تأثير شديد في اقتصادات

[1] د. جورج لبكي، **"المعاهدات الدولية للإنترنت"**، مصدر سابق، ص. 37.

الدول، وكذلك النص على مسؤولية الأشخاص المعنوية عن الأفعال التي ترتكب لمصلحة الشخص المعنوي من قبل أي شخص يتصرف لمصلحته سواء أكان استناداً إلى تمثيل قانوني أم باعتباره مناطاً به اتخاذ قرار عن الشخص القانوني، أو لأنه خاضع لسلطته، بما في ذلك أفعال التحريض والتدخل والمساعدة الجنائية، وكذلك مسؤولية الرؤساء عن غياب أو تخلّف الرقابة والإشراف والتحكم بتصرفات الأشخاص المعنيين بالعمل. ويلاحظ هنا وفقاً للاتفاقية امتداد نطاق المساءلة الجنائية للشخصين الطبيعي والمعنوي.

أما بالنسبة إلى العقوبات والتدابير فقد أوجبت الاتفاقية على الدول الأعضاء في الاتفاقية إقرار العقوبات الملائمة والفعالة لهذه الجرائم بما فيها العقوبات المانعة للحرية بالنسبة إلى الأشخاص الطبيعيين مثلما هو الحال في القانون الأمريكي، والغرامات المالية بالنسبة إلى الأشخاص المعنويين[1].

ومن أهداف الاتفاقية حماية الأطفال من الاستغلال الجنسي، فقد صاغت الاتفاقية في إطار دولي قواعد قانونية لمكافحة هذا الاستغلال غير القانوني، وهذا ما نظمته المادة 9 من الاتفاقية[2].

وفي احترام حقوق الإنسان تؤكد هيكليتها وكذلك المادة رقم 15 أنه يجب الأخذ بعين الاعتبار الحاجة إلى ضمان وجود توازن مناسب بين المصالح المتحصلة من إجراء عملية قمعية واحترام حقوق الإنسان الأساسية. ونصت على ذلك أيضاً اتفاقية العهد الدولي الخاصة بالحقوق المدنية والسياسية التابع للأمم المتحدة[3].

ونظمت الاتفاقية تسليم المتهمين، حيث تنص المادة 24 على وجوب تسليم المتهمين بين الأطراف في ما يتعلق بالجرائم الواردة في المواد من 2 – 11 من الاتفاقية شرط أن تكون تلك الجرائم معاقباً عليها بموجب القوانين المرعية الإجراء في بلد كل من الطرفين المعنيين بحرمان من الحرية لفترة أقصاها سنة على الأقل أو بعقوبة أشد في غياب اتفاق آخر إجباري على أساس التشريعات المتبادلة الموحدة أو معاهدة نافذة حول موضوع تسليم المتهمين[4]. وحول التنسيق التقني تفرض المادة 3/25 من الاتفاقية في حالة الاتصالات المتعلقة بطلبات التعاون المشترك أن تتم هذه الاتصالات عبر قنوات توفر القدر الكافي من الأمان والتوثيق بما في ذلك التشفير إذا تطلب الأمر ذلك.

---

[1] وليد طه، نقل بتصرف، مصدر سابق، ص. 15.

[2] انظر المادة 9 من الاتفاقية.

[3] جان فرنسوا هنرت، **"أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي"**، نقل بتصرف، ص.106.

[4] كرستينا سكولمان، **"كتاب برنامج تعزيز حكم القانون في بعض الدول العربية"**، مصدر سابق، ص. 120.

وعن التعاون الدولي تنص المادة 35 من الاتفاقية على التالي:

"كل دولة نقطة اتصال يمكن الاتصال بها على مدار 24 ساعة وكذلك على مدار الأسبوع لضمان تقديم المساعدة الفورية أثناء التحقيق في الانتهاكات القانونية المتعلقة بنظم وبيانات إلكترونية أو بهدف جمع أدلة ذات طابع إلكتروني عن انتهاكات قانونية"[1].

وقد طبق كثير من البلدان الاتفاقية في إطار قوانينها الوطنية. ويتضح ذلك على سبيل المثال في تشريع رومانيا الذي يلتزم بنص الاتفاقية بشكل كبير، ويعتبر التشريع الروماني كاملاً وسهل الفهم وفعالاً في الوقت نفسه[2].

وبالتالي يمكن القول إن الاتفاقية تغطي مجموعة كبيرة من الجرائم الجنائية، وأنها تميزت بأهمية قانونية من حيث إنها ركزت على اتخاذ التدابير التشريعية الموضوعية لمكافحة هذه الجريمة، وألزمت الدول إضافة للقواعد الموضوعية بالاهتمام بالقواعد الإجرائية. وعن أهمية المسؤولية الجنائية جاهد المشرّع لتقنين قواعدها، وألزم الدول الأعضاء باتخاذ تدابير تشريعية، ووضع القواعد القانونية لتنظيمها. وأوجبت تعزيز أطر التعاون الدولي والإقليمي، ولا سيما توقيع معاهدات لتسليم المجرمين بين الدول حتى تفوت فرصة الهروب من هذه الجرائم عند المجرمين.

2- أهم الاتفاقيات والمعاهدات الدولية المتعلقة بالجرائم الإلكترونية:

بعد أن أيقنت الدول أن هناك حاجة ملحة لعقد اتفاقيات من أجل مكافحة الجرائم السيبرانية تمّ عقد الاتفاقيات والمعاهدات الدولية العديدة التي ساهمت في مكافحة الجرائم الإلكترونية منها:

أ. اتفاقية حماية الأفراد في مجال المعالجة الآلية للبيانات الشخصية 1981[3].

ب. الاتفاقية الأمريكية المتعلقة بجرائم الحاسوب الآلي والإنترنت لسنة 1999: عقد في جامعة ستانفورد في ولاية كاليفورنيا في الولايات المتحدة الأمريكية مؤتمر (6-7 كانون الأول/ديسمبر 1999) بمشاركة العديد من الهيئات والمنظمات الدولية والممثلين القانونيين. وتم اقتراح هذه الاتفاقية لتعزيز الحماية من الإرهاب وجرائم الحاسوب الآلي 65.

---

[1] جان فرنسوا هنرت، **"أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي"**، نقل بتصرف، مصدر سابق، ص. 106-109

[2] كرستينا سكولمان، مصدر سابق، ص. 64.

[3] Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. 2017.
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?docum

ج. اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، وقد تم التوقيع عليها في مدينة باليرمو "السويد" عام 2000.

د. الاتفاقية الأوروبية لمكافحة الإجرام المعلوماتي "بودابست" عام 2001.

ه. اتفاقية الأمم المتحدة بشأن استخدام الخطابات الإلكترونية في العقود الدولية "نيويورك 2005".

الفرع الثالث: المؤتمرات الدولية

لإبراز الجهود التي قطعتها الدول لمكافحة الجرائم السيبرانية في إطار المؤتمرات الدولية، سنحاول استعراض أهمّ وأبرز هذه المؤتمرات التي ساهمت في مكافحة الجرائم الإلكترونية والحدّ منها:

1- المؤتمر الدولي الأول لحقوق الإنسان الخاص بأثر التقدم التكنولوجي في حقوق الإنسان "مؤتمر طهران 1968" والذي تبنت الجمعية العامة للأمم المتحدة توصياته، حيث تم الاعتراف بحق الخصوصية وبأن من حق الإنسان أن يعيش لوحده بعيداً عن كشف أسراره، فسنّت بعض دول العالم في أوروبا وآسيا وأمريكا واليابان تشريعاتها في مجال حماية الخصوصية من الاعتداء، ألزمت من خلالها مواقع الإنترنت المعنية بجمع المعلومات بتسجيل أغراضها وإخضاع عملياتها لرقابة مفوض الخصوصية في الدولة باعتباره جهة قضائية معنية بحماية الأفراد من أي اعتداء[1].

2- مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين، والذي عقد في هافانا عام 1990.

3- مؤتمر الأمم المتحدة العاشر الذي عقد في فيينا عام 2000.

4- القمة العالمية لمجتمع المعلومات التي عقدت في جنيف 10-12 كانون الأول 2003.

5- أجندة تونس 2005 الفقرة 15 من مبادئ المرحلة الثانية من القمة العالمية لمجتمع المعلومات تحت رعاية الأمم المتحدة[2].

[1] أجندة تونس التي تم تبنيها في 15 تشرين الثاني 2005، متاحة على الموقع:
www.pdf.fr_agenda_tunis/pdf.fr_agenda_11327544873tunis/20687/files/fr/ci/org

[2] الاتحاد الدولي للاتصالات، القمة العالمية لمجتمع المعلومات، الوثائق الصادرة عن القمة، جنيف 2003 وتونس 2005م، مصدر سابق، ص. 59-77.

6- توصيات مؤتمر ورشة العمل على "التدابير الرامية إلى مكافحة الجريمة المتصلة بأجهزة الحاسوب" الذي عقد في بانكوك في 22 نيسان 2005 كجزء من مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية[1].

7- ورشتا عمل حول مكافحة استخدام الإرهابيين للإنترنت 18-2009/10/19 ومنع الإرهابيين من حيازة واستخدام أسلحة الدمار الشامل أو مكوناتها 20-2009/10/21. وقد عقدتا بمشاركة الأمانة العامة لمجلس وزراء الداخلية العرب وخبراء من الدول العربية والأمم المتحدة والمنظمة العربية لتكنولوجيات الاتصال والمعلومات والمنظمات الإقليمية والدولية المعنية. وصدر عن كل منهما مجموعة من التوصيات[2].

8- المؤتمر العالمي لتنمية الاتصالات في حيدر آباد (الهند) (WTDC-10) في حزيران/يونيو 2010. وكان من بين المقررات أن الاتحاد ينبغي أن يساعد الدول الأعضاء، وخصوصاً البلدان النامية، في وضع التدابير القانونية المناسبة والعملية المتصلة بالحماية من التهديدات السيبرانية[3].

9- مؤتمر الأمم المتحدة الثاني عشر – البرازيل – السلفادور عقد عام 2010 وغطى ثماني مسائل منها مشاكل جرائم الإنترنت أو الشبكة العنكبوتية[4].

10- مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية 2-12نيسان لسنة 2015 المنعقد في الدوحة[5].

11- مؤتمر قمة الأمن السيبراني - مملكة البحرين 22 – 20 تشرين الأول 2014 ناقشت هذه القمة الموضوعات التالية: بحث سبل إعادة الأمن واستراتيجية تكنولوجيا المعلومات، وإعادة تعريف المخاطر، وتنفيذ أفضل الممارسات لتحقيق مدونة التهديدات، وتخفيف مخاطر أدوات التواصل الاجتماعي الجديدة، واستراتيجية مواجهة التهديدات المتنقلة، والاستغلال الجنسي للأطفال.

---

[1] د. جورج لبكي **"المعاهدات الدولية للإنترنت"**، نقل بتصرف، مصدر سابق، ص. 103.

[2] أ. عبد الله حامد الكيلاني، بحث الكتروني منشور بعنوان: **"جهود مكافحة الإرهاب النووي على الصعيد العربي، قطاع الشؤون القانونية جامعة الدول العربية"**، الرياض، 2013، ص10.

[3] الاتحاد الدولي للاتصالات (ITU)، الأمن السيبراني، ص21، متاح على الرابط:
https://www.itu.int/net/itunews/issues/2010/09/pdf/201009ar.pdf.11.1.2017

[4] مؤتمرات الجريمة ومؤتمر 2015-2017-1-23، نقل بتصرف، متاح على Wikipedia
https://ar.wikipedia.org/wiki/

[5] UN تقرير مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية الدوحة 2015م، الفقرة ج من حلقة العمل بشأن تعزيز تدابير منع الجريمة والعدالة الجنائية للتصدي للأشكال المتطورة للجريمة، مثل الجرائم الإلكترونية "السيبرانية"

12- مؤتمر قمة الأمن السيبراني "مينابولس، مينيسوتا الولايات المتحدة الأمريكية" بتاريخ 21-22 تشرين الأول/أكتوبر 2014. حيث شارك فيه ممثلون من القطاعين العام والخاص لمناقشة التدابير المضادة للتهديدات الإلكترونية، وتعزيز أمن القطاع العام والخاص في مواجهة الجرمية الإلكترونية، وقياس مدى تأمين برامج الحاسوب الآلي ضد الهجمات، وتطوير تحقيقات الشرطة ومهارات التحقيق التقنية والأدلة العلمية والإستراتيجيات الشاملة لمواجهة الجريمة الإلكترونية.

13- مؤتمر الإنتربول واليوروبول الثاني للجريمة الإلكترونية "سنغافورة" المنعقد في 1-3 تشرين الأول/أكتوبر 2014[1]. ودعمت عقد هذا المؤتمر إحدى الجهات الاعتبارية الدولية الفاعلة في مكافحة الجريمة الإلكترونية، وتعرف بـ"الجهود الدولية في الجريمة الإلكترونية"، وتسمى اختصاراً Glacy120. وقد أسهمت بدعمها بتمكين خبراء في الجريمة الإلكترونية من أكثر من عشرين دولة من المشاركة في المؤتمر الذي يهدف إلى تسهيل مهمة الوحدات المتخصصة في مكافحة الجريمة الإلكترونية في الاتصال بين بعضها بعضاً من خلال الشبكة الدولية International Networking.

14- مؤتمر الأمن السيبراني/جامعة نيويورك للتكنولوجيا في 18 ايلول/سبتمبر 2014 شارك في هذا المؤتمر خبراء الإنترنت والشركات والحكومات. وناقش المؤتمر الموضوعات التالية:

الخصوصية – الابتكارات في المؤسسة الأجنبية – أنظمة الأمن والإنترنت – حماية البنية التحتية الحساسة والمنظمات والأفراد من الهجمات الإلكترونية.

15- مؤتمر (Glacy) لبناء القدرات في بورلويس عاصمة جزر موريشيوس 11-14 آب/أغسطس 2014.

Glacy: Capacity Building in Mauritius-Conference and workshops

عقد هذا المؤتمر تحت رعاية "الجهود الدولية في الجريمة الإلكترونية Glacy". وقام مجلس أوروبا للجريمة الإلكترونية بدعم سلسلة من نشاطات بناء القدرات في 11 – 14 آب/أغسطس 2014. وناقشت ورش العمل والمؤتمر الموضوعات التالية: اتفاقية مجلس أوروبا للجريمة الإلكترونية ومدى إمكانية حصول سلطات إنفاذ القانون على المعلومات (Law enforcement access to data)، واستراتيجيات تدريب منتسبي سلطات

[1] Interpol/Europol Cybercrime Conference 2014, 1-3 October 2014.

تنفيذ القانون ومنتسبي السلطات القضائية، وحماية الطفل، وإعادة النظر في القانون الجنائي لمواكبة مقتضيات مكافحة الجريمة الإلكترونية والتعاون الدولي[1].

16- المؤتمر العالمي الرابع للفضاء الإلكتروني الذي عقد في مدينة لاهاي بهولندا خلال الفترة 16-17نيسان/أبريل لعام 2015.

الفرع الرابع: التعاون الدولي في مكافحة هذه الجريمة

يُعد التعاون الدولي في مجال مجابهة جرائم صناعة الموت، بشكل عام، ضرورة مُلحّة تفرضها التحديات والتطورات العالمية الراهنة خاصة بعد تنامي حجم الإرهاب السيبراني العابر للحدود، بحيث أصبحت نادرة في البلدان التي لم تكتوِ بنيران الإرهاب، وصارت الجرائم الإرهابية السيبرانية شراً مستطيراً في الآونة الأخيرة.

وفي حالات ليست قليلة يفلت مرتكبو هذه الجرائم من العقاب، وتتعدد أوجه التحديات والعوائق التي تُصعب من إمكانيات التعاون الفعال بين الدول بغرض مجابهة ذلك الخطر الداهم الحديث، الذي يهدد الدول والهيئات والشركات وغيرها تهديداً خطيراً ومباشراً.

يُشكل اختلاف النظم التشريعية للدول التي تطمح إلى تحقيق التعاون فيما بينها في مجال مجابهة الجرائم الإرهابية السيبرانية، عقبة كبيرة تحول في معظم الحالات دون تحقيق غايات وأهداف الدول خاصة عندما لا تواكب بعض الدول التطورات الهائلة الحاصلة في نوعية هذه الجرائم المعقدة، بإصدارها التشريعات المتطورة التي تلاحق الثورة الكبيرة في مجال استخدام الحاسوب وشبكات المعلومات العالمية في ارتكاب جرائم الإرهاب السيبراني على وجه الخصوص.

وتبرز هذه العقبة في حالات كثيرة حينما تكون التشريعات الجنائية الوطنية لبعض الدول قد سُنّت بفترة طويلة قبل نشوء هذه الجرائم شديدة التعقيد، وتكون الجرائم المشار إليها عصيّة الملاحقة في أحيان كثيرة بسبب ذلك القصور التشريعي وعدم مجابهة الأفعال التي يستحدثها مرتكبي الجرائم المعلوماتية والإرهابية عن طريق شبكات المعلومات وأجهزة الحاسوب.

وتؤدي هذه الفجوة المشار إليها إلى البطيء في التعاون القضائي الدولي في مجال مواكبة التطورات السريعة الحاصلة في الجريمة الإرهابية السيبرانية.

أيضاً كثيراً ما يُعيق التعاون القضائي بين الدول لمجابهة الجريمة السيبرانية، اختلاف البيئات والعادات والتقاليد والديانات والثقافات من مجتمع لآخر، وبالتالي اختلاف السياسات والنظم التشريعية

[1] **"الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها"**، مصدر سابق، ص71-72.

من مجتمع لآخر، فضلاً عن اختلاف الدول في تحديد المصطلحات وتكييفها للجريمة السيبرانية، وكل ما سبق ينعكس سلباً على إجراءات التعاون الدولي، ويُعيق من تأطير آليات التعاون القضائي المختلفة لمكافحة هذه الجريمة الخطيرة، وهنا يفلت الجناة بجرائمهم من العقاب، وتهدر حقوق ضحايا الجرائم الإلكترونية في أن يحصلوا على الإنصاف والجبر المستحقين.

لذلك فعلى كافة الدول أن تأخذ بعين الاعتبار التداعيات السلبية التي تنشأ عن القصور التشريعي في مجال مجابهة هذا النوع من الجرائم الخطيرة، وتُبادر من فورها بتجريم الأفعال الإرهابية السيبرانية عن طريق إصدار التشريعات الوطنية الملائمة، والتشريعات العقابية التي تسد الباب على محاولات مرتكبي هذه الجرائم الإفلات من العقاب، فضلاً عن المراجعة وإعادة النظر في التشريعات المختلفة السارية في ذلك الصدد وتعديل ما تفرضه مستجدات التطور المتلاحقة والمستمرة للجرائم الإرهابية السيبرانية، والأهم من ذلك تقنين تلك التشريعات في الاتفاقيات الدولية سواء الثنائية أو المتعددة الأطراف.

إن التطور الهائل في استغلال الإرهابيين لوسائل التقنية الحديثة، ومنها بالطبع شبكات المعلومات العالمية، ما فتئ يشكل تحديات جد عويصة لجهات وهيئات الإنفاذ القانون في الأساس، فأصبح عنصر "الدولية" مضافاً أو مرادفاً لمعظم الجرائم وهذا يعني أن الآليات البطيئة للتعاون الدولي في شأن ملاحقة الجرائم الإلكترونية والإرهابية من شأنها أن تُخرج التحقيقات عن مسارها، أو يعيقها في حالات أخرى، لذلك يجب على الدول أن تتفاوض فيما بينها من أجل إبرام اتفاقيات دولية على المستوى الثنائي أو المتعدد الأطراف بغرض إرساء إطاراً تنظيمياً حاكماً لمكافحة كل أشكال الجرائم المستحدثة، وخاصة منها الجرائم الإلكترونية العابرة للحدود، ثم تستهدي وتستقي منها التشريعات الوطنية الجديدة أو تنقح تشريعاتها الموجودة بالفعل على هدي من هذه الاتفاقيات الدولية التي تم إبرامها.

من أبرز القضايا المثيرة التي تُدلل على التضارب في المصالح بين الدول فضلاً عن غياب التعاون القضائي في ملاحقة أحد المواطنين البريطانيين بارتكاب الجرائم الإرهابية السيبرانية، حيث كان المتهم اخترق أنظمة الحاسوب للجيش الأميركي، فضلاص عن وكالة الفضاء الأميركية، وبعد مرافعات ومحاولات مضنية من جانب الإدارة الأميركية لتسليمه إليها لمحاكمته أمام القضاء الأميركي، رفضت المملكة المتحدة تسليمه للولايات المتحدة، كما رفضت محاكمته أمام محاكمها.

إن الطبيعة الدولية لجرائم الإرهاب السيبراني العابر للحدود تجعل من مسائل التنازع حول اختصاص القضاء الوطني لأكثر من دولة بملاحقة الجريمة السيبرانية العابرة للحدود خاصة في الحالات، التي يعمد مرتكبيها إلى إخفاء هويتهم، حيث تحتاج المحاكم الوطنية إلى مزيد من الوقت

والتدبر للتيقن من مدى اختصاصها بملاحقة الجريمة المرتكبة من خارج إقليم دولة المحكمة التي تلاحق الجريمة ولا تكمن الصعوبة في تحديد القضاء الوطني المختص بالملاحقة لهذه الجريمة العابرة للحدود فقط، ولكن ايضاً عندما لا تكون الجريمة مشمولة في أحد تشريعات إحدى الدول التي يرتكب فيها جزء من الفعل السيبراني الإرهابي.

وتثار أيضاً إشكالية قضائية أخرى تتعلق بالولاية القضائية حين ترتكب الجريمة الإرهابية السيبرانية من جانب مواطن من إحدى الدول، لكن الجريمة استهدفت فعلاً العديد من الضحايا في دول مختلفة، وهنا تدفع كل دولة بحق بمواطنها أو مواطنيها الذين وقع عليهم ضرراً جراء ارتكاب الجريمة، وهنا نجد أن اتفاقية مجلس أوروبا بخصوص الجريمة السيبرانية التي صدرت في بودابست عام 2001، قد وضعت الحل التوافقي الذي يتمثل في قيام الدول الأطراف في الاتفاقية والتي تدفع بولايتها القضائية على ملاحقة الجريمة بالتشاور فيما بينها بغرض التوصل لأفضل محكمة تختص بالنظر في الدعوى.

واقع الأمر، أفضت الجرائم المنظمة عبر الوطنية "الجرائم الذكية" والجرائم الإرهابية السيبرانية المتنامية، بانتشارها الدولي المتسارع والمتراكمة بأضرارها في أكثر من دولة، إلى إنشاء إشكاليات في تجريمها أو معرفة مرتكبيها لصعوبة الاستهداء إلى أماكنهم لطبيعة جرائمهم التي ترتكب عن بعد بفعل الثورة العلمية المعاصرة، فقد افضى استعمال التكنولوجيا والفضاء السيبراني إلى تجهيل المكان والزمان للجرم المرتكب، وتأخر انكشاف الضرر في دولة أو أكثر، إضافة إلى غموض الأفعال وصعوبات التعرف على الجاني أو الجناة الفعليين المنفذين والمشاركين والمساهمين في هذه الجرائم.

وبالنظر إلى ما سبق بيانه من صعوبة تحديد الولاية القضائية في ملاحقة الجريمة السيبرانية، والتي تنشأ عن التنازع في الاختصاص الولائي لدولتين أو عدة دول وأحياناً لا ينعقد أي اختصاص ولائي في بعض الحالات، فقد بادر مجلس أوروبا بتدشين عديد الجهود في ذلك الصدد بغرض رئيسي يتمثل في مكافحة الجريمة السيبرانية الإرهابية وسد أية ثغرات تمكن مرتكبيها من الإفلات من العقاب والذي قد ينشأ نتيجة التنازع في الاختصاص القضائي بين الدول الأعضاء في منظمة مجلس أوروبا.

