المواجهة الجنائية لجرائم تقنية المعلومات

في التشريع المصري

في ضوء أحكام القانون (١٧٥) لسنة ٢٠١٨م

مقارناً بالمواثيق الدولية والتشريعات المقارنة

إعداد

د / رامي متولي القاضي

أستاذ القانون الجنائي المساعد

بكلية الشرطة

مقدمة عامة

١- التعريف بالموضوع وأهميته: تشكل جرائم تقنية المعلومات في الوقت الراهن إحدى أبرز الجرائم المرتكبة، بالنظر إلى ذيوع استخدام الحواسب الآلية والتطبيقات الإلكترونية وشبكة المعلوماتية الدولية" الإنترنت" والتقنيات المستحدثة، ودخولها في كافة مناحي الحياة، بالشكل الذي بات يشكل عالماً افتراضياً موازياً للعالم الواقعي[١]، وهو ما جعل هذه التقنيات والتطبيقات مجالاً خصباً ونطاقاً واسعاً لارتكاب العديد من الجرائم التي تمس حقوق الإنسان ومملكاته وخصوصياته؛ وهو ما يتطلب ضرورة بسط حكم القانون على هذه الأنشطة التقنية المستحدثة، وتوفير حماية قانونية متكاملة لحقوق الأفراد في مواجهة هذه النوعية المستحدثة من الجرائم، والتي أطلق عليها الجرائم المعلوماتية أو الإلكترونية أو جرائم تقنية المعلومات[٢].

---

(١) تشير تقديرات مكتب الأمم المتحدة المعني بالمخدرات والجريمة والاتحاد الدولي للاتصالات إلى أن عدد مستخدمي الانترنت في عام ٢٠١١ (٢،٣مليار نسمة) يعادل أكثر من ثلث سكان العالم، يعيش أكثر من ٦٠% منهم بالدول النامية(٦٢%)، ولا يتجاوز عمر ٤٥% منهم الـ٢٥عاماً، وأنه في عام ٢٠١٧ من المتوقع أن تناهز نسبة المشتركين في خدمة الانترنت النقالة ذات النطاق العريض٧٠% من مجموع سكان العالم، كما أنه من المتوقع كذلك أن يفوق عدد الأجهزة المتصلة بالشبكة (إنترنت الأشياء) عدد الناس بنسبة ستة إلى واحد، مما سيؤدي إلى تغيير المفاهيم الحالية للإنترنت. انظر: دراسة بعنوان:" دراسة شاملة عن الجريمة السيبرانية"، مسودة فبراير ٢٠١٣، وثائق مكتب الأمم المتحدة المعني بالمخدرات والجريمة، نيويورك،٢٠١٣، ص١؛ قياس مجتمع المعلومات، قاعدة بيانات الاتصالات العالمية، مؤشر تكنولوجيا المعلومات، الصادر عن الاتحاد الدولي للاتصالات، ٢٠١٢؛ دراسة العوامل التي تؤثر على إمكانيات الشباب لتصبح ضحية التحرش على الانترنت، المجلة الدولية لعلم الجريمة السيبرانية، ٤(١، ٢)، ص ص٦٨٥-٦٩٨.

(٢) تبرز الإشارة إلى أن مضبطة مجلس النواب المصري تضمنت قبل مناقشة القانون تنويه الأستاذ الدكتور رئيس المجلس بأن مشروع القانون بشأن مكافحة جرائم تقنية المعلومات ذو أهمية كبرى، وقد استغرق وقتاً كافياً في الدراسة والحوار المجتمعي. انظر: مضبطة مجلس النواب المصري، =

وتبرز أهمية مواجهة هذه الجرائم في أنها -وبالنظر إلى حجم تجارة المعلومات، والتي تشكل(٨%) من حجم التجارة الدولية[١]- باتت تهدد أمن وسلامة الأفراد والمؤسسات، فمع تزايد الاعتماد على المعلومات[٢]، واستخدام شبكة الإنترنت والتقنيات الحديثة في تبادلها، والتوسع في أنشطة التجارة الإلكترونية وغيرها من الأنشطة الاقتصادية، فلم يعد هناك مجالاً اقتصادياً أو اجتماعياً أو إدارياً، إلا وتباشر فيه الحاسبات وتقنية المعلومات دوراً رئيسياً في أدائه وتطويره كالبنوك والمؤسسات الحكومية[٣]، ومن ثم فسوف تتزايد صور الاعتداءات والتهديدات للأفراد،وهو ما يستلزم ضرورة التصدي لها بكل حسم، حفاظاً على حقوق المواطنين،وبالشكل الذي يُحقق فاعلية في مواجهتها[٤].

ومما يبرز قدر الخطورة التي وصلت إليها جرائم تقنية المعلومات، ما أشار إليه السيد/ بان كي مون "الأمين العام السابق للأمم المتحدة" في كلمته خلال مؤتمر

=

الفصل التشريعي الأول، دور الانعقاد العادي الثالث، مضبطة الجلسة السادسة والخمسين، المعقودة في ٢٠١٨/٥/١٤م، ص٣٨.

(١) يرى البعض أن المعلومات باتت أهم وأثمن الموارد على الإطلاق. انظر: د. إسماعيل عبد النبي شاهين: أمن المعلومات في الإنترنت بين الشريعة والقانون، مؤتمر القانون والكمبيوتر والإنترنت، كلية القانون، جامعة الإمارات العربية، ٢٠٠٠، ص١.

(٢) يرى جانب من الفقه أن المعلومات تتزايد يوماً بعد يوم، ولا تتناقص بالاستخدام أو الاستهلاك، ومن ثم فهي تعتبر مصدر قوة اقتصادية وسياسية وعسكرية واجتماعية. انظر: د. هشام محمد فريد رستم: قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط،١٩٩٢، ص١.

(٣) د. هدى حامد قشقوش: جرائم الحاسب الإلكتروني والتشريع المقارن، دار النهضة العربية،١٩٩٢، ص٧؛ جمال توفيق وآخرون: الجرائم المعلوماتية وطرق مواجهتها، دراسة مركز بحوث الشرطة، الإصدار الثالث، يونيو ٢٠٠٥، القاهرة، ص١٠.

(٤) أنظر للمؤلف: الجرائم المعلوماتية وطرق مواجهتها، مؤتمر الجرائم المُستحدثة- كيفية إثباتها ومواجهتها، المركز القومي للبحوث الاجتماعية والجنائية، يومي ١٥-٢٠١٠/١٢/١٦، ص١.

الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية الذي عقد عام ٢٠١٥ بالدوحة، حيث اعتبر أن جرائم الإنترنت باتت في الوقت الراهن نشاط أعمال يتجاوز المليارات من الدولارات سنوياً في عمليات الاحتيال عبر الإنترنت، وسرقة الهوية، والملكية الفكرية المفقودة حيث يمس ملايين الناس عبر العالم إضافة لمجال الأعمال والحكومات.

أضف على ذلك أنه مع التقدم المُذهل في استخدامات شبكة المعلومات الدولية "الإنترنت" والتقنيات الحديثة، فقد أصبح الأمن المعلوماتي مُهدداً بأساليب إجرامية لم تعرفها التشريعات الجنائية من قبل، مثل: مُحاولات التسلل لنظم المعلومات بقصد التعديل أو التبديل فيها أو تعطيلها، والاعتداء علي الحقوق المُرتبطة بها، وهو ما أفرز قصوراً تشريعياً في مواجهة مثل هذه الصور الإجرامية الخطيرة[١].

علاوة على التطورات الحادثة في مجال استخدام شبكة الانترنت والتحول إلى أنترنت الأشياء، وتطور تطبيقات الحاسب الآلي نحو أنظمة الذكاء الاصطناعي، وهو ما سيؤدي إلى دخول البشرية في مرحلة جديدة، يصعب فيها تصور وقوع جريمة ما (معلوماتية أو تقليدية) لا تنطوي على أدلة رقمية[٢]، وهو ما يتطلب ضرورة وضع إطار قانوني حاكم لهذه الاستخدامات الجديدة، ولا شك في أن وجود هذا الإطار القانوني يتطلب وجود تصور واقعي لاستخدامات الذكاء الاصطناعي وتأثيراتها على السلوك الإنساني والاجتماعي للإنسان والمصالح القانونية المختلفة الجديرة بالحماية القانونية.

---

(١) د. ممدوح عبد الحميد عبد المطلب: جرائم استخدام شبكة المعلومات العالمية– الجريمة عبر الإنترنت، مؤتمر القانون والكمبيوتر والإنترنت، كلية القانون،جامعة الإمارات العربية، ٢٠٠٠، ص٢.

(٢) انظر: دراسة مكتب الأمم المتحدة المعني بالمخدرات والجريمة حول الجريمة السيبرانية، مرجع سابق، صxiii.

وتشير تقديرات مكتب الأمم المتحدة المعني بالمخدرات والجريمة إلى أن التأثير السلبي لجرائم تقنية المعلومات أضحى حالياً أكثر تأثيراً على الأفراد من الجرائم التقليدية، حيث تتراوح معدلات الضرر من جرائم تزوير بطاقات الائتمان وانتحال الشخصية على الانترنت والتصيد الاحتيالي واختراق حسابات البريد الالكتروني ما بين (١-١٧%) من نسبة السكان من مستخدمي الانترنت في ٢١دولة من دول العالم، مقارنة بمعدلات الضرر من جرائم السطو والسلب وسرقة السيارات التي تقل عن ٥% من نسبة السكان في هذه البلدان نفسها، وكانت معدلات الضرر بسبب الجريمة السيبرانية أعلى في البلدان الأقل نمواً، مما يبرز الحاجة إلى تعزيز جهود منع الجريمة في هذه البلدان[١].

وأخيراً وليس بآخر تبرز الإشارة إلى خطورة العدوان على نظم المعلومات في تهديد حياة المواطنين وتعريضهم للخطر، بالنظر إلى ارتباط الكثير من الأسلحة النووية بهذه النظم[٢]، وهو ما يتطلب ضرورة توفير حماية متكاملة لوقاية الجنس البشري من مخاطر هذه الأسلحة، ونذكر في هذا الصدد الفيروس المعلوماتي الذي ضرب أجهزة الحاسب الآلي الخاصة بالمفاعلات النووية الإيرانية، والذي أصاب العديد من أجهزة الحاسبات الآلية بالشلل في العديد من الدول الأسيوية.

وغني عن البيان أن الفضاء الإلكتروني بات أحد العوامل المساعدة على ارتكاب الجرائم بصفة عامة، بالنظر إلى أن هذا العالم الافتراضي يسهل لضعاف النفوس ارتكاب جرائم ما كانوا ليرتكبوها في العالم الحقيقي، ويشجعهم على ذلك من

---

(١) المرجع السابق، صxxii.

(٢) د. غنام محمد غنام: عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، مؤتمر القانون والكمبيوتر والإنترنت، كلية القانون، جامعة الإمارات العربية المتحدة، ٢٠٠٠،ص٥.

خلال تمكينهم من إخفاء هوياتهم الحقيقية واستخدام هويات مزيفة، فضلاً عما توفره شبكة الإنترنت ومواقع التواصل الاجتماعي من فرص لاصطياد المجني عليهم وبصفة خاصة من خلال شبكات التواصل الاجتماعي، كما أن هذا الفضاء الالكتروني أضحى مجالاً خصباً لنقل عدوى الجريمة، من خلال ما توفره شبكة الإنترنت من فرص للالتقاء الاعتباري في غرف الدردشة ومواقع التواصل لتبادل الخبرات الإجرامية وتبادل المعلومات والبرمجيات والأدوات التقنية في الأسواق غير المشروعة للاتجار بالبيانات والمعلومات، واستثمار هذا الواقع الافتراضي من جانب جماعات الجريمة المنظمة واستغلال هذا الفضاء الالكتروني في أنشطتها الإجرامية.

٢- مدى الحاجة لوجود تشريع لمكافحة جرائم تقنية المعلومات[١]: يمكن إجمال أبرز المبررات لوجود تشريع لمكافحة جرائم تقنية المعلومات، فيمايلي:-

أ- تصاعد معدلات ارتكاب جرائم التصيد الاحتيالي، والاختراق غير المشروع لأنظمة الحاسب والقرصنة المعلوماتية، وتنامي تسويق أدوات إساءة استخدام الحاسب بشكل خطير، بما يستوجب ضرورة وضع نصوص تجريمية للحد من هذه الجرائم المستحدثة[٢].

---

[١] عددت دراسة مكتب الأمم المتحدة المعني بالمخدرات والجريمة ست وظائف لتشريعات جرائم تقنية المعلومات، تتبلور في: وضع معايير سلوكية واضحة لاستخدام أجهزة الحاسب الآلي، وردع الجناة وحماية المواطنين، وتمكين سلطات إنفاذ القانون من إجراء التحقيقات مع حماية الخصوصية الفردية، وتوفير إجراءات عادلة ومنصفة للعدالة الجنائية، والإلزام بالحد الأدنى من معايير الحماية في مجالات مثل التصرف في البيانات والتحفظ عليها، وتمكين التعاون بين الدول في المسائل التي تنطوي على جرائم معلوماتية وأدلة رقمية. انظر: دراسة مكتب الأمم المتحدة المعني بالمخدرات والجريمة، مرجع سابق، ص٧٤.

[٢] المرجع السابق، ص١١.

ب- عجز النصوص الحالية عن توفير إطار تشريعي حاكم لمواجهة هذه الجرائم: بالنظر إلى طابعها التقني[١]، وارتباطها بالتطورات التقنية المتلاحقة، فضلاً عن عدم قدرة التشريعات الوطنية علي حصرها، ووضع حد لانتشارها[٢]، علاوة على أن وجود تشريع لمكافحة هذه الجرائم المستحدثة يعد تكريساً لمبدأ الشرعية الجنائية والذي يعد من أهم المبادئ الدستورية التي تقوم عليها النظم القانونية في كافة الدول، وهو ما يتطلب وجوب أن يكون الفعل مناط التجريم منصوصاً عليه بوضوح في القانون، ومن ثم تمديد الحماية الجنائية للمصالح القانونية ضد الأنماط الجديدة من الأفعال المتصلة بتقنية المعلومات.

ج- صعوبة مُكافحة هذه الجرائم: ومنها صعوبة السيطرة على شبكة الإنترنت، وعلى الجرائم التي ترتكب عليها، بل وصعوبة اكتشافها أو تحديد مصدرها أو إيقافها بالنظر إلى سرعة نشر المعلومات وتسجيلها على أجهزة الحاسبات الخادمة Servers في الخارج، واتسامها بطابع عبر وطني مُتجاوزٍ للحدود الجغرافية بين الدول، علاوة على ما قد يلجأ إليه الجناة من استخدام تقنيات ومهارات تصعب من وسائل كشفهم وتتبعهم، أو التوصل إلى أدلة ضدهم.

---

[١] أثارت الطبيعة المعنوية للمعلومات جدلاً في أوساط الفقه الجنائي، في ضوء عدم انطباق النموذج القانوني لبعض الجرائم على جرائم تقنية المعلومات، ففي جريمة سرقة البيانات والمعلومات -على سبيل المثال- فإن نزع الملكية من المجني عليه قد لا يتوافر بالنظر إلى بقاء البيانات في حيازة المجني عليه، كما أن انطباق مدلول المكان العام كعنصر من عناصر جريمة السب أو القذف العلني أو جريمة التحرش الجنسي قد لا تشمل ارتكاب الجريمة عبر شبكة الإنترنت، الأمر الذي يتطلب وجوب مسايرة القواعد القانونية لتكنولوجيا المعلومات الجديدة. انظر:

SIEBER (U.): Straftaten und Strafverfolgung im Internet, In: Gutacten des deutschen Juristentags, Munich,2012,C.H.Beck,pp.14-15.

[٢] أنظر للباحث: دور وزارة الداخلية في مُكافحة الجرائم المعلوماتية، ندوة الواقع الأمني مسئوليات– إنجازات، مركز بحوث الشرطة، القاهرة، يوم ٢٠١١/١/٩، ص٣.

د- غياب الأطر القانونية المُتفق عليها لتنظيم التعامل الدولي مع مثل هذه الجرائم، ومن ثم غياب مبدأ التجريم المزدوج الذي تؤسس عليه آليات التعاون الدولي لمكافحة الجرائم، فعدم وجود نصوص قانونية لتجريم هذه الأفعال في دولة ما، من شأنه إتاحة ملاجئ آمنة للجناة، إذ من غير المرجح أن تقدم دولة ما المساعدة القانونية لدولة أخرى في تحقيقات جنائية لديها، يتهم فيها أشخاص مشمولون بحمايتها عن أفعال غير مجرمة في إقليمها[١].

هـ- إظهار الإحصائيات لدلالات تؤكد على خطورة انتشار جرائم تقنية المعلومات من الناحية الاقتصادية: إذ تشير التقديرات - على الرغم من تعددها وتباينها- إلى أن هذه الجرائم تتسبب في خسائر مالية هائلة في العديد من الدول، ففي الولايات المتحدة الأمريكية تقدر خسائر هذه الجرائم ما بين (٣-٥) مليار دولار سنوياً[٢]، بينما أشار التقرير السنوي الثامن لمكتب التحقيقات الفيدرالية الأمريكي الصادر عام ٢٠٠٣ بعنوان:" جرائم الحاسب"، إلى أنه على الرغم من أن متوسط تكلفة الجريمة المعلوماتية الواحدة يقدر بحوالي (٣) آلاف دولار

---

[١] يكون هؤلاء الجناة -في الدول التي لا تجرم الأفعال الضارة المشتملة على استخدام تقنية المعلومات- طلقاءً في استهداف المجني عليهم في دول أخرى، حيث لا تستطيع هذه الدول أن تبسط حماية فعالة ضد الآثار المترتبة على الأنشطة الإجرامية العابرة للحدود الوطنية لهؤلاء الجناة، حتى ولو كان قانونها الجنائي يسمح بسريان الولاية القضائية على الأفعال التي يرتكبها هؤلاء الجناة فيها، إلا بموافقة أو مساعدة الدولة المتواجد بها الجناة، سواء تعلق الأمر بجمع الأدلة أو تسليم مرتكب الجريمة. انظر: دراسة مكتب الأمم المتحدة، المرجع السابق، ص ص٨٥، ٨٦.

[٢] أشارت مجلة لوس أنجلوس تايمز في عددها الصادر في ٢٠٠٠/٣/٢٢ أن خسارة الشركات الأمريكية من جراء هذه الجرائم بلغت ١٠ مليار دولار سنوياً، بينما قدر تقرير مكتب التحقيق الفيدرالي FBI الخسائر المادية للشركات الأمريكية جراء هذه الجرائم خلال الفترة من (٢٠٠٠-٢٠٠٣) تضاعفت من حوالي (١٨) مليون دولار عام ٢٠٠٢ إلى ما يقارب (٦٥) مليون دولار عام ٢٠٠٣. انظر: د. إيمان شريف قائد: الجريمة المعلوماتية وأبعادها، ندوة الواقع الأمني مسئوليات- إنجازات، مركز بحوث الشرطة، القاهرة، ٢٠١١/١/٩، ص ص٤-٦.

سنوياً، وهي تكلفة شراء جهاز حاسب آلي بملحقاته واتصاله بشبكة الإنترنت، إلا أن الخسائر الناجمة عنها في مجال الاستيلاء على المعلومات تتعدى (٧٠) مليون دولار، بينما تتجاوز جرائم تعطيل نظم المعلومات (٦٥,٥) مليون دولار[١]، وأن حوالي (٢٧٣) شركة أمريكية في عام ٢٠٠٠ بلغت خسائرها أكثر من (٢٥٦) مليون دولار، كما أشارت تقديرات الجمعية الأمريكية للأمن الصناعي إلى أن خسائر الجرائم المعلوماتية قد بلغت (٦٣) مليون دولار، وأن الفقد السنوي بسبب سوء استخدام الحاسب الآلي قد بلغ (٥٥٥) مليون دولار، بينما أشارت تقديرات أخرى إلى أن أعمال قرصنة البرامج في عام ٢٠٠٢ قد بلغت (١٣،١) مليار دولار سنوياً[٢].

وعلى نحوٍ موازٍ أشارت التقديرات في بريطانيا إلى وقوع ما يقرب من (٢٦٢) جريمة معلوماتية في أواخر الثمانيات، قدرت خسائرها بنحو (٩٢) مليون جنيه إسترليني، بينما أشارت إحصاءات مُنظمة (سوفت وير للأعمال) إلى أن خسائر الجرائم المعلوماتية قد بلغت (٣٠) مليون دولار في السعودية والإمارات، ومليون وأربعمائة ألف دولار في لبنان[٣].

أما في مصر فقد أشارت بعض الدراسات والتقديرات الحديثة إلى تصاعد حجم تلك الجرائم عام ٢٠٠٩، حيث تم ضبط (٣٨٣) جريمة حاسب آلي واختراق شبكة

---

[١] د. فؤاد جمال: جرائم الحاسبات والإنترنت، ندوة المواجهة الأمنية للجريمة المعلوماتية، مركز بحوث الشرطة، القاهرة، ٢٠٠٩/٤/٧، ص ص١١-١٨.

[٢] د.عفيفي كامل عفيفي: جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، القاهرة، بدون ناشر، ٢٠٠٠، ص٨٨؛ د. فؤاد جمال، مرجع سابق، ص٢٣.

[٣] د. إيمان شريف قائد، مرجع سابق، ص ص٤-٦.

المعلومات[١]، بينما تشير بعض التقديرات الرسمية إلى أن هذه الجرائم المرتكبة في مصر في تزايد مستمر، إذ تشير هذه التقديرات إلى تضاعف أعداد البلاغات لجهات إنفاذ القانون من وقوع جرائم معلوماتية، خلال الفترة من (٢٠٠٢-٢٠١٧)، ففي عام ٢٠٠٢ بلغ أعداد هذه البلاغات (٧) بلاغات، ليصبح في عام ٢٠١٧ (٨٦١٤) بلاغاً، ليصبح عدد البلاغات خلال الفترة من (٢٠٠٢-٢٠١٧) تقدر بنحو (٣٠٧٦٠) بلاغاً، وهو ما يشير بلا أدنى شك إلى تصاعد أعداد الجرائم المعلوماتية في مصر، وبصفة خاصة خلال الخمس سنوات الأخيرة، بعد أن كانت أعداد هذه الجرائم محدودة للغاية[٢]، وتبرز الإشارة إلى أن هذه الأعداد مرشحة للزيادة بصدور القانون الجديد رقم (١٧٥) لسنة ٢٠١٨ في ضوء ما تضمنه من تجريم لصور جديدة من الجرائم.

ومن ثم فقد استقر الفقه والقضاء المقارن على أن من شأن استخدام التقنيات الرقمية وانتشار استخدامها في كافة مناحي الحياة أن تظهر الحاجة إلى قانون جديد للإجراءات الجنائية يختلف في قواعده عن القوانين الحالية[٣].

---

(١) د. أحمد محمود محمد مصطفى، مرجع سابق، ص ص١٣-١٤.

(٢) تشير التقديرات الرسمية إلى تضاعف عدد البلاغات في عام ٢٠٠٣ إلى (٢٤) بلاغاً، ثم ارتفعت في العام الذي يليه (٢٠٠٤) إلى (٢٩) بلاغاً، وفي العام الذي يليه (٢٠٠٥) ارتفعت لتصبح (١٦١) بلاغاً، حتى أصبحت في عام ٢٠٠٦ (٢٥٣) بلاغاً، ثم تزايدت في ٢٠٠٧ لتصبح (٣٤٧) بلاغاً، ثم في العام الذي يليه ٢٠٠٨ ارتفعت إلى (٣٧٣) بلاغاً، وفي عام ٢٠٠٩ تزايدت لتصبح (٣٨١) بلاغاً، ليتضاعف العدد في العام الذي يليه ٢٠١٠، ليصبح (٥٩٤) بلاغاً، ثم بعد ذلك يتضاعف في العام الذي يليه ٢٠١١، ليصبح (١١١١) بلاغاً، ثم يتزايد عدد البلاغات ليصبح في عام ٢٠١٢ (١١٢٠) بلاغاً، وفي عام ٢٠١٣ (٢٣٤٤) بلاغاً، وفي عام ٢٠١٤ (٣٦٤٣) بلاغاً، وفي عام ٢٠١٥ (٥٠٥١) بلاغاً، وفي عام ٢٠١٦ (٦٧٠٩) بلاغاً.

(٣) انظر من الفقه المصري: د. أشرف توفيق شمس الدين: مخاطر العملات الافتراضية في نظر السياسة الجنائية، المؤتمر الدولي الخامس عشر لكلية الشريعة والدراسات الإسلامية بجامعة الشارقة بعنوان (العملات الافتراضية في الميزان)، الشارقة، دولة الإمارات العربية المتحدة، ص٦٨٤؛ ومن الفقه المقارن انظر:

=

وفي سياق متصل أشارت دراسة مكتب الأمم المتحدة المعني بالمخدرات والجريمة إلى أن خطورة واقع الجريمة السيبرانية وما تهيئه تكنولوجيا المعلومات وزيادة استخدام الانترنت من فرص جديدة للمجرمين وتيسير تنامي الجريمة، والذي يشكل نموذجاً إجرامياً فريداً يفرض تحديات على مكافحتها، فظهور الفضاء السيبراني أوجد ظواهر إجرامية جديدة، تختلف عن الفرص التي يوفرها وجود أنظمة الحاسب الآلي لارتكاب الجرائم، فمن الممكن أن يرتكب أشخاص جرائم في الفضاء السيبراني ما كان لهم أن يرتكبوها في الواقع المادي بحكم وضعهم ومكانتهم، علاوة على ما يمكن أن توفره شبكات الانترنت من إمكانية اتخاذ هويات غير ثابتة وإخفاء الهوية وغياب الرادع كأحد الحوافز على السلوك الإجرامي في الفضاء السيبراني[1].

٣- الإطار الدستوري لمكافحة جرائم تقنية المعلومات في التشريع المصري: حرص المشرع الدستوري المصري على تأكيد أهمية مكافحة الجرائم المعلوماتية في دستور ٢٠١٤ في مادتيه (٣١) الخاصة بأمن الفضاء المعلوماتي والتي تقضي بأنه:" *أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، تلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون*"، والمادة (٧٥) التي أشارت إلى حرمة المراسلات الإلكترونية، والتي تقضي بأنه:" للحياة الخاصة حرمة، وهى مصونة لا تمس. *وللمراسلات البريدية،*

=

Orin S. KERR: Search warrants in an era of digital evidence, Mississippi Law Journal, Vol. 75, 2005, p. 86.

[1] شملت الدراسة في إطار إعدادها ورود معلومات ذات صلة بمكافحة الجريمة المعلوماتية من ٦٩ دولة، ١١ منهم من قارة أفريقيا و١٣ من الأمريكتين و١٩ من قارة أسيا و٢٤ من أوروبا و٢ من أوقيانوسيا، فضلاً عن مشاركة ٤٠منظمة من القطاع الخاص و١٦ منظمة حكومية و١١ منظمة حكومية دولية، كما تضمنت استعراض أكثر من ٥٠٠وثيقة من مصادر مفتوحة. انظر: دراسة مكتب الأمم المتحدة المعني بالمخدرات والجريمة، مرجع سابق، ص ص١١، ١٢.

والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائى مسبب، ولمدة محددة، وفى الأحوال التى يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، وينظم القانون ذلك"، ومن ثم يتضح أن المشرع حرص على إصدار قانون لمكافحة جرائم تقنية المعلومات التزاماً بالنص الدستوري باتخاذ التدابير اللازمة للحفاظ على أمن الفضاء المعلوماتي.

٤- أهداف البحث: يسعى البحث إلى مدارسة وتحليل نصوص قانون مكافحة جرائم تقنية المعلومات المصري رقم (١٧٥) لسنة ٢٠١٨، بهدف تقديم رؤية تحليلية للقانون، وهو ما يتحقق من خلال الأهداف التالية:-

أ- بحث مدى الحاجة لوجود قانون لمكافحة جرائم تقنية المعلومات.

ب- إلقاء الضوء على نصوص القانون المصري لمكافحة جرائم تقنية المعلومات.

ج- تقدير مدى مواكبة هذا للقانون للتطورات الحادثة في مجال تكنولوجيا المعلومات للتعامل مع الظواهر التقنية الحديثة كأنظمة الذكاء الاصطناعي وإنترنت الأشياء[١].

د- الإشارة إلى موقف الاتفاقيات الدولية والإقليمية الخاصة بمُكافحة هذه الجرائم، ومواقف التشريعات المقارنة ذات الصلة.

---

[١] تبرز الإشارة إلى اتجاه الجامعات المصرية إلى إنشاء كليات جديدة في تخصص الذكاء الاصطناعي، وهو ما يشير إلى أهمية وضع إطار قانوني منظم لهذه التطورات التقنية المستحدثة المتوقع انتشار استخداماتها في كافة مناحي الحياة.

هـ- تسليط الضوء على الأحكام الجنائية الموضوعية والإجرائية ذات الصلة بمكافحة هذه الجرائم.

٥- صعوبات البحث: تتمثل أبرز صعوبات البحث في حداثة هذا التشريع في النظام المصري، فضلاً عن تناثر نصوص مكافحتها في العديد من القوانين المصرية، وهو ما يتطلب وضع إطار عام حاكم لمكافحة هذه الجرائم بشكل متكامل لتحقيق مواجهة فاعلة لها.

٦- منهج البحث: استعان الباحث بالمنهج الوصفي التحليلي الذي يسعى إلى وصف وتحليل وتشخيص موضوع البحث من مُختلف جوانبه وأبعاده، بهدف التوصل إلى نظرة واضحة عن الآليات المُلائمة لمُكافحة هذه الظاهرة الإجرامية المُستحدثة، كما استعان الباحث بمنهج الدراسة المُقارنة، وبصفة خاصة الاتفاقيات الدولية والإقليمية، وخاصة التشريعات العربية بهدف تحديد موقف هذه التشريعات من مُكافحة هذه الطائفة من الجرائم.

٧- خطة البحث: تتضمن خطة البحث تناول موضوع البحث من خلال مبحث تمهيدي وفصلين، حيث نتناول في المبحث التمهيدي: الإطار الدولي والوطني لمكافحة جرائم تقنية المعلومات، ونتطرق في الفصل الأول للأحكام الموضوعية لجرائم تقنية المعلومات، ونستعرض في الفصل الثاني الأحكام الإجرائية لجرائم تقنية المعلومات المصري، وتسير الخطة التفصيلية للبحث على النحو التالي:-

مقدمة عامة.

المبحث التمهيدي: الإطار الدولي والوطني لمكافحة جرائم تقنية المعلومات.

الفصل الأول: الأحكام الموضوعية لجرائم تقنية المعلومات.

الفصل الثاني: الأحكام الإجرائية لجرائم تقنية المعلومات.

الخاتمة والتوصيات.

المبحث التمهيدي

الإطار الدولي والوطني لمكافحة جرائم تقنية المعلومات

أولاً- الإطار الدولي والإقليمي لمكافحة جرائم تقنية المعلومات: حرص المجتمع الدولي على مواجهة جرائم تقنية المعلومات كأمر واقع يستلزم وجود قواعد قانونية دولية متفق عليها لتنظيم مواجهتها، ومن أبرز الصكوك الدولية والإقليمية التي اهتمت بهذه الجرائم الاتفاقية الأوروبية (اتفاقية مجلس أوروبا) بشأن الجريمة السيبرانية لعام٢٠٠١، والبروتوكول الإضافي للاتفاقية المعني بتجريم أفعال ذات طبيعة عنصرية أو كراهية الأجانب المرتكبة بواسطة النظم الحاسوبية، وقراري الاتحاد الأوروبي لعام ٢٠٠١ بشأن الاحتيال والتزوير في وسائط الدفع غير النقدية، ولعام ٢٠٠٥ بشأن الهجمات ضد نظم المعلومات، والمشروع التوجيهي للاتحاد الأوروبي لعام ٢٠١٠ بشأن الهجمات ضد نظم المعلومات، وتوجيه الاتحاد الأوروبي لعام ٢٠١١ بشأن مكافحة الاعتداء الجنسي والاستغلال الجنسي للأطفال واستغلال الأطفال في المواد الإباحية.

فضلاً عن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠، والقانون العربي النموذجي لمكافحة جرائم تقنية أنظمة المعلومات لعام ٢٠٠٤ (قانون الإمارات النموذجي)، ومشروع اتفاقية الاتحاد الأفريقي بشأن إنشاء إطار قانوني للمساعدة في الأمن السيبراني في أفريقيا لعام ٢٠١٢، ومشروع القانون النموذجي للكوميسا (السوق المشتركة لشرق وجنوب أفريقيا) لعام ٢٠١١ بشأن الأمن السيبراني، والمشروع التوجيهي للإيكواس (الجماعة الاقتصادية لدول غرب أفريقيا) لعام ٢٠٠٩ بشأن مكافحة الجريمة السيبرانية داخل دول غرب أفريقيا.

علاوة على البروتوكول الاختياري الملحق باتفاقية حقوق الطفل لعام ٢٠٠٠ بشأن بيع الأطفال وبغاء الأطفال واستغلال الأطفال في المواد الإباحية، والنصوص التشريعية النموذجية لعام ٢٠١٠ بشأن الجرائم السيبرانية والأدلة الإلكترونية للإتحاد الدولي للاتصالات والجماعة الكاريبية والاتحاد الكاريبي للاتصالات، واتفاقية كومنولث الدول المستقلة بشأن التعاون في مكافحة الجرائم المتعلقة بالمعلومات الحاسوبية واتفاقية منظمة شنغهاي للتعاون في مجال أمن المعلومات الدولية.

ومن الجدير بالذكر أنه حتى كتابة هذه السطور لم تنجح مساعي منظمة الأمم المتحدة للوصول إلى اتفاقية أممية لمكافحة جرائم تقنية المعلومات، على غرار الاتفاقيات النظيرة لمكافحة الجريمة المنظمة عبر الوطنية ومكافحة الفساد وغير ذلك من الاتفاقيات الأممية، وهو ما يرى الباحث وجوب سعي المجتمع الدولي إلى صياغة صك دولي أممي لمواجهة هذه الطائفة الخطيرة من الجرائم.

علاوة على ذلك هناك من ينادي بضرورة العمل على تعديل الاتفاقية الأوروبية بشأن الجريمة السيبرانية لوضع قواعد قانونية تنظم التطورات الحادثة في مجال تكنولوجيا المعلومات ومن أبرزها انترنت الأشياء ونظم الذكاء الاصطناعي[1].

---

[1] يقصد بإنترنت الأشياء الجيل الجديد من الإنترنت الذي يتيح التفاهم بين الأجهزة المترابطة مع بعضها (عبر بروتوكول الإنترنت)، وتشمل هذه الأجهزة الأدوات والمستشعرات والحساسات وأدوات الذكاء الاصطناعي المختلفة وغيرها. ويتخطى هذا التعريف المفهوم التقليدي وهو تواصل الأشخاص مع الحواسيب والهواتف الذكية عبر شبكة عالمية واحدة ومن خلال بروتوكول الإنترنت التقليدي المعروف، وما يميز إنترنت الأشياء أنها تتيح للإنسان التحرر من المكان، أي أن الشخص يستطيع التحكم في الأدوات من دون الحاجة إلى التواجد في مكان محدد للتعامل مع جهاز معين. بينما يقصد بالذكاء الاصطناعي تزويد الحاسب الآلي ببرامج وإمكانيات تشبه ذكاء البشر وذلك لجعل الحاسب قادراً على القيام بعمليات ذكية. انظر: د. محمد محمد طه خليفة: الذكاء الاصطناعي في ميزان التشريع، مجلة دبي القانونية، النيابة العامة بدبي، العدد ٢٨، مارس ٢٠١٨، دبي، دولة الإمارات العربية المتحدة، ص٣١.

موقف التشريع المقارن من جرائم تقنية المعلومات: تبرز الإشارة إلى اختلاف موقف التشريعات المقارنة بشأن هذه الجرائم ما بين اتجاهين:

(الأول) أفرد تشريعات مستقلة بمكافحة جرائم تقنية المعلومات كالتشريع السويدي لعام ١٩٧٣، الأمريكي، الإنجليزي، الكندي، الدنماركي، السويسري، الألماني، الياباني، المجري والبولندي، ومن التشريعات العربية، نذكر التشريع الإماراتي، البحريني، الكويتي، العماني والقطري[١]والسوداني، والنظام السعودي[٢]، ويشار في هذا السياق، إلى أن مثل هذه القوانين الخاصة لمكافحة جرائم تقنية المعلومات هي قوانين مكملة أو تكميلية لقانون العقوبات[٣].أما الجانب الآخر من التشريعات فهي التي أدرجت نصوص مكافحة جرائم تقنية المعلومات في إطار مدونتها العقابية، ونذكر منها على سبيل المثال التشريع الفرنسي (المواد ٣٢٣-١ حتى ٣٢٣-٧ عقوبات فرنسي) والتشريع والفنلندي والنرويجي، ومن التشريعات العربية التشريع الجزائري (المواد ٣٩٤مكرر عقوبات جزائري وما بعدها).

---

(١) تبرز الإشارة إلى أن كلاً من التشريعين العماني والقطري كانا ينصان على تجريم الجرائم المعلوماتية في إطار المدونة العقابية، حيث كان التشريع العماني يجرم الجرائم المعلوماتية بموجب المواد أرقام (٢٧٦مكرر-٢٧٦مكرر٤ عقوبات عماني)، بينما كان التشريع القطري ينص على جرائم الحاسب الآلي بالفصل الخامس من قانون العقوبات القطري رقم (١١) لعام ٢٠٠٤ بموجب المواد أرقام (٣٧٠-٣٨٧) عقوبات، إلا أنهما قد تحولا عن هذا الاتجاه، من خلال إصدارهما لتشريع خاص لمكافحة الجرائم المعلوماتية.

(٢) يعاقب على الجرائم المعلوماتية بدولة الإمارات العربية المتحدة بموجب القانون الاتحادي رقم (٥) لسنة ٢٠١٢ المعدل للقانون الاتحادي رقم (٢) لسنة ٢٠٠٦ بشأن مكافحة الجرائم المعلوماتية، بينما يعاقب على الجرائم المعلوماتية في النظام السعودي نظام مكافحة الجرائم المعلوماتية الصادر بموجب المرسوم الملكي رقم (م/ ١٧)، وفي دولة السودان القانون رقم (٢) لسنة ٢٠٠٧ بشأن مكافحة الجرائم المعلوماتية، وفي دولة البحرين القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات، وفي دولة الكويت القانون (٦٣) لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات.

(٣) د. حسني الجندي: التشريعات الجنائية الخاصة في دولة الإمارات العربية المتحدة، الكتاب الثالث- قانون مكافحة جرائم تقنية المعلومات في دولة الإمارات العربية المتحدة، ط١، ٢٠٠٩، ص ص٤، ٥.

وقبل ترك الحديث في هذه المسألة، تبرز الإشارة إلى أن المشرع المصري لم يكن ببعيد عن مكافحة جرائم تقنية المعلومات، وإنما عمل -قبل إقراره للقانون- على الإشارة في بعض القوانين المتفرقة إلى تجريم بعض الصور لهذه الجرائم، ومن بين هذه القوانين: قانون الأحوال المدنية رقم (١٤٣) لسنة ١٩٩٤، والقانون رقم (١٢٦) لسنة ٢٠٠٨، وقانون التوقيع الإلكتروني رقم (١٥) لسنة ٢٠٠٤، وقانون حماية الملكية الفكرية رقم (٨٢) لسنة ٢٠٠٢ وقانون الاتصالات رقم (١٠) لسنة ٢٠٠٣، وقانون المحاكم الاقتصادية رقم (١٢٠) لسنة ٢٠٠٨ وأخيراً قانون مكافحة الإرهاب المصري الجديد رقم (٩٤) لسنة ٢٠١٥.

موقف التشريع المصري: تبرز الإشارة إلى أن من أبرز أسباب تناول هذا الموضوع بالمدارسة والتحليل من جانب الباحث اعتقاده بتأخر المشرع المصري في إصدار قانون لمكافحة جرائم تقنية المعلومات، ليس فقط بالنسبة للتشريعات المقارنة التي استقى منها أحكامه العقابية كالتشريع الفرنسي على سبيل المثال، وإنما أيضاً بالنسبة لجانب من التشريعات العربية التي كانت قد اقتبست من تشريعنا العقابي غالبية نصوصها الجنائية، إلا وأنها في مجال مكافحة جرائم تقنية المعلومات، فإنها قد سبقت المشرع المصري، ونذكر منها على سبيل المثال بعض التشريعات الخليجية كالتشريع الإماراتي والقطري والكويتي والبحريني.

وقد حرص المشرع المصري على معالجة هذا القصور بإصدار قانون لمكافحة جرائم تقنية المعلومات برقم (١٧٥) لسنة ٢٠١٨، والذي ارتكز على فلسفة تشريعية تستهدف مواكبة التشريع المصري للتغيرات المتلاحقة التي تشهدها الساحة من ظهور أنماط جديدة من الجرائم المرتبطة بالتطورات التكنولوجية في وسائل الاتصالات، وتحقيق التوازن بين الحماية الجنائية لحرمة الحياة الخاصة التي يكفلها الدستور والمحافظة على المعلومات وكفالة سريتها وعدم إفشائها أو التنصت عليها إلا بأمر

قضائي مسبب، وبين مواجهة تلك الجرائم والأفعال ومكافحتها والحد من آثارها[١].

الغايات التي استهدفها المشرع المصري من إصدار قانون مكافحة جرائم تقنية المعلومات: أشارت المذكرة الإيضاحية للقانون إلى أن إعداد هذا القانون توخى الأهداف الآتية[٢]:-

١-مكافحة الاستخدام غير المشروع للحاسبات وشبكات المعلومات، وتقنيات المعلومات وما يرتبط بها من جرائم، مع التزام الدقة في تحديد الأفعال المعاقب عليها، وتجنب التعبيرات الغامضة بوضع تعاريف دقيقة لها، وتحديد عناصر الأفعال المجرمة بكثير من العناية، ومع الاعتبارات المتعلقة بالمصلحة العامة وحماية الأمن والاقتصاد القوميين.

---

(١) أشارت المذكرة الإيضاحية للقانون إلى أن التطور المستمر في نظم معالجة البيانات والمعلومات الآلية وتخزينها وتبادلها وتخليقها وتطويرها، وتعدد المواقع والحسابات الخاصة والاتساع المطرد في استخدام البريد الإلكتروني والأجهزة والمعدات التقنية، إلى جانب التطور المذهل في وسائل الاتصال المعلوماتي، أوجد حاجة ملحة وضرورية لإصدار هذا القانون بهدف تحقيق التوازن بين الحماية الجنائية لحرمة الحياة الخاصة التي يكفلها الدستور والمحافظة على المعلومات وكفالة سريتها وعدم إفشائها أو التنصت عليها إلا بأمر قضائي مسبب، وبين مواجهة تلك الجرائم والأفعال ومكافحتها والحد من آثارها، وأن شبكة الإنترنت وما أوجدته من أفاق رحبة أمام الأشخاص جعلت من العالم كله قرية صغيرة، نتيجة تدفق وانسياب المعلومات وكثافتها الهائلة بشكل غير مسبوق. كما تضيف المذكرة الإيضاحية للقانون أن شبكة الإنترنت فتحت آفاقاً رحبة أمام الأشخاص، حيث سمحت لهم على اختلاف مواقعهم وتباعدهم، وعلى اختلاف ثقافاتهم ولغاتهم وجنسياتهم بالدخول إليها وتبادل المعلومات بحرية دون أدنى تقيد بالحدود الجغرافية بين الدول، ودون أدنى نظر إلى مستوى تلك الدول التقني رقياً أو انحداراً حتى قيل -وبحق- أن العالم كله قد أصبح من الناحيتين: التقنية والمعلوماتية قرية واحدة صغيرة، نتيجة تدفق وانسياب المعلومات وكثافتها الهائلة بشكل غير مسبوق. انظر: مضبطة مجلس النواب المصري، الجلسة ٥٦، المعقودة في ٢٠١٨/٥/١٤م، مرجع سابق، ص٤١.

(٢) انظر: مضبطة مجلس النواب المصري، الجلسة ٥٦، مرجع سابق، ص ص٤١، ٤٢.

٢- ضبط الأحكام القضائية الخاصة بجمع الأدلة الإلكترونية وتحديد حجيتها في الإثبات[١].

---

[١] لم يقف القضاء المصري مكتوف الأيدي بالنسبة لمسألة القصور التشريعي بشأن تجريم الجرائم المعلوماتية، وإنما عمل على تفسير النصوص الجنائية، بما أتاح المعاقبة على الجرائم التقليدية التي ترتكب بالوسائل المستحدثة بالنظر إلى أن القانون لا يعتد بالوسيلة التي يتحقق بها السلوك المجرم، ومن أبرز الأمثلة التي تشير إلى ذلك، موقف محكمة النقض من الجرائم الإرهابية التي ترتكب باستخدام نظم المعلومات، حيث يشير البعض إلى موقف مرن من جانب محكمتنا العليا عبرت به عن إدراكها لمفهوم الإرهاب الإلكتروني أو الجريمة الإرهابية الإلكترونية في ضوء النصوص الخاصة بالإرهاب بقانون العقوبات قبيل صدور قانوني مكافحة الإرهاب رقم ٩٤ لـ٢٠١٥ وقانون مكافحة جرائم تقنية المعلومات رقم ١٧٥لـ٢٠١٨، لتظهر قدراً من سعة الأفق يتجاوز النص القاصر في حينه، حيث قضت بأنه:" السلوك الإجرامي في جريمة الإرهاب يتخذ شكل العنف بمعناه الواسع بما يشير إليه من معانٍ مختلفة تتضمن استخدام القوة أو التهديد أو الترويع بها على النحو الذي حدده القانون، ويتسع هذا المعنى إلى الصور التي خلفتها التكنولوجيا الحديثة فلا يقف عند المعنى المادي للعنف، فيعتبر من قبيل العنف المكون للإرهاب استخدام نظم المعلومات لأغراض إرهابية". انظر: الطعن رقم ١٤٠٨٨ لسنة ٨٦ق، بتاريخ ٢٠١٧/٣/١١، مشار إليه د. أحمد الضبع: إشكاليات مواجهة الإرهاب بين النظرية والتطبيق، موسوعة الثقافة القانونية، الهيئة المصرية العامة للكتاب، ط١، ص٨٥.

<u>وفي اتجاه آخر</u>، اعتدت محكمة النقض بسريان وصف المحرر في جريمة التزوير على بطاقات الائتمان الممغنطة باعتبارها من أوراق البنوك، وأن تزوير بطاقات الائتمان الممغنطة الخاصة ببنك تساهم الدولة بنصيب في رأس ماله يشكل جناية التزوير في محررات شركة مساهمة تشارك الدولة في مالها بنصيب.انظر: الطعن رقم ٣٩٥٠٥ لسنة ٧٧ق، جلسة ٢٠١٦/٣/١٥،النشرة التشريعية والقانونية لمحكمة النقض،الصادرة عن المكتب الفني لمحكمة النقض،إصدار يوليو وأغسطس وسبتمبر ٢٠١٦، ص ص١٢٧، ١٢٨.

<u>وفي حكم آخر</u>، أدانت إحدى المحاكم الاقتصادية أحد الأشخاص لقيامه باستخدام تطبيق الواتس آب والحساب الخاص على مواقع التواصل الاجتماعي الفيسبوك في إرسال رسائل للمجني عليه تتضمن ألفاظ سب تمثل خدشاً للشرف الاعتبار، بالنظر إلى أن استخدام التطبيقات الحديثة للتواصل المثبتة على التليفون كتطبيق الواتس آب ما تتحقق به الجرائم التقليدية كجريمتي السب العلني بطريق التليفون وجريمة تعمد إزعاج ومضايقة الغير بإساءة استعمال أجهزة الاتصالات الواردة في قانوني العقوبات والاتصالات رقم ١٠ لـ٢٠٠٣، وقد أشار الحكم المذكور إلى أن استخدام مواقع التواصل الاجتماعي (الإلكترونية) ومن بينها موقع فيسبوك، يتم من خلال إنشاء حساب إلكتروني عن طريق خدمة البريد الإلكتروني التي تتيحها شبكة الإنترنت، وهي شبكة تتألف من مئات =

٣- وضع القواعد والأحكام والتدابير اللازم اتباعها من قبل مقدمي الخدمة لتأمين خدمة تزويد المستخدمين بخدمات التواصل بواسطة تقنية المعلومات، وتحديد التزاماتهم في هذا الشأن.

٤- حماية 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 كانت.

٥- حماية البيانات والمعلومات الشخصية، من استغلالها استغلالاً يسئ إلى أصحابها، خاصة في ظل عدم كفاية النصوص التجريمية التقليدية المتعلقة بحماية خصوصية الأفراد وحرمة حياتهم الخاصة في مواجهة التهديدات والمخاطر المستحدثة لاستخدام تقنية المعلومات.

=

الحاسبات الآلية المرتبطة ببعضها البعض عن طريق خطوط التليفون أو عن طريق الأقمار الصناعية، وأن تحقيق الاتصال بالشبكة يتطلب وجود جهاز حاسب آلي مزود بجهاز مودم يرتبط بخط الهاتف، لتلقي وإرسال البيانات عبر مزود الخدمة. انظر: حكم محكمة طنطا الاقتصادية في القضية رقم ١٠٩٩ لسنة ٢٠١٨ جنح طنطا الاقتصادية، جلسة ٢٠١٨/٨/٣٠م.

وفي قضية أخرى اتهمت النيابة العامة أحد الأشخاص لقيامه باستغلال البريد الإلكتروني لزوجته في إرسال رسائل إلكترونية للمجني عليها تضمنت تهديداً بإفشاء أمور خاصة بها ونسبة أمور أخرى لها مخدشة للشرف، وقد كان ذلك التهديد مصحوباً بطلب هو الامتناع عن الذهاب إلى أحد المصانع، وكذلك بتكليف بأمر وهو سداد ما يشغل ذمتها، كما تضمن ذلك ألفاظاً تعد سب في حقها، وقد اعتبرت النيابة العامة أن هذه الأفعال شكلت تعمداً لإزعاج المجني عليها بإساءة استعمال أجهزة الاتصالات، وطلبت عقابهم عملاً بالمواد ٣٠٦، ٣٠٨، ٣٢٧ من قانون العقوبات و١، ٤/٥، ٦، ٧/١٣، ٧٠، ٧٦ من القانون رقم ١٠ لسنة ٢٠٠٣ بشأن تنظيم الاتصالات. انظر: حكم محكمة جنايات القاهرة الاقتصادية في القضية رقم ٦٨٧٧ لسنة ٢٠١١ جنايات المرج، جلسة ٢٠١٤/٢/٤م، مشار إليه المستشار د. محمد سمير: قانون العقوبات الاقتصادي، نادي القضاة، ط١، ٢٠١٩، ص١٨٨. والواقع أن ما سبق يشير بشكل جلي إلى النهج المحمود من القضاء المصري في إعمال النصوص الجنائية على الوسائل التكنولوجية والمستحدثة التي تستخدم في ارتكاب الجرائم التقليدية.

٦- وضع تنظيم إجرائي دقيق ينظم إجراءات الضبط والتحقيق والمحاكمة المتعلقة بتلك الجرائم، بالإضافة إلى تحديد حالات التصالح وإجراءاته وتنظيم عمل الخبراء المتخصصين العاملين في مجال مكافحة تقنية المعلومات، والقرارات والأوامر الجنائية المتعلقة بتنفيذ أحكام القانون.

مدى الحاجة إلى إدراج مادة للتعاريف ذات الصلة بقانون مكافحة جرائم تقنية المعلومات؟ نظراً للطابع الخاص بجرائم تقنية المعلومات وقيامها على مصطلحات غريبة أو مستحدثة في مجال القانون الجنائي، فقد اتجهت العديد من التشريعات المقارنة والمواثيق الدولية والإقليمية على تضمين تشريعات مكافحة جرائم تقنية المعلومات إشارة إلى التعاريف التشريعية للمصطلحات المرتبطة بها[١].

وقد تضمن قانون مكافحة جرائم تقنية المعلومات عدداً من التعاريف ذات الصلة بجرائم تقنية المعلومات، وتبرز أهمية تصدي القانون لوضع تعريفات محددة لهذه المصطلحات بالنظر إلى أن وضوح النصوص الجنائية قد يتطلب إدراج تعاريف للمفاهيم ذات الصلة بجرائم تقنية المعلومات، فحداثة هذا النوع من الجرائم يتطلب وصف دقيق للمفاهيم المحيطة بها، لتفهم طبيعة الأشياء والمصالح القانونية التي تحظى بالحماية[٢]، وصفوة القول أن المشرع المصري حرص على وضع تعريفات

---

[١] أشارت المذكرة الإيضاحية للقانون أن المادة الأولى منه تناولت تعريف المصطلحات الواردة بالقانون، والتي جاءت في قائمة مطولة، نظراً لكون معظم هذه المصطلحات غير متداولة بصورة واسعة خاصة بمنطوقها في اللغة العربية خارج دائرة المتخصصين أو تداوله بمفاهيم غير واضحة وغامضة، وبعضها قصد من إيراده في التعريف توحيد مفهومها في نطاق تطبيق هذا القانون. انظر: مضبطة مجلس النواب المصري، الجلسة ٥٦، المعقودة في ٢٠١٨/٥/١٤م، مرجع سابق، ص٤٢.

[٢] انظر دراسة مكتب الأمم المتحدة حول الجريمة السيبرانية، مرجع سابق، ص١٨.

محددة لكافة المصطلحات القانونية المستحدثة ذات الصلة بجرائم تقنية المعلومات[١]، بالنظر إلى أن وضوح النصوص الجنائية – كما سبق أن أشرنا- قد يتطلب وصفاً دقيقاً للمفاهيم المحيطة بهذه الجرائم، لتفهم طبيعتها والمصالح القانونية المرتبطة بها.

تعريف جرائم تقنية المعلومات[٢]: تبرز أهمية وضع تعريف لجريمة تقنية المعلومات في وضع إطار محدد لهذه الجرائم، والذي يشمل العديد والعديد من الصور الإجرامية، وعلى الرغم من خلو القانون من تعريف لجريمة تقنية المعلومات، إلا أن تقرير اللجنة المشتركة من لجنة الاتصالات وتكنولوجيا المعلومات ومكتب لجنتي الشئون الدستورية والتشريعية والدفاع والأمن القومي عن مشروع قانون مكافحة جرائم تقنية المعلومات أشار إلى أن جرائم تقنية المعلومات هي الجرائم التي تكون المعلومات إما محلاً لها أو أداة في ارتكابها[٣].

وقد خلت غالبية الصكوك الدولية والإقليمية والتشريعات المقارنة من تعريف للجريمة المعلوماتية، اللهم بعض التشريعات التي حرصت على وضع تعريف محدد لها،

---

(١) ومن جانب آخر يتضح لنا تشابه التعاريف التي أخذت بها غالبية التشريعات العربية مع بعضها البعض اتساقاً مع التعاريف الواردة بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠.

(٢) تبرز الإشارة إلى تباين موقف التشريعات المقارنة بشأن تسمية جرائم تقنية المعلومات أو الجرائم المعلوماتية، فهناك جانب من التشريعات يسميها جرائم الحاسب الآلي كالتشريع السوداني والسريلانكي والماليزي، وجانب آخر يسميها جرائم تكنولوجيا المعلومات كالتشريع السعودي والهندي والفنزويلي والفيتنامي، وثالث يسميها جرائم التكنولوجيا المتقدمة كالتشريع الصربي، وأخيراً جرائم الاتصالات الالكترونية كالتشريع الفرنسي والألباني. انظر في تفصيلات ذلك دراسة مكتب الأمم المتحدة المعني بالمخدرات والجريمة حول الجريمة السيبرانية، مرجع سابق، ص١٧.

(٣) انظر: مضبطة مجلس النواب المصري، الجلسة السادسة والخمسين، المعقودة في ٢٠١٨/٥/١٤م، مرجع سابق، ص٣٩.

نذكر منها على سبيل المثال التشريع السعودي[١] والكويتي[٢] والأمريكي[٣]، ويعنينا في هذا المقام الحديث عن تبنى مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين تعريفاً جامعاً للجرائم المعلوماتية، حيث عرفها بأنها:" أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"، كما تبنى مكتب الأمم المتحدة المعنى بالمخدرات والجريمة مؤخراً تعريفاً للجريمة المعلوماتية بأنها:" الجرائم التي تمس بسرية البيانات أو النظم الحاسوبية وسلامتها وتوافرها، بالإضافة إلى الجرائم المنفذة بواسطة الحواسيب والرامية إلى تحقيق مكاسب شخصية أو مالية أو إحداث أضرار؛ بما في ذلك أشكال الجرائم المتصلة بالهوية وبمحتوى الحواسب الآلية"[٤].

بينما لم تشر مدونة الأمم المتحدة بشأن الجرائم المعلوماتية إلى توصل الخبراء الدوليين إلى تعريف مُحدد لها، كما أن اللجنة الأوروبية لمشاكل الجريمة التابعة للمجلس الأوروبي عام ١٩٨٩ لم تشر في الإرشادات العامة بشأن الجرائم

---

(١) عرف نظام مكافحة جرائم المعلوماتية السعودي الجريمة المعلوماتية بأنها:" أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام"(م١).

(٢) عرف التشريع الكويتي الجريمة المعلوماتية بأنها: "كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون".

(٣) عرف التشريع الأمريكي رقم (١٢١٣) لسنة ١٩٨٦ جرائم الكمبيوتر بأنها:" الاستخدام غير المصرح به لأنظمة الكمبيوتر المحمية أو ملفات البيانات أو الاستخدام المتعمد الضار لأجهزة الكمبيوتر أو ملفات البيانات، وتتراوح خطورة تلك الجريمة ما بين جنحة من الدرجة الثانية إلى جناية من الدرجة الثالثة".

(4) Comprehensive Study on Cybercrime, United Nations Office of Drugs and Crime, Draft February 2013, Published by UNODC, New York,2013, pp.11-12.

المعلوماتية وتصنيفاتها إلى تعريف أوروبي موحد، وتركت ذلك للدول المعنية. وتذهب دراسة مكتب الأمم المتحدة حول الجريمة السيبرانية إلى مسار مختلف، حيث ترى أنه من الأفضل اعتبار الجريمة السيبرانية كمصطلح قانوني قائم بذاته، كما هو الوضع في تعريف الفساد، ومن ثم يكون من الأفضل اعتبارها بمثابة مجموعة من الأفعال أو السلوك التي تلزم الدول بتجريمها في إطار جرائم تقنية المعلومات[١].

وتبرز الإشارة إلى اختلاف الفقه بين مدلولين يخصان جرائم تقنية المعلومات هما جرائم الحاسب الآلي وجرائم الانترنت أو الجرائم السيبرانية، حيث يرى الاتجاه الأول أن الجرائم السيبرانية أوسع نطاقاً من جرائم الحاسب الآلي، فالأخيرة تقتصر على الجرائم المرتكبة دون الولوج إلى شبكة الانترنت، كالجرائم الماسة بسرية البيانات أو الأنظمة المعلوماتية وسلامتها وتوافرها، بينما الأولى تشمل نطاقاً أوسع من الجرائم المرتكبة وفقاً لما توفره شبكة الإنترنت من فرص للمجرمين لارتكاب جرائم جديدة، كالجرائم المرتكبة بدافع مالي والجرائم المتصلة بالمحتوى الحاسوبي، بينما يرى الرأي الآخر أن جرائم الحاسب الآلي تتسع لتشمل جرائم الانترنت بالنظر إلى استخدام الحاسبات الآلية في ارتكاب هذه الجرائم، فالأخيرة تتطلب وجود شبكة المعلومات، ومن ثم يخرج من نطاقها الجرائم المرتكبة التي يستخدم في ارتكابها أنظمة معلوماتية مستقلة بذاتها، والأوقع لدينا عدم أهمية هذه التفرقة بالنظر إلى أن مدلول جرائم تقنية المعلومات يتسع ليشمل المدلولين.

---

[١] انظر دراسة مكتب الأمم المتحدة حول الجريمة السيبرانية، مرجع سابق، ص١٨.

الفصل الأول

الأحكام الموضوعية لجرائم تقنية المعلومات

تمهيد وتقسيم: حدد الباب الثالث من القانون الجرائم المرتكبة والعقوبات المُوقعة، فى تسعة فصول، حيث تناول القانون جرائم الاعتداء على سلامة الشبكات وأنظمة وتقنيات المعلومات، والجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات، والجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتى غير المشروع، والجرائم المرتكبة من مقدم الخدمة، وهو ما سوف نعرض له في ستة مباحث، وذلك على النحو التالي:-

المبحث الأول

جرائم الاعتداء على سلامة الشبكات ونظم المعلومات

تقسيم: تضمن الفصل الأول الخاص بجرائم الاعتداء على سلامة الشبكات وأنظمة وتقنيات المعلومات، تجريم الانتفاع غير المشروع بخدمة معلوماتية، وتجاوز الحق في الولوج لموقع أو حساب أو نظام معلوماتي، والولوج أو البقاء غير المشروع لموقع أو حساب أو نظام معلوماتي، والدخول أو البقاء غير المشروع أو تجاوز الحق في الولوج لموقع أو حساب أو نظام معلوماتي يخص الدولة أو أحد الأشخاص الاعتبارية العامة، والاعتراض غير المشروع للبيانات والمعلومات، والاعتداء على سلامة الأنظمة المعلوماتية، والاعتداء على موقع أو حساب خاص أو بريد إلكتروني لآحاد الناس، والاعتداء على تصميم المواقع الإلكترونية، والاعتداء على سلامة الشبكة المعلوماتية، وتجريم حيازة وإحراز والاتجار غير المشروع في أجهزة أو معدات تستخدم في ارتكاب أو تسهيل الجرائم المعلوماتية، وهو ما سنتناوله في عشرة مطالب على النحو التالي:-

المطلب الأول

جريمة الانتفاع غير المشروع بخدمات الاتصالات

وقنوات البث المسموع والمرئي

نص التجريم: أشارت المادة (١٣) إلى جريمة الانتفاع بدون حق بخدمات الاتصالات والمعلومات وتقنيتها، حيث تقضي المادة المذكورة بأنه:" *يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من انتفع بدون وجه حق عن طريق شبكة النظام المعلوماتي، أو إحدى وسائل تقنية المعلومات بخدمة اتصالات أو خدمة من خدمات قنوات البث المسموع أو المرئي*"[1].

العلة من التجريم: ترجع العلة من التجريم في حرص المشرع المصري على توفير الحماية لأصحاب حقوق خدمات الاتصالات وخدمات البث، من الأضرار المادية الواقعة عليهم من أعمال القرصنة الإلكترونية.

محل الجريمة: تطلب القانون أن يقع الانتفاع على خدمة من خدمات الاتصالات أو خدمات قنوات البث التليفزيوني أو الإذاعي، ومن صور خدمات الاتصالات تمرير الاتصالات الدولية أو المكالمات التليفونية عبر شبكة الإنترنت، وذلك باستخدام برامج خاصة عبر أجهزة الحاسب الآلي أو الأقمار الصناعية، ويقصد بالاتصالات أو المكالمات

---

[1] ومن التشريعات العربية التي حرصت على تجريم الانتفاع غير المشروع بخدمات الاتصالات وقنوات البث المسموع والمرئي التشريع الإماراتي (م٣٤)، بينما تضمن قانون الاتصالات رقم (١٠) ٢٠٠٣ تجريم أفعال إنشاء وتشغيل شبكات الاتصال وتقديم خدمات الاتصال وتمرير المكالمات بدون الحصول على ترخيص(م٧٢).

التليفونية الاتصال الصوتي بين طرفين، سواء تم هذا الاتصال سلكياً أو لاسلكياً[١]، ويكون الاتصال دولياً إذا عبر الحدود الجغرافية لمصر إلى أي دولة أخرى أو مكان خارجها وأن يتم ذلك من خلال المعابر الدولية للاتصالات، والتي قد تأخذ شكل الكابلات البحرية أو الأرضية أو وصلات الميكروويف أو الأقمار الصناعية أو غيرها من التكنولوجيا التي تتحقق من خلالها الاتصالات الدولية[٢]، أما أمثلة الاعتداء على خدمات البث الإذاعي والتليفزيوني نقل المباريات أو القنوات التليفزيونية أو الإذاعية المشفرة.

الركن المادي: يتحقق الركن المادي في هذه الجريمة من عنصرين:-

أ) الحصول على منفعة: يتحقق الركن المادي في هذه الجريمة بكل فعل إيجابي من شأنه حصول الجاني على منفعة، ويستوي لدى القانون أن يكون تحقق المنفعة للجاني نفسه أم للغير. ومن صور السلوك الإجرامي قيام الجاني بأي وسيلة من الوسائل التقنية بتمرير المكالمات التليفونية الدولية، من خلال الإرسال إلى خارج النطاق الجغرافي للحدود المصرية إلى دول أو أماكن أخرى أو الاستقبال داخل هذا النطاق الجغرافي بدون ترخيص بذلك من الجهة المختصة وهي الجهاز القومي لتنظيم الاتصالات، وذلك بإعداد المكان المناسب وتزويده بالأجهزة والمعدات السلكية واللاسلكية التي يكون من شأنها إرسال أو استقبال الاتصال الدولي، ثم توصيله على أحد الخطوط التليفونية المحمولة مما يترتب عليه وصول المكالمات التليفونية الدولية أو إرسالها بعيداً عن الشبكة الدولية

---

[١] المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٥١٠.

[٢] انظر: حكم محكمة جنح مستأنف القاهرة الاقتصادية، جلسة ٢٠١٣/٤/٨، الدعوى رقم ٢٠٤ لسنة ٢٠١٢ جنح مستأنف القاهرة الاقتصادية، مشار إليها: المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٥١٦، هامش رقم ١.

للشركة المصرية للاتصالات[١].

وسيلة ارتكاب الجريمة: تطلب القانون أن يكون التحصل على المنفعة بوسيلة معينة، وهي أن يكون ذلك عن طريق إحدى وسائل تقنية المعلومات أو الشبكة المعلوماتية، ومن ثم تتحقق الجريمة إذا استخدم الجاني برامج لالتقاط خدمات الاتصالات أو تمريرها، أو برامج لفك التشفير الخاص بقنوات البث التليفزيوني والإذاعي، بغرض الحصول على خدمات الاتصالات أو خدمات قنوات البث التليفزيوني أو الإذاعي، وكان القانون قد عرف الشبكة المعلوماتية بأنها:"مجموعة من الأجهزة أو نظم المعلومات تكون مرتبطة معاً، ويمكنها تبادل المعلومات والاتصالات فيما بينها، ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية،والتطبيقات المستخدمة عليها"، بينما عرف تقنية المعلومات بأنها:" أي وسيلة أو مجموعة وسائل مترابطة أو غير مترابطة تُستخدم لتخزين واسترجاع وترتيب وتنظيم ومعالجة وتطوير وتبادل المعلومات أو البيانات، ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة سلكياً أو لاسلكياً"[٢].

---

[١] ومن أبرز قضايا تمرير المكالمات الدولية التي قضت فيها محكمة القاهرة الاقتصادية، قضية تخابر لمصلحة دولة أجنبية بقصد الإضرار بالمصالح القومية بالبلاد لصالح إحدى أجهزة المخابرات، من خلال قيام المتهم الأول ويعمل مهندس اتصالات متخصصاً في الأقمار الصناعية والشبكات بتمرير المكالمات الدولية المصرية الواردة للبلاد عبر الإنترنت الخاص بدولة أجنبية بغرض السماح لأجهزة الأمن لديها بالتنصت على تلك المكالمات والاستفادة بما تتضمنه من معلومات مما يضر بالأمن القومي المصري ويعرضه للخطر. انظر: حكم محكمة جنح القاهرة الاقتصادية جلسة ٢٠١٢/٥/٢٠، الدعوى رقم ٥٩ لسنة ٢٠١٢ جنح اقتصادي، انظر في تفصيلات هذه القضية: المستشار د. محمد سمير: قانون العقوبات الاقتصادي: مرجع سابق، ص ص٥١١-٥١٦.

[٢] ومن التشريعات المقارنة التي تضمنت تعريف لتقنية المعلومات التشريع البحريني والإماراتي والكويتي والسوداني.

تساؤل: هل الضرر عنصر من عناصر الركن المادي؟ لم يشر المشرع إلى تطلب عنصر الضرر في الجريمة لتحققها، ولكن الضرر في الجريمة مفترض بمجرد تحقق الانتفاع، بالنظر إلى هذه الخدمات تقوم بالمال لصالح الجهات المزودة بهذه الخدمات، ومن ثم فإن تحصل الجاني على خدمات الاتصال أو البث الإذاعي أو التليفزيوني دون الرجوع إلى الجهة صاحبة حقوق البث أو الاتصالات، من شأنه الإضرار بتلك الجهات المزودة بهذه الخدمات، نظراً لعدم قيام الجاني بالحصول على موافقة هذه الجهات، أو سداد مقابل الاستفادة بهذه الخدمات لها، ومن جانب آخر تبرز الإشارة إلى أن القانون لم يشترط تحقق الضرر لصاحب حقوق خدمات الاتصالات أو البث، ومن ثم تتحقق الجريمة سواء ترتب على الانتفاع ضرر لمقدم الخدمة أم لا.

ب) أن يكون الانتفاع بدون وجه حق: يتطلب القانون لتحقق الركن المادي في هذه الجريمة أن يكون الانتفاع بدون وجه حق، ويكون ذلك إذا كان هذه الانتفاع مخالفاً لشروط توفير خدمات الاتصالات أو البث، أو المخالفة للحقوق الاقتصادية لأصحاب حقوق خدمات الاتصالات والبث. ومن التطبيقات القضائية لهذه الجريمة قيام الجاني بتشغيل شبكة اتصالات لقنوات تليفزيونية مشفرة دون ترخيص ودون إذن من المؤلف وأصحاب الحقوق المجاورة[1].

الركن المعنوي: هذه الجريمة من الجرائم العمدية التي يتحقق فيها الركن المعنوي بتوافر القصد الجنائي العام بعنصريه العلم والإرادة.

أ) العلم: يجب أن يكون الجاني عالماً بأن من شأن فعله الانتفاع بخدمة من خدمات

[1] انظر: الطعن رقم ١١٨٦٥ لسنة ٨٠ ق جلسة ٢٠١١/١١/٢٨، مجموعة المبادئ القانونية الصادرة عن محكمة النقض (الدوائر الجنائية) في الجرائم الاقتصادية، المكتب الفني لمحكمة النقض، ص٢٩.

الاتصالات أو قنوات البث التليفزيوني والإذاعي، وأن تحصله على هذه الخدمات بدون وجه حق، وأن من شأن تحصله على هذه المنفعة الإضرار بحقوق أصحاب الحق في خدمات الاتصالات أو البث.

ب) الإرادة: يجب أن تتجه إرادة الجاني إلى استخدام البرامج وتقنيات المعلومات أو شبكة الإنترنت للحصول على خدمات الاتصالات أو قنوات البث، ولا عبرة للباعث على ارتكاب الجريمة، فتتحقق الجريمة ولو كان الباعث على ذلك نبيلاً، أم كان بقصد الإضرار بأصحاب حقوق البث.

العقوبة: يعاقب القانون على هذه الجريمة بعقوبة الحبس مدة لا تقل عن ثلاثة أشهر والغرامة التي لا تقل عن عشرة آلاف ولا تجاوز خمسين ألفاً أو إحداهما، ومن ثم يجوز للقاضي الحكم بالحد الأقصى للحبس وهو ثلاث سنوات وفقاً لسلطته التقديرية في ضوء ظروف وملابسات القضية دون رقابة عليه في ذلك، كما له أن يقضي بعقوبة الحبس أو بعقوبة الغرامة، أو بالعقوبتين معاً، كما يجوز له أن يأمر بوقف تنفيذ العقوبة وفقاً للمادة (٥٥) عقوبات، والتي تقضي بأنه:" يجوز للمحكمة عند الحكم في جناية أو جنحة بالغرامة أو بالحبس مدة لا تزيد على سنة أن تأمر في نفس الحكم بإيقاف تنفيذ العقوبة إذا رأت من أخلاق المحكوم عليه أو ماضيه أو سنه أو الظروف التي ارتكب فيها الجريمة ما يبعث على الاعتقاد بأنه لن يعود إلى مخالفة القانون""، ويجب أن يبين الحكم بيان الواقعة المستوجبة للعقوبة بما يحدد عناصر التهمة التي دان بها المحكوم عليه.

ومن جانب آخر قد يشكل سلوك الجاني جريمتي الانتفاع غير المشروع بخدمات الاتصالات وتمرير المكالمات الدولية، وفي هذه الحالة سيطبق القاضي عقوبة الجريمة الأشد وهي جريمة تمرير المكالمات الدولية، وهي جريمة معاقب عليها

بالحبس مدة لا تقل عن ستة أشهر ولا تجاوز خمس سنوات وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز خمسمائة ألف جنيه أو بإحدى هاتين العقوبتين، تطبيقاً لحكم المادة ٣٢ عقوبات.

المطلب الثاني

جريمة الدخول والبقاء غير المشروع

نص التجريم: عاقبت المادة (١٤) من القانون على جريمة الدخول غير المشروع بتجريم أفعال الدخول والبقاء غير المشروع لموقع أو حساب أو نظام معلوماتي، حيث تقضي المادة المذكورة بأنه:" ***يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمداً، أو دخل بخطأ غير عمدي وبقى بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه. فإذا أنتج عن ذلك إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي، تكون العقوبة الحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين***"[(١)].

---

(١) ومن الصكوك الدولية متعددة الأطراف التي حرصت على تجريم الدخول غير المشروع لأنظمة الحاسب الآلي الاتفاقية العربية بشأن مكافحة جرائم تقنية المعلومات (م٦) والقانون النموذجي العربي لمكافحة جرائم تقنية المعلومات (المواد ٣و٥و١٥و٢٢) واتفاقية بودابست (الاتفاقية الأوروبية) بشأن الجريمة الإلكترونية (م٢)، وقرار دول الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات (م١/٢) والمقترح التوجيهي لدول الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات (م٣) ومشروع اتفاقية الاتحاد الأفريقي (م١٥/ج، ١٦/ج)، ومشروع ميثاق الكوميسا (م١٨و١٩). بينما كان من ضمن التشريعات المقارنة التي حرصت على تجريم الدخول والبقاء غير المشروع في المواقع والنظم المعلوماتية التشريع الفرنسي والإماراتي والكويتي، حيث تقضي المادة (٣٢٣-
=

العلة من التجريم: تتمثل العلة من التجريم فيمايلي[1]:-

١- مواجهة حالات الاعتداء غير المشروع على الأنظمة المعلوماتية والمواقع الإلكترونية والحسابات الشخصية، وتجريم مسلك الجاني الذي يقوم بالدخول فيها بغير وجه حق.

٢- حماية أجهزة المعلومات وما عليها من مواقع أو أنظمة من الوصول إليها من أشخاص ليس لهم الحق في ذلك.

٣- إضفاء الحماية القانونية على المواقع والحسابات والأنظمة المعلوماتية، ولخصوصية مستخدمي هذه المواقع والأنظمة في مواجهة القراصنة والمجرمين.

٤- أهمية مواجهة أفعال الاختراق المعلوماتي بالنظر إلى خطورة هذه الأفعال والتي تعد الخطوة الأولى في مراحل التعامل مع الشبكة المعلوماتية والمرحلة الأولية في غالبية الجرائم المعلوماتية، حيث يبدأ الجاني بالدخول بدون وجه حق إلى المواقع أو اختراقها.

محل الجريمة: يتمثل محل الجريمة في المواقع الإلكترونية والنظم المعلوماتية

=

١) عقوبات فرنسي بأنه: "يعاقب على الدخول أو البقاء عن طريق الغش في كل أو جزء من نظام المعالجة الألية للمعطيات بعقوبة الحبس لمدة عامين وغرامة قدرها ٣٠ ألف يورو. وإذا ترتب على ذلك حذف أو تغيير لمعطيات النظام أو تخريب لنظام تشغيل النظام تكون العقوبة الحبس ثلاث سنوات وغرامة قدرها ٤٥ ألف يورو. وإذا ارتكبت الجرائم المشار إليها في الفقرتين السابقتين ضد نظام المعالجة الآلية للبيانات الشخصية التي تنفذها الدولة فإن العقوبة تزيد إلى الحبس لمدة خمس سنوات وغرامة قدرها ٧٥ ألف يورو"، بينما يجرم هذا السلوك كل من التشريع الإماراتي (م٢) والتشريع الكويتي (م٢).

[1] د.حسنى الجندي:قانون مكافحة جرائم تقنية المعلومات، مرجع سابق، ص ص٧٢-٧٤.

والحسابات الخاصة-كما سبق أن أشرنا-، ولا ينصرف محل الجريمة إلى المكونات المادية للنظام المعلوماتي، أو إلى المعلومات ذاتها، وإنما قد يؤدي النشاط الإجرامي إلى إتلاف أو محو أو تغيير البيانات أو المعلومات الموجودة على الموقع أو النظام أو الحساب الخاص، وهو ما يجرمه المشرع مع تشديد العقاب[١].

وكان المشرع المصري قد عرف كل من النظام المعلوماتي بأنه:"*مجموعة برامج وأدوات معدة لغرض إدارة ومعالجة البيانات والمعلومات، أو تقديم خدمة معلوماتية*"[٢]، والموقع بأنه:"*مجال أو مكان افتراضي له عنوان محدد على شبكة معلوماتية، يهدف إلى إتاحة البيانات والمعلومات للعامة أو الخاصة*"[٣]، وغالباً ما تستخدم هذه المواقع الإلكترونية في بث البيانات والمعلومات في مجال أو موضوع ما، بينما عرف المشرع الحساب الخاص بأنه:" *مجموعة من المعلومات الخاصة بشخص*

---

[١] المرجع السابق، ص٧٥.

[٢] ومن التشريعات المقارنة التي تضمنت تعريف للنظام المعلوماتي التشريع الإماراتي والكويتي والنظام السعودي.

[٣] يقصد بمواقع الويب برامج تتيح عرض المعلومات والبيانات وهي في الأصل أرقام ولكن يتم ترجمتها إلى كلمات تعرض للمستخدم على الشاشة، والويب عبارة عن مجموعة من الوثائق والمصادر المرتبطة مع بعضها البعض عن طريق روابط فائقة وعناوين إنترنت، وهي تختلف عن شبكة الإنترنت نفسها، والتي تعتبر مجموعة من الحواسب المتصلة معاً عن طريق أسلاك نحاسية وكابلات ألياف بصرية وتوصيلات لاسلكية وما إلى ذلك. وهناك العديد من البرامج التي تعمل كمتصفحات الويب؛ نذكر منها: (إنترنت إكسبلورر-فيرفوكس- جوجل كروم)، التي تقوم بالدخول إلى صفحات الويب، وتمكن المستخدم من التجول من صفحة لأخرى، وتحتوى صفحة الويب تقريباً على مزيج من بيانات الحاسوب بما فيها الصور الفوتوغرافية، الرسوميات، الصوتيات، النصوص، الفيديو، الوسائط المتعددة ومحتويات تفاعلية بما في ذلك الألعاب وغيرها، وتشير التقديرات إلى أن عدد مواقع الإنترنت في العالم قد بلغت ما يزيد على مائتي وثلاثين مليون موقع إلكتروني حسب إحصاءات موقع جوجل في مارس ٢٠١٠، تبرز الإشارة إلى اتفاق التشريعات العربية على تعريف الموقع الإلكتروني، ومنها التشريع الإماراتي والكويتي والسوداني والنظام السعودي.

طبيعي أو اعتباري، تخول له الحق دون غيره الحق في الدخول على الخدمات المتاحة أو استخدامها من خلال موقع أو نظام معلوماتي".

الركن المادي: يتحقق الركن المادي في هذه الجريمة من خلال اختراق المواقع الإلكترونية والحسابات الشخصية أو الأنظمة المعلوماتية، والوصول بدون وجه حق إلى موقع أو نظام معلوماتي أو حساب شخصي، بكل فعل من شأنه الدخول أو البقاء غير المشروع في المواقع أو الأنظمة المعلوماتية أو الحسابات الخاصة، وذلك على النحو التالي:-

أ) الدخول غير المشروع: يتحقق الركن المادي في الجريمة بأي فعل إيجابي من شأنه الدخول إلى موقع إلكتروني أو حساب شخصي أو نظام معلوماتي، ومن ثم يتطلب الدخول للمواقع أو الحسابات الخاصة أو الأنظمة المعلوماتية، وجود جهاز حاسب آلي، أو أي جهاز تقني أو وسيلة تقنية المعلومات يستخدمها الجاني، وكذا توافر خدمة الإنترنت، بما يسمح للجاني بالوصول إلى المواقع الإلكترونية أو الحسابات الخاصة الموجودة على مواقع الإنترنت، ويستوي لدى القانون الكيفية التي تم الدخول بها لهذا الموقع أو الحساب أو النظام المعلوماتي، سواء حدث الدخول بكسر كلمة السر، أو بحل الشفرة، أم عن طريق شبكات الاتصال التليفونية[١]، أو باستخدام برمجيات خبيثة كالبوتنت[٢]يتم تركيبها بالنظام المعلوماتي[١].

---

[١] د. على عبد القادر القهوجي: الحماية الجنائية للبيانات المعالجة إلكترونياً، مؤتمر القانون والكمبيوتر والإنترنت، كلية القانون، جامعة الإمارات العربية المتحدة، ٢٠٠٠، ص٥٠؛ د. مدحت رمضان: الحماية الجنائية للتجارة الإلكترونية، القاهرة، دار النهضة العربية، ص٥١.

[٢] تعرف البوتنت أو شبكات الروبوت، بأنها الأداة الرئيسية في ارتكاب جرائم الإنترنت، وكلمة البوتنت مشتقة من كلمتين "روبوت" و"نت"، وهي تتألف من شبكة مترابطة من أجهزة الحاسب =

=

يتم التحكم فيها عن بعد، ببرمجيات خبيثة تحول الأنظمة المصابة إلى "روبوت"، وفي أغلب الأحيان يجهل الملاك الشرعيون لهذه الأجهزة حقيقة الإصابة التي تتم عن طريق الحواسيب التي يتحكم فيها الجناة وتعرف باسم خوادم القيادة والسيطرة، ويتم استخدام شبكات الروبوت في عدد من الأفعال منها هجمات حجب الخدمة الموزعة، وإرسال البريد الإلكتروني الطفيلي، وسرقة المعلومات الشخصية، واستضافة المواقع الإلكترونية الخبيثة، ونقل حملات من البرمجيات الخبيثة، وتشير التقديرات الدولية إلى أن أكثر من مليون عنوان فريد من عناوين بروتوكولات الإنترنت في عام ٢٠١١ يعمل على الصعيد العالمي كخادم لشبكة الروبوت للتحكم في الشبكات المعلوماتية ومراقبتها، بينما تشير تقديرات دولية أخرى إلى أن أجهزة الحاسب المصابة بفيروس الحواسب المدمرة "زومبي" والتي تشكل جزءاً من شبكة روبوت تتجاوز أكثر من سبعة ملايين جهاز حاسب آلي على الصعيد العالمي. انظر: دراسة مكتب الأمم المتحدة، مرجع سابق، ص ص٤٦-٤٨.

UNODC calculations based on Microsoft, 2010. Microsoft Security Intelligence Report. Volume 9. Figure as of first half 2010. This estimate is of the same order of magnitude as that of Symantec, 2011. Internet Security Threat Report. 2011. Volume 17 (estimate of 4.5 million for 2010); Acohido, B., 2010. Are there 6.8 million –or 24 million– botted PCs on the Internet? The Last Watchdog. : Available at: http://lastwatchdog.com/6-8-million-24-million-botted-pcs-internet/

ويعد تركيب البرمجيات الخبيثة في النظام المعلوماتي المملوك للأفراد أو إحدى المنشآت من قبيل جريمة الدخول غير المشروع واختراق البيانات أو نظام المعلومات بطريق غير مشروع، كما يعد انتاج برمجيات الروبوت أو بيعها أو حيازتها أو توزيعها من قبيل سوء استخدام أدوات الحاسب، كما قد تستخدم شبكات الروبوت في ارتكاب جرائم استخدام الحاسب في الاحتيال وفي جرائم الهوية وإرسال أو التحكم في إرسال الرسائل الإلكترونية الطفيلية. انظر:

NATO Cooperative Cyber Defence Centre of Excellence and ENISA, 2012. : Legal Implications of Countering Botnets.

OECD, 2008. Malicious Software (Malware). A Security Threat to the Internet Economy. DSTI/ICCP/REG(2007)5/FINAL. 28 April 2008; Hogben, G. (ed.) 2011. Botnets: Detection, Measurement, Disinfection and Defence. European Network and Information Security Agency(ENISA).

ومما يشير إلى خطورة شبكات الروبوت ما أجراه باحثون أكاديميون من رقابة لأحد شبكات الروبوت المتصلة بحوالي ١٨٣ ألف جهاز زومبي لمدة عشرة أيام فقط، والتي أسفرت عن عدد =

كما يستوي لدى القانون أن يكون الدخول قد تم بشكل عمدي أو عن طريق الخطأ، ومن ثم تتحقق مسئولية الجاني عن فعل الدخول، ولو كان عن طريق المصادفة، ويرى الفقه الجنائي[٢] أن مصطلح الدخول في جرائم تقنية المعلومات لا ينصرف إلى المعنى المادي، كما في الدخول إلى الغرفة التي يوجد بها جهاز الحاسب، وإنما هذا الدخول يكون ذا طبيعة معنوية، ينصرف إلى النشاط الذهني الذي يقوم به الجاني للوصول إلى موقع على الحاسب أو إلى نظام معلوماتي به أو حساب خاص، وقد يرتكب الفعل المادي للتوصل عن طريقه إلى اختراق الإجراءات الأمنية التي تحمي الموقع أو النظام المعلوماتي أو الحساب الخاص[٣]، ولم يتطلب القانون صفة خاصة فيمن يقوم بعملية الدخول، فقد يكون محترفاً أم غير محترف، عاملاً في الجهة التي حدث فيها دخول الموقع أو النظام المعلوماتي أو الحساب الخاص أو من غير العاملين لديه[٤].

ومن التطبيقات لهذا الفعل قيام الجاني باستخدام برامج اختراق لأجهزة

=

من المعلومات الخطيرة، أبرزها: أن متوسط أعداد الأجهزة النشطة لهذه الأجهزة في أي وقت ٤٩ ألف جهاز معظمها في شمال أوروبا وأمريكا الشمالية، وقد تمثلت الأضرار الناجمة عن هذه الشبكة في الوصول إلى أوراق اعتماد حسابات ٨،٣٠٠ ضحية في ٤٠٠ مؤسسة مالية مختلفة، وتفاصيل ١٧٠٠ بطاقة ائتمان وأسماء ٢٩٨ ألف من مستخدمي وكلمات مرور لضحايا بالبريد الإلكتروني مواقع التواصل الاجتماعي وإرسالها إلى خادم القيادة والتحكم بهذه الشبكة، وعرض النطاق الترددي الكلي حسب حواسب "الزومبي" لشن هجوم حجب الخدمة الموزعة. انظر في تفصيلات ذلك في تفصيلات ذلك:

Stone-Gross, B., et al., 2009. Your Botnet is My Botnet: Analysis of a Botnet Takeover. CCS '09

(1) **NATO Cooperative Cyber Defence Centre of Excellence and ENISA, 2012. : Legal Implications of Countering Botnets.**

(2) **GASSIN (R.) : Fraud informatique, Dalloz,1995, No. 100. P.16.**

(٣) د. حسنى الجندي: قانون مكافحة جرائم تقنية المعلومات، مرجع سابق، ص٧٦.

(٤) الموضع السابق.

الحسابات، ليتمكن من خلالها اختراق الحاسب الآلي للمجني عليها، وتشغيل الميكروفون والكاميرا الخاصة به للتجسس عليها وعلى أسرتها والتقاط صور لها أثناء تواجدها بمنزلها دون علمها، وفي قضية أخرى قيام أحد الأشخاص الفرنسيين بالدخول عن طريق الإنترنت بطريق الغش إلى نظام المعالجة الآلية الخاصة بأحد المستشفيات، والمحجوز بها زوجته، وقيامه بتغيير المعلومات الطبية الخاصة بها مما أدى إلى وفاتها[1].

الدخول بطريق الخطأ: كما أن الجريمة من المتصور وقوعها بخطأ غير عمدي، إذا كان هذا الدخول قد تم عن طريق الإهمال وعدم الاحتراز أو تقصير الجاني في واجباته أو عن طريق الرعونة، أما فعل البقاء، فهو لا يتصور إلا بطريق العمد، ويتحقق الدخول بطريق الخطأ حينما لا يراعي الجاني التعليمات والقواعد الخاصة بأمن المعلومات الواجب على الشخص العادي مراعاتها، فيترتب على ذلك الدخول غير المشروع إلى موقع إلكتروني أو حساب شخصي أو نظام معلوماتي.

ب) البقاء غير المشروع: يتحقق الركن المادي بالبقاء أو المكوث أو التواجد غير المشروع على موقع إلكتروني أو حساب شخصي أو نظام إلكتروني، ويستوي لدى القانون أن يكون دخول الجاني للموقع الإلكتروني أو النظام المعلوماتي مصرحاً به أم غير مصرحاً به، فقد يكون دخول الجاني للموقع أو الحساب الشخصي أو النظام المعلوماتي مشروعاً، ولكنه تجاوز حدود الحق في الدخول، أو أن يكون مصرحاً له بالدخول للموقع أو الحساب أو النظام المعلوماتي، فيتجاوز ذلك ويبقى على الموقع الإلكتروني أو الحساب الشخصي أو النظام المعلوماتي لمدة من الزمن، وتبرز الإشارة في هذا السياق إلى أن جريمة

[1] أنظر د. جميل عبد الباقي، الإنترنت والقانون الجنائي، مرجع سابق، ص٤١.

الدخول غير المشروع لموقع إلكتروني هي جريمة وقتية، أما جريمة البقاء غير المشروع على موقع إلكتروني فهي جريمة مستمرة، لاستغراقها مدة من الزمن قد تطول أو تقصر.

تساؤل: هل الضرر عنصر من عناصر الركن المادي؟ الواقع أن المشرع قد جرم الدخول أو البقاء غير المشروع بمجرد تحققه، ولو لم يترتب على ذلك ضرر، ولكنه اعتد بعنصر الضرر كظرف مشدد للعقاب على النحو التالي ذكره بشأن العقوبة المقررة لهذين الفعلين.

أن يكون الدخول أو البقاء بغير وجه حق: تطلب القانون في الدخول أو البقاء أن يكون بدون وجه حق؛ أي أن يكون الجاني غير مصرح له بالدخول له أو محظور عليه ذلك، فيكون الدخول إلى المواقع الإلكترونية أو الأنظمة المعلوماتية أو الحسابات الخاصة غير مشروع إذا كان بدون رضاء صاحبه، أو بدون إذن من الشخص المسئول عن هذا النظام[١]، أو أن يكون الجاني غير مخولاً بالبقاء عليه، أو أن يتجاوز المدة الزمنية المسموح له للبقاء فيها على الموقع أو النظام المعلوماتي.

الركن المعنوي: هذه الجريمة يمكن أن تقع عمداً أو بطريق غير عمدي، وهو ما أشار إليه المشرع بعبارة:" دخل عمداً أو بخطأ غير عمدى وبقى بدون وجه حق"، ومن ثم فهذه الجريمة قد تتحقق بطريق العمد[٢] بتوافر القصد الجنائي العام بعنصريه

---

[١] محمد خليفة: الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن،٢٠٠٧، ص١٣٩.

[٢] تبرز الإشارة إلى أن كافة الصكوك الدولية متعددة الأطراف تشترط أن ترتكب جريمة اقتحام نظام حاسوبي بصورة غير مشروعة بشكل متعمد، وجرت العادة أن يترك تعريف ما يشكل اتجاه نية الجاني إلى الدول الأطراف، ونذكر على سبيل المثال الاتفاقية الأوروبية بشأن الجرائم الإلكترونية التي ينص التقرير التفسيري المرافق لها صراحة على أنه يتعين تعريف المعنى الدقيق للفعل المتعمد وفقاً للتفسير الوطني. انظر: دراسة مكتب الأمم المتحدة المعني بالمخدرات والجريمة بشأن الجريمة السيبرانية، مرجع سابق، ص ص١١٩، ١٢٠.

العلم والإرادة، بأن يعلم الجاني بدخوله بدون وجه حق لموقع إلكتروني أو حساب شخصي أو نظام معلوماتي وبقاءه عليه، وأن تتجه إرادته إلى تحقيق ذلك، بينما يتحقق الركن المعنوي في صورة الخطأ غير العمدي، كما سبق أن أشرنا، حينما تنصرف الإرادة على السلوك دون النتيجة، وذلك حينما تتجه الجاني إلى فتح الحاسب الآلي ولا يراعى التعليمات والقواعد الخاصة بأمن المعلومات، فيترتب على ذلك الدخول إلى الموقع أو الحساب الشخصي، أو النظام المعلوماتي.

العقوبة: ميز القانون في العقوبة بين حالتين:-

(الحالة الأولى) السلوك المجرد: عاقب القانون في هذه الحالة على الدخول أو البقاء غير المشروع بعقوبة الحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن خمسين ألفاً ولا تجاوز مائة ألف جنيه أو إحداهما، ومن ثم يجوز للقاضي وفقاً لسلطته التقديرية في ضوء ظروف وملابسات القضية أن يقضي بعقوبة الحبس أو بعقوبة الغرامة، أو بالعقوبتين معاً، كما يجوز له أن يأمر بوقف تنفيذ العقوبة وفقاً للمادة (٥٥) عقوبات، إذا رأت من أخلاق المحكوم عليه أو ماضيه أو سنه أو الظروف التي ارتكب فيها الجريمة ما يبعث على الاعتقاد بأنه لن يعود إلى مخالفة القانون.

(الحالة الثانية) تحقق ضرر من جراء الدخول أو البقاء: عاقب القانون على الدخول أو البقاء غير المشروع بعقوبة الحبس مدة لا تقل عن سنتين والغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف أو إحداهما، إذا أنتج عنه ضرر تمثل في إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر البيانات الموجودة عليه[1]،

---

[1] تجدر الإشارة إلى أن بعض الصكوك الدولية متعددة الأطراف كالاتفاقية العربية لمكافحة جرائم تقنية المعلومات تنص على تشديد العقاب إذا كان الدخول إلى النظام الحاسوبي يؤدي إلى "*محو ات المحفوظة أو تعديلها أو تحريفها أو استنساخها أو إزالتها أو تدمير الأدوات الإلكترونية وشبكات الاتصال والأنظمة الحاسوبية، وإلحاق أضرار بالمستخدمين أو المستفيدين، أو الحصول على معلومات حكومية سرية*"، بينما ينص القانون العربي النموذجي لمكافحة جرائم تقنية المعلومات على تشديد العقاب متى اقترن ارتكاب جريمة الدخول غير المشروع "*بنية إلغاء أو أو تدمير أو الكشف عن أو تغير أو إعادة نشر البيانات أو المعلومات*
=

ومن ثم اعتبر المشرع الإضرار بالنظام المعلوماتي أو الموقع أو الحساب الخاص ظرفاً مشدداً للعقاب، ويشترط لتحقق هذا الظرف المشدد مايلي:-

١) تحقق إحدى صور الضرر المشار إليها في القانون، وهي:-

أ) الإتلاف: يتحقق ذلك بإحداث خلل في تشغيل البيان أو المعلومة، ويستوي أن يتحقق ذلك بواسطة استخدام البرامج الخبيثة[١] كالفيروسات، أو قطع التيار أثناء معالجة البيانات، أو وضع شريحة أو دائرة مطبوعة في غير مكانها الصحيح، أو التلاعب فيها، كما يتحقق بإفناء المعلومة أو البيان أو هلاكه كلياً أو جزئياً.

ب) المحو: ويقصد به محو البيانات أو المعلومات؛ أي تعديلها بالحذف من النظام المعلوماتي أو الموقع الإلكتروني أو الحساب الشخصي.

ج) التغيير: ويكون ذلك بإحداث تعديل في البيانات، بحيث تفقد قيمتها وحقيقتها التي كانت عليها، كما يتحقق أيضاً بكل تعد مادي على البيانات أو المعلومات، وقد

= *الشخصية* "(م٣)، أو "*عند اضطلاعه بمهامه، أو قام بتسهيل ارتكاب الجرائم من قبل طرف ثالث* "(م٥)، بينما يشترط المشروع التوجيهي لقرار دول الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات لتشديد العقاب لارتكاب جرائم اقتحام نظام حاسوبي بصورة غير مشروعة: أن يتم ذلك في إطار منظمة إجرامية، أو من خلال استخدام إحدى الأدوات المصممة لشن هجمات تؤثر على عدد كبير من نظم المعلومات، أو هجمات تتسبب في أضرار كبيرة، مثل تعطيل خدمات النظام، تكبد نفقات مالية أو فقد بيانات شخصية، أو من خلال إخفاء الجاني الهوية الحقيقية والتسبب في إلحاق الضرر بالمالك القانوني للهوية (م١٠). انظر: دراسة مكتب الأمم المتحدة المعني بالمخدرات والجريمة بشأن الجريمة السيبرانية، مرجع سابق، ص ص١٢٠، ١٢١.

[١] من الجدير بالذكر أن مشروع قرار رئيس مجلس الوزراء بإصدار اللائحة التنفيذية للقانون رقم ١٧٥ لسنة ٢٠١٨ كان قد تضمن تعريفاً للبرامج الخبيثة، بأنها:" برامج أو ملفات أو شفرات أو أكواد تؤثر سلبياً بشكل مباشر أو غير مباشر على تقنية المعلومات أو الاتصالات أو الشبكات المستخدمة.

يتخذ صورة المحو أو التشويه، وكذلك كل عمل يؤدي إلى جعل النظام المعلوماتي أو الموقع الإلكتروني أو الحساب الشخصي غير صالح لأداء ما أعد له، أو يؤدي إلى تعديل مسار البيانات أو المعلومات على النحو الذي كان يتعين أن يسير فيه.

د) النسخ: ويتحقق ذلك من خلال قيام الجاني بإعادة استنساخ المعلومات أو البيانات الموجودة على النظام المعلوماتي أو الموقع الإلكتروني أو الحساب الشخصي، ومن ثم التحصل على نسخة منها.

هـ) إعادة النشر: ويتحقق ذلك في الحالات التي يتم فيها استبعاد الموقع أو المعلومة لعدم الحاجة إليها، فيقوم الجاني بإعادة نشرها.

٢) أن يكون وقوع الضرر على النظام المعلوماتي أو الموقع الإلكتروني أو الحساب الشخصي.

٣) توافر رابطة السببية بين سلوك الجاني في اختراق النظم المعلوماتية أو المواقع أو الحسابات الشخصية وإحداث الضرر الواقع عليها.

فالمشرع يشدد العقاب على الدخول أو البقاء غير المشروع إذا أسفر عنه أي ضرر مادي وقع على النظام المعلوماتي أو الموقع الإلكتروني أو الحساب الشخصي، من خلال تغيير في محتواه أو إتلافه أو محوه، أو من خلال الإضرار بمستخدم هذه المواقع أو الأنظمة، من خلال نسخ محتواه أو إعادة نشر البيانات الموجودة عليه، ومن ثم يجوز للقاضي وفقاً لسلطته التقديرية في ضوء ظروف وملابسات القضية أن يقضي - في حال توافر الظرف المشدد- بعقوبة الحبس أو بعقوبة الغرامة، أو بالعقوبتين معاً، وليس للقاضي في هذه الحالة أن يأمر بوقف تنفيذ العقوبة، لأن عقوبة الحبس لا تقل مدتها عن سنتين.

المطلب الثالث

جريمة تجاوز حدود الحق في الدخول

نص التجريم: تناولت المادة (١٥) من القانون جريمة تجاوز حدود الحق فى الدخول لموقع أو حساب أو نظام معلوماتي، حيث تقضي المادة المذكورة بأنه:" *يُعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتي مستخدماً حقاً مخولاً له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول*"، وتبرز الإشارة إلى أن جريمة تجاوز الحق في الدخول هي من جرائم الاختراق المعلوماتي، فهي تفترض قيام الجاني بالدخول إلى الحاسب الآلي أو النظام المعلوماتي، على النحو المقرر ذكره لاحقاً، وتبرز أهمية التمييز بين الجريمتين في رغبة المشرع الجنائي في أن يميز في العقاب بين من يصرح له بالدخول للحاسب الآلي أو النظام المعلوماتي ويخالف حدود الحق في الدخول، ومن يقوم بالدخول للحاسب الآلي أو النظام المعلوماتي بصفة عامة.

العلة من التجريم: ترجع العلة من التجريم في مواجهة صور الاعتداء على أنظمة وتقنيات المعلومات، من خلال تجريم عمليات الدخول غير المشروع للمواقع أو الحسابات أو الأنظمة المعلوماتية، من خلال تجاوز حدود استعمال الحق في الدخول لهذه المواقع والأنظمة المعلوماتية.

محل الجريمة: تطلب القانون أن تقع الجريمة على موقع إلكتروني أو حساب خاص أو نظام معلوماتي، وقد سبق لنا تناول تعريف كل من الموقع الإلكتروني والنظام المعلوماتي والحساب الخاص في الجريمة السابقة، ومن ثم نحيل إليها منعاً للتكرار، ويكفي لتحقق الجريمة أن ينصب الفعل على أيا منهم.

الركن المادي: يتحقق الركن المادي في هذه الجريمة من عنصرين:-

أ) الدخول إلى موقع أو حساب أو نظام معلوماتي: يتحقق الركن المادي في هذه الجريمة بدخول الجاني إلى موقع إلكتروني أو حساب خاص أو نظام معلوماتي، فهذه الجريمة تفترض قيام الجاني بالدخول إلى الحاسب الآلي أو النظام المعلوماتي، ولكن هذا الدخول قد تم من شخص مصرح له بذلك، إلا أنه قد خالف حدود هذا الحق في الدخول، ويستوي لدى القانون أن يكون الدخول لهذا الحساب أو الموقع أو النظام المعلوماتي قد تم باستخدام كلمة سر أو رمز أو كود سري أم بوسيلة أخرى.

ب) تجاوز حدود الحق المخول للجاني في الدخول: تفترض هذه الجريمة أن الجاني مخول بالدخول للموقع الإلكتروني أو الحساب الخاص أو النظام المعلوماتي، ولكنه قد خالف القواعد أو القيود التي تنظم هذا الدخول، سواء أكانت هذه القيود زمانية أم مكانية أم موضوعية، بأن تجاوز مستوى الدخول المصرح له به، ويستوي لدى القانون أن يكون التصريح للجاني بالدخول للموقع الإلكتروني أو الحساب الخاص أو النظام المعلوماتي بسبب وظيفته أم غير ذلك.

الركن المعنوي: هذه الجريمة من الجرائم العمدية التي يتحقق فيها الركن المعنوي بتوافر القصد الجنائي العام بعنصريه العلم والإرادة.

أ) العلم: يجب أن يكون الجاني عالماً بأن من شأن فعله الدخول إلى نظام معلوماتي أو موقع إلكتروني أو حساب خاص، وبأنه قد تجاوز حدود الحق المخول له في الدخول لهذه المواقع أو الحسابات أو الأنظمة المعلوماتية.

ب) الإرادة: يجب أن تتجه إرادة الجاني إلى الدخول إلى موقع إلكتروني أو حساب خاص أو نظام معلوماتي، وأن تتجه إلى تجاوز حدود الحق المخول له في الدخول.

العقوبة: يعاقب القانون على هذه الجريمة بعقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه أو بأحدهما، ومن ثم يجوز للقاضي وفقاً لسلطته التقديرية في ضوء ظروف وملابسات القضية أن يقضي بعقوبة الحبس أو بعقوبة الغرامة، أو بالعقوبتين معاً، كما يجوز له أن يأمر بوقف تنفيذ العقوبة وفقاً للمادة (٥٥) عقوبات، إذا رأت من أخلاق المحكوم عليه أو ماضيه أو سنه أو الظروف التي ارتكب فيها الجريمة ما يبعث على الاعتقاد بأنه لن يعود إلى مخالفة القانون.

المطلب الرابع

جريمة الاعتراض غير المشروع

نص التجريم: تضمن القانون في المادة (١٦) جريمة الاعتراض غير المشروع، حيث تقضي المادة المذكورة بأنه:" *يُعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتين وخمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعترض بدون وجه حق أي معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها* "[1].

[1] ومن المواثيق الدولية التي حرصت على تجريم الاعتراض غير المشروع الاتفاقية العربية بشأن مكافحة جرائم تقنية المعلومات (م٧) والقانون النموذجي العربي لمكافحة جرائم تقنية المعلومات (م٨) واتفاقية بودابست (الاتفاقية الأوروبية) بشأن الجريمة الإلكترونية (م٣)، والمقترح التوجيهي لدول الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات (م٦) ومشروع اتفاقية الاتحاد الأفريقي (م٢٣/ج)، ومشروع ميثاق الكوميسا (م٢١).
وعلى نحو موازٍ تبرز الإشارة إلى أن المادة (٧٤) من قانون الأحوال المدنية (١٤٣) لسنة ١٩٩٤، نصت على تجريم المساس بسرية البيانات الخاصة بالأحوال المدنية بالإطلاع أو الحصول عليها أو الشروع في ذلك أو تغييرها بأية صورة كانت أو إذاعتها أو إفشائها.

العلة من التجريم: ترجع العلة من تجريم هذا الفعل فيمايلي:-

١- منع انتهاك سرية المراسلات الخاصة، وتوفير الحماية القانونية للبيانات والمعلومات المتداولة من الاطلاع عليها بدون مسوغ قانوني، فالأصل أن البيانات المعروضة على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وغير ذلك تتمتع بالسرية، ومن ثم لا يجوز لأحد مطلقاً الاطلاع عليها إلا بمسوغ قانونى صحيح، فإذا قام شخص بالاعتداء على هذه الحرمة وانتهاك تلك السرية، فانه يكون مرتكباً لجريمة الاعتراض غير المشروع.

٢- حماية الحق في احترام نقل البيانات والحق في احترام الاتصالات والمراسلات وكل أشكال النقل الإلكتروني للبيانات[١].

محل الجريمة: تعرف معظم الصكوك الدولية متعددة الأطراف والمعنية بمكافحة جرائم تقنية المعلومات الاعتراض غير المشروع بأنه نقل بيانات حاسوبية غير عامة، ومن ثم يقتصر محل جريمة الاعتراض غير المشروع على المراسلات الخاصة[٢]. وقد تطلب القانون أن تقع الجريمة على المعلومات أو البيانات، وكل ما يمكن تداوله عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما فى حكمها، فالبيانات هي عبارة عن كلمات وأرقام ورموز وحقائق وإحصائيات لا صلة بينها، ولكنها تصلح لتكوين فكرة أو معرفة بواسطة الإنسان أو الأدوات أو الأجهزة التي يسخرها لمعالجة هذه البيانات[٣]، بينما المعلومات فهي بيانات خضعت للتشغيل

---

[١] د. حسنى الجندي: قانون مكافحة جرائم تقنية المعلومات، مرجع سابق، ص٢٥.

[٢] انظر: دراسة مكتب الأمم المتحدة المعني بالمخدرات والجريمة بشأن الجريمة السيبرانية، مرجع سابق، ص١٢٣.

[٣] د. حسنى الجندي: قانون مكافحة جرائم تقنية المعلومات، مرجع سابق، ص١١٧.

والتحليل والتفسير لتحقيق زيادة المعرفة لمتخذي القرار ومساعدتهم لتحقيق أغراض معينة[١].

وكان القانون المصري قد عرف البيانات والمعلومات الإلكترونية بأنها: "***كل ما يمكن إنشاؤه أو تخزينه أو معالجته أو تخليقه أو نقله أو مشاركته أو نسخه، بواسطة تقنية المعلومات، كالأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور والأصوات، وما في حكمها***"[٢].

بينما عرف القانون الحاسب بأنه: "كل جهاز أو معدة تقنية تكون قادرة على التخزين وأداء عمليات منطقية أو حسابية، وتستخدم لتسجيل بيانات أو معلومات أو تخزينها أو تحويلها أو تخليقها أو استرجاعها أو ترتيبها أو معالجتها أو تطويرها أو

---

(١) د. إبراهيم أحمد الصعيدي: نظام التشغيل الإلكتروني للبيانات، القاهرة، مطبعة المعرفة،١٩٨١، ص١٣؛ د. حسنى الجندي: قانون مكافحة جرائم تقنية المعلومات، مرجع سابق، ص١١٨.

(٢) تبرز الإشارة إلى أن التفرقة بين كل من البيانات والمعلومات كانت محل نقاش من أعضاء البرلمان، حيث أشار أحد أعضاء البرلمان إلى أن اتفاقية بودابست بشأن الجريمة الإلكترونية قد ميزت بين كل من البيانات والمعلومات، وأن البيانات وهي عبارة عن مشاهدات أو قياسات أو حروف أو كلمات، فهي بمثابة المادة الخام للمعلومات، وهي ساكنة، أما الديناميكية الخاصة بها التي تحركها فهي المعالجة العلمية لها، وقد أشار السيد المهندس وزير الاتصالات وتكنولوجيا المعلومات إلى أن القانون قد أخذ في اعتباره الفرق بين البيانات والمعلومات، من خلال التعاريف الكثيرة للبيانات الشخصية والبيانات الحكومية والمعالجات الإلكترونية وتوقيت البيانات التي تتحول إلى معلومات. انظر: مضبطة مجلس النواب المصري، الجلسة السادسة والخمسين، المعقودة في ٢٠١٨/٥/١٤م، مرجع سابق، ص٨٦.

وباستعراض موقف التشريعات المقارنة بشأن التفرقة بين البيانات والمعلومات، يتبين وجود اتجاهين: (الأول) يرى الجمع بين المدلولين في تعريف موحد، وهذا هو اتجاه التشريع المصري والسوداني والعماني، و(الثاني) يرى إفراد تعريف منفصل لكل منهما، حيث يميز هذا الاتجاه بين البيانات والمعلومات التي يتم معالجتها من خلال الحاسب الآلي، فالمعلومات هي المرحلة التالية أو هي نتاج معالجة البيانات باستخدام الحاسب الآلي، ونذكر من الاتجاه الثاني كل من التشريع الإماراتي والسعودي والأردني والبحريني والكويتي.

تبادلها أو تحليلها أو للاتصالات"[١]. وتبرز الإشارة إلى توسع مدلول الحاسب الآلي ليشمل كل من الخوادم Serversوأجهزة الحاسب التقليدية كأجهزة الحاسب المكتبية الشخصية وأجهزة الحاسب المحمولة والهواتف الذكية والأجهزة اللوحية، وأجهزة الوسائط المتعددة مثل الطابعات ومشغلات الـMP3 والكاميرات الرقمية[٢].

وحسناً فعل المشرع المصري بوضع تعريف موحد لكل من البيانات والمعلومات الإلكترونية بالنظر إلى توفيره للحماية الجنائية للأمرين، سواء أكانت البيانات في مرحلة ما قبل المعالجة الآلية أم المعلومات في مرحلة ما بعد المعالجة الالكترونية، منعاً للخلط والالتباس في التطبيق القضائي، فكل من البيانات والمعلومات محمية جنائياً وفقاً لأحكام القانون.

وتجدر الإشارة إلى أن المشرع المصري قد فرق بين نوعين من البيانات بحسب طبيعتها، الأولى هي البيانات العامة أو الحكومية والثانية هي البيانات الخاصة

---

(١) تبرز الإشارة إلى سابقة تعريف المشرع المصري للحاسب الآلي، بموجب نص المادة (٢/فقرة أولى) من القرار رقم (٨٢) لسنة ١٩٩٣ في شأن قانون حماية حق المؤلف فيما يتعلق بمُصنفات الحاسب الآلي، والذي عرف الحاسب الآلي بأنه:" جهاز قادر على تخزين ومُعالجة وتحليل واسترجاع البيانات أو المعلومات"، ومن التشريعات العربية النظام السعودي، وقد عرفت الاتفاقية الأوروبية المتعلقة بالجرائم الإلكترونية منظومة الكمبيوتر بأنها:"أي جهاز أو مجموعة من الأجهزة المتصلة أو المتعلقة ببعضها البعض، ويقوم واحد أو أكثر، تبعاً لبرنامج، بعمل معالجة آلية للبيانات" (م١ من اتفاقية بودابست)، وترجع أهمية وضع تعريف محدد للحاسب الآلي في ارتباطه عضوياً أو غائياً بتعريف الجريمة المعلوماتية. ويمكن التمييز بين الحواسب العادية والخوادم Servers، والحاسب الخادم فهو الحاسب الآلي الذي ينفذ الخدمات وهو يحتوي على معلومات يمكن الإطلاع عليها عن بعد باستخدام حاسبات آلية أخرى أو نهاية طرفية والوحدة الطرفية Terminal هي جهاز ادخال واخراج لإرسال واستقبال المعلومات على خط الاتصال. انظر: د. جميل عبد الباقي الصغير: القانون الجنائي والإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٢، ص٦ وص٦٣.

(٢) انظر دراسة مكتب الأمم المتحدة حول الجريمة السيبرانية، مرجع سابق، ص٢٠.

أو الشخصية، فقد عرف المشرع البيانات الحكومية بأنها:" *بيانات متعلقة بالدولة أو سلطاتها، وأجهزتها أو وحداتها، أو الهيئات العامة، أو الهيئات المستقلة والأجهزة الرقابية، أو غيرها من الأشخاص الاعتبارية العامة وما في حكمها، والمتاحة على الشبكة المعلوماتية أو على أي نظام معلوماتي أو على حاسب أو ما في حكمها* "[١].

بينما عرف البيانات الشخصية بأنها:" أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى".

وحسناً فعل المشرع بتعريفه لهذه النوعية من البيانات، تمييزاً لها عن غيرها، وإفراداً لنصوص خاصة لحمايتها من الاعتداء والحفاظ على خصوصية الأفراد، وعلى النحو الأخر توفير الحماية المناسبة للبيانات الحكومية بالنظر إلى أهميتها للأفراد وللمجتمع[٢].

---

[١] ومن التشريعات التي تضمنت تعريف للبيانات الحكومية التشريعين الإماراتي والعماني.

[٢] يميز الباحثون في شأن جرائم تقنية المعلومات بين ثلاثة أنواع من البيانات، الأولى هي بيانات المشترك وتشمل البيانات والتفاصيل الخاصة بالمستخدم مثل الاسم والعنوان، والثانية هي بيانات حركة المرور وتشير إلى المنشأ، المقصد، المسار، الوقت، التاريخ، الحجم، المدة الزمنية، نوع الاتصالات التي تمت من خلال أحد النظم المعلوماتية، وأخيراً بيانات المحتوى وتشمل المحتوى الحقيقي لأي من الاتصالات. انظر في الفقه المقارن:

Sieber, U., 2008. Mastering complexity in the global cyberspace: The harmonization of computer-related criminal law. In: Delmas-Marty, M., Pieth, M., Sieber, U. (eds.). Les chemins de l'Harmonisation Pénale/Harmonising Criminal Law. Collection de L'UMR de Droit Comparé de Paris. Paris: Société de législation comparée.

الركن المادي: يتحقق الركن المادي في هذه الجريمة من عنصرين، وذلك على النحو التالي:-

الاعتراض: يتحقق الاعتراض بأي فعل من شأنه الاطلاع على البيانات أو المعلومات والحصول عليها بدون مسوغ قانوني[1]، وقد عرف المشرع الاعتراض بأنه:" مشاهدة البيانات أو المعلومات أو الحصول عليها، بغرض التنصت أو التعطيل أو التخزين أو النسخ أو التسجيل أو تغيير المحتوى أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه، وذلك لأسباب غير مشروعة ودون وجه حق".

وهذا الاطلاع أو الحصول على البيانات قد يقع من الجاني نفسه أو من الغير، ولا يُشترط أن يشاهد الجاني هذه البيانات بعينه، فيتوافر الاعتراض إذا شاهد الغير هذه البيانات حتى ولو لم يشاهدها الذي أظهرها فعلاً، كما لا يشترط أن يحصل الجاني على هذه البيانات لنفسه أو بنفسه، وإنما يتحقق الاعتراض إذا تحصل الغير على هذه البيانات، ولو لم يتحصل الفاعل نفسه عليها، فإذا لم يشاهدها أو يحصل عليها أحد، فإن الاعتراض لا يكون موجوداً، ولا يشترط تحميل أو تصوير أو تسجيل هذه البيانات، فالاعتراض يتوافر بمجرد مشاهدتها أو سماعها أو معرفتها أو الحصول عليها حتى ولو لم يتم تحميلها أو تصويرها.

---

[1] عرفت العديد من التشريعات جريمة الاعتراض غير المشروع، ومن بين هذه التشريعات التشريع الإماراتي (م١٥) والتشريع الكويتي (م٤) والنظام السعودي(م٣)، حيث تستخدم التشريعات السالف الإشارة إليها مصطلح الالتقاط، بينما يأخذ الجانب الآخر من التشريعات المقارنة ومنها التشريع المصري بمصطلح الاعتراض، وعلى خلاف ذلك انظر: نص المادة ٣٠٩مكرراً عقوبات مصري الذي نص على تجريم الالتقاط أو النقل بجهاز من الأجهزة أيا كان نوعه صورة شخص في مكان خاص.

ويستوي لدى القانون أن يكون الإطلاع أو المشاهدة قد تمت بشكل متعمد؛ أي أن الجانى يعلم أماكنها، فدخل عليها وفتح صفحاتها لمشاهدتها، أو أنها قد جاءت بشكل عرضي، كأن تكون هناك بيانات مفتوحة على شاشة الحاسب الآلي بمعرفة شخص مخول بفتحها، ويأتي شخص آخر لمشاهدة هذه البيانات على الرغم من إنه غير مصرح له بمشاهدتها، ولا يشترط لوقوع الجريمة أن يكون الجانى هو الذي قام بإعداد أجهزة معينة لبث هذه البيانات من أجل أن يشاهدها، وإنما يكفي أن تتم المشاهدة حتى ولو لم يكن الجانى له أي دور في إظهار هذه البيانات، ويكفى أن تكون البيانات صالحة للمشاهدة وقت ارتكاب الجريمة حتى ولو أصابها بعد ذلك عطب أو عطل يجعلها غير صالحة للمشاهدة، أو تم حذف هذه البيانات بعد ذلك من الشبكة المعلوماتية أو المكان الذي كانت منشورة به.

ويشترط في الجاني أن يكون قادراً على المشاهدة بعينه وقت ارتكاب جريمته، فإن ثبت أنه كان كفيفاً أو كان بصره ضعيفاً جداً وقت وقوع الجريمة، ولا يقدر على مشاهدة البيانات، فإن الجريمة تنتفى، إما إن ثبت أنه وقت الجريمة كان قادراً على المشاهدة بعينه الطبيعية أو باستخدام نظارة طبية أو أداة تمكنه من المشاهدة بوضوح، فإن الجريمة تتحقق بشأنه، حتى ولو أصبح بعد ذلك كفيفاً، ولا يستطيع الإبصار، كما تتحقق الجريمة أيضاً بمجرد الحصول عليها، سواء كان هذا الحصول بنسخ البيانات على ذات جهاز الحاسب الآلي أو على أسطوانات أو كتابتها يدوياً بواسطة أوراق وأقلام أو تم طبعها على أجهزة الطباعة المختلفة أو حفظها في العقل البشرى...إلخ.

أن يكون الاعتراض غير مشروعاً: يشترط في الجريمة أن يكون الاعتراض دون مسوغ قانونى، فتنتفي الجريمة إذا كان الذي يشاهد البيانات أو يتحصل عليها له صفة قانونية تبيح له مشاهدتها أو الحصول عليها.

الركن المعنوي: هذه الجريمة من الجرائم العمدية التي يتحقق فيها الركن المعنوي بتوافر القصد الجنائي بعنصريه العلم والإرادة لدى الجاني، وعادة ما تشترط الصكوك الدولية متعددة الأطراف أن تتوافر نية الفعل المتعمد عند ارتكاب جريمة الاعتراض غير المشروع[1].

أ) العلم: يجب أن يعلم الجاني أن سلوكه يمثل جريمة الالتقاط المؤثمة قانوناً، حيث يقوم بمشاهدة بيانات أو يتحصل عليها دون مسوغ قانونى يبيح له ذلك، فإن كان المتهم يعتقد أن ما يشاهده أو يتحصل عليه لا يمثل جريمة الالتقاط، حيث يظن أنتلك البيانات من الممكن لأي شخص مشاهدتها والاطلاع عليها دون أي شروط أو متطلبات معينة في شخصية المشاهد أو القائم بالحصول عليها، فإن الجريمة تنتفى بشأنه.

ب) الإرادة: يجب أن تتجه إرادة الجاني ونيته إلى المضي قدماً من أجل هذه المشاهدة أو الحصول على تلك البيانات، ومن ثم تنتفي الجريمة أيضاً إذا كان المتهم لا يريد المشاهدة أو الحصول على البيانات؛ كمن يريد تحميل برنامج أو موضوع معين، ثم يكتشف أنه قام بتحميل هذه البيانات عن طريق الخطأ، ويقع على النيابة العامة إثبات أن المتهم توافرت في شأنه كافة العناصر المطلوبة للقصد الجنائى لديه، فعليها إثبات أنه كان يعلم أن سلوكه يمثل جريمة الالتقاط وأنه كان يريد فعلاً تحقق هذه الجريمة.

---

[1] تقرر الاتفاقية الأوروبية بشأن الجرائم الإلكترونية للدول الأطراف إمكانية أن تحد من الأفعال التي تشكل جريمة الاعتراض غير القانوني في الحالات التي ارتكبت فيها، والمقترنة بتوافر نية احتيالية لدى الجاني. انظر: دراسة مكتب الأمم المتحدة المعني بالمخدرات والجريمة بشأن الجريمة السيبرانية، مرجع سابق، ص١٢٥.

العقوبة: عاقب القانون على هذه الجريمة بعقوبة الحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي وخمسين ألف جنيه، أو بإحدى هاتين العقوبتين، ومن ثم يجوز للقاضي الحكم بالعقوبتين معاً، أو بعقوبة الحبس بمفردها، أو الغرامة بمفردها، كما يجوز له استعمال سلطته التقديرية في وقف تنفيذ العقوبة إعمالاً لحكم المادة (٥٥) عقوبات.

المطلب الخامس

جريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية

نص التجريم: تنص المادة (١٧) على جريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية، حيث تقضي المادة المذكورة على أنه: "*يُعاقب الحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل، أو عدل مسار، أو ألغى كلياً أو جزئياً، متعمداً وبدون وجه حق البرامج والبيانات أو المعلومات المخزنة أو المعالجة أو المولدة أو المخلقة على أي نظام معلوماتي وما في حكمه، أياً كانت الوسيلة التي استخدمت في الجريمة*"[(١)].

---

(١) ومن المواثيق الدولية التي حرصت على تجريم التدخل غير المشروع في نظام حاسوبي أو بيانات حاسوبية الاتفاقية العربية بشأن مكافحة جرائم تقنية المعلومات (م٨) والقانون النموذجي العربي لمكافحة جرائم تقنية المعلومات (م٦) وقرار دول الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات (م٣) والمقترح التوجيهي دول الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات (م٤) ومشروع اتفاقية الاتحاد الأفريقي (م١٩/ج و٢٠/ج)، ومشروع ميثاق الكوميسا (م٢٠ب).
ومن التشريعات المقارنة التي عرفت تجريم الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية التشريع الفرنسي، حيث تقضي المادة (٣٢٣-٢) عقوبات فرنسي بأنه: "يعاقب على تعطيل أو إفساد نظام المعالجة الآلية للمعطيات بعقوبة الحبس لمدة خمس سنوات وغرامة قدرها =

العلة من التجريم: تتمثل العلة من التجريم في توفير الحماية الجنائية لسلامة البرامج والنظم المعلوماتية ومحتواها من البيانات والمعلومات من أفعال الإتلاف المادي أو المعنوي، سواء أتخذ ذلك صور التخريب أو الإتلاف أو التعطيل.

محل الجريمة: أشارت المادة المذكورة إلى أن محل جريمة الإتلاف يشمل البرامج والنظم المعلوماتية وما تتضمنها من بيانات ومعلومات، حيث أشارت المادة المذكورة إلى كل من البرامج والبيانات أو المعلومات المخزنة، أو المعالجة، أو المولدة، أو المخلقة على أي نظام معلوماتي وما في حكمه، وقد سبق لنا تناول مدلول النظام المعلوماتي والبيانات والمعلومات الإلكترونية في الجرائم السابقة، وهو ما سوف نحيل إليه منعاً للتكرار، بينما يقصد بالبرنامج المعلوماتي:" ***مجموعة الأوامر والتعليمات المعبر عنها بأي لغة أو رمز أو إشارة والتي تتخذ أي شكل من الأشكال، ويمكن استخدامها بطريق مباشر أو غير مباشر في حاسب آلي لأداء وظيفة أو تحقيق نتيجة، سواء كانت هذه الأوامر والتعليمات في شكلها الأصلي أو في أي شكل آخر تظهر فيه من خلال حاسب آلي، أو نظام معلوماتي***"[1].

=

٧٥ ألف يورو. وإذا ارتكبت الجريمة ضد نظام المعالجة الآلية للبيانات الشخصية التي تنفذها الدولة فإن العقوبة تزيد إلى الحبس لمدة سبع سنوات وغرامة قدرها ١٠٠ ألف يورو"، بينما تقضي المادة (٣٢٣-٣) عقوبات فرنسي بأنه: "يعاقب على الإدخال للمعطيات بطريق الغش في نظام المعالجة الآلية أو محوها أو التعديل بطريق الغش للمعطيات التي يحتويها بعقوبة الحبس لمدة خمس سنوات وغرامة قدرها ٧٥ ألف يورو. وإذا ارتكبت الجريمة ضد نظام المعالجة الآلية للبيانات الشخصية التي تنفذها الدولة فإن العقوبة تزيد إلى الحبس لمدة سبع سنوات وغرامة قدرها ١٠٠ ألف يورو". كما نص على هذه الجريمة كذلك الفقرة الأولي من المادة الرابعة من الاتفاقية الأوروبية للإجرام المعلوماتى، والتشريع الإنجليزي (م١٧ من قانون إساءة استخدام الحاسبات الآلية في المملكة المتحدة)، ومن التشريعات العربية التشريع الجزائري (م٣٩٤ مكرر)، وقانون سلطنة عمان (م٨٣ من مشروع المعاملات والتجارة الإلكترونية العماني)، بينما جرمت بعض التشريعات العربية تعطيل أنظمة التشغيل كالتشريع الجزائري(م٣٩٤ مكرر/٣ عقوبات جزائري) والنظام السعودي (م٥)، والقانون الأردني (م٣)، والقانون السوداني (م٨).

[1] ومن التشريعات التي تضمنت تعريف للبرنامج المعلوماتي التشريعين الإماراتي والأردني.

الركن المادي: يتكون الركن المادي للجريمة من عنصرين: الأول هو الإضرار بسلامة البيانات، والثاني أن يكون ذلك بطريق غير مشروع، وذلك على النحو التالي:-

أ) تحقق إحدى صور الإضرار بسلامة البيانات: وتفترض هذه الجريمة قيام الجاني بأي سلوك أو سلبي من شأنه الإضرار بسلامة البيانات والمعلومات والنظم المعلوماتية، ويستوي لدى القانون الوسيلة المستخدمة في إحداث الإضرار بالبيانات والمعلومات، فقد تكون أداة مادية أو برنامج ضار كالفيروس أو التروجنس أو خلافه، ومن أبرز صور الضرر التي تلحق بالبيانات والمعلومات والنظم المعلوماتية، والتي أشار إليها القانون، الإتلاف والتخريب والتعطيل وتعديل المسار والإلغاء، وذلك على النحو التالي:-

١) الاتلاف: ويقصد به إفناء مادة الشيء أو هلاكه كلياً أو جزئياً، ويتحقق بأي فعل إيجابي أو سلبي من شأنه جعل النظام المعلوماتي أو البيانات أو المعلومات غير صالحة للاستخدام، وقد يكون هذا الإتلاف مادياً، يتمثل في أي عمل إيجابي أو سلبي يترتب عليه الإضرار بهذه الأجهزة والمُعدات وإتلافها أو تعطيها عن العمل، وقد يكون الإتلاف معنوياً يستهدف نظم التشغيل والبرامج والتطبيقات وقواعد البيانات، وتتم بواسطة برامج خبيثة (فيروسات وتروجنس)، وقد يتخذ الإتلاف المعنوي إحدى الصور التالية:

(الصورة الأولى) هي تدمير البيانات والمعلومات، على النحو السالف.

(الصورة الثانية) هي الإدخال غير المشروع للمعلومات والبيانات داخل أنظمة الحاسبات الآلية، أو تدميرها أو التعديل غير المشروع لها، ويتم ذلك عن طريق إضافة معطيات جديدة لم تكن موجودة من قبل على الدعامة الخاصة سواء كانت خالية أو كان يوجد بها معطيات، وذلك قد يتم بهدف التشويش على صحة البيانات والمعلومات القائمة.

(الصورة الثالثة)، فهي التعديل غير المشروع للمعلومات والبيانات، ويقصد بها إجراء نوع من التغيير غير المشروع للمعلومات والبيانات المحفوظة داخل النظام واستبدالها بمعطيات ومعلومات جديدة أخري باستخدام إحدى وظائف الحاسب الآلي[١].

تساؤل: هل يعد إخفاء المعلومات إتلافاً لها؟ ميزت التوصية الصادرة من المجلس الأوروبي بشأن الجرائم المعلوماتية بين شكلين من أشكال التدمير الذي يلحق بالمعلومات، (الأول) يتعلق بمحو المعلومات تماماً، (والثاني) بإخفاء المعلومات، بحيث لا يمكن الوصول إليها دون أن يترتب على ذلك محوها تماماً، وقد ذهب البعض[٢]- بحق- إلى أن إخفاء المعلومات والبيانات دون محوها لا يشكل تدميرا لها، ومؤدى ذلك أن إخفاء أحد الملفات على سبيل المثال لا يترتب عليه محو المعلومات التي يحتوى عليها من ذاكرة الحاسب الآلي وإنما يؤدي فقط إلى تعديل في قائمة الملفات، وهو ما يعد تعديلاً، وليس تدميراً لها.

---

(١) ومن التشريعات المقارنة التي جرمت صورة تعديل المعلومات كإحدى صور الركن المادي لجريمة الإتلاف القانون الإنجليزي (م ١٧ من قانون إساءة استخدام الحاسبات الآلية البريطاني ١٩٩٠م) والقانون العماني (البند السادس من المادة ٢٧٦مكرر من قانون الجزاء العماني، والمادة٨٣ من مشروع المعاملات والتجارة الإلكترونية العماني). وكانت التوصية الصادرة عن المجلس الأوروبي السالفة الذكر قد فرقت بين التعديلات غير المشروعة التي تؤدي إلى نتائج سلبية وبين التعديلات غير المشروعة والتي تساعد على تحسين أي من المكونات المنطقية للحاسب الآلي ونظامه، حيث طالبت التوصية بإدراج التعديلات ذات الآثار السلبية ضمن القائمة الأساسية للجرائم المعلوماتية، في حين أنها اكتفت بخصوص التعديلات ذات النتائج الإيجابية بإدراجها ضمن القائمة الاختيارية. أنظر: مقال بعنوان صور الاعتداء على المكونات المنطقية للحاسب الآلي، والمنشور على الموقع الإلكتروني:http://irbd.hooxs.com/t16011-topic

(٢) الموضع السابق

٢) التخريب: ويعني توقف الشيء تماماً عن أن يؤدي منفعته كلياً أو جزئياً، ويتحقق بأي فعل مادي من شأنه إيقاف الأجهزة المادية القائمة على تشغيل النظام المعلوماتي عن العمل.

٣) التعطيل: ويقصد به توقف الشيء عن القيام بوظيفته لفترة مؤقتة، ويتحقق بأي فعل من شأنه إيقاف عمل النظام المعلوماتي.

٤) تعديل المسار: ويقصد بذلك تغيير المعطيات الخاصة بالبرامج أو البيانات أو المعلومات في النظام المعلوماتي، ومن ثم تغيير مسارات تشغيلها باستخدام إحدى وظائف الحاسب الآلي، وهو ما يتحقق باستخدام برمجيات متخصصة في ذلك[١].

٥) الإلغاء: يقصد به إزالة البيانات أو المعلومات الموجودة داخل البرنامج أو النظام المعلوماتي، ويستوي لدى القانون أن يكون الإلغاء كلياً أو جزئياً[٢].

ب) أن يكون الإضرار بدون وجه حق: تطلب القانون لتحقق الجريمة أن يكون الإضرار بسلامة البيانات بدون وجه حق؛ أي أن يكون غير مشروع، وهو أمر بديهي، ويكون الإتلاف غير مشروع إذا كان غير مطابقاً للقوانين أو اللوائح والتعليمات، ويرجع تقدير هذه الأمور لسلطة قاضي الموضوع، يقدرها في ضوء ظروف وملابسات الجريمة.

وتبرز الإشارة إلى أن المشرع الفرنسي يميز بين إتلاف النظام المعلوماتي والذي يخضع لنص المادة (٣٢٣-٢)، وإتلاف المعلومات المخزنة على الذاكرة أو على وسائط التخزين، والذي يخضع لنص المادة (٣٢٣-٣) من قانون العقوبات، حيث يشدد

---

[١] د. حسنى الجندي: قانون مكافحة جرائم تقنية المعلومات، مرجع سابق، ص١٢٢.

[٢] قارن: الموضع السابق.

المشرع الفرنسي العقوبة في الحالة الأولى عنها في الحالة الثانية، ومن التطبيقات القضائية لجريمة إتلاف المعلومات إدانة إحدى محاكم الاستئناف الفرنسية عام ١٩٩٠ لأحد الأشخاص لقيامه بإدخال بيانات غير صحيحة إلى نظام الحاسب الآلي، وهو ما أكدت عليه محكمة النقض الفرنسية في حكم لها صادر عام ١٩٩٩ حينما ذهبت إلى أن إدخال بيانات يترتب عليها إتلاف لأي من المكونات المنطقية لنظام الحاسب الآلي هو سلوك معاقب عليه ولو كان للجاني حق الدخول إلى هذا النظام، بينما أدانت إحدى المحاكم الفرنسية في قضية أخرى عام ١٩٩٤م أحد المتهمين لقيامه بإدخال برنامج خبيث "حصان طروادة" إلى نظام الحاسب الآلي، مما ترتب عليه إتلاف للمعلومات، فضلاً عن إعاقة النظام عن أداء وظائفه، وهو ما أكدت عليه محكمة النقض الفرنسية حينما ذهبت في حكم لها عام ١٩٩٦م إلى أن إدخال البرامج الخبيثة إلى نظام الحاسب الآلي هو سلوك معاقب عليه تطبيقا المادة (٢/٣٢٣) من قانون العقوبات[١].

الركن المعنوي: هذه الجريمة من الجرائم العمدية التي يتحقق فيها الركن المعنوي بتوافر القصد الجنائي العام بعنصريه العلم والإرادة[٢]، بأن يعلم الجاني بأن فعله يشكل اعتداء على سلامة الأنظمة المعلوماتية، وأن تتجه إرادته إلى تحقيق ذلك، وهو ما أشارت إليه المادة (١٧) صراحة بذكرها عبارة:"كل من أتلف...متعمداً"، ومن

---

[١] أنظر في تفصيلات حكم محكمة جنح ليموج الفرنسية وحكم محكمة النقض الفرنسية: د.جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، مرجع سابق، ص ص٦٢،٦٣.