فالاتفاقية المشار إليها سالفاً، تعدّ أول اتفاقية دولية في مجال مكافحة الجرائم الإلكترونية، حيث تقوم بتنسيق التشريعات الوطنية لدول المجلس في ذلك السياق وتحسين تقنيات التحريات الجنائية حول مرتكبي الجريمة الإلكترونية، وتوطيد التعاون بين دول مجلس أوروبا في مجال المكافحة لهذه الجريمة، وتم إقرار الاتفاقية في ستراسبورغ – فرنسا، في الجلسة التاسعة بعد المائة في 9 نوفمبر عام 2001، وتبرز أهمية الاتفاقية من عدة وجوه أهمها: تحديد المفاهيم والمصطلحات القانونية

الأساسية والتي تساعد في إنفاذ التعاون القضائي بين الدول أطراف هذه الاتفاقية، مثل مصطلح "بيانات الحاسوب" ومصطلح "سير البيانات" على سبيل المثال.

وتهدف الاتفاقية الدولية لمجلس أوروبا إلى مكافحة الجرائم التي ترتكب من خلال الإنترنت وشبكات الحاسوب الأخرى، وتتناول الاتفاقية بشكل خاص انتهاك حقوق النشر والتأليف، وجرائم الاحتيال الإلكتروني، والاستغلال المنافي للأطفال، وتعدّ الاتفاقية مثلاً يحتذي به في عدة مجالات في مجال مكافحة الإرهاب السيبراني بشكل خاص، ولا يتسع المجال لحصر الآليات العديدة التي استحدثتها الاتفاقية[1].

الفرع الخامس: التعاون القضائي في مكافحة هذه الجريمة

يعتبر التعاون القضائي الدولي في المجال الجنائي بشكل عام أحد مظاهر التقدم الحضاري، فإذا كانت الغاية الأساسية للتضامن بين الدول في المجال السياسي هو حفظ السلم والأمن الدوليين، فإن هذا التضامن في المجال الجنائي يقتضي ضرورة تعاون الدول في مكافحة الإجرام وبصفة خاصة الإجرام الحديث المعلوماتي بما فيه ذلك الإجرام الواقع على التجارة الإلكترونية بشكل خاص، وذلك من خلال البحث عن المجرمين وملاحقتهم والقبض عليهم وتنفيذ العقوبات المحكوم بها عليهم، والاعتداد بالأحكام الصادرة ضدهم في غير الدولة الموجودين على إقليمها، لا سيما وأن فكرة السيادة الدولية لم تعد تتنافر مع الحدود والقيود التي يقتضيها التعاون السياسي والاجتماعي بين الدول، بالإضافة إلى التعاون الدولي القانوني والقضائي.

ومن جهة أخرى، يلعب التعاون الدولي في مكافحة الجريمة – بمفهومه الواسع – دوراً مهماً في مجال الوقاية من الجريمة، كونها الغاية الأساسية للسياسة الجنائية الحديثة، حيث تبلورت سياسة الوقاية من الجريمة على الصعيد الدولي بصورة واضحة من خلال جهود المنظمات الدولية والإقليمية وأعمال المؤتمرات الدولية لمنع الجريمة ومعاملة المجرمين. ويتخذ التعاون بين الدول في هذه الحالة صورة التعاون الدولي الأمني أو الشرطي في مكافحة الإجرام، لا سيما الجرائم المعلوماتية ذات الطابع العالمي، من خلال تبادل المعلومات فيما بين أجهزة الشرطة في الدول المعنية، وخلق قنوات اتصال لهذا التعاون بين الدول كإنشاء المنظمة الدولية للشرطة الجنائية (الإنتربول) والأجهزة الشرطية الإقليمية (كنظام الإيروبول في أوروبا).

كما أن التعاون الدولي يلعب في مكافحة الجريمة دوراً أساسياً في مجال الحد من الآثار الضارة التي تترتب على الجريمة المعلوماتية، متى وقعت بالفعل، ويتخذ التعاون بين الدول في

[1] www.skynewsarabia.com

المجال الجنائي في هذه الحالة صورة المساعدات القانونية المتبادلة بين الدول في المجال الجنائي، والتي تهدف إلى الكشف عن الجريمة وملاحقة مرتكبيها من الفاعلين والشركاء ومواجهة ما ترتب عليها من آثار، من خلال تبادل المعلومات والأدلة والمستندات وسماع الشهود والخبراء، وفحص الأشياء والإنابات القضائية الدولية، والتعاون الدولي لأغراض مصادرة الأموال المتحصلة من الجريمة، وصولاً إلى التعاون الدولي في تنفيذ الأحكام الجنائية الدولية.

كما تتجلى أهمية التعاون الدولي القضائي بما فيه الاعتراف بحجية الأحكام الجنائية الأجنبية بحسبانه إحدى الصور التي تساهم في مكافحة الإجرام، حيث يسهم التعاون الدولي في تنفيذ الأحكام الأجنبية في خلق نوع من التقارب بين التشريعات الجنائية الوطنية، لا سيما في مجال تحديد الأفعال محل التجريم والعقوبات التي توقع على مرتكب هذه الأفعال على نحو يجعل الحديث عن – توحيد القانون الجنائي أو عالمية القانون الجنائي – أمراً قابلاً للتحقيق وليس ضرباً من ضروب الخيال.

وكمثال على المبادرة الأخيرة لمكافحة إساءة استخدام الحاسب الآلي، وهي تحالف تم تشكيله في ناير من عام 2001 فيما بين تسعة عشر من أكبر شركات تكنولوجيا المعلومات، وتحالف – تكنولوجيا المعلومات، ومركز مشاركة وتحليل المعلومات (ITISAC) مدعوم من جانب حكومة الولايات المتحدة وتسعى للتأكد من التحديد السريع للتهديدات الأمنية التي تتطلب بنية تحتية معلوماتية مثل الإنترنت وذلك لتقديم النصائح المتبادلة حول الحلول الفعالة.

ونخلص من ذلك إلى أنه يجب على المشرع العربي بشكل عام والمشرع اليمني بشكل خاص أن يستفيد من تجارب كل ما سبق بيانه من منظمات إقليمية ودولية في مجال التعاون القضائي الدولي لمكافحة الجريمة الإلكترونية، والعمل على إبرام الاتفاقيات الدولية الإقليمية والثنائية للعمل على محاربة الجريمة الإلكترونية، وتبادل المعلومات والبيانات التي تساعد في ضبط الجريمة والمجرم أينما كان[1].

يلعب القضاء في أي دولة دوراً هام في مواجهة حالات التعدي المؤثم الماس بمصالح المجتمع وأفراده على حد سواء وذلك من خلال تطبيق القوانين وتفسيرها بما يتفق مع الغاية من سنّها والمصالح التي تبقى حمايتها، فمن الرؤى البعيدة تصور أن يكون للقضاء دوراً وقائياً مشابهاً لدور الشرطة في مكافحة الجرائم، إلا أنه في الواقع يلعب دوراً هاماً في ردع كل من تسوّل له نفسه في الاعتداء على المصالح الاجتماعية والاقتصادية محل الحماية القانونية.

[1] المحامي الدكتور مفيد عبد الجليل الصلاحي، **"التعاون القضائي الدولي..."**، 2018، الإنترنت: www.m.facebook.com

لا شك أن القاضي الجنائي يلعب دوراً هام من خلال دوره في محو التقدم التقني وما ينتج عنه باعتباره متفهم جيداً لدوره ولما يملكه من سلطة أوسع من نظيره في القضاء المدني، حيث أن الحماية القانونية لن تأتي إلا من خلال قاضي قادراً على إدراك ذلك، وخاصة مع صدور قوانين خاصة تتطلب الإلمام ببعض المعرفة الفنية وأنظمتها، وما يستخدم في هذا المجال.

تكمن الصعوبة في الجرائم التي يستخدم فيها الحاسب في مسألتين هامتين تتمثل الأولى، في تقيين أدلة الجريمة بواسطة قاضي جنائي في ضوء أنظمة الإثبات السائدة. والثانية، تتمثل في التكييف القانوني للأفعال المستحدثة بواسطة التشريعات التجريمية الحديثة والخاصة بهذه الجرائم والتي تختلف كثيراً عن نظيرتها في المجال التقليدي.

1- <u>التعاون القضائي الرسمي بين الدول</u>

توصي دراسة الأمم المتحدة بضرورة إيجاد آليات رسمية وغير رسمية للتعاون القضائي بين الدول، إما بموجب اتفاقيات دولية أو ثنائية، أو بموجب القانون الوطني، أو وفق مبدأ المعاملة بالمثل، وذلك تفادياً للتعرض لسيادة الدول. إذ قد يكون من الضروري تمكين الدول من القيام بأعمال تحقيق في أراضي دول أخرى، باعتبار أن 50 في المائة من الدول المستفتاة أفادت بأن أكثر من 50 في المائة من الجرائم السيبرانية تتضمن عنصراً دولياً. ويبدو أن الآليات الرسمية للتعاون هي الطاغية، إلا أنها تتطلب وقتاً قد يصل إلى عدة أشهر في حالة استرداد المجرمين. كما يمكن الاستفادة من خدمة "7/24" للتعاون بين الدول بواسطة مكاتب الإنتربول الموجودة فيها.

ووفقاً لدراسة الأمم المتحدة تشكل الآليات الرسمية 70 في المائة من تبادلات التعاون واستناداً إلى اتفاقيات ثنائية في أغلب الأحيان (60 في المائة من الحالات)، في حين تشكل حالات استعمال خدمة "7/24" 6 في المائة.

وإضافة إلى التعاون في مجال التحقيقات القضائية، يهدف التعاون الدولي أيضاً إلى تبادل المعلومات والدروس المستفادة من التجارب والممارسات الفضلى في دول أخرى لرفع مستوى الأمن السيبراني في الدولة.

وقد أنشأت اتفاقية بودابست شبكة تعاون "7/24"، وكذلك فعلت مجموعة الدول الصناعية G8. وتجدر الإشارة إلى اتفاقية الأمم المتحدة حول الجريمة المنظمة العابرة للدول وبروتوكولاتها الثلاثة التي تتضمن آليات للتعاون، وهي غير مخصّصة للجرائم السيبرانية، ولكنها قابلة للتطبيق في هذا السياق على الجرائم التي ترتكبها مجموعات منظمة، وتكون داخلة ضمن نطاق الاتفاقية.

2- التعاون القضائي غير الرسمي بين الدول

أما في نطاق الآليات غير الرسمية للتعاون، فيجري عادة تعيين نقطة اتصال من كل جهة، ويتم الاتصال مباشرة بين وحدات الشرطة لتبادل المعلومات والمستندات، ولتحديد أماكن وجود المتهمين والشهود، ولإجراء المقابلات. ويُتبع الإجراء غير الرسمي بإجراء آخر أكثر رسمية؛ وهذا ما تنص عليه اتفاقية بودابست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات من حيث إجراء المراسلة غير الرسمية التي تتبع بتأكيد رسمي[1].

ويشكل التعاون غير الرسمي مباشرة بين أجهزة الشرطة 9 في المائة، في حين يشكل الاتصال المباشر مع مزوّد خدمات الشبكة 8 في المائة. غير أن طلبات التعاون والاسترداد قد أكدت رسمياً وفق ما أفادت به الدول المستفتاة، والتي استعمل بعضها (50 في المائة) البريد الإلكتروني أو الفاكس أو الأنظمة المعلوماتية على الخط (5 في المائة) في هذه الطلبات. وقد أفادت 70 في المائة من دول آسيا أن التعاون غير الرسمي ممكن لديها عن طريق اتفاقيات ثنائية أو إقليمية أو عن طريق الإنتربول أو شبكات التعاون القائمة.

إن الهدف الأساسي من آليات التعاون غير الرسمية هو تفادي البيروقراطية وتفادي ضياع الأدلة المعلوماتية السريعة الزوال. وتخضع طلبات التعاون إلى شروط موضوعية تتعلق بتجريم الأعمال المرتكبة في مختلف الدول وهو ما يدعى بـ"التجريم المزدوج" وإلى شروط إجرائية ملائمة.

المطلب الثاني: الأُطر الأمنية

قبل البحث في موضوع الجانب الأمني للحماية من الجريمة الإلكترونية لا بدّ من الإشارة إلى صعوبات إثبات الجريمة الإلكترونية، فبخلاف ما يتصوّره كثير من الباحثين والمختصين في مجال مكافحة الجريمة الإلكترونية، فإن ظاهرة انتشار التشريعات والقوانين للحدّ من هذه الآفة أخذت في الازدياد في كثير من دول العالم. وأغلب هذه القوانين لم تأخذ في الاعتبار عند إنشائها أنّ الجريمة المعلوماتية تنشأ في بلد ليحدث أثرها في بلد آخر.

وتتعقّد المشكلة عندما يتعلق الأمر بمعلومات أو بيانات تمّ تخزينها في الخارج بواسطة شبكة الاتصال عن بعد. والقواعد التقليدية في الإثبات لا تكفي لضبط مثل هذه المعلومات بحثاً عن الأدلة وتحقيقها، فمن الصعب إجراء التفتيش للحصول على الأدلة في هذه الحالة في داخل دولة أجنبية، حيث إن هذا الإجراء يتعارض مع سيادة الدولة الأخيرة.

[1] انظر المرفق الخامس من هذه الدراسة المتعلق بنتائج الاستبيان المرسل لدول المنطقة في إطار هذه الدراسة.

ولمّا كانت أدلّة الإثبات المتحصّلة من التفتيش على نظم الحاسوب والإنترنت تحتاج إلى خبرة فنية ودراية فائقة في هذا المجال، فإن نقص خبرة سلطات جمع الاستدلالات والتحقيق والمحاكمة، قد يؤدي إلى ضياع الدليل، بل تدميره أحياناً. ويضاف إلى ذلك أن كل المعطيات ليس لها تجسيد دائم على أي دعامة؛ بمعنى أنها لا توجد مسجلة على أسطوانة صلبة أو مرنة، ولا على أي دعامة مادية منقولة أياً كانت، فقد توجد هذه المعطيات في الذاكرة الحية للحاسوب، ويتم محوها في حال عدم حفظها أو تسجيلها على أي أسطوانة، وحتى لو كانت المعطيات قد تمّ تخزينها على دعامة مادية، إلا أنه قد يكون من الصعب الدخول إليها بسبب وجود نظام معلوماتي للحماية.

وعلاوة على ذلك قد يتقاعس المجني عليه عن التبليغ عن الجرائم المعلوماتية إلى السلطات المختصة، بالإضافة لما تقدم من صعوبات ومشكلات[1].

وتقدّم أن الجرائم الإلكترونية هي (الجرائم النظيفة)؛ وذلك لصعوبة اكتشاف دليل ثبوتها؛ فلا أثر فيها لأي عنف أو دماء، وإنما مجرد أرقام وبيانات يتمّ تغييرها أو محوها من السجلات المخزونة في الحواسيب الآلية وليس لها أثر خارجي مادي[2].

الفرع الأول: الإطار الأمني المحلّي

باتت الجرائم الإلكترونية والوقاية منها أو ما يعرف "بالأمن السيبراني" أو " Cyber Security"، همّاً يقض مضاجع المسؤولين في كل دول العالم ومنها لبنان، لصلته الوثيقة ليس فقط بالأمن التقليدي وجرائم الإرهاب، بل لعلاقته بكل ما يتعلق بتكنولوجيا المعلومات والاتصالات والاقتصاد وعالم المال والمصارف، إذ بات كل فرد في المجتمع يتمتع إلى جانب هويته الوجودية التقليدية، بهوية رقمية لمجرد اتصاله بشبكة الإنترنت، ما يعني أن اقتصادات دول العالم والشؤون المالية للأفراد لا تتمتع بالضرورة بحماية كاملة، وأن احتمال الخرق يبقى وارداً والشواهد على ذلك كثيرة، وهذا ما يفتح الباب أمام خسائر اقتصادية واجتماعية فادحة.

التعريف العلمي لمكافحة الجرائم الإلكترونية أو الأمن السيبراني، يعني خلق "مجموعة وسائل تقنية وتنظيمية وإدارية يتم استعمالها لمنع استخدام غير المصرح به واستغلاله". ويمكن وضع هذه الوسائل في خانة السلاح الإستراتيجي بيد الحكومات والأفراد، لأن أمن المعلومات والإنترنت بات حاجة ملحة لا تقلّ أهمية عن الأمن الاجتماعي لأي بلد ومنها لبنان، الذي تنصب الجهود فيه لمكافحة الجرائم الإلكترونية عبر أجهزة الدولة الأمنية بمختلف مؤسساتها عبر مكتب مكافحة الجرائم

[1] المحامي الدكتور مفيد عبد الجليل الصلاحي، **"التعاون القضائي الدولي..."**، 2018.
[2] المرجع نفسه.

الإلكترونية، وزارة الاتصالات عبر دائرة الاستثمار والصيانة ومصرف لبنان المركزي عبر هيئة التحقيق الخاصة، والهدف هو بناء جدران الحماية التي تمنع الهجمات الإلكترونية وتقلل من تأثير رقابة واختراقات الحسابات وأنظمة المعلومات الحكومية والخاصة، لأن الجميع متفق على أن لهذه الهجمات تأثيراً على الأمن الوطني بمفهومه الشمولي والاقتصاد والمؤسسات المصرفية ومعلومات الدولة.

كثرت في الآونة الأخيرة الشكاوى المقدمة إلى المديرية العامة لقوى الأمن الداخلي مكتب مكافحة جرائم المعلوماتية وحماية الملكية الفكرية في لبنان من مواطنين حول تعرضهم للابتزاز من قِبل قراصنة الإنترنت الذين يقومون بإضافتهم كأصدقاء على أحد مواقع التواصل الاجتماعي (فايسبوك أو تويتر... إلخ) أو عبر تطبيقات الهواتف (واتساب، فايبر... إلخ) منتحلين صفة نساء، ثم يعملون على تصويرهم في أوضاع محرجة ويعمدون لاحقاً إلى ابتزازهم بمبالغ مالية بعد تهديدهم بنشر الصور أو الفيديوهات على الإنترنت في حال تمنّعهم عن تحويل مبلغ من المال لهم.

بين اللحاق بسرعة التكنولوجيا، والتقاعس في تطوير القوانين المترهّلة، يقف لبنان كالريشة في مهب الريح، لولا الجهود التي يقوم بها مكتب مكافحة جرائم المعلوماتية، ضمن مسؤوليته في ملاحقة الجريمة الإلكترونية. وفي وقت لا يسود العالم السيبيري في بلادنا اي قانون، ولم تتعرّف النصوص التشريعية بعد إلى عبارة "إنترنت" تطبق القوانين السارية كقانون العقوبات على جرائم السرقة والاحتيال والاعتداء الجنسي وغيرها من الجرائم التي يمكن إلباسها طابعاً تقليدياً، لكن في المقابل تجد الملاحقة القضائية صعوبة في توصيف عدد من الجرائم الخاصة بالفضاء السيبيري، مثل الدخول والبقاء غير المشروع في نظام معلوماتي، أو تشويهه وعرقلة تشغيله، أو إدخال معلومات وحذف أخرى، أو إنتاج رسوم وأشرطة مخلة بالحشمة وتسويقها واقتنائها... فيحاول القضاء الاجتهاد لسد ثغرات القانون.

الساحة اللبنانية ليست فقط متلقية للإجرام الإلكتروني، فقد ألقى مكتب مكافحة جرائم المعلوماتية في قوى الأمن الداخلي القبض أخيراً على عصابة من القراصنة اللبنانيين والفلسطينيين والسوريين، بعدما تمكنت من سرقة الأرقام السرية لعدد كبير من بطاقات الائتمان، التي سبق استخدامها في عمليات شراء عبر الإنترنت، ثم استعملتها في شراء بطاقات سفر وبضائع متنوعة، قبل إنشاء "فوروم" على الشبكة العنكبوتية لتصريف الكمية الكبيرة المتبقية لأنها عجزت عن استخدامها، مستبقة بذلك تعطيل مفعولها.

ولا تسلم المواقع الإلكترونية الرسمية والخاصة في لبنان من الهجمات الإلكترونية وبثّ الفيروسات، بحيث سيطر مجرمون قبل أشهر على عدد من المواقع دفعة واحدة، وأقفلوها طالبين من

مالكيها تحويل الأموال لإعادة تشغيلها، ومن الملفت أن القراصنة استخدموا في هجومهم حسابات كثيرة "بريئة"، وفق ما بيّنت التحقيقات، بعدما اخترقوها وسيطروا عليها وجندوها لتكوين الطاقة الإلكترونية اللازمة لتنفيذ الهجوم.

قبل البحث في موضوع الجانب الأمني للحماية من الجريمة الإلكترونية لا بدّ من الإشارة إلى صعوبات إثبات الجريمة الإلكترونية، فبخلاف ما يتصوّره كثير من الباحثين والمختصّين في مجال مكافحة الجريمة المعلوماتية، فإن ظاهرة انتشار التشريعات والقوانين للحدّ من هذه الآفة أخذت في الازدياد في كثير من دول العالم، وأغلب هذه القوانين لم تأخذ بعين الاعتبار عند إنشائها أن الجريمة الإلكترونية تنشأ في بلد ليحدث أثرها في بلد آخر.

ولفت رئيس مكتب مكافحة الجرائم المعلوماتية السابق ألبرت خوري إلى أن هناك عدم وعي لدى المواطنين في التعامل مع قضايا الأمن السيبراني، حيث أكد أن المكتب يكافح بشكل متواصل عمليات الابتزاز على الإنترنت والتي وصلت إلى 4000 قضية خلال السنة الماضية فقط.

يبرز الخطر الأكبر على الأمن السيبراني في لبنان من خلال تعرض مصرف لبنان لهجمات سيبرانية كبيرة، ما دفع المصرف إلى أخذ تدابير حماية وأصبح لديه منظومة عمل أمنية تعمل منذ أكثر من 7 سنوات، بحسب زينة عون ممثلة عن قسم الأمن السيبرالي في مصرف لبنان.

وأكد رئيس مجتمع الإنترنت في لبنان نبيل بو خالد أن هناك ثغرات كبيرة ونقص في التشريعات اللبنانية، خصوصاً فيما يرتبط بقطاع الإنترنت الذي يحتاج إلى الخصخصة من أجل تطويره.

أما قانون المعاملات الإلكترونية الذي أقر سنة 2018، فهو يعاني من ثغرات مرتبطة بمن سيدير أسماء النطاقات، إضافة إلى الكثير من الملاحظات التي تعزز انتهاك حرية التعبير والمحتوى على الإنترنت.

تحدثت وزير الدولة لشؤون التنمية الإدارية السابق عناية عز الدين أن هناك مجموعة من نقاط الضعف مرتبطة بالأمن السيبراني من بينها عدم الربط بين الإدارات والوزارات بمنظومة حماية متكاملة مما يعرض معلومات المواطنين وبياناتهم الشخصية إلى خطر. لذلك، تقوم اليوم وزارة التنمية الإدارية بمسح للإدارات والوزارات لمعرفة الواقع، لتكوين رؤية متكاملة بالأمن الرقمي وتطبيقها.

في المقابل، أشارت ممثلة وزارة العدل القاضية هانية الحلوة إلى أن هناك خلل تشريعي، إضافة إلى الخلل التقني، واعتبرت حلوة أن هناك نقص في قانون العقوبات اللبناني مقارنة مع بلدان

ككندا وفرنسا ورومانيا والمغرب لجهة تضمنته لقضايا الجرائم الإلكترونية، وبالتالي فهو بحاجة إلى تطوير.

الفرع الثاني: الإطار الأمني الدولي

لا بد أن نقف على حقيقة الصعوبات التي تواجه كافة أطراف المنظومة الأمنية والقضائية في هذا الصدد، والتي تتجلى عندما تكون الجريمة واقعة على برامج الحاسوب وبياناته أو بواسطتها، وذلك بالنظر إلى قلّة الآثار المادية التي قد تنتج عن هذا النوع من الجرائم، وكثرة عدد الأشخاص الذين قد يتردّدون على مسرح الجريمة خلال المدة الفاصلة بين وقوع الجريمة والكشف عنها[1].