[٢] تشترط العديد من الصكوك متعددة الأطراف المعنية بمكافحة جرائم تقنية المعلومات أن تتوافر نية الفعل المتعمد أو نية القصد الاحتمالي لقيام جريمة التدخل غير القانوني في النظم أو البيانات كالاتفاقية العربية بشأن مكافحة جرائم تقنية المعلومات (م٨) وقرار دول الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات (م٣) والمقترح التوجيهي دول الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات (م٤) ومشروع اتفاقية الاتحاد الأفريقي (م١٩/ج و ٢٠/ج)، ومشروع ميثاق الكوميسا (م٢٠ب).

ثم لا تتحقق الجريمة إذا كان تحقق الإتلاف قد تم بدون قصد من الفاعل، أو كان عن طريق الخطأ، وإثبات القصد الجنائي من الأمور الباطنية غير الظاهرة، والتي يجوز إثباتها بكافة طرق الإثبات.

العقوبة: عاقب القانون على هذه الجريمة بعقوبة الحبس مدة لا تقل عن سنتين والغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، ومن ثم يكون القاضي وفقاً لظروف وملابسات الدعوى الحكم بالحبس الذي لا تقل مدته عن سنتين ولا تجاوز ثلاث سنوات فقط، أو بالغرامة التي لا يقل حدها الأدنى عن مائة ألف جنيه ولا يتجاوز حدها الأقصى ثلاثمائة ألف جنيه فقط، أو بالعقوبتين معاً[1].

المطلب السادس

جريمة الاعتداء على البريد الإلكتروني أو المواقع أو الحسابات الخاصة

نص التجريم: تنص المادة (١٨) على جريمة الاعتداء على موقع أو حساب خاص أو بريد إلكتروني لآحاد الناس، حيث تقضي المادة المذكورة بأنه:" *يُعاقب بالحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل أو أبطأ أو اخترق بريداً*

(١) لم تقرر الصكوك الدولية متعددة الأطراف المعنية بمكافحة جرائم تقنية المعلومات شروطاً لتشديد العقاب في جرائم التدخل غير القانوني في البيانات، ألا أن بعض المواثيق كالمشروع التوجيهي للإتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات قد طالب الدول بأن تقر الظروف المشددة في حالة تورط منظمات إجرامية، أو إذا ارتكبت الجريمة من خلال استعمال أدوات مصممة للهجوم على عدد من نظم المعلومات الهامة، أو عند إخفاء الهوية الحقيقية للجاني(م١٠). انظر: دراسة مكتب الأمم المتحدة، مرجع سابق، ص١٣١.

إلكترونياً أو موقعاً أو حساباً خاصاً بآحاد الناس. فإذا وقعت الجريمة على بريد إلكتروني أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة، تكون العقوبة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتين ألف جنيه، أو بإحدى هاتين العقوبتين".

العلة من التجريم: تتمثل العلة من التجريم في توفير الحماية الجنائية خصوصية الأفراد مستخدمي الشبكة المعلوماتية ووسائل الاتصالات والمعلومات، من خلال تجريم الاعتداء على حساباتهم الخاصة أيا كانت صورتها، سواء أكانت بريداً إلكترونياً أو موقعاً خاصاً أو حساباً خاصاً.

محل الجريمة: يتمثل محل الجريمة في البريد الإلكتروني والمواقع الإلكترونية والحسابات الخاصة، وقد سبق لنا تناول تعريف المواقع الإلكترونية والحسابات الخاصة في الجرائم السابقة، بينما عرف القانون البريد الإلكتروني بأنه:"*وسيلة لتبادل رسائل إلكترونية على عنوان محدد، بين أكثر من شخص طبيعي أو اعتباري، عبر شبكة معلوماتية، أو غيرها من وسائل الربط الإلكترونية من خلال أجهزة الحاسب الآلي وما في حكمها*"[1]، فالبريد الإلكتروني هو برنامج معد لتبادل الرسائل الإلكترونية بسرعة فائقة سواء أكانت معلومات أم بيانات أم صور، ومن أبرز مواقع البريد الإلكتروني موقع ياهو وهوتميل وجيميل.

---

[1] ومن التشريعات المقارنة التي عرفت البريد الإلكتروني التشريع الفرنسي، حيث عرفت المادة الأولى من القانون الصادر في ٢٠٠٤/٦/٢٢ بشأن الثقة في الاقتصاد الرقمي في فرنسا البريد الإلكتروني بأنه:" كل رسالة، أيا كان شكلها نصية أو صوتية، أو مصحوبة بصور وأصوات، يتم إرسالها عبر شبكة عاملة للاتصالات، ويتم تخزينها على أحد خوادم هذه الشبكة او في المعدات الطرفية للمرسل إليه حتى يتمكن هذا الأخير من استعادتها". انظر: المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٢٢٣.

وقد انتقد البعض[١] هذا التعريف لما ينطوي عليه من اتساع وخلط بين رسائل البريد الإلكتروني والرسائل الإلكترونية المرسلة عبر تطبيقات التواصل المختلفة كالواتس آب والفيسبوك والماسنجر، وهو ما يتنافى مع التعريف القانوني السليم الذي يجب ألا يختلط به شيء آخر، إلا أن الباحث يرى أن من شأن هذا التوسع شمول الحماية الجنائية لكافة المراسلات الإلكترونية، بينما يعرف البعض الآخر[٢] البريد الإلكتروني بأنه:" خط مفتوح على كافة أنحاء العالم، وفي ثوان معدودة، ويحتفظ الحاسب بالرسائل في صندوق البريد، ويتيح خدمة كتابة الرسائل وإمكانية إرسال الصور والرسائل الصوتية وغيرها، ويكون لكل مستخدم له بعنوان بريدي وشفرة سرية".

الركن المادي: يتحقق الركن المادي في هذه الجريمة باعتداء الجاني على البريد الإلكتروني أو موقع أو حساب خاص للمجني عليه، ويستوي لدى القانون أن يكون المجني عليه فرداً أم شخصاً اعتبارياً خاصاً، إلا أن المشرع قد ميز بينهم من حيث العقوبة فكانت العقوبة بالنسبة للأخير أشد من المقررة للأول، وتتعدد صور الاعتداء المجرم، لتشمل صور الإتلاف أو التعطيل أو الإبطاء أو الاختراق، ولا شك في أن الأفعال الثلاثة الأولى تفترض أن الجاني قد تمكن من الدخول غير المشروع للبريد الإلكتروني أو الموقع الإلكتروني أو الحساب الخاص، حتى يتمكن من ارتكاب الأفعال المشار إليها، ومن ثم جاء النص القانوني ليشير إلى فعل الاختراق لتتحقق الحماية الجنائية المتكاملة لهذه المواقع أو الحسابات أو البريد الإلكتروني، ومن ثم يرى الباحث

---

[١] انظر: المستشار د. محمد سمير: قانون العقوبات الاقتصادي، الموضع السابق.

[٢] انظر: د. عبد الهادي العوضي: الجوانب القانونية للبريد الإلكتروني، دار النهضة العربية، القاهرة، ٢٠٠٥، ص١٣ ومابعدها؛ د.محمود عبد العزيز أبازيد: الحماية الجنائية لتكنولوجيا الحاسب الآلي والنظم المعلوماتية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ٢٠١٥، ص١١؛ المستشار د. محمد سمير: المرجع السابق، ص٢٢٣.

أن كان من الأحرى بالمشرع تقديم فعل الاختراق على الأفعال الأخرى بالنظر إلى أن هذه الأفعال هي أفعال تالية على الاختراق أو الدخول غير المشروع، وبالتالي يكون النص أكثر منطقية، من حيث تجريمه للفعل الأولي بداءةً وهو الاختراق ثم يلي ذلك تجريم الإتلاف والتعطيل والإبطاء بالنظر إلى اعتبارهم أفعال تالية لفعل الاختراق، وفيمايلي نتناول صور السلوك الإجرامي المكون لهذه الجريمة، وذلك على النحو التالي:-

١) الاختراق: عرف القانون الاختراق بأنه:" الدخول غير المرخص به أو المخالف لأحكام الترخيص، أو الدخول بأي طريقة غير مشروعة إلى نظام معلوماتي أو حاسب آلي أو شبكة معلوماتية وما في حكمها"[1]، ومن ثم يتحقق فعل الاختراق بأي فعل من شأنه تمكين الجاني من الدخول غير المشروع للبريد الإلكتروني للمجني عليه أو موقعه أو حسابه الخاص.

وغالباً ما يكون الاختراق باستخدام برامج متخصصة لاختراق المواقع والأنظمة المعلوماتية والحسابات الشخصية، أي بدون أن يكون مصرح للجاني بالدخول لهذا البريد أو الحساب أو الموقع باستخدام كلمة أو كود رمزي للمرور إليه. كما قد يتحقق الاختراق من خلال تمكن المتهم من الاستيلاء على جهاز الحاسب الآلي الشخصي للمجني عليه والولوج إلى البريد الإلكتروني أو الحساب الخاص على مواقع التواصل الاجتماعي أو الموقع الإلكتروني الخاص بالمجني عليه.

وقد أدانت إحدى المحاكم أحد المتهمين لقيامه بسرقة الحاسب الآلي المحمول الخاص بالمجني عليها واستخدامه في الاستيلاء على البروفايل (الحساب) الخاص بها

---

[1] تبرز الإشارة إلى أن التشريع المصري قد عرف جريمة الاختراق بينما أخذت التشريعات العربية بمصطلح الدخول غير المشروع، ومن أبرزها التشريع الكويتي والنظام السعودي.

على موقع فيسبوك، عن طريق الدخول إلى شبكة الإنترنت بجهاز حاسب آلي مرتبط على خط هاتف غير منزلي والمسجل باسم المتهم، وكانت النيابة العامة قد أسندت إلى المتهم قيامه بالتوصل بغير حق إلى الحصول على توقيع الوسيطين الإلكترونيين (البريد الإلكتروني وحساب الفيسبوك) الخاص بالمجني عليها[١].

٢) الإتلاف: ويتحقق ذلك بأي فعل من شأنه جعل البريد الإلكتروني أو الموقع أو الحساب الخاص غير صالح للاستخدام، كما لو قام الجاني بتغيير المحتوى المعلوماتي له أو حذف البيانات من عليه، بما يعيق صاحبه من استخدامه أو استعماله مرة أخرى، والإتلاف قد يكون كلياً أو جزئياً.

وفي إحدى القضايا الأخرى أدانت إحدى المحاكم أحد المتهمين لقيامه باختراق موقع إحدى الشركات الخاصة على شبكة المعلومات الدولية الإنترنت، من خلال جهاز حاسب آلي متصل بشبكة الإنترنت مرتبط بخط هاتف مسجل باسم شركة مملوكة للمتهم، وقيامه بحذف جميع البيانات من على موقع الشركة وتحميل مقطع فيديو بغرض الاستهزاء بالموقع، نظراً لوجود منافسة بين المتهم وصاحب الشركة في العمل، حيث أن كلاهما يعملان في مجال الأمن التكنولوجي، وكانت النيابة العامة قد أسندت إلى المتهم قيامه بالتوصل بغير حق إلى الحصول على توقيع الوسيط الإلكتروني (الموقع الإلكتروني الخاص بالمجني عليه) واختراق الوسيط الإلكتروني وتعييبه[٢].

---

[١] انظر حكم محكمة جنح القاهرة الاقتصادية، جلسة ٢٠١٢/٤/٢٨، الدعوى رقم (٣٢٧) لسنة ٢٠١٢ جنح القاهرة الاقتصادية، مشار إليها المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص ص٦٦١، ٦٦٢.

[٢] انظر حكم محكمة جنح القاهرة الاقتصادية، جلسة ٢٠١٢/١/٢٢، الدعوى رقم (١٩٠١) لسنة ٢٠١١ جنح القاهرة الاقتصادية، مشار إليها المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص ص٦٦٢، ٦٦٣.

وتبرز الإشارة إلى أن التطبيقات السابقة كانت تؤسس إدانتها على أحكام القانون رقم ١٥ لسنة ٢٠٠٤ في شأن تنظيم التوقيع الإلكتروني من خلال إسناد تهمة بالتوصل بغير حق إلى الحصول على توقيع الوسيط الإلكتروني، حيث اعتبرت المواقع الإلكترونية والحسابات الخاصة والبريد الإلكتروني من قبيل الوسيط الإلكتروني، وكانت المادة الأولى من قانون تنظيم التوقيع الإلكتروني تعرف الوسيط الإلكتروني بأنه:" أداة أو أدوات أو أنظمة إنشاء التوقيع الإلكتروني"، وأن التوصل بغير حق يتحقق به فعل الاعتداء على هذه المواقع والحسابات، وذلك باختراق هذه الوسائط الإلكتروني.

ويرى الباحث أن هذا النهج القضائي في اعتبار هذه المواقع أو الحسابات الخاصة من قبيل الوسائط الإلكترونية بغرض بسط الحماية الجنائية على مثل هذه الجرائم، نظراً لغياب النص القانوني الصريح لتجريم الاعتداء على البريد الإلكتروني أو المواقع أو الحسابات الخاصة.

٣) التعطيل: ويتحقق ذلك بأي فعل من شأنه إيقاف عمل البريد الإلكتروني أو الموقع أو الحساب الخاص للمجني عليه، ويستوي لدى القانون أن يكون التعطيل دائماً أم مؤقتاً.

٤) الإبطاء: ويتحقق ذلك بأي فعل من شأنه تقليل كفاءة وسرعة استخدام البريد الإلكتروني أو الموقع أو الحساب الخاص للمجني عليه.

الركن المعنوي: هذه الجريمة من الجرائم العمدية التي يتحقق فيها الركن المعنوي بتوافر القصد الجنائي العام بعنصريه العلم والإرادة، بأن يعلم الجاني بأن من شأن فعله إتلاف أو تعطيل أو إبطاء أو اختراق البريد الإلكتروني للغير أو موقع أو حساب خاص بآحاد الناس أو أحد الأشخاص الاعتبارية الخاصة، وأن تتجه إرادته إلى تحقيق ذلك.

العقوبة: ميز القانون في العقوبة بين حالتين، بحسب صفة المجني عليه، حيث شدد العقاب في حال كون المجني عليه أحد الأشخاص الاعتبارية الخاصة، وذلك على النحو التالي:-

(الحالة الأولى) كون المجني عليه من أحاد الناس: عاقب القانون على هذه الجريمة بعقوبة الحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى العقوبتين، ومن ثم يجوز للقاضي وفقاً لسلطته التقديرية في ضوء ظروف وملابسات القضية أن يقضي بعقوبة الحبس أو بعقوبة الغرامة، أو بالعقوبتين معاً، كما يجوز له أن يأمر بوقف تنفيذ العقوبة وفقاً للمادة (٥٥) عقوبات.

(الحالة الثانية) كون المجني عليه من الأشخاص الاعتبارية الخاصة: عاقب القانون على هذه الجريمة في حال كون المجني عليه أحد الأشخاص الاعتبارية الخاصة كالشركات التجارية والمؤسسات الخاصة والجمعيات الخاصة بعقوبة الحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه أو بإحدى العقوبتين، ومن ثم يجوز للقاضي -كما سبق أن أشرنا- وفقاً لسلطته التقديرية في ضوء ظروف وملابسات القضية أن يقضي بعقوبة الحبس أو بعقوبة الغرامة، أو بالعقوبتين معاً، كما يجوز له أن يأمر بوقف تنفيذ العقوبة وفقاً للمادة (٥٥) عقوبات.

المطلب السابع

جريمة الاعتداء على تصميم الموقع الإلكترونية

نص التجريم: تضمنت المادة (١٩) جريمة الاعتداء على تصميم موقع، حيث تقضي المادة المذكورة بأنه:" *يُعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل*

من أتلف أو عطل أو أبطأ أو شوه أو أخفي أو غير تصاميم موقع خاص بشركة أو مؤسسة أو منشأة أو شخص طبيعي بغير وجه حق"[١].

العلة من التجريم: تتمثل العلة من التجريم في توفير الحماية الجنائية للمحتوى المعلوماتي الخاص بالمواقع الإلكترونية، والذي يمثل أحد أبرز وسائل تعريفه وتمييزه عن غيره، ألا وهو التصميم الخاص بالموقع الإلكتروني، فضلاً عن اعتبار هذه الجريمة من جرائم التلاعب بمعطيات الحاسب الآلي من أجل إعاقة أو إنشاء النظم والمواقع الإلكترونية.

محل الجريمة: تنصب هذه الجريمة على تصاميم المواقع الإلكترونية، والتصميم هو أول عملية في سلسلة التعامل مع معطيات الحاسب الآلي وهي تمثل إخراج المعطيات إلى الوجود، بينما الموقع الإلكتروني هو مساحة تمثلها مؤسسة أو شخص ما في الفضاء الإلكتروني، ويتوقف تقرير نوع الموقع الذي يراد إنشاؤه أو تصميمه، على ماذا تريد أن تعرضه فيه، أو ماذا يفعل زائر الموقع به وعلى ما يحتوي عليه هذا الموقع، فكل جهة أو شركة أو مؤسسة تضع بياناتها على شبكة الإنترنت، يكون لها موقع محدد له عنوان يمكن لأي مستخدم الدخول بواسطته إلى الموقع بسهولة، ويقوم مؤسسوا هذا الموقع بتصميم هذه الصفحة بطريقة تعبر عن هويتهم ونشاطاتهم والخدمات التي يوفرونها، مع الأخذ في الاعتبار ضرورة تصميمه بطريقة جذابة ومثيرة لاجتذاب أكبر عدد من الزائرين لهذا الموقع، وأيضاً بطريقة منظمة لتسهيل عملية التجول داخل الموقع والاطلاع على أي بيانات متاحة للمشتركين[٢].

---

[١] ومن التشريعات العربية التي عرفت تجريم الاعتداء على تصاميم المواقع الإلكترونية، التشريع الإماراتي (م٥) والتشريع الكويتي(م٤).

[٢] د. جميل عبد الباقي الصغير، المرجع السابق، ص٥٨، هامش١.

الركن المادي: يمثل الركن المادي في الاعتداء على الموقع الإلكتروني والذي يتخذ صور الإتلاف أو التعطيل أو الإبطاء أو التشويه أو الإخفاء أو التغيير للتصميم الخاص بالموقع الإلكتروني، ويستوي لدى القانون أن يكون هذا الموقع يخص شخص طبيعي أو شخص معنى خاص كشركة أو مؤسسة أو منشأة. وقد سبق تناول أفعال الإتلاف، والتعطيل، وهو ما سنتناوله بإيجاز على النحو التالي:-

١) الإتلاف: وهو كل فعل من شأنه جعل الموقع غير صالح للاستخدام.

٢) التعطيل: وهو ما يتحقق بكل فعل من شأنه إيقاف عمل الموقع.

٣) تغيير تصميم الموقع: ويقصد به تعديل البيانات أو المعطيات التي تخص إنشاء أو تكوين أو بناء الموقع الإلكتروني، ومن بينها بيانات الأسماء والصور والنصوص وعنوان الموقع.

٤) الإخفاء: ويقصد به كل فعل يقوم به الجاني يكون من شأنه عدم إظهار الموقع الإلكتروني على الشبكة المعلوماتية، ومن ثم ستره وحجبه عن الظهور على الشبكة المعلوماتية.

٥) الإبطاء: وهو من صور تعطيل الموقع الإلكتروني ويقصد به كل من شأنه الإقلال من كفاءة وسرعة الموقع.

٦) التشويه: وهو من صور الإتلاف فيقصد به كل فعل من شأنه الإساءة إلى شكل الموقع الإلكتروني، وبظهوره بشكل غير مقبول من جانب مستخدميه، فالتشويه هو إتلاف جزئي، فقد يقع الإتلاف على الموقع بأكمله، فيكون إتلافاً، وقد يكون جزئياً، فيحدث تشويهاً أو تعييباً فيه، ويحدث ذلك من خلال قيام الجاني بإدخال فيروس داخل

الموقع أو باستخدام البرامج الخبيثة، بحيث يعمل على التقليل من كفاءته، أو فقدان بعض ملفاته أو مسحها[١].

أن يكون التغيير بطريق غير مشروع: يتطلب القانون أن يكون هذا التغيير بغير وجه حق، بأن يكون هذا التعديل أو التغيير قد تم من شخص غير مصرح له قانوناً بالدخول أو بتعديل البيانات أو تغييرها، فمناط عدم المشروعية هو انعدام سلطة الجاني في الدخول إلى الموقع مع علمه بذلك[٢].وتبرز الإشارة إلى أن الاعتداء على تصاميم المواقع الإلكترونية يفترض ارتكاب الجاني لفعل الدخول غير المشروع للموقع الإلكتروني حتى يتسنى له تغيير تصاميم الموقع، وهو ما يتحقق من خلال اتخاذ الموقع لشكل آخر غير الذي كان عليه قبل الدخول إليه، أو أن يقوم الجاني بمحو بعض بيانات الموقع أو برامجه ويضع محلها بيانات أخرى.

الركن المعنوي: هذه الجريمة من الجرائم العمدية التي يتحقق فيها الركن المعنوي بتوافر القصد الجنائي العام بعنصريه العلم والإرادة، بأن يعلم الجاني بأن فعله يمثل دخولاً غير مشروع إلى موقع إلكتروني، وبأن الجاني ليس مصرحاً له بدخول الموقع الإلكتروني، وأن من شأن فعله الإضرار بسلامة البيانات والمعلومات التي تشكل الموقع الإلكتروني، وأن تتجه إرادته إلى الدخول غير المشروع والإضرار بسلامة بيانات المواقع الإلكترونية بتغيير تصميم الموقع أو إتلاف الموقع أو تعطيله أو تشويهه، وهذه الجريمة من جرائم القصد الجنائي الخاص، فيجب أن تتجه نيه الجاني إلى تغيير شكل الموقع الإلكتروني أو إخفائه أو تشويهه أو إتلافه[٣].

---

[١] د. حسنى الجندي: قانون مكافحة جرائم تقنية المعلومات، مرجع سابق، ص١٩١.

[٢] د. حسنى الجندي: المرجع السابق، ص١٩٠؛ د. نائلة عادل محمد فريد قورة: المرجع السابق، ص٣٣٣.

[٣] د. حسنى الجندي: المرجع السابق، ص١٩١.

العقوبة: عاقب القانون على هذه الجريمة بعقوبة الحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى العقوبتين، ومن ثم يجوز للقاضي -كما سبق أن أشرنا- وفقاً لسلطته التقديرية في ضوء ظروف وملابسات القضية أن يقضي بعقوبة الحبس أو بعقوبة الغرامة، أو بالعقوبتين معاً، كما يجوز له أن يأمر بوقف تنفيذ العقوبة وفقاً للمادة (٥٥) عقوبات.

المطلب الثامن

جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة

نص التجريم: أقر القانون عقوبة رادعة لجريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة، وتجريم الولوج أو البقاء غير المشروع أو تجاوز الحق في الولوج لموقع أو حساب أو نظام معلوماتي يخص الدولة أو أحد الأشخاص الاعتبارية العامة، حيث تنص المادة (٢٠) على جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة، حيث تقضي المادة المذكورة بأنه:" *يُعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمداً، أو دخل بخطأ غير عمدي وبقي بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوي الدخول أو اخترق أو بريداً إلكترونياً أو حساباً خاصاً أو نظاماً معلوماتياً يُدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوك لها، أو يخصها. فإذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية، تكون العقوبة السجن، والغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه. وفى جميع الأحوال، إذا ترتب على أي من الأفعال السابقة إتلاف تلك البيانات أو مات أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي أو البريد*

الإلكتروني، أو تدميرها، أو تشويهها أو تغييرها أو تغيير تصاميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها، أو إلغاؤها كلياً أو جزئياً، بأي وسيلة كانت، تكون العقوبة السجن، والغرامة التي لا تقل عن مليون جنيه ولا تجاوز خمسة ملايين جنيه"[١].

العلة من التجريم: تتبلور العلة من تجريم الاعتداء على الأنظمة المعلوماتية والمواقع الإلكترونية الخاصة بالدولة أو الأشخاص المعنوية العامة فيمايلي:-

١- مواجهة محاولات الاعتداء على الأنظمة المعلوماتية والمواقع الإلكترونية والحسابات المملوكة للدولة أو أحد الأشخاص الاعتبارية العامة، وتوفير الحماية القانونية لتأمين هذه المواقع أو الحسابات.

٢- تعد المواقع الحكومية هي المواقع الأكثر رسمية وتمثيلاً لسيادة الدولة على الفضاء الإلكتروني، وأن العدوان عليها يؤثر بشكل كبير في هيبة الدولة وفي نفوس المواطنين[٢].

محل الجريمة: استلزم القانون أن يكون محل الجريمة موقعاً أو بريداً إلكترونياً أو حساباً خاصاً أو نظاماً معلوماتياً يدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوك لها أو يخصها، ومن يخرج من نطاق التجريم بموجب هذا النص المواقع أو الحسابات الشخصية المملوكة للأفراد أو أشخاص القانون الخاص،

---

(١) تبرز الإشارة إلى أن قانون مكافحة الإرهاب رقم ٩٤ لـ٢٠١٥ قد سبق قانون مكافحة جرائم تقنية المعلومات في تجريم الدخول غير المصرح به على المواقع الإلكترونية الحكومية بقصد الحصول على البيانات أو المعلومات الموجودة عليها أو إتلافها أو تزويرها لغرض إرهابي(م٢٩/ فقرة٢)، ومن التشريعات العربية التي جرمت الدخول غير المصرح به لموقع إلكتروني أو نظام معلوماتي أو شبكة معلوماتية بقصد الحصول على بيانات حكومية، التشريع الإماراتي (م٤).

(٢) د. أحمد الضبع: إشكاليات مواجهة الإرهاب، مرجع سابق، ص٩٥.

والتي يخضع الاعتداء عليها المواد ١٥ و١٦ من القانون، وقد سبق لنا تعريف كلاً من الموقع والحساب الخاص والنظام المعلوماتي والبريد الإلكتروني. وتبرز الإشارة إلى أن المواقع الحكومية هي المواقع التابعة للنطاق الإلكتروني الخاص بالدولة، وغالباً ما ينتهي عنوانها بـgov، تمييزاً لها عن غيرها[1].

ويذهب البعض إلى أن العدوان على الصفحات الرسمية الحكومية على مواقع التواصل الاجتماعي يبقى خارج نطاق التجريم، حيث أن هذه الصفحات وإن كانت حكومية إلا أنها منشأة على مواقع إلكترونية غير حكومية، بالنظر إلى أن مواقع التواصل الاجتماعي هي مواقع خاصة مملوكة لشركات خاصة، ولا يمكن أن ينسحب وصف المواقع الإلكترونية الحكومية على تلك الصفحات، ومع أن الرأي السابق وإن كان صحيحاً، إلا أن هذا النص القانوني الوارد بالمادة ٢٠ من قانون مكافحة جرائم تقنية المعلومات يتسع ليشمل الحسابات الخاصة للدولة على مواقع التواصل الاجتماعي، فنص المادة ٢٠ من القانون يشير إلى تقرير الحماية الجنائية لأي موقع أو بريد إلكتروني أو حساب خاص أو نظام معلوماتي يدار بمعرفة الدولة أو لحسابها أو أحد الأشخاص الاعتبارية العامة أو مملوك لها أو يخصها.

وتبرز الإشارة في هذا المقام إلى العبرة في إصباغ الحماية الجنائية المقررة للمواقع الإلكترونية أو الحسابات الخاصة أو البريد الإلكتروني يكون بنعتها بالصفة الرسمية عليها، وهو ما لا يتحقق إلا بوجود رابطة بينها وبين الدولة، وهذه الرابطة هي أن هذا الموقع أو الحساب الخاص يدار بمعرفة الدولة أو أحد الأشخاص الاعتبارية العامة أو لحساب الدولة أو أحد أشخاصها الاعتبارية، أو كان مملوكاً للدولة أو أحد أشخاصها الاعتبارية أو يخصهما، ومن ثم يكون الحساب أو الموقع رسمياً إذا كان

---

[1] الموضع السابق.

خاضعاً لإدارة الدولة أو مملوكاً لها. ويقصد بالدولة الحكومة وأجهزتها ووحدات الحكم المحلي، بينما يقصد بالأشخاص الاعتبارية العامة الهيئات والمؤسسات العامة وغيرها من الجهات التي يقرر لها القانون الشخصية الاعتبارية العامة.

الركن المادي: يتحقق الركن المادي في هذه الجريمة من خلال صور السلوك الإجرامي التالية:-

أ) الدخول غير المشروع: يتحقق الركن المادي بفعل الدخول غير المشروع الذي سبق الإشارة إليه بمعرض هذا البحث، ويستوي لدى القانون كما سبق أن أشرنا أن يكون الدخول عمداً أو بخطأ غير عمدي.

ومن ثم يتحقق الركن المادي للجريمة بمجرد الدخول بدون وجه حق ولو لم يقم الجاني بأي نشاط آخر عقب هذا الدخول كحذف البيانات أو العبث بها[1].

ب) تجاوز حدود الحق المخول في الدخول: يتحقق الركن المادي بتجاوز حدود الحق المخول في الدخول كما سبق أن أشرنا، ويستوي لدى القانون أن يكون هذا التجاوز في حدود الحق المخول له من حيث الزمان أو مستوى الدخول.

ج) البقاء غير المشروع: يتحقق الركن المادي بفعل البقاء بدون وجه حق على النحو السالف الإشارة إليه سابقاً.

د) الاختراق: يتحقق الركن المادي بفعل الاختراق، وهو ما يختلف عن الدخول بأن الأخير يكون بفتح جهاز الحاسب الآلي أو باستخدام كلمة سر أو رمز أو كود سري، بينما الاختراق يكون بأية وسيلة أخرى، كأن يكون ذلك باستخدام برامج متخصصة لاختراق المواقع والأنظمة المعلوماتية والحسابات الشخصية، ويعتقد الباحث أن وجه

[1] د. أحمد الضبع: إشكاليات مواجهة الإرهاب، مرجع سابق، ص٩٧.

التمييز بين كل من الدخول والاختراق أن الدخول غير المشروع كان يقصد به الدخول من جانب أحد المتعاملين مع المواقع الإلكترونية أو البريد الإلكتروني أو الحساب الخاص أو النظام المعلوماتي الذي يخص الدولة من الموظفين العموميين العاملين لديها، ومن المصرح لهم بالتعامل معها، فيخالف القواعد والتعليمات الخاصة بالدخول أو البقاء، بينما الاختراق فيكون من غير العاملين بالدولة المصرح لهم بالتعامل مع هذه المواقع الإلكترونية أو الحسابات أو النظم المعلوماتية، كأن يكون شخصاً أجنبياً يحاول الدخول إلى هذه المواقع أو الحسابات أو الأنظمة المعلوماتية الحكومية.

ومن أبرز الوقائع ذات الصلة بالاعتداء على الأنظمة المعلوماتية الخاصة بالدول محاولة اختراق لمستندات المفاعل النووي الإيراني والتي قدرت بحوالي نصف طن من المستندات عن طريق وحدة متخصصة في الجيش الإسرائيلي معروفة بالوحدة ٨٢٠٠[1].

الركن المعنوي: هذه الجريمة -كما سبق أن أشرنا- يمكن أن تقع عمداً أو بطريق غير عمدي، وهو ما أشار إليه المشرع بعبارة:" دخل عمداً أو بخطأ غير عمدى وبقى بدون وجه حق"، ومن ثم فهذه الجريمة قد تتحقق بطريق العمد بتوافر القصد الجنائي العام بعنصريه العلم والإرادة، بأن يعلم الجاني بدخوله بدون وجه حق لموقع إلكتروني أو حساب شخصي أو نظام معلوماتي وبقاءه عليه أو تجاوزه حدود الحق المخول له في الدخول، أو باستخدامه أية برامج لاختراق ودخول هذه المواقع والحسابات، وأن تتجه إرادته إلى تحقيق ذلك، بينما في حالة الخطأ غير العمدي، فإرادة

---

[1] تم الإشارة إلى هذا المثال خلال مناقشات البرلمان المصري لقانون مكافحة جرائم تقنية المعلومات. انظر: مضبطة مجلس النواب المصري، الجلسة السادسة والخمسين، المعقودة في ٢٠١٨/٥/١٤م، مرجع سابق، ص١٠٠.

الجاني لا تتجه إلى الدخول غير المشروع للمواقع أو الحسابات أو النظم المعلوماتية، ولكن الدخول يتحقق بفعل الجاني نتيجة عدم مراعاته لقواعد أمن الحاسبات والمعلومات.

العقوبة[1]: فرق المشرع المصري في العقوبة المقررة للجريمة بحسب طبيعة القصد الجنائي؛ إذ ميز في العقوبة بين القصد العام المجرد والقصد الجنائي الخاص، كما ميز المشرع كذلك في العقوبة إذا ترتب على الجريمة ضرر ما، وهو ما سوف نتناوله في الحالات الثلاث التالية:-

(الحالة الأولى) القصد الجنائي العام: عاقب القانون في هذه الحالة بعقوبة الحبس مدة لا تقل عن سنتين والغرامة التي لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو إحداهما، ومن ثم يجوز للقاضي وفقاً لسلطته التقديرية في ضوء ظروف وملابسات القضية أن يقضي بعقوبة الحبس أو بعقوبة الغرامة، أو بالعقوبتين معاً، وليس للقاضي في هذه الحالة أن يأمر بوقف التنفيذ.

---

[1] تبرز الإشارة إلى مناداة أحد أعضاء البرلمان بتشديد العقوبة الخاصة بجريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة، بالنظر إلى أن العقوبة المقررة لها لا تتناسب مع خطورة الجرم، وأن من يقوم بهذا الاختراق أو التعطيل لتلك الأنظمة إما دول أو عصابات دولية منظمة متعددة الجنسيات، وأن هذا كفيل بإيقاف كافة أنظمة الدولة والمصارف والبورصات المحلية، وأن الخسائر الناجمة عن ذلك قد تصل إلى مليارات الجنيهات، وقد رد السيد المهندس وزير الاتصالات وتكنولوجيا المعلومات بأن هناك تدرج كبير في العقوبات في هذه المادة، سواء كانت العقوبات بالسجن من ثلاث سنوات إلى خمس عشرة سنة، وكذلك تدرج في العقوبات المالية لتصل إلى خمسة ملايين جنيه، وأنه عند إعداد هذا القانون تم النظر إلى القوانين الدولية، بينما نوه السيد الأستاذ الدكتور رئيس مجلس النواب بأن القوانين الخاصة بالإرهاب منصوص فيها على عقوبة لمثل هذه الجريمة، ومن ثم فإن من يقوم بتعطيل الشبكة ينتقل إلى نوع آخر من أنواع التجريم، حيث تصل العقوبات عليها هناك إلى عقوبة السجن المشدد، وأنه بالتصويت على المقترح لم يلق قبولاً من جانب أعضاء البرلمان. انظر: مضبطة مجلس النواب المصري، الجلسة السادسة والخمسين، المعقودة في ٢٠١٨/٥/١٤م، مرجع سابق، ص١٠١.

(الحالة الثانية) توافر قصد خاص: شدد المشرع الجنائي العقوبة في جريمة الدخول غير المشروع للأنظمة المعلوماتية الخاصة بالدولة، بالنظر إلى خطورة مقصد الجاني وتعمده الدخول غير المشروع للأنظمة المعلوماتية الخاصة بالدولة، فالجاني في هذا الحالة قصد الحصول على البيانات أو المعلومات الموجودة على الأنظمة المعلوماتية التي تخص الدولة أو الاطلاع عليها، وهذا الفعل أشد خطورة من الحالة الأولى، بالنظر لما اتجهت إليه الإرادة الآثمة للجاني.

فقد تطلب القانون أن يكون الدخول بقصد خاص يتمثل في الحصول أو الإطلاع على البيانات الحكومية ولو لم يتحقق له قصده، فإذا ما دخل الجاني للموقع الإلكتروني بطريق غير مشروع بقصد السطو على ما به من بيانات، إلا أن الدفاعات الإلكترونية للجهة صاحبة الموقع تمكنت من وقف هذا الدخول غير المشروع دون أن يخلف نشاطه ضرر قامت الجريمة في حق الجاني كاملة[١]، ويميز البعض في هذه الجريمة بين كل من النتيجة الإجرامية المتمثلة في نجاح الجاني في الدخول غير المصرح به على المواقع الإلكترونية، والقصد من هذا الدخول سواء أكان للاطلاع أو الحصول على البيانات التي يتضمنها هذا الموقع أو الحساب[٢]، وفي هذه الحالة تُشدد العقوبة لتصبح السجن والغرامة التي لا تقل عن مائتي ألف جنيه ولا تجاوز خمسمائة ألف جنيه.

وكان القانون قد عرف الاعتراض بأنه:"*مشاهدة البيانات أو المعلومات أو الحصول عليها، بغرض التنصت أو التعطيل أو التخزين أو النسخ أو التسجيل أو تغيير المحتوى أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه، وذلك لأسباب غير مشروعة ودون وجه حق*"، وقد سبق لنا تعريف البيانات الحكومية بأنها:" *بيانات*

---

[١] د. أحمد الضبع: إشكاليات مواجهة الإرهاب، مرجع سابق، ص٩٧.

[٢] الموضع السابق.

***تعلقة بالدولة أو إحدى سلطاتها، أو أجهزتها أو وحداتها، أو الهيئات العامة، أو الهيئات المستقلة أو الأجهزة الرقابية، أو غيرها من الأشخاص الاعتبارية العامة وما في حكمها، والمتاحة على الشبكة المعلوماتية أو على أي نظام معلوماتي أو على حاسب أو ما في حكمها*"، ومن ثم فإن توافر هذا القصد الخاص من شأنه تغيير وصف الجريمة من الجنحة إلى الجناية.**

(الحالة الثالثة) تحقق ضرر من جراء الدخول أو البقاء: أشار القانون إلى أنه: "*وفى جميع الأحوال إذا ترتب على أي من الأفعال السابقة إتلاف تلك البيانات أو المعلومات أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتى أو البريد الإلكتروني أو تدميرها أو تشويهها أو تغييرها أو تغيير تصاميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها أو إلغائها كلياً أو جزئياً بأي وسيلة كانت، تكون العقوبة السجن والغرامة التي لا تقل عن مليون جنيه ولا تجاوز خمسة ملايين جنيه*"، وسبق لنا تناول صور الإضرار المختلفة بالبيانات والمعلومات، والمشار إليها في ظرف التشديد، ومن ثم نحيل إلى ما سبق لنا تناوله في هذا الشأن، ويترتب على توافر هذا القصد الخاص تغيير وصف الجريمة من الجنحة إلى الجناية، ومن ثم يشترط لتحقق الظرف المشدد مايلي:-

١- تحقق إحدى صور الضرر المشار إليها في القانون، وهي الإتلاف أو التدمير أو التشويه أو التغيير أو تغيير التصاميم أو النسخ أو التسجيل أو تعديل المسار أو إعادة النشر أو الإلغاء، على النحو السابق الإشارة إليه في الجرائم السابقة.

٢- أن يقع الضرر على نظام معلوماتي أو موقع إلكتروني أو حساب أو بريد إلكتروني حكومي، يدار بمعرفة أو لحساب الدولة، أو أحد الأشخاص الاعتبارية العامة، أو مملوك لها، أو يخصها.

٣- توافر رابطة السببية بين سلوك الجاني وتحقق الضرر.

ويجوز للقاضي - في هذه الحالة- النزول بالعقوبة وفقاً للسلطة التقديرية المخولة له بالمادة (١٧) عقوبات، وتبرز الإشارة إلى أن المشرع حرص على تجريم هذه الأفعال بوصف الجناية، وتشديد العقوبة عليها لتصل إلى السجن والغرامة، بهدف توفير حماية قانونية لمواجهة صور المساس بالمواقع الإلكترونية والحسابات والأنظمة المعلوماتية المملوكة للدولة، وتحقيق الردع لكل من تسول له نفسه العبث بالمواقع والأنظمة المعلوماتية التي تمتلكها أو تديرها أو تشرف عليها الدولة أو أحد الأشخاص المعنوية العامة، ومن ثم فإن توافر صفة العمومية في البيانات أو المعلومات أو في الموقع أو الحساب الخاص أو النظام المعلوماتى أو البريد الإلكتروني يعد من الظروف المشددة التي تعدل من وصف الجريمة من وصف الجنحة إلى وصف الجناية.

المطلب التاسع

جريمة الاعتداء على سلامة الشبكة المعلوماتية

أولاً- نص التجريم: تنص المادة (٢١) على جريمة الاعتداء على سلامة الشبكة المعلوماتية، حيث تقضي المادة المذكورة على أنه:" ***يُعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من تسبب متعمداً في إيقاف شبكة معلوماتية عن العمل أو تعطيلها أو الحد من كفاءة عملها أو التشويش عليها أو إعاقتها أو اعتراض عملها أو أجرى بدون وجه حق معالجة إلكترونية للبيانات الخاصة بها. ويُعاقب كل من تسبب بخطئه في ذلك بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين.فإذا وقعت الجريمة على شبكة معلوماتية تخص الدولة أو أحد الأشخاص الاعتبارية العامة أو تمتلكها أو تدار***

بمعرفتها تكون العقوبة السجن المشدد، وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه"[1]، وتبرز الإشارة إلى أن المشرع الجنائي حرص على تجريم كافة صور السلوك الإجرامي العمدي وغير العمدي الذي من شأنه التسبب في إيقاف الشبكة المعلوماتية، وهو ما سوف نتناوله لاحقاً.

ثانياً- العلة من التجريم: تتمثل العلة من التجريم فيمايلي:-

أ-حرص المشرع الجنائي على حماية الشبكة المعلوماتية ضد محاولات العبث بها.

ب- ضمان أن تؤدي وظيفتها على أفضل وجه ممكن في ضوء ما تحمله من بيانات ومعلومات يمكن أن تفيد المجتمع وأعضاءه.

ج- المحافظة على الأجهزة والبرامج والبيانات والمعلومات المدونة فيها من أعمال التخريب والإتلاف وما يكون من شأنه إيقافها عن العمل أو تعطيلها أو تدميرها، في ضوء ما يمثله الاعتداء عليها من مخاطر كثيرة لمستخدميها.

د- إضفاء الحماية للشبكة المعلوماتية التي تخص الدولة أو أحد الأشخاص الاعتبارية العامة أو كانت تخدم مرفق عامة أو تقدم خدمة عامة للمواطنين.

ثالثاً- الصور الأولى- الإيقاف العمدي للشبكة المعلوماتية: ونتناول فيمايلي

---

[1] تضمنت المادة (٧٥) من قانون الأحوال المدنية رقم (١٤٣) لسنة ١٩٩٤ تجريم أفعال التعطيل والإتلاف الواقعة على شبكة معلومات الأحوال المدنية سواء أكان هذا التعطيل عمدياً أو على سبيل الخطأ غير العمدي، كما جرمت المادة (٧١) من قانون الاتصالات رقم (١٠) لسنة ٢٠٠٣ سلوك كل من تسبب في قطع الاتصالات سواء أكان هذا القطع بشكل عمدي أو غير عمدي، وكل من هدم أو تلف عمداً شيئاً من المباني أو المنشآت المخصصة لشبكات الاتصالات أو لبنيتها الأساسية أو لخط من خطوط الاتصالات أو جعلها كلها أو بعضها غير صالحة للاستعمال بأية كيفية بحيث ترتب على ذلك انقطاع الاتصالات ولو مؤقتاً، مع إلزام من قام بالفعل بأداء قيمة الأشياء التى هدمت أو أتلفت أو بنفقات إعادة الشيء إلى أصله، وكذا النص على الحق فى التعويض المناسب، ومن بين التشريعات التي عرفت تجريم إيقاف الشبكة المعلوماتية التشريع الإماراتي(م١٠).

جريمة الإيقاف العمدي للشبكة المعلوماتية، من خلال التطرق لمحل الجريمة وركنيها المادي والمعنوي، وذلك على النحو التالي:-

محل الجريمة: وهو الشبكة المعلوماتية، وقد عرفها القانون المصري بأنها: "*مجموعة من الأجهزة أو نظم المعلومات تكون مرتبطة معاً، ويمكنها تبادل المعلومات والاتصالات فيما بينها، ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية، والتطبيقات المستخدمة عليها*"[١]، ويتضح من التعريف السابق أن الشبكة المعلوماتية تشتمل على مكونين: (الأول) مادي، ويضم أجهزة الحاسب الآلي والأجهزة المادية والمعدات وخطوط الربط التي تتكون منها الشبكات، و(الثاني) البرامج والبيانات والمعلومات ونظم تشغيل الشبكات التي تشكل المكون المعنوي أو المنطقي للشبكة[٢]، ومن أبرز الشبكات المعلوماتية شبكة المعلومات الدولية "الإنترنت"[٣]، والتي تسمى بشبكة الشبكات، وهي شبكة حواسيب ضخمة متصلة مع بعضها البعض، وتخدم شبكة الإنترنت ما يقرب من ثلاثة ونصف مليار مستخدم، وتنمو بشكل سريع للغاية بنسبة تصل إلى ١٠٠% سنوياً، ومن أبرز استخدامات شبكة الإنترنت المتعددة، من أبرزها

---

(١) ومن التشريعات المقارنة التي تضمنت تعريف للشبكة المعلوماتية التشريع الإماراتي والكويتي والسوداني والنظام السعودي.

(٢) د. حسنى الجندي: المرجع السابق، ص١١٧؛ د. نائلة عادل محمد فريد قورة: جرائم الحاسب الاقتصادية، مرجع سابق، ص١٩١؛ د. حسين الغافري ومحمد الألفي: جرائم الإنترنت بين الشريعة والقانون، مرجع سابق، ص١٧٦.

(٣) يرجع ظهور الإنترنت إلى عام ١٩٦٩، حيث تبنت وزارة الدفاع الأمريكية مشروع إنشاء شبكة معلومات لأغراض عسكرية أبان الحرب الباردة عرف بـ (أربانت) عن طريق ربط الجامعات ومؤسسات الأبحاث لاستغلال أمثل للقدرات الحسابية للحواسب المتوفرة، وقد تخلت الحكومة الأمريكية عن الشبكة لصالح الشركات التجارية، ليبدأ عصر الإنترنت.

خدمات البريد الإلكتروني، ومحركات البحث[١]، ومواقع الويب، وعقد الاجتماعات والمؤتمرات[٢]، ومواقع أو شبكات التواصل الاجتماعي[٣].

الركن المادي: يتمثل الركن المادي في الجريمة من ثلاثة عناصر هي: السلوك الإجرامي والنتيجة الإجرامية وعلاقة السببية بين السلوك والنتيجة، وهو ما سوف نتناوله على النحو التالي:-

أ) السلوك الإجرامي: يتمثل السلوك الإجرامي في كل فعل إيجابي من شأنه الاعتداء على سلامة الشبكة المعلوماتية وينتج عنه إيقافها عن العمل أو تعطيلها، أو التشويش عليها أو إعاقتها أو اعتراض عملها، وهو ما أشار إليه المشرع صراحة بقوله:" كل من تسبب متعمداً في إيقاف شبكة معلوماتية عن العمل..."، ومن ثم فالسلوك الإجرامي قد يتخذ صورة فعل إدخال برنامج ضار، أو إجراء معالجة إلكترونية للبيانات الخاصة بها بدون وجه حق، وهو ما سوف نتناوله على النحو التالي:-

١) فعل إدخال برنامج ضار: يقصد بفعل الإدخال الولوج إلى الشبكة المعلوماتية للتعامل على ما هو موجود عليها للتعامل معها، أو إدراج المعلومات،

---

(١) محركات البحث هي برامج تفيد المستخدم في الوصول للمعلومات المتوفرة على شبكة الإنترنت بسرعة وسهولة، حيث يقوم المستخدم بوضع كلمات البحث لكي يتم البحث عنها.

(٢) يمكن استخدام الإنترنت في عقد الاجتماعات والمؤتمرات من خلال برامج نقل الصورة والصوت عبر الشبكة بكل سهولةVideo Conference، والدردشة عبر الإنترنت سواء كان في شكلIRC أو القنوات، أو عن طريق المراسلة الفورية يسمح للزملاء البقاء على اتصال دائم عن طريق وسيلة مريحة للغاية تعمل في حواسيبهم طول الوقت، ومن أبرز هذه البرامج سكايب. هذا بالإضافة لخدمات التسوق عبر الإنترنت.

(٣) ومن أشهر مواقع التواصل الاجتماعي فيسبوك الذي تأسس في عام ٢٠٠٤ ويضم في الوقت الحالي أكثر من مليار مستخدم على مستوى العالم، وهذا البرنامج يمكن مستخدميه من التواصل الاجتماعي عن طريق نشر الأخبار وتبادل الصور ومقاطع الفيديو إلى غير ذلك من سبل التواصل الاجتماعي.

ويستخدم فيه الصوت أو الصورة أو الأصابع أو الماسح، ويكون الإدخال أيضاً بالاختراق من خلال تحميل الجهاز ببعض البرامج التي يكون لها أثر ضار على الجهاز أو ما يحتوى عليه، وأكثر ما يحدث فعل الإدخال للشبكة عن طريق الاختراق وبث أو زرع أو نشر الفيروسات أو البرمجيات الخبيثة كالبوتنت على الشبكة المعلوماتية، ويستوي لدى القانون أن يكون الإدخال قد تم بشكل مشروع، بأن كان الجاني من المخول له بالدخول إلى الشبكة، أو بدون وجه حق، وتعد الفيروسات أو البرامج الضارة من أبرز الوسائل المستخدمة في تعطيل أو إيقاف الشبكة المعلوماتية، وتتنوع ما بين عدة أنواع وأشكال من بينها البوتنت أو شبكات الروبوت ودودة الإنترنت والقنابل المنطقية والفيروسات الاستعراضية[1].

---

[1] يقسم الباحثون الفيروسات من حيث تكوينها وأهدافها إلى فيروس عام العدوى، وفيروس محدد العدوى، بينما تقسم الفيروسات من حيث الأضرار التي تحدثها بأجهزة الحاسب الآلي إلى: فيروسات قطاع التشغيل، وفيروسات الملفات، وتنقسم إلى نوعين: الأول يصيب الملفات التنفيذية والثاني ينسخ نفسه داخل ملف خفي على إحدى وحدات التخزين، أو ينسخ نفسه على الأسطوانة دون حاجة إلى ملف، وهناك الفيروسات المقيمة والتي تتخذ من الذاكرة المؤقتة مكاناً دائماً لها، وتعمل على كتابة بيانات وهمية داخل الذاكرة المؤقتة، مما يؤدي إلى عدم وجود مساحة كافية لتشغيل التطبيقات الأخرى على الحاسب، وهناك الفيروسات النائمة التي تصيب الحاسب ثم تنتظر لحين تحقق شرط معين أو واقعة معينة دون أن تظهر أثاراً تخريبية، لتقوم بذلك بعد تحققه، وهناك كذلك الفيروسات الاستعراضية التي يزرعها مصمموها دون رغبة إحداث ضرر يترتب عليها، وإنما يهدفون إلى إبراز قدراتهم في التصميم، وهناك فيروسات الثغرات التي تعتمد على الثغرات الموجودة داخل نظم التشغيل كنظام الويندوز، وتحتاج إلى قدرة عالية من المبرمج على تحليل نظام التشغيل واكتشاف الأخطاء الموجودة به ثم استغلالها، وهناك فيروسات الماكرو والتي تصيب بشكل أساسي الملفات التي تعمل على مجموعة برامج الأوفيس والملفات الخاصة ببرنامج الوورد، فتجعل التعامل معها غير متاح، ويسفر دائما عن ظهور رسائل الخطأ، وهناك دودة الإنترنت، وهي فيروس ينتقل عبر شبكة الإنترنت، ويعتمد على استخدام برنامج أوتلوك إكسبريس بشكل أساسي للقيام بعملية الانتشار، وإصابة أكبر عدد ممكن من الأجهزة، ويقوم مصممه بزرعه داخل رسالة بريد إلكتروني، ويرسلها لعدد كبير من مستخدمي الشبكة، وبمجرد قيامهم بفتحها يبدأ الفيروس في الحصول على دفتر العناوين الخاص بكل واحد منهم، ثم إرسال هذه الرسالة للعديد من أصدقائهم، فيفتحونها دون أدنى شك لمعرفتهم للمرسل، فيقعوا ضحية لهذا الفيروس، وهناك فيروس القنابل =

٢) إجـراء معالجـة إلكترونيـة للبيانـات الخاصـة بالـشبكة: عـرف المـشرع المصري المعالجة الإلكترونية بأنها:" أي عملية إلكترونية أو تقنية تتم كلياً أو جزئياً لكتابة أو تجميع أو تسجيل أو حفظ أو تخزين أو دمج أو عرض أو إرسال أو استقبال أو تداول أو نشر أو محو أو تغيير أو تعديل أو استرجاع أو استنباط البيانات والمعلومات الإلكترونية، وذلك باستخدام أي وسيط من الوسائط أو الحاسبات أو الأجهزة الأخرى الإلكترونيـة أو المغناطيـسية أو الـضوئية أو مـا يُـستحدث مـن تقنيـات أو وسـائط أخرى"[1].

ومن ثم تتحقق هذه الصورة بقيام الجاني بإجراء تعديل على البيانات الخاصة بالشبكة، ومن ثم تغيير النظام المعلوماتي أو البرامج التي تنظم عمل هذه الشبكة، بالشكل الذي يؤدي إلى تعطيها أو إيقاف العمل بها، وقد تطلب القانون في هذه الحالة أن تكون هذه المعالجة الإلكترونية للبيانات الخاصة بالشبكة قد تمت بدون وجه حق، ويتحقق ذلك إذا كان الدخول للشبكة قد تم من شخص غير مصرح له بالدخول أو البقاء داخل الشبكة أو النظام المعلوماتي أو كان الدخول من شخص مخول له ذلك ولكنه تجاوز حدود الدخول أو البقاء على الشبكة.

ب) النتيجـة الإجراميـة: تتمثـل النتيجـة الإجراميـة فـي أن يـؤدي الإدخـال أو المعالجة الإلكترونية للبيانات إلى اضطراب عمل الشبكة أو تعطيلها أو إيقافها، وتلعب

= المنطقية، ويعمل هذا الفيروس كالقنبلة؛ إذ يظل في حالة سكون حتى يتم تفجيره في الوقت المناسب؛ إذ يظل البرنامج موجوداً ولا تأثير له حتى يجد بيانات مخزنة في مكان محدد لها قيمة معينة، أو بعد تشغيل البرنامج لعدة مرات معينة، وفي المرة التالية يبدأ الفيروس في العمل، وهذا الفيروس يصمم لإصابة برامج محددة وتطبيقات معينة يوجه إليها. انظر: د. حسنى الجندي: التشريعات الجنائية الخاصة، مرجع سابق، ص١١٩، هامش رقم ١.

[1] ومن التشريعات التي تضمنت تعريف للمعالجة الإلكترونية التشريعين الكويتي والقطري.

الفيروسات المعلوماتية -كما سبق أن أشرنا- دوراً في تحقيق ذلك لما لها من قدرة على الاختراق والاختفاء والانتشار والتدمير المعلوماتي، حيث يتمكن من الدخول إلى النظام المعلوماتي، مما يؤدي إلى إيقاف البرامج أو البيانات أو المعلومات عن العمل، أو تعطيلها، أو تدميرها أو مسحها، أو حذفها، أو إتلافها أو تعديلها، وفيما يلي نتناول صور الآثار المترتبة على الشبكة المعلوماتية من جراء سلوك الجاني، وذلك على النحو التالي:-

١) إيقاف شبكة معلوماتية عن العمل: يقصد به توقف برامج أو أجهزة تشغيل الشبكة عن العمل، وإن كان ذلك يتم عن طريق أجهزة الشبكة نفسها، وهذا التوقف قد يكون بشكل دائم أو بصورة مؤقتة.

٢) تعطيل الشبكة المعلوماتية: هذا التعطيل قد يكون بإعاقة سير عمل الشبكة المعلوماتية أو النظام المعلوماتي المشغل لها، بفعل يتسبب في تباطؤ أو ارتباك نظام عملها، أو يترتب عليه تغيير فيه، وقد يتحقق ذلك بتضخيم البريد الإلكتروني، بإرسال نسخ مكررة بعدد كبير من الرسالة ذاتها لنظام البريد الإلكتروني الخاص بالغير بما يترتب عليه تعطيل أو إعاقة سير النظام التقني بشكل منضبط، أو نقل المعلومات بواسطة برامج الاتصال، الأمر الذي يؤدي إلى تعطيل أو إيقاف النظام المعلوماتي عن العمل.

٣) الحد من كفاءة عمل الشبكة المعلوماتية: يتمثل في التقليل من كفاءة عمل الشبكة أو تشغيلها، كاستخدام برامج ضارة لإبطاء عمل الشبكة.

٤) التشويش على الشبكة المعلوماتية أو إعاقتها، أو اعتراض عملها: يتمثل ذلك في استخدام برامج للتشويش أو اعتراض للبيانات والمعلومات التي يتم تداولها من خلال الشبكة المعلوماتية.

ج) رابطة السببية: ينبغي أن تتوافر رابطة السببية بين فعل الجاني وما ترتب على ذلك من إيقاف عمل الشبكة المعلوماتية أو تعطيلها، وعلاقة السببية المتطلبة هي علاقة مادية تبدأ بالعمل الذي اقترفه الجاني، وترتبط من الناحية المعنوية بما يجب عليه أن يتوقعه من النتائج المألوفة لفعله إذا أتاه عمداً، ورابطة السببية هي مسألة موضوعية تفصل فيها محكمة الموضوع بتقديرها، مادام تقديره سائغاً مستنداً إلى أدلة مقبولة في العقل والمنطق ولها أصل في الأوراق[1].

الركن المعنوي: هذه الجريمة من الجرائم العمدية التي يتحقق فيها الركن المعنوي بتوافر القصد الجنائي العام بعنصريه العلم والإرادة، وذلك على النحو التالي:-

أ) العلم: بأن يعلم الجاني بأن ما يقوم به ينصب على شبكة معلوماتية، وأن هذا الفعل من شأنه التسبب في إيقاف عملها أو تعطيلها أو التشويش عليها، سواء أكانت الشبكة المعلوماتية الدولية أو شبكة معلوماتية تخص الغير أو الدولة أو أحد الأشخاص الاعتبارية العامة، وينتفي هذا العلم إذا كان الجاني قد استعمل اسطوانة مملوكة له- وقت القيام بالسلوك- دون علم بإصابتها بفيروس من الفيروسات الضارة بالحاسب، أو بأحد برامجه أو بياناته أو معلوماته، فيؤدي ذلك إلى انتقال الفيروس إليه، أو أن يعتقد ملكيته للشبكة المعلوماتية.

ب) الإرادة: يجب أن تتجه إرادة الجاني إلى ارتكاب الفعل وإحداث النتيجة الإجرامية المتمثلة في إيقاف الشبكة المعلوماتية أو تعطيلها عن العمل، فإذا انتفت هذه الإرادة، فإن ذلك يترتب عليه انتفاء القصد الجنائي، كما لو حدث فعل إدخال البرنامج

---

[1] انظر: الطعن رقم ٣٥٦١ لسنة ٨٢ق جلسة ٢٠١٢/١٢/٢٧، المستحدث من المبادئ الصادرة عن الدوائر الجنائية من أول أكتوبر ٢٠١٢ لغاية آخر سبتمبر ٢٠١٣، الصادرة عن المكتب الفني لمحكمة النقض، المجموعة الجنائية، ص ص ٩٢، ٩٣.

الضار دون أن يكون للجاني شأن في ذلك، وينتفي القصد أيضاً إذا لم تكن إرادة الجاني قد اتجهت إلى إحداث الضرر المتمثل في إيقاف او تعطيل الشبكة المعلوماتية.

رابعاً- الصور الثانية- الإيقاف غير العمدي للشبكة المعلوماتية: وتتحقق جريمة الإيقاف غير العمدي للشبكة المعلوماتية، من خلال تسبب الجاني خطأ بإيقاف الشبكة المعلوماتية، ويتحقق ذلك على النحو التالي:-

الركن المادي- الخطأ غير العمدي: يتحقق الركن المادي بفعل الجاني غير العمدي الذي يتسبب في إيقاف عمل الشبكة المعلوماتية أو تعطيلها، والذي قد يتخذ صورة الإهمال أو التقصير أو الإخلال بالواجبات، والذي يسفر عن نتيجة تتمثل في إيقاف عمل الشبكة المعلوماتية أو تعطيلها ورابطة سببية تربط بين الفعل والنتيجة[١].

١) الخطأ: يعرف الخطأ في الجرائم غير العمدية عموماً بأنه: "تصرف إرادي يؤدى إلى نتيجة ضارة توقعها الفاعل أو كان عليه أن يتوقعها ولكنه لم يقصد إحداثها ولم يقبل وقوعها"[٢]، ويقوم الخطأ على الإخلال بواجبات الحيطة التي تقضى بها ظروف الحياة العادية إخلالاً يتضح منه انحراف مسلك الجاني عن مسلك الرجل العادي متى وجد فى ظروف مماثلة للظروف التى أحاطت بالجاني[٣].

صور الخطأ غير العمدي: تتحدد صور الخطأ غير العمدي في ثلاث صور، هي: الاهمال، وعدم التحرز والاحتياط، والإخلال بواجبات الوظيفة.

أ) الإهمال: يقصد به عدم الحيطة في أداء عمل ما على نحو صحيح، وقد يكون

---

[١] نقض ١٩٩٢/١١/١٩، طعن رقم ٥٣٢٢، ص٥٩.

[٢] نقض ١٩٦٩/١٠/٢٧، سابق الإشارة إليه.

[٣] د.عمر السعيد رمضان: شرح قانون العقوبات، القسم العام، دار النهضة العربية، ١٩٨٦، ص ٩٠.

الإهمال بالامتناع التام عن أداء العمل المطلوب، وقد يكون الامتناع عن أداء بعض الواجبات، ويستوي لدى القانون كون الامتناع صريحاً أم ضمنياً.

ب) عدم التحرز والاحتياط: ويقصد به عدم التبصر بالعواقب التي يجب توافرها لدى الشخص العادي.

ج) الإخلال بالواجبات التي يفرضها القانون: يقصد بها كل تقصير يقع من الجاني أو خروج عن إحدى الواجبات التى يفرضها عليه القانون، سواء تعلقت تلك الواجبات بكيفية أداء العمل أم بغير ذلك[١].

٢) تحقق الضرر والمتمثل في إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها.

٣) توافر رابطة السببية بين الفعل والنتيجة، ومناط توافر علاقة السببية بين السلوك والنتيجة هنا أن يكون السلوك الخاطئ للجاني فى ذاته وفى الظروف التى بوشر فيها من شأنه أن يؤدى إلى النتيجة التى حدثت وفقاً للمجرى العادى للأمور[٢].

ج) الركن المعنوي: يقوم الركن المعنوي فى جريمة الإيقاف غير العمدى للشبكة المعلوماتية على الخطأ غير العمدى من قبل الجانى، والذى يتسبب عنه ضرر يصيب الشبكة المعلوماتية.

خامساً- العقوبة: ميز القانون في العقوبة بين حالتين-كما سبق أن أشرنا-، حالة الإيقاف العمدي للشبكة المعلوماتية، وحالة الإيقاف غير العمدي، وذلك على النحو التالي:-

---

[١] الموضع السابق.

[٢] د.السيد عتيق: القسم الخاص، مرجع سابق، ص ٢٩٧؛ د.حامد راشد: القسم الخاص، مرجع سابق، ص ١٥٦.

١) العقوبة المقررة في جريمة الإيقاف العمدي للشبكة المعلوماتية: وقد ميز القانون في العقوبة بين حالتين، بحسب محل الجريمة، وذلك على النحو التالي:-

(الحالة الأولى) كون محل الجريمة الشبكة المعلوماتية الدولية "الإنترنت": عاقب القانون على هذه الجريمة بعقوبة بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه أو إحداهما، ومن ثم يجوز للقاضي وفقاً لسلطته التقديرية في ضوء ظروف وملابسات القضية أن يقضي بأي من عقوبة الحبس أو عقوبة الغرامة، أو بالعقوبتين معاً، كما يجوز له أن يأمر بوقف تنفيذ العقوبة وفقاً للمادة (٥٥) عقوبات.

(الحالة الثانية) كون محل الجريمة شبكة معلوماتية تخص الدولة أو أحد الأشخاص الاعتبارية العامة: عاقب القانون على هذه الجريمة بعقوبة السجن المشدد والغرامة التي لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه، وعقوبة السجن المشدد تتراوح ما بين (٣-١٥) سنة، دون تحديد حد أدني للعقوبة، ومن ثم يقدر القاضي العقوبة المناسبة للمحكوم عليه في ضوء ظروف وملابسات الجريمة، والحكم في هذه الحالة بالسجن المشدد والغرامة وجوبياً، ويجوز للقاضي النزول بعقوبة السجن المشدد وفقاً للسلطة التقديرية المخولة له بالمادة (١٧) عقوبات. ويتضح لنا أن المشرع اعتبر كون الشبكة المعلوماتية الواقع عليها الاعتداء مملوكة للدولة ظرفاً مشدداً مغيراً لوصف الجريمة؛ إذ يترتب على توافر هذه الصفة تحول الجريمة من وصف الجنحة لوصف الجناية.

(٢) العقوبة المقررة في جريمة الإيقاف غير العمدي للشبكة المعلوماتية:عاقب المشرع المصري على جريمة التسبب خطأ في إيقاف الشبكة المعلوماتية بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه أو بإحدى هاتين العقوبتين، ويجوز للقاضي أن يحكم بوقف

التنفيذ، إعمالاً لحكم المادة ٥٥ عقوبات، فإذا كانت الشبكة المعلوماتية مملوكة للدولة أو أحد الأشخاص المعنوية العامة، عوقب الجاني بالعقوبة المقررة بعاليه، وهي السجن المشدد والغرامة التي لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه، ويجوز للقاضي النزول بالعقوبة للسجن أو الحبس الذي لا يقل عن ثلاثة أشهر إعمالاً لنص المادة ١٧ عقوبات.

المطلب العاشر

جريمة حيازة الأجهزة والمعدات المستخدمة

في ارتكاب جرائم تقنية المعلومات والاتجار فيها

نص التجريم: تنص المادة (٢٢) المعنونة بـ"البرامج والأجهزة والمعدات المستخدمة في ارتكاب جرائم تقنية المعلومات" على أنه:" ***يُعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من حاز أو أحرز أو جلب أو باع أو أتاح أو صنع أو أنتج أو استورد أو صدَّر أو تداول بأي صورة من صور التداول، أي أجهزة أو معدات أو أدوات أو برامج مصممة أو مطورة أو محورة أو أكواد مرور أو شفرات أو رموز أو أي بيانات مماثلة، بدون تصريح من الجهاز أو مسوغ من الواقع أو القانون، وثبت أن ذلك السلوك كان بغرض استخدام أي منها في ارتكاب أو تسهيل ارتكاب أي جريمة من جرائم المنصوص عليها في هذا القانون، أو إخفاء آثارها أو أدلتها أو ثبت ذلك الاستخدام أو التسهيل أو الإخفاء***"[1].

---

[1] تتناول غالبية الصكوك الدولية متعددة الأطراف المعنية بمكافحة جرائم تقنية المعلومات تجريم إساءة استعمال أدوات الحاسب من أجهزة وبرامج ورموز في ارتكاب جرائم تقنية المعلومات، إلا أن بعض هذه الصكوك يقتصر هذا التجريم على جرائم بعينها كقرار دول الإتحاد الأوروبي بشأن =

العلة من التجريم: تتبلور علة التجريم فيمايلي:-

١-العمل على تجريم الأعمال التحضيرية لارتكاب الجرائم المعلوماتية، من خلال تجريم حيازة وإحراز أدوات إساءة استعمال الحاسب من الأجهزة والمعدات التي تستخدم في ارتكاب أو تسهيل الجرائم المعلوماتية، كأحد صور النهج التشريعي المشدد للتعامل مع الجرائم المعلوماتية في ضوء ما يمثله هذا الفعل من خطورة إجرامية، ومعاونة حقيقية للجناة على ارتكاب أنشطتهم غير المشروعة.

٢- مواجهة عمليات استعمال البرمجيات والأدوات الأخرى لاختراق كلمات المرور والكلمات السرية للدخول الخاصة بالأفراد، والتي أصبحت بمثابة مادة غير مشروعة يتم تداولها من خلال القراصنة المعلوماتيون بالأسواق السرية لجرائم تقنية المعلومات في إطار جماعات الجريمة المنظمة عبر شبكة الإنترنت[١].

=

الاحتيال وتزوير وسائط الدفع غير النقدية الذي يجرم استعمال الأجهزة والأدوات وبرامج الحاسب وأي وسائل أخرى تستخدم في ارتكاب جرائم تزوير وتزييف وسائط الدفع لاستعمالها بشكل احتيالي. انظر: دراسة مكتب الأمم المتحدة، مرجع سابق، ص١٣٣.

ومن التشريعات المقارنة التي جرمت التعامل في الأجهزة والمعدات المستخدمة في ارتكاب الجرائم المعلوماتية التشريع الفرنسي، حيث تقضي المادة (٣٢٣-٣-١) عقوبات فرنسي بأنه: "يعاقب على الأفعال التي ترتكب – بدون وجه حق- الاستيراد أو الحيازة أو العرض أو البيع أو توفير أي معدات أو أدوات أو برامج معلوماتية أو أي بيانات مصممة أو مخصصة لارتكاب واحدة أو أكثر من الجرائم المنصوص عليها في المواد ٣٢٣-١ إلى ٣٢٣-٣ بالعقوبات المقررة للجريمة نفسها أو للجريمة الأشد في عقوبتها".

[١] انظر: تقرير منظمة الشرطة الأوروبية اليورو بول بشأن تقييم خطر الجريمة المنظمة عبر الإنترنت

Europol, 2011. Threat assessment (abridged). Internet facilitated organised crime. iOCTA. File No.: 2530–264. The Hague. 7 January. Available at: https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf ;

=

محل الجريمة: يتمثل محل الجريمة في البرمجيات والأجهزة وكلمات المرور، وهو ما اشار إليه النص بـ"*أي أجهزة أو معدات أو أدوات أو برامج مصممة أو مطورة أو محورة أو أكواد مرور أو شفرات أو رموز أو أي بيانات مماثلة*" تستخدم في ارتكاب أو تسهيل ارتكاب جرائم تقنية المعلومات[١]، ويعد من قبيل ذلك البرمجيات الخبيثة كبرمجيات الروبوت أو البوتنت[٢]، والفيروسات، وأجهزة التشفير وتمرير الاتصالات وبرامج كسر كلمات السر والمرور إلى غير ذلك من الأدوات والبرمجيات والأجهزة.

الركن المادي: تبرز الإشارة قبل التطرق لشرح هذه الجريمة إلى أن المشرع قد اعتبرها من جرائم الخطر التي لا يشترط فيها المشرع وقوع الضرر، وإنما تتحقق الجريمة بمجرد ارتكاب الجاني للسلوك المجرم، بالنظر إلى ما يمثله هذه السلوك من خطورة إجرامية ومساس بالأمن المعلوماتي كأحد المصالح الاجتماعية الجديرة بالحماية الجنائية، ويتكون الركن المادي للجريمة من عدة صور للسلوك الإجرامي، من أبرزها:-

---

=

Fallmann, H., Wondracek, G. and Platzer, C., 2010. Covertly probing underground economy marketplaces. Vienna University of Technology.

وكذلك انظر المذكرة التفسيرية المرافقة لاتفاقية مجلس أوروبا بشأن الجريمة الإلكترونية والتي تشير إلى أن الأساس المنطقي لتجريم أدوات إساءة استعمال الحاسب يتمثل في استهداف الأفعال السابقة للجريمة مثل القرصنة، بالإضافة على منع إنشاء أسواق سوداء لهذه المواد. انظر: دراسة مكتب الأمم المتحدة، مرجع سابق، ص١٣٢.

[١] عادة ما تتضمن الصكوك الدولية متعددة الأطراف المعنية بمكافحة جرائم تقنية المعلومات تجريم كل من الأجهزة والبرمجيات والرموز كأدوات لإساءة استعمال الحاسب. انظر: دراسة مكتب الأمم المتحدة، مرجع سابق، ص١٣٢.

[2] NATO Cooperative Cyber Defence Centre of Excellence and ENISA, 2012. : Legal Implications of Countering Botnets.

الحيازة والإحراز: يقصد بالحيازة السيطرة الفعلية لشخص على شيء يجوز التعامل فيه[١]، وهي الأدوات والآلات التي تستخدم في ارتكاب الجرائم المعلوماتية، وللحيازة عنصرين: عنصر مادي يتمثل في مجموعة الأفعال التي تكون الحيازة، وعنصر معنوي يقصد به إرادة الظهور على الشيء بمظهر المالك والتصرف فيه لحسابه الخاص، وقد استقر الفقه والقضاء المصري على أنه يكفي لتحقق الحيازة أن يكون سلطان المتهم مبسوطاً على الشيء ولو أحرزه مادياً شخص غيره[٢]. أما الإحراز فيقصد به مجرد الاستيلاء على الشيء استيلاء مادياً بغض النظر عن الباعث عن الإحراز[٣].

الجلب: يقصد بالجلب إدخال الشخص للأدوات أو الأجهزة أو المعدات داخل إقليم الدولة بأي وسيلة، وتقع الجريمة بمجرد إدخال الشخص هذه الأدوات والأجهزة إلى أرض الدولة أو مياهها الإقليمية أو في إقليمها الجوي، ويرجع في تحديد إقليم الدولة بعناصره الثلاثة الأرضي والمائي والجوي إلى قواعد القانون الدولي العام[٤]، وجلب الأجهزة والمعدات هو فعل مادي يتضمن إدخال هذه الأجهزة والمعدات في أراضي الجهورية المصرية بأية كيفية كانت، فتقديره خاضع لسلطة قاضي الموضوع[٥].

---

(١) قارن: د. فوزية عبد الستار: شرح قانون مكافحة المخدرات، القاهرة، دار النهضة العربية، ١٩٩٠، ص٣٣.

(٢) قارن: د. فوزية عبد الستار، المرجع السابق، ص٣٥.

(٣) قارن: نقض ١٩٥٥/٤/١١، مجموعة أحكام محكمة النقض، س٦، رقم ٢٥١، ص٨١٤، مشار إليه د. فوزية عبد الستار، مرجع سابق، ص٣٨.

(٤) المرجع السابق، ص٣٣.

(٥) قارن: نقض ١٩٢٨/١١/٢٩، مجموعة القواعد القانونية، ج١، رقم ٢٧، ص٥٥، مشار إليه د. فوزية عبد الستار، الموضع السابق.

البيع: يقصد بالبيع تقديم الشخص للأدوات أو ألأجهزة المستخدمة في ارتكاب الجرائم المعلوماتية في مقابل الحصول على مبلغ مالي أو منفعة مادية أو معنوية، كأن يكون المقابل في صورة أداء خدمة لصالح البائع، فالبيع عقد يلتزم بمقتضاه البائع أن ينقل للمشتري ملكية شيء أو حقاً مالياً آخر في مقابل ثمن نقدي، ويتم البيع بجرد انعقاد العقد، ولا يشترط لاكتمال العقد الذي تتم به الجريمة أن يتم تسليم الشيء أو ان يتم دفع الثمن، ولذلك تقع الجريمة سواء تم تسليم الشيء أو لم يتم، وسواء كان التسليم -إذا تم- فعلياً أو رمزياً[١].

الإتاحة: يقصد بالإتاحة السماح للغير باستخدام الأجهزة أو المعدات، سواء أكان ذلك بمقابل أو بدون مقابل، وهذه الإتاحة يفترض قيام الجاني بتسهيل استخدام هذه الأجهزة أو المعدات لارتكاب الجريمة المعلوماتية، وتتحقق عندما يسمح الجاني لشخص ما استخدام حاسبه الآلي أو هاتفه المحمول المتصل بشبكة الانترنت لارتكاب أحد الجرائم المنصوص عليها في هذا القانون.

التصنيع والإنتاج: يقصد بالتصنيع والإنتاج إيجاد مادة لم تكن موجودة من قبل؛ أي إيجاد أو بناء أو تكوين الأجهزة أو المعدات المستخدمة في ارتكاب الجرائم المعلوماتية، ويستوي لدى القانون الوسيلة التي بها تصنيع أو إنتاج الأجهزة أو المعدات، سواء أكان ذلك بطريق يدوية أو آلية[٢].

الاستيراد أو التصدير: يقصد بالاستيراد طلب إدخال الأدوات أو الأجهزة من الخارج، سواء تحقق إدخال هذه الأجهزة أم لا، وتبرز الإشارة إلى أن مصطلح الجلب يرادف مصطلح الاستيراد، إلا أنه يمكن التمييز بين المصطلحين بأن الجلب يكون إدخال

(١) قارن: د. فوزية عبد الستار، مرجع سابق، ص ص٤٥، ٤٦.
(٢) قارن: المرجع السابق، ص ص٢٩، ٣٠.

الأجهزة بصحبة الجاني، بينما في الاستيراد لا يكون إدخال الأجهزة والمعدات بصحبة الجاني، بينما يقصد بالتصدير إرسال الأدوات والأجهزة المشار إليها إلى الخارج، فالتصدير يقصد به إخراج الأجهزة أو المعدات من إقليم الدولة، فتقع الجريمة تامة بمجرد تجاوز هذه الأدوات أو الأجهزة حدود الدولة إلى الخارج، ويستوي لدى القانون أن يكون الجاني وقت الاستيراد أو التصدير خارج الدولة أو داخلها[١]، وترجع علة تجريم الاستيراد والتصدير إلى رغبة المشرع في أن يبسط رقابته على عمليات التجارة الدولية[٢]، والحد من التعامل في هذه الأجهزة.

أن يكون التعامل في هذه الأدوات أو الأجهزة بطريق غير مشروع: تطلب القانون أن التعامل في هذه الأجهزة أو الأدوات أو البرامج بالحيازة أو الإحراز أو الاتجار بطريق غير مشروع، وهو ما يتحقق حينما يكون التعامل في هذه الأجهزة أو الأدوات بغير تصريح من الجهاز القومي لتنظيم الاتصالات أو مسوغ من الواقع أو القانون، كأن يثبت المتهم أن استعماله لهذه الأدوات والأجهزة ليس بسبب إساءة استعمال الحاسب أو ارتكاب أو تسهيل ارتكاب أي من جرائم تقنية المعلومات الواردة بالقانون.

الركن المعنوي: هذه الجريمة من الجرائم العمدية التي يتحقق فيها الركن المعنوي بتوافر القصد الجنائي الخاص وهو نية استخدامها في ارتكاب جرائم تقنية المعلومات أو تسهيل ارتكابها، ومن ثم يتطلب الركن المعنوي تحقق القصد الجنائي بعنصريه العلم والإرادة، بأن يعلم الجاني بأنه يحرز أو يحوز أو يتعامل في أجهزة أو

---

(١) قارن: المرجع السابق، ص٢٤.

(٢) قارن: نقض ١٩٧٠/٤/٦، مجموعة أحكام محكمة النقض، س٢١، رقم ١٣٠، ص٥٤٧، مشار إليه د. فوزية عبد الستار، الموضع السابق.

معدات تستخدم في ارتكاب أو تسهيل ارتكاب الجرائم المعلوماتية، وأن تتجه إرادته إلى تحقيق ذلك، فضلاً على انصراف نية الجاني إلى استخدام أي من هذه الأدوات أو الأجهزة في ارتكاب أو تسهيل ارتكاب أي من جريمة تقنية المعلومات الواردة في هذا القانون، أو إخفاء آثارها أو أدلتها[1].

العقوبة: عاقب القانون على هذه الجريمة بعقوبة الحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه أو إحداهما، ومن ثم يجوز للقاضي -كما سبق أن أشرنا- وفقاً لسلطته التقديرية في ضوء ظروف وملابسات القضية أن يقضي بأي من عقوبة الحبس أو عقوبة الغرامة، أو بالعقوبتين معاً، فضلاً عن الحكم بالمصادرة للأدوات والأجهزة المضبوطة.

[1] عادة ما تتطلب الصكوك الدولية متعددة الأطراف المعنية بمكافحة جرائم تقنية المعلومات توافر نية خاصة لاستخدام هذه الأدوات لأغراض جنائية. انظر: دراسة مكتب الأمم المتحدة، مرجع سابق، ص١٣٢.

المبحث الثاني

الجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات

تقسيم: تضمن الفصل الثاني من القانون الجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات، وتشمل جرائم الاحتيال والاعتداء على البطاقة الائتمانية وأدوات الدفع الإلكتروني والجرائم المتعلقة باصطناع المواقع والحسابات الخاصة والبريد الإلكتروني، وذلك في مطلبين على النحو التالي:-

المطلب الأول

جرائم الاحتيال والاعتداء على البطاقة الائتمانية وأدوات الدفع الإلكتروني

نص التجريم: تنص المادة (٢٣) على جرائم الاحتيال[١] والاعتداء على

[١] تتمثل صور جرائم الاحتيال المعلوماتي في ما يمكن ارتكابه من عمليات تغيير للبيانات في مرحلة إدخال البيانات، والتي تتم في المراحل الأولية لتشغيل النظام المعلوماتي، حيث يعتمد مُرتكب الجريمة بإدخال بيانات غير صحيحة أو بيانات مزورة، أو عمليات التلاعب حال إعداد أو تطوير البيانات، أو التلاعب في نظم المعالجة الإلكترونية للبيانات عن بُعد كالجرائم التي تستهدف اختراق أنظمة التحويل الإلكتروني للأموال والودائع المصرفية، وتتعدد صور الاحتيال المعلوماتي المرتكبة على شبكة الانترنت، ونذكر في هذا المقام عدد من القضايا، من أبرزها: قيام أحد الأشخاص بإنشاء حساب وهمي على شبكات التواصل الاجتماعي وإدعائه كذباً وانتحاله صفة أحد رجال السلطة القضائية واستخدامه لهذا الحساب المصطنع لإيهام المجني عليها وإقناعها بإمكان مساعدتها في إلحاق نجلها بسلك القضاء، وتحصله منها مقابل ذلك على مبالغ مالية، ومن الأمثلة الأخرى قيام الجاني بإدعائه كذباً وانتحاله صفة أستاذ جامعي وإيهامه للمجني عليها بإمكانية منحها شهادة ماجستير من إحدى الكليات مقابل مبلغ مالي طلبه منها، وقيام المجني عليها بتسليمه المال نظير حصولها على شهادة اكتشفت بعد ذلك أنها شهادة مزورة، ونذكر أيضاً حالة قيام الجاني بانتحال شخصية أحد الأشخاص، وتواصله مع بعض الشخصيات العامة مطالباً إياهم بدعمه ومساندته مادياً في بعض الحملات الداعمة للسياحة وفي بعض المجالات الأخرى، وذلك على غير الحقيقة، وهو ما تتحقق به جريمة النصب الواردة في قانون العقوبات.

بطاقات البنوك والخدمات وأدوات الدفع الإلكتروني[١]، حيث تقضي المادة المذكورة بأنه: " *يُعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة التي لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الإلكترونية. فإن قصد من استخدامها في الحصول على أموال الغير أو ما تتيحه من خدمات يُعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين. وتكون العقوبة الحبس مدة لا تقل عن سنة، غرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو إحدى هاتين العقوبتين، إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على تلك الخدمات أو مال الغير* "[٢].

العلة من التجريم: تتمثل علة التجريم فيمايلي:-

١- مواجهة صور الاعتداء على الأموال من خلال ارتكاب عمليات الاحتيال عبر شبكة الانترنت والاستخدام غير المشروع لبطاقات الائتمان.

---

(١) كان المشروع المقدم من الحكومة ينص على جرائم الاحتيال والاعتداء على البطاقة الائتمانية وأدوات الدفع الإلكتروني، وقد تم تعديل عنوان المادة خلال مناقشات لجنة الاتصالات بمجلس النواب، لتصبح على النحو الحالي، حيث كانت التسمية الأولية تقصر الحماية الجنائية على بطاقات الائتمان فحسب، بينما جاءت التسمية الحالية لتشمل كافة بطاقات البنوك والخدمات من بطاقات ائتمان وبطاقات وفاء ودفع إلكتروني.

(٢) ومن التشريعات العربية التي حرصت على تجريم الوصول إلى بيانات وأرقام بطاقات البنوك التشريع الإماراتي (م١٢) والتشريع الكويتي(م٥).

٢- توفير الحماية لوسائل الدفع أو الوفاء باستعمال البطاقات البنكية التي حلت محل النقود والشيكات[١]، والتي ينتشر استخدامها في كافة دول العالم[٢].

محل الجريمة: يتمثل محل الجريمة في أدوات الدفع الإلكترونية التي تشمل البطاقات البنكية وبطاقات الخدمات، وقد ورد النص على هذه الطوائف من البطاقات على سبيل المثال وليس الحصر، حيث أشار القانون إلى عبارة:" *أو غيرها من أدوات الدفع الإلكترونية* "، ومن ثم فلا تقتصر الحماية الجنائية على البطاقات البنكية أو بطاقات الخدمات فحسب، وإنما تمتد لكل أداة تستخدم في الدفع الإلكتروني [٣]، وفيمايلي نتناول بإيجاز ماهية كل من البطاقات البنكية وبطاقات الخدمات، وذلك على النحو التالي:-

١) البطاقات البنكية[٤]: أدى إدخال الحاسب الآلي في مجال عمليات البنوك إلى تطور

---

[١] د. جميل عبد الباقي الصغير: الحماية الجنائية لبطاقات الائتمان الممغنطة، دراسة تطبيقية في القضاء الفرنسي والمصري، دار النهضة العربية،١٩٩٩، ص٣؛ د. عمر سالم: الحماية الجنائية لبطاقة الوفاء، دراسة مقارنة، ط١، ١٩٩٥، القاهرة، دار النهضة العربية، ص١٤.

[٢] تشير التقديرات إلى أن حجم بطاقات الائتمان على مستوى العالم حتى نهاية عام ٢٠١٢ قد بلغ (٦٨،٦٦) مليار بطاقة. انظر: دليل عمل الإدارة العامة لمباحث الأموال العامة لعام ٢٠١٤، وزارة الداخلية، ص٤١٥.

[٣] ومن التشريعات التي عرفت بطاقات الدفع الإلكتروني التشريع القطري والعماني.

[٤] يرجع أول ظهور للبطاقات البنكية إلى عام ١٩٥٠ في الولايات المتحدة الأمريكية، حيث أصدرت مؤسسة داينرز كلوب الأمريكية أو بطاقة بنكية تستخدم في أعمال الدفع البنكي، وقد انتشر بعد ذلك استخدامها في داخل الولايات المتحدة وانتقلت بعد ذلك إلى مختلف دول العالم كبديل عن النقود وانتشر استخدامها من خلال العديد من المؤسسات المالية والمصرفية. ومن أشهر المؤسسات المالية الدولية العاملة في مجال البطاقات البنكية مؤسسات فيزا الدولية وماستر كارد العالمية وداينرز كلوب العالمية وجي سي بي وشركة أميريكان إكسبريس.

وتضطلع هذه المؤسسات بدور مهم في منظومة الدفع البنكي، من خلال: إضفاء القبول والصفة الدولية للبطاقات المصدرة من البنوك الأعضاء المصرح لها بالتعامل في هذا المجال، وإدارة عمليات بطاقات الدفع الإلكتروني من خلال شبكات المعلومات والاتصالات الخاصة بها، والتي توفر للبنوك الأعضاء عمليات المقاصة والتسويات الإلكترونية فيما بينهم، علاوة على وضع المعايير =

الخدمات المصرفية التي تقدمها البنوك للأفراد، من خلال إعطاء العملاء إمكانية سحب النقود، من خلال أجهزة التوزيع الأوتوماتيكي، باستخدام بطاقات السحب المنتشرة في أماكن كثيرة، وفي أيام العطلات، دون حاجة إلى الرجوع إلى البنك نفسه الذي يوجد به حساب العميل، فضلاً عن إجراء عمليات الشراء من العديد من المتاجر باستخدام هذه البطاقات البنكية، على أن يقوم العميل بسداد قيمة ما تلقاه من خدمة أو مسحوبات نقدية وفقاً لشروط وأوضاع معينة[١]، وهو ما استغله بعض المجرمين في الاستيلاء على أموال الناس بأساليب التلاعب في هذه البطاقات، سواء كان ذلك باستعمال بطاقات الائتمان التي فقدها أصحابها، أو بتزوير هذه البطاقات[٢].

وبطاقات الدفع البنكية -من ناحية الشكل- هي قطعة من البلاستيك لها مواصفات كيميائية محددة ذات أبعاد قياسية[٣]، وهي – من الناحية القانونية- أداة دفع

=

والنظم وتحديد القواعد والإجراءات التي تقوم البنوك الأعضاء بتطبيقها لتحديد حقوق والتزامات كل عضو ومدى مسئوليته تجاه الآخرين، كما تقوم بدور لجنة التحكيم في حالة النزاعات بين أعضائها.

وتستحوذ منظمة الفيزا العالمية على النصيب الأكبر من حجم هذه البطاقات والذي يقارب النصف بنسبة ٤٩،٦%، بينما تأتي منظمة ماستر كارد في المرتبة الثانية بنسبة ٣٢،٥%، ثم أميريكان اكسبريس بنسبة ٨،٥%، يونيون باي بنسبة ٦،٩%، ثم JCB بنسبة ٢،٣% وأخيراً داينرز كلوب بنسبة ٠،٢%. انظر: دليل عمل الإدارة العامة لمباحث الأموال العامة لعام ٢٠١٤، مرجع سابق، ص٤١٥.

(١) المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٦٥٦؛ انظر: الطعن المدني رقم ٧٢٠ لسنة ٧٦ق، جلسة ٢٠١٢/٥/١٢.

(٢) د. حسنى الجندي: شرح قانون العقوبات- القسم الخاص، جرائم الأموال، ٢٠٠١، ص٨٠ ومابعدها.

(٣) تصنع البطاقات البنكية من مادة "البولي فينيل كلورايد"PVC بأبعاد (طول ٨٥،٦ممxعرض٥٣،٩مم وبسمك٠،٧٦مم). انظر: دليل عمل الإدارة العامة لمباحث الأموال العامة لعام ٢٠١٤، مرجع سابق، ص٤١٤.

أو وفاء، تقوم مقام النقود والشيكات في التعامل، يبين فيها: اسم الجهة المصدرة لها، وشعارها، ورقمها، واسم حاملها، وتوقيعه، ورقم حسابه، وتاريخ صلاحيتها وانتهائه، ويستطيع صاحبها أن يسحب مبالغ نقدية من أجهزة التوزيع الأوتوماتيكي لأوراق البنكنوت، أو أن يحصل على ما يحتاجه من سلع أو خدمات بتقديم بطاقته إلى التاجر الذي يدون بياناتها باستخدام آلة طابعة إلكترونية أو يدوية في فاتورة يوقعها العميل، يرسل نسخة منها إلى الجهة المصدرة للبطاقة لسداد قيمتها.

أ) الطبيعة القانونية للبطاقات البنكية: لا تعتبر بطاقات الدفع البنكي أداة وفاء مثل الشيك، ومن ثم لا تطبق عليها أحكام جريمة إصدار شيك بدون رصيد، كما لا تعتبر بمثابة نقود ورقية، وإنما هي أداة وفاء الكتروني ذات طبيعة خاصة[١].

ب) أنواع البطاقات البنكية[٢]:يمكن لدواعي التبسيط التمييز بين نوعين من البطاقات البنكية هما بطاقات الائتمان وبطاقات الخصم، الأولى تعمل بفكرة القرض المحمول، فمنح هذه البطاقة يشكل قرضاً ممنوحاً لعميل البنك، فحينما يصدر البنك بطاقة ائتمان لأحد الأشخاص وفقاً لضوابط البنك الموضوعة سلفاً، فإنه يحدد له سقف ائتماني معين، أو حد أقصى للنقود التي يمكن إنفاقها باستخدام

---

[١] د. حسنى الجندي: التشريعات الجنائية الخاصة، مرجع سابق، ص١٥٧.

[٢] يمكن التمييز من حيث الصنع بين نوعين من بطاقات الدفع الإلكتروني، الأولى- البطاقات الممغنطة، وهي بطاقات بلاستيكية تحتوي على شريط ممغنط من الخلف يستخدم في إدخال وتخزين البيانات التي يتم تشفيرها عليها من خلال ثلاث مسارات نفضية، ويتم قراءة تلك البيانات بواسطة نقاط البيع الالكتروني POS وماكينات الصراف الآلي، والنوع الثاني من البطاقات هو البطاقات الرقائقية وهي بطاقات بلاستيكية مزودة بشريحة إلكترونية من مادة السيليكون تستخدم في إدخال وتخزين البيانات، إلا أنها أكثر أماناً من البطاقات الممغنطة لصعوبة قراءة البيانات التي عليها والحصول على نسخة منها. انظر: دليل عمل الإدارة العامة لمباحث الأموال العامة لعام ٢٠١٤، مرجع سابق، ص٤١٩

البطاقة، وفور حصول العميل على تلك البطاقة، فإنه يمكن استخدامها في أعمال الشراء أو الحصول على الخدمات من المحال التجارية بدلاً من الدفع النقدي، حيث يتم تسجيل وتلك المعاملات فور حدوثها، ويقوم البنك المصدر للبطاقة بالسداد الفوري، ويمنح العميل فترة سماح تتراوح بين (٣٠، ٥٥ يوماً) للسداد خلالها.

أما النوع الثاني من البطاقات البنكية فهي بطاقات الخصم، وهي تشكل الجزء الأكبر من حجم بطاقات الدفع المصدرة حول العالم؛ إذ تشير التقديرات إلى أن ربع سكان العالم البالغين يستخدمونها، وهي تتماثل مع بطاقات الائتمان من حيث الشكل، فكلتاهما بطاقات بلاستيكية تحمل اسم صاحبها ورقم حسابه، ويتم استخدامها لسداد المدفوعات، بينما يمكن التمييز بين البطاقتين من حيث الاسم، فكلمة ائتمان تعني اقتراض وكلمة خصم تعني سحب من رصيد فعلي، فبينما تتيح بطاقة الائتمان لصاحبها السداد فيما بعد، توجب بطاقة الخصم الدفع الفوري متزامناً مع حدوث المعاملة، لذلك فإن بطاقة الخصم تكون مرتبطة مباشرة بالحساب البنكي لصاحبها، وهو حينما يقوم باستخدامها، فإنه يستخدم رصيد حسابه البنكي فقط[١].

بينما يميز جانب آخر من الفقه الجنائي[٢] بين أربعة أنواع من بطاقات الدفع البنكي، وهي: بطاقات الاعتماد، وبطاقات الخصم الشهري، وبطاقات الخصم الفوري، بطاقات ضمان الشيكات، فالأولى تستخدم كأداة وفاء وائتمان في نفس الوقت، لأنها تتيح لحاملها الحصول على السلع والخدمات فور تقديمها مع الدفع الآجل لقيمة هذه المشتريات للبنك المصدر لتلك البطاقة، ومن الأمثلة لها: الفيزا كارد، والماستر كارد،

---

[١] المرجع السابق، ص ص٤١٩، ٤٢٠.

[٢] د. عمر سالم: الحماية الجنائية لبطاقة الوفاء، مرجع سابق، ص١٤؛ د. نائلة عادل محمد فريد قورة، مرجع سابق، ص٥١١.

وأمريكان اكسبريس، والثانية تستخدم كأداة وفاء وائتمان، إلا أن فترة الائتمان لا تتعدى شهر، والثالثة تستخدم كأداة وفاء فقط، أما النوع الرابع، وهي بطاقات ضمان الشيكات فهي وسيلة لضمان حصول التاجر أو مقدم الخدمة على المقابل الذي تم تسويته عن طريق الشيك.إلا أننا نميل إلى الأخذ بالتقسيم الأول نظراً لبساطته وواقعيته في التطبيق العملي.

ج) موقف القضاء المصري من البطاقات البنكية: نستعرض في شأن البطاقات البنكية موقف كل من المحاكم الاقتصادية ومحكمة النقض، وذلك على النحو التالي:-

موقف المحاكم الاقتصادية من البطاقات البنكية: ترى المحاكم الاقتصادية أن بطاقات الائتمان عبارة عن مجموعة من الأفكار والمعاني صادرة عن البنوك أو المؤسسات المالية تتوافر فيها مقومات المحرر، وبالتالي إذا وقع تغييراً في أحد بياناتها مثل البيانات باسم الحامل ورقم الحساب وتاريخ الصلاحية، فإن الأمر يشكل تزويراً في محرر عرفي، إذا كانت الجهة المصدرة للبطاقة بنكاً خاصاً أو أجنبياً، ويعتبر تزوير في محرر رسمي إذا كانت البطاقة صادرة عن أحد المصارف المملوكة للدولة أو تساهم في رأس مالها بنصيب ما، سواء كان تغيير الحقيقة واقعاً على البيانات المرئية، أو وقع التغيير على البيانات الإلكترونية "الشريط الممغنط" غير المرئية بالعين المجردة، فخفاء معنى المحرر على العين المجردة واحتياجه لإجراءات خاصة لقراءته لا ينفي وجوده[1].

[1] انظر: حكم محكمة جنح مستأنف القاهرة الاقتصادية، جلسة ٢٠١٠/٤/٤، الدعوى رقم ١٦ لسنة ٢٠١٠، جنح مستأنف المقيدة برقم ٣٧٢٧ لسنة ٢٠٠٩ جنح اقتصادي، وقارن حكم محكمة جنح مستأنف القاهرة الاقتصادية، جلسة ٢٠١١/٥/١٢، الدعوى رقم ٣١٥ لسنة ٢٠١١، جنح مستأنف المقيدة برقم ١٠٠٧ لسنة ٢٠١١ جنح اقتصادي.

بينما اختلف موقف بعض المحاكم الاقتصادية بشأن بطاقات الائتمان ما بين اتجاهين الأول لا يراها من قبيل المحررات الإلكترونية لكونها لا تشكل رسالة بيانات[١]، واتجاه آخر يراها من قبيل المحررات الإلكترونية، وهو اتجاه محكمة الجنح المستأنفة بالمحاكم الاقتصادية والتي ترى بطاقات الائتمان من قبيل المحررات الإلكترونية، حيث قضت بتوافر جريمة التزوير في المحررات الإلكترونية واستعمالها، إذا ما قام المتهم بإزالة البيانات الأصلية المكورة على الشريط الممغنط، وقام باستحداث بيانات جديدة عليها، ثم استعماله بتقديمه إلى أحد المتاجر، ليحصل على ثمن البضائع التي اشتراها مع علمه بوجود هذا التزوير[٢]. وكانت المادة الأولى من قانون تنظيم التوقيع الإلكتروني رقم ١٥ لسنة ٢٠٠٤ تعرف المحرر الإلكتروني بأنه:" رسالة تتضمن معلومات تنشأ أو تدمج أو تخزن أو ترسل أو تستقبل كلياً أو جزئياً بوسيلة إلكترونية أو رقمية أو ضوئية أو بأية وسيلة أخرى متشابهة".

موقف محكمة النقض من البطاقات البنكية: بينما جرى قضاء النقض على سريان وصف المحرر في مفهوم جريمة التزوير على بطاقات الائتمان الممغنطة باعتبارها ورقة من أوراق البنك، ومن ثم فإن تزوير بطاقات الائتمان الممغنطة الخاصة ببنك تساهم الدولة بنصيب في رأس ماله يشكل جناية التزوير في محررات شركة مساهمة تشارك الدولة في مالها بنصيب، بينما كانت إحدى محاكم الجنايات قد اعتبرت كروت الائتمان "الفيزا" من قبيل المحررات العرفية الإلكترونية[٣].

---

(١) انظر حكم محكمة جنح القاهرة الاقتصادية، جلسة ٢٠١١/٥/١٢، الدعوى رقم ٣١٥ لسنة ٢٠١١، جنح مستأنف المقيدة برقم ١٠٠٧ لسنة ٢٠١١ جنح اقتصادي، مشار إليها المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٦٥٧.

(٢) انظر حكم محكمة جنح مستأنف القاهرة الاقتصادية، الدعوى رقم (٢٥٦٩) لسنة ٢٠٠٩ جنح القاهرة الاقتصادية، جلسة ٢٠٠٩/١٠/١١، مشار إليها المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص ص٦٥٦، ٦٥٧.

(٣) انظر: الطعن رقم ٣٩٥٠٥ لسنة ٧٧ق، نقض جنائي جلسة ٢٠١٦/٣/١٥، ص٢.

وكانت محكمة النقض في حكم سابق قد ردت على دفاع الطاعنين بأن البطاقات الائتمانية موضوع الدعوى تخرج عن نطاق المحررات الرسمية بالمعنى الذي قصده القانون، وأنها لا تعدو إلا محررات عرفية إلكترونية، حيث قررت محكمتنا العليا بأنه:" لما كان ذلك، وكان المحرر في جريمة التزوير يعرف بأنه مجموعة من الكلمات التي لها معنى والتي ينسب صدورها إلى شخص معين "طبيعي أو معنوي" من شأنها أن ترتب مركزاً أو آثاراً قانونية، ومن خصائص هذا المحرر قابليته للقراءة وثبات معانيه. ولا يقدح في انطباق هذا التعريف وتلك الخصائص على بطاقات الائتمان الممغنطة أنها لا تشتمل إلا على بيان لاسم وبيان الجهة المصدرة للبطاقة وبيان التوقيع؛ ذلك أن بيان الجهة المصدرة وبيان الاسم وبيان التوقيع يفيد صدور هذه البطاقة من جهة معينة لصالح شخص معين، وأن هذا المحرر بوصفه بطاقة للتعامل مع البنك مباشرة، أو من خلال شخص الغير، فإن مضمونه يفيد معنى معين يصلح محلاً للحماية الجنائية بمقتضى أحكام التزوير، إذا ورد تغير على هذا المعنى، ولا يغير من توافر صفة المحرر في بطاقات الائتمان الممغنطة أيضاً مدى قابلية تلك البطاقات للقراءة بحسبان أن البيانات المكتوبة على الشريط الممغنط والمتعلقة بحساب العميل من ناحية ورقمه ورصيده من ناحية أخرى والتي تشكل جزءاً لا يتجزأ من البطاقة بوصفها محرراً لا يمكن قراءتها بالعين المجردة، ولكن ذلك لا يحول دون قراءتها بواسطة أجهزة الكمبيوتر الخاصة بالبنك أو تلك التي يضعها البنك تحت تصرف التاجر، فليس في القانون ما يستوجب أن تكون بيانات المحرر مقروءة بالعين المجردة، وتأسيساً على ما تقدم فإن البطاقات الممغنطة يسري عليها وصف المحرر في مفهوم جريمة التزوير باعتبارها ورقة من أوراق البنوك... ولما كانت البنوك تنتمي إلى الشركات المساهمة ولما كانت الدولة تساهم بنصيب في رأس مال معظم تلك البنوك ومنها البنك المجني عليه في الدعوى المطروحة فإن تزوير بطاقات الائتمان الممغنطة الخاصة به تشكل

جناية التزوير في محررات شركة مساهمة تشارك الدولة في مالها بنصيب وفقاً لقانون العقوبات المصري[١].

ويأتي هذا الاجتهاد القضائي للقضاء المصري في ظل غياب التنظيم القانوني لمثل هذه البطاقات[٢]، حيث اعتبرت المحاكم الاقتصادية بطاقات الائتمان من قبيل المحررات الإلكترونية وطبقت عليها أحكام التزوير في محررات إلكترونية عملاً

---

[١] انظر: الطعن رقم ٤٥٣٠٢ لسنة ٧٦ق، نقض جنائي جلسة ٢٠٠٧/١١/٢٠، حكم غير منشور، ص ص٥-٧.

[٢] يثير موقف محكمة النقض المصرية بشأن اعتبار بطاقات الائتمان البنكية من قبيل المحررات العرفية الالكترونية وأنه يسري عليها أحكام جريمة التزوير في المحررات تساؤلاً لدى الفقه الجنائي بشأن التفسير القضائي للنصوص الجنائية؛ إذ يقتصر القياس في المواد الجنائية على المواد الإجرائية ويحظر في مواد التجريم والعقاب.

ويقصد بالقياس في مواد التجريم إلحاق فعل مباح بفعل مجرم لاشتراكهما في علة التجريم، أي استكمال ما يشوب القانون من نقص عن طريق إيجاد الحل لمسألة لم ينظمها القانون وذلك عن طريق استعارة الحل الذي قرره القانون لمسألة مماثلة، والسماح للقاضي بذلك يحوله من قاضي إلى مشرع يقوم بخلق قاعدة عقابية جديدة لم ينص عليها المشرع فعلياً.

وهو ما يراه البعض- وبحق- خروجاً من جانب محكمتنا العليا عن الأصول المستقرة بشأن تفسير النصوص الجنائية؛ إذ ما كان يجب عليها تقرير سريان وصف المحرر في مفهوم جريمة التزوير على بطاقات الائتمان البنكية لغياب النص، فمن شأن هذا الحكم -فيما أورده من قياس محظور- إنشاء لنص تجريمي جديد، وهو ما يخرج عن اختصاص محكمتنا العليا، وأنه كان ينبغي على محكمتنا العليا بدلاً من تقريرها لهذا القياس المحظور عليها، أن تناشد المشرع الجنائي بسرعة التدخل بإصدار نص صريح يجرم تزوير بطاقات الائتمان البنكية.

فالقاضي الجنائي يجب عليه عند تفسيره للنص العقابي التزام جانب الدقة وعدم تحميل عبارات النص فوق ما تحتمل، وهذا التفسير المنضبط لقانون العقوبات لا يحول بالطبع دون محاولة تطويع النصوص لتحيط بالمعطيات التكنولوجية الحديثة وخاصة في مجال ثورة المعلومات، ولكن على القاضي إذا اتضح أن الأمر قد تجاوز حدود التفسير المنضبط إلى حد خلق جرائم جديدة، وجب عليه الحكم بالبراءة تاركاً الأمر لتدخل تشريعي. انظر: هشام عبد السيد الصافي: الجرائم الإلكترونية في مصر ودستورية مبدأ الشرعية الجنائية، بحث منشور بمجلة جيل الأبحاث القانونية المعمقة، العدد١٤، مايو ٢٠١٧، مركز جيل البحث العلمي، الجزائر، ص١٥٣.

بالقانون رقم ١٥ لسنة ٢٠٠٤ بشأن تنظيم التوقيع الإلكتروني، بينما ذهبت محكمة النقض إلى أن هذا المحرر بوصفه بطاقة للتعامل مع البنك مباشرة، أو من خلال شخص الغير مضمونه يفيد معنى معين يصلح محلاً للحماية الجنائية بمقتضى أحكام التزوير، إذا ورد متغير على هذا المعنى[1]، ومن ثم طبقت أحكام التزوير على بطاقات الائتمان،

(1) وقد أشارت محكمة النقض المصرية في أحد أحكامها إلى أن:" لما كان المحرر في جريمة التزوير يعرف بأنه مجموعة من الكلمات التي لها معنى والتي ينسب صدورها إلى شخص معين – طبيعي أو معنوي- من شأنها أن ترتب مركزاً أو آثاراً قانونية، ومن خصائص هذا المحرر قابليته للقراءة، ولا يقدح في انطباق هذا التعريف وتلك الخصائص على بطاقات الائتمان الممغنطة أنها لا تشتمل إلا على بيان الاسم وبيان الجهة المصدرة للبطاقة وبيان التوقيع؛ ذلك أن بيان الجهة المصدرة وبيان الاسم وبيان التوقيع يفيد صدور هذه البطاقة من جهة معينة لصالح شخص معين، وأن هذا المحرر بوصفه بطاقة للتعامل مع البنك مباشرة، أو من خلال شخص الغير مضمونه يفيد معنى معين يصلح محلاً للحماية الجنائية بمقتضى أحكام التزوير، إذا ورد متغير على هذا المعنى، ولا يغير من توافر صفة المحرر في بطاقات الائتمان الممغنطة أيضاً مدى قابلية تلك البطاقات للقراءة بحسبان أن البيانات المكتوبة على الشريط الممغنط والمتعلقة بحساب العميل من ناحية ورقمه ورصيده من ناحية أخرى والتي تشكل جزءاً لا يتجزأ من البطاقة بوصفها محرراً لا يمكن قراءتها بالعين المجردة، ولكن ذلك لا يحول دون قراءتها بواسطة أجهزة الكمبيوتر الخاصة بالبنك أو تلك التي يضعها البنك تحت تصرف التاجر، فليس في القانون ما يستوجب أن تكون بيانات المحرر مقروءة بالعين المجردة، وقد فسر المشرع الفرنسي شكاً كان يثار حول ما يسمى بالمحرر الإلكتروني وذلك عندما عدل المادة ١/١٤٤ من قانون العقوبات الفرنسي حتى تتضمن الإشارة إلى المحررات التي تتكون من بيانات إلكترونية، وتأسيساً على ما تقدم فإن البطاقات الممغنطة يسري عليها وصف المحرر في مفهوم جريمة التزوير باعتبارها ورقة من أوراق البنوك،....، ولما كانت البنوك تنصب على الشركات المساهمة، ولما كانت الدولة تساهم بنصيب في رأس مال محفظة تلك البنوك ومنها البنك المجني عليه في الدعوى المطروحة، فإن تزوير بطاقات الائتمان الممغنطة الخاصة به تشكل جناية التزوير في محررات شركة مساهمة تشارك الدولة في مالها بنصيب وفقاً لقانون العقوبات المصري، وذلك على خلاف نص القوانين العربية. لما كان ذلك، وكان الحكم المطعون فيه قد التزم هذا النظر مطرحاً دفاع الطاعن في هذا الخصوص بأسباب سائغة بعد أن اعتبر التزوير في البطاقات الائتمانية موضوع الاتهام وهي محررات لإحدى الشركات المساهمة المصرية "بنك مصر" تزويراً في محررات رسمية وأوقع عليه العقوبة المنصوص عليها في المادة ٢١٤مكرراً عقوبات باعتبارها عقوبة أشد من العقوبات المنصوص عليها في القوانين الأخرى، ومن ثم فإنه يكون قد طبق أحكام القانون تطبيقاً صحيحاً، ويضحى ما يثيره الطاعن بأسباب طعنه من دعوى الخطأ في تطبيق القانون غير سديد". انظر: الطعن رقم ٣٩٥٠٥ لسنة ٧٧ق، جلسة =

وعليه نجد أن القضاء المصري قد توسع في تطبيق النصوص الجنائية الواردة في قانون العقوبات وقانون تنظيم التوقيع الإلكتروني لتسري على بطاقات الائتمان، وأن القضاء المصري لم يكن له خياراً في هذا النهج بالنظر إلى عدم وجود نصوص تشريعية تنظم استخدام هذه البطاقات، ومن ثم فإن الباحث يرى أنه كان من الأحرى بالمشرع المصري أن يضمن هذا القانون نصاً لتجريم تزوير بطاقات الدفع البنكي كما فعلت العديد من التشريعات المقارنة[١].

٢) بطاقات الخدمات: لم يقتصر التجريم على بطاقات الوفاء البنكي فحسب، وإنما يمتد كذلك ليشمل الكروت الخاصة بالخدمات مثل الكارت الخاص بالبنزين والكارت الخاص بالتموين[٢]، وحسناً فعل المشرع المصري بالنص على ذلك لما فيه من توفير الحماية الجنائية لمثل هذه الطائفة من كروت الخدمات ذات الصلة بتقديم الدعم الحكومي للمواطنين، حماية لحقوقهم والاقتصاد القومي. ويمكن التمييز بين هذا النوع من البطاقات والبطاقات البنكية أن الأخيرة ترتبط بعمل البنوك سواء أكانت حسابات بنكية أو ائتمان، بينما تتصل الأولى بالخدمات التي تقدمها الدولة للمواطنين، ومن ثم ترتبط الأولى بعمل الجهات الحكومية بينما ترتبط الأخيرة بعمل البنوك.

=

٢٠١٦/٣/١٥، النشرة التشريعية والقانونية لمحكمة النقض، الصادرة عن المكتب الفني لمحكمة النقض، إصدار يوليو وأغسطس وسبتمبر ٢٠١٦، ص ص١٢٧، ١٢٨.

[١] ومن التشريعات العربية التي جرمت تزوير بطاقات الائتمان التشريع الإماراتي(م١٣) والتشريع العماني (م٢٨) والتشريع القطري(م١٢).

[٢] انظر: مضبطة مجلس النواب المصري، الجلسة السادسة والخمسين، المعقودة في ٢٠١٨/٥/١٤م، مرجع سابق، ص١٠٣.

الركن المادي: يتحقق الركن المادي للجريمة من العناصر التالية:-

السلوك الإجرامي- الوصول إلى بيانات البطاقات البنكية: تطلب القانون أن يكون هذا الوصول أو التحصل باستخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، وأن يقع ذلك على بيانات البطاقات البنكية أو بطاقات الخدمات، وهو ما يتحقق بكل فعل إيجابي من شأنه استخدام أو استعمال الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، في الوصول بدون وجه حق إلى أرقام أو بيانات بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الإلكترونية.

وقد يتم الحصول على أرقام وبيانات البطاقات من خلال بعض المواقع الإلكترونية أو منتديات بعض القراصنة عبر شبكة الانترنت، أو من خلال استخدام أجهزة تقنية لالتقاط أرقام هذه البطاقات الخاصة ببعض العملاء، أو من خلال استخدام برامج لتخليق أرقام بطاقات الائتمان، يتم تزويدها بالرقم الخاص بالبنك المُصدر للبطاقة[1]، أو عن طريق الاحتيال بواسطة البريد الإلكتروني، والقمار عبر الإنترنت، ويتم استخدام هذه الأرقام في الحصول على الخدمات والسلع من خلال شبكة الإنترنت، ومن ثم تكون الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات كالبرامج الخاصة، هي وسيلة هذا الفعل.

صور السلوك الإجرامي: نستعرض فيما يلي أبرز صور السلوك الإجرامي للوصول إلى بيانات وأرقام البطاقات البنكية، وذلك على النحو التالي:-

١) استخدام بعض المواقع أو الأسواق غير المشروعة للحصول على أرقام بطاقات الائتمان: حيث يقوم الجاني بالتواصل عبر شبكة الانترنت بمجموعات من

---

[1] د. جميل عبد الباقي الصغير: الحماية الجنائية لبطاقات الائتمان الممغنطة، مرجع سابق، ص٧ ومابعدها.

قراصنة المعلومات والدخول إلى المواقع الإلكترونية والأسواق غير المشروعة للاتجار في أرقام بطاقات الائتمان، والحصول على هذه البيانات والأرقام منها، سواء أكان ذلك بمقابل أو بدون مقابل، ويقوم بعد ذلك باصطناع بطاقات بنكية مزورة، يتم تلقينها بأرقام البطاقات البنكية المتحصل عليها[١].

٢) القرصنة عبر شبكة الانترنت: وتتم من خلال لجوء أحد القراصنة بالدخول عبر شبكة الانترنت إلى مواقع التسوق التي لا تتوافر لها إجراءات تأمين وحماية كافية للحصول على بيانات بطاقات الدفع الإلكتروني الخاصة بعملائها، أو من خلال إطلاق بعض برامج التجسس عبر شبكة الانترنت، من خلال المساحات الإعلانية وبعض المواد الدعائية، واستغلالها في التقاط بيانات الدفع الإلكتروني الخاصة بمستخدمي الشبكة[٢].

٣) استخدام برامج لتخليق أرقام بطاقات الائتمان: وهذه البرامج يتم تسويقها من خلال بعض مواقع القراصنة على شبكة الانترنت، ومن أشهرها برنامج كارد ماستر، وتستخدم هذه البرامج في تخليق أرقام بطاقات الائتمان وتوفيقها، من خلال تزويدها برقم بطاقة ائتمانية صحيحة منسوبة لأحد البنوك، ليتولى البرنامج تخليق ما يقرب من مائة رقم بطاقة صحيحة منسوبة لذات البنك، حيث يتم استخدام تلك الأرقام بعد ذلك في عمليات شراء وتسوق خصماً من الرصيد

---

[١] ومن التطبيقات القضائية لهذا الأسلوب الإجرامي قيام أحد المتهمين بالتحصل على أرقام وبيانات البطاقات من أحد المواقع على شبكة الانترنت، وقيامه اصطناع وتزوير البطاقات الائتمانية وتسليمها لشركائه للقيام بعمليات شراء وتسوق، حيث تبين أن البطاقات المضبوطة مزورة كلياً وملقن الشريط الممغنط الخاص بها ببيانات بطاقة أخرى خاصة بعملاء بنوك بالولايات المتحدة الأمريكية. انظر: دليل عمل الإدارة العامة للأموال العامة، مرجع سابق، ص ص ٤٤٨-٤٥٠.

[٢] المرجع السابق، ص ص٤٣٦، ٤٣٧.

الائتماني لصاحب البطاقة الأصلية، والأصل في تحديد بطاقات الائتمان أنها تخضع لمعادلات رياضية معقدة، ويحكمها شفرة خاصة بكل بنك، ويتم تحديدها سلفاً بمعرفة المنظمات الدولية المسئولة عن هذا النشاط مثل فيزا وماستر كارد[١].

٤) استخدام أجهزة تقنية لنسخ بيانات الشريط الممغنط لبطاقات الائتمان: ويتم ذلك من خلال استخدام وحدة إلكترونية صغيرة الحجم لنسخ وتخزين البيانات الملقنة للأشرطة الممغنطة، حيث يمكن للوحدة الواحدة التقاط وتخزين بيانات لعشرين بطاقة دفع إلكتروني، ويتبع عملية الالتقاط، عملية تفريغ محتوى هذه الوحدة إلى أحد الملفات على الحاسب الآلي، ليتم إعادة تلقينها بعد ذلك من خلال الحاسب الآلي على أشرطة ممغنطة لبطاقات بلاستيكية خام أو مقلدة أو صحيحة منتهية الصلاحية باستخدام وحدة تكويد الأشرطة الممغنطة[٢].

٥) السطو الإلكتروني على ماكينات الصراف الآلي ATM:حيث يقوم الجناة بزرع أجهزة مسح أو استنساخ لأرقام بطاقات الائتمان وكاميرات رقمية لمعرفة الرقم

---

[١] ومن التطبيقات القضائية لهذا الأسلوب الإجرامي قيام أحد المتهمين بتخليق أرقام بطاقات دفع إلكتروني من رقم بطاقة صحيحة لعملاء بعض البنوك المصرية والأجنبية، وقيامه بإجراء عمليات شراء لأجهزة كمبيوتر نقال وهواتف محمولة وأجهزة تابلت من شركات موبايل شوب عن طريق مواقع تلك الشركات على شبكة الإنترنت، وتم خصم قيمتها من حساب تلك البطاقات الائتمانية المستولى عليها. المرجع السابق، ص ص٤٣٢-٤٥٨.

[٢] ومن التطبيقات القضائية لهذا الأسلوب الإجرامي قيام أحد المتهمين وزوجته بالاستيلاء على بيانات البطاقة الائتمانية الخاصة بعملاء البنوك من خلال استخدام جهاز قارئ للبيانات المكودة على الشرائط الممغنطة لبطاقات الدفع الإلكتروني لعملاء المحلات التجارية بأسلوب مغافلة العميل وتمرير بطاقته على جهاز صغير يمكن إخفائه في راحة اليد، ويقوم بعد ذلك باستخدام جهاز حاسب آلي لإعادة تكويدها تلك البيانات مرة أخرى على بطاقات مزورة باستخدام الجهاز ذاته، واستخدام البطاقات المزورة في إجراء عمليات سحب أموال من ماكينات الصراف الآلي من حسابات المجني عليهم. المرجع السابق، ص٤٥١.

السري للبطاقة PIN بأجهزة الصراف الآلي ATM ، حيث تقوم وحدة المسح والاستنساخ SKIMMER بالتقاط ونسخ بيانات وأرقام البطاقات الممغنطة التي يتم إيلاجها داخل تلك الماكينات والتقاط الرقم السري الشخصي باستخدام الكاميرات الرقمية التي يتم زرعها بماكينة الصرف، حيث يتم إرسال هذه البيانات إلى شخص آخر بالقرب من موضع الماكينة، يتولى استقبال هذه الأرقام، ليتم بعد ذلك إعادة تلقينها مرة أخرى إلى بطاقات مزورة واستعمالها في عمليات سحب نقدي أخرى[١].

وهناك أسلوب إجرامي آخر مشابه للأسلوب السابق يسمى الحلقة اللبنانية Lebanese Loop، يتم فيه تركيب حاجز داخل فتحة دخول البطاقة بماكينة الصراف الآلي ATM، والذي يقوم بحجز البطاقة عند مرورها ويحول دون انزلاقها بالماكينة، مما يضطر الضحية لتركها، فيقوم الجناة باستخراج الحاجز وما يحويه من بطاقات، أو يقوموا بنسخ البيانات الملقنة بالشريط الممغنط للبطاقات، وذلك بتثبيت الناسخ عند فتحة دخول البطاقة، والحصول على أرقامهم السرية، بتثبيت كاميرا فيديو مخفية بجوار لوحة المفاتيح[٢].

٦) التصيد الاحتيالي من خلال رسائل البريد الإلكتروني: حيث تتم عملية اصطياد

---

[١] ومن التطبيقات القضائية لهذا الأسلوب الإجرامي قيام أحد المتهمين بتثبيت واجهة بلاستيكية بها جهاز ناسخ لبيانات البطاقات "اسكيمر"، ملحق به كاميرا دقيقة، على بعض ماكينات الصراف الآلي المنتشرة بالقاهرة، الأمر الذي مكنه من الاستيلاء على بيانات بطاقات الائتمان والأرقام السرية الخاصة بعدد من عملاء البنوك المصرية، وإعادة تلقين تلك البيانات على بطاقات بلاستيكية أخرى، واستخدامها في سحب مبالغ مالية من حسابات المجني عليهم، وكان المتهم يتحصل على الواجهات البلاستيكية من إحدى الشركات الصينية، والتي ترد إليه عن طريق شركة DHL، وكان يقوم بإرسال البيانات الإلكترونية المستولى عليها إلى شريك له مقيم بدولة كندا، والذي كان يتولى فك شفرات البطاقات وإعادة تكويدها وإرسالها إليه عبر البريد الإلكتروني. انظر: المرجع السابق، ص ص٤٣٥-٤٥٥.

[٢] المرجع السابق، ص٤٤٣.

البيانات الشخصية والمصرفية عن طريق بريد إلكتروني تتلقاه الضحية، والذي يبدو للوهلة الأولى أنه مرسل من بنك أو مؤسسة حكومية أو مالية، ويتضمن هذا البريد طلب تحديث البيانات الخاصة بالضحية بهذه الجهة، من خلال الدخول على صفحة هذه الجهة والتي يوجد عنوانها بالبريد الإلكتروني، وهي صفحة مزيفة أنشأها القرصان لاستقبال بيانات الضحية، وما أن يتم الدخول إلى عنوان هذه الصفحة، يتم وإدخال البيانات، فإنها تذهب إلى هذا القرصان[1].

أن يكون الوصول إلى أرقام أو بيانات بطاقات البنوك أو الخدمات قد تم بدون وجه حق: أي أن يكون ذلك قد تم بطريق غير مشروع، وهو ما يتحقق بمجرد تحصل الجاني على هذه البيانات التي تخص الغير، بدون علمه أو رضائه، فهذه البيانات أو الأرقام شخصية، وتخص الشخص حامل البطاقة، وهو الشخص الذي لديه حساباً شخصياً لدى البنك المصدر للبطاقة، وهو الشخص المخول من البنك باستخدامها، حيث يصدر البنك مثل هذه البطاقات لتسهيل عملية حصول هذا الشخص على الخدمات المصرفية التي يقدمها البنك له.

---

[1] ومن أبرز التطبيقات القضائية المشهورة لهذا الأسلوب الإجرامي قيام أحد المتهمين الروس ببث عدة آلاف من الرسائل الإلكترونية الخادعة عبر شبكة الانترنت، مستهدفاً عملاء متجر epay الالكتروني، وقام بشراء أجهزة إلكترونية وحاسبات آلية محمولة باستخدام أرقام وبيانات بطاقات الائتمان التي حصل عليها، وقام بإجراء تحويلات نقدية عن طريق مؤسسة وسترن يونيون إلى حساب قام بفتحه في أحد البنوك بمدينة لوس أنجلوس الأمريكية، ثم قام بتحويلها بعد ذلك إلى حسابين بنكيين في كل من ليتوانيا وأوكرانيا، إلى أن تم ضبطه بمعرفة الشرطة التايلاندية في مايو ٢٠٠٣.

وفي قضية أخرى قام أحد المتهمين بالاتصال بعدد من عملاء عدد من البنوك، منتحلاً صفة أحد موظفي البنك، وترغيبهم في زيادة الحد الائتماني لبطاقاتهم كمبرر لطلب بيانات بطاقاتهم الائتمانية، واستخدامه تلك البيانات في الدخول على المواقع الالكترونية لإحدى شركات الاتصالات، طالباً منتجات منها، وتحميل قيمتها على حسابات البطاقات المستولي عليها، وكان المتهم قد استغل سابقة عمله كمندوب تسويق بإحدى شركات التأمين، وتوافر أسماء وبيانات بعض العملاء لديه، وتمكن من خلال تبادله لتلك البيانات مع مندوبي التسويق بالبنوك المختلفة، لإعداد قاعدة بيانات عن عملاء جدد، من الحصول على بيانات عملاء هذه البنوك. المرجع السابق، ص ص٤٣٩-٤٥٧.

استخدام أرقام أو بيانات بطاقات البنوك أو الخدمات للحصول على أموال الغير أو خدمات: تعد عملية الوصول إلى بيانات البطاقة البنكية التي تخص الغير هي المرحلة الأولى، والتي تتلوها مراحل أخرى، من خلال استعمالها في عمليات شراء البضائع والسلع والخدمات عبر شبكة الإنترنت، أو الاحتيال للاستيلاء على أموال الغير، حيث تبين أن بعض الجناة من معتادي التعامل بشبكة الانترنت قد تمكنوا من التقاط أرقام بطاقات الدفع الإلكترونية الخاصة ببعض العملاء من الشبكة، واستخدموا أرقامها في الحصول على السلع التي يرغبونها، وتم خصم القيمة من حساب العملاء الشرعيين لهذه البطاقات[١].

والاستخدام للبطاقات البنكية في الحصول على الأموال والخدمات يتحقق من خلال إبراز البطاقة أو أرقامها أو بياناتها وتقديمها أو الاحتجاج بها في السحب من أجهزة التوزيع الآلي، أو الحصول على الخدمات، وهو فعل وإن كان يتسم بأنه ذو طبيعة مستمرة، فيماثل بذلك فعل استعمال المستندات المزورة، إلا أنه يمكن أن يعتبر – حسب الوقت الذي يستغرقه- من قبيل الأفعال الوقتية، التي تبدأ بتقديم البطاقة أو رقمها أو بياناتها، وهو كذلك فعل يقبل التجدد بتجدد هذا الاستخدام، بمعنى أن هذه الجريمة تتحقق بكل عناصرها في كل مرة يتم فيها استخدام البطاقة في سحب أموال الغير أو الحصول على الخدمات التي تتيحها[٢].

وقد يؤدي استخدام الجاني لأرقام وبيانات البطاقة البنكية الخاصة بالمجني عليه، والتي تحصل عليها بدون وجه حق إلى استعمالها، وهو حامل غير شرعي لها، في الحصول على مال من حساب صاحبها، أو شراء سلع أو خدمات من التجار، وهو ما

---

[١] د. حسنى الجندي: التشريعات الجنائية الخاصة، مرجع سابق، ص٢٨.

[٢] د. جميل الصغير: الانترنت والقانون الجنائي، مرجع سابق، ص ص٣٦-٣٨.

يندرج تحت وصف الاحتيال أو النصب باتخاذ المتهم صفة غير صحيحة لإيهام التاجر أو البنك بأنه هو الحامل الشرعي للبطاقة، أو اتخذ اسماً كاذباً، وهو ما يعاقب عليه المشرع ولو لم يتوصل الجاني إلى الحصول على أموال الغير بالفعل، فالمشرع جعل من مجرد المحاولة أو الشروع في الحصول على أموال الغير جريمة قائمة بذاتها.

فإذا توصل بالفعل إلى الاستيلاء على مال الغير لنفسه أو لغيره، باستخدام هذه الأرقام أو البيانات للبطاقات البنكية، فإنه يعاقب بالعقوبة المشددة الواردة بالفقرة الثالثة من المادة ٢٤ من القانون، أما إذا لم يتوصل إلى ذلك، فيخضع للعقوبة المقررة في الفقرة الثانية من المادة المذكورة، والعبرة في ذلك ليست بمجرد المحاولة، ولكن بكل فعل يكون من شأنه –لو تسلسلت نتائجه- التوصل إلى حصول الجاني على أموال الغير أو الخدمات التي تتيحها البطاقة الائتمانية[1].

الركن المعنوي: هذه الجريمة من الجرائم العمدية التي يتحقق فيها الركن المعنوي بتوافر القصد الجنائي العام بعنصريه العلم والإرادة، بأن يكون الجاني عالماً باستخدامه لبيانات أو أرقام تخص بطاقات بنكية للغير، وأن هذا الوصول لهذه البيانات قد تم بشكل غير مشروع، وأن تتجه إرادته إلى الاستفادة من هذه البيانات أو الأرقام في الحصول على أموال الغير أو غير ذلك من الخدمات.

العقوبة: ميز القانون في عقوبة الاحتيال باستخدام بطاقات البنوك بين ثلاث حالات، وذلك على النحو التالي:-

١) القصد الجنائي العام: عاقب القانون هذه الحالة بعقوبة الحبس مدة لا تقل عن ثلاثة أشهر، والغرامة التي لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف

[1] د. حسنى الجندي: التشريعات الجنائية الخاصة، مرجع سابق، ص١٦١.

جنيه، أو بإحدى هاتين العقوبتين، إذا استعمل الجاني الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الحصول بدون وجه حق على البيانات أو الأرقام الخاصة بالبطاقات البنكية للغير، ومن ثم فالقاضي مخير بين الحكم بالحبس والغرامة معاً، أو الحكم بالحبس أو بالغرامة فقط، في ضوء السلطة التقديرية المخولة له ووفقاً لظروف وملابسات القضية وظروف الجاني وخطورته الإجرامية، كما يحكم القاضي أيضاً بالمصادرة كعقوبة تكميلية.

٢) قصد الحصول على أموال الغير أو خدمات: عاقب القانون هذه الحالة بعقوبة الحبس مدة لا تقل عن ستة أشهر وبالغرامة التي لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، إذا كان قصد الجاني من استعمال بيانات وأرقام البطاقات البنكية في الحصول على أموال للغير أو خدمات تتيحها هذه البطاقات، ولو لم يحصل بالفعل على هذه الموال أو الخدمات، ومن ثم فالقاضي مخير بين الحكم بالحبس والغرامة معاً، أو الحكم بالحبس أو بالغرامة فقط، في ضوء السلطة التقديرية المخولة له ووفقاً لظروف وملابسات القضية وظروف الجاني وخطورته الإجرامية، ونلاحظ أن المشرع قد شدد العقوبة في هذه الحالة من خلال مضاعفة الحد الأقصى لعقوبة الحبس، كما رفع حد الغرامة من (٣٠-٥٠) ألف جنيه إلى (٥٠-١٠٠) ألف جنيه، بالإضافة إلى الحكم بالمصادرة.

٣) تحقق استيلاء الجاني لنفسه أو غيره على مال الغير أو خدمات متاحة له: عاقب القانون هذه الحالة بعقوبة الحبس مدة لا تقل عن سنة، والغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز مائتين ألف جنيه، أو إحدى هاتين العقوبتين، والعقوبة المقررة أيضاً في هذه الحالة أكثر شدة من الحالتين السابقتين، فالمشرع تدرج في العقوبة بحسب المرحلة التي وصلت لها الجريمة، فإذا

اقتصر الأمر على التوصل إلى البيانات أو الأرقام الخاصة بالبطاقات البنكية، فتكون العقوبة المقررة هي العقوبة المقررة في الفقرة الأولى، فإذا كان القصد من استخدام هذه البيانات أو الأرقام الحصول على أموال أو خدمات من الغير، كانت العقوبة المقررة هي الواردة بالفقرة الثانية، فإذا تحصل بالفعل على هذه الأموال أو الخدمات عوقب بالعقوبة المقررة في الفقرة الثالثة، والقاضي كما سبق أن أشرنا مخير بين الجمع بين الحبس والغرامة أو الحكم بأيهما وفقاً لسلطته التقديرية في اختيار العقوبة المناسبة للمحكوم عليه في ضوء ظروف الجريمة وخطورة الجاني، ويجوز للقاضي الحكم بوقف تنفيذ العقوبة وفقاً للمادة ٥٥ عقوبات، كما يحكم بالمصادرة.

المطلب الثاني

الجرائم المتعلقة باصطناع المواقع والحسابات الخاصة والبريد الإلكتروني

نص التجريم: تنص المادة (٢٤) على الجرائم المتعلقة باصطناع المواقع والحسابات الخاصة والبريد الإلكتروني[1]، حيث تقضي المادة المذكورة بأنه:"*يُعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز ثلاثون ألف جنيه أو بإحدى هاتين العقوبتين، كل من اصطنع بريداً إلكترونياً أو موقعاً أو حساباً خاصاً ونسبه زوراً إلى شخص طبيعي أو اعتباري. فإذا استخدم الجاني البريد*

[1] كان المشروع المقدم من الحكومة ينص على تسمية المادة بالجرائم المتعلقة بالبريد الإلكتروني، وقد تم تعديل عنوان المادة خلال مناقشات لجنة الاتصالات بمجلس النواب، لتصبح على النحو الحالي، لتتسع لتشمل جرائم اصطناع المواقع والحسابات الخاصة والبريد الإلكتروني، بعد أن كانت التسمية الأولية تقتصر على الجرائم المتعلقة بالبريد الإلكتروني فحسب.

أو الموقع أو الحساب الخاص المصطنع في أمر يسئ إلى من نُسب إليه، تكون العقوبة الحبس الذي لا تقل مدته عن سنة، والغرامة التي لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين. وإذا وقعت الجريمة على أحد الأشخاص الاعتبارية العامة، تكون العقوبة السجن، والغرامة التي لا تقل عن مائة ألف جنيه، ولا تزيد عن ثلاثمائة ألف جنيه".

العلة من التجريم: ترجع العلة من تجريم هذا الفعل لمواجهة عمليات الغش والخداع الإلكتروني، من خلال اصطناع حسابات أو مواقع أو بريد إلكتروني غير حقيقي.