وممّا تقدم نشير هنا إلى أبرز الصعوبات التي تعترض إثبات الجريمة الإلكترونية:

1. البعد الدولي: يجري النفاذ إلى أنظمة الحاسوب في أحد البلدان، ويتمّ التلاعب بالبيانات في بلد آخر، وتسجّل النتائج في بلد ثالث، ناهيك عن أنه يمكن تخزين أدلة الجريمة الإلكترونية في جهاز حاسوب موجود في بلد غير البلد الذي ارتكب فيه المجرم فعله. وبالتالي يستطيع المجرم الإلكتروني إخفاء هويّته، ونقل المواد من خلال قنوات موجودة في بلدان مختلفة[2]، في قارات مختلفة قبل الوصول إلى المرسَل إليهم، نتيجة القدرة على التنقّل إلكترونياً من شبكة إلى أخرى والنفاذ إلى قواعد البيانات في قارات مختلفة، بحيث تقع الجريمة في عدة دول وتحكمها عدة قوانين وقواعد معنية بذلك، مما يشكّل تحدياً أمام الجهات القضائية في تطبيق القانون، ويزيد من صعوبة التحقيق فيها[3].
2. مهارة التخزين الإلكتروني للمعطيات التي تجعلها غير مرئية وغير مُدرَكة بالعين المجرّدة.
3. تشفير البيانات المخزنة إلكترونياً أو المنقولة عبر شبكات الاتصال.
4. سهولة محو الأدلّة في زمن قصير.

---

[1] د. علي حسن الطوالبه، **مشروعية الدليل الإلكتروني المستمدّ من التفتيش الجنائي**، مصدر سابق، ص. 69.

[2] محمد علي العريان، **الجرائم المعلوماتية**، مصدر سابق، ص. 84.
وانظر: عبد الرحمن بحر، **معوقات التحقيق في جرائم الإنترنت "دراسة مسحيّة على ضباط الشرطة في دولة البحرين"**، أكاديمية نايف العربية للعلوم الأمنية، 1999م-1420هـ؛ رامي علي وشاح، **الصعوبات المادية التي تعترض الإثبات بالمحررات الإلكترونية**، الأكاديمية للدراسات الاجتماعية والإنسانية، 2010 (ص. 44-52)؛ بدور عبد الله الملحم، **تحديات نظام مكافحة الجرائم الإلكترونية السعودي**، مركز التميز لأمن المعلومات؛ د. ناول عبد الهادي، **تقييم فعاليات المواجهة التشريعية لجرائم الإنترنت**، مجلة العدل، العدد 31، رجب 1427.

[3] الإجراءات الوقائية والتعاون الدولي لمحاربة الجريمة الإلكترونية، ضمن أعمال الندوة الإقليمية حول "الجرائم المتصلة بالكمبيوتر"، 19-20 نيسان/يونيو 2007، المملكة المغربية، ص. 119.

لأجل هذه الصعوبة فإن إعداد رجال الضبط الجنائي وقضاة الحكم، للبحث عن أدلة الإثبات في ميدان الجرائم الإلكترونية، يكتسب أهمية بالغة؛ إذ لا بد لهم من الدراية الكافية لطبيعة هذا النوع من الجرائم الذي يتسم الكشف عنه وإثباته بصعوبات بالغة. وفي عالم "المعلوماتية وشبكات الحاسوب" القائم على تقنية الاتصالات والتوصيلات والوسائط الإلكترونية، لا تستطيع سلطة البحث والتحري والتحقيق تطبيق الإجراءات التقليدية على غالبية جرائم تقنية المعلومات. من أجل ذلك لا بد من تدريب وتهيئة رجال الضبط الجنائي والتحقيق والقضاة المختصين بجرائم تقنية المعلومات فيما يتعلق بالأساليب الفنية المستخدمة في ارتكاب الجريمة، وفيما يتعلق بالكشف عنها، والقرائن والدلائل والأدلة المستحدثة في مجال إثباتها، وكيفية معاينتها والتحفظ عليها وفحصها فنياً، مع ضرورة تدريب القضاة على معالجة هذا النوع من القضايا لتمكينهم من الفصل فيها. وتكمن الصعوبة الأساسية التي تعترض سلطات البحث والتحري في ميدان الجرائم الإلكترونية، أن مرتكبي هذه الجرائم لا يتركون في غالب الأحيان آثاراً تدل على ارتكابهم لهذه الجرائم؛ إذ تكوّن المعلومات محفوظة تحت رقم أو رمز سري أو مشفّرة كلياً، إذ يصعب الولوج إليها أو معرفتها، وبالتالي إقامة الدليل ضد هؤلاء الجناة، لذا لا بد من خلق وحدات خاصة تكون مهمتها الأساسية مراقبة وتتبّع الشبكة عن طريق الإبحار فيها، ومثل هذه المراقبة القبلية قد تعطي نتائج هامة على مستوى الحد من الجريمة قبل ارتكابها عن طريق الوقاية منها[1].

لذا فإنه للحفاظ على مسرح الجريمة لا بدّ من تحقيق ما يلي:

1- تصوير الحاسوب وما قد يتصل به من أجهزة بدقة تامة، وأخذ صورة لأجزائه الخلفية وسائر ملحقاته.

2- ملاحظة طريقة إعداد نظام الحاسوب بعناية بالغة.

3- إثبات الحالة التي تكون عليها توصيلات وكابلات الحاسوب والمتصلة بمكونات النظام.

4- عدم التسرُّع في نقل أي مادة معلوماتية من مكان وقوع الجريمة خشية إتلاف البيانات المخزنة[2].

لذا يمكننا في ضوء التعامل مع العصر الرقمي واحتياجاته التشريعية، أن نلحظ تخبّطاً في التعامل مع المتطلبات التشريعية لتقنية المعلومات، وهو أشبه بحالة التخبط التي شهدتها النظام المقارنة

[1] السيد عبد الرزاق سندالي، **التشريع المغربي في مجال الجرائم المعلوماتية**، ضمن أعمال الندوة الإقليمية حول "الجرائم المتصلة بالكمبيوتر"، 19—20 نيسان/أبريل، 2007، المملكة المغربية، ص. 71-72.

[2] وليد عكوم، **التحقيق في جرائم الحاسوب**، مصدر سابق، ص. 6.

في مطلع السبعينيات وخلال الثمانينيات. ولا تزال تشهد بعضاً من ملامحه في عدد من مسائل تقنية المعلومات في الوقت الحاضر.

وفي هذا السياق، يلمس المتابع عدم وضوح الرؤية، ويلمس اتجاه المؤسسات التشريعية في الدول النامية إلى حلول مبتورة، وليست كافية، لتدرك التحديات التقنية ذاتها، وتدرك حالة التغير والتطور في الاحتياجات القانونية لمواجهة العصر الرقمي، وتدرك أكثر أن الحلول المقتبسة دون إعادة تناغم واع ومدروس على الأقل، هي حلول معطلة وليست فاعلة لاعتبارات اجتماعية وسياسية واقتصادية وقانونية، حتى أننا لا نكون مبالغين إن قلنا إن هذه الحلول الجزئية المقتبسة تزيد التحديات ولا توفر حلولاً لها، كما أنها في بعض الأحيان تقيم مزيداً من العوائق نحو الأهداف النبيلة في خطط توظيف التقنية بدلاً من أن تذلّل هذه العوائق.

إن شيوع الحاسوب، وفي ما بعد الاتجاه نحو التشبيك عبر مختلف أنواع شبكات المعلومات وفي مقدمتها الإنترنت، وبناء شبكات وقواعد المعلومات هي أمور أفرزت حاجة ملحّة للتدخل من أجل حماية أمن المعلومات وحماية الخصوصية والتنظيم الصحيح لحماية الملكية الفكرية، ومراعاة آثارها في المجتمع، ومن أجل حماية المستهلك، والاعتراف بالحجية وملاءمة الوسائل الإلكترونية للتصرفات القانونية بنفس القدر من الملاءمة المقبولة والمعترف بها للوسائل غير الإلكترونية، إلى جانب أهمية تنظيم معايير ومقاييس التقنية وحماية المستخدم في نطاقها، وتنظيم البنى التحتية ضمن تدابير تكفل نماء توظيف التقنية بشكل صحيح وملائم لحاجات المجتمع.

إن أخطر ما يواجه فعالية نظم حماية المعلومات وفعالية الأدوات التشريعية لتنظيم استخداماتها وتطبيقاتها وصورها المعالجات الجزئية للتحديات القانونية المتصلة بتقنية المعلومات، تلك المعالجات التي يظن البعض أنها الحل القانوني الكامل في حين أنها قطعة فسيفسائية من لوحة قانون تقنية المعلومات. والأخطر أنها حلول لم تدرك عاملين رئيسيين، الأول، أننا نتحدث عن تنظيم مسائل أثيرت منذ منتصف الستينيات تقريباً، ودراسة مسيرتها التاريخية يدلّنا على اتجاهات تطورها مستقبلاً، فإن لم يدرك الماضي ولم يستشرف المستقبل أصبحنا كأننا ننظم الحاضر فقط، فإن أضفنا أنه حاضر غيرنا لا حاضرنا أصبحت المخاطر أكثر عمقاً وأكثر احتمالية للتحقق، وأصبح التدبير غير ذي أثر. والثاني، أنها مسائل تعرضت للتشوه أو على الأقل غياب المقاييس العلمية لتبيان الصواب والخطأ بشأنها، وكبديل عن إعادة التقييم الواعي من قبل الجهات المتخصصة في هذا الحقل، اعتمدنا فكرة الثقة بتقدير جهات خارجية أقل ما توصف أنها ذاتها لا تزال تعاني تحديات الصواب

والخطأ، وتجرب وتعيد التجربة، مما يعني أن ما نثق به محل شك، ولهذا يصبح التدبير ذاته محلّ شك[1].

وتظهر الدراسة التحليلية لموضوع الجريمة الإلكترونية أهمية الحاجة إلى حزمة متكاملة من التشريعات في حقل تقنية المعلومات، تمتد لتغطية عناصر أساسية أربعة:

الأوّل: الاعتراف القانوني بالمعلومات ووسائل حمايتها المدنية والجزائية في النظام القانوني، وهذا الأساس يغطي طائفة تشريعات الأمن والخصوصية والسرية وبناء قواعد البيانات، ومواقع المعلوماتية، إضافة إلى القواعد الإجرائية وقواعد الإثبات المتصلة بهذه الموضوعات وما يتعلق بمنازعاتها ودعاويها.

الثاني: التنظيم الملائم لوسائل التقنية ومعاييرها ومواصفاتها، وتغطي مساحة المسائل المتصلة بتوظيف التقنية والاستثمار والاتجار بها وتوريد الخدمات وإدامتها، إنتاجاً ونقلاً وتبادلاً، وقواعد المنافسة المشروعة في القطاع وغيرها.

الثالث: الاعتراف القانوني بصلاحية الوسائل الإلكترونية في بيئة الأعمال والخدمات والاستثمار، وهذه تتصل بالإطار القانوني للتجارة الإلكترونية والحكومة الإلكترونية والبنوك الإلكترونية والأعمال اللاسلكية.

الرابع: الاعتراف القانوني بمصالح المستهلك والمستخدم وتوفير الحماية القانونية من عيوب ومخاطر التقنية وتطبيقاتها.

هذه الأسس الأربعة تفرز عشرات التشريعات وليس تشريعاً واحداً فقط، أو تفرز تشريعاً شمولياً قادراً على تغطيتها، لأن التنظيم القانوني لتقنية المعلومات يمتد لتغطية مختلف فروع القانون المدني والجزائي والتجاري والإداري والمالي والمصرفي، وتشريعات الإجراءات والإثبات، والتشريعات المرتبطة بمختلف الخدمات وفي مقدمتها الاتصالات، وتلك الخاصة بتنظيم الإنتاج الصناعي بمختلف مسائله، وتشريعات الثقافة والإعلام، والمعايير والمقاييس، وحقوق الإنسان وغيرها. والأهم يراعي التواؤم بينها، كي لا نخلق في النظام القانوني الواحد ما يهدم أحكامه، وما يوفر ثغرات النفاذ التي تستغلّ التناقض في المعالجة والتباين في الحلول التشريعية.

وفي ما يخصّ الجانب الأمني من الحماية، كان لا بد من التدابير الموضوعية المتعين اتخاذها على المستوى الوطني، وكما يلي:

---

[1] انظر للمؤلف سلسلة المقالات الأسبوعية (كل يوم أحد) المنشورة منذ آب/أغسطس 2001 في صحيفة العرب اليوم الأردنية تحت عنوان **"تحديات العصر الرقمي"**.

- **المعايير المتعين اتباعها على المستوى الوطني measures to be taken at the national level**

لقد تضمنت اتفاقية بودابست عام 2001 أقساماً ثلاثة، الأول حول التدابير الموضوعية، والثاني حول التدابير الإجرائية، والثالث حول الاختصاص، وبهذا المطلب تكون الاتفاقية قد قدّمت الإطار القانوني للتدابير التشريعية الموضوعية والإجرائية المتعيّن اتخاذها لمواجهة جرائم الحاسوب والإنترنت.

لقد أوجدت الاتفاقية تقسيماً جديداً نسبياً بشأن جميع جرائم الحاسوب وأحكامها (القواعد الموضوعية)، وتضمّن هذا التقسيم أربع مجموعات رئيسة لجرائم الحاسوب، ومجموعة خامسة تتعلق بأحكام المساهمة والعقوبات لهذه المجموعات الأربع، ويجري تقسيم هذه المجموعات على النحو التالي:

1. المجموعة الأولى – العنوان الأول: الجرائم التي تستهدف عناصر أمن المعلومات وهي السرية والسلامة، وتوفر معطيات نظم الحاسوب، وتشمل جريمة الدخول غير القانوني مادة 2، والاعتراض غير القانوني مادة 3، والتدخل في المعطيات مادة 4، والتدخل في نظم الحاسوب مادة 5، وإساءة استخدام الأجهزة مادة 6.
2. المجموعة الثانية – العنوان الثاني: الجرائم المرتبطة بالحاسوب، وتشمل التزوير المرتبط بالحاسوب مادة 7، والاحتيال المرتبط بالحاسوب مادة 8.
3. المجموعة الثالثة – العنوان الثالث: الجرائم المرتبطة بالمحتوى. وتشمل صورة واحدة من هذه الجرائم هي جرائم دعارة الأطفال المادة 9.
4. المجموعة الرابعة – العنوان الرابع: الجرائم المرتبطة بحقّ المؤلف والحقوق المجاورة، وتشمل الجرائم الجنائية التي تعد اعتداء على المصنفات المحمية بحق المؤلف والحقوق المجاورة مادة 10.
5. المجموعة الخامسة – العنوان الخامس: المساهمة الجرمية والعقوبة، ويعالج هذا الجزء الشروع attempt والمساعدة aiding والتحريض abetting (م/11) ومسؤولية الأشخاص المعنوية dorporate liability مادة 12، ومعايير العقاب sanctions and measures مادة 13.

ويتعين الإشارة هنا إلى أن خلافاً لا ينتهي ولا يزال قائماً بشأن تقسيم طوائف جرائم الحاسوب. وبغضّ النظر عن إطار التقسيم الأكاديمي، فإن الاتفاقية وجدت من المناسب أن تضع هذه النصوص التجريمية ضمن الطوائف المتقدمة.

هذه هي الأفعال الجرمية التي أوجبت الاتفاقية على الدول الأعضاء اتخاذ التدابير التشريعية لتجريمها ومكافحتها. ويلاحظ بوجه عام أنها شملت طوائف جرائم الحاسوب المتعارف على وصفها بجرائم التقنية الاقتصادية، وكذلك جرائم الملكية الفكرية التي تستهدف المصنفات الرقمية، وكذلك ما يعرف بجرائم المحتوى الضار أو غير القانوني، أي أن الاتفاقية غطت ثلاث موجات تشريعية في حقل جرائم الحاسوب. ويلاحظ أنها لم تغطّ جرائم الخصوصية أو الاعتداء على البيانات الشخصية المخزّنة في نظم المعلومات. ومرد ذلك وجود الاتفاقية الأوروبية لحماية البيانات ووجود قواعد تشريعية للاتحاد الأوروبي ومجلس أوروبا والمفوضية الأوروبية، وكذلك لدى الدول الأعضاء في هذه المنظمات في ميدان حماية الحق في الخصوصية من مخاطر المعالجة الآلية للبيانات، وكذلك القواعد التنظيمية لانتقال البيانات عبر الحدود ومبادئ جمعها وتخزينها ومعالجتها.

وقد تناولت الاتفاقية في المادة الحادية عشرة القواعد العامة المتعلقة بالمساهمة الجنائية والعقوبة بشأن الجرائم المشار إليها في المواد من 2-10. وأوجبت على الدول الأعضاء اتخاذ تدابير تشريعية للنص على المسؤولية عن الشروع والتدخل والتحريض في ارتكاب هذه الجرائم أو ما تختاره الدولة منها، وكذلك النص على مسؤولية الأشخاص المعنوية عن الأفعال التي ترتكب لمصلحة الشخص المعنوي من قبل الشخص الطبيعي الذي يتصرف لمصلحته استناداً إلى تمثيل قانوني، أو باعتباره مناطاً به اتخاذ القرار عن الشخص القانوني، أو لأنه خاضع لسلطته بما في ذلك أفعال التحريض والتدخل والمساعدة الجنائية، وكذلك مسؤولية الأشخاص الطبيعية والمعنوية عن غياب أو تخلف الرقابة والإشراف والتحكم بتصرفات الأشخاص الطبيعيين. ووفقاً للاتفاقية يتعين أن يمتد نطاق المساءلة الجنائية للشخصين الطبيعي والمعنوي معاً. أما بالنسبة إلى العقوبات والتدابير فقد أوجبت الاتفاقية على الدول المنضمة إقرار العقوبات الملائمة والفعالة لهذه الجرائم بما فيها العقوبات المانعة للحرية بالنسبة إلى الأشخاص الطبيعيين والغرامات المالية بالنسبة إلى الأشخاص المعنوية.

الفرع الثالث: دور الإنتربول في مكافحة الجريمة الإلكترونية

في إطار حملة جديدة لتوعية العموم، يوجّه الإنتربول رسالة مفادها أن الجريمة الإلكترونية هي جريمة فعلية وأنه ينبغي حملها على محمل الجد أسوة بسائر الجرائم.

وستزود الحملة العموم بمعلومات عن أخطر التهديدات السيبرية وكيفية كشفها، وبإرشادات عامة عن الأمن السيبري من أجل المساعدة في تقليص خطر التعرض لها.

وسيستخدم الإنترول حساباته على شبكات التواصل الاجتماعي من أجل تعميم رسائل أساسية في شكل منشورات ورسوم بيانية وأشرطة فيديو. وستتناول الرسائل الجرائم الإلكترونية التالية المعتبرة تهديدات رئيسية على الصعيد العالمي:

1- التصيد الاحتيالي

2- برمجيات انتزاع الفدية

3- الابتزاز الجنسي

4- القرصنة لتعدين العملات المشفرة

5- الاحتيال بالبريد الإلكتروني المهني لتحويل الأموال

6- الاعتداءات الجنسية على الأطفال عبر الإنترنت

وستتضمن الحملة نصائح عامة بشأن الوقاية من الاعتداءات السيبرية وتوفر لعامة الناس إرشادات بسيطة وعملية عن حماية أنفسهم وأجهزتهم وحساباتهم الإلكترونية من مرتكبي الجرائم السيبرية.

قال كريغ جونز، مدير مكافحة الجريمة السيبرية في الإنتربول: "يمكن لمرتكبي الجرائم السيبرية خداع أكثر الناس إلماماً بالإنترنت، لذا يجب توخي الحذر عند الإبحار في العالم الافتراضي".

وقال السيد جونز: "يتسم عالم المجرمين السيبريين بالمرونة والقدرة على التكيف والترابط الإلكتروني والتعاون بطريقة ما كنا لنتخيلها قبل بضعة سنوات. ويجب أن تتكيف أجهزة إنفاذ القانون مع هذه البيئة الإجرامية التي لا تنفك تتغير لكي تتمكن من حماية مجتمعاتنا في المجال السيبري بشكل فعال".

وختم قائلاً: "لعل أهم رسالة على الإطلاق هي أن الجريمة الإلكترونية هي جريمة فعلية، وإذا وقعتم ضحية لها فسارعوا إلى إبلاغ الشرطة مثلما كنتم لتفعلوا لو وقعتم ضحية أي جريمة أخرى".

وتُنفّذ حملة التوعية هذه تحت مظلة مشروع الإنتربول لبناء القدرات Cyber Americas II ويمدّها برنامج الإنتربول لمكافحة الجريمة السيبرية بالخبرات اللازمة. وتموّل حكومة كندا هذا المشروع الذي أطلق في عام 2018 من أجل تعزيز القدرة على التصدي لهذه الجرائم في 35 من

البلدان المستفيدة في أمريكا اللاتينية ومنطقة البحر الكاريبي، وذلك عن طريق تقديم التدريب المتخصص لأجهزة إنفاذ القانون وتنفيذ مبادرات وقائية في هذا المجال.

وستقوم أجهزة إنفاذ القانون في مجمل منطقة الأمريكتين والعالم وكذلك الشركات الرئيسية المعنية بالأمن السيبري بتعميم رسائل الحملة باستخدام وسم #onlinecirmelsrealcrime لإيصالها إلى أوسع جمهور ممكن.

ولمواجهة التحديات التي تواجهها الشرطة في منع الجريمة السيبرية والتحقيق فيها على الصعيد العالمي، جمع مؤتمر الإنتربول – اليوروبول السابع لمكافحة الجريمة السيبرية خبراء في المجال السيبري من أجهزة إنفاذ القانون والقطاع الخاص والمنظمات الدولية والأوساط الأكاديمية، لإجراء مناقشات معمقة لآخر التهديدات والاتجاهات والاستراتيجيات السيبرية.

وفي إطار موضوع "إنفاذ القانون في مستقبل مترابط إلكترونياً"، ركّزالمؤتمر الذي استمر ثلاثة أيام 9-11 تشرين الأول/أكتوبر على التطورات الجديدة في التكنولوجيا التي يمكن أن يستغلها المجرمون، ولكنها تستخدم أيضاً لصالح الشرطة.

وشملت المواضيع الرئيسية فوائد وتحديات الذكاء الاصطناعي بالنسبة للشرطة، والآثار المحتملة لتكنولوجيا الجيل الخامس 5G، والوصول إلى الأدلة الإلكترونية عبر الحدود، والعقبات في وجه التعاون الدولي في التحقيقات المتعلقة بالجريمة الإلكترونية، وأهمية بناء القدرات السيبرية، واتجاهات تحديات العملة المشفرة، واستخدام استخبارات المصادر المفتوحة والاعتبارات المتعلقة بالخصوصية.

وفي ضوء التطور المستمر للمجرمين السيبريين وتغيير أساليب عملهم، ذكر مدير مكافحة الجريمة السيبرية في الإنتربول كريغ جونز أن نموذج العمل الشرطي التقليدي "يواجه تحديات لا سابق لها".

وفي مراسم افتتاح المؤتمر، أطلق السيد جونز حملة الإنتربول العالمية #BECareful للتوعية بالاحتيال بالبريد الإلكتروني المهني. وهذه الحملة التي ستستمر شهراً ترمي إلى إطلاع عامة الناس على هذا النوع المتفاقم من الاحتيال وتزودهم بتعليمات للبقاء في مأمن منه.

وعرض الإنتربول أيضاً خلال المؤتمر استنتاجات التقييم الأول لتهديدات الجريمة السيبرية. ويقدم التقرير تحليلاً لأحدث اتجاهات الجريمة السيبرية التي كشفت في مختلف المناطق انطلاقاً من المعلومات الواردة من البلدان الأعضاء وشركاء القطاع الخاص واستخبارات المصادر المفتوحة.

ويتمثل أحد الاتجاهات التي كشفت في التحول من استهداف الحواسيب بالبرمجيات الخبيثة إلى استهداف الأجهزة النقالة بالهجمات بسبب تزايد استخدام الأجهزة النقالة كمنصات للدفع. وإزاء تزايد حالات قرصنة حواسيب الغير لصنع عملات مشفرة (Cryptojacking)، عمّم الإنتربول أكثر من 170 تقريراً عن مكافحة الأنشطة السيبرية تضمنت توصيات عن منع هذه الأنشطة والتخفيف من تبعاتها.

وقال السيد ستيفن ولسون، رئيس المركز الأوروبي لمكافحة الجريمة السيبرية (EC3) التابع ليوروبول: "أظهر التداول مع الشركاء من أجهزة إنفاذ القانون والقطاع الخاص والأوساط الأكاديمية لمدة ثلاثة أيام ما يمكننا تحقيقه عندما نعمل معاً بتعاون وثيق، لبحث مسألة الجريمة السيبرية العالمية".

وأضاف قائلاً: "كل هذه العناصر ضرورية من أجل تعطيل أنشطة الجريمة المنظمة وتقليل التهديد الذي يمكن أن تتعرض له عبر الإنترنت الشركات والحكومات، وفي المقام الأول المواطنون الأوروبيون. إنني أتطلع إلى الانطلاق من علاقاتنا الموثوقة لتقديم رد دولي محسّن لهذا التحدي المتفاقم باستمرار".

وهذا المؤتمر الذي ضم حوالي 400 مندوب من 70 بلداً أعطى اليوروبول والإنتربول أيضاً فرصة التأكيد مجدداً على التزامهما الراسخ بمواصلة تعاونهما في مكافحة الجريمة السيبرية[1].

الفرع الرابع: المكافحة على صعيد سلطات إنفاذ القانون

لا بدّ من إعطاء أهمية لمتطلبات تطبيق القانون وتحدّياته النائية عن الإنترنت، ولا سيما في ما يتعلق بالموارد والتدريب والحاجة إلى خبرات وأدوات تحقيق جديدة، والتعاون بين جهات تطبيق القانون المحلية، ومع الشركاء الدوليين. كما أنه ينبغي القيام بحملات توعية وتدريب لجميع المعنيين بالأمان السيبراني من الرجال أو النساء، سواء في السلك القضائي أو الإجرائي والجزائي، حتى لو تلقوا دورات سابقة، وذلك لمواكبة التطور الأساليب التي يتبعها المرتكبون[2].

أكثر من 90 في المائة من البلدان المتعاونة في مجال مكافحة الجرائم السيبرانية أفادت أن معظم الجرائم السيبرانية وصلت إلى سلطات إنفاذ القانون من خلال تقارير الأفراد أو الشركات.

[1] www.interpol.int

[2] Steven Titch, Four principles for effective cybersecurity law and policy, 25 April, 2014, p.4.

وتشير نتائج استطلاع القطاع الخاص العالمي أن 80 في المائة من ضحايا جرائم الإنترنت لا يفيدون الشرطة عن الحادث. ينشأ عدم الإبلاغ عن عدم الوعي حيال عمليات الخداع وآليات الإبلاغ بالإضافة إلى حرج الضحية من الإبلاغ والشعور بالعار[1].

أما الشركات، فإن عدم التبليغ يُجنّبها إلحاق الضرر بسمعتها. وقد أبرزت السلطات في جميع مناطق العالم مبادرات لزيادة إعداد التقارير، بما فيها الخط الساخن للتقارير، حملات التوعية العامة، الاتصال بالقطاع الخاص، تعزيز توعية عناصر الشرطة وضمان تبادل المعلومات[2].

لذلك تنوي سلطات إنفاذ القانون التوجه إلى غير المبلغين عن هذه الجرائم من خلال مجموعة من التدابير بما في ذلك التوعية والإرشاد.

ويجب أن يترافق تعامل سلطات إنفاذ القانون مع جرائم الإنترنت مع استراتيجية متوسطة وطويلة الأجل تركز على أسواق الجريمة والمهندسين أو المخططين للجريمة.

إن نسبة الجرائم السيبرانية التي تمّ ضبطها من خلال التحقيقات الاستباقية لأجهزة إنفاذ القانون ما تزال ضئيلة، لكن عدداً من الدول يركز حالياً على العمليات الإستراتيجية المتخفية، وهذا الأمر يتطلب انخراط عناصر متخفّية من الشرطة، من شأنهم استهداف المجرمين من خلال مواقع التواصل الاجتماعي، غرف التحادث، خدمات التراسل الفوري وP2P، نأخذ مثلاً على ذلك طرق كشف المنحرفين الذين يروجون للأفلام والصور الإباحية للأطفال حيث يأخذ الشرطي دور الطفل ويقوم باستدراج المجرم عبر وسائل تقنية تسمح بالكشف عن أي معلومة تقنية من شأنها أن تحدد هوية المعتدي ليُصار بعدها إلى ملاحقته محلياً أو دولياً عبر قنوات التواصل الدولية.

تجدر الإشارة إلى أنه في لبنان، بوشر بمكافحة جرائم المعلوماتية على الصعيد الوطني وذلك من خلال البدء بإنشاء ما يعرف بفريق الاستجابة لطوارئ الإنترنت (CERT) على صعيد الهيئة الناظمة للاتصالات "TRA" وكذلك بالتعاون بين الـ(AUF) Agence Universitaire de la Francophonie وقوى الأمن الداخلي والجيش ووزارة الاتصالات والجامعات والشركات الخاصة وغيرها جرائم المعلوماتية و Computer forensics department في شعبة المعلومات في قوى الأمن الداخلي الذي أنشئ عام 2009 والذي كان له فضل كبير في الكشف عن العديد من العمليات الإرهابية والجرائم الهامة.

[1] Marco Gercke, cit., ed. p.98.
[2] Comprehensive Study on Cybercrime, cit.,ed. P.227

وقد أظهرت دراسة للإتحاد الأوروبي أن أكثر من نصف البلدان ذكرت أنه ما بين 50 و100 في المائة من الجرائم الإلكترونية التي واجهتها الشرطة تتسم بطابع دولي.

في الوقت نفسه، أشارت البلدان المتجاوبة أن غالبية الجرائم الإلكترونية لفتت اهتمام الشرطة من خلال تقارير الضحايا بشكل فردي، بالرغم من ذلك فإن جرائم الإنترنت تحدث على الصعيد العالمي، ولكن يفاد عنها محلياً.

قد تصل الشكاوى إلى خط ساخن لدى المركز الوطني لمكافحة الجرائم الإلكترونية أو وحدة الشرطة المتخصصة، ولكن يمكن أيضاً أن تصل إلى مكتب الشرطة البلدية أو مخافر الشرطة التي هي أكثر اعتياداً على التعامل مع الجرائم "التقليدية" مثل السطو والسرقة أو القتل. وكما الجريمة "التقليدية" كذلك ضحايا جرائم "الإنترنت" ومرتكبي الجرائم السيبرانية" على حد سواء، هم أفراد حقيقيون موجودون في مواقع جغرافية حقيقية، وكلاهما يقع ضمن اختصاص الشرطة المحلية.

ومع ذلك، يجب أن يترافق طلب الاستجابة لجرائم الإنترنت مع تحقيقات استراتيجية متوسطة وطويلة الأجل تركز على تعطيل سوق جرائم الإنترنت، وتقديم المهندسين والمخططين لهذه الشبكات الإجرامية للعدالة. إن منع أي شكل الجريمة يتطلب اتباع نهج استباقي وموجّه نحو المشكلة لحفظ الأمن، لذلك يتوجب على أجهزة الشرطة أن تعمل جنباً إلى جنب مع الشركاء الآخرين في هذا المجال على صعيد القطاعين العام والخاص لبلوغ الهدف العام من المحافظة على النظام الاجتماعي والسلامة العامة.

في هذا السياق، تطرح مسائل عديدة، منها: إعادة النظر في آليات إصدار التشريع، وإقراره، والهيئات المخولة اقتراح وإصدار القوانين والأنظمة وبرامج إعداد وتأهيل السلطات المعنية بالمكافحة والتحقيق، إضافة إلى استحداث إدارات خاصة تعالج المواضيع الإجرائية والإدارية الخاصة بقطاع المعلومات والاتصالات ومعالجة المعلومات. ويمكن إيراد بعض الأفكار في هذا المجال، مثل: التحول نحو إقرار القواعد التي تحكم تقنيات الاتصالات والمعلومات، عبر مراسيم عوض عن القوانين، وذلك لكونها، أكثر قرباً من الواقع العملي، ولا تتطلب وقتاً طويلاً، لوضعها موضع التنفيذ.

كما يجب التعاون لتعزيز الأمن، حيث لا بدّ من إيجاد الإطار التشريعي والتنظيمي الحاضن، الذي يشجّع مبادرات التعاون، إذ أن استمرارية عمل تقنيات المعلومات والاتصالات، وفي مقدّمها الإنترنت، كما استقرار الفضاء السيبراني، يستدعيان سياسات لمعالجة الثغرات الأمنية، ولمواجهة الأخطار والحدّ من آثار الأعمال الجرمية.

وبالتالي، لا بدّ من دعم الجهود الآيلة إلى وضع مقاييس ومعايير دولية، كما لا بدّ من دعم وإقرار الأطر القانونية والتنظيمية، والإفادة من أفضل الممارسات والتجارب الناجحة، التي تعزز الثقة في الفضاء السيبراني وتؤمّن بيئة داعمة لنمو النشاط الاقتصادي والاجتماعي في الفضاء السيبراني.

وفي هذا الإطار، لا بدّ من الابتعاد عن السياسات، التي تتعارض وطبيعة عمل الإنترنت المفتوحة وإمكاناتها التي تشكّل أرضية للإبداع، والنمو الاقتصادي والاجتماعي، بحيث لا تتحول هذه السياسات إلى أدوات تعيق الانسياب الحرّ للمعلومات، والوصول إليها تحت ذريعة تحقيق الأمن والحماية.

على خط موازٍ، لا بدّ لسياسات الأمن أن تعزّز المبادرات الفردية والجماعية العاملة على تحقيق الأمن والحماية. فنجاح خطط الحماية والأمن السيبراني يفرض ترابطاً وتكاملاً بين إستراتيجيّات الأمن وسياساته، كما يفترض إمكانية وصول الجمهور إليها ليس فقط على المستوى الوطني، وإنما على المستويين الإقليمي والعالمي أيضاً.

كذلك، هنالك حاجة لمشاركة الجميع، في وضع الحلول، بحيث تأتي هذه الأخيرة، ناجعة، ومؤسِّسة لتفاهم اجتماعي وسياسي، بما يعزّز فرص نجاحها وفعاليتها.

كما أنه لا بدّ لمتخذي القرار أن يأخذوا مقترحات القطاعات المهنية والاختصاصيين والمجتمع المدني وغيرهم بعين الاعتبار لدى صياغة التشريعات ووضع الأطر التنظيمية.

أيضاً، يجب تطوير البنية الإدارية، فالثقة في الفضاء السيبراني ترتبط بقدرة الأجهزة المعنية على ضبط الأمور كما ترتبط بوضوح المسؤوليات والمرجعيات المعنية بإقرار الحقوق وحمايتها وبالقدرة على الردع والملاحقة لكل عمل جرمي أو تصرف يعرّض استقرار المعاملات والفضاء السيبراني. وتتطلب المكافحة الفاعلة، أجهزة متخصصة وعناصر تتميز بالكفاءة والقدرة على الإحاطة بجوانب كيفية إدارة أنظمة المعلومات، وطرق معالجة البيانات، والحقوق المتصلة بها. يضاف إلى ذلك، ضرورة وجود مرجعية تشرف على توثيق الحقوق وإرساء قواعد متينة للثقة في العاملين في مجال معالجة المعلومات والأنظمة المتصلة بها، كما الحقوق الناشئة عنها في سجلات خاصة ذات قيود موثقة.

يرتكز اقتصاد الإنترنت، كما نموها، بشكل أساسي، على الانسياب الحرّ للمعلومات. وإذا كانت الدول المختلفة، مدعوّة إلى وضع سياسات تعزّز هذا الانسياب، وتشجعه، وتدعمه، إلا أنها في المقابل، مدعوّة أيضاً، إلى تأمين الإطار القانوني الذي يوفّر حماية الحق في الخصوصية، والبيانات

الشخصية، والحريات الفردية، وبعض الفئات العمرية، كالأطفال والشباب، والملكية الفكرية. ومن هنا، ضرورة التفاتها إلى الأمن السيبراني، والعمل على إرساء قواعد ثابتة له.

ويتصل انسياب المعلومات، بالطبيعة المفتوحة للإنترنت، التي تتّكل بدورها، على اعتماد مقاييس ومعايير تقنية عالمية. وترد في هذا الإطار أيضاً سياسات المنافسة والسوق المفتوح والتنوع، والخدمات العابرة للحدود، التي تسمح بتأمين خدمات، بكلفة معقولة، تساهم في إتاحة الإنترنت للجميع.

إذا التفتنا إلى الجانب التقني وصعوبة تحديد المسؤوليات في بعض المسائل، لا سيما منها تلك المرتبطة بالسلامة والأمن كاختراق البرامج وسرقة البيانات وانتشار البرامج الخبيثة، وصعوبات ضبط المحتوى غير المشروع، ومتابعة التصرفات الجرمية، نجد أن بعض القوانين ذات الطبيعة التقنية، كالقانون الجوّي، والقانون البحري، قد أوجدت حلولاً تقنية طالت ليس فقط نوعية قواعدها، وإنما أيضاً مصادرها. ففي القانون الجوي، تساهم المنظمة الدولية للنقل الجوي (أياتا)، وهي تجمّع ذي طابع خاص في صناعة القانون الجوي، من خلال تولّيها القواعد الخاصة بمسؤولية الناقل، بينما أوكل أمر إعداد وتطوير الملاحق الخاصة بمعاهدة شيكاغو إلى هيئة تقنية متخصصة، هي المنظمة الدولية للطيران المدني.

أما من حيث المضمون، فقد تولّت المعاهدات الخاصة بمنع الاصطدام البحري، وضع قواعد المرور والإشارة في البحر مقرّة بسلوكيات وتدابير ذات طبيعة تقنية يعتبر الخروج عنها بمثابة خطأ معلن للمسؤولية. وعليه، ومراعاة لطبيعة الفضاء السيبراني التقنية والعالمية والدينامية، يبدو ملحاً التعاون مع الهيئات الدولية الموجودة حالياً، كالاتحاد الدولي للاتصالات، على إعداد أرضية إطار قانوني يضمن سلامة وأمن الفضاء السيبراني.

كذلك، فقد طورت العديد من قواعد المسؤولية، في مجال النقل البحري، لتنسجم مع التطورات التقنية التي تمنع المراقبة الدقيقة للبضاعة المشحونة من قِبل الناقل بسبب ظروف العمل، فلحظت آلية لإبداء التحفظات ومبادئ لإقرار صحتها وتقرير المسؤوليات ودفعها.

وعليه، ليس ما يمنع، أن تُطوَّر قواعد مسؤولية خاصة، تأخذ بعين الاعتبار جميع الأطراف المعنية بالحفاظ على استقرار الفضاء السيبراني، من قطاع خاص مسيطر على البنية التحتية، ومورّدي خدمات يتحكمون في الوصول إلى الشبكة العالمية للإنترنت، ودولة مسؤولة عن حماية أمنها القومي وأمن مواطنيها وسلامة مصالحهم، ومستخدمين للشبكة العالمية معنيون مباشرة بما

يُضخ من محتوى. كما يمكن وضع أصول عمل، تستند إلى التقنية، وأخلاقيات مهنية واجتماعية، تعتبر مخالفتها أرضية لتحديد المسؤوليات[1].

الفرع الخامس: المكافحة على صعيد التوعية والتدريب

إن الطبيعة التقنية الخاصة والمعقدة للمعلوماتية، وما تتطلبه من قواعد خاصة لحكمها، سواء على الصعيد الإجرائي أو على الصعيد الموضوعي، واللغة التقنية الخاصة التي قد يضطر القاضي لاستعمالها، تفرض إجراء دورات تدريبية خاصة للقضاة والمحققين ورجال الشرطة للتعامل مع الجرائم السيبرانية والأدلة المعلوماتية.

وبالتالي يجب رفد برامج التوعية ببرامج خاصة بتدريب القضاة ومحققي الشرطة بحيث تتضمن كيفية مباشرة التحقيقات الجزائية في الجرائم السيبرانية وفهم ماهية هذه الجرائم وكيفية جمع الأدلة المعلوماتية الجرمية حولها. ولا بد من وجود جهاز تقني مساعد للشرطة مؤلف من تقنيين يتمتعون بالكفاءة بحيث يتم تدريبهم وتجهيزهم بالبرامج والأدوات المعلوماتية الخاصة بالتحقيقات، ومنحهم الرواتب الملائمة لتجنب استقطابهم من القطاع الخاص الذي قد يغريهم برواتب أعلى.

كما ينبغي إدخال النساء والرجال سوية في البرامج التدريبية نظراً للحاجة إلى محققين من الجنسين للتعامل مع مرتكبي الجرائم السيبرانية أو مع الضحايا من الجنسين.

يجب التنويه إلى أن وجود النساء في طاقم التحقيق يسهل التعامل مع الضحايا من النساء، ففي الكثير من الدول العربية، ونظراً للعادات الاجتماعية والثقافية، قد تفضل المرأة، إذا وقعت ضحية جريمة سيبرانية، أن تبلغ عنها امرأة أخرى في الشرطة أو السلك القضائي بدلاً من تبليغ الرجال، أو قد تختار الكتمان خوفاً من التشهير وحفاظاً على السمعة الشخصية.

ومن الممارسات الفضلى في العالم، مساهمة المدعين العامين والمحققين في مجال الجرائم السيبرانية في تنبيه المشرّع إلى بعض الإشكاليات الإجرائية والموضوعية في هذا المجال، ومساعدته في صياغة القواعد القانونية الملائمة بصددها[2].

أيضاً، إن توعية وتدريب المستخدمين على المبادئ الأساسية للأمن السيبراني يجب أن تكون جزءاً أساسياً من أي استراتيجية أو مبادرة وطنية أو إقليمية لمكافحة الجرائم السيبرانية[3]. وقد تنبهت

---

[1] د. الأشقر منى جبور، مرجع سابق، ص. 24.

[2] University of Mississipi, School of Law, National Center for Justice and the Rule of law, Combating cyber crime: essential tools and effective organizational structures. A guide for policy makers and managers, http://www.olemiss.edu/depts/ncjrl/pdf/CyberCrimebooklet.pdf , p.47

[3] ITU, Marco Gercke, Understanding Cybercrime: Phenomena, Challenges and Legal Response, September 2012, p.18.

معظم الدول في العالم إلى ذلك، وهي تعمل على توعية المستخدمين بالمخاطر السيبرانية والجرائم السيبرانية وكيفية تفاديها. ويكون الهدف من التوعية والتدريب الموجه للأفراد تمكينهم من تعلم الوسائل التي تتيح لهم حماية أنفسهم في الفضاء السيبراني، ومن ثم الوقاية من الجرائم السيبرانية، وكذلك معرفة آليات المساعدة في حال الوقوع ضحية لجريمة سيبرانية وكيفية التصرف عند حدوث ذلك، والإجراءات القانونية المفروض اتخاذها من قبل المراجع الرسمية المختصة. ويساهم ممثلو القضاء ومكاتب المدعين العامين وأجهزة التحقيق في عدد من الدول في عمليات التوعية والتدريب، باعتبار أن ذلك من شأنه تغيير سلوك الأفراد والتخفيف من تأثير الجرائم السيبرانية ودعم جهود مكافحة هذه الجرائم.

لقد كان المحتالون يستعملون برامج لمسح بوّابات أجهزة الحاسوب والعثور على غير المحميّ منها أو اختراق كلمات السرّ. ومع تطور برامج مكافحة الفيروسات والتجسّس المعلوماتي وبرامج مكافحة البرمجيات الخبيثة عموماً، وازدياد فعاليتها، أصبح المعتدون يلجأون أكثر إلى ما يسمى "الهندسة الاجتماعية" للوصول إلى ضحاياهم. وهذه الطريقة ترتكز على التفاعل الإنساني عن طريق منتديات النقاش أو رسائل البريد الإلكتروني، وتهدف إلى خداع الضحية لتنزيل برامج تحكّم على حواسيبها أو فضح معلومات شخصية عنها. وهذه الطريقة غير التقنية لاستهداف الضحايا تنجح حتى في حالة الحواسيب المحميّة تقنياً.

ويمكن أيضاً اعتماد عدة وسائل لنشر الوعي حول المخاطر في الفضاء السيبراني عن طريق: البرامج التلفزيونية، والمقابلات الإعلامية، وتوزيع الكتيّبات، والمحاضرات في الجامعات والمدارس، والأفلام القصيرة، واللعب التفاعليّة، وإنشاء مواقع إلكترونيّة أو صفحات على الإنترنت أو الفيسبوك للتوعية، والرسائل النصيّة القصيرة، والمؤتمرات، والخطابات الموجهة للجمهور. ويمكن أن تتضمن هذه البرامج وصفاً لأشكال وأنواع الجرائم السيبرانية بما فيها تلك التي تستهدف النساء والأطفال.

كما ينبغي للدول العربية الاهتمام بالتوعية بمخاطر العنف ضد المرأة على الفضاء السيبراني، ويحبّذ أن تتفاعل السلطات الحكومية مع المنظمات غير الحكومية ومنظمات المجتمع المدني المعنية بشؤون المرأة لتثقيف النساء حول الجريمة الإلكترونية وآليات الحماية والأمن في الفضاء السيبراني، وذلك نظراً لكونها موضع ثقة للنساء في المجتمع، ولكونها وسيلة جيدة للوصول إلى أكبر طيف من النساء سواء في المدينة أو في الريف.

كما يمكن زيادة التوعية وبشكل خاص عند النساء، عن طريق نشر بعض التجارب أو القصص التي قامت فيها السيدات بالإبلاغ عن جرائم سيبرانية خاصة بهنّ مع ضرورة الحفاظ على

السرية والخصوصية عند سرد مثل هذه التجارب. ويمكن للدول الأقل نمواً طلب المساعدة في مجال التوعية والتجريب من الدول الأكثر نمواً، خاصة تلك التي لها مصلحة في ذلك، والاستفادة من الخبرات التي اكتسبتها في مجال التوعية.

المبحث الثاني

الإطار الإجرائي فيما يختص بهذا النوع من الجرائم

شكل استخدام التكنولوجيا حدثا هاما في تاريخ البشرية و ارتبط بشكل قوي بمختلف مجالات النشاط الإنساني حتى أصبحت أمرا ضروريا يستحيل الإستغناء عنها و مقوما أساسيا من مقومات دفع عجلة التقدم بالأمم و الحضارات و مقياسا لتقدمها ، غير أنه في المقابل اقترنت هذه التقنية بظهور أفعال غير مشروعة أصبحت تشكل ظاهرة إجرامية من نوع خاص تختلف عن الظواهر الإجرامية العادية و الكلاسيكية ، إذ قلبت العديد من المفاهيم القانونية السائدة سواء على مستوى القانون الموضوعي من حيث التجريم و العقاب بفعل ازدواجية طبيعتها بين جريمة معلوماتية محضةتستهدف الأنظمة و البيانات المعلوماتية في حد ذاتها أو كجريمة عادية مرتكبة بواسطة تقنية المعلومات كآلية من أجل التواصل و التخطيط لتنفيذ المشاريع الإجرامية ، أو على مستوى القانون الإجرائي بفعل تغلبها على القواعد المسطرية المقررة كأصل عام للبحث و ملاحقة مرتكبي الجرائم العادية و محاكمتهم[1]، مما يتعين القول معه بأن الإجرام المعلوماتي قد أحدث ثورة في فلسفة التجريم و العقاب و الإجراءات الجنائية[2].