محل الجريمة: حدد المشرع محل جريمة الاصطناع في البريد الإلكتروني والمواقع الإلكترونية والحسابات الخاصة، وذلك على النحو السابق الإشارة إليه سابقاً. وكان القضاء المصري- قبل إصدار القانون- يعتبر البريد الإلكتروني والحسابات الخاصة من قبيل المحررات الإلكترونية، حيث سبق وأن قضت محكمة النقض بأن إنشاء حساب وهمي على موقع الفيسبوك بشبكة المعلومات الدولية على غرار الحسابات الصحيحة ونسبته زوراً للمجني عليها وإثبات بيانات وصور به على خلاف الحقيقة ما يشكل تزويراً في محرر إلكتروني[١]، بينما سبق لمحكمة القاهرة الاقتصادية أن قضت بأن البريد الإلكتروني يعد من قبيل المحررات الإلكترونية وفقاً لأحكام المواد ١، ١٥، ١٦ من القانون رقم ١٥ لسنة ٢٠٠٤ بشأن التوقيع الإلكتروني، وأن ذلك البريد مستوفي للشرائط اللازمة لتحقق الشروط اللازمة لحجية المحررات الإلكترونية في الإثبات وفقاً للمادة ٨ من اللائحة التنفيذية للقانون المشار إليه سلفاً[٢].

---

[١] انظر: الطعن رقم (١٥٤٢) لسنة ٨٢ ق، جلسة ٢٠١٣/٧/٣، مشار إليه المستشار د.محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٢٤٣.

[٢] انظر: حكم محكمة القاهرة الاقتصادية، جلسة ٢٠١٥/١/٣١، الدعوى رقم (٤١) لسنة ٢٠١٣، مشار إليه المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٢٤٨.

الركن المادي: يتحقق الركن المادي في هذه الجريمة، من خلال العنصرين التاليين:-

الاصطناع: وهو إنشاء شيء غير موجود، أو إنشاءه من العدم، ومحل هذا الإنشاء يكون موقع إلكتروني أو حساب خاص، بريد إلكتروني، وقد يقوم الجاني بهذا الإنشاء أو الاستحداث باستخدام بيانات تخصه أو تخص غيره، سواء أكانت هذه البيانات حقيقية أو وهمية.

نسبة الشيء المصطنع إلى الغير: لا تقوم الجريمة بمجرد اصطناع البريد الإلكتروني أو الموقع أو الحساب الخاص، وإنما يتطلب القانون أن يقوم الجاني بإسناد ذلك الشيء المصطنع إلى الغير، ويستوي لدى القانون أن يكون هذا الغير شخصاً طبيعياً أم اعتبارياً.

الإساءة للغير: تطلب القانون استخدام الجاني للبريد الإلكتروني أو الموقع أو الحساب الخاص المصطنع في الإساءة إلى الغير، سواء أكان هذا الغير شخصاً طبيعياً، أو أحد الأشخاص الاعتبارية العامة، وتتحقق الإساءة من خلال الإضرار بالمجني عليه، سواء أكان الضرر مادياً أم معنوياً، وقد شدد المشرع العقاب في الحالة الأخيرة بالنظر لما في ذلك من مساس بسمعة الدولة وأجهزتها.

وكانت إحدى المحاكم قد أدانت متهمين لقيامهم باصطناع بريداً إلكترونياً ونسبته زوراً إلى المجني عليه واستخدامه بغية الإضرار به، من خلال إرسال رسائل إلكترونية لأحدى الشركات الأجنبية لتحويل مبلغ مالي من الصفقة التي أبرمها المجني عليه مع هذه الشركة، وهو ما اعتبرته المحكمة ما شكل جريمة التزوير في المحررات الإلكترونية [1].

---

[1] انظر حكم محكمة جنح القاهرة الاقتصادية، جلسة ٢٠١٣/١١/١١، الدعوى رقم (٨٤٤) لسنة ٢٠١٣ جنح القاهرة الاقتصادية، مشار إليها المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٦٦٤.

ويتفق الباحث مع الرأي[١] الذي يذهب إلى أن هذا النهج القضائي كان بغرض بسط الحماية الجنائية على مثل هذه الجرائم، التي لم تكن مجرمة في ذلك الحين، حيث توسعت المحاكم في تطبيق أحكام القانون رقم ١٥ لسنة ٢٠٠٤ بشأن تنظيم التوقيع الإلكتروني، بالنظر إلى المدلول الواسع الذي أخذ به المشرع المصري في تعريف المحرر الإلكتروني بحسبانه مفهوم أوسع وأشمل من التوقيع الإلكتروني، حيث تنص المادة (٢٣) من قانون التوقيع الإلكتروني على أنه:"مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من :.... (ب) أتلف أو عيَّب توقيعاً أو وسيطاً أو محرراً إلكترونياً، أو زور شيئاً من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر".

وقد أيدت محكمة النقض هذا الاتجاه القضائي والمتمثل في اعتبار كل من البريد الإلكتروني والموقع الإلكترونية والحساب الخاص من قبيل الوسائط الإلكترونية المشار إليها في قانون تنظيم التوقيع الإلكتروني رقم ١٥ لسنة ٢٠٠٤، بأن قضت في أحد أحكامها الحديثة بأنه:" لما كان ما تقدم، فإنه يكون قد استقر في يقين هذه المحكمة أن المتهم: ارتكب تزويراً في محرر إلكتروني وكان ذلك بطريق الاصطناع بأن اصطنع حساباً على موقع الفيسبوك بشبكة المعلومات الدولية على غرار الحسابات والصفحات الصحيحة ونسبه زوراً للمجني عليها... وأثبت به بيانات وصور على خلاف الحقيقة للمجني عليها سالفة الذكر وذلك على النحو المبين بالتحقيقات"[٢].

---

[١] المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٦٦٤.

[٢] انظر الطعن الجنائي رقم (١٥٤٢) لسنة ٨٢ ق، جلسة ٢٠١٣/٧/٣، مشار إليها المستشار د. محمد سمير: الموضع السابق.

الركن المعنوي: هذه الجريمة من الجرائم العمدية التي يتحقق فيها الركن المعنوي بتوافر القصد الجنائي العام بعنصريه العلم والإرادة، بأن يعلم الجاني بأنه اصطنع بريداً أو حساباً أو موقعاً خاصاً ونسبته على غير الحقيقة للغير بغرض الإساءة إليه، وأن تتجه إرادته إلى تحقيق ذلك.

تبرز الإشارة إلى اختلاف الفقه الجنائي بشأن طبيعة القصد الجنائي في جريمة التزوير في المحررات الإلكترونية بين اتجاه أول[١] يراه قصداً عاماً بالنظر إلى أن عبارة النص –على غرار النص العام في قانون العقوبات- خلت مما يفيد تطلب القصد الخاص، ومن ثم تصبح الجريمة تامة ولو لم يرد الجاني استعمال المحرر المزور فيما بعد، بينما يذهب جانب آخر[٢] إلى إنه يجب لقيام الجريمة توافر القصد الخاص الذي ينهض على اتجاه الجاني إلى إلحاق الضرر بصاحب التوقيع الإلكتروني أو الوسيط أو المحرر، وأنه إذا انتفى القصد الخاص انتفت الجريمة لتخلف أحد أركانها.

ويرى الباحث أن هذه الجريمة تقوم بالقصد الجنائي العام دون الخاص، وأن تحقق القصد الخاص المتمثل في قصد الإساءة للغير يتحقق به التشديد في العقاب الذي قرره المشرع، فتقوم الجريمة بالسلوك المجرد، فإذا تحقق الضرر للمجني عليه شدد الشارع العقاب على الجاني على النحو التالي ذكره لاحقاً.

ومتى توافر للقصد الجنائي عنصراه، فلا عبرة بعد ذلك بالباعث على الجريمة، فقد يكون شريفاً أو غير ذلك، فالباعث ليس عنصراً من عناصر القصد الجنائي، ولا

---

[١] د. أسامة حسنين عبيد: دروس في الجرائم المضرة بالمصلحة العامة، دار النهضة العربية، القاهرة، ط١، ٢٠٠٦، ص٢٢٥؛ المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٦٦٥.

[٢] المستشار د. محمد الشهاوي: شرح قانون التوقيع الإلكتروني رقم ١٥ لسنة ٢٠٠٤- دراسة مقارنة، دار النهضة العربية، القاهرة، ط١، ٢٠١٠، ص١٨٨.

يمكن أن يؤثر على قيام الجريمة، وإنما كل تأثيره في أنه قد يكون محل تقدير لدى المحكمة عند الحكم بالعقوبة[١].

العقوبة: ميز القانون في العقوبة بين الحالات الثلاث التالية:-

١) السلوك المجرد: عاقب القانون هذه الحالة بعقوبة الحبس مدة لا تقل عن ثلاثة أشهر وبالغرامة التي لا تقل عن عشرة آلاف جنيه ولا تجاوز ثلاثين ألفا أو إحداهما[٢]، ومن ثم يجوز للقاضي أن يحكم بعقوبة الحبس فقط أو بعقوبة الغرامة فقط بوقف التنفيذ إعمالاً للمادة ٥٥ عقوبات.

٢) تحقق ضرر- الإساءة للغير: شدد القانون العقوبة في حال وقوع ضرر على الغير من الأشخاص الطبيعيين أو من الأشخاص الاعتبارية الخاصة، ففي هذه الحالة تكون العقوبة الحبس مدة لا تقل عن سنة وغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه أو إحداهما، ويجوز للقاضي في هذه الحالة كذلك أن يحكم بوقف التنفيذ إعمالاً للمادة ٥٥ عقوبات.

٣) صفة المجني عليه "أحد الأشخاص الاعتبارية العامة": كما غلظ المشرع العقوبة في حال وقوع الإساءة على أحد الأشخاص الاعتبارية العامة، حيث عاقب الجاني هذه الحالة بعقوبة السجن وغرامة لا تقل عن مائة ألف جنيه ولا تزيد على ثلاثمائة ألف جنيه، بالنظر لما في ذلك من مساس بسمعة الدولة وأجهزتها العامة، ويجوز للقاضي النزول بالعقوبة إلى الحبس الذي لا تقل مدته عن ثلاثة أشهر، إعمالاً للمادة ١٧ عقوبات.

---

[١] المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٦٦٥.

[٢] تبرز الإشارة إلى أن أحد أعضاء البرلمان قد طالب بجعل توقيع الحبس والغرامة في هذه الجريمة وجوبياً وليس على سبيل الاختيار، بالنظر إلى أن الشخص الطبيعي هو الذي يمس أكثر وخصوصيته تنتهك وتنسب إليه أفعال أو أقوال أو موقع أو بريد إلكتروني غير خاص به، وأن هذه الحالة منتشرة أكثر، إلا أن هذا المقترح لم يوافق عليه. انظر: مضبطة مجلس النواب المصري، الجلسة السادسة والخمسين، المعقودة في ٢٠١٨/٥/١٤م، مرجع سابق، ص ص١٠٤، ١٠٥.

المبحث الثالث

الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتي غير المشروع

تقسيم: تضمن الفصل الثالث من القانون الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتي غير المشروع، وتشمل جرائم انتهاك الحياة الخاصة للغير وجريمة التشهير بالغير، وذلك في مطلبين على النحو التالي:-

المطلب الأول

جريمة انتهاك الحياة الخاصة للغير

نص التجريم: تنص المادة (٢٥) من القانون على أنه:" *يُعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعتدى على أي من المبادئ أو القيم الأسرية في المجتمع المصري أو انتهك حرمة الحياة الخاصة، أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقته، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخباراً أو صوراً وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة*"[(١)].

---

(١) تبرز الإشارة إلى أن المادة (٧٦) من قانون الاتصالات رقم (١٠) لسنة ٢٠٠٣ نصت على معاقبة كل من تعمد إزعاج أو مضايقة الغير بإساءة استعمال أجهزة الاتصالات بعقوبة الحبس وبغرامة لا تقل عن خمسمائة جنيه ولا تجاوز عشرين ألف جنيه أو بإحدى هاتين العقوبتين، ومن ثم يمتد هذا =

وتبرز الإشارة إلى انتهاج المشرع المصري لتجريم انتهاك حرمة الحياة الخاصة وإغراق البريد الإلكتروني للمجني عليه بالرسائل والاعتداء على المبادئ والقيم الأسرية في نص واحد على خلاف نهج العديد من التشريعات المقارنة التي عملت على إفراد نص خاص بكل جريمة على حدة، وهو نهج كان من الأولى بالمشرع المصري الأخذ به، لتمايز كل صورة إجرامية عن النموذج القانوني للجريمة الأخرى.

العلة من التجريم: تتمثل علة التجريم في حرص المشرع على مايلي:-

أ- توفير الحماية الجنائية لخصوصية الأفراد من انتهاكات الغير.

ب- المحافظة على كيان الأسرة وعلى المبادئ التي تحكمها والقيم التي تخضع لها والأخلاق المتعارف عليها[1].

ج- الحد من تأثيرات شبكة الإنترنت ووسائل تقنية المعلومات على المجتمع وعلى الأسرة التي هي إحدى مكوناته الأساسية.

=

النص لتجريم أفعال السب والتهديد والتشهير ونشر الصور عبر الانترنت، كما تنص المادة (٧٣) من القانون ذاته على تجريم أفعال المساس بسرية رسائل الاتصالات المتمثلة في الإذاعة أو النشر أو التسجيل لمضمون رسالة الاتصالات، أو إخفاء أو تغيير أو تحوير رسالة الاتصالات، أو الامتناع عن إرسالها، أو الإفشاء لأية معلومات خاصة بمستخدمي شبكات الاتصالات.

ومن التشريعات المقارنة التي حرصت على تجريم انتهاك الحياة الخاصة للغير التشريع الفرنسي والإماراتي، ففي التشريع الفرنسي تعاقب المادة ٢٢٦-٢/١ عقوبات فرنسي على فعل تثبيت أو تسجيل أو نقل صورة شخص موجود في مكان خاص، وذلك دون موافقته، كما يجرم التشريع الإماراتي هذا السلوك (م٢١). انظر: د. جميل عبد الباقي الصغير: الإنترنت والقانون الجنائي، مرجع سابق، ص٢٤.

[1] ومن الجدير بالذكر أن الدستور المصري المعدل لعام ٢٠١٤ قد نص في مادته العاشرة على أن: "الأسرة أساس المجتمع، قوامها الدين والأخلاق والوطنية، وتحرص الدولة على تماسكها واستقرارها وترسيخ قيمها".

د- احترام حرمة الحياة الخاصة والعائلية[١].

محل الجريمة: يتمثل محل الجريمة أو الموضوع المادي لها في المبادئ والقيم الأسرية، ويقصد بها كفالة كرامة الأسرة وأعضائها، وحرمة الحياة الخاصة أو العائلية للأفراد، ويقصد بها صيانة الحياة الشخصية والعائلية للفرد بعيداً عن الانكشاف أو المفاجأة من الآخرين بغير رضاه، أو هي أمن الشخص على عوراته وحرماته هو وأسرته، التي يحرص على أن تكون بعيدة عن كافة أشكال وصور تدخل الغير[٢].

الركن المادي: يتكون الركن المادي للجريمة من عدة صور للسلوك الإجرامي، أفردها المشرع على النحو التالي:-

أ) الاعتداء على المبادئ أو القيم الأسرية في المجتمع المصري[٣]: حرص المشرع الجنائية على حماية المبادئ والقيم الأسرية التي يقوم عليها المجتمع، والتي يتعين احترامها ومراعاتها وعدم الخروج عليها أو مخالفتها للحفاظ على كيانه واستقراره، بالنظر إلى خطورة الاعتداء على هذه المبادئ والقيم وتداعيات الخروج عليها في هدم هذا المجتمع، كالزواج الشرعي كأساس لتكوين الأسرة، والإنجاب في إطار هذا الزواج الشرعي، وحماية القيم الأخلاقية والإنسانية والاجتماعية المتعارف عليها في المجتمع، ومن ثم فإن السلوكيات والأنشطة التي نجمت عن استخدام شبكة الانترنت، ومن أبرزها الدعوة للعلاقات الجنسية خارج إطار الزواج، والعلاقات المحرمة كزنا المحارم، وعرض الصور ومقاطع الفيديو الإباحية، وغرف الدردشة التي

---

[١] د. حسنى الجندي: التشريعات الجنائية الخاصة، مرجع سابق، ص٢٠١، د. مدحت رمضان: جرائم الاعتداء على الأشخاص والإنترنت، القاهرة، دار النهضة العربية، ٢٠٠٠، ص١٠١ ومابعدها.

[٢] د. حسنى الجندي: التشريعات الجنائية الخاصة، مرجع سابق، ص٢٠٢.

[٣] ومن التشريعات العربية التي جرمت الاعتداء على القيم والمبادئ الاجتماعية التشريع القطري (م٨) وكان التشريع الإماراتي ينص على تجريمه قبل تعديله.

تتناول حوارات عن الجنس خارج الزواج، واستخدام شبكة الإنترنت في نشر أو إذاعة أنباء تسيئ إلى الأسرة أو أحد أفرادها[١]، أو تدعو إلى تبادل الزوجات.

ب) انتهاك حرمة الحياة الخاصة:وهو ما يتحقق من خلال نشر معلومات أو أخبار أو صور تمس خصوصية الغير وبدون موافقته، وهو ما أشار إليه المشرع صراحة، يستوي لدى القانون أن تكون هذه الأخبار أو المعلومات تخص الشخص ذاته أو أحد أفراد عائلته، بالنظر إلى أن مدلول الحياة الخاصة للشخص يتسع ليشمل الحياة الخاصة أو العائلية للفرد، ومن ثم يشمل ذلك أفراد أسرته وعائلته والمقربين له، كما يستوي لدى القانون أن تكون هذه المعلومات المنشورة عن المجني عليه صحيحة أم غير صحيحة، والأمثلة على انتهاك الحرمة الشخصية للفرد عبر استخدام تقنية المعلومات متعددة، نذكر منها على سبيل المثال: نشر أخبار عبر الإنترنت حول شخص معين أو أسرة بعينها، تفتح مسكنها لممارسة الرذائل لمن يرغب في ذلك، أو نشر بعض الصور التي تتعلق بتواجد الشخص هو وعائلته في أحد الأماكن الخاصة، أو نشر أخباراً حول شخص عن اتهامه في قضية ما، أو تقديمه إلى المحاكمة عنها، أو إلصاق إحدى التهم به، أو بكونه متهرباً من الضرائب، أو أشهر إفلاسه، أو إفشاء أسرار تتعلق بأحد الأفراد حول حياته الشخصية، أو العائلية، أو المالية، أو الصحية، أو وضع كاميرات داخلية تقوم بتعرية الفرد والتطلع إلى أسراره، أو اختراق الملفات الشخصية لأحد الأشخاص والإطلاع عليها والسماح للغير بالإطلاع عليها بدون إذن صاحبها[٢].

---

[١] المرجع السابق، ص٢٠٠.

[٢] المرجع السابق، ص٢٠٣.

تساؤل: عن مدى تحقق جريمة انتهاك حرمة الحياة الخاصة بمجرد النشر؟ ذهب جانب مهم من الفقه الجنائي[١]-وبحق- إلى أن الجريمة تقع بمجرد النشر على شبكة الانترنت دون أن يتطلب ذلك تلقي أو استقبال لمثل هذه الصور أو الأخبار عبر شبكة الإنترنت، لأن ذلك لا يمنع من وجود المتلقي بمجرد الإطلاع على هذه الأخبار أو الصور من خلال الشبكة المعلوماتية أو باستخدام إحدى وسائل تقنية المعلومات.

ويشترط في النشر أن يكون بغير رضاء المجني عليه، أو إذنه حتى تتحقق الجريمة، ولا تقع الجريمة إذا كان الشخص في مكان عام يمكن رؤيته فيه، أو يسمح للغير بالتقاط صور معه أو عنه، وقد تقوم الجريمة عن طريق عمل مونتاج (تركيب) لصورة شخص بدون رضائه، بشكل يمس حرمة الحياة الخاصة أو العائلية له، كأن تكون الصورة التي تم تركيبها لأحد الأشخاص تظهره بشكل يسئ له[٢]، كما لا تقوم الجريمة إذا تعلق الأمر بنشر كتابة أو رسوم تتعلق بالشخص، على الرغم من أن هذه الأفعال قد تشكل جرائم أخرى كالقذف أو السب في علانية والتشهير[٣].

تساؤل: حول مدى انتهاك الحياة الخاصة للشخص حال تصويره بعد وفاته؟ ذهب جانب مهم من الفقه الجنائي[٤]-وبحق- إلى أن الأصل أن يتعلق انتهاك حرمة الحياة الخاصة للشخص وهو على قيد الحياة، غير أن ذلك لا يمنع من امتداد الحماية له بعد وفاته، كأن يصور وهو في مرض الموت، لأن ذلك وإن كان لا يمس حرمة الحياة الخاصة للمتوفي، فهو يمس حرمة الحياة العائلية للشخص ذاته.

---

[١] الموضع السابق.

[٢] د. حسنى الجندي: المرجع السابق، ص٢٠٤؛ د. مدحت رمضان: المرجع السابق، ص١٠٦ ومابعدها.

[٣] د. حسنى الجندي: الموضع السابق.

[٤] الموضع السابق.

ج- إرسال رسائل إلكترونية بكثافة للغير[١]: وهو ما يعرف بالرسائل الإلكترونية الطفيلية Spam، ويتحقق ذلك من خلال قيام الجاني بإرسال العديد من الرسائل الإلكترونية للبريد الإلكتروني لشخص معين دون موافقته[٢]، وبشكل مكثف، وهو ما يتحقق به إزعاج المجني عليه[٣]، من خلال استقباله لعدد من رسائل البريد الإلكتروني بشكل متكرر غير مرغوب فيه، ويخضع تقدير ذلك للسلطة التقديرية للقاضي، ويرى الباحث أن عنصر كثافة الرسائل يتحقق بعدد ثلاثة رسائل أو أكثر، وهو الحد الأدنى في الجمع.

ويقصد بالإزعاج كل ما يقلق راحة الشخص وطمأنينته أو ما يعكر صفوه أو يصيبه بالضجر، ولا يشترط في الإزعاج أن يتضمن قذفاً أو سباً أو إهانة، وإنما هو أقل مرتبة من ذلك، فيتحقق الإزعاج أو المضايقة بمجرد إرسال رسائل على البريد الإلكتروني تتضمن أي أمر يسبب له المضايقة، أو تعكير صفوه[٤].

---

(١) الموضع السابق.

(٢) ومن التشريعات الجنائية التي نصت على تجريم إغراق البريد الإلكتروني بالرسائل التشريع الإماراتي (م١٠).

(٣) غالباً ما تعرف رسائل البريد الإلكتروني الطفيلي بأنها إرسال كميات كبيرة من الرسائل غير المرغوب فيها، وقد عرفت المادة (١٩) من مشروع القانون النموذجي للكوميسا إرسال البريد الإلكتروني الطفيلي بأنه:" أي شخص يرسل أي معلومات إلكترونية غير مرغوب فيها إلى شخص آخر بغرض التجارة أو التعامل غير المشروع أو أي أنشطة أخرى غير قانونية"، وتشير التقديرات الدولية إلى أن هذه الرسائل الإلكترونية الطفيلية تشكل حوالي ٧٠% من إجمالي حركة مرور البريد الإلكتروني عبر الإنترنت خلال عام ٢٠١٢، وتتسبب هذه الرسائل الإلكترونية الطفيلية في استياء مستخدمي الإنترنت واستهلاك قدرة الخوادم والبنية التحتية للشبكات، كما إنها تعد نقطة دخول لانتشار البرمجيات الخبيثة، وعمليات انتحال الصفة للحصول على كلمات سر الدخول والمعلومات المالية.انظر:دراسة مكتب الأمم المتحدة،مرجع سابق،ص ص١٣٥، ١٣٦.

(٤) المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٥٢٢؛ وقارن: الطعن رقم (١١٩٤ لسنة ٨٠ق، جلسة ٢٠١١/٣/١٤؛ نقض ١٩٩٥/١/١، مجموعة أحكام محكمة النقض، س٤٦، ص٢٤.

ولا يلزم أن تثبت النيابة العامة أن سلوك الجاني ألحق المضايقة أو الإزعاج للمجني عليه، وإنما يكفي أن يكون نشاط الجاني من شأنه أن يحقق الإزعاج أو المضايقة طبقاً للمجرى العادي للأمور[١].

وتبرز الإشارة إلى أن محكمة جنح مستأنف القاهرة الاقتصادية قد قررت أن المراسلات التي ترسل عبر البريد الإلكتروني لا تتسم بالعلانية، حيث قضت بأن إرسال رسالة من البريد الإلكتروني إلى بريد إلكتروني آخر لا يتحقق به ركن العلانية مما ينتفي معه جريمة القذف[٢]، على اعتبار أن ركن العلانية في جريمة القذف ركن جوهري، ولا يوجد قذف غير علني كالسب[٣].

د- منح البيانات الشخصية للغير إلى نظام أو موقع إلكتروني: ويتحقق ذلك من خلال قيام الجاني باستخدام البيانات الشخصية للغير وتقديمها للمواقع الإلكترونية كمواقع ترويج السلع أو الخدمات، وذلك دون موافقته.

الركن المعنوي: هذه الجريمة من الجرائم العمدية التي تتحقق بتوافر القصد الجنائي العام بعنصريه العلم والإرادة، وذلك على النحو التالي:-

أ) العلم: ينبغي أن يعلم الجاني أن من شأن فعله الاعتداء على المبادئ أو القيم الأسرية، أو المساس بحرمة الحياة الخاصة للآخرين، بأن يعلم أن الصور أو الأخبار التي ينشرها عبر شبكة الإنترنت تمس حرمة الحياة الخاصة أو العائلية للمجني عليه، فإذا كان يعتقد أن ما يقوم بنشره هو من الأمور العامة التي تتعلق بالمجني عليه، والتي

---

[١] المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٥٢٣.

[٢] انظر: حكم محكمة جنح مستأنف القاهرة الاقتصادية، جلسة ٢٠١٠/١١/٢٢، الدعوى رقم ٥٩١ لسنة ٢٠١٠ جنح مستأنف، والمقيدة برقم ١٠٥٩ لسنة ٢٠١٠ جنح القاهرة الاقتصادية.

[٣] المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٢٥٢.

يعلمها الكثيرون، وليس محظورة النشر، فإن ذلك يترتب عليه انتفاء العلم اللازم لقيام القصد الجنائي، كما ينبغي أن يعلم الجاني أن من شأن فعله إرسال العديد من الرسائل الإلكترونية على البريد الإلكتروني للغير.

ب) الإرادة: ينبغي أن تتجه إرادته إلى ارتكاب فعل الاعتداء على المبادئ أو القيم الأسرية للمجني عليه، أو إلى القيام بنشر الصور أو الأخبار التي تمس حرمة الحياة الخاصة أو العائلية للمجني عليه، وينتفي هذا العنصر إذا كان الجاني يجهل أن ما يقوم بنشره من صور أو أخبار يتعلق بحرمة الحياة الخاصة للمجني عليه، أو أن نشره لهذه الأمور لم يكن بقصد الإساءة إلى هذا المجني عليه، كما ينتفي عنصر الإرادة كذلك، إذا كان الشخص قد نسى جهاز التليفون المحمول الخاص به مفتوحاً على شاشة الكاميرا، مما أدى إلى التقاط صورة لأحد الأشخاص[١].

ويذهب جانب من الفقه[٢] إلى أن جريمة إغراق البريد الإلكتروني للمجني عليه بالرسائل لا تنهض بتوافر الخطأ غير العمدي، ولو كان جسيماً، كما لو أرسل المجني عليه رسالة أو أكثر لآخر على سبيل الخطأ مما شكل إزعاجاً له، كما أنه لا عبرة بالبواعث على هذه الجريمة فقد يكون الحقد أو الانتقام أو مجرد التسلية، فالباعث لا يعد من عناصر القصد الجنائي.

العقوبة: عاقب القانون على هذه الجريمة بعقوبة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف أو بإحدى العقوبتين، ويجوز للقاضي أن يحكم بوقف التنفيذ، إعمالاً للمادة ٥٥ عقوبات.وتبرز الإشارة إلى أن سلوك الجاني بإرسال رسائل إلكترونية بكثافة للغير قد يشكل جريمة تعمد إزعاج

---

[١] د. حسنى الجندي: المرجع السابق، ص٢٠٥.

[٢] المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٥٣١.

الغير بإساءة استعمال أجهزة الاتصالات المعاقب عليها بالمادة ٧٦ من قانون الاتصالات رقم ١٠ لسنة ٢٠٠٣، وهو ما يشكل تعدداً معنوياً للجرائم طبقاً لأحكام المادة ٢/٣٢ من قانون العقوبات، والتي توجب تطبيق العقوبة الأشد للجريمتين[١]، ومن ثم تطبق في هذه الحالة العقوبة الخاصة بجريمة انتهاك حرمة الحياة الخاصة للغير الواردة بقانون مكافحة جرائم تقنية المعلومات[٢].

المطلب الثاني

جريمة الإساءة للغير

نص التجريم: تنص المادة (٢٦) من القانون على أنه:" *يُعاقب بالحبس مدة لا تقل عن سنتين ولا تجاوز خمس سنوات، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز ثلاثمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها بمحتوي منافٍ للآداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه*".

---

[١] قارن: حكم محكمة جنح القاهرة الاقتصادية، جلسة ٢٠١١/٤/٢٩، الدعوى رقم (١٧٠٨) لسنة ٢٠١١ جنح اقتصادي، مشار إليه المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٥٢٦.

[٢] تقضي المادة (٧٦) من القانون ١٠ لسنة ٢٠٠٣ في شأن تنظيم الاتصالات بأنه:" مع عدم الإخلال بالحق في التعويض المناسب، يعاقب بالحبس وبغرامة لا تقل عن خمسمائة جنيه ولا تجاوز عشرين ألف جنيه أو بإحدى هاتين العقوبتين كل من: ١- استخدام أو ساعد على استخدام وسائل غير مشروعة لإجراء اتصالات٢- تعمد إزعاج أو مضايقة غيره بإساءة استعمال أجهزة الاتصالات" وقد انتقد البعض صياغة هذه المادة لإدراج عبارة:"مع عدم الإخلال بالحق في التعويض المناسب" بالنظر إلى هذه العبارة قد صيغت على سبيل التزيد الذي ينبغي أن ينزه عن المشرع بحسبانها مجرد تطبيق للقواعد العامة. انظر: المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٥٣٣.

العلة من التجريم: ترجع العلة من تجريم هذا الفعل في حماية حق الإنسان في حفظ اعتباره وشرفه ممن يحاولون إهانته وتحقيره والتشهير بسمعته.

الركن المادي- الاستخدام: يتحقق الركن المادي في هذه الجريمة بأي فعل من شأنه تحقير المجني عليه والتشهير به، كأن يستخدم الجاني برامج أو تطبيقات كبرامج الفوتوشوب لمعالجة معطيات شخصية للغير لربطها بمحتوى منافٍ للآداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه، كأن تظهر المجني عليه في حالة أو وضع غير مقبول اجتماعياً، كإظهاره في أحد الملاهي الليلية مع أحد الساقطات أو غير ذلك من الأحوال التي تؤدي إلى تحقيره أمام غيره أو مسائلته القانونية إن صحت، ومن أبرز التطبيقات لهذه الجريمة قيام الجاني بتركيب صور للمجني عليه على صور مخلة بغرض الإساءة إليه وتحقيره أمام ذويه.

وسيلة ارتكاب الجريمة: أشار المشرع إلى تجريم استخدام البرامج والتقنية المعلوماتية للتشهير بالغير، وكان المشرع قد عرف البرنامج المعلوماتي -كما سبق أن أشرنا- بأنه:" *مجموعة الأوامر والتعليمات المعبر عنها بأية لغة أو رمز أو إشارة والتي تتخذ أي شكل من الأشكال، ويمكن استخدامها بطريق مباشر أو غير مباشر في حاسب آلي لأداء وظيفة أو تحقيق نتيجة، سواء كانت هذه الأوامر والتعليمات في لها الأصلي أو في أي شكل آخر تظهر فيه من خلال حاسب آلي، أو نظام معلوماتي*"، بينما عرف تقنية المعلومات بأنها:"أي وسيلة أو مجموعة وسائل مترابطة أو غير مترابطة تُستخدم لتخزين واسترجاع وترتيب وتنظيم ومعالجة وتطوير وتبادل المعلومات أو البيانات، ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة سلكياً أو لاسلكياً".

أن يكون من شأن استخدام الوسائل التقنية الإساءة للمجني عليه: تطلب القانون أن يكون استخدام البرامج والتقنيات من شأنه الإساءة إلى سمعة المجني عليه واعتباره، كأن تستخدم الوسائل التقنية في ربط معطياتها الشخصية بمحتوى مناف للآداب العامة،ومن أمثلة ارتكاب جرائم التشهير عبر شبكة الإنترنت قيام أحد الأشخاص بإنشاء بريدين إلكترونيين، وقيامه بتركيب صورة إحدى السيدات المجني عليها على فيلم إباحي مثلاً، ورفعه ذلك الفيلم الإباحي على البريد الإلكتروني الذي أنشأه، وقيامه بإرسال خطابات بريدية لأقاربها تتضمن عبارات سب وقذف وتشهير بالمجني عليها، وأنها ترغب في إقامة علاقات جنسية مع كل من يرغب في كونها ذات السيدة المتواجدة بالفيلم الممثل، مشيراً إلى كيفية مشاهدة الفيلم بإعطائه كلمة المرور الخاصة بالبريد الإلكتروني، الأمر الذي ترتب عليه الإضرار بالمجني عليها أدبياً ونفسياً[1]، ومن الأمثلة كذلك قيام الجاني بنشر مشاركات تتضمن عبارات تشهير وإساءة لسمعة المجني عليه واتهامه بأنه شريك في إحدى الجرائم، أو قيام الجاني باستخدام حساب على شبكات التواصل الاجتماعي لنشر مشاركات تتضمن عبارات سب وقذف وتشهير بحق المجني عليها، أو قيام الجاني بإنشاء حساب على شبكة التواصل الاجتماعي باسم وصورة المجني عليها ونشر رقم تليفونها المحمول مصحوب بعبارات تشهير في حقها، أو قيام الجاني بإرسال رسائل للمجني عليه وأخرى تحتوي على صور لهما تم تركيبها على صور إباحية وعبارات تهديد بنشرها.

تساؤل: هل يشترط وقوع الضرر لتحقق الجريمة؟ الواقع أن المشرع لم يشر إلى تطلب وقوع الضرر للمجني عليه لتحقق الجريمة، فالجريمة تقع بمجرد استعمال

---

[1] مشار إلى هذه القضية: د. محسن العبودي: المواجهة الأمنية لجرائم الإنترنت، ص٧، منشورة على شبكة الإنترنت على الموقع الإلكتروني: http://www.eastlaws.com/Uploads/Morafaat/153.pdf

الجاني لبرامج أو تقنيات المعلومات في معالجة المعطيات الشخصية للمجني عليه بشكل الذي تتحقق به الإساءة في حقه، ولو لم يستخدم هذه المعطيات أو لم يقم بنشرها على شبكة الإنترنت أو إرسالها عبر البريد الإلكتروني.

الركن المعنوي: هذه الجريمة من الجرائم العمدية التي يتحقق فيها الركن المعنوي بتوافر القصد الجنائي العام بعنصريه العلم والإرادة، وهو ما أشار إليه المشرع صراحة بالنص على أنه:" *كل من تعمد استعمال*"، ومن ثم ينبغي أن يعلم الجاني بأن من شأن استخدامه لوسائل التقنية الحديثة الإساءة والتحقير وتشويه سمعة المجني عليه، وأن تتجه إرادته إلى إحداث ذلك.

العقوبة: عاقب القانون على هذه الجريمة بعقوبة الحبس مدة لا تقل عن سنتين ولا تجاوز خمس سنوات والغرامة التي لا تقل عن مائة ألف ولا تجاوز ثلاثمائة ألف جنيه، أو بإحدى هاتين العقوبتين، ومن ثم يجوز للقاضي الحكم بالحبس فقط أو بالغرامة فقط أو بالعقوبتين معاً، ويلاحظ أن المشرع الجنائي قد خرج عن الحدود القانونية المقررة لعقوبة الحبس وهي ثلاث سنوات، لتصبح خمس سنوات، وقدر الغرامة المقررة بين حدين الحد الأدنى مائة ألف جنيه والحد الأقصى ثلاثمائة ألف جنيه.

المبحث الرابع

الجرائم المرتكبة من مدير الموقع

تقسيم: تضمن الفصل الرابع من القانون الجرائم المرتكبة من مدير الموقع، وتشمل جريمة إنشاء موقع أو حساب على شبكة معلوماتية بهدف ارتكاب أو تسهيل ارتكاب جريمة، وجريمة العبث في الأدلة الرقمية، وتجريم الخطأ غير العمدي لمقدم الخدمة في وقوع الجرائم المعلوماتية، وذلك في ثلاثة مطالب على النحو التالي:-

المطلب الأول

جريمة إنشاء موقع أو حساب على شبكة معلوماتية

بهدف ارتكاب أو تسهيل ارتكاب جريمة

نص التجريم: تنص المادة (٢٧) من القانون على أنه:"*في غير الأحوال المنصوص عليها في هذا القانون، يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن مائة ألف جنيه، ولا تزيد عن ثلاثمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أنشأ أو أدار أو استخدم موقعاً أو حساباً خاصاً على شبكة معلوماتية يهدف إلى ارتكاب أو تسهيل ارتكاب جريمة معاقب عليها قانوناً*"[1]، وتبرز الإشارة إلى أن

[1] تبرز الإشارة في هذا السياق إلى وجود بعض القوانين المصرية التي تناولت تجريم إنشاء المواقع الإلكترونية ونشر المعلومات بشأن ارتكاب الجرائم الترويج لها أو تسهيل ارتكابها، ومن أبرز هذه القوانين قانون مكافحة الإرهاب ٩٤ لـ٢٠١٥ الذي سبق قانون مكافحة جرائم تقنية المعلومات في تجريم إنشاء واستخدام المواقع الإلكترونية للترويج للإرهاب والأفكار الداعية له أو لبث ما يهدف إلى تضليل السلطات الأمنية أو التأثير في سير العدالة(م٢٩)، كما أشار قانون الطفل إلى استخدام شبكات المعلومات والانترنت لتحريض الأطفال على الانحراف أو استغلالهم في الدعارة والأعمال الإباحية (م١١٦ مكرراً أ/ فقرة٢).

=

المشرع قد نص على تجريم فعل "كل من أنشأ أو أدار.."، ومن ثم فهذه الجريمة يمكن أن ترتكب من أي شخص، على الرغم من أن المشرع قد أوردها ضمن الجرائم المرتكبة من مدير الموقع، ولكن المشرع في هذه الجريمة لم يتطلب صفة خاصة في فاعل الجريمة.

العلة من التجريم: تتمثل علة التجريم في مواجهة السلوك الإجرامي الضار المرتكب على شبكة الإنترنت، والمتمثل في استخدام المواقع الإلكترونية والحسابات الخاصة في ارتكاب الجرائم أو تسهيل ارتكابها، ومن ثم فإن هذا النص يشكل إطاراً لتجريم لاستخدام المعلوماتية أو المواقع الإلكترونية كوسيلة لارتكاب الجريمة أيا كانت صورتها.

محل الجريمة: حدد المشرع الجنائي محل الجريمة في المواقع الإلكترونية والحسابات الخاصة، وقد عرف القانون كل من الموقع الإلكتروني والحساب الخاص في القانون، حيث عرف الأول بأنه:" *مجال أو مكان افتراضي له عنوان محدد على شبكة معلوماتية، يهدف إلى إتاحة البيانات والمعلومات للعامة أو الخاصة*"، ومن ثم فالموقع

=

ومن ناحية أخرى، تجدر الإشارة إلى أن المشرع المصري قد خالف النهج الذي سارت عليه العديد من التشريعات العربية التي حرصت على تجريم إنشاء موقع أو حساب إلكتروني بهدف ارتكاب بعض صور الجرائم الخطيرة كالاتجار بالبشر والاتجار بالمخدرات والإرهاب، ومن أبرز هذه التشريعات التشريع الإماراتي التي نص على تجريمه إنشاء المواقع الإلكترونية لارتكاب عدد من الجرائم المحددة، وذلك في المواد أرقام (٢٣-٣٣).

وتبرز الإشارة إلى أن غالبية التشريعات العربية قد سايرت نهج الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي تنص -كما سبق أن أشرنا- على تجريم إنشاء موقع على شبكة معلوماتية أو إحدى وسائل تقنية المعلومات لأغراض الإرهاب أو تحويل الأموال غير المشروعة أو بقصد الاتجار بالمخدرات أو بالأشخاص والأعضاء البشرية أو بالأسلحة أو بالآثار والتحف الفنية (المواد أرقام ١٥-١٧).

هو مكان افتراضي على شبكة المعلومات يؤجر على الشبكة لشخص ما، ينشر عليه ما يريد من نصوص أو صور، أو ينشئ روابط معلوماتية مع المواقع الأخرى[1]،بينما يقصد بالثاني:"***مجموعة من المعلومات الخاصة بشخص طبيعي أو اعتباري، تخول له دون غيره الحق في الدخول على الخدمات المتاحة أو استخدامها من خلال موقع أو نظام معلوماتي***".

الركن المادي: يحقق الركن المادي في هذه الجريمة من عنصرين: الأول هو صور السلوك، والثاني هو الغرض من السلوك، وهو ما سوف نتناوله على النحو التالي:-

صور السلوك الإجرامي: يتحقق السلوك الإجرامي في هذه الجريمة بأفعال الإنشاء أو الإدارة أو الاستخدام، وهو ما سوف نتناوله على النحو التالي:-

أ) الإنشاء: يقصد بإنشاء المواقع أو الحسابات الخاصة تكوين الموقع وبثه عبر شبكة الانترنت وتزويده بالبيانات والمعلومات المطلوبة، وقد يستخدم الجاني في إنشاء المواقع برامج أو تطبيقات خاصة بذلك، تعني بوضع البيانات والمعلومات على الموقع الإلكتروني ورفعها على شبكة الانترنت، ومن التطبيقات لهذا الفعل قيام أحد الأشخاص بإنشاء حساب على شبكات التواصل الاجتماعي ونشر مشاركات للترويج لبيع المواد المخدرة، ومن مثال آخر إنشاء حساب لنشر مشاركات تحريضية ضد رموز الدولة ومؤسساتها، وكذلك قيام أحد الأشخاص بإنشاء مجموعة بتطبيق الواتس آب ينشر من خلالها أسئلة وإجابات امتحانات إحدى المراحل الدراسية أثناء أداء الطلاب الامتحانات بهدف الإخلال بمنظومة الامتحانات ونشر إجابات الامتحان بقصد مساعدة الطلب ة على الغش داخل اللجان.

---

[1] د. حسنى الجندي: التشريعات الجنائية الخاصة، مرجع سابق، ص٢٠٧.

ب) الإدارة: يقصد بالإدارة تنظيم عمل الموقع أو الحساب الخاص، فقد يتولى هذا الموقع الإلكتروني مدير الموقع يعرف بأنه:"كل شخص مسئول عن تنظيم أو إدارة أو متابعة أو الحفاظ على موقع أو أكثر على الشبكة المعلوماتية، بما فيها حقوق الوصول لمختلف المستخدمين على ذلك الموقع، أو تصميمه، أو توليد وتنظيم صفحاته أو محتواه، أو المسئول عنه".

ومن التطبيقات القضائية لهذا الفعل قيام أحد الأشخاص بإدارة إحدى الصفحات على شبكات التواصل الاجتماعي ونشر مشاركات تتضمن إدعائه بتزوير المستندات والوثائق والمحررات الرسمية لمن يطلب ذلك.

ومن التطبيقات القضائية كذلك إدانة أحد المديرين النشطاء المعروفين دولياً لأحد المواقع الإسلامية المتطرفة بالتحريض على جرائم العنف، لتورطه في توزيع معلومات تتعلق بمتفجرات وتوجيه نداء لارتكاب العنف، وكان المتهم المذكور قد قام بوضع عدداً من المنشورات التي تعبر عن ميوله للآراء المتطرفة، بالتزامن مع تشجيع الأعضاء الآخرين بإتباع عقيدته للاشتراك في ارتكاب أعمال جرائم عنف في أمريكا الشمالية ضد أهداف مثل أقسام الشرطة، ومكاتب البريد، والمعابد، والمنشآت العسكرية، ومرافق النقل، وقيامه من أجل دعم هذه الهجمات بنشر رابط إلكتروني لوثيقة مطولة تحتوي على خطوات تفصيلية عن تصنيع المتفجرات[1].

ج) الاستخدام: يقصد بالاستخدام استعمال الموقع أو الحساب الخاص في ارتكاب جريمة ما أو تسهيل جريمة ما، بأن يقوم الجاني بنشر معلومات على هذا الموقع أو الحساب بغرض ارتكاب أو تسهيل ارتكاب جريمة ما. وينبغي أن يكون

---

[1] انظر: دراسة مكتب الأمم المتحدة، مرجع سابق، ص١٦٤.

الاستخدام أو الإنشاء أو الإدارة بغرض ارتكاب جريمة جنائية أو تسهيل ارتكابها، ويستوي لدى القانون طبيعة الجريمة فقد تكون جناية أو جنحة أو مخالفة، بالنظر إلى عمومية النص، إلا أن الباحث يرى أنه كان ينبغي من المشرع أن يحدد هذه الجرائم لتكون جناية أو جنحة، مع استبعاد المخالفات بالنظر إلى بساطتها وقلة خطورتها الإجرامية.

الركن المعنوي: هذه الجريمة من الجرائم العمدية التي يتحقق فيها الركن المعنوي بتوافر القصد الجنائي العام بعنصريه العلم والإرادة، كما تتطلب هذه الجريمة توافر قصد جنائي خاص يتمثل في أن يكون إنشاء الموقع أو الحساب أو استخدامه بنية ارتكاب أو تسهيل ارتكاب جريمة معاقب عليها قانوناً.

العقوبة: عاقب القانون على هذه الجريمة بعقوبة الحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن مائة ألف جنيه ولا تزيد عن ثلاثمائة ألف جنيه أو بإحدى هاتين العقوبتين، ومن ثم يجوز للقاضي أن يقضي بالعقوبتين معاً أو بإحدى العقوبتين الحبس أو الغرامة، ومن ثم يجوز للقاضي الحكم بالحبس الذي لا تقل مدته عن سنتين ولا تزيد على ثلاث سنوات وهو الحد الأقصى للحبس، وأن يوقع الغرامة بين حدين الحد الأدنى مائة ألف جنيه والحد الأقصى ثلاثمائة ألف جنيه.

المطلب الثاني

جريمة العبث في الأدلة الرقمية

نص التجريم: تنص المادة (٢٨) من القانون على أنه:" ***يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين، كل مسئول عن إدارة موقع أو حساب خاص أو بريد نـي أو نظام معلوماتي إذا أخفى أو عبث بالأدلة الرقمية لإحدى الجرائم***

***المنصوص عليها في هذا القانون والتي وقعت على موقع أو حساب أو بريد إلكتروني بقصد إعاقة عمل الجهات الرسمية المختصة"*.**

العلة من التجريم: تتمثل علة التجريم في مجابهة كافة محاولات المسئولين عن إدارة المواقع الإلكترونية لتضليل العدالة من خلال العبث في أدلة الجريمة، في ضوء ما يشكله هذا السلوك من مساعدة لهم للهروب من المسائلة، فضلاً عما يمثله الدليل الرقمي من أهمية في عملية الإثبات الجنائي للجرائم المعلوماتية باعتباره الوسيلة الوحيدة والرئيسية لإثبات هذه الجرائم(١)، ومن ثم يشكل هذا العبث في الأدلة الرقمية تقويضاً لجهود رجال العدالة الجنائية وتضليلاً لهم في ضبط مثل هذه الجرائم الخطيرة والوصول إلى الحقيقة التي تتغياها العدالة الجنائية.

محل الجريمة: يتمثل محل الجريمة في الدليل الرقمي، وقد عرفه القانون بأنه:"*أي معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها، ويمكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة*"، ومن ثم يقصد بالدليل الرقمي أي أثر أو دليل يخلفه الجاني في النظام المعلوماتي أو شبكة المعلومات وتتصل بارتكاب الجريمة.

صفة الجاني: تطلب القانون في فاعل الجريمة أن يكون مسئولاً عن إدارة موقع أو حساب خاص أو بريد إلكتروني أو نظام معلوماتي، وكان القانون قد عرف مدير الموقع بأنه:"كل شخص مسئول عن تنظيم أو إدارة أو متابعة أو الحفاظ على

---

(١) عبد الناصر محمد محمود فرغلي وآخر: الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية- دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي الذي نظمته جامعة نايف العربية للعلوم الأمنية خلال الفترة (١٢-١٤/١١/٢٠٠٧)، الرياض، ص١١.

موقع أو أكثر على الشبكة المعلوماتية، بما فيها حقوق الوصول لمختلف المستخدمين على ذلك الموقع، أو تصميمه، أو توليد وتنظيم صفحاته أو محتواه، أو المسئول عنه".

الركن المادي: يتكون الركن المادي في هذه الجريمة من أفعال الإخفاء والعبث بالأدلة الرقمية وذلك على النحو التالي:-

أ) الإخفاء: يقصد بالإخفاء ستر الشيء عن أعين الناس وعدم إظهاره لهم، ويجب أن ينصب هذا الإخفاء على دليل رقمي يخص جريمة وقعت بالفعل، وهو ما تتحقق به جريمة إعاقة سير العدالة المنصوص عليها في غالبية التشريعات الجنائية، ويستوي لدى القانون الوسيلة المستخدمة في تحقيق الإخفاء، فقد تكون برنامج أو أية وسيلة تقنية، كما يستوي لدى القانون أن يكون هذا الدليل هو الدليل الوحيد في الدعوى، أم أنه أحد الأدلة المرتبطة بالدعوى، ومن ثم قد يتخذ فعل الإخفاء صورة مسح الدليل أو إلغاؤه.

ب) العبث بالأدلة الرقمية: يقصد بالعبث بالدليل الرقمي قيام الجاني بأي فعل إيجابي من شأنه تغيير طبيعة هذا الدليل أو عناصره، ومن ثم التشكيك في نسبته إلى الجاني بما تتحقق به كذلك إعاقة العدالة، ومن ثم قد يتخذ العبث صورة تعديل معطيات الدليل الرقمي، بالشكل الذي يغير من شكل الدليل أو طبيعته، أو موقعه، أو تعديل مساره، وتبرز الإشارة إلى أن المشرع قصر العبث على الأدلة الرقمية الناجمة عن إحدى الجرائم الواقعة على المواقع أو الحسابات الخاصة أو البريد الإلكتروني.

ويتحقق هذا العبث من خلال استخدام الجاني لأية تقنية كالبرمجيات أو التقنيات أو الأدوات التي من شأنها تعديل المعطيات والبيانات، أو تغيير الطبيعة المعنوية للدليل الرقمي، حيث يستوي لدى القانون الوسيلة التي يستخدمها الجاني في

تحقيق العبث بالدليل الرقمي، سواء أكانت هذه البرامج أو التقنيات قد استخدمت عبر شبكة معلوماتية أو باستخدام برمجيات خبيثة تقوم بتغيير أو تعديل أو محو المعلومات أو البيانات التي تشكل الدليل الرقمي.

الركن المعنوي- من جرائم القصد الخاص: هذه الجريمة من الجرائم العمدية التي يتحقق فيها الركن المعنوي بتوافر القصد الجنائي العام بعنصريه العلم والإرادة، فضلاً عن توافر قصد جنائي خاص يتمثل في قصد إعاقة عمل الجهات الرسمية المختصة، حيث يجب أن تتجه إرادة الجاني إلى الإخفاء أو العبث بغرض إعاقة سير السلطات الرسمية، ويقصد بالسلطات الرسمية في هذه الجريمة السلطات العامة المعنية بمكافحة الجرائم المعلوماتية، من جهات الضبط أو التحقيق أو المحاكمة.

العقوبة: عاقب القانون على هذه الجريمة بعقوبة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين، ومن ثم يجوز للقاضي توقيع عقوبة الحبس أو الغرامة أو العقوبتين معاً، ويجوز للقاضي في هذه الجريمة أن يحكم بإيقاف التنفيذ وفقاً لأحكام المادة ٥٥ عقوبات، والخطأ في الجرائم غير العمدية هو الركن المميز لها، ومن ثم يجب على المحكمة بيان عنصر الخطأ المرتكب والدليل عليه[١].

[١] انظر الطعن رقم ٢١٣٣٥ لسنة ٧٧ق جلسة ٢٠١٣/٣/٢٥، المستحدث من المبادئ الصادرة عن الدوائر الجنائية من أول أكتوبر ٢٠١٢ لغاية آخر سبتمبر ٢٠١٣، الصادرة عن المكتب الفني لمحكمة النقض، المجموعة الجنائية، ص ص٥٣، ٥٤.

المطلب الثالث

تعريض المواقع أو الحسابات الخاصة أو البريد الإلكتروني أو النظام المعلوماتي لوقوع الجرائم المعلوماتية

نص التجريم: تنص المادة (٢٩) من القانون على أنه:" *يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين، كل مسئول عن إدارة الموقع أو الحساب الخاص أو البريد الإلكتروني أو النظام المعلوماتي عرض أياً منها لإحدى الجرائم المنصوص عليها في هذا القانون. ويعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل مسئول عن إدارة الموقع أو الحساب الخاص أو البريد الإلكتروني أو النظام المعلوماتي تسبب بإهماله في تعرض أي منها لإحدى الجرائم المنصوص عليها في هذا القانون، وكان ذلك بعدم اتخاذه التدابير والاحتياطيات التأمينية الواردة في اللائحة التنفيذية لهذا القانون*".

العلة من التجريم: تتمثل علة التجريم في تقرير المسئولية الجنائية لمقدم الخدمات المعلوماتية عن تعريض المواقع أو الحسابات أو أي نظام معلوماتي أو بريد إلكتروني لوقوع الجرائم المعلوماتية، سواء أكان ذلك بشكل عمدي أو عن طريق الخطأ.

صفة الجاني: تطلب القانون أن يكون الجاني مسئولاً عن إدارة المواقع أو الحسابات الخاصة أو البريد الإلكتروني أو الأنظمة المعلوماتية، كما سبق أن أشرنا، في الجرائم السابقة.

الركن المادي: يتكون الركن المادي في هذه الجريمة من صور السلوك الإجرامي التالية:-

أ) السلوك العمدي: تعريض المواقع أو الحسابات الخاصة أو البريد الإلكتروني

أو النظام المعلوماتي لإحدى الجرائم المنصوص عليها في القانون، ومن ثم فإن الركن المادي في هذه الجريمة يتكون من ثلاثة عناصر، وذلك على النحو التالي:-

١) تعريض المواقع أو الأنظمة المعلوماتية للخطر: وهو ما يتحقق بأي سلوك إيجابي أو سلبي من شأنه تعريض المواقع أو الحسابات الخاصة أو الأنظمة المعلوماتية أو البريد الإلكتروني لخطر وقوع الجرائم المعلوماتية، وهو ما يتحقق حينما يتسبب المسئول عن إدارة المواقع الإلكترونية عمداً في وقوع إحدى الجرائم المعلوماتية، بسبب عدم اتخاذه الإجراءات التأمينية المناسبة لمنع الاختراقات المعلوماتية، كاستخدام الجدران النارية Firewall، مما قد يؤدي إلى وقوع أي من الجرائم المنصوص عليها في القانون.

٢) توافر علاقة السببية: يتطلب القانون ضرورة توافر علاقة السببية بين سلوك الجاني ووقوع إحدى الجرائم المعلوماتية الواردة بالقانون.

٣) وقوع إحدى الجرائم المعلوماتية المنصوص عليها في القانون، وتبرز الإشارة إلى التساؤل عما إذا كان يشترط تحقق الضرر في هذه الجريمة؟، والواقع أن الضرر مفترض في هذه الجريمة بالنظر لما ترتبه هذه الجرائم المعلوماتية من أضرار على المجني عليه.

ب) السلوك غير العمدي: تتحقق الجريمة بإحدى صور الخطأ غير العمدي التي تتخذ صور: الإهمال وعدم اتخاذ التدابير والاحتياطات التأمينية لمنع تعريض المواقع أو الحسابات الخاصة أو البريد الإلكتروني أو النظام المعلوماتي لإحدى الجرائم المنصوص عليها في القانون، ويقصد بالإهمال -كما سبق أن أشرنا-عدم الحيطة في أداء عمل ما على نحو صحيح، بينما يقصد بعدم اتخاذ التدابير والاحتياطات التأمينية اللازمة لمنع وقوع الجرائم المعلوماتية على المواقع الإلكترونية والحسابات الخاصة والبريد الإلكتروني والأنظمة المعلوماتية.

الركن المعنوي: يتحقق الركن المعنوي في الجريمة بصورتيه القصد الجنائي العام والخطأ غير العمدي، وذلك على النحو التالي:-

أ) القصد الجنائي العام: يتحقق القصد الجنائي العام بأن يعلم الجاني بأن من شأن فعله التسبب في وقوع جريمة معلوماتية، وأن تتجه إرادة الجاني إلى تحقيق ذلك.

ب) الخطأ غير العمدي: ويتحقق ذلك بأن يعلم الجاني بأن من شأن فعله التسبب في وقوع جريمة معلوماتية دون أن تتجه إرادة الجاني إلى وقوع أي جريمة معلوماتية.

العقوبة: ميز القانون في العقوبة على هذه الجريمة ما بين ما إذا كان السلوك عمدياً أم غير عمدي، وذلك على النحو التالي:-

أ) عقوبة السلوك العمدي: عاقب المشرع على السلوك العمدي بعقوبة الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين، ومن ثم يجوز للقاضي توقيع عقوبة الحبس أو الغرامة، أو العقوبتين معاً، كما يجوز للقاضي أن يحكم بوقف التنفيذ، إعمالاً لحكم المادة ٥٥ عقوبات.

ب) عقوبة السلوك غير العمدي: عاقب المشرع على السلوك غير العمدي بعقوبة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، ومن ثم يجوز للقاضي الحكم بعقوبة الحبس وحدها أو الغرامة وحدها أو بالعقوبتين معاً، ويجوز له أن يحكم بإيقاف التنفيذ وفقاً لأحكام المادة ٥٥ عقوبات، والخطأ في الجرائم غير العمدية هو الركن المميز لها، ومن ثم يجب على المحكمة بيان عنصر الخطأ المرتكب والدليل عليه[1].

---

[1] انظر الطعن رقم ٢١٣٣٥ لسنة ٧٧ق جلسة ٢٠١٣/٣/٢٥، سالف الإشارة إليه، ص ص٥٣، ٥٤.

المبحث الخامس

الجرائم المرتكبة من مقدمي الخدمة

تقسيم: نتناول في هذا المطلب المسئولية الجنائية لمقدمي الخدمة، من خلال تناول الجرائم التي ترتكب من مقدمي الخدمة، ومن أبرزها: جريمة الامتناع عن تنفيذ القرارات القضائية بحجب المواقع، وجريمة إفشاء البيانات الشخصية للمستخدمين، وجريمة امتناع مقدم الخدمة عن تنفيذ قرارات جهة التحقيق بتسليم البيانات، وجريمة الإخلال بالالتزامات الواجبة على مقدمي الخدمة، وذلك في أربعة مطالب، وذلك على النحو التالي:-

المطلب الأول

جريمة الامتناع عن تنفيذ القرارات القضائية بحجب المواقع

نص التجريم: أفرد الفصل الخامس للمسئولية الجنائية لمقدمي الخدمة، حيث تنص المادة (٣٠) من القانون على أنه:" ***يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه، أو بإحدى هاتين العقوبتين، كل مُقدم خدمة امتنع عن تنفيذ القرار الصادر من المحكمة الجنائية المختصة بحجب أحد المواقع أو الروابط أو المحتوى المشار إليه في الفقرة الأولى من المادة (٧) من هذا القانون. فإذا ترتب على الامتناع عن تنفيذ القرار الصادر من المحكمة، وفاة شخص أو أكثر، أو الإضرار بالأمن القومي، تكون العقوبة السجن المُشدد، والغرامة التي لا تقل عن ثلاثة ملايين جنيه ولا تجاوز عشرين مليون جنيه، وتقضى المحكمة فضلاً عن ذلك بإلغاء ترخيص مزاولة النشاط***".

العلة من التجريم: تتمثل علة التجريم في مواجهة تقاعس مقدمي الخدمات المعلوماتية عن تنفيذ القرارات القضائية ذات الصلة بحجب المواقع الإلكترونية، بالنظر إلى أن مثل هذا السلوك يشكل إحدى صور إعاقة أجهزة العدالة عن أداء وظيفتها.

صفة الجاني: تطلب القانون أن يكون الجاني من مقدمي الخدمة، وقد عرف القانون مقدم الخدمة بأنه:" *أي شخص طبيعي أو اعتباري يزود المستخدمين بخدمات تقنية المعلومات والاتصالات، ويشمل ذلك من يقوم بمعالجة أو تخزين المعلومات بذاته أو من ينوب عنه في أي من تلك الخدمات أو تقنية المعلومات*".

الركن المادي: يتحقق السلوك الإجرامي بفعل الامتناع عن تنفيذ قرار حجب أحد المواقع أو الروابط أو المحتوى المعلوماتي، والامتناع هو كل سلوك سلبي من شأنه عدم إتيان فعل واجب القيام به، ويشترط لقيام الامتناع وجود واجب قانوني يلزم بفعل إيجابي، وهو في هذه الحالة التزام مقدم الخدمة بتنفيذ الأحكام القضائية واجبة النفاذ بحجب المواقع الإلكترونية، فضلاً عن أن يكون في استطاعة الممتنع القيام بهذا الفعل بإرادته، وهو ما يتحقق بالفعل بالنسبة لمقدم الخدمة فيما يتصل بحجب المواقع الإلكترونية أو الروابط أو المحتوى، وقد عرف القانون المحتوى بأنه:"أي بيانات تؤدي بذاتها، أو مجتمعة مع بيانات أو معلومات أخرى، إلى تكوين معلومة أو تحديد توجه أو اتجاه أو تصور أو معنى أو الإشارة إلى بيانات أخرى"[1]، والامتناع كالفعل الإيجابي سلوك إرادي، يتطلب القانون فيه ضرورة توافر رابطة السببية بين الإرادة والسلوك السلبي للممتنع[2].

---

[1] ومن التشريعات التي تضمنت تعريف للمحتوى التشريع الإماراتي والسوداني والبحريني.

[2] د. حامد راشد: شرح قانون العقوبات- القسم العام، مرجع سابق، ص١٦٣.

الركن المعنوي: هذه الجريمة من الجرائم العمدية التي يتحقق فيها الركن المعنوي بتوافر القصد الجنائي العام بعنصريه العلم والإرادة، بأن يعلم مقدم الخدمة بصدور حكم قضائي من المحكمة بحجب أحد المواقع الإلكترونية أو الروابط أو المحتوى، وأن يعلم بأن من شأن امتناعه عدم تنفيذ هذا الحكم، وأن تتجه إرادته إلى السلوك السلبي المتمثل في عدم تنفيذ الحكم القضائي بحجب المواقع أو الروابط أو المحتوى المعلوماتي، ولا عبرة بالبواعث في الجريمة.

العقوبة: عاقب القانون على هذه الجريمة بعقوبة الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه، أو بإحدى هاتين العقوبتين، ومن ثم يجوز للقاضي توقيع الحبس أو الغرامة أو العقوبتين معاً، كما يجوز له أن يحكم بوقف التنفيذ، إعمالاً لحكم المادة ٥٥ عقوبات.

حالات تشديد العقاب: شدد القانون العقوبة المقررة للجريمة لتصبح السجن المُشدد وغرامة لا تقل عن ثلاثة ملايين جنيه ولا تجاوز عشرين مليون جنيه، إذا ترتب على الامتناع عن تنفيذ القرار الصادر من المحكمة، وفاة شخص أو أكثر، أو الإضرار بالأمن القومي، وقد سبق للقانون بيان المقصود بالأمن القومي بأنه:" *كل ما يتصل باستقلال واستقرار وأمن الوطن ووحدته وسلامة أراضيه، وما يتعلق بشئون رئاسة الجمهورية ومجلس الدفاع الوطني ومجلس الأمن القومي، ووزارة الدفاع والإنتاج الحربي، ووزارة الداخلية، والمخابرات العامة، وهيئة الرقابة الإدارية، والأجهزة التابعة لتلك الجهات*"، ومن ثم اعتبر المشرع جسامة الضرر الواقع على الأفراد أو الدولة، ظرفاً مشدداً يغير من وصف العقوبة من الجنحة إلى الجناية، كما تقضي المحكمة في هذه الجريمة كذلك بإلغاء مزاولة النشاط لمقدم الخدمة، وهذه العقوبة وجوبية.

المطلب الثاني

جريمة إفشاء البيانات الشخصية للمستخدمين

نص التجريم: تنص المادة (٣١) من القانون على أنه:" *يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز عشرين ألف جنيه، أو بإحدى هاتين العقوبتين، كل مُقدم خدمة خالف الأحكام الواردة بالبند (٢) من الفقرة أولاً من المادة (٢) من القانون، وتتعدد عقوبة الغرامة بتعدد المجني عليهم من مستخدمي الخدمة* "[١]، وكان البند الثاني من الفقرة الأولى من المادة الثانية من القانون قد حدد الالتزام الواجب على مقدم الخدمة في المحافظة على سرية البيانات التى تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة – ويشمل ذلك البيانات الشخصية لأى من مستخدمي خدمته، أو أية بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التى يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التى يتواصلون معها[٢].

---

[١] ذهب المشرع المصري إلى تجريم أفعال المساس بسرية البيانات الإلكترونية قانون التوقيع الإلكتروني رقم (١٥) لسنة ٢٠٠٤، وذلك من أجل تحقيق الثقة فيها وإسباغ الحماية الكاملة للمحررات والتوقيعات الإلكترونية؛ حيث أشار في المادة (٢٣/ د) من قانون التوقيع الإلكتروني إلى معاقبة كل من يخالف أياً من أحكام المادتين (١٩، ٢١) من هذا القانون، وتتمثل أحكام المادة (٢١) من القانون في ضرورة عدم إفشاء سرية بيانات التوقيع والوسائط الإلكترونية والمعلومات التي تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الإلكتروني، ولا يجوز لمن قدمت إليه تلك البيانات أو اتصل بها بحكم عمله إفشاؤها للغير أو استخدامها في غير الغرض الذي قدمت من أجله. ويعاقب على هذه الجريمة بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين، كما تُزاد العقوبة بمقدار المثل في حالة العودة، ويجب الحكم بنشر حكم الإدانة في جريدتين يوميتين واسعتي الانتشار وعلى شبكات المعلومات الإلكترونية المفتوحة على نفقة المحكوم عليه.

[٢] ومن التشريعات العربية التي بينت ماهية المعلومات التي تخص المشتركين التشريع الكويتي.

العلة من التجريم: تتمثل علة التجريم في توفير الحماية الجنائية لخصوصية البيانات والمعلومات الخاصة بالأفراد، بإفشاء البيانات الشخصية لمستخدمي الخدمات المعلوماتية.

صفة الجاني: تطلب القانون في هذه الجريمة كذلك أن يكون من مقدمي الخدمة، وقد سبق لنا تعريفه في الجريمة السابقة.

الركن المادي: يتكون الركن المادي للجريمة من فعل الإفشاء، ويقصد به الكشف أو الإفصاح أو الإخبار للغير عن البيانات الخاصة بالمستخدمين المحفوظة والمخزنة لدى مقدم الخدمة، وقد عرف القانون المستخدم بأنه:" كل شخص طبيعي أو اعتباري، يستعمل خدمات تقنية المعلومات، أو يستفيد منها بأي صورة كانت".