المطلب الأول: دواعي الحماية الجنائية للمعلوماتية من الجرائم التي قد تقع عليها

إن الخصوصية هي أحد حقوق الإنسان الرئيسية التي تتعلق بكرامته وبقيم مادية ومعنوية أخرى، وقد أصبح الحق في الخصوصية واحداً من أهم حقوق الإنسان في العصر الحديث، وجرى الاعتراف بالخصوصية في ثقافات وأنظمة غالبية الدول، فجرت حمايتها في الإعلان العالمي لحقوق الإنسان، وفي غالبية اتفاقيات حقوق الإنسان الدولية والإقليمية وفي معظم الدساتير الحديثة، وحتى

[1] هشام ملاطي ، خصوصية القواعد الإجرائية للجرائم المعلوماتية-محاولة لمقاربة مدى ملائمة القانون الوطني مع المعايير الدولية- ، سلسلة ندوات محكمة الاستئناف بالرباط العدد السابع ،2014 ، ص.1012

[2] عبد الرحمان اللمتوني ،الإجرام المعلوماتي بين ثبات النص و تطور الجريمة، سلسلة ندوات محكمة الاستئناف بالرباط ، العدد السابع ،2014، ص.DOI :0008694/4810.12816

في الدول التي لم تتضمن دساتيرها أو قوانينها اعترافاً بالخصوصية، فإن المحاكم فيها قد أقرّت هذا الحق استناداً إلى الاتفاقيات الدولية التي اعترفت بهذا الحق.

ومع شيوع استخدام شبكة الإنترنت التي تشكو نقصاً فادحاً في مستوى الأمن الفعلي فيها، نتيجة أسباب متعددة أبرزها أنها كشبكة دولية لا تخضع لأية رقابة ولائية للسلطة المركزية التي تدير التبادل المعلوماتي الحاصل بين مئات الملايين من المستخدمين المنتشرين حول العالم أو تراقبه، برزت حاجة المتعاملين في شبكة الإنترنت، لا سيما الاختصاصيين منهم إلى ابتكار وسائل تكنولوجية متطورة – إلى جانب القانون تساعد على تأمين وظائف الأمن والسرية والإثبات والفعلية للكثير من البيانات الحساسة المتبادلة.

الفرع الأول: تدريب القضاء والضابطة العدلية على التحقيق في هذه الجرائم المستحدثة

1- تدريب خاص للقضاة ومحققي الشرطة:

إن الطبيعة التقنية الخاصة والمعقدة للمعلوماتية، وما تتطلبه من قواعد خاصة لحكمها، سواء على الصعيد الإجرائي أو على الصعيد الموضوعي، واللغة التقنية الخاصة التي قد يضطر القاضي لاستعمالها، تفرض إجراء دورات تدريبية خاصة للقضاة والمحققين ورجال الشرطة للتعامل مع الجرائم السيبرانية والأدلة المعلوماتية.

وبالتالي يجب رفد برامج التوعية ببرامج خاصة بتدريب القضاة ومحققي الشرطة بحيث تتضمن كيفية مباشرة التحقيقات الجزائية في الجرائم السيبرانية وفهم ماهية هذه الجرائم وكيفية جمع الأدلة المعلوماتية الجرمية حولها. ولا بد من وجود جهاز تقني مساعد للشرطة مؤلف من تقنيين يتمتعون بالكفاءة بحيث يتم تدريبهم وتجهيزهم بالبرامج والأدوات المعلوماتية الخاصة بالتحقيقات، ومنحهم الرواتب الملائمة لتجنب استقطابهم من القطاع الخاص الذي قد يغريهم برواتب أعلى.

كما ينبغي إدخال النساء والرجال سوية في البرامج التدريبية نظراً للحاجة إلى محققين من الجنسين للتعامل مع مرتكبي الجرائم السيبرانية أو مع الضحايا من الجنسين.

يجب التنويه إلى أن وجود النساء في طاقم التحقيق يسهل التعامل مع الضحايا من النساء، ففي الكثير من الدول العربية، ونظراً للعادات الاجتماعية والثقافية، قد تفضل المرأة، إذا وقعت ضحية جريمة سيبرانية، أن تبلغ عنها امرأة أخرى في الشرطة أو السلك القضائي بدلاً من تبليغ الرجال، أو قد تختار الكتمان خوفاً من التشهير وحفاظاً على السمعة الشخصية.

ومن الممارسات الفضلى في العالم، مساهمة المدعين العامين والمحققين في مجال الجرائم السيبرانية في تنبيه المشرّع إلى بعض الإشكاليات الإجرائية والموضوعية في هذا المجال، ومساعدته في صياغة القواعد القانونية الملائمة بصددها[1].

يعتبر بناء قدرات القانونين من أهم الأنشطة التي تقوم بها الدول للحفاظ على الأمان السيبراني. ويتم ذلك عبر إطلاق دورات تدريبية تخصصية للعاملين في مجال السلامة المعلوماتية ومكافحة الجرائم السيبرانية لتمكينهم من القيام بمهامهم على أكمل وجه، وتحديث معارفهم، ولا سيما مع تسارع التطور التقني وابتكارات المجرمين والمخترقين. ويهدف التدريب الموجه إلى القضاة والمحققين وإلى الرجال والنساء العاملين في الشرطة إلى بناء قدراتهم ومعارفهم لمحاربة الجرائم السيبرانية، وتدريبهم على استخدام الأدوات المعلوماتية في التحقيقات الجزائية.

وتتضمن مواضيع التدريب الموجهة إلى المحققين الإطار القانوني للجرائم والتحقيقات وضبط أو جمع الأدلة الرقمية وحفظها وتحليلها، والتحقيقات المتوفرة على الإنترنت، وضبط أجهزة الهاتف النقال وتحليلها[2]، إضافة إلى كيفية التعامل مع القضايا الحساسة وتلك المتعلقة بالعنف ضد المرأة. ويتم التدريب بواسطة متخصص بالتدريب ضمن القضاء ووحدات الشرطة، كمعهد القضاة وأكاديمية الشرطة، وبالاستعانة بخبراء محليين ودوليين.

أما الحالات الأكثر تعقيداً من الجرائم السيبرانية، أو تلك التي تستخدم تقنيات متقدمة، فتترك لوحدات متخصصة من الشرطة[3].

ومن الأهمية بمكان إدراج مواضيع الجرائم السيبرانية المتعلقة بالنوع الاجتماعي والجرائم التي تستهدف النساء بشكل خاص ضمن برامج الدورات التدريبية.

ويبين التدريب كيفية مقاربة الجرائم التقليدية ضد المرأة بجرائم سيبرانية، والآليات المطلوب اعتمادها لمعالجة هذه الجرائم، وينبغي أن تشمل حملات التوعية والتدريب جميع المعنيين بالأمان السيبراني من الرجال أو النساء، سواء في السلك القضائي أو الإجرائي أو الجزائي، حتى لو تلقوا دورات سابقة، وذلك لمواكبة التطور التقني وتطور الأساليب التي يتبعها المرتكبون.

---

[1] University of Mississipi, School of Law, National Center for Justice and the Rule of law, Combating cyber crime: essential tools and effective organizational structures. A guide for policy makers and managers, http://www.olemiss.edu/depts/ncjrl/pdf/CyberCrimebooklet.pdf , p.47

[2] United Nations Office on Drugs and Crime, UNODC, Comprehensive study on cybercrime, draft, February 2013, p. 175.

[3] Australian Government, Attorney General's Department, National Plan to Combat Cybercrime, http://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Documents/National%10Plan%20to%20Combat%20Cybercrime.pdf , p.17.

2- دورات تدريبية للتقنيين في جهاز الشرطة أو مراكز الاستجابة لطوارئ الحاسوب:

ينبغي أن تجري الدولة دورات تدريبية تخصصية دورياً للتقنيين في جهاز الشرطة أو مراكز الاستجابة لطوارئ الحاسوب، لتمكينهم من القيام بعملهم على أكمل وجه، وتحديث معارفهم في ظل التطور التقني المتسارع. وتشمل هذه الدورات المواضيع التالية:

أ. جمع الأدلة الرقمية وحفظها.

ب. التحليل المتقدم للأدلة الرقمية.

ج. اكتشاف الحوادث السيبرانية والإنذار المبكر.

د. المعالجة أو الإدارة المتقدمة للحوادث السيبرانية.

ه. كيفية إنشاء مركز للاستجابة لطوارئ الحاسوب.

و. تحليل الفيروسات وبرامج التجسس والاختراق.

ز. مكامن الضعف للبرامج.

ح. أمن الشبكات والمعلومات.

ط. أمن الإنترنت والسيناريوهات المختلفة للهجمات.

ي. كتابة البرمجيات الآمنة.

ك. الضمان المتعلق بموردي البرامج[1].

الفرع الثاني: تطوير الآليات التشريعية لتجريم الأفعال المستحدثة

من المؤكد أن إدخال أي تكنولوجيا جديدة يؤدي إلى ظهور تحديات قانونية جديدة. غير أنه من الممكن مع التطور التكنولوجي المعلوماتي تطبيق التشريعات التقليدية التي تركز على الأشياء الملموسة ضمن حدود معينة، على أن يصاحبها صياغة نصوص قانونية جديدة لتحكم مفاهيم جديدة غير ملموسة مثل البيانات والأنظمة المعلوماتية، حيث يصعب تحديد صاحب أو حائز المعلومة، ولا سيما على صعيد التجريم والاختصاص القضائي وإجراءات التحقيق والأدلة المعلوماتية. ويبدو من ردود الدول المستفتاة، ضمن دراسة الأمم المتحدة، أن بعض الجرائم السيبرانية هي مجرّمة وفق

[1] ENISA, Roadmap to provide more proactive and efficient computer Emergency Response Team training, http://www.enisa.europa.eu/activities/cert/support/exercise/roadmap-to-provide-more-proactive-and-efficient-cert-training .

النصوص العامة التقليدية، وأن هنالك جرائم سيبرانية أخرى جرى تجريمها بنصوص خاصة[1]. هذا، مع العلم أن النوع الثاني من الجرائم السيبرانية يخضع أيضاً للنصوص العامة وللنظرية العامة لقانون العقوبات في ما يتعلق بتحديد أركان الجريمة والمشتركين والمحاولة الجرمية وأسباب الدفاع المشروع وغيرها. ويبدو أن معظم الدول تحاول توسيع نطاق تطبيق تشريعاتها التقليدية لتشمل الفضاء السيبراني والجرائم السيبرانية. وعلى صعيد الدول العربية يجهد القضاء لمحاولة تطبيق نصوص قانون العقوبات التقليدي على الجرائم السيبرانية لتدارك النقص في التشريعات السيبرانية.

1- ضرورة تحديث التشريعات:

يقتضي التأكيد على أنه بغية تجريم بعض الأفعال بهدف حماية المعلومات والاتصالات في الفضاء السيبراني، يجب سن التشريعات الخاصة والواضحة قدر الإمكان، لا الاعتماد على تفسيرات ملتبسة للقانون العام[2].

ويتبين من ردود الدول المستفتاة، ضمن دراسة للأمم المتحدة، أن النصوص القانونية المتعلقة بالجرائم السيبرانية ليست مقننة ضمن نص قانوني واحد، بل مبعثرة ضمن عدة قوانين هي: قوانين العقوبات، وقوانين جرائم تكنولوجيا المعلومات، وقوانين الإجراءات الجزائية، وقوانين التنصت، وقوانين الإثبات (البيّنات)، وقوانين الاتصالات الإلكترونية، وقوانين أمن أنظمة تكنولوجيا المعلومات، والقوانين حول البيانات الشخصية وحمايتها، وقوانين المعاملات الإلكترونية، وقوانين الأمن السيبراني، والقوانين حول التعاون الدولي.

كما يتبين من ردود الدول أن العمل التشريعي موجه نحو تعزيز العمل على النواحي الأخرى للجرائم السيبرانية، غير التجريم، كالإجراءات وجمع الأدلة والتعاون الدولي. ويتبين أيضاً من الدراسة أن بعض الدول أصدرت قوانين إجرائية خاصة بجمع الأدلة المعلوماتية وحفظها وضمان مصداقيتها، في حين تطبق دول أخرى عليها ذات القوانين الإجرائية الجزائية المطبقة على الجرائم العادية[3].

ويبدو أن دولاً عديدة في العالم ما زالت تعمل على تحديث تشريعاتها في الجانب الموضوعي، وكذلك في الجانب الإجرائي، وذلك لضمان محاربة الجرائم السيبرانية. فبعض الظواهر الإجرامية ازدادت وتعاظمت الأضرار الجرمية الناتجة عنها، وأصبح من المفترض إعداد تشريعات خاصة

[1] United Nations Office on Drugs and Crime, UNODC, Comprehensive study on cybercrime, draft, February 2013, p. 51-52.
[2] Stein Schjolberg, The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva, December 2008, https://www.cybercrimelaw.net/documents/cybercrime_history.pdf, p.2.
[3] United Nations Office on Drugs and Crime, UNODC, Comprehensive study on cybercrime, draft, February 2013, p.55.

لتجريمها. وهذه الظواهر تتمثل بالبريد الواغل spam (أو غير المرغوب فيه)، وسرقة الهوية، وتجريم الأعمال التحضيرية، وليس فقط في المحاولات الجرمية والهجمات السيبرانية المنسقة والهائلة ضد البنية الأساسية الحساسة وغيرها.

وقد أضيفت إلى الجرائم السيبرانية الجرائم الخاصة بالعنف ضد المرأة والمطاردة والمضايقة على الفضاء السيبراني، وتبين الدراسات أن بعض الإجراءات المرتبطة بالجريمة السيبرانية، قد تكون أيضاً موجودة في قوانين العنف المنزلي أو قوانين التحرش بالمرأة[1].

وتضيف بعض الدول على نصوص تجريم الجرائم السيبرانية ظروفاً مشددة للعقوبة في بعض الحالات، منها: ارتكاب الفعل بقصد جلب منفعة غير مشروعة أو بقصد الإضرار بالغير، والتسبب بضرر بالغ، والتسبب بفوضى عامة، ومحو البيانات أو تعديلها، وإعاقة عمل النظام المعلوماتي أو وقف بعض وظائفه، وتسهيل أو دعم الإرهاب، وإعاقة بنية أساسية حساسة، وارتكاب الفعل من قبل مجموعة منظمة، وتزامن الفعل مع سلوك عنيف.

ويقتضي التمييز، في نطاق تحديث التشريع، بين قوانين الجرائم السيبرانية التي تركز على قمع الفعل الجرمي بعد حدوثه وبين القوانين الناظمة للفضاء السيبراني أو قوانين تخفيض المخاطر السيبرانية، وهي قوانين استباقية تهدف إلى تخفيض المخاطر السيبرانية وجعل التحقيقات الجزائية أسهل في حال وقوع أفعال جرمية، ومن الأمثلة على ذلك عمليات التصفية (الترشيح) على الإنترنت Filtering، وحماية البيانات وحفظها، والأعمال الاستباقية ضد البنية التحتية للمجرمين. وهذه الأعمال الاستباقية يجب أن تتم ضمن حدود عدم التعرض لحقوق الأفراد أو الاستخدام المفرط للقوة[2].

2- تنسيق التشريعات بين الدول:

تناط بالمؤسسات الدولية مسؤولية تنسيق التشريعات السيبرانية بين الدول، وهذا التنسيق ممكن تحقيقه بفضل الاتفاقيات الدولية والتوصيات أو الإرشادات[3] الإقليمية أو الدولية.

وتوصي دراسة للأمم المتحدة بتنسيق التشريعات السيبرانية بين الدول بغية إنهاء وجود الملاذات الآمنة للمرتكبين وضمان جمع الأدلة المعلوماتية، باعتبار أن بعض الدول تشترط التجريم المتبادل للفعل Dual criminality من أجل التعاون قضائياً[4]. وتظهر اختلافات فيما يتعلق بمعظم

[1] http://www.genderit.org/sites/default/upload/flowresearch_cnyst_legtrend_august22_I.pdf
[2] United Nations Office on Drugs and Crime, UNODC, Comprehensive study on cybercrime, draft, February 2013, p.55.
[3] Stein Schjolberg, The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva, December 2008, https://www.cybercrimelaw.net/documents/cybercrime_history.pdf, p.1.
[4] United Nations Office on Drugs and Crime, UNODC, Comprehensive study on cybercrime, draft, February 2013, p.56-60.

الجرائم السيبرانية على صعيد تقدير خطورتها، ومن ثم تحديد عقوبتها، وكذلك على صعيد العناصر المكونة لها، فمثلاً تربط بعض الدول جرم الدخول غير المشروع إلى نظام معلوماتي بإحداث ضرر أو تغيير بيانات أو بأن يتم ذلك بصورة قصدية أو احتيالية أو دون حق؛ وتربط بعض الدول جرم اعتراض البيانات بكون البيانات غير عامة أي غير مباحة للجمهور أو أن الاعتراض يجري بوسائل تقنية.

كما تثار إشكاليات قانونية بين الدول حول بعض الجرائم السيبرانية، مثل جرم إساءة استخدام تجهيزات معلوماتية، من حيث التفريق بين ما هومحاولة جرمية معاقب عليها وما هو عمل تحضيري غير معاقب عليه، ومن حيث ازدواجية استعمال التجهيزات المعلوماتية المباحة بطبيعتها في عمل مشروع أو عمل جرمي، وكذلك فيما يتعلق بتطبيق النصوص التقليدية على جريمة الاحتيال المعلوماتي إذا كانت مرتكبة من قبل المحتال ضد نظام معلوماتي وليس شخص، فإذا لم يلحظ النص هذه الفرضية، فيجب تعديله[1].

ويتبين من دراسة للأمم المتحدة أن معظم الجرائم السيبرانية المعروفة هي مجرّمة في معظم الدول، باستثناء جرائم البريد الواغل، وبدرجة أقل جرم إساءة استعمال التجهيزات المعلوماتية، والعنصرية عبر الإنترنت، وجرم استدراج الأطفال عبر الإنترنت[2]. ومن المفترض أن يؤدي التشريع إلى ضمان تطبيق تدابير فعالة للأمن السيبراني، مثل إعطاء السلطات المختصة الصلاحيات والوسائل الضرورية لتطبيق الدفاع، في الفضاء السيبراني، عن الوظائف الحيوية للمجتمع[3].

وبهدف تنسيق تشريعات الجرائم السيبرانية على مستوى المنطقة العربية، أعدّت الإسكوا الإرشاد الخاص بالجرائم السيبرانية والذي يحدد أنواع هذه الجرائم[4] والتي تمّ حصرها بـ 51 نوع (مادة)، أما الاتفاقية العربية لمكافحة جرائم تقنية المعلومات فقد حدّدت 13 جريمة عامة خاصة بتقنية المعلومات.

[1] ITU, Marco Gercke, Understanding Cybercrime: Phenomena, Challenges and Legal Response, Semptember 2012, p.217.
[2] United Nations Office on Drugs and Crime, UNODC, Comprehensive study on cybercrime, draft, February 2013, p.77.
[3] Secretariat of the Security and Defense Committee, Finland's Cyber security Strategy. http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf, p.10.
[4] http://isper.escwa.un.org/Portals/0/Cyber%20Legislation/Regional%20Harmonisation%20Project/Directives/Dir-5Cybercrimes.pdf

3- التوازن في التشريع والتنسيق مع الإجراءات التنظيمية:

لعل الإشكالية تكمن أيضاً في التوازن بين حماية الأشخاص والممتلكات والبنية الأساسية، والحاجة إلى احترام حقوق الملكية والحقوق المدنية[1]، إذ إن زيادة الرقابة على الإنترنت بغرض ضمان الأمن السيبراني يمكن أن يساء استخدامه لمراقبة الأشخاص والتعرض لخصوصياتهم. ومن أجل احترام خصوصية الأفراد، تفرض القوانين في العالم، في معرض الإجراءات الجزائية، قيوداً على بعض البيانات وفق طبيعتها وكيفية الوصول إليها، ووجوب عدم إفشائها من قبل المحققين، وتلزم، في حالة بعض الإجراءات، بالحصول على إذن قضائي، كما تحدد نطاق الإجراء في الزمان والمكان في ما يخص الأشخاص.

ويجب أن يضمن التشريع الذي يحكم أي تصرف غير مشروع على الإنترنت أن السلوكيات "على الخط" on.line تتم معالجتها بطريقة متوازية مع تلك التي تجري "خارج الخط" offline، في ظل حياد تقني، وفي ظل احترام الخصوصية والحريات الخاصة.

يجب إعطاء الأهمية لمتطلبات تطبيق القانون وتحدياته الناشئة عن الإنترنت، ولا سيما في ما يتعلق بالموارد والتدريب والحاجة إلى خبرات وأدوات تحقيق جديدة، والتعاون الخاص فيما يتعلق بسلوكيات التعامل وتطوير وسائل تقنية ملائمة والعمل على تثقيف وتوعية مستخدمي الإنترنت لمنع مخاطر النشاطات غير المشروعة على الإنترنت أو للتقليل منها[2]. وقد أوصى مؤتمر القمة العالمية لمجتمع المعلومات الدول بوضع تشريعات تضمن التحقيق وملاحقة جرائم الإنترنت، كما أوصى باتخاذ التدابير الملائمة لضمان استقرار الإنترنت وسلامتها ومحاربة الجرائم السيبرانية، في ظل احترام الخصوصية وحرية الرأي.

الفرع الثالث: الحماية الإجرائية من خلال خصوصية الملاحقة والإثبات

1- الضبط الإداري:

من خلال المنع والوقاية من هذه الجرائم، من خلال جهات متخصصة وفرض برامج الحماية وإمكانيات الوصول والذي تنتهجه بعض الدول، وكذلك مراكز الرصد والبحث الاستقصائي والتحليل

[1] Steven Titch, Four principles for effective cybersecurity law and policy, 25 April 2014, http://www.rstreet.org/2014/04/25/four-principles-for-effective-cybersecurity-law-and-policy, p.2.
[2] A working group established by the U.S. President, The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet. March 2000, Stein Schjolberg, The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva, December 2008, https://www.cybercrimelaw.net/documents/cybercrime_history.pdf, p.7.

المعلوماتي المتخصص في مجال تكنولوجيا المعلومات لتحديد مواطن الخلل ودراسة الظواهر الإجرامية المستحدثة والمتعلقة بشبكة الحاسوب والإنترنت واقتراح أنسب السبل للمواجهة المبكرة.

2- الضبط الجنائي:

والذي يتضمن الملاحقة الإجرائية من قبل سلطات الضبط القضائي لمرتكبي هذه الجرائم، وذلك من خلال إقرار قواعد إجرائية خاصة بمتابعة وملاحقة هذه الجرائم ومرتكبيها، بحيث تعطي مأموري الضبط القضائي وسلطات التحقيق الإمكانيات القانونية الإجرائية والقدرة على التحرك السريع والمواجهة من خلال تمكينهم قانونياً من خلال إقرار الإجراءات التي تمكنهم ممن ضبط هذه الجرائم.

ولعل بعض القواعد الإجرائية تذهب باتجاه الاستفادة من هذه التطورات التكنولوجية الحديثة بحيث تستخدم هذه النظم في التواصل فيما بين السلطات المختصة لتحقق السرعة في المواجهة، بحيث يتم استخدام التقنيات الحديثة في التواصل وإقرار الإجراءات والذي يتطلب معه إيجاد الكوادر المتخصص في جميع مراحل هذه الإجراءات ابتداءً من مأموري الضبط القضائي مروراً بجهات التحقيق وانتهاء بسلطة المحاكمة والعقاب.

وهناك الكثير من التحديات الإجرائية لجرائم الكمبيوتر والإنترنت والتي تواجه سلطات الضبط القضائي، وذلك كونها تتمتع بطبيعة افتراضية تجعلها متمايزة عن غيرها من الجرائم التقليدية، حيث أن هذه الجرائم لا تترك أثراً مادياً في مسرح الجريمة كغيرها من الجرائم ذات الطبيعة المادية كما أن مرتكبيها يملكون القدرة على إتلاف أو المادية كما أن مرتكبيها يملكون القدرة على إتلاف أو تشويه أو إضاعة الدليل في فترة قصيرة.

وأهم الصعوبات التي تواجه الملاحقة الإجرائية هو ما يتعلق بإجراءات التفتيش ومحله، إذ أن التفتيش في هذا النمط من الجرائم عادة ما يتم على نظم الكمبيوتر وقواعد البيانات وشبكات المعلومات، وقد تتجاوز هذه الجرائم من النظام المشتبه به إلى أنظمة أخرى مرتبطة به وفي ظل الوضع الحالي على مستوى العالم من شيوع التشبيك بين الحواسيب وانتشار الشبكات الداخلية، فإن امتداد التفتيش إلى النظم غير النظام المشبه به إنما يخلق التحديات الكبيرة في مدى قانونية الإجراء في الأصل وكذلك مساسه بحقوق الخصوصية المعلوماتية لأصحاب النظم التي يمتد إليها التفتيش.

3- <u>في الإثبات وضبط الدليل:</u>

وكذلك عملية الضبط لا تتوقف على تحريز جهاز الكمبيوتر فقد يمتد من ناحية ضبط المكونات المادية إلى مختلف أجزاء النظام التي تزداد يوماً بعد يوم، والأهم أن الضبط ينصب على

المعطيات والبيانات والبرامج المخزنة في النظام أو النظم المرتبطة بالنظام محل الاشتباه، أي على أشياء ذات طبيعة معنوية معرضة بسهولة للتغيير والإتلاف، وهذه الحقائق تثير مشكلات متعددة، منها المعايير المقبولة للضبط المعلوماتي ومعايير التحريز إضافة إلى مدى مساس إجراءات ضبط محتويات نظام ما بخصوصية صاحبه.

وهذا هو أيضاً حال الأدلة المتحصلة من التفتيش والضبط في الجرائم الإلكترونية، ذلك أن الدليل الجنائي إما يجب أن يتّصف بالوضوح والعقلانية والإقناعية والمشروعية وذلك بجانب موضوعيته وقضائيته، وكذلك هنالك ما يثار حول قواعد الاختصاص القضائي وذلك كون هذه الجرائم في كثير من الأحيان إنما هي بطبيعتها عابر للحدود ولا ترتبط بجنسيات ويرتبط بمشكلات الاختصاص وتطبيق القانون، مشكلات امتداد أنشطة الملاحقة والتحري والضبط والتفتيش خارج الحدود، وما يحتاجه ذلك إلى تعاون دولي شامل للموازنة بين موجبات المكافحة ووجوب حماية السيادة الوطنية.

وعليه فإن البعد الإجرائي لجرائم الكمبيوتر والإنترنت ينطوي على تحديات ومشكلات جمة، عناوينها الرئيسة، الحاجة إلى سرعة الكشف خشية ضياع الدليل، وخصوصية قواعد التفتيش والضبط الملائمة لهذه الجرائم، وقانونية وحجية أدلة جرائم الكمبيوتر والإنترنت، ومشكلات الاختصاص القضائي والقانون الواجب التطبيق. والحاجة إلى تعاون دولي شامل في حقل امتداد إجراءات التحقيق والملاحقة خارج الحدود والذي يجعل هذه الجرائم محل اهتمام الصعيدين الوطني والدولي.

هذا كله إنما يذهب بنا إلى ضرورة مواكبة التطورات الإجرائية والحاجة إلى الخصوصية بالإجراء وهذا كله مرتبط بشكل عام بالمشروعية الإجرائية التي يجب توافرها، وذلك كاستثناء سلبي على حرية القاضي في الاقتناع بالدليل، ذلك أن الحرية في تكوين القانعة مقيدة بالمشروعية فلا يجوز للقاضي الحكم إلا بناء على أدلة مشروعة، بحيث يتطلب إقرار قواعد إجرائية خاصة وتشكيل أجهزة الضبط القضائي المختصة قانونياً وتقنياً، بحيث تواكب القدرات المتعاظمة للإجرام الإلكتروني مع توفير كامل الإمكانات المادية والتدريبية.

ولعله من المناسب في إقرار القوانين ذات الصلة التأكيد على وجود بعض الوسائل والأدلة الإلكترونية الحديثة مثل بطاقات الصراف الآلي وبطاقات الائتمان والكمبيالة الإلكترونية، وأيضاً النص بما يقنن التوقيعات الإلكترونية والسجل الإلكتروني والبصمة الإلكترونية، وكل ما يمكن الإفادة منه في إطار تسهيل المواجهة من أجل الوصول إلى حماية النظام العام الإلكتروني، ولعل مشاريع القوانين والتي ما زالت قيد الدراسة والإقرار، يمكن أن تشكل المحاور الأساسية في توفير الغطاء

التشريعي القانوني لهذا الفضاء الإلكتروني الافتراضي، ولكن يجب أن يتم ذلك في إطار تكاملي بحيث يضمن شمولية المواجه.

الفرع الرابع: أهم الآليات الإجرائية التي أرساها المنتظم الدولي في هذه الجريمة

إذا كان البحث في مسألة قدرة القواعد الإجرائية التقليدية في ضبط الجريمة الإلكترونية أمرا صعبا فإن الصعوبة تنطلق من إعطاء مفهوم للجريمة الإلكترونية ذاتها ، لذلك يذهب معظم المهتمين إلى القول بأن الجريمة الإلكترونية باعتبارها مظهرا جديدا من مظاهر السلوك الإجرامي لا يمكن تصورها إلا من خلال ثلاث مظاهر ، إما أن تتجسد في شكل جريمة تقليدية يتم اقترافها بوسائل إلكترونية أو معلوماتية، أو في شكل استهداف للوسائل المعلوماتية ذاتها وعلى رأسها قاعدة المعطيات و البيانات أو البرامج المعلوماتية ، أو أن يتم اقتراف الجرائم العادية في بيئة إلكترونية كما هو الأمر بالنسبة لجرائم الصحافة[1]. فلقد أثارت هذه الجريمة بعض التحديات القانونية و العملية أمام الأجهزة المعنية بالبحث عن الجرائم وضبطها و خصوصا فيما يخص مباشرة إجراءات البحث و التحري التقليدية في بيئة افتراضية لا مكان فيها للأدلة المادية ، مما أظهر مدى الحاجة إلى تطوير آليات البحث بما يتلاءم و خصوصيات هذه الجرائم، وجعل مسألة ملاءمة الإجراءات الجنائية في البحث و التحري مع خصوصية الجريمة الإلكترونية تستأثر بإهتمام المشرعين في مختلف الدول.فوعيا من المنتظم الدولي بضرورة وضع إطار دولي لحل مختلف المشاكل التي أصبحت تطرحها الجريمة الإلكترونية و من بينها المشاكل الإجرائية ، عمل من خلال مختلف الصكوك الدولية من اتفاقيات و برتوكولات ذات الصلة إلى تضمين مقتضيات خاصة بالقواعد الإجرائية سواء على مستوى البحث و التحري أو ملاحقة مرتكبي الجرائم الإلكترونية أو على مستوى آليات و قواعد الاختصاص في مجال البحث عنها .

وعليه فإن الإشكال الذي يطرح في هذا الموضوع هو مدى إمكانية القول بأن ما أرساه المنتظم الدولي من آليات إجرائية خاصة قد يساعد الأجهزة المكلفة بالبحث و التحري على ضبط الجريمة الإلكترونية والتصدي لها ؟

لقد كان السبق لمبادرة لجنة الوزراء بمجلس أوروبا من خلال توصيتها الصادرة سنة 1995 تحت رقمR(95)13 في شأن المشاكل الإجرائية المرتبطة بتكنولوجيا المعلومات ، و التي تبنتها لجنة الوزراء بالدول الأعضاء بمجلس أوروبا بتاريخ 11 شتنبر من نفس السنة، و ذلك – حسب ما ورد في ديباجتها – بهدف تجنب مخاطر الأنظمة المعلوماتية و ضرورة مسايرة الأنظمة الإجرائية للدول

[1] عبد الحكيم الحكماوي ، الإثبات في الجريمة الالكترونية ، سلسلة ندوات محكمة الاستئناف بالرباط ، العدد السابع ،2014 ، ص.145

الأعضاء في جمع الأدلة الجنائية و ملاءمة الوسائل القانونية لتمكين أجهزة البحث و التحري من الكشف عن الجرائم المعلوماتية.

و قد جاءت التوصية الأوروبية رقمR(95)13 في إطار استكمال مضامين التوصيات السابقة الصادرة عن مجلس أوروبا في مجال مكافحة الجريمة الإلكترونية.

هذا و تشمل التوصية الأوروبية الخاصة بالمشاكل الجنائية المرتبطة بتكنولوجيا المعلومات على ملحق يضم سبعة محاور أساسية تهم التفتيش و الحجز، و الحراسة التقنية ، وواجبات التعاون مع السلطات المكلفة بالبحث ، و الإثبات الالكتروني ، و استعمال التشفيرات ، بالإضافة إلى مقتضيات تخص البحث و الإحصائيات و التكوين و التعاون الدولي[8]، كما أكدت هذه التوصية على ضرورة مراجعة القوانين في مجال الإجراءات الجنائية للسماح باعتراض الرسائل الإلكترونية و تجميع البيانات المتعلقة بتداول المعلومات في حالة التحريات المتعلقة بجريمة من الجرائم الخطيرة الماسة بسرية أو سلامة الإتصالات أو أنظمة الكمبيوتر.

كما نصت هذه التوصية على بعض التدابير ، التي تهم تجميع الأدلة و إلزام أي شخص بحوزته هذه الأدلة على مساعدة الأجهزة المكلفة بالبحث و التحري ، و إمكانية اعتراض البيانات أو الدخول إليها و التحفظ السريع على هذه البيانات كما نصت أيضا على ضرورة تسليم مزودي الخدمات معلومات عن المستخدم بناء على أوامر السلطات المختصة المكلفة بالبحث.

1- القواعد الإجرائية الواردة في اتفاقية بودابست:

في إطار تأكيد الإقتناع بضرورة إتباع سياسة جنائية مشتركة تهدف إلى حماية المجتمع ضد الجريمة الإلكترونية، و استكمال المبادرات التشريعية الدولية و الوطنية في هذا الصدد لاسيما فيما يخص دعم الأبحاث و الإجراءات الجنائية المتعلقة بالجرائم الإلكترونية و جعلها أكثر فاعلية ، تم اعتماد الإتفاقية المتعلقة بالجريمة الإلكترونية من طرف لجنة الوزراء بالمجلس الأوروبي بتاريخ 8 نونبر 2001، والتي رأت في إقرارها تحقيق التعاون الدولي و كبح جماح مجرمي الكمبيوتر لأغراض غير مشروعة.

فهذه الإتفاقية تهدف إلى توحيد السياسة الواجب إتباعها في مكافحة الجرائم المعلوماتية المرتكبة في الفضاء الإفتراضي و إلى التنسيق بين التشريعات الوطنية لتسهيل مكافحة الإجرام المعلوماتي، و تطبيق إجراءات تحقيق و ملاحقة تتلاءم مع الفضاء الافتراضي ووضع نظام تعاون دولي يتميز بالسرعة و الفعالية في التنفيذ.

هذا ، و قد اتخذت المقتضيات المتعلقة بالقواعد الإجرائية حيزا هاما ضمن أحكام اتفاقية بودابست ، وذلك من خلال تخصيص 22 مادة من أصل 48 مادة مكونة للإتفاقية المذكورة للقواعد الإجرائية، حيث تم التأكيد عند تحديد نطاقها على ضرورة اعتماد كل دولة طرف ما قد يلزم من تدابير تشريعية و تدابير أخرى لإقرار القواعد الإجرائية الواردة في الإتفاقية لأغراض الأبحاث و الإجراءات الجنائية.

وقد تضمنت الإتفاقية المذكورة مجموعة من القواعد الإجرائية الخاصة بالبحث و التحري من خلال المواد من 16 إلى 21 حيث يمكن إجمالها فيما يلي :

- سرعة التحفظ على بيانات الكمبيوتر المخزنة ؛
- إجبار مقدمي الخدمات على التزويد بالمعلومات المطلوبة ؛
- تفتيش و حجز بيانات الكمبيوتر المخزنة ؛
- التجميع الفوري لبيانات الكمبيوتر و إمكانية اعتراض هذه البيانات .

كما تضمنت الإتفاقية قواعد إجرائية متعلقة بالإختصاص القضائي في المادة 22 منها ضوابط سريان الإختصاص القضائي على الجريمة الإلكترونية ، مؤكدة على ضرورة اعتماد الدول الأطراف على ما يلزم من تدابير تشريعية و تدابير أخرى لإقرار الإختصاص القضائي على الجرائم الواردة في الإتفاقية ، فالمادة 22 وضعت مجموعة من المعايير و التي بمقتضاها تنسق الأطراف المتعاقدة حدود صلاحياتها المتعلقة بالجرائم الواردة في الإتفاقية ، وذلك عندما ترتكب الجريمة في إقليم الدولة أو على متن إحدى السفن التي ترفع علمها أو على متن إحدى الطائرات المسجلة بموجب قوانينها و كذا على كل جريمة مرتكبة من جانب أحد مواطنيها إذا كانت الجريمة معاقب عليها بموجب القانون الجنائي بمكان ارتكابها أو في حالة ارتكاب الجريمة خارج الإختصاص القضائي لأية دولة ، كما نصت الإتفاقية على عدم استبعاد الإختصاص الجنائي الذي ينص عليه أحد الأطراف وفقا لقانونه الوطني و مطالبة الدول الأطراف في الإتفاقية بالتشاور حول الإختصاص القضائي الأكثر ملاءمة لمحاكمة مرتكبي الجرائم الإلكترونية في حالة تعدد المطالبة من طرف الأطراف بإختصاصه القضائي حول واقعة معينة.

كما أن ما تضمنته هذه الإتفاقية من آليات في مجال التعاون بين الدول في مجال الإجراءات، حيث يمكن لإحدى الجهات أن تطلب من جهة أخرى من أن تأمر أو تفرض حماية سريعة و بطريقة مختلفة لبيانات مخزنة في نظم معلوماتية داخل حدود هذه الجهة الثانية لتسهيل عملية البحث عنها و

الوصول إليها ، فبهذه الآلية يصبح الوصول إلى البيانات المخزنة خارج الحدود ممكنا و سهلا لأي جهة تود أو تطلب ذلك.

وعليه فإنه يظهر من خلال كل هذه التدابير الإجرائية التي تضمنتها اتفاقية بودابست، أن الهدف منها إجراء تحقيقات أكثر فعالية فيما يتعلق بالجرائم الإلكترونية، كما يجب التأكيد على أن هذه التدابير الإجرائية يمكن استخدامها في مواجهة أي جريمة تستخدم فيها تكنولوجيا المعلومات و الإتصالات.

2- الآليات الإجرائية الواردة في الإتفاقيات المشتقة عن اتفاقية بودابست

بعد الوقوف عند مختلف القواعد الإجرائية التي تضمنتها اتفاقية بودابست في مجال البحث عن الجريمة الإلكترونية ، ستكون دراستنا لهذا المطلب محاولة لمعرفة مختلف الآليات الإجرائية التي تهم الجريمة الإلكترونية و التي تضمنتها مختلف المبادرات التي تلت اتفاقية بودابست ، حيث سنحاول الوقوف عند الآليات الإجرائية التي تضمنها بروتوكول ستراسبورغ ثم بعد ذلك سنتعرض للآليات الإجرائية الواردة في الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.

3- الآليات الإجرائية الواردة في بروتوكول ستراسبورغ

تم وضع هذا البروتوكول الإضافي خلال سنة 2003 بهدف تتميم مضامين اتفاقية الجريمة المعلوماتية، حيث تضمن هذا البروتوكول 17 مادة وقد ورد ضمن أحكام الفصل الثالث من البروتوكول المعنون ب" العلاقة بين الإتفاقية و هذا البروتوكول" في المادة الثامنة منه إلى أن القواعد الإجرائية المضمنة باتفاقية بودابست تطبق على الجرائم المشار إليها في البروتوكول، وذلك فيما يخص أحكام الإختصاص المشار إليها في المادة 22 من اتفاقية بودابست مع ما قد يلزم من تعديل " Mutatis mutandis "،وكذا أحكام المواد من 14 إلى 21 المتعلقة بنطاق تطبيق القواعد الإجرائية و الشروط و الضمانات المرتبطة بها و القواعد الإجرائية المتعلقة بسرعة التحفظ على بيانات الكمبيوتر المخزنة و إصدار الأوامر و تفتيش و حجز بيانات الكمبيوتر و التجميع الفوري لها.

4- الآليات الإجرائية الواردة في الإتفاقية العربية لمكافحة جرائم تقنية المعلومات

بادرت الدول العربية إلى وضع اتفاقية عربية لمكافحة الجرائم الإلكترونية وذلك في إطار مواكبة الجهود المبذولة على مستوى المنتظم الدولي، بهدف تعزيز التعاون بين الدول العربية و تدعيمه في مجال مكافحة جرائم تقنية المعلومات.

وجاءت مضامين الإتفاقية العربية المذكورة مطابقة لأحكام اتفاقية بودابست خاصة على مستوى القواعد الإجرائية ، سواء من حيث نطاق التطبيق أو طبيعة هذه القواعد ، حيث نصت على

مجموعة من القواعد الإجرائية أوجبت على الدول الأطراف ملاءمتها مع قوانينها الوطنية فيما يتعلق بالأبحاث الجنائية كتدابير التحفظ على بيانات الكمبيوتر المخزنة و كشفها و إصدار الأوامر بتسليمها، و إجراءات التفتيش على المعلومات المخزنة و حجزها و التجميع الفوري لها و اعتراض محتواها و ذلك من خلال المواد من 23 إلى 29 من الاتفاقية.

هذا وقد تناولت الإتفاقية العربية لمكافحة جرائم تقنية المعلومات ، الإختصاص من خلال المادة الثلاثون منها ، حيث نصت على التزام كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص علها في هذه الإتفاقية وذلك إذا ارتكبت الجريمة كليا أو جزئيا أو تحققت و ذلك في الحالات التالية:

أ. في إقليم الدولة الطرف ؛

ب. على متن سفينة تحمل علم الدولة الطرف ؛

ج. على متن طائرة مسجلة تحت قوانين الدولة الطرف ؛

د. من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكابها أو إذا ارتكبت خارج منطقة الاختصاص القضائي لأية دولة ؛

ه. إذا كانت الجريمة تمس أحد المصالح العليا للدولة.

فالملاحظ من خلال مقتضيات الإتفاقية العربية المتعلقة بالإختصاص القضائي على أنها لم تخرج عن الضوابط التي أقرتها اتفاقية بودابست و اعتمدت نفس ضوابط سريان الإختصاص القضائي على الجريمة الإلكترونية.

الفرع الخامس: مدى ملائمة القوانين المقارنة مع هذه الآليات الإجرائية

لا زالت القواعد الإجرائية في مجال البحث عن الجريمة الإلكترونية لم تجد لها موقعا في مختلف التشريعات العربية باستثناء بعض التشريعات التي كان لها السبق في إرساء قواعد إجرائية تتوافق وطبيعة الجريمة الإلكترونية ،حيث أن مختلف القوانين العربية ما تزال تقتصر على القواعد الإجرائية العادية في مجال البحث عن الجريمة الإلكترونية.

لذلك سنحاول الوقوف عند النماذج التي أفرَدَت بعض القواعد الإجرائية في مجال البحث عن الجريمة الالكترونية.

1- الجزائر

أصدر المشرع الجزائري القانون 09/04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال حيث أرسى قواعد إجرائية جديدة تستطيع معها أجهزة إنفاذ القانون ممارسة إجراءات خاصة تتوافق و طبيعة الجرائم الإلكترونية، إذ تضمن الفصل الثالث من هذا القانون القواعد الإجرائية الخاصة بالتفتيش و الحجز في مجال الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و ذلك وفقا للمعايير العالمية المعمول بها في هذا الشأن ، إذ خول هذا القانون لأجهزة إنفاذ القانون الدخول و التفتيش و لو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها مع إمكانية اللجوء إلى مساعدة السلطات الأجنبية المختصة من أجل الحصول على المعطيات المبحوث عنها في منظومة معلوماتية تقع في بلد أجنبي (المادة الخامسة) ، كما سمح القانون المذكور باستنساخ المعطيات محل البحث في حال تبين جدوى المعلومات المخزنة في الكشف عن الجرائم أو مرتكبيها (المادة السادسة) ،

بالإضافة إلى الإلتزامات التي ألقاها هذا القانون على مقدمي الخدمات وذلك بمساعدة السلطات العمومية في مواجهة هذه الجرائم و الكشف عن مرتكبيها و ذلك من خلال الفصل الرابع من نفس القانون، حيث فرض المشرع الجزائري من خلال المادتين 10 و 11 من قانون 09/04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها على مقدمي الخدمات حفظ المعطيات بشكل يسمح بالتعرف على الأشخاص المساهمين في إنشاء المحتويات على الانترنيت و ذلك من أجل التبليغات المحتملة للسلطات القضائية أو في حال طلب هذه الأخيرة لأجل التحريات أو المعاينات أو المتابعات القضائية للجرائم المرتكبة ، و القيام بحفظ المعطيات المتعلقة بحركة السير، منها المعطيات التي تسمح بالتعرف على مستعملي الخدمة وكذا الخصائص التقنية و تاريخ ووقت و مدة الإتصال.

كما عالج هذا القانون مسألة الإختصاص من خلال مقتضيات المادة 15 حيث نصت هذه المادة " على أنه زيادة على قواعد الإختصاص المنصوص عليها في قانون الإجراءات الجزائية ، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا و تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للإقتصاد الوطني" .

علاوة على هذه الآليات الإجرائية التي تضمنها القانون 09/04 ، فقد تضمن قانون الإجراءات الجزائي الجزائري مجموعة من الآليات الخاصة بالتحريات و التحقيقات في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال مثل الآلية المتعلقة باعتراض المراسلات (المواد من 65 مكرر 5

إلى المادة 65 مكرر 10 من قانون الإجراءات الجزائري) ، كما سمح بامتداد اختصاص الأجهزة المكلفة بالبحث و التحري إلى كامل الإقليم الوطني إذا تعلق الأمر بجريمة إلكترونية من خلال المادة 16 من قانون الإجراءات الجزائري على امتداد اختصاص ضباط الشرطة القضائية إلى كامل الإقليم الوطني إذا تعلق الأمر ببحث و معاينة لجرائم ماسة بأنظمة المعالجة الآلية للمعطيات ، و كذا من خلال ما نصت عليه المادة 37 على جواز امتداد الاختصاص المحلي للنيابة العامة إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

2- الأردن

أصدر المشرع الأردني سنة 2010 قانونا أطلق علية قانون جرائم أنظمة المعلومات ، حيث يتضمن هذا القانون 17مادة موزعة بينما هو موضوعي و ما هو إجرائي و يظهر من خلال استقراء مختلف المواد التي جاء بها قانون جرائم أنظمة المعلومات الأردني أنه خصص بعض مقتضيات المادة 12 منه للقواعد الإجرائية التي تسمح للأجهزة المكلفة بالبحث بإمكانية الدخول إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب أي من جرائم ينص عليها القانون المذكور ، كما يجوز لهم تفتيش الأجهزة و الأدوات و البرامج و الأنظمة و الوسائل التي تشير الدلائل في استخدامها لإرتكاب أي من تلك الجرائم كما أعطت الفقرة الثانية من نفس المادة المذكورة الإمكانية لأجهزة البحث لضبط الأجهزة و الأدوات و البرامج و الأنظمة و الوسائل المستخدمة لارتكاب أي من الجرائم المنصوص عليها أو يشملها القانون المذكور و التحفظ على المعلومات و البيانات المتعلقة بارتكاب أي منها.

كما تعرضت المادة16 لمسألة الإختصاص حيث أعطت الصلاحية للقضاء الأردني إذا ارتكبت أي من الجرائم التي نص عليها قانون جرائم أنظمة المعلومات باستخدام أنظمة معلومات داخل الأردن أو ألحقت إضرار بأي من مصالحها أو بأحد المقيمين فيها أو ترتبت أثار الجريمة فيها كليا أو جزئيا أو ارتكبت من أحد الأشخاص المقيمين فيها.