ويستوى لدى القانون أن يكون الإفشاء كلياً يشمل كافة بيانات المستخدم أم جزئياً ليشمل بعض البيانات الخاصة به، كما أن القانون لا يحفل كذلك بوسيلة الإفضاء، فقد يكون ذلك شفاهة أو كتابة أو بالإشارة، كما لا يحفل بعدد من حصل الإفضاء إليه، فقد يكون شخصاً واحداً؛ كالزوجة أو قريب أو صديق أو أكثر من شخص[1]، وموضوع الإفشاء ينصب على البيانات الشخصية لأى من مستخدمى خدمته، أو أية بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التى يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التى يتواصلون معها، وهذه البيانات قرر لها المشرع الحماية الجنائية، وأوجب على مقدم الخدمة الالتزام بسريتها، وهذا الالتزام بعدم إفشاء بيانات العملاء أو المستخدمين، قرر عليه المشرع استثناءً وحيداً، ممثلاً في عدم امتداده إلى الجهات القضائية المختصة، حيث حظر القانون على مقدم الخدمة الإفصاح عن هذه البيانات بغير أمر مسبب من إحدى الجهات القضائية المختصة.

---

[1] قارن: د. حسنين عبيد: شرح قانون العقوبات- القسم الخاص، جرائم الاعتداء على الأشخاص والأموال، القاهرة، دار النهضة العربية، ط٩، ٢٠٠٩، ص٢٦٦.

الركن المعنوي: هذه الجريمة من الجرائم العمدية التي يتحقق فيها الركن المعنوي بتوافر القصد الجنائي العام بعنصريه العلم والإرادة، بأن يعلم الجاني أن من شأن فعله الإفصاح عن البيانات المحفوظة أو المخزنة لدى مقدم الخدمة، وأن تتجه إرادته إلى إفصاح هذه البيانات للغير، ولا عبرة للبواعث على الجريمة[1].

العقوبة: عاقب القانون على هذه الجريمة بالحبس مدة لا تقل عن سنة، وغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز عشرين ألف جنيه، أو بإحدى هاتين العقوبتين، ومن ثم يجوز للقاضي توقيع عقوبة الحبس أو الغرامة أو العقوبتين معاً، كما يجوز للقاضي أن يحكم بوقف التنفيذ، إعمالاً لحكم المادة ٥٥ عقوبات، وتبرز الإشارة إلى أن المشرع قد حرص على تطبيق قاعدة مفادها ربط مبلغ الغرامة المحكوم بها بحسب عدد المجني عليهم من مستخدمي الخدمة، حيث أشار إلى أنه:" *وتتعدد عقوبة الغرامة بتعدد المجني عليهم من مستخدمي الخدمة*"؛ أي أن القاضي يحكم بمقدار الغرامة المحدد في القانون مضروباً في عدد المجني عليهم في القضية، ولا شك في أن ذلك من شأنه تحقيق عنصري الإيلام والردع بصورتيه العام والخاص للفاعلين في هذه الجريمة من مقدمي خدمات الاتصالات والمعلومات، بالنظر إلى المبالغ المالية الضخمة التي يمكن الحكم بها عليه في جرائم إفشاء بيانات العملاء.

---

[1] المرجع السابق، ص٢٦٩.

المطلب الثالث

جريمة امتناع مقدم الخدمة عن تنفيذ قرارات جهة التحقيق بتسليم البيانات

نص التجريم: تنص المادة (٣٢) من القانون على أنه:" *يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل مُقدمة خدمة امتنع عن تنفيذ القرار الصادر من جهة التحقيق المختصة بتسليم ما لديه من البيانات أو المعلومات المشار إليها في المادة (٦) من هذا القانون*".

العلة من التجريم: تتمثل علة التجريم في مواجهة تقاعس مقدمي الخدمات المعلوماتية عن معاونة جهات التحقيق وتقديم البيانات والمعلومات المطلوبة عن الجرائم المعلوماتية، بالنظر إلى أن مثل هذا السلوك يشكل إحدى صور إعاقة أجهزة العدالة عن أداء وظيفتها.

صفة الجاني: تطلب القانون في هذه الجريمة كذلك أن يكون من مقدمي الخدمة، وقد سبق لنا تعريفه في الجريمة السابقة.

الركن المادي: يتكون الركن المادي للجريمة من فعل الامتناع عن تسليم البيانات والمعلومات لجهات التحقيق المختصة، وتفترض هذه الجريمة وجود تحقيق جنائي مفتوح من جانب جهات التحقيق المختصة بصدد إحدى الجرائم المرتكبة، أيا كانت هذه الجريمة، حيث نرى أن الالتزام الواجب على الأفراد على معاونة أجهزة العدالة لا يقتصر على جريمة بعينها، وإنما هو التزام عام يشمل كافة الجرائم المرتكبة، ومن ثم لا يقتصر الالتزام الواقع على مقدم الخدمة على الجرائم المعلوماتية فحسب.

الركن المعنوي: هذه الجريمة من الجرائم العمدية التي يتحقق فيها الركن المعنوي بتوافر القصد الجنائي العام بعنصريه العلم والإرادة، حيث ينبغي أن يعلم مقدم الخدمة بصدور قرار من جهة التحقيق المختصة بتسليم ما لديه من بيانات أو المعلومات، وأن تتجه إرادته إلى الامتناع عن الإفضاء بالبيانات والمعلومات المطلوبة لجهات التحقيق المختصة، ولا عبرة للبواعث على الجريمة.

العقوبة: عاقب القانون على هذه الجريمة بعقوبة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، ومن ثم يجوز للقاضي أن يحكم بالحبس أو بالغرامة أو بالعقوبتين معاً، كما يجوز للقاضي أن يحكم بوقف التنفيذ، إعمالاً لحكم المادة ٥٥ عقوبات.

المطلب الرابع

جريمة الإخلال بالالتزامات الواجبة على مقدمي الخدمة

نص التجريم: تنص المادة (٣٣) من القانون على أنه:" *يعاقب بغرامة لا تقل عن خمسة ملايين جنيه ولا تجاوز عشرة ملايين جنيه، كل مُقدم خدمة أخل بأي من التزاماته المنصوص عليها في البند (١) من الفقرة أولاً من المادة (٢) من هذا القانون. وتضاعف عقوبة الغرامة في حالة العود، وللمحكمة القضاء بإلغاء الترخيص. ويعاقب بغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتي ألف جنيه، كل مُقدم خدمة خالف أحكام الفقرة (ثانياً) و(رابعاً) من المادة (٢) من هذا القانون. ويعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبالغرامة التي لا تقل عن مائتي ألف جنيه ولا تجاوز مليون جنيه، كل مقدم خدمة خالف أحكام الفقرة ثالثاً من المادة (٢) من هذا القانون*".

العلة من التجريم: تتمثل علة التجريم في مواجهة تقاعس مقدمي الخدمات المعلوماتية وإخلالهم بالواجبات الواقعة عليهم في مواجهة الجرائم المعلوماتية.

صفة الجاني: تطلب القانون في هذه الجريمة كذلك أن يكون من مقدمي الخدمة، وقد سبق لنا تعريفه في الجريمة السابقة.

الركن المادي: يتحقق الركن المادي للجريمة بأي فعل إيجابي أو سلبي يتحقق به إخلال مقدم الخدمة بالالتزامات المقررة به بموجب القانون ومنها[1]:-

---

[1] نصت المادة الثانية من القانون المعنونة بالتزامات وواجبات مقدم الخدمة، على أنه:"(أولاً): مع عدم الإخلال بالأحكام الواردة بهذا القانون وقانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣ المشار إليه، يلتزم مقدمو الخدمة بما يأتي:- (١) حفظ وتخزين سجل النظام المعلوماتي أو أى وسيلة لتقنية المعلومات، لمدة مائة وثمانون يوماً متصلة. وتتمثل البيانات الواجب حفظها وتخزينها فيما يلى:- أ - البيانات التى تمكن من التعرف على مستخدم الخدمة. ب- البيانات المتعلقة بمحتوى ومضمون النظام المعلوماتي المتعامل فيه متى كانت تحت سيطرته. ج- البيانات المتعلقة بحركة الاتصال. د - البيانات المتعلقة بالأجهزة الطرفية للاتصال. هـ- أى بيانات أخرى يصدر بتحديدها قرار من مجلس إدارة الجهاز. (٢)المحافظة على سرية البيانات التى تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة – ويشمل ذلك البيانات الشخصية لأي من مستخدمي خدمته، أو أية بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التى يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التى يتواصلون معها. (٣)تأمين البيانات والمعلومات بما يحافظ على سريتها. عدم اختراقها أو تلفها. (ثانياً): مع عدم الإخلال بأحكام قانون حماية المستهلك، يجب على مقدم الخدمة أن يوفر لمستخدمي خدماته ولأي جهة حكومية مختصة، في الشكل وبالطريقة التى يمكن الوصول إليها بصورة ميسرة ومباشرة ومستمرة، البيانات والمعلومات الآتية: - (١) اسم مقدم الخدمة وعنوانه. (٢) معلومات الاتصال المتعلقة بمقدم الخدمة، بما في ذلك عنوان الاتصال الإلكتروني. (٣) بيانات الترخيص لتحديد هوية مقدم الخدمة، وتحديد الجهة المختصة التي يخضع لإشرافها. (٤) أية معلومات أخرى يقدر الجهاز أهميتها لحماية مستخدمي الخدمة، ويحددها قرار يصدره الوزير المختص. (ثالثاً): مع مراعاة حرمة الحياة الخاصة التي يكفلها الدستور يلتزم مقدمو الخدمة، أن يوفروا حال طلب أجهزة الأمن القومي ووفقاً لاحتياجاتها كافة الإمكانيات الفنية من معدات ونظم وبرامج والتي تتيح لتلك الجهات ممارسة اختصاصاتها وفقاً للقانون. (رابعاً): يلتزم مقدمو خدمات تقنية المعلومات ووكلائهم وموزعيهم التابعين لهم المنوط بهم تسويق تلك الخدمات بالحصول على بيانات المستخدمين، ويحظر على غير هؤلاء القيام بذلك".

١- الالتزام بحفظ وتخزين سجل النظام المعلوماتى أو أي وسيلة لتقنية المعلومات لمدة ١٨٠ يوماً متصلة.

٢- الالتزام بالمحافظة على سرية البيانات التي تم حفظها وتخزينها وعدم إفشائها بغير إذن مسبب من إحدى الجهات القضائية، وهذا الالتزام عاقب المشرع مقدم الخدمة على مخالفته بموجب المادة (٣١) من القانون.

٣- التزامه بتأمين البيانات، بما يحافظ على سريتها، وعدم اعتراضها أو اختراقها أو تلفها[1].

---

[1] نصت المادة الثانية من اللائحة التنفيذية للقانون على أنه:" يلتزم مقدمو خدمات تقنيات المعلومات باتخاذ الإجراءات التقنية والتنظيمية التالية تنفيذًا للبندين (٢ و٣) من الفقرة أولاً من المادة رقم (٢) من القانون: ١- تشفير البيانات والمعلومات بما يحافظ على سريتها، وعدم اختراقها باستخدام نظام تشفير قياسي متماثل أو غير متماثل لا يقل في تأمينه عن Advanced (ASE-128) Encryption Standard بمفتاح شفرة لا يقل عن (١٢٨ بت)، مع مسئوليته بالحفاظ على سرية وأمان مفتاح التشفير. ٢- تنصيب واستخدام نظم وبرامج ومعدات مكافحة البرمجيات والهجمات الخبيثة والتأكد من صلاحيتها وتحديثها. ٣-استخدام بروتوكولات آمنة، مثل بروتوكول نقل النص التشعبى المؤمنHTTPS . ٤- وضع صلاحيات بالشبكات والملفات وقواعد البيانات وتحديد المسئولين، لضمان حماية الوصول المنطقي Logical Access إلى الأصول المعلوماتية والتقنية لمنع الوصول غير المصرح به. ٥- إعداد قائمة بالأجهزة والمعدات وأرقامها المميزة والمسلسلة وطرازاتها وكذا بيان بالنظم والبرامج والتطبيقات وقواعد البيانات المستخدمة ومواصفاتها. ٦- تطبيق أفضل الممارسات والضوابط عند اختيار مواصفات كلمات السر أو المرور وفقًا للملحق رقم (١) المرفق باللائحة التنفيذية. ٧- توثيق إجراءات التنصيب والتشغيل الخاصة بالأنظمة. ٨- ضمان تنفيذ وتشغيل وصيانة الأنظمة وإلزام الأطراف المتعاقد معها بإبرام اتفاقيات تحدد مستوى تقديم الخدمة مع الجهة وحدود مسئولية كل جهة. ٩- إجراء التحديثات الخاصة بالنظم والبرامج والتطبيقات بشكل دوري وإتمام الاختبارات اللازمة قبل إجراء التحديثات. ١٠- إجراء اختبار سنوي للكشف عن الاختراقات أو المخاطر الأمنية. ١١- استخدام معدات وأجهزة ونظم وبرمجيات الجدران النارية (NGFW-UTM-Firewalls) لحماية الشبكات والنظم"، بينما نصت المادة ٣ من اللائحة على أنه:" يلتزم مقدمو خدمات تقنية المعلومات والاتصالات التي تمتلك أو تدير أو تشغل البنية التحتية المعلوماتية الحرجة المخاطبين بأحكام هذا القانون، باتخاذ الإجراءات التقنية والتنظيمية التالية تنفيذًا للبندين (٢و٣) من الفقرة أولاً من المادة رقم (٢) من =

=

القانون: ١- إعداد سياسة أمن معلومات واعتمادها من الإدارة العليا للبنية التحتية المعلوماتية الحرجة وضمان مراجعتها كل عام لضمان استمرار ملائمة وكفاية وفاعلية تلك السياسة. على أن تتضمن تلك السياسة متطلبات الأجهزة والجهات الرقابية والتنظيمية المختصة بالبنية التحتية المعلوماتية الحرجة، والمتطلبات القانونية ، والمتطلبات الخاصة بالموارد البشرية. ٢- ضمان التأكد من الامتثال لما ورد بهذا القانون ولائحته والقرارات التنفيذية ذات الصلة من التزامات تقنية أو تنظيمية. ٣- تشفير البيانات والمعلومات بما يحافظ على سريتها، وعدم اختراقها باستخدام نظام تشفير قياسي متماثل أو غير متماثل لا يقل تأمينه عن Advanced Encryption Standard (AES-256)بمفتاح شفرة لا يقل عن (٢٥٦ بت) يتم توليده باستخدام نظام عشوائي آمن. واستخدام نظام إدارة مفاتيح تشفير قياسي للحفاظ على سريتها ودورة حياتها ومستويات استخدامها فى التطبيقات المختلفة. ٤ - استخدام شهادات تصديق إلكتروني صادرة من جهة من جهات إصدار شهادات التوقيع الإلكتروني المعترف بها في جمهورية مصر العربية وبضوابط قانون تنظيم التوقيع الإلكتروني ولائحته التنفيذية، وذلك لكافة المستخدمين لأنظمة المعلومات الخاصة بالبنية المعلوماتية التحتية الحرجة. ٥- منع الوصول المادي لغير المخول أو المصرح لهم الدخول أو الوصول لمقار وأجهزة ومعدات أنظمة البنية التحتية المعلوماتية الحرجة. ٦- استخدام ضوابط نفاذ قوية Strong Authentication وفعالة من خلال فئتين أو أكثر من فئات التوثق Multi-factor Authenticationوبحسب مستوى المخاطر، بما يضمن تحديد المسئولية وعدم الإنكار. ٧- توثيق إجراءات التنصيب والتشغيل الخاصة بنظم البنية التحتية المعلوماتية الحرجة وإتاحتها للمستخدمين المخول لهم ذلك عند حاجتهم إليها، وإلزام الموردين بتزويد الجهة بكامل الوثائق الخاصة بالإجراءات التشغيلية. ٨- ضمان تنفيذ وتشغيل وصيانة أنظمة البنية التحتية المعلوماتية الحرجة وإلزام الأطراف المتعاقد معها بإبرام اتفاقيات تحدد مستوى تقديم الخدمة مع الجهة. ٩- تنصيب واستخدام نظم وبرامج ومعدات المكافحة والحماية من البرمجيات والهجمات الخبيثة، والكشف عنها والتأكد من صلاحيتها وتحديثها. ١٠- إجراء التحديثات الخاصة بالنظم والبرامج والتطبيقات بشكل دوري. مع الأخذ في الاعتبار ضوابط التعامل مع إجراء التحديثات على أنظمة التحكم الصناعي مع عدم اتصالها المباشر بشبكة الإنترنت ، وإتمام الاختبارات اللازمة قبل إجراء التحديثات. ١١- إجراء مسح سنوي لأنظمة التحكم الصناعي للكشف عن الثغرات ونقاط الضعف واتخاذ الإجراءات اللازمة للتعامل معها. ١٢- إجراء اختبار سنوي للكشف عن الاختراقات أو المخاطر الأمنية وتثبيت أجهزة المنع والكشف عن الاختراقات. ١٣- اتخاذ الإجراءات الملائمة للتعامل مع الثغرات الفنية للأجهزة وللنظم والبرامج والتطبيقات عند العلم بها. ١٤- إجراء عمليات أخذ نسخ احتياطية شهرية للبيانات والمعلومات، والاحتفاظ بها وتخزينها مشفرة فى موقع آخر. ١٥- استخدام معدات وأجهزة ونظم وبرمجيات الجدران النارية-NGFW) (UTM-Firewallsلحماية الشبكات والنظم. ١٦- استخدام بروتوكولات آمنة ، مثل بروتوكول نقل النص التشعبى المؤمن HTTPS .١٧-إعداد قائمة بالأجهزة والمعدات وأرقامها المميزة

=

٤- الالتزام بتوفير بعض البيانات لمستخدمي الخدمة ولأي من جهات الدولة

=

والمسلسلة وطرازاتها وكذا بيان بالنظم والبرامج والتطبيقات وقواعد البيانات المستخدمة ومواصفاتها. ١٨- تحديد مسئوليات الإدارة العليا ومسئولي تكنولوجيا المعلومات وأمن المعلومات بشكل واضح وصلاحيات وسلطات وواجبات والتزامات كل منهم، مع ضرورة اتساق ذلك مع ما تقوم به إدارات الموارد البشرية وشئون العاملين من إعداد للهياكل، والتوصيف الوظيفي، والأنشطة التدريبية وغيرها من أنشطة وعمليات تلك الإدارات. ١٩- إبلاغ المركز الوطني للاستعداد لطوارئ الحاسب والشبكات بالجهاز عن أي حوادث أو اختراقات فور العلم بحدوثها. ٢٠- وضع خطة استمرارية العمل والبدائل المقترحة في حال حدوث أي مخاطر أو أزمات تتعلق بتقديم الخدمة أو انقطاعها، والقدرة على استعادة الخدمة والعمل في حال الكوارث، واختبار الخطة دوريًا". وقد عرفت اللائحة التنفيذية للقانون البنية التحتية المعلوماتية الحرجة Critical Information Infrastructure: مجموعة أنظمة أو شبكات أو أصول معلوماتية أساسية يؤدى الكشف عن تفصيلاتها تعطيلها أو تغيير طريقة عملها بطريقة غير مشروعة، أو الدخول غير المصرح به عليها، أو الدخول أو الوصول بشكل غير قانوني للبيانات والمعلومات التي تحفظها أو تعالجها، أو يؤدى القيام بأي فعل غير مشروع آخر بها إلى التأثير على توافر خدمات الدولة ومرافقها الأساسية أو خسائر اقتصادية أو اجتماعية كبيرة على المستوى الوطني. ويعد من البنية التحتية المعلوماتية الحرجة على الأخص ما يستخدم في الطاقة الكهربائية، الغاز الطبيعي والبترول، الاتصالات، والجهات المالية والبنوك، والصناعات المختلفة، والنقل والمواصلات والطيران المدني، والتعليم والبحث العلمي، والبث الإذاعي والتليفزيوني، ومحطات مياه الشرب والصرف الصحي والموارد المائية ، والصحة، الخدمات الحكومية وخدمات الإغاثة وخدمات الطوارئ، وغيرها من مرافق المعلومات والاتصالات التي قد تؤثر على الأمن القومي أو الاقتصاد القومي والمصلحة العامة وما فى حكمها"، وقد عرفت المادة الأولى من اللائحة كلاً من نظام التحكم الصناعى ونقاط الضعف، حيث عرفت نظام التحكم الصناعي بأنه: حاسب أو مجموعة حواسب متصلة ببعضها البعض، وبالمعدات المتحكم بها وأدوات الاتصال المتبادل بينهم رقمية Digitalأو تناظرية Analog ، أو غيرها بما فى ذلك الحساسات والمنفذات Actuator لتشغيل هذه المعدات والتحكم بها منطقيًا طبقًا للصناعة المعنية، أو الأعمال المطلوبة فى مكان واحد أو موزعة فى أماكن متقاربة أو موزعة جغرافيًا مع اتصال النظام بالإنترنت أو بغيره من الأنظمة المماثلة أو غير المماثلة أو استقلاله وعدم اتصاله بما عداه مع تراكم مستوى التحكم أو عدم تراكمه، بينما عرفت اللائحة نقاط الضعف Vulnerabilities بأنها: خلل أو ثغرة فى نظام تشغيل أو تطبيقات أو شبكات المعلومات أو العمليات أو السياسات الخاصة بتأمين المعلومات أو فى بيئة تقنية المعلومات أو الاتصالات والتى يمكن استغلالها فى عمليات الاختراق أو الهجوم أو الاتلاف أو التجسس أو أى عمل غير مشروع".

المختصة، بصورة مباشرة وميسرة؛ كاسم المستخدم وعنوانه وبيانات الترخيص، والجهة المختصة التي يخضع لإشرافها، مع التأكيد على التزام مقدمي الخدمة ووكلائهم وموزعيهم التابعين لهم المنوط بهم تسويق تلك الخدمات بالحصول على بيانات المستخدمين، وحظر القيام بذلك على غيرهم.

٥- الالتزام بتوفير كافة الإمكانيات الفنية التي تتيح لتلك الجهات الرسمية ممارسة اختصاصاتها وفقا للقانون.

٦- التزام مقدمي الخدمة ووكلائهم وموزعيهم التابعين لهم المنوط بهم تسويق تلك الخدمات بالحصول على بيانات المستخدمين، وحظر القيام بذلك على غيرهم.

ويشمل هذا النص تجريم مخالفة مقدم الخدمة للالتزامات التالية:-

أولاً- الالتزام بحفظ وتخزين سجل النظام المعلوماتي أو أي وسيلة لتقنية المعلومات لمدة ١٨٠ يوماً متصلة، وتتعلق هذه البيانات بمحتوى النظام المعلوماتي المتعامل فيه وحركة الاتصال والأجهزة الطرفية للاتصال، وبما يمكن من التعرف على مستخدم الخدمة، ومن ثم تتحقق الجريمة بمجرد إخلال مقدم الخدمة بالالتزام الخاص بحفظ وتخزين البيانات والمعلومات خلال المدة المحددة في القانون وهي ١٨٠ يوماً متصلة، فإذا انقضت هذه المدة، سقطت المسئولية الجنائية المقررة على مقدم الخدمة في هذا الشأن. وقد عرف القانون حركة الاتصال (بيانات المرور) بأنها: "بيانات ينتجها نظام معلوماتي تبين مصدر الاتصال وجهته والوجهة المرسل منها والمرسل إليها والطريق الذي سلكه وساعته وتاريخه وحجمه ومدته ونوع الخدمة"[١].

ثانياً- الالتزام بتوفير بعض البيانات لمستخدمي الخدمة ولأي من جهات الدولة

[١] ومن التشريعات المقارنة التي تضمنت تعريف لبيانات المرور التشريع القطري.

المختصة، بصورة مباشرة وميسرة ومستمرة؛ كاسم المستخدم وعنوانه، ومعلومات الاتصال المتعلقة بمقدم الخدمة، بما في ذلك عنوان الاتصال الإلكتروني، وبيانات الترخيص، والجهة المختصة التي يخضع لإشرافها، وأي معلومات أخرى يقدر الجهاز القومي لتنظيم الاتصالات أهميتها لحماية مستخدمي الخدمة، ويصدر بتحديدها قرار من الوزير المعني بشئون الاتصالات وتكنولوجيا المعلومات، وذلك مع عدم الإخلال بأحكام قانون حماية المستهلك.

ثالثاً- الالتزام بتوفير كافة الإمكانيات الفنية التي تتيح للجهات الرسمية، ومنها جهات الأمن القومي، ممارسة اختصاصاتها وفقاً للقانون.

رابعاً- التزام مقدمي الخدمة ووكلائهم وموزعيهم بالحصول على بيانات المستخدمين دون غيرهم.

ومن ثم تتحقق الجريمة بأي سلوك إيجابي أو سلبي من شأنه مخالفة أي من الالتزامات المقررة بعاليه على مقدم الخدمة، فضلاً عن ضرورة توافر رابطة السببية بين سلوك الجاني ومخالفة الالتزامات القانونية الواقعة على عاتق مقدم الخدمة.

الركن المعنوي: هذه الجريمة من الجرائم العمدية التي يتحقق فيها الركن المعنوي بتوافر القصد الجنائي العام بعنصريه العلم والإرادة، فيجب أن يعلم مقدم الخدمة أن من شأن فعله الإخلال بالالتزامات الواجبة عليه تجاه مستخدمي الخدمة، وذلك بالمخالفة لأحكام القانون، وأن تتجه إرادته إلى تحقيق ذلك.

العقوبة: عاقب القانون على هذه الجريمة بثلاث عقوبات، تختلف بحسب طبيعة الالتزام التي خالفه الجاني، وذلك على النحو التالي:-

أ) مخالفة الالتزام بحفظ وتخزين البيانات والمعلومات للمدة القانونية المقررة: عاقب المشرع على هذه الجريمة بالغرامة التي لا تقل عن خمسة ملايين جنيه ولا

تجاوز عشرة ملايين جنيه، ويجوز للقاضي مضاعفة الغرامة في حالة العود؛ أي سابقة تكرار الجريمة، كما يجوز للقاضي الحكم كذلك بإلغاء الترخيص كعقوبة تكميلية، فهذه العقوبة جوازية للمحكمة.

ب) مخالفة الالتزام بتوفير البيانات لمستخدمي الخدمة ولجهات الدولة المختصة ومخالفة التزام مقدمي الخدمة ووكلائهم وموزعيهم بالحصول على بيانات المستخدمين دون غيرهم: وقد عاقب المشرع على هذه الجريمة بالغرامة التي لا تقل عن عشرون ألف جنيه ولا تجاوز مائتي ألف جنيه.

ج) مخالفة الالتزام بتوفير الإمكانيات الفنية التي تتيح لجهات الأمن القومي ممارسة اختصاصاتها: عاقب المشرع مُقدمي الخدمة فيها بالحبس مدة لا تقل عن ثلاثة أشهر وبالغرامة التي لا تقل عن مائتي ألف جنيه ولا تجاوز مليون جنيه.

تقدير موقف المشرع المصري: يتضح من العرض السابق للجرائم الواردة بقانون جرائم تقنية المعلومات أن أغلب هذه الجرائم من قبيل الجنح، ومن ثم فإن المشرع المصري لم يجد في هذه الجرائم من الخطورة التي يرى تشديد العقوبة فيها لتصبح في مصاف الجنايات، إلا في بعض الأحوال التي يقع فيها الإضرار بالبيانات والمعلومات التي تخص الدولة، وهذا النهج من جانب المشرع كان من الواجب مراجعته، بالنظر إلى خطورة وذيوع وانتشار أنشطة الجرائم المعلوماتية، وبما يحقق الردع بصورتيه العام والخاص.

المبحث السادس

الأحكام الجنائية الخاصة بجرائم تقنية المعلومات

تقسيم: بعد أن تناولنا للنموذج القانوني الخاص بكل جريمة من صور الجرائم المعلوماتية، نعرض للأحكام الجنائية الخاصة لهذه الجرائم، وتشمل حالات التعدد المعنوي وتشديد العقاب، والمسئولية الجنائية للشخص الاعتباري، والعقوبات التكميلية، وأحكام الشروع والإعفاء من العقاب، وذلك في أربعة مطالب على النحو التالي:-

المطلب الأول

حالات التعدد المعنوي وتشديد العقاب

في جرائم تقنية المعلومات

أولاً- حالة التعدد المعنوي في جرائم تقنية المعلومات: تعرض المشرع الجنائي لحالة التعدد المعنوي في جرائم تقنية المعلومات، حينما يشكل سلوك الجاني أكثر من جريمة، أي أن فعل الجاني يخضع لأكثر من نص من نصوص التجريم[1]، حيث ينص القانون وفقاً لأحكام الفقرة الأولى من المادة (٣٢) عقوبات على معاقبة المتهم بالعقوبة المقررة للجريمة ذات الوصف الأشد، وهو ما حرص المشرع الجنائي في قانون مكافحة جرائم تقنية المعلومات من النص عليه في المادة (١٢) من القانون بقوله:" ***مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون العقوبات أو أي قانون آخر، ومع مراعاة أحكام قانون الطفل الصادر بالقانون رقم ١٢ لسنة ١٩٩٦ ، يعاقب على***

[1] د. جميل عبد الباقي الصغير: النظرية العامة للعقوبة، القاهرة، دار النهضة العربية، ١٩٩٧، ص١٢٨.

الجرائم التالية بالعقوبات المبينة قرين كل جريمة "[١]، فالأصل أن قانون العقوبات هو القانون الذي يحدد الأفعال التي تعد من قبيل الجرائم، ويحدد العقوبات المقررة لها[٢]، إلا أن المشرع قد ينص على عقوبات جنائية في قوانين أخرى كما هو الحال في قوانين مكافحة جرائم تقنية المعلومات ومكافحة المخدرات والاتجار بالبشر، ولذلك نص القانون المصري صراحة على الرجوع إلى نصوص قانون العقوبات أو أي قانون وطني آخر في حال عدم توافر صور التجريم في جرائم تقنية المعلومات، تطبيقاً لحالة التعدد المعنوي للجرائم التي ورد النص عليها في المادة (٣٢) عقوبات، ويعرف التعدد المعنوي للجرائم بأنه ارتكاب الجاني فعلاً إجرامياً واحداً ينطبق عليه أكثر من نص عقابي، ومن ثم تقوم به أكثر من جريمة، لما ينطوي عليه من تعدد في التكييفات القانونية[٣]،ومن ثم فإن المحكمة إذا أدانت الشخص في جريمتين وكانت العقوبة للجريمة الأولى أشد من عقوبة الجريمة الثانية وطبقت حكم المادة ٣٢ من قانون العقوبات ووقعت على المحكوم عليه عقوبة الجريمة الأولى الأشد، فإن الحكم يكون قد طُبق تطبيقاً صحيحاً[٤]،وتبرز الإشارة في هذا المقام إلى تأكيد المشرع المصري على احترام أحكام قانون الطفل فيما يقرره من أحكام جنائية مخففة لصالح الأطفال وهم كل من لم يبلغ الثامنة عشرة من العمر(م٢).

---

[١] ومن التشريعات المقارنة التي حرصت على التأكيد على مبدأ عدم الإخلال بالعقوبة الأشد في الجرائم المعلوماتية في حالة التعدد المعنوي كل من التشريع الإماراتي (م٤٨)، والتشريع البحريني(المواد أرقام ٤ و٥ و١٠)، والتشريع القطري(م٤٤).

[٢] د. عبد العظيم وزير: شرح قانون العقوبات- القسم العام، النظرية العامة للجريمة، القاهرة، دار النهضة العربية، ط٦، ٢٠٠٨، ص٥.

[٣] د. أحمد عوض بلال: مبادئ قانون العقوبات المصري- القسم العام، مرجع سابق، ص٩٤٩ وما بعدها.

[٤] انظر: الطعن رقم ٢١٥٣ لسنة ٨٠ق جلسة ٢٠١١/٥/٤، المستحدث من المبادئ الصادرة عن الدوائر الجنائية من أول أكتوبر ٢٠١٠ لغاية آخر سبتمبر ٢٠١١، الصادرة عن المكتب الفني لمحكمة النقض، المجموعة الجنائية، ص١٨٣.

ثانياً- حالات تشديد العقاب في الجرائم المعلوماتية:تطرق الفصل السادس من القانون إلى الظروف المشددة في الجريمة، حيث نصت المادة (٣٤) على أنه:" *إذا وقعت أي جريمة من الجرائم المنصوص عليها في هذا القانون بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر أو الإضرار بالأمن القومي للبلاد أو بمركزها الاقتصادي أو منع أو عرقلة ممارسة السلطات العامة لأعمالها أو تعطيل أحكام الدستور أو القوانين أو اللوائح أو الإضرار بالوحدة الوطنية والسلام الاجتماعي، تكون العقوبة السجن المشدد*"، ومن ثم حدد القانون الظروف المشددة في الجرائم المعلوماتية، وهي جميعاً من الظروف المادية، ذات الصلة بماديات الجريمة، وتتسم هذه الظروف بطابع مشترك في أنها تمثل اعتداءً على الدولة أو المجتمع ككل، ومن ثم تشدد العقوبة في الجرائم المعلوماتية المنصوص عليها في القانون إذا كان الغرض من ارتكابها تحقيق مايلي:-

أ) الإخلال بالنظام العام:يقصد بذلك النظام العام في الدولة بجوانبه المختلفة الأخلاقية والاجتماعية والاقتصادية والسياسية،ويتسع مدلول النظام العام ليشمل مدلولات الأمن العام والصحة العامة والسكينة العامة، وهو مدلول مرن يختلف بحسب الزمان والمكان، وقد انتقد البعض[١]استخدام المشرع لعناصر الإخلال بالنظام العام وتعريض سلامة وأمن المجتمع للخطر في تعريف جريمة الإرهاب، بالنظر إلى أنهما لا يصلحان ضابطاً لتمييز هذه الجريمة، فكافة الجرائم يستهدف بها الجناة الإخلال بالنظام العام كما أنها تؤدي إلى تعريض سلامة المجتمع وأمنه للخطر، كما أن هناك الكثير من الأفعال التي يصعب استخلاص هذا القصد فيها كجريمة مقاومة السلطات التي ينطوي

[١] د. أشرف توفيق شمس الدين: السياسة التشريعية لمكافحة الإرهاب ومدى اتفاقها مع أصول الشرعية الجنائية-دراسة نقدية للقانون المصري، القاهرة، دار النهضة العربية،٢٠٠٦، ص١٣.

على إخلال بالنظام العام دون أن يكون عملاً إرهابياً وجريمة تخريب وسائل الإنتاج والممتلكات العامة (٨٩ و ٩٠عقوبات) التي لا تعتبر في نظر المشرع من جرائم الإرهاب[١]، ومن ناحية ثانية، لا يعد الإخلال بالنظام العام وتعريض أمن المجتمع من الوقائع المحددة التي تصلح لأن تشكل قصداً جنائياً خاصاً في جرائم الإرهاب، كما أنهما يتسمان بالمرونة الاتساع، وهو ما يتعارض مع الأصول الدستورية المستقر عليها من أن تكون أركان الجريمة واضحة وبعيدة عن الغموض والالتباس، كما أن فكرة النظام العام هي فكرة نسبية تتغير بتغير الزمان والمكان والفلسفات السياسية والاجتماعية والاقتصادية التي تسود في المجتمع، ومن ثم يصعب تحديد مدلولها أو الوقوف على محتواها، كما أن عدم وضوح مدلول النظام العام من شأنه صعوبة إثبات القصد الجنائي الخاص في جريمة الإرهاب[٢].

ب) تعريض سلامة المجتمع وأمنه للخطر: يقصد بتعريض سلامة المجتمع للخطر تعطيل مظاهر الحياة العادية في الدولة، أما تعريض الأمن للخطر يقصد به زعزعة السكينة لدى أفراد المجتمع سواء انصب ذلك على أشخاصهم أو على أموالهم، ويكفي أن يكون من شأن الإرهاب تعريض سلامة المجتمع وأمنه للخطر فلا يلزم أن يحدث الخطر فعلاً.

ج) الإضرار بالأمن القومي للبلاد أو بمركزها الاقتصادي:يقصد بالإضرار بالأمن القومي بمدلوله الموسع الذي يشمل الأمن الداخلي والخارجي، وقد عرف القانون الأمن القومي بأنه:"كل ما يتصل باستقلال وأمن الوطن ووحدته وسلامة أراضيه، وما يتعلق بشئون رئاسة الجمهورية ومجلس الدفاع الوطني ومجلس الأمن

---

[١] المرجع السابق، ص١٤.

[٢] المرجع السابق، ص١٣.

القومي، والقوات المسلحة والإنتاج الحربي، ووزارة الداخلية، والمخابرات العامة، وهيئة الرقابة الإدارية، والأجهزة التابعة لتلك الجهات"، بينما يقصد بالإضرار بالمركز الاقتصادي للبلاد، كأن تمس بطاقة البلاد الإنتاجية أو تؤثر على قيمة نقدها أو تضر بالمصلحة القومية، وهى أية مصلحة تمس الشعب أو قطاعاً منه[1].

د) منع أو عرقلة ممارسة السلطات العامة لأعمالها: يقصد به تعطيل السلطات أو منعها على ممارستها أعمالها الدستورية والقانونية، ويستوي في ذلك السلطة التشريعية أو التنفيذية أو القضائية، أو منع أو عرقلة دور العبادة عن ممارسة الشعائر الدينية، وكذلك منع المؤسسات التعليمية والدينية عن القيام بدورها.

هـ) تعطيل أحكام الدستور أو القوانين أو اللوائح: مثل استخدام القوة لمنع رئيس الجمهورية عن ممارسة سلطاته الدستورية أو منع إجراء الانتخابات.

و) الإضرار بالوحدة الوطنية والسلام الاجتماعي: وقد عرفت المادة الأولى من القانون رقم (٣٤) لسنة ١٩٧٢ بشأن حماية الوحدة الوطنية، الوحدة الوطنية بأنها هي:" الوحدة القائمة على احترام نظام الدولة والمقومات الأساسية للمجتمع، كما حددها الدستور وعلى وجه الخصوص، ١- تحالف قوى الشعب العاملة. ٢- تكافل الفرص والمساواة بين المواطنين في الحقوق والواجبات العامة. ٣- حرية العقيدة وحرية الرأي بما لا يمس حرية الآخرين أو المقومات الأساسية للمجتمع. ٤- سيادة القانون. وتقوم الوحدة الوطنية على أساس إعطاء الأولوية دائماً لأهداف النضال

[1] تجدر الإشارة إلى اعتداد المشرع بالإضرار المركز الاقتصادي للبلاد كأحد الشروط المشددة في جريمة اختلاس المال العام إذا ارتكبت الجريمة في زمن الحرب وترتب عليها إضراراً بمركز البلاد الاقتصادي أو بمصلحة قومية لها، وذلك بقانون العقوبات في مادته ١١٢عقوبات. انظر: د. محمد السعيد عبد الفتاح: شرح قانون العقوبات- القسم الخاص، الجرائم المضرة بالمصلحة العامة، القاهرة، دار النهضة العربية، بدون سنة نشر، ص١٤٠.

الوطني والتحرري وعلى أفضلية المصالح القومية الشاملة على المصالح الخاصة لكل قوة أو طائفة أو فئة اجتماعية"، بينما السلام الاجتماعي فيقصد به توافر الطمأنينة والسكون والألفة بين المواطنين والقضاء على الكراهية والحقد بينهم وعدم اللجوء إلى وسائل غير سلمية لحل مشاكل الجماهير، ومن ثم فأي إضرار بالوحدة الوطنية أو السلام الاجتماعي، كإشاعة الفتنة الطائفية بين طوائف الشعب المختلفة، فإن ذلك من شأنه تحقق الظرف المشدد للعقاب في مثل هذه الجرائم.

طبيعة الظروف المشددة: اعتبر المشرع الظروف السابقة من الظروف التي تغير من وصف الجريمة من الجنحة إلى الجناية، وعاقب على توافرها بالسجن المشدد.

المطلب الثاني

المسئولية الجنائية للشخص الاعتباري

تناول الفصل السابع من القانون المسئولية الجنائية للشخص الاعتباري، وباستعراض نصوص المواد أرقام (٣٦-٣٨)، نجدها تتحدث عن المسئولية الجنائية للأشخاص الطبيعية من المسئولين عن الإدارة الفعلية للشخص الاعتباري عن عدم الإبلاغ عن الجرائم المعلوماتية التي تتعرض لها المواقع والحسابات والبريد الإلكتروني المخصص للكيان الذي يديره، وكذلك المسئولية الجنائية للأشخاص الطبيعية المسئولة عن الإدارة الفعلية للشخص الاعتباري، فضلاً عن العقوبات المقررة على الشخص الاعتباري ذاته، وأخيراً الإشارة إلى أن تقرير مسئولية الإدارة الفعلية للشخص الاعتباري استبعاد المسئولية الجنائية للأشخاص الطبيعيين المشاركين في الجريمة، وهو ما سوف نتناوله على النحو التالي:-

أولاً- صور المسئولية الجنائية: يعرف القانون الجنائي صورتين للمسئولية الجنائية:(الأولى) هي المسئولية الجنائية للأشخاص الطبيعيين، (والثانية) هي

المسئولية الجنائية للأشخاص الاعتبارية[١]، والأخيرة هي الصورة الأحدث في القانون الجنائي، فالقانون الجنائي استناداً إلى مبدأ شخصية العقوبة يفترض مسائلة الشخص مرتكب الجرم، وأن الأشخاص الاعتبارية لا تسأل جنائياً عما يقع من ممثليها من جرائم أثناء قيامهم بأعمالها، على أن الذي يسأل مرتكب الجريمة منهم شخصياً، إلا أن التطور الحادث في قواعد القانون الجنائي أجاز الاعتداد بالمسئولية الجنائية للأشخاص الاعتبارية، ويرجع إقرار المسئولية الجنائية للأشخاص الاعتبارية إلى ما تضمنته المادة (١٠) من اتفاقية الأمم المُتحدة لمُكافحة الجريمة المنُظمة من النص على مبدأ المسئولية الجنائية للأشخاص الاعتبارية المشاركة في الجرائم الخطيرة التي تضطلع بها جماعة إجرامية منظمة والجرائم المنصوص عليها في هذه الاتفاقية[٢].

وعلى الرغم من أن الأصل العام في القانون الجنائي المصري هو الاعتداد بالمسئولية الجنائية للأشخاص الطبيعيين[٣]، إلا أن المشرع المصري قد أخذ بمبدأ

---

[١] يقصد بالأشخاص الاعتبارية المقصودة في القانون الجنائي هي الأشخاص الاعتبارية الخاصة وليست العامة، ويقصد بها " كل مجموعة من الأشخاص الطبيعيين بهدف معين ونشاط محدد، أو تجمع أموال رصدت لنشاط بعينه، اعتبر لها القانون بالشخصية القانونية في حدود مباشرة النشاط المنشأة من أجله باستقلال عن الأشخاص الطبيعيين المكونين له".

[٢] تشترط المادة العاشرة من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة أن تعتمد كل دولة طرف ما قد يلزم من تدابير، بما يتفق مع مبادئها القانونية، لإرساء مسئولية الهيئات الاعتبارية عن المشاركة في الجرائم الخطيرة، التي تكون ضالعة فيها جماعة إجرامية منظمة، والأفعال المجرمة وفقا للمواد ٥ و٦و٨ و٢٣ من هذه الاتفاقية. وتنص الفقرة الثانية من المادة المذكورة على أنه، رهنا بالمبادئ القانونية للدولة الطرف، يجوز أن تكون مسؤولية الهيئات الاعتبارية جنائية أو مدنية أو إدارية.

[٣] انظر: الطعن رقم ٦١٩٧ لسنة ٥٢جلسة ١٩٨٣/٢/٦ س ٣٤ ق رقم ٣٧ص٢٠٢.

المسئولية الجنائية للأشخاص الاعتبارية حديثاً في جرائم بعينها[١]، من بينها جرائم تقنية المعلومات، فالمشرع المصري لم يقتصر على النص على المسئولية للأشخاص الطبيعيين؛ وإنما نص على تقرير المسئولية الجنائية للأشخاص الاعتبارية والمسئولية الجنائية لممثليهم.

ويشترط الفقه الجنائي[٢]والقضاء[٣]للاعتداد بالمسئولية الجنائية للأشخاص الاعتبارية ضرورة توافر شرطين: (الأول) أن يكون ارتكاب الجريمة بواسطة أحد أعضاء الشخص الاعتباري أو أحد ممثليه، (والثاني) أن يكون ارتكاب الجريمة لصالح وحساب الشخص الاعتباري، والمسئولية الجنائية للشخص الاعتباري في القانون المصري مسئولية مباشرة؛ لا تتوقف عند ثبوت مسئولية أحد العاملين به أو صدور

---

(١) ومن أبرز الجرائم التي أخذ فيها المشرع المصري بالمسئولية الجنائية للأشخاص الاعتبارية جرائم الاتجار بالبشر وتهريب المهاجرين (م١١) من القانون ٦٤ لـ٢٠١٠، (م١٤) من القانون ٨٢ لـ٢٠١٦.

(٢) د. عمر سالم: المسئولية الجنائية للأشخاص الاعتبارية، القاهرة، دار النهضة العربية، ١٩٩٥، ص٧.

(٣) تذهب أحكام محكمة النقض الفرنسية إلى أنه:" وفقاً لأحكام المادة ٢١٢-١ من قانون العقوبات الفرنسي فإنه لا يمكن اعتبار الأشخاص الاعتبارية مسئولين جنائياً، إلا إذا ثبت أن مخالفة ارتكبت لحسابهم من طرف هيئاتهم أو ممثليهم، وتفرض هذه الآلية أن المخالفة المسندة للشخص الاعتباري موصوفة بكل عناصرها، خاصة العنصر المعنوي، على أنها تمت على يد إحدى هيئات الشخص الاعتباري أو أحد ممثليه". انظر حكم الغرفة الجنائية الصادر في١٩٩٧/١٢/٢. Cass. Crim., 2nd Dec. 1997.

وفي حكم آخر قضت المحكمة بأنه:" تنص المادة ١٢١-٢ من قانون العقوبات الفرنسي على أن المسئولية الجنائية للأشخاص الاعتبارية لا تنطبق إلا على المخالفات المرتكبة لحسابهم من طرف هيئاتهم أو ممثليهم. وفي حال المخالفة المبينة، يمنع إعفاء هيئة الشخص الاعتباري أو ممثله شخصياً من البحث عن المسئولية الجنائية للشخص الاعتباري عن الأفعال التي يكون هذا الممثل قد ارتكبها لحساب الشخص الاعتباري". انظر حكم الغرفة الجنائية الصادر في ٢٠٠٤/٩/٨. Cass. Crim., 8th Sep.2004.

حكم جنائي عليه، كما أن المسئولية الجنائية للشخص الاعتباري لا تخل بالمسئولية الجنائية للشخص الطبيعي الذي يمكن أن يتم تحريك الدعوى الجنائية بشأنه أيضاً رغم تحريكها ضد الشخص الاعتباري[١]، وهو الأمر المستقر عليه دولياً وفقاً لأحكام المادة (٣/١٠) من اتفاقية الأمم المُتحدة لمُكافحة الجريمة المنُظمة[٢]، وهو ما أخذت به كذلك المادة (٣٧) من قانون مكافحة جرائم تقنية المعلومات، والتي تقضي بأنه: "*في تطبيق أحكام هذا القانون، لا يترتب على تقرير مسئولية الإدارة الفعلية للشخص الاعتباري استبعاد المسئولية الجنائية للأشخاص الطبيعيين الفاعلين الأصليين أو الشركاء عن ذات الوقائع التي تقوم بها الجريمة*"، ويشير جانب مهم من الفقه الجنائي[٣] إلى أن المسئولية الجنائية للشخص الاعتباري لا يجب أن تؤسس على مسئولية الشخص الطبيعي الذي يعمل لديه، بل يجب أن يثبت أن ما قام به الشخص الطبيعي من أفعال تمت باسمه أو نيابة عنه.

ثانياً- جريمة عدم الإبلاغ عن الجرائم المعلوماتية التي تقع على المواقع أو الحسابات الخاصة أو البريد الإلكتروني أو الأنظمة المعلوماتية:

نص التجريم: تنص المادة (٣٥) من القانون على أنه:" *يعاقب بالحبس مدة لا ل عن ثلاثة أشهر، وبغرامة لا تقل عن ثلاثون ألف جنيه ولا تزيد عن مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل مسئول عن الإدارة الفعلية لأي شخص اعتباري*

---

[١] تقرر محكمة النقض بأن مسئولية عمال الشخص الاعتباري وممثليه عن أفعالهم الشخصية ولو كانت لمصلحة الشخص الاعتباري الذي يمثله وباسمه. انظر: الطعن ١٣٧٠٨ لسنة ٧٥ ق جلسة ٢٠١٢/١١/١، المستحدث من المبادئ الصادرة عن الدوائر الجنائية من أول أكتوبر ٢٠١٢ لغاية آخر سبتمبر ٢٠١٣، الصادرة عن المكتب الفني لمحكمة النقض، المجموعة الجنائية، ص٥١.

[٢] نصت المادة (٣/١٠) من اتفاقية الأمم المُتحدة لمُكافحة الجريمة المنظمة على أن:" لا تخل هذه المسئولية بالمسئولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجرائم المشار إليها".

[٣] د. أحمد فتحي سرور: القانون الجنائي الدستوري، القاهرة، دار الشروق،١٩٩١، ص٢٣٠.

إذا تعرض الموقع أو الحساب الخاص أو البريد الإلكتروني أو النظام المعلوماتي المخصص للكيان الذي يديره لأي جريمة من الجرائم المنصوص عليها في هذا القانون ولم يبلغ بذلك الجهات الرسمية المختصة وقت علمه بالجريمة".

العلة من التجريم: تتمثل العلة من التجريم في مواجهة تقاعس الأشخاص المسئولين عن الإدارة الفعلية للشخص الاعتباري عن الإبلاغ عن الجرائم المعلوماتية للسلطات الرسمية.

صفة الجاني: تتطلب القانون أن يكون الجاني مسئولاً عن الإدارة الفعلية للشخص الاعتباري، ومن ثم إذا لم يكن الشخص من المسئولين عن الإدارة الفعلية للشخص الاعتباري، فلا تتحقق صفة التجريم في سبيله.

محل الجريمة: تتطلب القانون أن تقع الجريمة على المواقع أو الحسابات الخاصة أو البريد الإلكتروني أو الأنظمة المعلوماتية للشخص الاعتباري، والشخص الاعتباري المقصود في هذه الجريمة هو الشخص الاعتباري الخاص، كالشركات والمؤسسات التجارية، ومن ثم يخرج من نطاق التجريم الأشخاص الاعتبارية العامة.

الركن المادي: يتحقق الركن المادي في الجريمة بفعل عدم الإبلاغ عن الجرائم المعلوماتية، وتفترض هذه الجريمة وقوع إحدى الجرائم المعلوماتية الواردة بالقانون على المواقع أو الأنظمة المعلوماتية التي تخص الشخص الاعتباري الخاص، وأن يصل العلم بوقوع هذه الجريمة لدى المسئول عن الإدارة الفعلية للشخص الاعتباري، فيتخذ سلوك سلبي يتمثل في عدم إخبار الجهات الرسمية المختصة بنبأ وقوع هذه الجرائم على الرغم من علمه بذلك، ويستوي لدى القانون الباعث على عدم قيام الجاني بالإبلاغ للجهات الرسمية، سواء أكان الخوف من الإساءة إلى سمعة الشخص الاعتباري أم غير ذلك، ويستوي في نظر القانون أن تقع الجريمة تامة، أو تقف عند حالة الشروع، فتقع

جريمة الامتناع عن الإبلاغ لو علم الشخص بشروع المتهم في ارتكاب الجريمة المعلوماتية، ولم يقم بإبلاغ السلطات بشأنه.

الركن المعنوي: هذه الجريمة من الجرائم العمدية التي يتطلب فيها القانون توافر القصد الجنائي العام بعنصريه العلم والإرادة، بأن يعلم الجاني بوقوع جريمة من الجرائم المنصوص عليها في القانون على المواقع الإلكترونية أو الحسابات الخاصة أو البريد الإلكتروني أو النظم المعلوماتية المخصصة للكيان الذي يديره، وأن تتجه إرادته إلى عدم إبلاغ الجهات الرسمية، أياً كان الباعث على ذلك، فالباعث لا يعد من عناصر الركن المعنوي للجريمة[1].

العقوبة: عاقب المشرع المصري على عدم إبلاغ المسئول عن الإدارة الفعلية للشخص الاعتباري عن الجرائم المعلوماتية بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن ثلاثون ألف جنيه ولا تزيد عن مائة ألف جنيه، أو بإحدى هاتين العقوبتين، ومن ثم يجوز لقاضي الحكم بالحبس أو الغرامة أو بالعقوبتين معاً، كما يجوز للقاضي الحكم بإيقاف التنفيذ، إعمالاً لحكم المادة ٥٥ عقوبات.

ثالثاً- العقوبات المقررة للمسئول عن الإدارة الفعلية للشخص الاعتباري: تنص المادة (٣٧) من قانون مكافحة جرائم تقنية المعلومات على المساواة في العقوبة بين المسئول عن الإدارة الفعلية للشخص الاعتباري والعقوبة المقررة للفاعل الأصلي للجريمة، وقد تطلب القانون لتقرير مسئولية الشخص المسئول عن الإدارة الفعلية للشخص الاعتباري توافر أحد شرطين: الأول يتمثل في أن يثبت علم الشخص المسئول عن الإدارة الفعلية بوقوع إحدى الجرائم المنصوص عليها في هذا القانون، وهو ما

[1] نقض ١٩٦٩/١٢/١، مجموعة أحكام محكمة النقض، س٢٠، ق٢٧٣، ص١٣٤٤.

يجوز إثباته بكافة طرق الإثبات، ومن بينها شهادة الشهود، بينما يتمثل الشرط الآخر في أن يقوم هذا الشخص بتسهيل ارتكاب إحدى الجرائم المنصوص عليها في القانون، تحقيقاً لمصلحة له أو لغيره، ويقصد بتسهيل ارتكاب الجريمة، أي فعل إيجابي أو سلبي من شأنه مساعدة الجناة على تنفيذ إحدى الجرائم المعلوماتية، ويستوي لدى القانون أن يكون هذا التسهيل تحقيقاً لمصلحة الشخص الاعتباري أو غيره، وهو ما أشارت إليه الفقرة الأولى من المادة (٣٦) من قانون مكافحة جرائم تقنية المعلومات، من أنه:" *في الأحوال التي ترتكب فيها أي من الجرائم المنصوص عليها في هذا القانون باسم ولحساب الشخص الاعتباري، يعاقب المسئول عن الإدارة الفعلية إذا ثبت مه بالجريمة أو سهل ارتكابها تحقيقاً لمصلحة له أو لغيره بذات عقوبة الفاعل الأصلي*".

العقوبات المقررة للأشخاص الاعتبارية في الجرائم المعلوماتية[1]: تنص الفقرة الثانية من المادة (٣٦) من القانون على أنه:" *وللمحكمة أن تقضى بإيقاف ترخيص مزاولة الشخص الاعتباري للنشاط مدة لا تزيد على سنة، ولها في حالة العود أن تحكم بإلغاء الترخيص أو حل الشخص الاعتباري بحسب الأحوال، ويتم نشر الحكم في جريدتين يوميتين واسعتي الانتشار على نفقة الشخص الاعتباري*"، ومن ثم يتضح

[1] ومن التشريعات المقارنة التي نصت على المسئولية الجنائية للأشخاص الاعتبارية في الجرائم المعلوماتية كل من التشريع الفرنسي والكويتي والبحريني والقطري، حيث تقضي المادة (٣٢٣-٦) عقوبات فرنسي على أنه: "تتحمل الأشخاص الاعتبارية المسئولية الجنائية في إطار الشروط المنصوص عليها في المادة ١٢١-٢ في الجرائم المحددة في هذا القسم إضافة إلى الغرامة وفقاً لأحكام المادة ١٣١-٣٨ والعقوبات المقررة في المادة ١٣١-٣٩. والحظر المذكور في الفقرة الثانية من المادة ١٣١-٣٩ ينطبق على النشاط أثناء وبمناسبة ارتكاب الجريمة"، فضلاً عن كل من (م١٤) من التشريع الكويتي، (م ٢١) من التشريع البحريني، (م٤٨) من التشريع القطري، وتبرز الإشارة إلى أن هذه التشريعات قد تأثرت في تقريرها للمسئولية الجنائية للأشخاص الاعتبارية بنص المادة ٢٠ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

من النص السابق، أن العقوبات التي قررها المشرع في مواجهة الشخص الاعتباري، وهي عقوبات (نشر الحكم الصادر بالإدانة- إيقاف الترخيص المؤقت- إلغاء الترخيص للشخص الاعتباري)، وذلك على النحو التالي:-

أ) عقوبة إيقاف ترخيص مزاولة النشاط المؤقت للشخص الاعتباري:أجاز قانون مكافحة جرائم تقنية المعلومات للمحكمة أن تقضي بإيقاف ترخيص مزاولة النشاط للشخص الاعتباري لمدة لا تتجاوز سنة، وهي من التدابير الجنائية التي تستهدف ردع الشخص المسئول عن الإدارة الفعلية للشخص الاعتباري عن ارتكاب الجرائم المعلوماتية، من خلال إيقاف مزاولة النشاط المؤقت للشخص الاعتباري، وقد حدد المشرع مدة وقف النشاط للشخص الاعتباري بألا تتجاوز سنة واحدة، وهي عقوبة جوازية للمحكمة، ولها سلطة تقديرية في تحديد مدة العقوبة المحكوم بها وفقاً لظروف وملابسات القضية.

ب) عقوبة إلغاء ترخيص مزاولة النشاط للشخص الاعتباري أو حله:كما أجاز القانون للمحكمة في حالة العود أن تقضي بإلغاء ترخيص مزاولة النشاط للشخص الاعتباري أو حله بحسب الأحوال، وهي عقوبة يترتب عليها إنهاء نشاط الشخص الاعتباري مستقبلاً، وهي عقوبة مشددة قررها المشرع في حال قيام أحد العاملين بالشخص الاعتباري بتكرار ارتكاب جرائم تقنية المعلومات باسم الشخص الاعتباري ولصالحه، فإذا ارتكب الشخص إحدى الجرائم المعلوماتية للمرة الأولى فإن القاضي يحكم بعقوبة إيقاف الترخيص المؤقت لنشاط الشخص الاعتباري، وإذا تكرر منه ذلك مرة أخرى، فإن القاضي يقضي بعقوبة إلغاء الترخيص أو الحل، وهي عقوبة جوازية للمحكمة[1].

---

[1] ومن الجدير بالذكر أن المشرع المصري قد أخذ بالعقوبات ذاتها المقررة على الأشخاص الاعتبارية في جرائم الاتجار بالبشر وتهريب المهاجرين، إلا أنه توسع في الأخيرة لتشمل عقوبة حل الشخص الاعتباري أو تصفيته.

ج) عقوبة نشر الحكم الصادر بالإدانة:أشار القانون إلى عقوبة نشر الحكم الصادر بالإدانة على نفقة الشخص الاعتباري في جريدتين يوميتين واسعتي الانتشار، وعقوبة النشر هي عقوبة تكميلية وجوبية يقضى بها في جميع الأحوال على النحو الذي نظمه القانون بأن يتم النشر في جريدتين يوميتين واسعتي الانتشار على نفقة المحكوم عليه، ومن ثم يجب أن يبين الحكم اسم الجريدتين اللتين سيتم النشر فيهما، فإذا قضى الحكم بالنشر دون بيان اسم الجريدتين، فإنه يكون قد خالف القانون[١]، وعقوبة النشر هي من العقوبات الماسة بالشرف والاعتبار، التي تستهدف إلصاق وصمة بسمعة المحكوم عليه أو الحط من منزلته أمام الناس، وتجدر الإشارة إلى أن نشر حكم الإدانة قد يؤدي إلى ردع القائمين على الشخص الاعتباري من خلال ما قد يؤدي إليه ذلك من إضرار بالمركز المالي للشخص الاعتباري والتأثير في إيراداته، وهي عقوبة لا شك في تحقيقها لقدر من الردع العام في مواجهة المجرمين المحتملين، لا سيما إذا كان نجاحهم في الحياة المهنية يرتبط بحسن السمعة[٢].

المطلب الثالث

العقوبات التبعية

أشار الفصل الثامن من القانون المعنون إلى"العقوبات التبعية" المقررة في الجرائم المعلوماتية، وقد ساير قانون مكافحة جرائم تقنية المعلومات نهج قانون العقوبات، بالنص على العقوبات التبعية، وقد مزج في هذا الموضع بين العقوبات

---

[١] أنظر: الطعن رقم ١٢٩٣٦ لسنة ٤ق جلسة ٢٠١٣/٧/٤، المستحدث من المبادئ الصادرة عن الدوائر الجنائية من أول أكتوبر ٢٠١٢ لغاية آخر سبتمبر ٢٠١٣، الصادرة عن المكتب الفني لمحكمة النقض، المجموعة الجنائية، ص٢٥٧.

[٢] د. أحمد عوض بلال: مبادئ قانون العقوبات المصري، مرجع سابق، ص٧٨١.

التبعية والتكميلية؛ إذ عبر عنها جميعاً بعنوان "العقوبات التبعية"[١]،إلا أن الباحث يرى أنه كان الأحرى بالمشرع تسمية هذا الفصل بالعقوبات التكميلية بالنظر إلى أن عقوبات المصادرة والعزل وغلق المحل من العقوبات التكميلية الواردة في قانون العقوبات والقوانين الجنائية الخاصة، وفيما يلي نتناول هذه العقوبات على النحو التالي[٢]:-

أولاً- المصادرة: تنص الفقرة الأولى من المادة (٣٨) من القانون على أنه: "***مع عدم الإخلال بحقوق الغير حسن النية،على المحكمة في حالة الحكم بالإدانة في أي جريمة من الجرائم المنصوص عليها في هذا القانون أن تقضي بمصادرة الأدوات***

---

[١] تكلم الشارع عن العقوبات التبعية في القسم الثاني من الباب الثالث من الكتاب الأول من قانون العقوبات، وقد مزج في هذا الموضع بين العقوبات التبعية والعقوبات التكميلية إذ عبر عنها جميعًا بعنوان "الجريمة التبعية"، رغم ما يميز هذين النوعين. فالعقوبات التبعية في المعنى الاصطلاحي تتميز بأنها تلحق المحكوم عليه بصفة حتمية أي بقوة القانون، وكنتيجة للحكم عليه ببعض العقوبات الأصلية، دون حاجة إلى أن ينص عليها القاضي في حكمه، بينما العقوبات التكميلية يجب أن ينص عليها الحكم لإمكان توقيعها على المحكوم عليه، وهي تلحق أنواعًا معينة من الجرائم.

[٢] ومن التشريعات المقارنة التي نصت على العقوبات التكميلية في الجرائم المعلوماتية التشريع الفرنسي والإماراتي والكويتي والقطري والنظام السعودي، حيث تقضي المادة (٣٢٣-٥) عقوبات فرنسي بأنه: يتحمل الأشخاص الطبيعيون المدانون بارتكاب الجرائم المنصوص عليها في هذا الفصل أيضاً بالعقوبات التكميلية التالية: ١- الحرمان لمدة خمس سنوات من مباشرة الحقوق المدنية، والمدنية المتصلة بالعائلة وفقاً لأحكام المادة ١٣١-٢٦. ٢- الحرمان لمدة خمس سنوات من شغل الوظائف العامة أو ممارسة نشاط مهني أو اجتماعي والتي تمت بسبب أو بمناسبة ارتكاب الجريمة. ٣- مصادرة الأشياء التي استخدمت أو كان ينوى استخدامها في ارتكاب الجريمة أو تلك التي نجمت عنها، مع استثناء المواد الخاضعة للتعويض. ٤- الغلق لمدة خمس سنوات للمحل أو المحال التي استخدمت في ارتكاب الجريمة. ٥- المنع لمدة خمس سنوات من المشاركة في أعمال المناقصات والمزايدات العامة. ٦- الحظر لمدة خمس سنوات من إصدار شيكات غير تلك التي تسمح للساحب باسترداد ماله لدى المسحوب عليه أو الشيكات المعتمدة. ٧- نشر الحكم وفقاً للمادة ١٣١-٣٥"، فضلاً عن كل من التشريع الإماراتي (م٤١)، والتشريع الكويتي(م١٣)، التشريع القطري (م٥٣)، النظام السعودي (م١٣).

الآلات والمعدات والأجهزة مما لا يجوز حيازتها قانوناً، أو غيرها مما يكون قد استخدم في ارتكاب الجريمة، أو سهل أو ساهم في ارتكابها "[١].

ويقصد بالأدوات الأشياء التي استعملت في ارتكاب الجريمة، بينما يقصد بالآلات والمعدات والأجهزة كل وسيلة مصنعة أو تقنية تستخدم في ارتكاب الجرائم المنصوص عليها في القانون، ولم يشترط المشرع لوجوب المصادرة إلا أن تكون هذه الأدوات أو الآلات أو المعدات أو الأجهزة قد استخدمت في ارتكاب الجريمة أو سهلت أو ساهمت في ارتكابها، وأن تكون حيازتها غير مشروعة، أن أي حيازتها أو إحرازها أو التعامل فيها يشكل جريمة.

طبيعة المصادرة في جرائم تقنية المعلومات: والمصادرة هي من العقوبات التكميلية التي أخذ بها المشرع المصري في قانون العقوبات(م١/٣٠) عقوبات، والتي جعلت مصادرة الأموال المضبوطة المتحصلة من جناية أو جنحة جوازية للقاضي، إلا أن المشرع ـخروجاً على القاعدة العامةـ قد جعل المصادرة وجوبية في قانون مكافحة جرائم تقنية المعلومات بنص القانون[٢].

---

[١] طالب أحد الأعضاء إضافة عبارة:"فضلاً عن مصادرة الأدوات والآلات والمعدات والأجهزة" قبل عبارة "مما لا يجوز حيازتها قانوناً"، وهو ما وافق عليه أعضاء البرلمان. انظر: مضبطة مجلس النواب المصري، الجلسة السادسة والخمسين، المعقودة في ٢٠١٨/٥/١٤م، مرجع سابق، ص ص١١٠-١١٣.

[٢] صار نقاش أثناء مناقشة قانون مكافحة جرائم تقنية المعلومات بالبرلمان حول طبيعة المصادرة، وهل يجب أن تكون وجوبية أم جوازية؟، حيث طالب السيد المستشار وزير شئون مجلس النواب بأن تكون المصادرة وجوبية، وذلك باستبدال كلمة (للمحكمة) الواردة في مشروع القانون بعبارة (على المحكمة)، وعلى الجانب الآخر كان يرى رئيس اللجنة المشتركة من لجنة الاتصالات وتكنولوجيا المعلومات ومكتبي لجنتي الشئون الدستورية والتشريعية والدفاع والأمن القومي ومقرر اللجنة أن تكون المصادرة جوازية للمحكمة، بالنظر إلى أن هذه المصادرة في بعض الأحيان قد تتسبب في مشكلة كبيرة إذا ما كانت هناك مجموعة من السيرفرات وتمت مصادرة أحدهم، وهو ما قد يترتب عليه هدم المنظومة بالكامل، ولذلك يكون من الأهمية إعطاء المحكمة سلطة جوازية =

العلة من تقرير عقوبة المصادرة: ترجع الحكمة من النص على مصادرة الأدوات والأجهزة والمعدات المستخدمة في ارتكاب الجرائم المعلوماتية في أن هذه الأجهزة والمعدات المستخدمة تنطوي على جانب من الخطورة، يلزم أن تتخذ حيالها تدابير وقائية تحول دون استعمالها مرة أخرى في ارتكاب الجريمة[١].

ومن ثم يحكم بالمصادرة في جميع الأحوال سواء قضي بإدانة المتهم أو ببراءته ما دام هذا الشرط قد تحقق، أما إذا لم يثبت استخدام الأداة أو الجهاز أو المعدة في ارتكاب الجريمة، فإنه لا يجوز الحكم بمصادرتها[٢]، وغني عن البيان أنه يجب – فيما يتعلق بمصادرة الأدوات والأجهزة المضبوطة التي استخدمت في ارتكاب الجريمة- عدم الإخلال بحقوق الغير حسن النية، فإذا كانت الأداة أو الجهاز قد استخدمت دون أن يكون صاحبها فاعلاً أو شريكاً في الجريمة، فإنه يجب ردها إلى مالكها حسن النية[٣].

ثانياً- غلق المحل أو الموقع: تنص الفقرة الثانية من المادة (٣٨) من القانون على أنه: "*وفي الحالات التي يتعين لمزاولة النشاط فيها الحصول على ترخيص من*

=

لتقدير مسألة المصادرة، من خلال الاستعانة بخبير ليقوم بتحديد ما إذا كانت المصادرة تؤثر على الهيكل العام للاتصالات أم لا؟، وقد وافق أعضاء البرلمان على استبدال عبارة "على المحكمة" بكلمة "للمحكمة"، ومن ثم إقرار مبدأ وجوبية المصادرة في جرائم تقنية المعلومات. انظر: مضبطة مجلس النواب المصري، الجلسة السادسة والخمسين، المعقودة في ٢٠١٨/٥/١٤م، مرجع سابق، ص ص١١٠-١١٣.

ومن الجدير بالذكر أن نهج المشرع في جعل المصادرة وجوبية سبق أن قرره في قانون مكافحة المخدرات (م٤٢)، وكذلك في قانون مكافحة الاتجار بالبشر (م١٣)، وقانون مكافحة الهجرة غير الشرعية وتهريب المهاجرين(م١٧).

[١] د. حسني الجندي: التشريعات الجنائية الخاصة، مرجع سابق، ص٢٧٠.

[٢] د. فوزية عبد الستار: شرح قانون مكافحة المخدرات، دار النهضة العربية، القاهرة، ١٩٩٠، ص١٠٢.

[٣] المرجع السابق، ص١٠٣.

إحدى الجهات الحكومية، وكان الشخص الاعتباري المُدان بأي جريمة منصوص عليها في هذا القانون لم يحصل على الترخيص فيحكم فضلاً عن العقوبات المقررة بالغلق"، ويتضح من النص السابق أن المشرع المصري أجاز الحكم بغلق المحل الخاص بالشخص الاعتباري، إذا لم يكن حاصلاً على ترخيص بمزاولة النشاط، من إحدى الجهات الحكومية، وترجع الحكمة في النص على غلق المحل أو الموقع في أنه كان وسيلة سهلت للجاني ارتكاب الجرائم المعلوماتية فيه، ومن ثم تحكم المحكمة بإغلاق المحل أو الموقع إذا كانت الجريمة قد ارتكبت بعلم مالكها، وذلك إغلاقاً كلياً أو للمدة التي تقدرها المحكمة[١].

وكان القضاء المصري والفرنسي قد اعتبر غلق المحل من التدابير الجنائية، حيث كانت محكمة النقض المصرية قد قضت في أحد أحكامها بأن:" الإغلاق ليس عقوبة من العقوبات الواجب توقيعها على من ارتكب الجريمة دون غيره، وإنما هو في حقيقته من التدابير الجنائية التي لا يحول توقيعها أن تكون آثارها قد تتعدى إلى الغير"[٢]، كما أنها قد قضت في حكم آخر بأن:" عقوبة إغلاق المحل... عن إدارة محل صناعي أو تجاري بغير ترخيص لا تعتبر عقوبة بحتة، لأنها لم تشرع للعقاب أو الزجر، وإن بدا أنها تتضمن معنى العقوبة، وإنما هي في حقيقتها من التدابير الوقائية"[٣]، بينما قضت محكمة النقض الفرنسية بأن إغلاق المحل يعد تدبيراً بوليسياً، ليس له غاية أكثر من وضع حد لمخالفات النظام العام[٤]، وتبرز الإشارة إلى أن القانون لم يبين مدة

---

[١] د. حسني الجندي: التشريعات الجنائية الخاصة، مرجع سابق، ص٢٧٠.

[٢] نقض ١٩٤٧/١٢/٢٢ مجموعة القواعد القانونية ج٢ ق٧٨ ص٨٥٧.

[٣] نقض ١٩٨١/١/١ مجموعة أحكام النقض س٣٢ ق١٣٢ ص٦٨٦؛ نقض١٩٨١/١/٢٢ ق٩ ص٦٨.

[4] Cass. Crim. 5th Mai1965, JCP, 1966, 1, No.14609, Note Legeus.

الغلق، وترك تقدير ذلك لقاضي الموضوع، فله أن يحكم بالغلق كلياً، أو يحدد له مدة معينة تقدرها المحكمة[١].

ثالثاً- العزل من الوظيفة: تنص المادة (٣٩) من القانون على عقوبة العزل من الوظيفة للجاني إذا كان موظفاً عاماً، حيث تقضي المادة المذكورة بأنه: "*للمحكمة إذا قضت بالإدانة على أحد الموظفين العموميين، لارتكابه جريمة من الجرائم المنصوص ليها في هذا القانون، أثناء وبسبب تأديته لوظيفته، أن تقضي بعزله من وظيفته مؤقتاً، إلا في الحالات المشار إليها في المادة (٣٤) من هذا القانون فيكون العزل وجوبياً*"[٢]، ومن ثم فجريمة العزل من الوظيفة تفترض أن الجاني موظفاً عاماً، فإذا الجاني لم يكن موظفاً عاماً، فإن هذه العقوبة لا يكون لها محل، والعزل هو حرمان المحكوم عليه من الوظيفة والمرتبات المقررة لها، والأصل في عقوبة العزل من الوظائف العامة أنها من العقوبات التبعية الواردة في المادة (٢٥) عقوبات فقرة أولى[٣]، والتى تقرر عقوبة العزل من الوظائف العامة لكل من يحكم عليه بعقوبة جناية، وهي من العقوبات التكميلية في جرائم اختلاس المال العام، بينما في جرائم تقنية المعلومات، فهي من العقوبات التكميلية، وهي عقوبة جوازية للقاضي، وتكون عقوبة العزل في هذه الحالة لمدة مؤقتة يحددها الحكم، اللهم في حال توافر أحد

---

[١] د. حسنى الجندي: التشريعات الجنائية الخاصة، مرجع سابق، ص٢٨٩.

[٢] تبرز الإشارة إلى أن النص المقترح بمشروع القانون لم يكن يتضمن كلمة "مؤقتاً"، إلا أن السيد المستشار وزير شئون مجلس النواب قد طالب بإضافة هذه الكلمة، بالنظر إلى أن العزل من الوظيفة يجب أن يكون مؤقتاً وليس مطلقاً. انظر: مضبطة مجلس النواب المصري، الجلسة السادسة والخمسين، المعقودة في ٢٠١٨/٥/١٤م، مرجع سابق، ص ص١١٣، ١١٤.

[٣] انظر: الطعن رقم٤١١٦ لسنة٨٠قجلسة ٢٠١١/١/١٠، المستحدث من المبادئ الصادرة عن الدوائر الجنائية من أول أكتوبر ٢٠١٠ لغاية آخر سبتمبر ٢٠١١، الصادرة عن المكتب الفني لمحكمة النقض، المجموعة الجنائية، ص ص١٦٣، ١٦٤.

الظروف المشددة الواردة في المادة ٣٤ من القانون، ففي هذه الحالة يكون العزل من الوظيفة العامة وجوبياً، وترجع العلة في تقرير هذه العقوبة إلى عدم صلاحية الشخص الذي يرتكب مثل هذه الجرائم من الاستمرار في خدمة الجهاز الإداري للدولة، نظراً لمخالفته لواجبات الوظيفة العامة وافتقاده للثقة الواجب توافرها في الموظفين العموميين.

المطلب الرابع

أحكام الشروع والإعفاء من العقاب

تضمن الفصل التاسع من القانون أحكام الشروع والإعفاء من العقاب، على النحو التالي:-

أولاً- الشروع في جرائم تقنية المعلومات:يقصد بحالة الشروع - وفقاً لنص المادة (٤٥) من قانون العقوبات المصري – البدء في تنفيذ فعل بقصد ارتكاب جناية أو جنحة إذا أوقف أو خاب أثره لأسباب لا دخل لإرادة الفاعل فيها"[1]، ويميز الفقه الجنائي في الشروع ما بين ثلاث صور للجريمة: الجريمة الموقوفة، وهي الجريمة التي يتجه فيها نشاط الجاني إلى تحقيق الجريمة ولكن لا يكتمل نشاطه لسبب خارج عن إرادته، كما في حال ضبطه قبل إتمام جريمته، والجريمة الخائبة التي يتجه فيها نشاط الجاني إلى تحقيق الجريمة ولكن يخيب أثره لسبب لا دخل لإرادة الجاني به، وأخيراً الجريمة المستحيلة، وهي الجريمة التي يتجه فيها نشاط الجاني إلى تحقيق الجريمة ولكن النتيجة الإجرامية لا تتحقق لاستحالة وقوعها.

---

[1] د. حامد راشد: شرح قانون العقوبات- القسم العام، النظرية العامة للجريمة، ج١، بدون دار نشر، ط١، ص١٨٧ وما بعدها.

والقاعدة في قانون العقوبات أنه لا عقاب على الشروع في الجنح إلا إذا نص المشرع صراحة على ذلك، أما جرائم الجنايات فيعاقب على الشروع فيها بعقوبة أخف من تلك المقررة للجريمة التامة وفقاً لأحكام المادة (٤٦) عقوبات، إلا أن المادة (٤٠) من القانون تضمنت حكماً مختلفاً عن القواعد العامة، يتضمن التشديد في مواجهة الجرائم المعلوماتية، من خلال المعاقبة على الشروع في ارتكاب جريمة من الجرائم المنصوص عليها بالقانون بنصف الحد الأقصى للعقوبة المقررة للجريمة التامة، إمعاناً منه في تقوية عنصر الردع العام إزاء جرائم قدر فيها خطورة خاصة[١]، حيث نصت المادة المذكورة على أنه:" *كل من شرع في ارتكاب الجنح المنصوص عليها في هذا القانون يعاقب بما لا يجاوز نصف الحد الأقصى للعقوبة المقررة للجريمة* "[٢].

ثانياً- الإعفاء من العقاب في جرائم تقنية المعلومات: تضمنت المادة (٤١) من القانون النص على الإعفاء من العقاب[٣]، حيث تقضي المادة المذكورة بأنه:" *يعفى*

---

(١) د. أحمد عوض بلال: مبادئ قانون العقوبات المصري، مرجع سابق، ص٣٨١.

(٢) يختلف موقف التشريعات المقارنة من المعاقبة على الشروع في الجريمة المعلوماتية ما بين تشريعات تعاقب على الشروع بالعقوبة ذاتها المقررة للجريمة التامة، ونذكر من هذه التشريعات التشريع الفرنسي، حيث تقضي المادة (٣٢٣-٧)عقوبات فرنسي بأنه: "يعاقب على الشروع في الجرائم المنصوص عليها في المواد ٣٢٣-١ إلى ٣٢٣-٣-١ بذات العقوبة المقررة تلك الجرائم"، بينما هناك جانب آخر من التشريعات المقارنة كالتشريع المصري والنظام السعودي يقرر للشروع في الجرائم المعلوماتية عقوبة أقل من العقوبة المقررة للجريمة التامة، حيث يعاقب التشريع المصري على الشروع بما لا يجاوز نصف الحد الأقصى للعقوبة المقررة للجريمة"، بينما تعاقب المادة العاشرة من النظام السعودي كل من شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة. وتبرز الإشارة إلى أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات قد نصت في الفقرتين الثانية والثالثة من مادتها التاسعة عشرة على تجريم الشروع والاشتراك في ارتكاب الجرائم.

(٣) طالب أحد أعضاء البرلمان منح المحكمة سلطة تخفيف العقاب بدلاً من الإعفاء، حتى لا يغري هذا النص الآخرين بارتكاب مثل هذه الجرائم، فضلاً عن أن القانون يعاقب من يشرع في ارتكاب إحدى الجرائم المعلوماتية بعقوبة تقدر بنصف الحد الأقصى المقرر لعقوبة هذه الجريمة، ولذلك يكون من =

من العقوبات المقررة للجرائم المنصوص عليها في هذا القانون كل من بادر من الجناة أو الشركاء إلى إبلاغ السلطات القضائية أو السلطات العامة بما يعلمه عنها قبل البدء في تنفيذ الجريمة وقبل كشفها.ويجوز للمحكمة الإعفاء من العقوبة أو التخفيف منها إذا حصل البلاغ بعد كشف الجريمة وقبل التصرف في التحقيق فيها إذا مكن الجاني أو الشريك،في أثناء التحقيق، السلطات المختصة من القبض على مرتكبي الجريمة الآخرين، أو على ضبط الأموال موضوع الجريمة، أو أعان أثناء البحث والتحقيق على كشف الحقيقة فيها، أو على القبض على مرتكبي جريمة أخرى مماثلة لها في النوع والخطورة.ولا يخل حكم هذه المادة، بوجوب القضاء برد المال المتحصل من الجرائم المنصوص عليها في هذا القانون"[١].

علة الإعفاء من العقاب: ترجع علة الإعفاء المقررة في هذا النص إلى رغبة المشرع في تشجيع الإبلاغ عن جرائم تقنية المعلومات سعياً وراء كشفها ومحاسبة مرتكبيها، تحقيقاً للردع العام[٢]، ويعتبر الإعفاء من العقاب مانعاً من موانع العقاب ويطلق عليه العذر المعفي من العقاب، ويفترض مانع العقاب أن الجريمة قد اكتملت أركانها ثم حدثت واقعة قدر معها المشرع أن عدم توقيع العقاب على الجاني أكثر

=

باب أولى عدم إعفاء من يرتكب الجريمة من العقوبة كاملة، إلا أن هذا المقترح لم يلق القبول من أعضاء البرلمان، بينما طالب أحد الأعضاء الآخرين استبدال كلمة "اعتراف" بكلمة "البلاغ" الواردة في بداية الفقرة الثانية من المادة، وطالب السيد المستشار وزير شئون مجلس النواب استبدال كلمة "الإبلاغ" بكلمة "البلاغ" الواردة في بداية الفقرة الثانية من المادة، إلا أن المقترحين الأخيرين لم يلق أى منهما القبول من جانب أعضاء البرلمان.انظر: مضبطة مجلس النواب المصري، الجلسة السادسة والخمسين، المعقودة في ٢٠١٨/٥/١٤م، مرجع سابق، ص ص١١٥-١١٧.

[١] ومن التشريعات المقارنة التي نصت على الإعفاء من العقوبة في الجرائم المعلوماتية التشريع الإماراتي (م٤٥)، والتشريع الكويتي (م١٢)، والنظام السعودي(م١١).

[٢] د. فوزية عبد الستار: شرح قانون مكافحة المخدرات، مرجع سابق، ص١١٩.

تحقيقاً للمصلحة العامة من توقيع العقاب[١]، وقد قرر المشرع إعفاء الجاني من العقاب في حالتين:-

(الأولى) إبلاغ السلطات العامة بالجريمة قبل البدء في تنفيذ الجريمة أو قبل كشفها:تفترض هذه الحالة أن الجاني قد أبلغ عن الجريمة قبل البدء في تنفيذها أو قبل أن تكتشف، فيكون للإبلاغ عنها فضل كشفها للسلطات، فحكمة النص تفيد أن الجريمة قد ساهم فيها عدد من الجناة سواء فاعلين أو شركاء، فجاء الإبلاغ عن الجريمة ابتداء من أحدهم، بحيث يفتح ذلك الطريق أمام السلطات لملاحقة باقي الجناة وضبط الأموال المتحصلة من الجريمة، أما إذا كانت الجريمة قد وصلت إلى علم السلطات قبل الإبلاغ، فلا سبيل إلى استفادة الجاني من مانع العقاب، إلا إذا توافرت الحالة الثانية، ويستوي لدى القانون الباعث الذي دفع الجاني إلى المبادرة إلى الإبلاغ، فقد يكون الخوف من العقاب، أو يقظة الضمير، أو الرغبة في الانتقام من باقي المساهمين، كذلك يستوي لدى القانون الجهة التي يقدم إليها البلاغ، سواء أكانت الشرطة أم النيابة العامة أم غيرها ما دام يصدق عليها صفة السلطة العامة[٢].

(الثانية) إبلاغ السلطات العامة عن الجريمة بعد علمها بها:إذا أبلغ الجاني عن الجريمة بعد وصولها إلى علم السلطات، فلا يستفيد من الإعفاء إلا إذا أدى الإبلاغ فعلاً إلى ضبط باقي الجناة والأموال المتحصلة من الجريمة، ويكفي لتحقق العلم لدى السلطات أن يكون منصباً على الجريمة، فليس بشرط أن تكون قد علمت بالمساهمين فيها، ولذلك فإن الإبلاغ في هذه الحالة لا يكون له من قيمة إلا إذا أدى إلى تمكين السلطات المختصة من القبض على مرتكبي الجريمة الآخرين، أو على ضبط الأموال

---

[١] المرجع السابق، ص١٢٠.

[٢] المرجع السابق، ص ص١٢١ ،١٢٢.

موضوع الجريمة، أو أعان أثناء البحث والتحقيق على كشف الحقيقة فيها، أو على القبض على مرتكبي جريمة أخرى مماثلة لها في النوع والخطورة، ويشترط في الإبلاغ أن يكون جدياً، فإذا نسب الجاني التهمة زوراً إلى بعض الأشخاص، فلا يجوز أن يستفيد من الإعفاء، وإلا استطاع –عن طريق الإيقاع بغيره- أن يخدع السلطات، فإذا لم يحقق الإبلاغ الهدف منه، أو تبين عدم صدقه فلا يستفيد من الإعفاء لتخلف الهدف الذي يكافأ عنه بميزة الإعفاء وهو تمكين السلطات من ضبط الجناة والأموال المتحصلة من الجريمة، ويلاحظ أنه إذا توافرت الجدية في إبلاغ المتهم عن باقي المساهمين يترتب حقه في الإعفاء ولو لم يضبط الجناة إذا كان عدم ضبطهم لا يرجع إلى عدم صدق الإبلاغ، بل إلى سبب آخر مثل تقاعس السلطات[١].

ويكفي لتحقق الهدف من الإبلاغ أن تكون المعلومات الصحيحة التي أفضى بها الجاني لرجال الشرطة قد أدت بذاتها إلى القبض على المساهم ولو كان أمر هذا المساهم معلوماً لرجال الشرطة من قبل حسبما أسفرت عنه التحريات، ما دام إبلاغ الجاني قد أضاف جديداً على المعلومات السابقة عليه، من شأنه تمكين السلطات من القبض عليه[٢]، ويلاحظ أن النص يشترط أن يكون إبلاغ الجاني قد أدى إلى ضبط باقي الجناة والأموال المتحصلة من الجريمة، والمقصود من ذلك، الجناة الذين يعرفهم الجاني، فلا يتصور أن يتطلب منه القانون أن يرشد عن أشخاص لا يعرفهم، إذ لا إلزام بمستحيل[٣].

---

[١] نقض ١٩٨١/٤/١، مجموعة أحكام محكمة النقض، س٣٢، رقم ٥٢، ص٣٠٠.

[٢] نقض ١٩٦١/١/٣١، مجموعة أحكام محكمة النقض، س١٨، رقم ٢٨، ص١٥٣. مشار إليه د. فوزية عبد الستار: المرجع السابق، ص١٢٤.

[٣] د. فوزية عبد الستار، الموضع السابق.

ويكتفي المشرع لمكافأة الجاني عن إبلاغه الذي أدى إلى ضبط باقي الجناة بأن يتم الضبط بناءً على هذا الإبلاغ، ولو أفضت المحاكمة بعد ذلك إلى براءتهم لبطلان الإجراءات مثلاً، أو لتوافر بعض موانع المسئولية لديهم، ويتطلب القانون لتحقق الإفادة من الإعفاء، أن يكون الإبلاغ قبل التحقيق أو أثناءه، ويستفيد المبلغ من الإعفاء إذا توافرت شروطه سواء أكان فاعلاً للجريمة أم شريكاً فيها، والإعفاء عن العقوبة بعد علم السلطات بالجريمة جوازي للمحكمة، ويقتصر على العقوبة الأصلية للجريمة دون غير ذلك من العقوبات كالمصادرة مثلاً، فإذا توافرت الشروط المحددة قانوناً تلتزم المحكمة بأن تحكم بالبراءة، كذلك فإن الإعفاء سبب شخصي لا يستفيد منه إلا من استوفى شروطه[1]، كما يجوز للمحكمة أن تحكم بتخفيف العقوبة إذا وجدت عدم استحقاق المتهم للإعفاء من العقوبة، وهو أمر تقديري للمحكمة تحكم به في ضوء ظروف وملابسات القضية.ولا يخل الإعفاء من العقوبة أو تخفيفها بوجوب الحكم برد المال المتحصل من الجرائم المنصوص عليها في هذا القانون.

[1] المرجع السابق، ص ص١٢٥، ١٢٤.

الفصل الثاني

الأحكام الإجرائية لجرائم تقنية المعلومات

تمهيد وتقسيم: حدد الباب الثاني من القانون الأحكام والقواعد الإجرائية الواجب إتباعها عند تنفيذ هذا القانون، بمراعاة خصوصية هذه الجرائم المستحدثة من ناحية، وحماية حرمة الحياة الخاصة من ناحية ثانية، وذلك بتحديد إجراءات الضبط والتحقيق والمحاكمة فيمثل هذا النوع من الجرائم المنصوص عليها، وجدير بالذكر أن ثمة تحديات تواجه أجهزة إنفاذ القانون في التحقيق في جرائم تقنية المعلومات، من أبرزها: الابتكارات الإجرامية، وصعوبة الحصول على الأدلة الرقمية، علاوة على أن المشتبه فيهم غالباً ما يلجأون إلى تقنيات إخفاء الهوية والتشويش، فضلاً عن سرعة وصول التقنيات الجديدة إلى جمهور المجرمين الواسع من خلال أسواق الجريمة على الإنترنت، ومن ثم تأتي أهمية القواعد الجنائية الإجرائية لوضع النصوص الجنائية الموضوعية موضع التنفيذ، ونقلها من حالة السكون إلى حالة الحركة[١]، وبما يحقق فاعلية النصوص الجنائية في مواجهة هذه الصورة من الإجرام المستحدث.وعلى صعيد آخر، ثمة تحديات أخرى تواجه أجهزة إنفاذ القانون في العديد من الدول تتمثل في صعوبة إقناع مؤسسات القطاع الخاص -التي تشرف على الخوادم التي تحتوي على البيانات والمعلومات- في التعاون من أجل الحصول على المعلومات والإيضاحات ذات الصلة بجرائم تقنية المعلومات[٢]، بحجة ما تمثله هذا الإفشاء من انتهاك للخصوصية،

---

[١] د. أحمد فتحي سرور: الوسيط في قانون الإجراءات الجنائية، القاهرة، دار النهضة العربية، ط٢٠١٢، ص٩.

[٢] انظر: دراسة مكتب الأمم المتحدة المعني بالمخدرات والجريمة حول الجريمة السيبرانية، مرجع سابق، صxxviii.

ومن ثم يلتزم مقدمي الخدمة بتقديم البيانات المطلوبة عن الجناة في إطار الأوامر القضائية الرسمية الصادرة من سلطات التحقيق والمحاكمة.

وفيما يلي نتناول الاختصاص القضائي بنظر جرائم تقنية المعلومات، وتحديد مأموري الضبط القضائي وإجراءات الاستدلال في هذه الطائفة من الجرائم، وأوامر البحث والتنقيب عن الأدلة، وإجراءات حجب المواقع الإلكترونية، والأمر بالمنع من السفر والصلح والتصالح، وذلك في تسعة مباحث على النحو التالي:-

المبحث الأول

نطاق تطبيق القانون من حيث المكان[1]

الطابع عبر الوطني لجرائم تقنية المعلومات وأثره على قواعد الاختصاص المكاني: لقد أفرز الارتباط الوثيق بين جرائم تقنية المعلومات وشبكة الإنترنت عن نتيجة مفادها أن غالبية كبيرة من هذه الجرائم تتم في إطار عبر وطني، فجرائم تقنية المعلومات بالنظر إلى طابعها عبر الوطني الذي تستخدم فيه شبكة المعلومات الدولية، فقد يجرى التخطيط والإعداد للجريمة في بلد ما ويجرى تنفيذها في بلد آخر وتتحقق آثارها في بلد ثالث.

وتشير تقديرات مكتب الأمم المتحدة المعني بالمخدرات والجريمة إلى أن غالبية الجرائم السيبرانية (٣٠-٧٠%) تشتمل على بعد عابر لحدود الوطن، وهذا البعد عابر الحدود ينشأ عندما يكون للجريمة المعنية عنصر أو أثر مهم في إقليم آخر،

---

[1] يرى الباحث أنه كان يجدر بالمشرع إيراد قواعد نطاق تطبيق القانون من حيث المكان وقواعد التعاون الدولي لمكافحة الجرائم المعلوماتية، في الشق المتصل بالأحكام الإجرائية للقانون، وليس في الشق المتصل بالأحكام العامة للقانون، في ضوء ما استقر عليه الفقه الجنائي من اعتبار قواعد نطاق تطبيق القانون من حيث المكان والتعاون الدولي من القواعد الإجرائية في القانون الجنائي.

أو عندما يكون أحد جوانب تنفيذ الجريمة قد تم في إقليم آخر، وأن القانون الدولي ينص على عدد من الأسس المتعلقة بالولاية القضائية بشأن الأفعال المعنية، بما في ذلك أشكال الولاية القضائية المستندة إلى الإقليم والمستندة إلى الجنسية[1].

وقد أشارت المادة الثالثة من القانون نطاق تطبيق القانون من حيث المكان، بالنظر لما تتمتع جرائم تقنية المعلومات بخصوصية تتصل بإمكان ارتكابها كلها أو بعضها، من خارج الإقليم المصري أو من داخله، أو عند وجود مرتكبها في الأراضي المصرية بعد ارتكابها في الخارج، ولذلك تبرز أهمية تحديد قواعد تطبيق قانون مكافحة جرائم تقنية المعلومات من حيث المكان بالنظر لهذا الطابع عبر الوطني الذي تتسم به هذه الجرائم، ومن ثم تصور ارتكابها خارج الدولة، وتحقق آثارها في الدولة المصرية أو دول أخرى، وبالتالي فقد بات من الضروري تنظيم قواعد الاختصاص الوطني بهذه الجرائم.

وقد حددت المادة المذكورة نطاق تطبيق القانون من حيث المكان بالنسبة للجرائم التي ترتكب من الأجانب خارج إقليم الدولة المصرية، توسعاً في قواعد الاختصاص الواردة في قانون العقوبات والمتمثلة في مبدأ الإقليمية والشخصية والعينية، حيث حرص المشرع المصري وبالنظر إلى الطابع عبر الوطني لهذه الجرائم، على التوسع في قواعد الاختصاص لتشمل الأخذ بمبدأ الشخصية في شقها السلبي ومبدأ العالمية، حيث تقضي المادة المذكورة بأنه:" ***مع عدم الإخلال بأحكام الباب الأول من الكتاب الأول من قانون العقوبات، تسرى أحكام هذا القانون على كل من ارتكب خارج جمهورية مصر العربية من غير المصريين جريمة من الجرائم المنصوص عليها في هذا القانون، متى كان الفعل معاقباً عليه في الدولة التي وقع فيها تحت أي وصف***

---

[1] انظر دراسة مكتب الأمم المتحدة حول الجريمة السيبرانية، مرجع سابق، صxxxi.

قانوني، وذلك في أي من الأحوال الآتية:-

١ -إذا ارتكبت الجريمة على متن أي وسيلة من وسائل النقل الجوي أو البرى أو المائي، وكانت مسجلة لدى جمهورية مصر العربية أو تحمل عملها.

٢ -إذا كان المجني عليهم أو أحدهم مصرياً.

٣ -إذا تم الإعداد للجريمة أو التخطيط أو التوجيه أو الإشراف عليها أو تمويلها في جمهورية مصر العربية.

٤ -إذا ارتكبت الجريمة بواسطة جماعة إجرامية منظمة، تمارس أنشطة إجرامية في أكثر من دولة من بينها جمهورية مصر العربية.

٥ -إذا كان من شأن الجريمة إلحاق ضرر بأي من مواطني جمهورية مصر العربية أو المقيمين فيها أو بأمنها أو بأي من مصالحها، في الداخل أو الخارج.

٦ -إذا وجد مرتكب الجريمة في جمهورية مصر العربية، بعد ارتكابها ولم يتم تسليمه "[1].

أولاً- قواعد الاختصاص المكاني العامة في التشريع المصري: تخضع جرائم تقنية المعلومات لقواعد الاختصاص العامة في قانون العقوبات المصري وهي: قواعد الإقليمية والشخصية الإيجابية والعينية، وذلك على النحو التالي:-

١) قاعدة الإقليمية: والتي تقضي بسريان القانون المصري على الجرائم التي ترتكب كلها أو بعضها في الإقليم المصري (م١ و١/٢ من قانون العقوبات).

---

(١) يتشابه نص المادة الثالثة من القانون مع بعض نصوص التشريعات المصرية ذات الصلة بمكافحة الجرائم عبر الوطنية، نذكر منها على سبيل المثال وليس الحصر، نص المادة (١٦) من قانون مكافحة الاتجار بالبشر رقم (٦٤) لسنة ٢٠١٠ ونص المادة (٢٠) من قانون مكافحة الهجرة غير الشرعية وتهريب المهاجرين رقم (٨٢) لسنة ٢٠١٦.

٢) قاعدة الشخصية في شقها الإيجابي: والتي تقضي باختصاص المحاكم المصرية بنظر الجرائم التي يرتكبها المصري في الخارج بشروط (م٣ من قانون العقوبات)، وهي أن يكون الفعل جناية أو جنحة وفقاً للقانون المصري، وأن يكون الفعل معاقباً عليه بمقتضى قانون البلد الذي ارتكبه فيه، وأن يعود الجاني إلى مصر.

٣) قاعدة العينية: والتي تقرر اختصاص المحاكم المصرية بنظر جرائم محددة تشكل في ذاتها مساساً بمصلحة أساسية للدولة أو تهدد كيانها (م٢/٢ من قانون العقوبات) ومن أبرز هذه الجرائم: الجرائم التي تمس أمن الحكومة من الداخل ومن الخارج وجرائم تزييف العملة.

أما الجرائم التي تقع خارج الدولة ولا يتوافر فيها الشروط الخاصة بمحاكمة المصريين وفقاً للمادة (٣) من قانون العقوبات أو لم تكن من الجرائم الواردة في المادة (٢/٢) عقوبات فإنها لا تخضع للقانون المصري.

ثانياً- أحوال التوسع في الاختصاص المكاني بالنسبة لجرائم تقنية المعلومات: إلا أن المشرع المصري حرص على توسيع نطاق اختصاصه بنظر جرائم تقنية المعلومات التي تقع في الخارج، من خلال النص على الأخذ بمبدأ عالمية القاعدة الجنائية، ومبدأ الشخصية في شقه السلبي، وامتداد اختصاصه ليشمل الأعمال التحضيرية للجريمة، وتجريم أنشطة جماعات الجريمة المنظمة التي تباشر أنشطتها في مصر، وذلك على النحو التالي:-

١) الحالة الأولى- الجرائم الواقعة على وسائل النقل المسجلة في مصر أو التي تحمل العلم المصري: وهذه الحالة تشمل حالة امتداد الاختصاص للجرائم التي تقع على السفن أو الطائرات التي تحمل العلم المصري أو المسجلة في مصر، حيث تقضي المادة الثالثة من القانون في بندها الأول إلى امتداد اختصاص القضاء المصري ليشمل جرائم

تقنية المعلومات التي تقع على متن وسيلة من وسائل النقل الجوي كالطائرات أو البري كالسيارات وأتوبيسات النقل أو المائي كالسفن، ولو وقعت في خارج الدولة؛ شريطة أن تكون وسائل النقل مسجلة لدى جمهورية مصر العربية أو تحمل علمها.

٢) الحالة الثانية- مبدأ الشخصية في شقه السلبي: ويقصد به امتداد القانون الجنائي للدولة لنظر الجرائم التي تقع على مواطنيها، أياً كان مكان ارتكاب الجريمة أو أياً كانت جنسية مرتكبها، ومن ثم يخضع للقانون المصري الذي يرتكب خارج الجمهورية جريمة على أحد مواطني جمهورية مصر العربية، حتى ولو وقعت من أجنبي خارج مصر[١].

٣) الحالة الثالثة- حالة وقوع الأعمال التحضيرية للجريمة داخل مصر:القاعدة في القانون الجنائي هو اختصاص المحاكم بنظر الأفعال التي تشكل في ذاتها جريمة وفقاً لقانونها، ويخرج من نطاق التجريم الأعمال التحضيرية للجريمة على اعتبار أنها لا تدخل في النموذج القانوني المكون للجريمة، وتشجيعاً للجناة على ترك الجريمة، ولا يكون العقاب على الأعمال التحضيرية إلا إذا كانت تلك الأفعال تشكل في نظر القانون جريمة بذاتها، وبالنظر إلى الطابع التنظيمي لهذه الجرائم وارتكابها من جانب جماعات إجرامية منظمة، وجسامة مثل هذه الجرائم وخطورتها على المجتمع، ونظراً لأن عدم تجريم تلك الأفعال من شأنه عدم إمكان مساءلة مرتكبي الجريمة، فقد حرص المشرع المصري على مد اختصاصه الجنائي ليشمل الأعمال التحضيرية في جرائم تقنية المعلومات التي ترتكب داخل مصر ولو وقعت هذه الجريمة في الخارج، من خلال تقرير اختصاص المحاكم المصرية بنظر الأعمال التحضيرية التي تتم داخل مصر وتشمل أفعال الإعداد للجريمة أو التخطيط أو التوجيه أو الإشراف عليها أو تمويلها.

---

[١] قارن: د. عبد العظيم مرسي وزير: القسم العام، مرجع سابق، ص ص١٠٤-١١٢.

٤) الحالة الرابعة- حالة وقوع الجريمة بواسطة جماعة إجرامية منظمة تمارس نشاطها الإجرامي في مصر: تقضي المادة الثالثة من القانون في بندها الرابع إلى امتداد اختصاص القضاء المصري ليشمل جرائم تقنية المعلومات التي تقع خارج الجمهورية بواسطة جماعة إجرامية منظمة تمارس أنشطة إجرامية في أكثر من دولة من بينها جمهورية مصر العربية، ومن الجدير بالذكر أن القانون لم يتضمن تعريف للجماعة الإجرامية المنظمة، إلا أن قوانين مصرية أخرى كقانون مكافحة الاتجار بالبشر وقانون مكافحة الهجرة غير الشرعية وتهريب المهاجرين عرفتها بأنها:" الجماعة المؤلفة وفق تنظيم معين من ثلاثة أشخاص على الأقل للعمل بصفة مستمرة أو لمدة من الزمن بهدف ارتكاب جريمة محددة أو أكثر من بينها جرائم (الاتجار بالبشر- تهريب المهاجرين) وحدها أو مع غيرها، وذلك من أجل الحصول بشكل مباشر أو غير مباشر على منفعة مادية أو معنوية أو لأي غرض، ولا يلزم أن يكون لأعضائها أدوار محددة أو أن تستمر عضويتهم فيها، ويرى الباحث أنه كان من الأولى بالمشرع المصري الإشارة إلى تعريف الجماعة الإجرامية المنظمة في التعاريف التي تضمنها.

وتشير تقديرات مكتب الأمم المتحدة المعني بالمخدرات والجريمة إلى أن غالبية جرائم تقنية المعلومات باتت ترتكب في إطار منظم، وأن مصدر أكثر من ٨٠% من الجريمة السيبرانية هو شكل من أشكال النشاط المنظم، حيث تقوم الأسواق السوداء للجرائم السيبرانية على دورة تتسم بإعداد البرمجيات الخبيثة والفيروسات الحاسوبية والتحكم بشبكات حاسوبية، من خلال البوت نت، وتلقف البيانات الشخصية والمالية وبيع البيانات والمتاجرة بالمعلومات المالية[1].

[1] انظر دراسة مكتب الأمم المتحدة حول الجريمة السيبرانية، مرجع سابق، صxxii.

٥) الحالة الخامسة- حالة الإضرار بأي من مواطني مصر أو المقيمين فيها أو بأمنها أو بأي من مصالحها: تقضي المادة الثالثة من القانون في بندها الخامس إلى امتداد اختصاص القضاء المصري ليشمل جرائم تقنية المعلومات التي تقع خارج الجمهورية والتي يكون من شأنها إلحاق الضرر بأي من رعايا الدولة من المواطنين أو المقيمين فيها أو الإضرار بأمنها أو بأي من مصالحها في الداخل والخارج.

٦) الحالة السادسة- مبدأ العالمية: ويقصد به سريان اختصاص المحاكم المصرية بنظر جرائم تقنية المعلومات التي يتم القبض على مرتكبيها في مصر، أيا كانت جنسيتهم وأياً كان مكان ارتكاب جريمتهم، ليشمل بذلك جرائم تقنية المعلومات التي ارتكبت خارج مصر ولو لم ترتكب من مصري، متى وجد مرتكب الجريمة بمصر سواء أكان فاعلاً أم شريكاً، ولا شك في أن هذا التوسع في اختصاص القانون المصري يتناسب مع طبيعة جرائم تقنية المعلومات عبر الوطنية والتي قد ترتكب بمعرفة جماعات الجريمة المنظمة، وهو ما من شأنه تحقيق مواجهة فعالة لهذه الجرائم في التشريع المصري وبسط سلطان سلطات إنفاذ القانون لمواجهة هذه الجرائم الخطيرة.

اختصاص النيابة العامة دون غيرها بتحريك الدعوى الجنائية عن الجرائم التي تقع بالخارج: تبرز الإشارة إلى أن المشرع المصري قد نص في المادة الرابعة من قانون العقوبات على أن "لا تقام الدعوى العمومية على مرتكب جريمة أو فعل في الخارج إلا من النيابة العامة. ولا يجوز إقامتها على من يثبت أن المحاكم الأجنبية قد برئته مما أسند إليه أو أنها حكمت عليه نهائياً واستوفى عقوبته"، ويقتصر نطاق هذا النص على الجرائم والأفعال التي ترتكب خارج الإقليم المصري كجرائم تقنية المعلومات وغيرها من الجرائم، وعلى الجرائم الواردة في المادتين الثانية والثالثة من قانون العقوبات، وطبقاً لهذا النص يُخضع المُشرع الدعوى الجنائية الناشئة عن الجرائم المُرتكبة في الخارج لقيدين: (الأول): اختصاص النيابة العامة دون غيرها وحدها

بسلطة تحريك الدعوى الجنائية. (الثاني): عدم جواز تحريك الدعوى إذا ثبت أن المحاكم قد برأت المتهم أو أدانته واستوفى العقوبة.

وترجع العلة من منح هذا الاختصاص للنيابة العامة دون غيرها من الأفراد الذين يجوز لهم الادعاء المباشر أمام القضاء الجنائي حال توافر شروطه القانونية، إلى أن النيابة العامة هي الأجدر دون غيرها ببحث مسألة التداخل في الاختصاص بين القانون المصري وغيره من القوانين الأخرى، وما يمكن أن تثيره المحاكمة من مشكلات مع دولة أخرى[١]، وبتقدير مدى ملائمة تحريك الدعاوى الجنائية عن مثل هذه القضايا التي تتطلب بحث ملابسات تلك الجرائم ومدى قانونية واختصاص القضاء المصري بنظر هذه الأفعال؛ نظراً لأن الأمر لا يخلو من الدقة التي يشق على المضرور تقديرها[٢].

قواعد الاختصاص المكاني العامة في المواثيق الدولية: حرص عدد من المواثيق الدولية على الإشارة إلى قواعد الاختصاص في الجرائم المعلوماتية، ومن أبرز هذه المواثيق الاتفاقية الأوروبية المتعلقة بالجرائم المعلوماتية (بودابست) والاتفاقية العربية لمكافحة جرائم تقنية المعلومات، حيث تضمنت المادة (٢٢) من اتفاقية بودابست النص على اعتماد الدول الأطراف للتدابير التشريعية أو أية تدابير أخرى لإقرار الاختصاص بشأن أي جريمة عندما ترتكب في إقليمها، أو على متن إحدى السفن ترفع علمه، أو على متن إحدى الطائرات المسجلة بموجب قوانينها، أو من جانب أحد مواطنيها، إذا كانت الجريمة معاقب عليها بموجب القانون الجنائي بمكان

---

[١] قارن: د. أحمد عوض بلال: مبادئ قانون العقوبات المصري- القسم العام، القاهرة، دار النهضة العربية، ٢٠١٠، ص٨٦.

[٢] قارن: د. عبد العظيم مرسي وزير: القسم العام، مرجع سابق، ص١١٤.

ارتكابها، أو في حالة ارتكاب الجريمة خارج الاختصاص القضائي الإقليمي لأية دولة. فضلاً عن اعتماد التدابير التشريعية وتدابير أخرى لإقرار الاختصاص القضائي بشأن الجرائم في الحالات التي يكون فيها الجاني المزعوم موجودا في إقليمه، ولا يقوم بتسليمه أو تسليمها لطرف آخر على سندٍ وحيدٍ من جنسيته أو جنسيتها، وذلك بعد طلب التسليم.

بينما تضمنت المادة (٣٠) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات النص على التزام كل دولة بتبني الإجراءات الضرورية لمد اختصاصها بشأن أي جريمة عندما ترتكب في إقليم الدولة الطرف، أو على متن سفينة ترفع علم الدولة الطرف، أو على متن طائرة مسجلة تحت قوانين الدولة الطرف، أو من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكابها، أو إذا ارتكبت خارج منطقة الاختصاص القضائي الإقليمي لأية دولة. فضلاً عن التزام كل دولة بتبني الإجراءات الضرورية لمد اختصاصها بشأن الجرائم في الحالات التي يكون فيها الجاني المزعوم حاضراً في إقليم تلك الدولة الطرف، ولا يقوم بتسليمه إلى طرف آخر بناء على جنسيته بعد طلب التسليم.

المبحث الثاني

الاختصاص القضائي بنظر جرائم تقنية المعلومات

اختصاص المحاكم الاقتصادية بنظر جرائم تقنية المعلومات: وقبل التطرق إلى الأحكام الإجرائية بالقانون، تبرز الإشارة إلى أن المحاكم المختصة بنظر جرائم المعلومات، كانت -قبل إقرار هذا القانون- المحاكم الاقتصادية[١]، وهذا ما تشير إليه اتجاهات القضاء المصري، حيث قضت محكمة النقض المصرية في أحد أحكامها الحديثة باختصاص المحاكم الاقتصادية بنظر جرائم الإنترنت أثناء نظرها لمسألة تنازع سلبي في الاختصاص بينها بين المحاكم العادية[٢]، وقد حرص المشرع المصري على

---

(١) نص قانون إنشاء المحاكم الاقتصادية رقم (١٢٠) لسنة ٢٠٠٨ على اختصاصها بنظر أغلب الدعاوى الجنائية في مواد الجنح والجنايات التي ترتكب عبر الانترنت والمتعلقة بها مثل انتهاك حقوق الملكية الفكرية والسب والتشهير والتهديد عبر الانترنت، والسطو على البنوك عبر الانترنت، والاعتداء على الأطفال واستغلالهم عبر الانترنت. هذا إلى جانب اختصاص محاكم الطفل المتخصصة بنظر القضايا التي يرتكبها الأطفال عبر الانترنت.

وكانت محكمة النقض المصرية قد قضت في أحد أحكامها الحديثة بأن قانونا تنظيم الاتصالات وحماية الملكية الفكرية من بين القوانين المنصوص عليها حصراً بالمادة الرابعة من القانون رقم ١٢٠ لسنة ٢٠٠٨ وأثره اختصاص المحاكم الاقتصادية بنظر الدعاوى الجنائية الناشئة عن الجرائم المنصوص عليها فيهما. انظر: الطعن رقم ١١٨٦٥ لسنة ٨٠ق جلسة ٢٠١١/١١/٢٨، مجموعة المبادئ القانونية الصادرة عن محكمة النقض (الدوائر الجنائية) في الجرائم الاقتصادية، المكتب الفني لمحكمة النقض، ص٢٩.

(٢) تعود وقائع هذه القضية إلى اتهام إحدى السيدات بارتكاب جريمة القذف العلني عن طريق شبكة الانترنت لقيامها بإسناد محادثات تليفونية للمجني عليه بواسطة النشر عن طريق شبكة الإنترنت لو كانت صادقة لأوجبت احتقاره عند أهل وطنه، ونقلت عن طريق شبكة الإنترنت محادثات تليفونية للمجني عليه، وأذاعت تلك المحادثات عن طريق الإنترنت بغير رضاء صاحب الشأن، حيث ارتأت محكمة النقض أن هذه الوقائع تشكل جريمتي إزعاج أو مضايقة الغير بإساءة استعمال أجهزة الاتصالات والاعتداء على حرمة الحياة الخاصة للأفراد بنقل محادثات جرت عن طريق التليفون، وأن هاتين الجريمتين تشكل حالة تعدد معنوي للجرائم، وهو ما يوجب وفق حكم المادة ٣٢ عقوبات الحكم بعقوبة الجريمة ذات الوصف الأشد، وهي جريمة تعمد الإزعاج أو مضايقة =

تأكيد هذا الاختصاص بموجب القانون رقم ١٤٦ لسنة ٢٠١٩ الذي نص صراحة على ذلك.

فقد نصت المادة (٤) من قانون إنشاء المحاكم الاقتصادية المعدلة القانون ١٤٦ لسنة ٢٠١٩ على أنه:"مع عدم الإخلال بالاختصاصات المقررة للمحاكم الاقتصادية المنصوص عليها في أي قانون آخر، تختص المحاكم الاقتصادية بدوائرها الابتدائية والاستئنافية، دون غيرها، نوعيا ومكانيا بنظر الدعاوى الجنائية الناشئة عن الجرائم المنصوص عليها فى القوانين الآتية: ١- قانون العقوبات فى شأن جرائم المسكوكات والزيوف المزورة. ٢- قانون الإشراف والرقابة على التأمين فى مصر. ٣- قانون شركات المساهمة وشركات التوصية بالأسهم والشركات ذات المسئولية المحدودة.٤- قانون سوق رأس المال.٥- قانون تنظيم نشاطي التأجير التمويلي والتخصيم.٦- قانون الإيداع والقيد المركزى للأوراق المالية. ٧- قانون التمويل العقارى. ٨- قانون حماية حقوق الملكية الفكرية. ٩- قانون البنك المركزى والجهاز المصرفى والنقد. ١٠- قانون الشركات العاملة فى مجال تلقى الأموال لاستثمارها. ١١- قانون تنظيم إعادة الهيكلة والصلح الواقى والإفلاس. ١٢- قانون حماية الاقتصاد القومى من الآثار الناجمة عن الممارسات الضارة فى التجارة الدولية. ١٣- قانون حماية المنافسة ومنع الممارسات الاحتكارية. ١٤- قانون حماية المستهلك. ١٥- قانون تنظيم الاتصالات. ١٦- قانون تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات. ١٧- قانون مكافحة غسل الأموال. ١٨- قانون تنظيم الضمانات

=

الغير بإساءة استعمال أجهزة الاتصالات التي تدخل في اختصاص المحاكم الاقتصادية، وقضت بتعيين محكمة جنح القاهرة الاقتصادية للفصل في الدعوى موضوع الطلب. انظر: الطعن الجنائي رقم ٧٨٤٣ لسنة ٧٨ قضائية، جلسة ٢٠ يناير ٢٠١٩، حكم غير منشور.

المنقولة. ١٩- قانون تنظيم نشاط التمويل متناهي الصغر. ٢٠- قانون الاستثمار. ٢١- قانون مكافحة جرائم تقنية المعلومات".

وهو ما أكدت عليه المادة السادسة من القانون ذاته والتي حددت اختصاص الدوائر الابتدائية بالمحاكم الاقتصادية، والتي تقضي بأنه:" فيما عدا المنازعات والدعاوى التي يختص بها مجلس الدولة، تختص الدوائر الابتدائية بالمحاكم الاقتصادية، دون غيرها، بنظر المنازعات والدعاوى، التي لا تجاوز قيمتها عشرة ملايين جنيه، والتي تنشأ عن تطبيق القوانين الآتية:١. قانون الشركات العاملة فى مجال تلقى الأموال لاستثمارها.٢. قانون سوق رأس المال.٣. قانون تنظيم نشاطي التأجير التمويلي والتخصيم.٤. قانون حماية الاقتصاد القومي من الآثار الناجمة عن الممارسات الضارة في التجارة الدولية.٥. قانون التجارة فى شأن نقل التكنولوجيا والوكالة التجارية وعمليات البنوك.٦. قانون التمويل العقاري.٧. قانون حماية حقوق الملكية الفكرية.٨. قانون تنظيم الاتصالات.٩. قانون تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.١٠. قانون حماية المنافسة ومنع الممارسات الاحتكارية.١١. قانون شركات المساهمة وشركات التوصية بالأسهم والشركات ذات المسئولية المحدودة وشركات الشخص الواحد.١٢. قانون البنك المركزي والجهاز المصرف والنقد.١٣. قانون التجارة البحرية.١٤. قانون الطيران المدني فى شأن نقل البضائع والركاب.١٥. قانون حماية المستهلك. ١٦. قانون تنظيم الضمانات المنقولة.١٧. قانون المناطق الاقتصادية ذات الطبيعة الخاصة.١٨. قانون تنظيم نشاط التمويل متناهي الصغر.١٩. قانون الاستثمار.٢٠. قانون مكافحة جرائم تقنية المعلومات. كما تختص بالحكم فى دعاوى التعويض أو التأمين الناشئة عن تطبيق أحكام القوانين المشار إليها بالفقرة السابقة بحسب الأحوال.ويكون الحكم الصادر فى الدعاوى المشار إليها فى الفقرتين السابقتين نهائياً إذا كانت قيمة الدعوى لا تجاوز

خمسمائة ألف جنيه.وتختص الدوائر الاستئنافية في المحاكم الاقتصادية، دون غيرها، بالنظر ابتداءً فى جميع المنازعات والدعاوى المنصوص عليها فى الفقرات السابقة إذا جاوزت قيمتها عشرة ملايين جنيه أو كانت الدعوى غير مقدرة القيمة.وتختص الدوائر الابتدائية والاستئنافية بالمحاكم الاقتصادية التى أصدرت الأمر بنظر تظلمات ودعاوى الرسوم القضائية الناشئة عن تطبيق أحكام هذا القانون والقرارات الصادرة من قضاة المحكمة".

وحسناً فعل المشرع المصري بالنص صراحة على اختصاص المحاكم الاقتصادية بنظر جرائم تقنية المعلومات، بالنظر إلى الطبيعة الخاصة لهذه الجرائم، والتي تتطلب تخصص القضاة الجنائيين المعنيين بالفصل في هذه النوعية من القضايا، فضلاً عن سابقة تصدي دوائر المحاكم الاقتصادية لجرائم تقنية المعلومات في إطار اختصاصاها بنظر الجرائم الواردة في قانون التوقيع الإلكتروني وقانون الاتصالات، علاوة على تجنب مشكلة تنازع الاختصاص بين القضاء العادي وقضاء المحاكم الاقتصادية بشأن الأفعال التي تشكل جرائم تدخل في قانون مكافحة جرائم تقنية المعلومات وجرائم أخرى تدخل في اختصاص هذه المحاكم كجرائم التوقيع الإلكتروني وجرائم إساءة استعمال الاتصالات.

المبحث الثالث

أعمال الاستدلال في جرائم تقنية المعلومات

نتناول في هذا المبحث أعمال الاستدلال في جرائم تقنية المعلومات، من خلال التطرق إلى مسألة تحديد الأشخاص المخولين صفة مأموري الضبط القضائي، وإجراءات جمع الاستدلالات في جرائم تقنية المعلومات، وذلك في مطلبين على النحو التالي:-

المطلب الأول

تحديد مأموري الضبط القضائي

في جرائم تقنية المعلومات

عنت المادة الخامسة من القانون بتحديد مأموري الضبط القضائي في جرائم تقنية المعلومات؛ إذ تقضي المادة المذكورة بأنه:" *يجوز بقرار من وزير العدل بالاتفاق مع الوزير المختص منح صفة الضبطية القضائية للعاملين بالجهاز أو غيرهم ممن تحددهم جهات الأمن القومي بالنسبة إلى الجرائم التي تقع بالمخالفة لأحكام هذا القانون والمتعلقة بأعمال وظائفهم*"، ومن ثم يتضح أن المشرع المصري أجاز لوزير العدل بالاتفاق مع الوزير المعني بشئون الاتصالات وتكنولوجيا المعلومات منح صفة الضبطية القضائية للعاملين بالجهاز القومي لتنظيم الاتصالات أو غيرهم ممن تحددهم جهات الأمن القومي المحددة بالقانون، وهي: رئاسة الجمهورية، ووزارة الدفاع،

ووزارة الداخلية، والمخابرات العامة، وهيئة الرقابة الإدارية[١]، بالنسبة للجرائم التي تقع بالمخالفة لأحكام هذا القانون والمتعلقة بأعمال وظائفهم، وجدير بالذكر أن وزارة الداخلية في مصر كان لها السبق في استحداث إدارة أمنية متخصصة، سُميت بإدارة مكافحة جرائم الحاسبات وشبكات المعلومات، تعنى بضبط ومكافحة جرائم تقنية المعلومات.

المقصود بمأموري الضبط القضائي: يقصد بمأموري الضبط القضائي الموظفين العموميين الذين خصهم المشرع الجنائي بمهمة الضبط القضائي؛ أي ضبط الجرائم ومرتكبيها وتقديمهم للعدالة من خلال جمع الأدلة والعناصر التي تلزم للتحقيق في الدعوى الجنائية، ويحدد المشرع الجنائي هؤلاء الموظفين في قانون الإجراءات الجنائية على سبيل الحصر، وغالباً ما تنص التشريعات المقارنة على تقرير صفة مأموري الضبط القضائي لأعضاء النيابة العامة وضباط ورجال الشرطة، هذا بالإضافة إلى طائفة أخرى من الموظفين العموميين الذين يتم تحديدهم بالاتفاق بين وزير العدل والوزير المختص لتخويلهم صفة الضبطية القضائية في ضبط جرائم معينة في نطاق عملهم، مثال ذلك: مفتشو الصحة والتموين...الخ[٢]، وقد نص القانون على تخويل الموظفين العموميين بالجهاز القومي لتنظيم الاتصالات صفة الضبطية القضائية في الجرائم المعلوماتية، ويتم تحديد الأشخاص المخولين لهذه الصفة من هؤلاء الموظفين بالاتفاق بين وزيري العدل والاتصالات وتكنولوجيا المعلومات، ومن ثم يمكن التمييز

---

[١] تبرز الإشارة إلى اقتراح أحد أعضاء البرلمان إضافة وزارة المالية ضمن جهات الأمن القومي، إلا أن هذا المقترح لم يلق قبولاً من أعضاء البرلمان. انظر: مضبطة مجلس النواب المصري، الجلسة السادسة والخمسين، مرجع سابق، ص٨٦.

[٢] د. مأمون سلامة: الإجراءات الجنائية في التشريع المصري، دار النهضة العربية،٢٠٠٣، ص٤٩٨ ومابعدها.

في هذا الشأن بين طائفتين من مأموري الضبط القضائي، الأولى من مأموري الضبط التقليديين من رجال الشرطة، والثانية من مأموري الضبط الفنيين أو المتخصصين من العاملين بوزارة الاتصالات وتكنولوجيا المعلومات ممن خولهم القانون صفة الضبطية القضائية.

موقف التشريع المقارن من تحديد مأموري الضبط القضائي في جرائم تقنية المعلومات:تختلف نهوج التشريعات المقارنة بشأن تحديد مأموري الضبط القضائي بشأن الجرائم المعلوماتية، ما بين اتجاهين: (الأول) التشريعات التي نصت على تحديد من تتوافر لهم صفة الضبطية القضائية في الجرائم المعلوماتية، ومن ضمن هذه التشريعات المقارنة التي أفردت أجهزة أمنية لمكافحة الجرائم المعلوماتية غالبية أجهزة الشرطة في الدول الغربية، ومنها أجهزة الشرطة الأمريكية، الكندية، الإنجليزية، السويدية، الهولندية، واليابانية، ومن ناحية أخرى، تضمنت غالبية التشريعات العربية، ومنها التشريع الإماراتي والعماني، حيث يقرر التشريع الإماراتي النص على أن يتم تحديد مأموري الضبط القضائي في الجرائم المعلوماتية بقرار من وزير العدل والشئون الإسلامية والأوقاف، بينما نص التشريع العماني في المادة (٣٤) منه على أنه: "تكون لموظفي الهيئة الذين يصدر بتحديدهم قرار من وزير العدل بترشيح من رئيس الهيئة، صفة الضبطية القضائية في نطاق تطبيق أحكام هذا القانون"،كما ينص التشريع السوداني على إنشاء شرطة متخصصة لجرائم المعلوماتية (م٣٠ من القانون السوداني)، أما (الاتجاه الثاني) فيشمل التشريعات المقارنة الأخرى التي لم تحدد طائفة خاصة من مأموري الضبط القضائي لضبط مرتكبي الجرائم المعلوماتية.

أبرز التحديات التي تواجه سلطات إنفاذ القانون في جرائم تقنية المعلومات: يشير الفقه الجنائي إلى وجود تحديات تواجه سلطات إنفاذ القانون من رجال الشرطة

في جرائم تقنية المعلومات، تختص عمليات الضبط وتتبع مرتكبيها، ونتناول فيما يلي أبرز هذه التحديات، على النحو التالي:-

١) خفاء الجريمة:تتسم جرائم تقنية المعلومات بطابع الخفاء؛ فهي تقع مُستترة خفية، لا يلحظها المجني عليه غالباً أو يدرى حتى بوقوعها، والإمعان في حجب وإخفاء السلوك المكون لها ونتائجها عن طريق التلاعب غير المرئي في التقنيات أو الذبذبات الإلكترونية التي تسجل البيانات عن طريقها، ليس عسيراً في الكثير من أحوالها بحكم توافر المعرفة والخبرة الفنية في مجال الحاسبات غالباً لدى مرتكبها، فاختراق قواعد البيانات وتغيير بعض محتوياتها بدس برامج خاصة ضمن برامجها قد لا يشعر به القائمون على تشغيلها، كما أن التخريب المنطقي للأنظمة يمكن تمويهه ليبدو كما لو كان خطأ مصدره البرامج أو الأجهزة أو نظام التشغيل أو النقل الكلى للنظام المعلوماتي[١].

ومن ناحية ثانية، تشير مسألة خفاء الجريمة إلى إشكالية إخفاء هوية الجناة، فغالباً ما يعمل مرتكبي جرائم تقنية المعلومات على إخفاء هوياتهم الحقيقية من خلال استخدام هويات مستعارة، لدرء المسئولية الجنائية أو الملاحقة القضائية عنهم، وهو ما يمثل أحد الصعوبات الحقيقية أمام أجهزة الشرطة وسلطات التحقيق في الجرائم المعلوماتية، والتي تسعى إلى مواجهتها من خلال تحديد جهاز الحاسب الآلي الذي استخدام في ارتكاب الجريمة، ثم تعقب مستخدم هذا الحاسب، وهو ما يتطلب ضرورة أن تتسم إجراءات البحث والتحرى بالسرية والمهنية لمنع مرتكبي هذه الجرائم من التعرف على متابعة الشرطة وسلطات التحقيق لهم.

---

[١] د. هشام محمد فريد رستم: الجوانب الإجرائية للجرائم، مرجع سابق، ص١٦ وما بعدها.

٢) غياب الدليل المرئي المُمكن فهمه بالقراءة: يتمثل أكثر ما تتيحه النظم المعلوماتية من أدلة على الجرائم التي تقع عليها أو بواسطتها في بيانات غير مرئية، لا تفصح عن شخصية معينة عادة، مسجلة إلكترونية بكثافة بالغة، على دعائم أو وسائط من تخزين ممغنطة، لا يترك التعديل فيها أي أثر، يمكن للإنسان قراءتها، وإن كانت قابلة للقراءة من قبل الآلة نفسها، ويعد كشف وتجميع أدلة لإثبات وقوع الجريمة والتعرف على مرتكبها أحد أبرز المشكلات التي يمكن أن تواجه جهات التحرى والملاحقة، وتتعدى هذه المشكلة بشكل عام في سائر مجالات التخزين والمعالجة الآلية للبيانات، حيث تنتمي قدرة ممثلي جهات التحقيق على أن يتولوا بطريقة مباشرة فحص حالات التلاعب في برامج الحاسبات نظراً لتطلب الفحص الكامل قدراً كبيراً من الوقت والعمل غالباً ما لا يكون له من الوجهة الاقتصادية مبرراً.

٣) افتقاد أكثر الآثار التقليدية: قد يتم في بعض العمليات، إدخال البيانات مباشرة في نظام الحاسب دون تطلب وجود وثائق مساندة (وثائق خاصة بالإدخال) كما هو الحال في بعض نظم العمليات المباشرة التي تقوم على إبدال الإذن الكتابي لإدخال البيانات بإجراءات أخرى تعتمد على ضوابط للإذن متضمنة في برنامج الحاسب، وفى العمليات المالية قد يجرى الحاسب بعض العمليات المحاسبية بغير حاجة إلى إدخال كما هو الحال في احتساب الفائدة على الإيداعات البنكية وقيدها آلياً بأرصدة حسابات العملاء على أساس الشروط المتفق عليها مسبقاً والموجودة في برنامج الحاسب؛ إذ يكون من السهل ارتكاب بعض أنواع من الجرائم، كاختلاس المال والتزوير، بإدخال بيانات غير معتمدة في نظام الحاسب أو تعديل برامجه أو البيانات المخزنة داخله دون أن يتخلف ما يشير إلى حدوث هذا الإدخال والتعديل.

٤) إعاقة الوصول إلى الدليل بوسائل الحماية الفنية: تحاط البيانات المخزنة الكترونياً أو المنقولة عبر الشبكات الاتصالية بسياج من الحماية الفنية لإعاقة

المحاولات الرامية للوصول غير المشروع للاطلاع عليها أو استنساخها، كذلك يمكن للمجرم المعلوماتي زيادة صعوبة عملية التفتيش المتوقع عن الأدلة التي تدينه بحزام من التدابير الأمنية يضربه حولها، ويشكل استخدام تقنيات التشفير خاصة لهذا الغرض أحد أكبر العقبات التي تعوق الرقابة على البيانات المنقولة عبر حدود الدولة، والتي تجعل حماية سرقة البيانات الشخصية المخزنة في مراكز الحاسبات أمر بالغ الصعوبة.

٥) سهولة محو الدليل أو تدميره في زمن قصير: من الصعوبات الإضافية التي يمكن أن تعترض العملية الإثباتية في مجال الجرائم المعلوماتية، سهولة محو الجاني أو تدميره لأدلة الإدانة في زمن متناه القصر، فضلاً عن سهولة تنصله عن مسئولية هذا العمل، وهو الأمر الذي يتطلب سرعة إجراء التحقيقات التي تتسم بالخبرة في مجال الجرائم المعلوماتية في إطار من التعاون الدولي مع كافة الدول[١].

٦) الضخامة البالغة لكم البيانات المتعين فحصها: يشكل الكم الهائل للبيانات التي يجرى في الأنظمة المعلوماتية تداولها أحد مصادر الصعوبات التي تعوق تحقيق الجرائم التي تقع عليها أو بواسطتها، أية ذلك أن طباعة لكل ما يوجد على الدعامات الممغنطة لمركز حاسب متوسط الأهمية يتطلب فئات الآلاف من الصفحات التي قد لا تثبت كلها شيئاً على الإطلاق.

٧) إحجام بعض المجني عليهم عن الإبلاغ: عن وقوع مثل هذه الجرائم سواء أكانوا من الأفراد أومن الشركات والمؤسسات المالية والتجارية؛ إذ تتحرى أكثر الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك، أو تمنى بخسائر فادحة من جراء

---

[١] كريستوفر بينتر: التهديد الذي تفرضه الجريمة المعلوماتية والحاجة إلى التعاون الدولي، المؤتمر الدولي السادس للجرائم المعلوماتية الذي نظمته المنظمة الدولية للشرطة الجنائية، القاهرة، ١٣-١٥/٤/٢٠٠٥، ترجمة مركز بحوث الشرطة، ص٦٦.

ذلك على عدم الكشف حتى بين موظفيها عما تعرضت له، وتكتفي باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنباً للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها.

وتشير التقديرات الدولية إلى أن الإبلاغ عن غالبية جرائم تقنية المعلومات (٩٠%) يكون من خلال البلاغات المقدمة من الضحايا من الأفراد والشركات، وأن نسبة التأذي الفعلي من جرائم تقنية المعلومات المبلغ عنها إلى الشرطة تقدر بـ ١%، بينما تشير إحدى الدراسات الاستقصائية الدولية للقطاع الخاص إلى أن ٨٠% من الضحايا الأفراد لا يبلغون عن هذه الجرائم. وتعزى حالات تدني الإبلاغ عن جرائم تقنية المعلومات إلى انعدام الثقة في قدرة أجهزة إنفاذ القانون على التصدي لهذه الجرائم، وعدم الوعي بالإيذاء وآليات الإبلاغ، والشعور بالخجل والارتباك، وتخوف الشركات من المخاطر المتصورة التي قد تهدد سمعتها[١]، ولا شك في أن مواجهة التدني في معدلات الإبلاغ عن جرائم تقنية المعلومات يتطلب مزيداً من التوعية للضحايا من الأفراد، وتطوي الشراكات بين القطاعين العام والخاص من أجل تعزيز عمليات الإبلاغ عن هذه النوعية من الجرائم[٢].

---

[١] انظر: دراسة مكتب الأمم المتحدة المعني بالمخدرات والجريمة حول الجريمة السيبرانية، مرجع سابق، ص ص١٦٨-١٧٢؛ وكذلك انظر: تقرير شركة سايمنتك عن جرائم الانترنت لعام ٢٠١٢ Symantec, 2012. Norton Cybercrime Report 2012.

[٢] انظر: دراسة مكتب الأمم المتحدة المعني بالمخدرات والجريمة، مرجع سابق، ص١٧٣.

المطلب الثاني

إجراءات الاستدلال في جرائم تقنية المعلومات

تبرز الإشارة إلى أن التحقيقات التي تجريها سلطات إنفاذ القانون في جرائم تقنية المعلومات تتطلب مزيجاً من تقنيات عمل الشرطة التقليدية والجديدة، كمراقبة المتهمين في الفضاء الإلكتروني، ومصادرة أو نسخ البيانات من الأجهزة التي تخص المتهم، والحصول على البيانات من أطراف أخرى كمقدمي خدمة الإنترنت، واعتراض المراسلات الإلكترونية[١]، كما أن توسيع نطاق الصلاحيات الإجرائية التقليدية لتشمل المجال الإلكتروني قد يؤدي إلى تحديات بشأن مشروعية جمع الأدلة ومدى مقبوليتها أمام القضاء الجنائي.

ويؤكد البعض[٢]على أهمية تمتع صلاحيات التحقيق بالقدرة على التصدي لبعض التحديات ذات الصلة بجرائم تقنية المعلومات، كالطبيعة الخاصة للأدلة الرقمية

---

(١) تشير دراسة مكتب الأمم المتحدة بشأن الجريمة السيبرانية إلى بعض التقنيات المتصلة بعمل الشرطة في مجال مكافحة جرائم تقنية المعلومات كاعتراض الاتصالات والمراقبة الإلكترونية وتشكيل وحدات سرية تستهدف المجرمين على مواقع التواصل الاجتماعي وغرف المحادثة والرسائل الفورية وخدمات النظراء P2P، ومن أمثلة ذلك، اختراق منتديات قراصنة بطاقات الائتمان عبر الإنترنت وفحص المنتديات التي يستخدمها الجناة في استغلال الأطفال في المواد الإباحية، وتنكر الموظفين المكلفين بإنفاذ القانون كقصر عبر الإنترنت، وفحص خوادم القيادة والسيطرة للبرمجيات الخبيثة. انظر دراسة الأمم المتحدة، مرجع سابق، ص ص١٧٤-١٧٦.