مدى ملاءمة بعض القوانين الأجنبية مع الآليات الإجرائية الدولية

سنحاول الوقوف عند ما أرسته بعض الدول الأجنبية من قواعد إجرائية خاصة للبحث عن الجريمة الإلكترونية، تماشيا مع ما أقرته التوصية الأوروبية لسنة 1995 و كذا اتفاقية بودابست لسنة 2001، لذلك سنكتفي ببعض نماذج من الدول الرائدة في هذا المجال و نخص بالذكر ، بلجيكا و فرنسا.

3- بلجيكا

يعد القانون البلجيكي المتعلق بالجريمة الإلكترونية الصادر بتاريخ 28 فبراير 2000 نموذجا للقوانين الرائدة في مجال مكافحة الجرائم الإلكترونية ، حيث تم تخصيص القسم الثالث بأكمله للمقتضيات الإجرائية المعدلة لقانون التحقيق الجنائي للقواعد الإجرائية للجرائم الإلكترونية.

فقد منح المشرع البلجيكي للنيابة العامة و قضاء التحقيق صلاحيات جد مهمة من قبيل نسخ المعطيات والبيانات المخزنة في حالة تعذر حجزها و اتخاذ جميع التدابير لمنع الولوج لها مع إمكانية جعلها غير ممكنة الولوج متى شكلت البيانات المخزنة جريمة أو وسيلة لارتكاب الجريمة أو ماسة بالنظام العام أو الأخلاق الحميدة أو تشكل خطرا على سلامة الأنظمة المعلوماتية أو البيانات المخزنة، و كذا أحقية قاضي التحقيق بإجراء بحث بنظام معلوماتي أو جزء منه المتواجد في مكان أخر إذا كان هذا الإجراء ضروري للوصول إلى الحقيقة أو مخافة ضياع وسائل الإثبات أو وجود خطر و كذا أخذ نسخ من البيانات إذا كانت غير موجودة على التراب البلجيكي، إذ نصت المادة 88 من قانون التحقيق البلجيكي على أنه " إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي أو جزء منه ، فإن هذا البحث يمكن أن يمتد إلى نظام معلوماتي أخر يوجد في مكان أخر غير مكان البحث الأصلي ، و يتم هذا الامتداد وفقا لضابطين:

أ. إذا كان ضروريا لكشف الحقيقة بشأن الجريمة محل البحث

ب. إذا وجدت مخاطر تتعلق بضياع الأدلة ، نظرا لسهولة عملية محو أو إتلاف أو نقل البيانات محل البحث.

كما سمح قانون التحقيق البلجيكي لقاضي التحقيق من خلال المادة 90 بأن يأمر أي شخص يفترض فيه بأن يكون على معرفة خاصة بخدمة الإتصالات و التي تكون موضوع الرصد أو الخدمات التي تسمح بحماية أو تشفير البيانات التي يتم تخزينها، و التي تمت معالجتها أو نقلها عن طريق نظام الكمبيوتر، بتوفير معلومات عن عملية من هذا النظام وكيفية الوصول إلى محتويات الإتصالات التي تم إرسالها، بطريقة مفهومة.

كما يمكن لقاضي التحقيق بتوجيه أمره لهؤلاء الأشخاص من أجل إتاحة محتوى هذه الإتصالات على الشكل الذي طلبت من أجله و تتبعها و ذلك في حدود إمكانياتهم.

4- فرنسا

كانت فرنسا [44]من الدول السباقة للتوقيع على اتفاقية بودابست وذلك بتاريخ 23 نونبر 2001 [45]، لذلك سعى المشرع الفرنسي إلى ملاءمة قانون المسطرة الجنائية مع الآليات و

القواعد الإجرائية التي جاءت بها اتفاقية بودابست في مجال البحث عن الجريمة الإلكترونية .، كان من بينها القواعد التي تسمح بالتفتيش و الحجز في البيئة الإلكترونية حيث نصت المادة 56 على أنه " في حالة ما إذا كانت الجريمة المرتكبة مما يمكن إثباته بواسطة معطيات أو وثائق معلوماتية توجد في حوزة الغير، فإنه يمكن لضابط الشرطة القضائية أن ينتقل إلى مقر هذا الأخير لإجراء تفتيش و تحرير محضر في الموضوع"، كما نصت الفقرتين الخامسة و السادسة من المادة56 أيضا على أنه " يتم حجز المعطيات والبرامج المعلوماتية الضرورية لإظهار الحقيقة بوضع الدعامات المادية المتضمنة لهذه المعلومات رهن إشارة العدالة أو بأخذ نسخ منها بحضور الأشخاص الذين حضروا التفتيش .

الفقرة الثانية من المادة1 -57 من قانون المسطرة الجنائية و التي سمحت صراحة بمباشرة بعض إجراءات البحث عن الجريمة الإلكترونية خارج الحدود الإقليمية كإمكانية تفتيش الأنظمة المعلوماتية المتصلة حتى ولو كانت متواجدة خارج إقليم الدولية ، حيث سمحت المادة المذكورة لضباط الشرطة القضائية بأن يقوموا بتفتيش الأنظمة المتصلة حتى ولو تواجدت خارج الإقليم مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية.

كما سمحت المادة 60-1 لضابط الشرطة القضائية في أن يستدعي أي شخص لسماعه، إذا تبين له أن بوسع هذا الشخص أن يمده بمعلومات حول الأفعال أو الأشياء أو الوثائق أو المستندات أو المعطيات المعلوماتية أو الأشياء المحجوزة، وأن يرغمه على الحضور في حالة امتناعه بعد إذن النيابة العامة.[50]

بالإضافة إلى بعض القواعد الإجرائية التي تضمنتها بعض القوانين الخاصة ، كما هو الحال في القانون المتعلق بحرية الإتصال لسنة 2000 الذي فرض على مزودي الخدمات من خلال المادة 43-9 بضرورة اتخاذ تدابير للحفاظ على البيانات[51].

هذه إذن كانت نظرة على بعض القوانين المقارنة و حدود ملاءمتها مع مختلف الآليات الإجرائية التي أرساها المنتظم الدولي.

يبقى أن نشير في الأخير إلى أن القواعد الإجرائية في البحث عن الجريمة الإلكترونية لم تنل حظها من الإهتمام داخل التشريع الجنائي اللبناني، فإذا كان المشرع اللبناني قد حاول وضع تشريع جنائي يعنى بتجريم مختلف الأفعال التي تشكل جرائم إلكترونية فإنه لم يخصص الجريمة الإلكترونية بأية قواعد إجرائية خاصة و تركها خاضعة للقواعد الإجرائية الواردة في قانون أصول المحاكمات الجزائية، حيث كان من المستحسن أن تأتي في إطار نص قانوني خاص .

لذلك فإننا ندعو المشرع إلى المبادرة بتخصيص الجريمة الإلكترونية بقواعد إجرائية خاصة تؤكد خصوصيتها و ذاتيتها مقارنة مع الجرائم العادية سواء على مستوى البحث أو التحري أو على مستوى الإختصاص و التعاون القضائي.

المطلب الثاني: المشكلات الإجرائية التي تثيرها الجريمة الإلكترونية

هناك مشكلات قانونية وعملية تواجه الجهود المبذولة لمكافحة الجرائم الإلكترونية على الصعيد الإجرائي، وهذه المشكلات تتعلق بضبط الجريمة وإثباتها، وبسلطات التحري والملاحقة، وأخيراً الاختصاص القضائي والقانون واجب التطبيق، وعليه سأتناول هذه المشكلات ضمن فروع ثلاثة.

الفرع الأول: المشكلات المتعلقة بضبط الجريمة الإلكترونية وإثباتها

لعل من أهم العناصر التي ترتبط بالجريمة هو مسرحها أو مكان وقوع أركانها، وهو العنصر الرئيس لضبط وتحري الجريمة وملاحقة مرتكبيها، وهذا هو الحال نفسه فيما يتعلق بالجريمة الإلكترونية، حيث أن مسرحها متوفر وحتى إن كان مختلفاً عن المسرح المادي للجريمة التقليدية كونه مسرحاً معنوياً، فتجول الشخص في الشبكة العنكبوتية يعني أن يترك آثار أقدامه وبصماته المعنوية في الموقع الذي يزوره، إذ يتم تحديد عنوانه الإلكتروني الدائم له، ويتم تحديد نوع الجهاز الذي يستخدمه والمكان الذي يدخل منه[1].

ويمكن تتبع هذه العناصر بطرق بسيطة أحياناً وبعضها متوفر للمستخدمين العاديين والتي تكشف معلومات المستخدم ويجعلها متاحة لأي شخص يود تتبع تحركات المجرم، فضلاً عن أن يقوم بذلك المتخصصون، وحتى أن جهاز المجرم الشخصي نفسه يحتفظ بملفات الكوكيز للمواقع التي دخلها.

ولكن الأمر ليس بهذا القدر من البساطة، فيما اكتشاف المجرمين البسطاء ربما بمثل هذه الطرق، أما المجرمين المتخصصين بل وحتى الهواة منهم يقومون بمحو آثارهم التي تمّ تسجيلها من خلال عدة طرق، منها: مسح ملفات الكوكيز الموجودة على أجهزتهم، وأيضاً القيام بإخفاء عناوينهم الإلكترونية الخاصة بأجهزتهم بطرق مختلفة[2].

---

[1] كامل السعيد، **"جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات"**، دراسات جنائية معمقة في القانون والفقه والقضاء المقارن، دار الثقافة للنشر والتوزيع، عمان،(2002)، ص. 46.

[2] مصعب القطاونة، مرجع سابق، ص7.

وتحاول مختلف الدول والشركات المقدمة لخدمات الإنترنت التغلب على هذه الاختراقات عبر برامج خاصة أحياناً وعبر رموز أخرى، وهذا يتطلب عند محاولة الاستفادة منه لغايات التحري تعاوناً من مزودي الخدمة، لأن هذه الرموز تخص مزود الخدمة يتعرف من خلالها على هوية المتصلين عبر خطوطهم[1].

هذا ويعتمد ضبط الجريمة وإثباتها في المقام الأول على جمع الأدلة التي حدد المشرع وسائل إثباتها على سبيل الحصر، وذلك لما فيها من مساس بحرية الأفراد وحقوقهم الأساسية، فلا يجوز أن تخرج الأدلة التي يتم تجميعها عن تلك التي اعترف لها المشرع بالقيمة القانونية، وتتمثل في وسائل الإثبات الرئيسة، وفي المعاينة، والخبرة، والتفتيش، وضبط الأشياء المتعلقة بالجريمة، أما غيرها من وسائل الإثبات كالاستجواب، والمواجهة، وسماع الشهود فهي مرحلة تالية من إجراءات التحقيق وجمع الأدلة، ولما كنا بصدد تناول الجريمة الإلكترونية وما تثيره من مشكلات إجرائية، فسنتعرض للمشكلات القانونية التي يثيرها إثبات هذه الجرائم دون غيرها من الإجراءات كالاستجواب، والمواجهة، وسماع الشهود، لأن هذه الأخيرة تتم في مواجهة البشر، أما المعاينة، والخبرة، والتفتيش فهي إجراءات فنية محلها الأشياء لا الأفراد وهو ما يهمنا في هذا الموضوع.

الفرع الثاني: الخبرة والمعاينة والتفتيش في الجرائم الإلكترونية

تعتبر كل من الخبرة والمعاينة أكبر العقبات التي تواجه الإثبات في الجرائم الإلكترونية، فالمعاينة إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد آثارها بنفسه، فيقوم بجمعها وجمع أي شيء يفيد في كشف الحقيقة، وتقتضي المعاينة إثبات حالة الأشخاص والأشياء الموجودة بمكان الجريمة، ورفع الآثار المتعلقة بها كالبصمات، والدماء، وغيرها مما يفيد التحقيق، والمعاينة تكون شخصية إذا تعلقت بشخص المجني عليه، أو مكانية إذا تعلقت بالمكان الذي تمت فيه الجريمة، ووضع الشهود والمتهم والمجني عليه، أما المعاينة العينية فهي التي تتعلق بالأشياء أو الأدوات المستخدمة في ارتكاب الجريمة، وقد يقتضي الأمر الاستعانة بخبير للتعرف على طبيعة المادة أو نوعها إذا كان ذلك يحتاج لرأي المتخصص، وفي هذه الحالة يتم إرسال هذه الأشياء إلى الخبير لنكون بصدد إجراء آخر من إجراءات التحقيق وهو الخبرة، فالخبرة هي أحد أهم وسائل جمع الأدلة، يلجأ إليها المحقق عند وجود واقعة مادية أو شيء مادي يحتاج التعرف عليه إلى حكم الخبير المتخصص، فهو يأخذ حكم الشاهد من حيث الحجية أو القوة في الإثبات[2].

---

[1] مصطفى محمد موسى، **دليل التحري عبر شبكة الإنترنت**، دار الكتب القانونية، مصر، 2005، ص. 48.

[2] عبد الفتاح حجازي، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت**، مرجع سابق، ص. 158-159.

يثور التساؤل هنا عن مدى إمكانية معاينة الجريمة الإلكترونية، فالقانون نصّ على انتقال المحقق لأي مكان ليثبت حالة الأمكنة والأشياء والأشخاص، ووجود الجريمة مادياً، فهل يكون للجريمة الإلكترونية وجود مادي يمكن للمحقق اللبناني معاينته؟ فالقانون أوجب على المحقق وضع الأشياء والأوراق التي تضبط في حرز مغلق وتربط كلما أمكن، فالحرز المغلق الذي يتم ربطه هو الإجراء العام الذي تخضع له كل الأشياء المضبوطة، وهنا نصطدم بالعقبة الأساسية أمام معاينة الجريمة الإلكترونية التي ترتكب داخل الفضاء الافتراضي، فالمحقق في هذه الحالة يتعامل مع بيئة مليئة بالنبضات الإلكترومغناطيسية والبيانات المخزنة داخل نظام معلوماتية شديدة الحساسية، ولا يتعامل مع أوراق أو أسلحة أو أشياء قابلة للربط وهو ما يؤكد القواعد الإجرائية التقليدية لتواجه سلوكاً مادياً يرتكب بواسطة آلات وأدوات قابلة للربط والتحريز.

أما السلوك الإجرامي في الجريمة الإلكترونية فهو عبارة عن بيانات مخزنة في نظام معلوماتي يتطلب إثباته انتقال محقق متخصص، حيث يتم التفتيش عن البيانات عن طريق نقل محتويات الأسطوانة الصلبة الخاصة بالجهاز، ويجب على المحقق أو ضباط الشرطة المتخصصين استخراج المعلومات التي من شأنها أن تساعد التحقيق، وأن يطلعوا زملائهم عليها، مثل القيام بالبحث في بنوك المعلومات، وفحص كل الوثائق المحفوظة، ومراسلات مرتكب الجريمة مثل الرسائل الإلكترونية، وفك شفرات الرسائل المشفرة[1]، وهو ما يحدث عندما ترتكب الجريمة عبر شبكة الإنترنت، ولكي ينجح المحققون في عملهم يجب أن يتتبعوا أثر الاتصالات منذ الحاسب المصدر إلى الحاسب أو المعدات الأخرى التي تملكها الضحية، مروراً بمؤدي الخدمة والوساطة في كل دولة، كما يقتضي ذلك أيضاً أن يعمل المحقق على الوصول إلى الملفات التاريخية التي تبين لحظات مختلف الاتصالات، من أين صدرت؟ ومن الذي يحتمل إجراؤها، بالإضافة إلى ضرورة إلمام المحقق بالحالات التي يكون عليه فيها التحفظ على الجهاز أو الاكتفاء بأخذ نسخة من الأسطوانة الصلبة للحاسب، والأوقات التي يستخدم فيها برامج استعادة المعلومات التي تم إلغاؤها[2].

فالمحقق الذي يقوم بمعاينة الجريمة الإلكترونية يجب أن يكون ملماً بمهارات هذه التقنية، أما الخبير ففي هذه الحالة يجب أن يكون ملماً بمهارات تحليل البيانات ومهارات التشفير التي تتلح له فك الرموز واستعادة البيانات الملغية[3].

ولما كانت الجرائم ترتكب عبر الشبكة الدولية، فقد نصت المادة 23 من اتفاقية بودابست على أن: "تتعاون كل الأطراف، وفقاً لنصوص هذا الفصل، على تطبيق الوسائل الدولية الملائمة بالنسبة

[1] سليمان العنزي، مرجع سابق، ص. 98-99.
[2] مصطفى موسى، مرجع سابق، ص. 143.
[3] عبدالله عبدالحكيم عبد الله، مرجع سابق، ص. 46.

للتعاون الدولي في المجال الجنائي والترتيبات التي تستند إلى تشريعات موحدة ومتبادلة، وكذلك بالنسبة للقانون المحلي على أوسع نطاق ممكن بين بعضهم البعض بغرض التحقيقات والإجراءات المتعلقة بالجرائم الجنائية للشبكات، والبيانات المعلوماتية، وكذلك بشأن الحصول على الأدلة في الشكل الإلكتروني لمثل هذه الجرائم، كما نصت المادة 30 من الاتفاقية على الكشف السريع عن البيانات المحفوظة، حيث نصت على: "أنه عند تنفيذ طلب حفظ البيانات المتعلقة بالتجارة غير المشروعة والمتعلقة باتصال خاص تطبيقاً لما هو وارد في المادة 29 فإن الطرف المساند إذا اكتشف وجود مؤدي خدمة في بلد آخر قد شارك في نقل هذا الاتصال، فإن عليه أن يكشف على وجه السرعة إلى الطرف طالب المساعدة كمية كافية من البيانات المتعلقة بالتجارة غير المشروعة حتى يمكن تحديد هوية مؤدي الخدمة هذا والطريق الذي تم الاتصال من خلاله"، كما أشارت المادة 31 من المساعدة المتعلقة بالدخول إلى البيانات المحفوظة، حيث أجازت لأي طرف أن يطلب من أي طرف آخر أن يقوم بالتفتيش أو أن يدخل بأي طريقة مشابهة وأن يضبط أو يحصل بطريقة مماثلة، وأن يكشف عن البيانات المحفوظة بواسطة شعبة المعلومات داخل النطاق المكاني لذلك الطرف والتي يدخل فيها أيضاً البيانات المحفوظة وفقاً للمادة 29 من الاتفاقية.

ويرى بعض الفقه أننا نواجه اليوم أخطر مظاهر العولمة، فالتعاون الدولي في المجال الجنائي لم يعد مقتصراً على نظام الإنتربول، فأصبح على الدولة أن تستخدم بروتوكولات موحدة لنظم التخزين والحماية المعلوماتية، كما حدث على مستوى الاتصالات الهاتفية، لأن التعاون بين دولة وأخرى سوف يتم بين أجهزة الخبرة الجنائية بشكل مباشرة وبطريقة متشابكة، وهو ما نصل معه إلى أن تطوير البنية التحتية المعلوماتية لأي دولة اليوم أصبح ضرورة ملحّة، ومطلباً أساسياً قد يترتب على غيابه انعزال الدولة وصيرورة نظامها المعلوماتي – إذا كان متواضعاً – مباحاً لمرتكبي الجرائم الإلكترونية[1].

نخلص من كل ما تقدم إلى أن الخبرة والمعاينة الجنائية في الجرائم الإلكترونية اليوم تحتاج إلى إدارة خاصة يعمل بها متخصصون في أنظمة المعلومات ويتمتعون بصفة الضبطية القضائية، وهو ما يتطلب إنشاء إدارة خاصة للخبرة والمعاينة في الجرائم الإلكترونية، ولا يجب الاكتفاء بمجرد تدريب القائمين على إدارة الخبرة الجنائية، أما رجال القضاء والنيابة والضبطية القضائية فلا شك أنهم يحتاجون للتدريب على استخدام مهارات الحاسب الآلي.

أما بالنسبة لإجراءات التفتيش، ففي هذا النمط من الجرائم يتم عادة على شبكات المعلومات، وقد يتجاوز النظام المشتبه به إلى أنظمة أخرى مرتبطة، وهذا هو الوضع الغالب في ظل شيوع

[1] محمد سامي الشوا، مرجع سابق، ص. 520.

الشبكات الداخلية على مستوى الشركات أو المؤسسات والشبكات المحلية والإقليمية والدولية على مستوى الدول[1].

يعتبر امتداد نطاق التفتيش إلى نظام غير النظام محل الاشتباه محل تحديات كبيرة أولها مدى قانونية هذا الإجراء ومدى مساسه بحقوق الخصوصية المعلوماتية لأصحاب النظم التي يمتد إليها التفتيش.

وبالنسبة لإجراءات الضبط فإن عملية الضبط لا يتوقف على تحريز جهاز الكمبيوتر فقد يمتد من ناحية ضبط المكونات المادية إلى مختلف أجزاء النظام التي تزداد يوماً بعد يوم، والأهم أن الضبط ينصب على المعطيات والبيانات والبرامج المخزنة في النظام أو النظم المرتبطة بالنظام محل الاشتباه، وأي أدوات دفع إلكترونية أو أي أشياء ذات طبيعة معنوية معرضة بسهولة للتغيير والإتلاف، وهذه الحقائق تثير مشكلات متعددة، منها المعايير المقبولة للضبط المعلوماتي ومعايير التحريز إضافة إلى مدى مساس إجراءات ضبط محتويات نظام ما بخصوصية صاحبه – وإن كان المشتبه به – عندما تتعدى أنشطة الضبط إلى كل محتويات النظام التي تضم عادة معلومات وبيانات قد يحرص على سريتها أو أن تكون محل حماية بحكم القانون أو لطبيعتها أو تعلقها بجهات أخرى[2].

الفرع الثالث: المشكلات المتعلقة بسلطات التحري والملاحقة

إن خصوصية الجرائم الإلكترونية انعكست على الإجراءات الجزائية المطبقة عليها، ومنها السلطة المختصة بالتحري والملاحقة.

فمن المعروف أن صفة الضابطة العدلية لا تُمنح إلا بموجب نص خاص، فهناك قسمين لرجال الضابطة العدلية، أولهما أعضاء الضابطة العدلية ذوي الاختصاص العام، والقسم الآخر هو الأعضاء المخولون بهذه الصفة بموجب قوانين خاصة، وخولهم المشرع اختصاصات ووظائف محددة في القانون تبدأ باستقصاء الجرائم وتنتهي مع انتهاء المحاكمة[3].

ولعل الجرائم الإلكترونية لم تجد بعد لها نصاً خاصاً يحدد من هي الضابطة العدلية المختصة بها، وإن كانت بعض الجهات التي منحها المشرّع صفة الضابطة العدلية الخاصة مثل موظفي مكتب حماية حق المؤلف، حيث يختصون ببعض الانتهاكات التي تقع على حقوق المؤلفين الواقعة باستخدام الوسائل المختلفة ومنها الوسائل الإلكترونية، وعليه فإن الضابطة العدلية العامة بحسب التشريع ي

---

[1] عبد الفتاح حجازي، **مكافحة جرائم الكمبيوتر والإنترنت**، دراسة معمقة في القانون المعلوماتي، دار الفكر الجامعي، الإسكندرية، ط1، ص. 14.

[2] عبد الفتاح حجازي، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت**، مرجع سابق، ص. 148.

[3] انظر: المواد 8 – 10 أصول جزائية أردني، والمواد 39-44 إجراءات جنائية كويتي.

المختصة قانوناً بتقصي الجرائم الواقعة في البيئة الإلكترونية ما لم يحدد سواهم للقيام بذلك وخصوصاً بوجود النصوص التي تسمح للمدعي العام الاستعانة بالخبراء في أي مجال ومنها المجال الإلكتروني.

هذا وتثير الجرائم الإلكترونية إشكاليات تتعلق بعمل سلطات الاستدلال والتحقيق، وهذه مردها الإحجام عن الإبلاغ ونقص خبرة هذه السلطات، هذا ولم يلزم المشرع اللبناني في قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي، الإبلاغ عن الجريمة الإلكترونية، إلا أن القواعد العامة في قانون أصول المحاكمات الجزائية جعلت الإبلاغ عن الجرائم إلزامي كقاعدة عامة.

نجح "مكتب مكافحة الجرائم الإلكترونية وحماية الملكية الفكرية" منذ إنشائه، في محاسبة أصحاب مدونات أو صحافيين أو ناشطين أو ناس عبّروا عمّا في بالهم، بطريقة "مخالفة". سمعنا أخباراً لا تحصى ولا تعدّ عن أناس اقتيدوا إلى التحقيق بسبب "بوست" أو "شير" على "فايسبوك"، أو تغريدة عبر "تويتر". مع العلم أن المكتب عبارة عن ضابطة عدلية تتولى التحقيق في القضايا التي تحيلها النيابة العامة عليها، وعملها لا يقتصر على مراقبة ما يحدث عبر مواقع التواصل الاجتماعي، بل ملاحقة المجرمين الحقيقيين الذين يمارسون الاحتيال والقرصنة والسرقة الإلكترونية، التي يقع ضحيتها كثيرون.

في المقابل، ليس في لبنان حتى الآن قانون خاص بالجرائم الإلكترونية. هو مجرد مشروع قانون ينتظر إعادة فتح أبواب مجلس النواب حتى يقرّ ويُنشر.

الفرع الرابع: المشكلات المتعلقة بالاختصاص والقانون واجب التطبيق

1- <u>على المستوى الدولي</u>

غالباً ما تدخل الأفعال الجرمية المرتكبة ضمن الاختصاص القضائي لعدة دول، إذ أن الفضاء السيبراني لا يلتزم بالحدود الجغرافية. ويتم تحديد الاختصاص القضائي لدولة ما بالأفعال الجرمية التي تقع ضمن إقليمها أو بالأفعال التي يرتكبها مواطنوها خارج أراضيها (مبدأ الجنسية الإيجابية "Principle of active nationality" أو تقع على مواطنيها في الخارج مبدأ الجنسية السلبية "Principle of passive nationality"، أو بالأفعال الجرمية التي تطال مصالحها الأساسية كدولة. ويكفي في بعض الأحيان توفر أحد عناصر الفعل الجرمي أو أحد آثاره أو نتائجه الجرمية أو نظام معلوماتي أو بيانات ضمن الإقليم الوطني لربط اختصاص المحاكم الوطنية. ويكفي لربط اختصاص المحاكم الإقليمي أن يكون أحد عناصر الفعل الجرمي، قد حصل في إقليم الدولة، كالنتيجة الجرمية مثلاً، ويسمى ذلك "مبدأ الإقليمية الموضوعية" "Principle of objective territory"، ويثير ذلك تنازع الاختصاص القضائي بين محاكم عدة دول.

فعلى سبيل المثال، يكفي استعمال البنية الأساسية لدولة ما، كاستضافة البيانات أو تقديم خدمة البريد الإلكتروني أو تقديم خدمات الاتصالات ونقل المعلومات، ولو انتقالياً، لتعتبر الجريمة ضمن الدولة حتى ولو كان المجرم أو الضحية خارجها. كما يمكن في بعض الدول إعطاء المحاكم صلاحية النظر في الأفعال الجرمية التي تمس مصالح المجتمع الدولي مبدأ العالمية " Principle of universality"، كالجرائم ضد الإنسانية أو جرائم الحرب أو جرائم الاتجار بالبشر أو الاستغلال الجنسي للمرأة خلال فترة الأزمات والحروب. ويتم حل النزاعات حول الاختصاص القضائي بين الدول بالتشاور بالطرق الرسمية أو غير الرسمية. وتقدر دراسة الأمم المتحدة أن بين 30 و70 في المائة من الجرائم السيبرانية تتضمن عنصراً دولياً.

بالنسبة للاختصاص بالنظر في الجريمة فإنه يلاحظ أن اختصاص القضاء بنظر الجرائم الإلكترونية والقانون الواجب تطبيقه على الفعل لا يحظى دائماً بالوضوح أو القبول أمام حقيقة أن غالبية هذه الأفعال ترتكب من قبل أشخاص من خارج الحدود، أو أنها تمر عبر شبكات معلومات وأنظمة معلومات خارج الحدود حتى عندما يرتكبها شخص من داخل الدولة على نظام في الدولة نفسها، وهو ما يبرز أهمية اختبار مدى ملاءمة قواعد الاختصاص والقانون واجب التطبيق، وما إذا كانت النظريات والقواعد القائمة في هذا المجال تطال هذه الجرائم، أم يتعين أفراد قواعد خاصة بها في ضوء خصوصيتها، وما تثيره من مشكلات في حقل الاختصاص القضائي، ويرتبط بمشكلات الاختصاص وتطبيق القانون مشكلات امتداد أنشطة الملاحقة، والتحري، والضبط، والتفتيش خارج الحدود وما يحتاجه ذلك إلى تعاون دولي شامل للموازنة بين موجبات المكافحة ووجوب حماية السيادة الوطنية[1].

2- <u>على المستوى الوطني</u>

شهدت نهاية العام 2018 وبداية العام 2019 تدخلاً للقضاء العسكري في قضايا الصحافة والرأي والتعبير، عبر ملاحقة عدة صحافيين ووسائل إعلام وإحالتهم إلى المحاكمة بتهم المسّ بسمعة القضاء العسكري والجيش والمؤسسات الأمنية وقياداتها ونشر أخبار كاذبة. وتضاربت الإجراءات المتخذة بين ملاحقة البعض أمام القضاء العسكري والبعض الآخر أمام محكمة المطبوعات خلافاً لصلاحيات القضاء العسكري الذي ينحصر في الجرائم العسكرية والجرائم المرتكبة من العسكريين أو عليهم[2].

[1] محمد الشوابكة، مرجع سابق، ص.13.
[2] www.haratfoundation.org

وكانت الوكالة الوطنية للإعلام قد نشرت في 15 شباط 2019 بياناً صادراً عن مفوض الحكومة لدى المحكمة العسكرية جاء فيه: "قررت النيابة العامة العسكرية إحالة كل خبر كاذب يُنشر في وسائل الإعلام على وسائل التواصل الاجتماعي ويتناول الجيش اللبناني والأسلاك الأمنية والقضاء العسكري على محكمة المطبوعات، واتخاذ صفة الادعاء بشأنها كي لا يرسخ في ذهن الرأي العام أي للأخبار الكاذبة أو المضللة التي تسيء إلى هذه المؤسسات ودورها.

لا يعني هذا البيان التوضحي أن النيابة العامة العسكرية كفّت يدها عن قضايا النشر التي تطال الجيش والمؤسسات الأمنية الأخرى ووضعتها في عهدة القضاء العدلي ومحكمة المطبوعات، وإنما يُفهم منه أن النيابة العامة العسكرية لن تحيل بعد الآن هذا النوع من القضايا إلى المحكمة العسكرية، ولكن سوف تضطلع بمهام التحقيق مع المتهمين أمام الشرطة العسكرية أو أي جهاز مولج بالتحقيق في إطار الضابطة العدلية العسكرية وسوف تدّعي مباشرة أمام محكمة المطبوعات بالجرائم والتّهم المذكورة في البيان.

هناك تخبط واضح في ممارسة القضاء العسكري لصلاحياته تجاه قضايا النشر والرأي والتعبير خلافاً لأحكام القانون.

منذ العام 1971 لم يعد القضاء العسكري مختصاً لملاحقة ومحاكمة جرائم النشر التي تتم بواسطة المطبوعات الصحافية انتقل اختصاص الملاحقة والحُكم بها إلى محكمة المطبوعات (بموجب القانون رقم 2 الصادر في 22 كانون الثاني من العام 1971 عدل اختصاص الملاحقة والحكم بموجب المادة 157 من المحكمة العسكرية إلى محكمة المطبوعات. بالنسبة لجرائم النشر التي تتم (بواسطة المطبوعات الصحفية) وبالتالي يدخل اختصاص الملاحقة والحكم في صلاحية محكمة المطبوعات بالنسبة لجرائم النشر التي تتم بواسطة وسائل النشر الصحافية التالية:

أ. النشر بواسطة المطبوعات الصحافية – ويشمل الصحف الورقية والصحف الإلكترونية أي المواقع الإخبارية الإلكترونية وفق اجتهاد محكمة المطبوعات ومحكمة التمييز.

ب. النشر بواسطة التلفزيون والراديو وفق أحكام قانون البث التلفزيوني والإذاعي التي توجب تطبيق أحكام قانون المطبوعات على الجرائم المرتكبة بواسطتها.

أما صلاحية القضاء العسكري وفق القوانين النافذة، فهي محدودة جداً، وتقتصر على ملاحقة جرائم النشر المحدّدة والمنصوص عنها في المادة 157 المذكورة أعلاه والتي تتم عبر وسائل التواصل الاجتماعي والتي لا علاقة لها بممارسة العمل الصحافي ونشر وتداول المعلومات، وقد تقدمت مؤسسة مهارات باقتراح قانون جديد للإعلام بالتعاون مع النائب السابق غسان مخيبر،

اقترحت فيه تطبيق نفس نظام الملاحقة والعقاب بالنسبة لجميع جرائم النشر، بما فيها تلك التي تتم بواسطة وسائل التواصل الاجتماعي. وطلبت إلغاء المادة 157 من قانون القضاء العسكري لكونها تتعارض مع حرية الرأي والتعبير وحرية تداول المعلومات من أجل المصلحة العامة.

أصدرت المحاكم الجزائية أحكاماً بالحبس ضد ما لا يقل عن ثلاثة أفراد في قضايا التحقير بين 2015 و2019. تلقى أحد هؤلاء الأفراد تسعة أحكام بالحبس غيابياً في تسع قضايا جنائية مختلفة رفعها عليه السياسي نفسه. أصدرت محكمة المطبوعات حكماً واحداً على الأقل بالحبس غيابياً بين 2015 و2019.

خلال الفترة نفسها، أصدرت المحاكم العسكرية ثلاثة أحكام بالحبس غيابياً، أُلغي اثنان منها عند الاستئناف بعد أن أعلنت المحاكم العسكرية عدم اختصاصها.

في السنوات الأخيرة، استُخدمت النصوص القانونية الجزائية المتعلقة بالقدح والذم في لبنان ضد الصحفيين، والنشطاء، وغيرهم من المواطنين الذين كتبوا عن فساد المسؤولين، أو تحدثوا عن سوء سلوك الأجهزة الأمنية، أو انتقدوا الوضع السياسي والاقتصادي الحالي، أو كشفوا الانتهاكات ضد الفئات المستضعفة.

الفرع الخامس: حلول مقترحة

تمثل هذه الحلول التشريعية في تدابير وقائية تتخذها الدولة وقوانين تسنّها من أجل مكافحة هذه الجريمة وحماية المجتمع ولكن لصعوبة التعامل مع هذه الجرائم الجديدة في الوقت الراهن يتطلب الأمر بداية اللجوء إلى حلول قصيرة المدى، ثم حلول طويلة المدى وهو إعادة النظر في معظم التشريعات، لأن معظم الإنترنت أصبح ظاهرة تمس جميع مجالات الحياة.

1- <u>الحلول التشريعية قصيرة المدى</u>

أ. إن هذه الحلول تتمثل في إصدار السلطة المختصة بعض المراسيم التنظيمية لمقاهي الإنترنت دون احتكار المعلومة فيمكن في إجراءات استعجالية فرض بعض الأمور على أصحاب مقاهي الإنترنت.

ب. وضع البرامج اللازمة لمنع الدخول إلى المواقع المخلة بالحياء، وهذا من أهم الظواهر التي برزت في مجتمعنا في ظل غياب التربية السليمة، مما يؤدي للانحلال الخلقي لشبابنا وحتى المراهقين الذي أصبح من السهل عليهم دخول أي موقع يشاءون بالإضافة إلى المواقع

الإباحية، هناك المواقع الإرهابية ومواقع للعنف كتعليم القتل، فلا بد من تدبير عاجل، لأن الحرية في المعلومة لا تكمن في دخول هذه المواقع.

ج. وضع برامج للحماية من الفيروسات وهذا كله بمراسيم تنظيمية، ويمكن للدولة أن تدعم هذه العملية بتخفيض المواقع.

د. وضع برامج للحماية من الفيروسات وهذا كله بمراسيم تنظيمية ويمكن للدولة أن تدعم هذه العملية بتخفيض أسعار هذه البرامج.

ه. التوعية القانونية والتعريف بمدى خطورة الجرائم الإلكترونية.

و. إصدار مراسيم من أجل تنظيم تكوين محققين ورجال شرطة وقضاة على التقنية المعلوماتية والمعرفة الكافية لجرائم الإنترنت.

ز. تعريض أشخاص أو مقاهي الإنترنت لغرامة مالية أو حتى إغلاق المقهى إذ تثبت أنه يسمح للمراهقين أو حتى الشباب بالدخول للمواقع السابقة. ففي المواد الجنائية لا يمكننا ذكر أكثر من هذا، احتراماً لمبدأ لا عقوبة إلا بنص قانوني.

أما من ناحية المواد المدنية والتجارية فإنه:

أ. يمكن للمحاماة لعب دور مهم لتكييف بعض السلوكيات والمعلومات مع محاولة القضاة تكييف بعض المنازعات التجارية الإلكترونية، قياساً على التجارة العادية لحين صدور التشريع المنظم للتجارة الإلكترونية.

ب. اعتماد حرية الإثبات في المجال التجاري.

ج. يجب على المشرّع أن يوقع بعض المعاهدات لمكافحة الجريمة الإلكترونية.

د. يجب على المشرع أن يوقع بعض الاتفاقيات التي تتبنى تعريف التوقيع الإلكتروني والعقد الإلكتروني ومسايرتها بسن قوانينها التنظيمية.

2- <u>الحلول التشريعية طويلة المدى</u>

أ. إن الطابع اللامادي والافتراضي لشبكة الإنترنت يستلزم تعديل العديد من التشريعات الحالية بالإضافة إلى استحداث أخرى، وهذا لا يضطرنا بالضرورة إلى خلق شيء جديد، بل يمكننا الاستفادة من الدول الأخرى التي سبقتنا في مجال التشريع لتجريم هذه السلوكيات ما دامت هذه التشريعات لا تخالف النظام العام والآداب العامة، وبما أنه لا يمكن معاقبة شخص من دون نص قانوني.

ب. الركن الشرعي إذن لا بد من سن نصوص قانونية تتناسب والتطور الحالي.

ولكننا نلاحظ أنه رغم زيادة انتشار الجرائم الإلكترونية وفعاليتها إلا أن المشرع لم يضع لحد الآن الإطار القانوني لأي من هذه الظواهر، لذا على المشرع أن يعدل أو يصدر قوانين جديدة. ففي نطاق الحماية الجنائية يتعين الإقرار بصلاحية المعلومات كمحل للحماية من أنشطة الاعتداء كافة فبدأ بالتشريعة العامة وهي القانون المدني، فعلى المشرع أن يعدل فيه بسن تشريع جديد يتضمن الجرائم الإلكترونية من بينها العقد الإلكتروني والتوقيع الإلكتروني وغيرها من المفاهيم في العالم الافتراضي الجديد.

ج. القانون التجاري لقد ظهر في عالمنا اليوم مفهوم جديد هو التجارة الإلكترونية والتسويق الإلكتروني والدفع عن طريق بطاقة الائتمان وهي مجالات خصبة للاحتيال فلا بد على المشرع أن ينظمها.

د. الإثبات وهذا في اعتقادنا من أهم الخطوات التي يجب أن يقوم بها المشرع وهذا بتبني الخبرة والمعاينة كأساليب للتحقيق وإثبات الجريمة الإلكترونية.

ه. تعديل قانون الإجراءات الجزائية وتعديل قانون حقوق المؤلف والحقوق المجاورة.

يمكن أن نلخص أساليب مكافحة الجرائم الإلكترونية كالآتي:

أ. رسم سياسات دولية تفرض عقوبات صارمة على مرتكبي جرائم الإنترنت، إذ يستلزم التدخل الحكومي والدولي نظراً للخطورة الجسيمة للأمر.

ب. الاعتماد على أساليب وتقنيات متطورة للتمكن من الكشف عن هوية مرتكب الجريمة، والاستدلال عليه بأقل وقت ممكن.

ج. توعية الأفراد ونصحهم لماهية الجرائم الإلكترونية وكل ما يترتب عليها من مخاطر.

د. الحرص على الحفاظ على سرية المعلومات الخاصة بالعناوين الإلكترونية كالحسابات البنكية، والبطاقات الائتمانية وغيرها.

ه. عدم الكشف عن كلمة السر نهائياً وتغييرها بشكل مستمر واختيار كلمات سر صعبة.

و. تجنب تخزين الصور الخاصة بالأفراد على مواقع التواصل الاجتماعي وأجهزة الحاسوب.

ز. تجنب تحميل أي برنامج مجهول المصدر.

ح. استمرارية تحديث برامج الحماية الخاصة بأجهزة الحاسوب ومنها MCafee, Norton.

ط. تأسيس منظمة خاصة لمكافحة الجرائم الإلكترونية والحدّ منها.

ي. المسارعة في الإبلاغ للجهات الأمنية فور التعرض لجريمة إلكترونية.

ك. مواكبة التطورات المرتبطة بالجريمة الإلكترونية والحرص على تطوير وسائل مكافحتها.

ل. استخدام برمجيات آمنة ونظم تشغيل خالية من الثغرات.

م. الحرص على استخدام كلمات سرية للوصول إلى البرامج الموجودة على جهاز الحاسوب.

ن. عدم ترك جهاز الحاسوب مفتوحاً.

س. فصل اتصال جهاز الحاسوب بشبكة الإنترنت في حال عدم الاستخدام.

ع. أخذ الحيطة والحذر وعدم تصديق كل ما يصل من إعلانات والتأكد من مصداقيتها عن طريق محركات البحث الشهيرة.

ف. وضع الرقم السري بشكل مطابق للمواصفات الجيدة التي تصعّب من عملية القرصنة عليه من هذه المواصفات بأن يحتوي على أكثر من ثمانية أحرف أن يكون متنوع الحروف والرموز واللغات إلخ.

ص. يفضل تغيير كلمة المرور الخاصة بك بصفة دورية.

ق. لا تضع معلومات على الإنترنت لا تحب أن يراها الجميع من تعرفهم ولا تعرفهم، وتذكر أنه بمجرد أن تضع معلومات على الإنترنت لن تتمكن أبداً من إرجاعها مرة أخرى حتى لو قمت بحذفها.

ر. معلوماتك الخاصة (اجعلها خاص) أن معلوماتك الخاصة مثل اسمك بالكامل ورقم هاتفك ورقم الهوية ورقم بطاقتك الائتمان وأيضاً عنوانك بالتفصيل هي معلومات خاصة لا يجب أن تتاح للجميع على الإنترنت لا شخص لا تعرفه فلا تفصح له عنها أو تضعها على أي موقع لا تثق به.

خاتمة

ازدهار الحضارة وانتشار التقدم التقني ساعد في تسهيل الكثير والكثير من أمور حياتنا، ولكنه في نفس الوقت جلب لنا العديد من المخاطر والأضرار المتعلقة بالحواسيب والشبكة العنكبوتية، مما جعل الحكومات والمجتمعات تنتبه إلى ضرورة نشر التوعية والتعريف بهذه الجرائم عن طريق شرحها وتحليلها للناس وبيان وسائل وطرق الوقاية منها.

لقد حاولت قدر الإمكان عرض بعض التعريفات المتداولة لجرائم الإنترنت مع بيان عددٍ من أنواعها، والتي لا تشكّل إلا القليل من الكمّ المتزايد يومياً[1]،[2] ويمكن القول أن البحث في هذا الموضوع يعدّ أمراً مشوّقاً. وقد تبيّن لي جملة الصعوبات التي تقف حاجزاً أمام مكافحة هذا الأخطبوط الذي سيطر على كافة بقاع العالم.

في نهاية عملي المتواضع، وكنتيجةٍ للموضوع يمكن تقديم بعض التوصيات المتمثّلة في:

1- ضرورة نموّ الجهود الدولية لمكافحة جرائم الإنترنت من خلال مجموعة تشريعات وطنية واتفاقيات دولية وإقليمية وثنائية، الدعوة إلى النظر في التفاوض على اتفاقية دولية تحت مظلة الأمم المتحدة وجامعة الدول العربية لمكافحة جرائم الإنترنت مع الأخذ في الاعتبار بالجهود الدولية السابقة في هذا المجال ومن أهمها "اتفاقية بودابست"، ودليل الأمم المتحدة لمنع الجريمة المتصلة بالحواسيب ومكافحتها.

2- تنمية وعي الثقافة المعلوماتية للعاملين في مجالات العدالة الجنائية من خلال عقد الندوات المتخصّصة والدورات التدريبية لهم في هذا المجال، دعوة الدول المتقدمة في المجال المعلوماتي إلى تقديم المساعدات للبلدان التي تحتاجها، خاصة البلدان الأقل نمواً، لتمكينها من مكافحة هذه النوعية من الجرائم من خلال توفير المزيد من برامج التدريب والمساعدات الفنية.

3- الاهتمام بعقد الدورات التدريبية التي تعتني بفحص سبل مكافحة جرائم المعلوماتية وعقد المؤتمرات الدولية سنوياً وبصفة دورية، والعمل على وضع أو إيجاد ضوابط لإلزام مقاهي الإنترنت، ومقدمي هذه الخدمة لتسجيل بيانات مستخدمي الشبكة العالمية للمعلومات

[1] Understanding Cybercrime: A guide for Developing Countries.
[2] Comprehensive Study on Cybercrime.

(الإنترنت)، وإلزام مسؤولي المواقع التي تستخدم البروكسيّات بالاحتفاظ بالبيانات الأساسية والحقيقية لمستخدمي مواقعهم على الشبكة[1]. [2]

ولكن ماذا يكمن خلف هذا العالم الظاهري الذي نراه؟ إن العالم الآخر الخفي والأكثر خطورة هو الشبكات المظلمة (Dark Web).

إن الشبكة المظلمة تشير إلى مجموعة من المواقع الإلكترونية التي تستخدم آليات معينة لإخفاء هوية المستخدم، كما أنها تتطلب استخدام متصفح مختلف عن تلك المتصفحات المعتادة، ومن ثم يصبح من الصعب تعقب مستخدمي تلك الشبكة. إن محتواها قد اختلف بشكل كبير عن محتوى المعلومات المقدمة على شبكة الإنترنت الأصلية[3]، فإن هذه المواقع تعرض المخدرات، القتلة المأجورين، المواد الإباحية الفاحشة، المرشدين غير الشرعيين لإعداد متفجرات من مواد بيتية، المعلومات السرية لهيئات حكومية وجيوش، التجارة بالبشر، والتنظيمات الإرهابية بأسرها.

هذه هي الشبكة التي تحت الشبكة والتي تحوي كل شيء[4]، فلا بدّ من تسليط الضوء عليها في وقت لاحق.

مقترحات:

1- حثّ الجامعات والمراكز البحثية العربية للبحث والدراسة في الجرائم المعلوماتية والجرائم عبر الإنترنت ومحاولة إنشاء دبلومات متخصصة في المجالات الفنية والقانونية المتعلقة بمكافحة تلك الجرائم.

2- العمل على تنمية الكوادر البشرية العاملة في مجالات مكافحة الجرائم المعلوماتية.

3- إنشاء مجموعات عمل عربية لدراسة ووضع استراتيجيات وسياسات وإجراءات تنفيذية لمواجهة مثل هذه الجرائم.

4- حث جامعة الدول العربية لإصدار قانون نموذجي موحّد لمكافحة الجرائم المعلوماتية.

[1] اللجنة الاقتصادية والاجتماعية لغربي آسيا: الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: توصيات سياساتية.

[2] إرشادات الإسكوا للتشريعات السيبرانية، مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية.

[3] http://www.sasapost.com/darknet/

[4] www.al-masdar.net/ عتمة-الإنترنت-عالم-الإنترنت-المظل