(2) Feigenbaum et al., A Model of Onion Routing with Provable Anonymity. Financial Cryptography and Data Security Lecture Notes in Computer Science, 2007, 4886:57-71; Schwerha, J.J., Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers," Council of Europe Discussion paper, 2010, pp.9-10; Walden, I., Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent. Privacy and Security for Cloud Computing. Computer Communications and Networks 2013, pp.45-71.

التي تتسم بسهولة زوالها وتغيرها، واستخدام الجناة لتقنيات التشويش واستعمال التشفير ووحدات الخدمة النائبة، وخدمة الحوسبة السحابية[١]، ونظم الحاسوب المصابة ببرمجيات خبيثة، ووصلات الإنترنت متعددة الموجة، أو برامج إخفاء الهوية، وهي ما تشكل تحديات خاصة تعترض طريق الصلاحيات التقليدية.

وفي ذات السياق، تشير بعض التقارير إلى ذيوع ممارسة جمع المعلومات عبر المصادر المفتوحة على شبكة الإنترنت؛ إذ يشير تقرير فريق الخبراء التابع للإتحاد الأوروبي إلى أن الوصول إلى البيانات من خلال البحث في المواد المتاحة للجمهور من المصادر المفتوحة عبر شبكة الإنترنت لأغراض العدالة الجنائية من قبيل الممارسات المقبولة بشكل عام[٢].

وقد خول القانون لمأموري الضبط القضائي بعض الاختصاصات والسلطات التي تمكنهم من أداء واجبهم في البحث والتحري عن الجرائم، كما منحهم بعض الاختصاصات في أحوال معينة نص عليها على سبيل الحصر[٣]، وقد حددت المادة ٢٤ إجراءات جنائية الإجراءات التي يجوز لمأمور الضبط القضائي اتخاذها حال وقوع

---

(١) يقصد بالحوسبة السحابية Cloud Computing خدمة تسمح بتحميل البيانات والمعلومات الخاصة بالأفراد على خوادم الإنترنت وتشغيل برامجهم عن بعد، بدلاً من تخزينها على حواسب المنزل أو العمل، أو شراء البرامج وتحديثها، حيث يتم تخزين هذه البيانات والمعلومات في مراكز للبيانات لدى مزودي الخدمات السحابية، وتقدم الحوسبة السحابية مميزات من حيث التكلفة والكفاءة، ولكنها تصاحبها بعض المخاطر، حيث تكون البيانات المخزنة في السحابة جاذبة للمتسللين، وفي حال انقطاع خدمة الحوسبة السحابية تتأثر الأعمال والأشخاص الذين يستخدمونها. انظر: دراسة الأمم المتحدة، مرجع سابق، ص٣٩٩.

(٢) انظر: الولاية القضائية والوصول عبر الحدود الإقليمية: ماهية الخيارات؟، تقرير الفريق العامل عبر الحدود الذي اعتمده T-CY في ٢٠١٢/١٢/٦، مجلس أوروبا، ٢٠١٢، مشار إليه بدراسة مكتب الأمم المتحدة، مرجع سابق، ص١٩١.

(٣) د. محمد عبد اللطيف فرج: شرح قانون الإجراءات الجنائية وفقاً لأحدث التعديلات التشريعية، ج١، ط٣، ٢٠١١، ص٤٦٤.

جريمة ما، فيمايلي: ١- تلقي البلاغات والشكاوى.٢-إجراء التحريات.٣- سماع أقوال الشهود والمشتبه فيهم. ٤- المعاينة.٥- الاستعانة بالخبراء.٦- تحرير محضر بإجراءات الاستدلال.

وتختص إدارة مكافحة جرائم الحاسبات وشبكات المعلومات، بالإدارة العامة لتكنولوجيا المعلومات بوزارة الداخلية، بكافة أعمال الاستدلال في جرائم تقنية المعلومات، من تلقي بلاغات وشكاوى المواطنين ذات الصلة بالجرائم المعلوماتية، وإجراء تحريات وجمع الاستدلالات...إلخ.

الانتقال والمُعاينة في جرائم تقنية المعلومات: يشير البعض[١]– وبحق- إلى أن التحقيق الجنائي في جرائم المعلومات لم يعد ميسوراً لكافة المحققين بوسائل وإجراءات التحقيق التقليدية، لأنه يواجه تقنيات حديثة في أسلوب وطريقة ارتكاب الجريمة، الأمر الذي يقتضي إحداث تطوير في قانون الإجراءات الجنائية يستوعب الإجراءات والوسائل الحديثة في كشف الجريمة وضبط فاعليها بما يواكب استخدام وسائل التقنية والاتصالات الحديثة في ارتكاب الجرائم، ويثير اتخاذ الإجراءات التقليدية في جمع الأدلة، ومنها المُعاينة بعض الإشكاليات في التطبيق.ويقصد بالانتقال ذهاب مأمور الضبط القضائي أو المُحقق الجنائي إلى المكان الذي ارتكبت فيه الجريمة (مسرح الجريمة)، حيث توجد آثارها وأدلتها، أما المُعاينة فيقصد بها قيام مأمور الضبط القضائي أو المُحقق الجنائي بإثبات حالة الأشخاص والأماكن والأشياء ذات الصلة بالجريمة عن طريق المُشاهدة أو الفحص المُباشر بالحواس بهدف جمع الآثار المادية التي تفيد في كشف الحقيقة قبل أن تنالها يد العبث والتخريب[٢]، فالمعاينة

---

[١] مستشار. د/ وليد نبيل طه: مرجع سابق، ص٢٣.

[٢] د. محمد عبد اللطيف فرج: شرح قانون الإجراءات الجنائية، مرجع سابق، ص٢٧٣.

بالمعنى الاصطلاحي هي رؤية مكان أو شخص أو شيء بالعين لإثبات حالته وضبط لكل ما يلزم لكشف الحقيقة بهدف المحافظة عليها خوفاً من إتلافها أو محوها أو تعديلها، وهي أحد إجراءات التحقيق الابتدائي التي يجوز للمحقق اللجوء إليها متى رأى لذلك ضرورة تتعلق بالتحقيق[١].

وتكمن أهمية المعاينة في أنها تتم بمسرح الجريمة بما يحتويه من آثار مادية فعلية، وتهدف المُعاينة إلى التحفظ على هذه الأدلة تمهيداً لفحصها من قبل المُحقق الجنائي لاستخلاص الدلائل والقرائن لإثبات ارتكاب الجاني لجريمته، فينبغي على مأمور الضبط القضائي أو المُحقق الجنائي سرعة الانتقال لمسرح الجريمة لأن ذلك من شأنه التحفظ على الأشياء التي تُساعد على جمع الأدلة المترتبة على ارتكاب الجاني لجريمته قبل أن تمتد إليها يد العبث أو قبل زوال معالمها.

إلا أن الفقه الجنائي يشير إلى حالة جرائم تقنية المعلومات التي يندر أن يتخلف عنها آثاراً مادية، بل قد تطول فيها الفترة الزمنية بين وقوع الجريمة واكتشافها، مما يعرض الآثار الناجمة عنها للعبث بها أو محوها وإتلافها[٢]، والأصل أن يحضر أطراف الدعوى الجنائية المُعاينة، وقد يقرر المُحقق أن يجريها في غيبتهم، ولا يلتزم المحقق بدعوة محامي المتهم للحضور، بل أن محكمة النقض كانت قد قضت

---

[١] د. محمود نجيب حسني: شرح قانون الإجراءات الجنائية، مرجع سابق، ص٥٢٨-٥٢٩؛ د. محمد أبو العلا عقيدة: شرح قانون الإجراءات الجنائية، ج٢، ٢٠٠٠، ص٦٤٤ وما بعدها؛ د. زكى أبو عامر: الإجراءات الجنائية، دار منشأة المعارف، الإسكندرية، الطبعة الثانية، ص٢٣٣.

[٢] د. محمد أبو العلا عقيدة: التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، ٢٦-٢٠٠٣/٤/٢٨، دبي- الإمارات العربية المتحدة، ص٧، منشور على الموقع الإلكتروني www.f-law.net ؛ د. هشام رستم: الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص٥٩.

بأن غياب المتهم عند إجراء المُعاينة ليس من شأنه أن يبطلها[١]، وقد تضمن قانون الإجراءات الجنائية النص على إجراء الانتقال والمُعاينة في المواد أرقام (٣١، ٩٠، ٩٣) إجراءات جنائية.

المُشكلات القانونية الخاصة بمعاينة مسرح جرائم تقنية المعلومات: يشير الفقه الجنائي إلى أهمية التمييز في مسألة مُعاينة مسرح الجريمة في جرائم تقنية المعلومات – حسب محل الجريمة - بين أمرين: (الأول) حالة ارتكاب الجريمة على المكونات المادية للحاسب، (والثاني) حالة ارتكاب الجريمة على المكونات غير المادية أو بواسطتها، وهو ما سوف نشير إليه على النحو التالي:-

أ) ارتكاب الجريمة على المكونات المادية للحاسب:مثل جرائم الاعتداء على أشرطة الحاسب وكابلات وشاشة العرض الخاصة به ومفاتيح التشغيل والأقراص وغيرها من مكونات الحاسب ذات الطابع المادى الملموس، ففي هذه الحالة، فإن الأمر لا يثير أدنى صعوبة للتقرير بصلاحية الجريمة الذي يحوى هذه المكونات لمعاينتها من قبل مأموري الضبط والتحفظ على الأشياء التي تُعد أدلة مادية تدل على ارتكاب الجريمة ونسبتها لشخص معين، وكذا وضع الأختام في أماكن التي تمت فيها المعاينة، وضبط كل ما أستعمل في ارتكاب الجريمة وتحفظ عليه مع إخطار النيابة بذلك.

ب) ارتكاب الجريمة على المكونات غير المادية أو بواسطتها:يأتي في مقدمة هذه الجرائم تلك الواقعة على برامج الحاسب وبيانات أو بواسطتها، وهنا يقرر الفقه الجنائي وجود صعوبات عدة، تحول دون فاعلية المعاينة أو فائدتها، ويمكن تلخيص هذه الصعوبات في عاملين رئيسيين (الأول) قلة الآثار المادية التي قد تتخلف عن

---

[١] مجموعة أحكام محكمة النقض: نقض ١٩٨٠/١/٣١، س٣١، رقم ٢٩، ص١٤٨.

الجرائم التي تقع على برامج الحاسب وبياناته بواسطتها، (والثاني) الأعداد الكبيرة من الأشخاص الذين قد يترددون على مسرح الجريمة خلال المدة الزمنية التي غالباً ما تكون طويلة نسبياً - وذلك ما بين اقتراف الجريمة والكشف عنها - الأمر الذي يمنح فرصة لحدوث تغيير أو تلفيق أو عبث بالآثار المادية أو زوال بعضها وهو ما يلقى ظلال من الشك على الدليل المستقى من المعاينة، وهو ما يتطلب ضرورة توخي الحذر حال إجراء المعاينة في مسرح الجريمة المعلوماتية.

ج) معاينة مسرح الجريمة على شبكة الإنترنت: قد يكون مسرح الجريمة المقرر معاينته من جانب مأمور الضبط القضائي موجوداً على شبكة الانترنت، وترجع صعوبة هذه المعاينة التي يجريها مأمور الضبط القضائي في وقوعها على محل أو مكان افتراضي على شبكة المعلومات، وأنه ليس له مكان محدد يتبع دائرة معينة، بل إنه في معظم الأحيان لا يتم الانتقال الفعلي إلى مكان محدد في جرائم تقنية المعلومات باعتبار أنه يمكن إجراء هذه المعاينة على شاشة الحاسب الآلي خاصة إذا كان على أحد مواقع الإنترنت[١].

وقد اشترط البعض[٢] ضرورة أن يكون الموقع الافتراضي الذي تتم معاينته على شبكة الإنترنت مفتوحاً؛ أي يجوز للعامة الدخول إليه دونما تصريحاً من مشغله، ومن ثم لا تصح المعاينة على شبكة الإنترنت إلا إذا تمت في أحد المواقع المفتوحة التي يمكن لأي شخص مشاهدتها، إما إذا تمت المعاينة في أحد المواقع الخاصة دونما الحصول على تصريح من مشغلها تحول إجراء المعاينة إلى إجراء تفتيش بما يستلزمه من ضمانات قانونية، وإلا أصبح الإجراء باطلاً حابط الأثر.

---

[١] المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٢١١.

[٢] المرجع السابق، ص٢١٠.

القواعد الواجب مُراعاتها عند إجراء المُعاينة في مسرح جريمة تقنية المعلومات: يشير الفقه الجنائي إلى ضرورة مراعاة مجموعة من التعليمات والقواعد حال إجراء المُعاينة في مسرح الجريمة المعلوماتية، وتتمثل هذه القواعد والإرشادات الفنية في الإجراءات التالية[١]:-

١ ـ تصوير الحاسب الآلي والأجهزة الطرفية المُتصلة به، على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة.

٢ ـ ملاحظة طريقة إعداد نظام الحاسب بعناية بالغة.

٣ـ ملاحظة وإثبات حالة توصيلات وكابلات الحاسب والتي تكون متصلة بمكونات النظام وذلك حتى يسهل القيام بعملية مقارنة وتحليل لها عند عرض الموضوع على المحكمة.

٤ ـ عدم التسرع في نقل أية مادة معلوماتية من مكان وقوع الجريمة، وذلك قبل إجراء الاختبارات اللازمة للتيقن من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي حتى لا يحدث أي إتلاف للبيانات المخزنة.

٥ ـ حفظ ما تحويه سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة أو المحطمة ورفع البصمات التي قد تكون على صله بالجريمة المرتكبة.

٦ ـ القيام بحفظ المستندات الخاصة بالإدخال وكذا مخرجات الحاسب الورقية التي قد تكون ذات صلة بالجريمة وذلك من أجل رفع ومضاهاة البصمات التي قد تكون موجودة عليها.

---

[١] د. هشام محمد فريد: الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص٥٩ وما بعدها؛ د. محمد أبو العلا عقيدة: التحقيق وجمع الأدلة: مرجع سابق، ص ص٧، ٨.

٧ ـ قصر عملية المعاينة على مأموري الضبط والمحققين ممن تتوافر فيهم الكفاءة العملية والخبرة الفنية في مجال الحاسبات واسترجاع المعلومات، ممن تلقوا التدريب الكافي لمواجهة هذه النوعية من الجرائم والتعامل مع أدلتها وما تخلفه من أثار على مسرح الجريمة.

مدى جواز إجبار المتهم أو الشاهد على الكشف عن رمز الدخول للحاسب الآلي أو النظام المعلوماتي: تثير جرائم تقنية المعلومات بعض الإشكاليات القانونية، من بينها مدى جواز إجبار المتهم أو الشاهد على الكشف عن رمز للدخول الحاسب الآلي أو النظام المعلوماتي -إن كان يعلم بها- لإجراء المعاينة لمسرح الجريمة المعلوماتية وجمع المعلومات أو الأدلة المتحصلة من الجريمة أو وفقاً لمقتضيات التحقيق أو المحاكمة، والواقع أن موقف التشريعات المقارنة تختلف في هذه المسألة بين تشريعات لا تلزم المتهم أو الشاهد بالإفصاح عن شفرة الدخول أو كلمة السر الخاصة بالحاسب الآلي أو النظام المعلوماتي كالتشريع الياباني والمجري والبولندي، ففي التشريع الياباني لا يلزم مالك الحاسب الآلي المستخدم في جريمة ما التعاون مع جهات التحقيق، أو إفشاء كلمات السر التي يستخدمها؛ إذا ما كان ذلك سيؤدي إلى إدانته، بينما يعطي التشريع المجري والبولندي المتهم الحق في عدم طبع سجلات الحاسب الآلي أو إفشاء كلمات السر أو الأكواد الخاصة بالبرامج، كما يعطي الشاهد أيضاً الحق في الامتناع عن طبع المعلومات المسترجعة من الحاسب الآلي، متى مكن ذلك إلى إدانته أو إدانة أحد أقاربه، بينما يذهب القانون البولندي إلى أبعد من ذلك،حيث ينص على ألا يقابل ذلك أي إجراء قسري أو تفسيره بما يضر مصلحة المتهم، ولاشك في أن ما قررته التشريعات السالف الإشارة إليها ما هو إلا تطبيق لمبدأ عدم جواز مساهمة الجاني في إدانة نفسه.

بينما اختلف الفقه والقضاء في الدول التي لم يشر إلى هذه المسألة، حيث يميز الفقه الجنائي بين موقفي كل من المتهم والشاهد، فبالنسبة للمتهم، يرى جانب من الفقه[١] عدم جواز إجباره على طباعة ملفات بيانات مخزنة داخل النظام المعلوماتي، أو إلزامه بالكشف عن الشفرات أو كلمات السر الخاصة بالدخول الى هذه المعلومات، أو إجباره على تقديم الأمر اللازم لوقف الفيروس أو القنبلة المنطقية، مستنداً في ذلك إلى قاعدة عدم إلزام الشخص باتهام نفسه، سواء عن طريق الشهادة، أو عن طريق تقديم عناصر الإثبات[٢]، وأن من حق المتهم الامتناع عن الإجابة أو الالتزام بالصمت دون أن يؤخذ ذلك على أنه قرينة لإدانته، ويشير الرأي السابق إلى أنه إذا كان الراجح فقهاً وقضاءً[٣] أنه لا يجوز إجبار الشخص على الإدلاء بأقوال لها دلالة الشهادة ضد نفسه، إلا أنه يجوز إجباره بأمر قضائي على كشف رمز الدخول لنظام الحاسب الآلي[٤].

ويضيف الرأي السابق إلى وجود عدة وسائل للضغط على المتهم في الجرائم المعلوماتية، فقد يؤدي رفض المتهم التعاون مع سلطات التحقيق والمحاكمة إلى التأثير السلبي على عقيدة القاضي فيحكم بإدانته، أو اتجاه سلطة التحقيق إلى حبسه احتياطياً، إذا كانت الجريمة مما يجوز فيها الحبس الاحتياطي، كما قد توحي سلطات التحقيق للمتهم بأن عدم تعاونه الإيجابي معهم أثناء التفتيش قد يؤدي إلى عدم ضبط النظام المعلوماتي فى مجموعه[٥].

---

(١) انظر من الفقه المصري: د. جميل الصغير: الحاسب الآلي كوسيلة لإثبات الجريمة، ندوة "الواقع الأمني مسئوليات- إنجازات" التي نظمها مركز بحوث الشرطة، القاهرة، ٢٠١١/١/٩، ص١٨.

(٢) انظر من الفقه المصري: د. جميل الصغير: الحاسب الآلي كوسيلة لإثبات الجريمة، مرجع سابق، ص١٨، ومن الفقه الفرنسي انظر:

VERGUCHT (Pascal), La repression des délits informatiques dans une perspective internationnale, Thése, Montpellier 1, 1996, N° 324, P. 401.

(٣) نقض ١٧ مايو ١٩٦٠، مجموعة أحكام محكمة النقض، س ١١، رقم ٩٠، ص٤٦٧.

(٤) د. جميل الصغير: الحاسب الآلي كوسيلة لإثبات الجريمة، مرجع سابق، ص١٩.

(٥) الموضع السابق.

بينما يذهب رأي آخر[١] إلى اعتبار هذا الإجبار من قبيل التفتيش -وهو إجراء من إجراءات التحقيق- الذي يخضع للقواعد العامة المقررة في الإجراءات الجنائية لصحته سواء في حالة التلبس أو الحصول على إذن، مع مراعاة الحصول على إذن بتفتيش المسكن إذا كان جهاز الحاسب الآلي به.

أما بالنسبة للشاهد، فالأمر مختلف؛ إذ يرى الرأي السابق أنه إذا كانت الشهادة تنصب على ما رآه الشاهد بإحدى حواسه فإنه يكون من الصعب أن نطلب منه أن يقدم مساعدته للكشف عن الدليل أو الوصول إليه، فلا يجوز مثلاً إجبار العامل الفني لأحد الأنظمة المعلوماتية أن يقوم- لحساب البوليس- بطباعة أو تحليل ذاكرة النظام المعلوماتي ليكشف له عن آثار بعض البيانات، فهذا البحث يدخل في اختصاص الخبير القضائي[٢].

ويشير الرأي السابق إلى بعض التطبيقات التشريعية في دول السويد وفنلندا والنرويج، حيث تنص تشريعاتها على أنه يقع على عاتق الشهود واجب بأن ينعشوا الذاكرة بفحص الأماكن والمستندات التى توجد تحت سيطرتهم، إذا لم تترتب على ذلك أضرار خطيرة[٣]، كما أنه فى بعض الدول الأنجلو أمريكية، يتسع فيها الالتزام بالتعاون ليس فقط لمجرد إصدار الأمر بإحضار الشهود، أو لإحضار بعض المستندات، وإنما إلزام الغير بتقديم المساعدة للسلطة القضائية عن طريق تقديم الأدلة أو المساعدة فى الوصول إليها، فالقانون الإنجليزي الصادر عام ١٩٨٤ بشأن البوليس والأدلة الجنائية يعطي للمحققين أن يطلبوا من الغير أن يمكنوهم من الدخول الى المعلومات المختزنة

---

[١] المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٢٢٤.

[٢] د. جميل الصغير: الحاسب الآلي كوسيلة لإثبات الجريمة، مرجع سابق، ص٢٠.

[٣] الموضع السابق.

في الحاسب الآلي أو الإطلاع عليها أو قراءتها، كما يتضمن التشريع الأمريكي قانون خاص بتعاون متعهدي خدمات الرسائل فى مجال الاتصالات الإلكترونية المسجلة[١].

بينما تجيز المادة (١٢٥) من قانون الإجراءات الجنائية الهولندي لقاضي التحقيق أن يأمر أي شخص، يفترض فيه أنه على علم بكيفية الدخول الى المعلومات المختزنة فى الحاسبات الآلية، للمساهمة مع سلطات التحقيق فى الكشف عن الحقيقة، طالما أن هذه المعلومات تم تخزينها أو معالجتها أو نقلها عن طريق نظام المعالجة الآلية للبيانات أو ُيمكن قاضي التحقيق من الدخول إلى هذه المعلومات. والأمر هنا يقتصر على المعلومات التى استخدمت فى ارتكاب الجريمة فحسب.

وطبقاً للمادة السابقة إذا كانت مصلحة التحقيق تقتضي فك شفرة البيانات يكون لقاضي التحقيق أن يأمر شخص يفترض فيه معرفة تشغيل نظام أمن المعالجة الآلية أثناء التفتيش- أن ُيمكنه من الدخول إلى أنظمة المعالجة الآلية أو فى جزء منها، أو أن يقوم بفك الشفرات. ويجب أن يوجه الأمر إلى الشخص الذي يفترض فيه العلم بكيفية فك الشفرة[٢].

كما تسمح بعض التشريعات بالاستفادة بالشهود كخبراء أو كمعاونين للقضاء، وذلك من تلقاء أنفسهم، وعلى ذلك فالشاهد أو القائم على تشغيل النظام المعلوماتي يلتزم بالكشف عن الشفرات أو كلمات السر التى يكون على علم بها، ولا يعفيه من ذلك سوى الالتزام بالسر المهني[٣]، ومع ذلك فليس ثمة جزاء جنائي يوقع على الشاهد إذا

---

[١] د. جميل الصغير: الحاسب الآلي كوسيلة لإثبات الجريمة، مرجع سابق، ص٢١.

[٢] الموضع السابق.

[٣] انظر: د. جميل الصغير، المرجع السابق، ص٢٣؛ وعكس ذلك د. هشام محمد فريد رستم، المرجع السابق، ص ٨٤.

رفض تقديم المعلومات المطلوبة إلا إذا وقع ذلك فى مرحلتي التحقيق الابتدائي والمحاكمة[١].

ويشير الرأي السابق إلى بعض الحالات التي تعاونت فيها شركات الخدمات المعلوماتية المباشرة مع سلطات التحقيق كشركة كمبيوسرف سبق أن تعاونت مع سلطات التحقيق لوقف البريد الإليكتروني، وفى حالة تحديد هوية المشتركين فى الإنترنت والذين يقومون بالتحرش الجنسي أو يرتكبون جرائم ضد القصر[٢].

ويرى جانب من الفقه[٣] أن الالتزامات التى فرضها قانون الإجراءات المصري على الشاهد لا تتضمن التزامه بالمعاونة الفعالة فى التحقيق الجنائي الذي يجري بشأن الجريمة التى يدلي فيها بشهادته، فالشاهد غير ملتزم إلا بالإجابة على الأسئلة المنصبة على ما سمعه أو رآه بنفسه من الوقائع المتعلقة بثبوت ارتكاب الجريمة وظروفها ونسبتها الى المتهم من عدمه، ومن ثم فلا يمكن إلزامه بالإدلاء بما لديه من معلومات لازمة لولوج الحاسب الآلي أو النظام المعلوماتي تنقيباً عن أدلة الجريمة داخله[٤]، فالشاهد غير ملزم بالتعاون فيما يجاوز ما يعلمه، وبالتالي فلا مجال لتحميل غير الملتزمين بالشهادة بواجب الإدلاء بمثل هذه المعلومات[٥].

ويشير الرأي السابق[٦] إلى عدة وسائل للضغط على الشهود لحملهم على التعاون مع سلطات التحقيق، ففي بعض الدول يسأل الشاهد الذي يخفي الشفرة أو كلمة

---

[١] د. جميل الصغير: الحاسب الآلي كوسيلة لإثبات الجريمة، مرجع سابق، ص٢٢.

[٢] الموضع السابق.

[٣] المرجع السابق، ص٢٣.

[٤] د. هشام محمد فريد رستم، الجوانب الإجرائية، المرجع السابق، ص ٩١.

[٥] المرجع السابق، ص٩٢.

[٦] د. جميل الصغير: الحاسب الآلي كوسيلة لإثبات الجريمة، مرجع سابق، ص٢٣.

السر أو الذي يعطي أوامر خاطئة عن جريمة شهادة الزور؛ لأنه يعوق سير العدالة، أو يسأل باعتباره شريكاً فى الجريمة موضوع المحاكمة، كما يمكن الضغط على الشهود عن طريق التهديد بضبط النظام المعلوماتي فى مجموعة أو وضعه تحت الجمع الأحمر، فهذه الإجراءات الخطيرة بالنسبة للمتهم قد تدفع الشاهد إلى التعاون الفعال والإيجابي مع سلطات التحقيق أو الحكم.

المبحث الرابع

إجراءات التحقيق الجنائي في جرائم تقنية المعلومات

تقسيم: تقترن جرائم تقنية المعلومات بأنماط ودرجات من التكنولوجيا تقتضى أن يستخدم في تحقيقها، بجانب قواعد وأساليب التحقيق الجنائي الفني المعروفة، تقنيات خاصة، كما تتطلب فيمن يتولى تحقيقها أن يكون متخصصاً في التحقيق الجنائي ومعالجة البيانات والمراجعة والمحاسبة، والقواعد الفنية التي يوصى أكثر الخبراء بالاسترشاد بها لإجراء تحقيقات ناجحة في جرائم تقنية المعلومات يتمركز أبرزها في إجراء تحرى أولى، بوسائل ومواصفات تلاءم طبيعة وخصائص بيئة تكنولوجيا المعلومات[١]. ويستهدف الاستدلال الأولى الحصول على أكبر قدر ممكن من المعلومات عن السلوك المكون للجريمة المعلوماتية وأسلوب وظروف ارتكابها، وجمع هذه المعلومات يمكن أن يتم، بصفة مبدئية عن طريق مقابلات استطلاعية تجرى مع ممثلي الجهة المجني عليها، وعلى طبيعة السلوك الإجرامي المرتكب يتحدد نطاق وتوقيت هذا الاستدلال والوقت الذي يستلزمه[٢]، وفيما يلي نتناول أوامر التحقيق ذات الصلة بالتنقيب عن الأدلة الرقمية ، وذلك في أربعة مطالب، وذلك على النحو التالي:-

---

[١] د. جميل عبد الباقى الصغير: الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية،٢٠٠٢، ص٢٨وما بعدها.

[٢] يجب مراعاة عدة عوامل أهمها: أن الدليل المسند إلى المعالجة الآلية للبيانات يمكن أن يكون متاحاً لفترة قصيرة من الزمن، كما أن الجريمة التي يجرى التحرى بشأنها يمكن أن تكون متمادية مستمرة سواء من حيث نتائجها أو تنفيذها، وأن الجريمة التي يجرى التحرى بشأنها يمكن أن تكون ستاراً لفعل إجرامي آخر، ويظهر الاستدلال الأولى عدة حقائق أهمها التثبت من وقوع الجريمة، ونمط وطبيعة الجريمة المرتكبة، والتقنيات المستخدمة في ارتكابها، والجناة المحتملون أو المشتبه فيهم، والأسباب والدوافع المحتملة لارتكاب الجريمة، والاستدلال على الشهود في حالة وجودهم. انظر: د. هشام محمد فريد رستم: الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص٣٢.

المطلب الأول

أوامر التحقيق ذات الصلة بالتنقيب عن الأدلة الرقمية[١]

وضع القانون تنظيماً دقيقاً للقرارات والأوامر الجنائية المؤقتة بالمادة السادسة والتي تصدر من المحكمة المختصة بناء على طلب النيابة العامة، في أحوال ضبط أو التحفظ على البيانات والمعلومات وتتبعها أو البحث والتفتيش والنفاذ إلى برامج الحاسب وقواعد البيانات، أو أمر مقدمي الخدمة بتشفير ما لديه من بيانات أو معلومات موجودة تحت سيطرته أو مخزنة لديه، وبيانات مستخدمي خدمته، حيث نظم القانون الأوامر القضائية الوقتية المسببة التي تصدر من سلطة التحقيق المختصة، لجهات الضبط القضائي، لمدة لا تزيد على ثلاثين يوماً قابلة للتجديد لمرة واحدة، في أحوال الضبط أو السحب أو الجمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات، وتتبعها مع تسليم أدلتها الرقمية للجهة مُصدرة الأمر، أو البحث والتفتيش والنفاذ والدخول إلى برامج الحاسب وقواعد البيانات، مع إلزام مقدم الخدمة بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتي أو جهاز تقنى موجودة تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمي خدمته وحركة الاتصالات التي تمت

---

[١] ومن أبرز الإجراءات التحقيقية في جرائم تقنية المعلومات في التشريع المقارن أوامر البحث والمصادرة، وتشمل (البحث عن البيانات وأجهزة الحاسب- مصادرة البيانات وأجهزة الحاسب)، والأوامر الخاصة بالبيانات، وتشمل الأمر الصادر لأي من الأشخاص لإمداد سلطات إنفاذ القانون بـ(معلومات عن أحد المشتركين- حركة البيانات المخزنة- محتوى البيانات المخزنة)، والوقت الحقيقي المستغرق لجمع (حركة البيانات- محتوى البيانات)، وقرارات التحفظ على البيانات وتشمل الأمر الصادر لأي من الأشخاص بالحفاظ على سلامة البيانات وصيانتها ووضعها تحت سيطرتهم لفترة زمنية محددة "الأمر المعجل بالتحفظ على البيانات، علاوة على استخدام التحاليل الجنائية الحاسوبية عن بعد، والوصول المباشر من جانب سلطات إنفاذ القانون للبيانات الحاسوبية خارج حدود الدولة "الوصول للبيانات الحاسوبية عبر الحدود". انظر في تفصيلات ذلك: دراسة مكتب الأمم المتحدة، مرجع سابق، ص١١٧ وما بعدها.

على ذلك النظام أو الجهاز التقني، ويكون استئناف الأوامر أمام المحكمة الجنائية المختصة منعقدة في غرفة المشورة، حيث تقضي المادة (٦) المعنونة بالأوامر القضائية المؤقتة بأنه: "*الجهة التحقيق المختصة، بحسب الأحوال، أن تصدر أمراً مسبباً لمأموري الضبط القضائي المختصين، لمدة لا تزيد على ثلاثين يوماً قابلة للتجديد لمرة واحدة، متى كان لذلك فائدة في ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون، بواحد أو أكثر مما يأتي:-*

١ - ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات أو تتبعها في أي مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه. ويتم تسليم أدلتها الرقمية للجهة مصدرة الأمر، على ألا يؤثر ذلك على استمرارية النظم وتقديم الخدمة إن كان لذلك مقتض.

٢ - البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقاً لغرض الضبط.

٣ -أن تأمر مقدم الخدمة بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتي أو جهاز تقنى موجودة تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمي خدمته وحركة الاتصالات التي تمت على ذلك النظام أو النظام التقني. وفى كل الأحوال، يجب أن يكون أمر جهة التحقيق المختصة مسبباً.

ويكون استئناف الأوامر المتقدمة أمام المحكمة الجنائية المختصة منعقدة في غ ة المشورة، في المواعيد ووفقاً للإجراءات المقررة بقانون الإجراءات الجنائية"[1].

---

[1] ومن أبرز هذه الصكوك الدولية متعددة الأطراف المعنية بمكافحة جرائم تقنية المعلومات التي تضمنت أحكام تتعلق بالأوامر الخاصة بالحصول على البيانات المخزنة الاتفاقية العربية بشأن =

ويتضح من النص السابق أن المشرع المصري قد أجاز لجهات التحقيق في الجرائم المعلوماتية إصدار بعض الأوامر القضائية لجهات الضبط القضائي، بهدف البحث والتنقيب عن الأدلة الإلكترونية، وقد أبان القانون لجهات التحقيق الأحوال والمبررات التي تستند عليها في إصدار مثل هذه الأوامر، بأن يكون لها فائدة في إظهار الحقيقة في إحدى الجرائم المنصوص عليها في القانون.

المدة القانونية لسريان أوامر التحقيق ذات الصلة بالتنقيب عن الأدلة الرقمية: حدد القانون لسلطات التحقيق المدة القانونية لسريان قراراتها القضائية ذات الصلة بالتنقيب عن الأدلة، بأن يصدر هذه الأوامر لمدة لا تزيد على ثلاثين يوماً قابلة للتجديد مرة واحدة.

تسبيب القرارات القضائية الصادرة بشأن الجرائم المعلوماتية: كما تطلب القانون من جهات التحقيق أن تكون القرارات القضائية الصادرة منها بشأن الجرائم المعلوماتية مسببة، وترجع العلة من تقرير ضرورة تسبيب مثل هذه القرارات القضائية، في منح المحكمة المختصة سلطة رقابة جهات التحقيق في إصدارها لهذه القرارات، وتمكين المتهم من الطعن على هذه القرارات أمام المحكمة الجنائية المختصة منعقدة في غرفة المشورة.

استئناف الأوامر القضائية ذات الصلة بالتنقيب عن الأدلة الرقمية: حدد القانون إجراءات استئناف الأوامر القضائية الصادرة عن جهات التحقيق للتنقيب عن الأدلة الرقمية، بأن ذلك يكون أمام المحكمة الجنائية المختصة منعقدة في غرفة

=

مكافحة جرائم تقنية المعلومات (م١/٢٥)، واتفاقية بودابست (الاتفاقية الأوروبية) بشأن الجريمة الإلكترونية (م١/١/١٨أ)، انظر: دراسة مكتب الأمم المتحدة المعني بالمخدرات والجريمة بشأن الجريمة السيبرانية، مرجع سابق، ص ص١٨٦.

المشورة، في المواعيد، ووفقاً للإجراءات المقررة بقانون الإجراءات الجنائية، ومن ثم إذا كانت الجريمة المنسوبة إلى المتهم من جرائم الجنح، فإن الاستئناف يكون أمام المحكمة الجزئية المختصة منعقدة في غرفة المشورة، بينما إذا كانت الجريمة المنسوبة إلى المتهم جناية، فإن الاستئناف يكون أمام محكمة الجنايات المختصة منعقدة في غرفة المشورة.

صور الأوامر القضائية ذات الصلة بالتنقيب عن الأدلة الرقمية: حدد القانون هذه الأوامر القضائية التي تصدرها جهات التحقيق لجهات الضبط القضائي للتنقيب عن الأدلة الرقمية، وتتمثل هذه الأوامر القضائية فيمايلي:-

١) الأمر بضبط البيانات والمعلومات والتحفظ عليها وتتبعها: وقد نص القانون على أن يكون الأمر القضائي المسبب الصادر من جهات التحقيق بضبط، أو سحب، أو جمع، أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات، وتتبعها في أي مكان، أو نظام، أو برنامج، أو دعامة إلكترونية، أو حاسب تكون موجودة فيه، وكان القانون قد عرف الدعامة الإلكترونية بأنها:"أي وسيط مادي لحفظ وتداول البيانات والمعلومات الإلكترونية ومنها الأقراص المدمجة أو الأقراص الضوئية أو الذاكرة الإلكترونية أو ما في حكمها"، على أن يتم تسليم أدلتها الرقمية للجهة مصدرة الأمر، وألا يؤثر ذلك في استمرارية النظم وتقديم الخدمة إن كان لذلك مقتضٍ[١].

[١] ومن التشريعات المقارنة التي سمحت بضبط الأدلة الرقمية التشريع الفرنسي والبلجيكي، حيث نظم قانون الإجراءات الجنائية الفرنسي ضبط كافة المعلومات المدونة على الحاسب الآلي أو الإنترنت، وذلك بوضع جهاز دون علم المتهم في جميع الأماكن الخاصة للاطلاع على المعلومات الإلكترونية وتسجيلها والاحتفاظ بها ونقلها، حيث يتم ذلك بمعرفة مأمور الضبط القضائي المختص بعد ندبه من قاضي التحقيق (المواد ٧٠٦-١٠٢-١ إلى ٧٠٦-١٠٢-٩ من القانون رقم ٢٦٧ الصادر في ٢٠١١/٣/١٤)، كما أجازت المادة (٣٩مكرراً) من قانون تحقيق الجنايات البلجيكي نسخ المواد المخزنة في نظم المعالجة الآلية للبيانات بقصد عرضها على الجهات القضائية. ومن التشريعات =

٢) الإذن بتفتيش البرامج والنظم المعلوماتية والدخول إليها بغرض الضبط: كما نص القانون على أن يكون الأمر القضائي المسبب الصادر من جهات التحقيق بالبحث والتفتيش، والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقاً لغرض الضبط[١]، وهو ما سوف نتناوله بشكل أكثر تفصيلاً في الفرع القادم

٣) الأمر بتسليم البيانات والمعلومات، وهذا الأمر يخص مقدم الخدمة، وقد نص القانون على أن يكون هذا الأمر بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتي أو جهاز تقنى، موجودة تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمي خدمته، وحركة الاتصالات التي تمت على ذلك النظام أو الجهاز التقني.

ويلاحظ أن هذه الأوامر القضائية تتشابه مع بعض الإجراءات الجنائية التقليدية، وهي الأمر بضبط الأشياء، والأمر بتفتيش الأماكن، ونرى أنه كان من المتوجب على المشرع المصري أن يضع تنظيماً لإجراء تفتيش البرامج والنظم المعلوماتية وضبط الأشياء المتحصلة عنه على النحو الذي ذهبت إليه بعض التشريعات

=

العربية التي أجازت لمأموري الضبط ضبط الأجهزة والأدوات المستخدمة في ارتكاب الجرائم المعلوماتية التشريع الأردني (م١٣). انظر: المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص ص٢٢٨، ٢٢٩؛ د. عمر محمد بن يونس: مذكرات في الإثبات الجنائي عبر الإنترنت، ندوة الدليل الرقمي التي نظمتها جامعة الدول العربية، القاهرة، خلال الفترة (٥-٨ مارس٢٠٠٦)،ص١٢.

[١] ومن التشريعات العربية التي أجازت لمأموري الضبط الدخول لأي مكان يشتبه في ارتكاب جريمة معلوماتية به وتفتيش الأجهزة والأدوات التي يشتبه استخدامها في ارتكاب الجرائم المعلوماتية التشريع الأردني (م١٣).

المقارنة على النحو التالي ذكره لاحقاً[١]، ويهمنا في هذا المقام أن نشير إلى إجرائي تفتيش الأماكن وضبط الأشياء في الجرائم المعلوماتية بشيء من التفصيل على النحو التالي ذكره لاحقاً.

الأمر بتسجيل الاتصالات الإلكترونية: أشار جانب من الفقه الجنائي[٢] إلى مسألة تسجيل الاتصالات الإلكترونية في جرائم تقنية المعلومات والتي قد يستلزم

---

[١] من الجدير بالذكر أن مشروع قرار رئيس مجلس الوزراء بإصدار اللائحة التنفيذية للقانون رقم ١٧٥ لسنة ٢٠١٨ كان قد تضمن مادة برقم (٦) تنص على أنه:" على مأموري الضبط القضائي المختصين وفقاً للأمر المسبب من جهة التحقيق المختصة القيام بالإجراءات الواردة في المادة رقم (٦) من القانون، وفق الضوابط التالية: أن تتم عملية ضبط أو جمع أو الحصول أو استخراج أو التحفظ على الأدلة الرقمية محل الواقعة، واستخراج النسخ الرقمية Digital Forensic Images من هذه الأدلة بأجهزة أو معدات أو برامج أو بأدوات البحث الجنائي الرقمي وبأساليب تقنية مثل Write Blocker أو ما يماثلها بما يضمن عدم تغيير أو تحديث أو محو أو تحريف للكتابة أو البيانات والمعلومات، أو أي تغيير أو تحديث أو إتلاف للأجهزة أو المعدات أو البيانات والمعلومات، أو أنظمة المعلومات أو البرامج أو الدعامات الإلكترونية وغيرها. ويجب أن تُثبت الإجراءات بمحضر الضبط وتقرير الفحص المبدئي وفقاً لما يلي: ١-أن تكون عملية البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات والأجهزة والنظم المعلوماتية، وفقاً للنطاق المحدد بقرار جهة التحقيق المختصة أو المحكمة، أو بتصريح مكتوب من صاحب الشأن وأن تكون مرتبطة فقط بالواقعة. ٢- معاينة وتوصيف وتصوير عملية الضبط ومسرح الجريمة أو الواقعة قبل عمليات الفحص والتحليل، وتوثيق مكان الضبط. ٣-توثيق وتسجيل الأرقام المسلسلة للأجهزة والمعدات المضبوطة مع تحديد أنواعها ومواصفاتها وأي ملحقات أخرى. مع بيان النظم والبرامج والتطبيقات وبياناتها إن أمكن. ٤- توصيف كيفية وأسلوب التحفظ على الأدلة وتحريزها ومكان حفظها لحين تسليمها لجهات الفحص والتحليل، مع توثيق كود وخوارزم Hash الناتج عن استخراج نسخ مماثلة ومطابقة للأصل من الأدلة الرقمية. ٥- في حالات الضبط التي يتضح فيها وجود تشفير مستخدم على الأجهزة أو المعدات أو البيانات أو المعلومات أو النظم المعلوماتية، يتم الفحص أثناء عملية الضبط وتوثيق وإثبات ذلك بمحضر الضبط والفحص المبدئي. ويتم الاسترشاد بمعيار الأيزو ISO 27037 كنموذج مرجعي للتعامل مع الأدلة الرقمية".

[٢] د. أحمد فتحي سرور: الوسيط في قانون الإجراءات الجنائية، مرجع سابق، ص٩٥٨؛ المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص ٢٢٩؛ د.محمد الألفي: الجرائم المضرة بأمن الدولة عبر الإنترنت، مرجع سابق، ص٣٧٧.

الكشف عنها إجراء هذا التسجيل، فهذا الأمر جائز بعد الحصول على إذن مسبب من القاضي الجزئي لمدة لا تزيد على ثلاثين يوماً، ويجوز له أن يجدد هذا الإذن مدة أو مدد مماثلة وفق القواعد العامة الواردة في المادتين ٩٥، ٣/٢٠٦ من قانون الإجراءات الجنائية، حيث يرى الرأي السابق أن هذه القواعد العامة تمتد لتسجيل كافة المحادثات، بما فيها المحادثات الإلكترونية، وأن العلة في اشتراط صدور إذن من القاضي الجزئي بالنظر إلى أن مراقبة المحادثات تختلف عن التفتيش، وهي تعد أشد وطأة في مساسها بحرمة الحياة الخاصة.

وقد قررت اللجنة المعنية بحقوق الإنسان بالأمم المتحدة أنه لا يعتبر اعتراض وتسجيل حركة البيانات بناءً على إذن كتابي من أحد قضاة التحقيق في سياق التحقيق القضائي الابتدائي بشأن تورط أحد الأفراد في إحدى الجماعات الإجرامية المنظمة، انتهاكاً لحق الخصوصية، وأوضحت اللجنة أن التشريع الذي بموجبه يصدر الإذن يجب أن يفصل الظروف المحددة التي تجيز التدخل، واعتباره مناسباً وضرورياً لتحقيق الأغراض المشروعة المتوخاة من مكافحة الجريمة[1].

المطلب الثاني

الأمر بالتحفظ على البيانات والمعلومات وضبطها

أجازت المادة السادسة من القانون لجهة التحقيق المختصة أن تأمر بضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات أو تتبعها في أي مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه، على أن

---

[1] انظر: قرار اللجنة المعنية بحقوق الإنسان بالأمم المتحدة في البلاغ CCPR/C/82/D/903/1999، مشار إليه دراسة مكتب الأمم المتحدة، مرجع سابق، ص٢٠٠.

يتم تسليم أدلتها الرقمية للجهة مصدرة الأمر، وألا يؤثر ذلك على استمرارية النظم وتقديم الخدمة إن كان لذلك مقتضٍ.

ويتضح من النص السابق أن المشرع المصري أشار إلى عدد من الإجراءات التي تستهدف جمع الأدلة الرقمية، والتي تشمل كل من التحفظ على البيانات والمعلومات وجمعها وتتبعها وسحبها لغرض الضبط وضبطها بالفعل، ولاشك في أن هذه الإجراءات تتماشى مع الطبيعة المعنوية الخاصة للبيانات والمعلومات وتتوافق مع النظام المعلوماتي، والتي تتطلب وتفترض إجراءات خاصة للتعامل معها بغرض ضبطها، وتسهيل إجراءات التحصل عليها من جانب السلطات العامة وأجهزة إنفاذ القانون، ولاشك في أن هذه الإجراءات مستحدثة وغير مألوفة في القواعد الإجرائية التقليدية المستخدمة في جمع الأدلة.

ومن جانب آخر، حرص المشرع المصري على أن تشمل إجراءات التحفظ على البيانات والمعلومات وضبطها كافة صور الإجراءات والتدابير التي تتناسب مع الطبيعة الخاصة للبيانات والمعلومات كجمع المعلومات وسحبها وتتبعها، والتحفظ عليها وضبطها، وذلك على النحو التالي:-

أ) الأمر بجمع البيانات والمعلومات: يفترض الأمر بجمع البيانات والمعلومات وجودها في أكثر من موقع أو خادم، ومن ثم تكليف مقدمي الخدمي بجمع هذه البيانات والمعلومات من مصادرها المتفرقة، ويهدف هذا الإجراء إلى تسهيل مهمة الجهات القائمة بجمع الأدلة.

تجميع البيانات في المواثيق الدولية والتشريع المقارن: ومن المواثيق الدولية التي أجازت للدول تجميع البيانات اتفاقية بودابست، حيث نصت المادة (٢٠) من الاتفاقية على التجميع في الوقت الفعلي لخط سير البيانات، وذلك بأن تتبنى الدول

الأطراف تشريعات تخول سلطة معينة القيام بجمع أو تسجيل عن طريق وسائل معينة موجودة على أرضها البيانات المتعلقة بخط سير البيانات في الوقت الصحيح، أو إلزام مقدم الخدمة في حدود قدرته الفنية بجمع وتسجيل البيانات المتعلقة بخط سير البيانات في الوقت الصحيح. ويختلف إجراء التجميع في الوقت الفعلي للبيانات المتعلقة بخط سير البيانات عن إجراء التحفظ السريع على البيانات المتعلقة بخط سير البيانات الذي نصت عليه المادة (١٦) من الاتفاقية في أن البيانات في حالة التحفظ موجودة لدى مقدمة الخدمة أي مخزنة بالنظام المعلوماتي للكمبيوتر أو في دعامة التخزين.

بينما في حالة التجميع أو التسجيل فالبيانات ليست مخزنة ويهدف هذه الإجراءات إلى جمعها أو تسجيلها وقت مباشرة الاتصال وهذا ما عبرت عنه الاتفاقية بالوقت الفعلي أو الصحيح، ولهذا فهو يحتاج إلى وسائل تقنية حديثة قد لا تتوفر لدى السلطة المختصة أو قد لا يكون بمقدورها القيام به وعلى ذلك أسندت الاتفاقية القيام بإجراء التجميع أو التسجيل للسلطة المختصة في الدول لتقوم به بنفسها أو تنفذه من خلال مقدم الخدمة أو بمساعدته، وهو ما نص عليه القانون الأمريكي في المادة (usc 18 2703) وكذلك القانون الفرنسي في قانون الإجراءات الجنائية في مادته (٢/٦٠ إجراءات).

كما نصت المادة (٢١) من الاتفاقية على ضرورة تبنى كل دولة طرف تشريعات تخول سلطة معينة القيام باعتراض محتوى البيانات المتعلقة بجرائم خطيرة ويتم الاعتراض بأحد الإجرائيين: (الأول) قيام السلطة المختصة بإجراءات التجميع أو التسجيل لمضمون البيانات، (والثاني) إلزام مقدم الخدمة بتجميع أو تسجيل محتوى البيانات.والمقصود باعتراض مضمون البيانات جمع أو تسجيل مضمون البيانات التي تنقل عبر وسائل الاتصال في حينها حتى تتمكن السلطات المختصة في الدولة من التعرف على الاستخدامات غير المشروعة لأنظمة الاتصالات بما يكفل منع ارتكاب العديد من الجرائم.

والأصل أن إجراء اعتراض مضمون البيانات تباشر سلطة معينة بالدولة، إلا أن الاتفاقية أجازت إلزام مقدم الخدمة للقيام به على أساس أنه قد تتوافر لديه الإمكانيات الفنية اللازمة لذلك، ويلاحظ بأن هذا الإجراء يختلف عن إجراء التحفظ السريع على مضمون البيانات الذي نصت عليه المادة (١٦) من الاتفاقية في أن البيانات المطلوب التعرف على مضمونها مخزنة، ويلتزم مقدم الخدمة بالتحفظ عليها، بينما يعد الاعتراض على مضمون البيانات نوعاً من المراقبة المعاصرة للاتصال، وجميع وتسجيل مضمون أية اتصالات تتعلق بمسائل غير مشروعة[١].

ب) الأمر بسحب البيانات والمعلومات: يفترض استخلاصها وإخراجها من الحاسب الآلي أو من النظام المعلوماتي بغرض ضبطها، ومن ثم يفترض هذا الأمر وجود البيانات والمعلومات داخل نظام معلوماتي ما وتكليف الجهة المسئولة عن هذا النظام باستخلاص البيانات والمعلومات التي تراها جهة التحقيق ذات صلة بجريمة ما. ومن التشريعات المقارنة التي أجازت الأمر بسحب البيانات التشريع البلجيكي، والذي أجاز لسلطات التحقيق سحب البيانات التي سبق أخذ نسخة منها، من الجهاز في الحالات الآتية: ١- إذا كانت محلاً للجريمة أو ناتجة عنها. ٢- إذا كانت مخالفة للنظام العام أو حسن الآداب. ٣- إذا كانت تمثل خطراً على الأنظمة الإلكترونية. ٤-إذا كانت تمثل خطراً بالنسبة للمعلومات المخزنة أو المعالجة أو المرسلة بهذه الأنظمة (م٣٩ مكرراً من قانون تحقيق الجنايات البلجيكي)[٢].

---

[١] نص المشرع الأمريكي على هذا الإجراء في المادة (18 usc 2703)، وقد أشارت المادة بضرورة أن يصدر الأمر باتخاذ هذا الإجراء من المحكمة أو من الإدارة العليا للعدل على ألا تزيد مدة الاعتراض عن ٣٠ يوماً، كما نص علي هذا الإجراء قانون الإجراءات الفرنسي في المادة ٩٥/٧٠٦. أنظر: مستشار د. وليد نبيل طه: المرجع السابق، ص٣١.

[2] Meunier (C.) La loi du 28 November 2000 relative a la criminalite informatique. Rev. dr. pen. Crim. 2002, P. 674.

ج) الأمر بتتبع البيانات والمعلومات: يقصد به ملاحقة ومتابعة تحركاتها، ومن ثم يفترض هذا الأمر تكليف مقدمي الخدمة بمتابعة تحركات البيانات والمعلومات وتتبع مصادرها لأغراض الضبط.

د) الأمر بالتحفظ على البيانات والمعلومات: ترجع أهمية التحفظ على البيانات بالنظر إلى الطابع المتواتر والتدفق المستمر للكم الهائل من المعلومات والبيانات التي يتم تبادلها بين الأفراد من خلال شبكات الاتصالات والمعلومات، ومن ثم يتجه مزودي خدمة الإنترنت إلى تخزين هذه البيانات لفترة زمنية مناسبة لأغراض معالجة هذه البيانات، بالنظر لما يتطلب تخزين هذه البيانات من موارد وأموال طائلة، ونظراً لمتطلبات التحقيق في جرائم تقنية المعلومات والتي تشترط ضرورة الحفاظ على أدلة الجريمة، علاوة على ما قد تشتمله الإجراءات القضائية من طلبات للتعاون القضائي الدولي التي تستغرق فترات زمنية طويلة، فقد انطوت العديد من المواثيق الدولية على أحكام تهدف إلى تأسيس آليات لتحقيق جرائم تقنية المعلومات منوط بها منع حذف البيانات، من خلال تقرير سلطة إعطاء أوامر للأشخاص المتحكمين في البيانات من مقدمي خدمة الإنترنت والاتصالات الإلكترونية وخدمات استضافة المواقع الإلكترونية بالحفاظ وصون سلامة البيانات لفترة زمنية محددة[1].

وقد أجازت المادة السادسة من القانون لجهة التحقيق المختصة أن تأمر بالتحفظ على البيانات والمعلومات أو أنظمة المعلومات، ويعد هذا الإجراء من

[1] ومن أبرز هذه الصكوك الدولية متعددة الأطراف المعنية بمكافحة جرائم تقنية المعلومات الاتفاقية العربية بشأن مكافحة جرائم تقنية المعلومات (م٢٣)، واتفاقية بودابست (الاتفاقية الأوروبية) بشأن الجريمة الإلكترونية (م١٦)، ومشروع اتفاقية الاتحاد الأفريقي (م٣-٥٣)، ومشروع ميثاق الكوميسا (م٣٣-٣٥). انظر: دراسة مكتب الأمم المتحدة المعني بالمخدرات والجريمة بشأن الجريمة السيبرانية، مرجع سابق، ص ص١٨٣، ١٨٤.

الإجراءات التحفظية التي خولها القانون لسلطة التحقيق، خشية ضياعها أو محوها أو إتلافها، وهو من الإجراءات الممهدة لجمع الأدلة، ويتولى القيام بها مقدمو خدمات الانترنت بتكليف من السلطات القضائية المختصة باعتبارها إجراءات لازمة وضرورية لتسهيل مهمة سلطة التحقيق في كشف جرائم تقنية المعلومات والبحث عن أدلتها وضبطها.

فالغرض من ذلك هو تمكين سلطة التحقيق من معرفة مضمون البيانات التي أرسلها المشترك أو استقبلها سواء عن طريق طلبها من مقدمي الخدمة أو خلال القيام بالتفتيش[1]، وعلى ذلك فإن الأمر الذي تصدره السلطة المختصة في الدولة يلتزم بمقتضاه مقدمي الخدمة بالحفاظ على البيانات وحمايتها من الضياع أو التعديل أو المحو وبالحفاظ على سريتها ومنع الغير من الحصول أو الوصول إليها.

التحفظ على البيانات في التشريع المقارن: ومن التشريعات المُقارنة التي أجازت الأمر بالتحفظ على البيانات التشريع البلجيكي الذي أجاز لقاضي التحقيق - خشية من محو أو إتلاف أو نقل أو ضياع الأدلة التي يتم الحصول عليها بطريق التفتيش- سلطة الأمر بالتحفظ عليها، إن وجدت على الأرض البلجيكية، أو أن يطلب من السلطات الأجنبية نسخة من هذه البيانات محل الجريمة، إن وجدت لدى دولة أجنبية. ويتم التحفظ على البيانات محل الجريمة، وكذلك الأدوات التي استخدمت في ارتكابها، أو الآثار المتخلفة عنها وتفيد في كشف الحقيقة (م "٨٨" من قانون تحقيق الجنايات البلجيكي المُضافة بالقانون الصادر في ٢٣ /١١/ ٢٠٠٠).

---

[1] مستشار. د. وليد نبيل طه: المرجع السابق، ص٢٥.

ويتم استخراج نسخة من المعلومات المضبوطة على الوسائط الخاصة بجهة التحقيق، وتبقى تحت تصرفها إلى حين انتهاء المحاكمة، ويرى البعض[١] ضرورة حفظ نسخة أخرى لدى المحضرين بالمحكمة، خشية تلف أو ضياع النسخة الوحيدة المرجوة تحت تصرف جهة التحقيق أو المحكمة.

وتختلف مدة التحفظ على البيانات من تشريع لآخر، ويختص بإصدار أمر التحفظ السلطة التي يحددها التشريع الداخل لكل دولة، وقد نظم المشرع الأمريكي في القانون الخاص بمكافحة جرائم الكمبيوتر والانترنت الصادر تنفيذاً لاتفاقية بودابست إجراءات التحفظ على مضمون البيانات بأن نص عليه في المادة(18 usc 2703)، ونص عليه المشرع الفرنسي في المادة ٥٦ من قانون الإجراءات الجنائية[٢].ومن ضمن التشريعات العربية التي أجازت التحفظ على المعلومات والبيانات المتعلقة بارتكاب الجرائم المعلوماتية القانون الأردني (م١٣/ب).

التحفظ على البيانات في المواثيق الدولية: ومن المواثيق الدولية التي حرصت على تقرير إجراءات التحفظ على البيانات والمعلومات الاتفاقية الأوربية بشأن الجرائم المعلوماتية (بودابست) والاتفاقية العربية لمكافحة جرائم تقنية المعلومات، فقد أجازت المادة (١٦) من اتفاقية بودابست لسلطات التحقيق المختصة أن تصدر أمراً أو طلباً بالتحفظ بصورة عاجلة على بيانات بعينها على حاسب آلي، بما في ذلك خط سير البيانات المُخزنة بواسطة نظام معلوماتي موجود بحوزة شخص أو تحت سيطرته من أجل الحفاظ على سلامة تلك المعلومات لمُدة لا تزيد على تسعين يوماً على الأكثر، فضلاً عن إلزامه بالمُحافظة على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الداخلي للدول الأعضاء.

---

(1) Meunier (C.) : Art. Prec. P. 669- 673.

(٢) مستشار. د. وليد نبيل طه: المرجع السابق، ص٢٦.

ويختلف إجراء التحفظ على البيانات المتعلقة بخط سير البيانات عن التحفظ السريع على مضمون البيانات الذي نصت عليه المادة ١/١٦ من الاتفاقية في أن التحفظ يقتصر على البيانات المتعلقة بالاتصال من حيث مصدرها ووقتها ومرسلها ومستقبلها، ومن ساهم في نقلها، ولا يشمل محتوى البيانات، وما تتضمنه من معلومات، وهذا الإجراء كسابقه يحتاج إلى تقنية عالية تساعد مقدم الخدمة في القيام به في وقت سريع بغية إعطاء السلطة المختصة فرصة اتخاذ الإجراء اللازم لكشف مرتكب الجريمة وضبط أدلتها[١].

كما أجازت المادة (١٧) من الاتفاقية النص على إمكانية الحفظ العاجل لخط سير البيانات المطلوب حفظها، بصرف النظر عن مُشاركة مُقدم خدمة واحد أو أكثر في عملية نقل هذه الاتصالات، فضلاً عن إمكانية الكشف العاجل للسلطات المختصة لدى الدولة الطرف أو شخص تعينه لقدر كافي من خط سير البيانات لتمكين الدولة الطرف من تحديد مزودي الخدمة والمسار الذي تم نقل الاتصال.

بينما أجازت المادة (٢٣) من الاتفاقية العربية للدول الأعضاء النص على إمكانية أن تصدر السلطات المختصة بالتحقيق في الجرائم المعلوماتية أمراً بالتحفظ العاجل لمعلومات تقنية المعلومات الموجودة بحوزة شخص أو تحت سيطرته من أجل الحفاظ على سلامة تلك المعلومات لمُدة أقصاها تسعين يوماً قابلة للتجديد، فضلاً عن إلزامه بالإبقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الداخلي للدول الأعضاء. كما أجازت المادة (٢٤) من الاتفاقية النص على إمكانية الحفظ العاجل لمعلومات تتبع المستخدمين، بغض النظر عن اشتراك واحد أو أكثر من مزودي الخدمة في بث تلك الاتصالات، فضلاً عن إمكانية الكشف العاجل

[١] الموضع السابق.

للسلطات المختصة لدى الدولة الطرف أو شخص تعينه لمقدار كاف عن هذه المعلومات (معلومات تتبع المستخدمين) لتمكين الدولة الطرف من تحديد مزودي الخدمة ومسار بث الاتصالات.

مدى دستورية الأمر بالتحفظ على البيانات: يثور التساؤل حول مدى دستورية الأمر بالتحفظ على البيانات في ضوء ما يشكله هذه الإجراء من مساس بالحق في الحياة الخاصة، حيث سبق وأن قضت المحكمة الأوروبية لحقوق الإنسان في أحد القضايا المنظورة أمامها بأن مجرد تخزين كميات من المعلومات الفردية يعتبر في هذا الصدد أحد أشكال التدخل في الحق في الحياة الخاصة[١]، وقد ذهبت في قضية أخرى إلى القول بأنه:"بالرغم من أن حرية التعبير وسرية المراسلات تعتبر من قبيل الاعتبارات الأولية، كما يجب أن يُمنح مستعملو الاتصالات السلكية واللاسلكية وخدمات الإنترنت ضماناً بأن خصوصيتهم وحرية تعبيرهم محل احترام، بيد أن هذه الضمانة لا يجوز أن تكون مطلقة، ويجب أن تخضع إلى سياق الأولويات المشروعة، مثل منع الفوضى والجريمة... حيث تكمن مهمة المشرع في هذا الصدد بتوفير إطار للتوفيق بين المطالبات المختلفة التي تباري للحماية في هذا السياق، حيث قضت المحكمة بأن عدم حصول سلطات إنفاذ القانون على بيانات المشترك من مقدم خدمة الإنترنت نظراً لحماية السرية من شأنه أن يعيق اتخاذ خطوة فعالة لتحديد الجاني وملاحقته قضائياً"[٢]، وفي قضاء آخر قضت بأنه:" صلاحيات المراقبة السرية للمواطنين، يوازي ما تفعله الدولة البوليسية، تعتبر مقبولة بموجب الاتفاقية الأوروبية لحقوق

---

[١] انظر: قرار المحكمة الأوروبية لحقوق الإنسان في الالتماس رقم ٨١/٩٢٤٨، مشار إليه دراسة مكتب الأمم المتحدة، مرجع سابق، ص١٨٤.

[٢] انظر: قرار المحكمة الأوروبية لحقوق الإنسان في الالتماس رقم ٠٢/٢٨٧٢، مشار إليه دراسة مكتب الأمم المتحدة، مرجع سابق، ص١٩٩.

الإنسان والحريات الأساسية فقط بقدر الضرورة القصوى لحماية المؤسسات الديمقراطية"[١]، ومن ثم اتجه البعض[٢] إلى القول بأن التحفظ على البيانات على الرغم من أهميته في الحفاظ على الأدلة الرقمية في سياق التحقيقات الجنائية عبر الوطنية، إلا أن إصدار أوامر التحفظ تتطلب تقييماً لمدى تناسب هذا الإجراء، لاسيما إذا تطلب الأمر الصادر بالتحفظ لمدة أطول من الفترة الزمنية المتوخاة من قبل التشريعات المعنية بحماية البيانات.

والواقع أن الأمر بالتحفظ على البيانات هو من الإجراءات الضرورية التي تناسب حالة الأدلة الرقمية المتغيرة، ومن ثم كان هذا الإجراء ضرورياً لمباشرة التحقيق في مثل هذه الطائفة من الجرائم، وأن المشرع المصري في تنظيمه لهذه المسألة قد وازن بين حق الأفراد في احترام خصوصيتهم والمصلحة العامة ومقتضيات حسن سير التحقيق في هذه الجرائم ذات الطبيعة الخاصة، من خلال التزام مقدمي الخدمة بعدد من الالتزامات، والتي من أبرزها قصر الالتزام بحفظ وتخزين سجل النظام المعلوماتي أو أي وسيلة لتقنية المعلومات لمدة زمنية محددة هي ١٨٠ يوماً متصلة، كما أوجب عليه المحافظة على سرية البيانات التي تم حفظها وتخزينها وعدم إفشائها بغير إذن مسبب من إحدى الجهات القضائية، وهذا الالتزام عاقب المشرع مقدم الخدمة على مخالفته بموجب المادة (٣١) من القانون، علاوة على التزامه بتأمين البيانات، بما يحافظ على سريتها، وعدم اعتراضها أو اختراقها أو تلفها.

---

(١) انظر: قرار المحكمة الأوروبية لحقوق الإنسان في الالتماس رقم ٩٥/٢٨٣٤١، مشار إليه دراسة مكتب الأمم المتحدة، مرجع سابق، ص٢٠١.

(2) Brown, I., 2010. Communications Data Retention in an Evolving Internet. International Journal of Law and Information Technology, 19(2):107.

الأمر بضبط البيانات: وهو إجراء الهدف منه ضبط الأدلة الرقمية بهدف الاستفادة منها في كشف الحقيقة في جرائم تقنية المعلومات، وهو إجراء مشابه لإجراء ضبط الأشياء المعروف في قانون الإجراءات الجنائية، وتثير مسألة ضبط البيانات والمعلومات بعض المسائل القانونية، نتناولها على النحو التالي:-

مدى صلاحية البيانات والمعلومات لأن تكون محلاً للضبط: يكون الأصل في الأشياء التي تكون محلاً للضبط أن تكون أشياء مادية يحوزها المُتهم، وهو ما يشير الفقه الجنائي إلى صعوبة عملية في مجال جرائم تقنية المعلومات نظراً لطبيعتها الخاصة، بل وأن محلها أي البيانات والبرامج تتسم بصورة معنوية غير محسوسة تصعب لأن تكون محلاً للضبط، وقد انقسم الفقه في هذا الأمر بين رأيين، وذلك على النحو التالي:-

(الأول) عدم صلاحية البيانات والمعلومات لأن تكون محلاً للضبط: ذهب البعض إلى عدم صلاحية بيانات الحاسب لأن تكون محلاً للضبط، ويستند في ذلك إلى الطبيعة المعنوية للبيانات التي لا تتماشى مع النصوص الإجرائية التي تشترط فيها أن تكون أشياء مادية؛ إذ ينتفي في هذه البيانات الطابع المادي المحسوس، ولا يكون هناك سبيلاً لضبطها إلا عن طريق نقلها على كيان مادي ملموس، سواء أكان ذلك عن طريق التصوير الفوتوغرافي، أو بنقلها على دعامة أو غيرها من الوسائل المادية[1].

(1) Kaspersen (H.W.K) : Computer crimes and others crimes aganiste information technology in the Netherlands. Rev. int. dr. pen. 1993. p. 474-502.

(الثاني) صلاحية البيانات والمعلومات لأن تكون محلاً للضبط: ذهب جانب ثان[1] من الفقه المُقارن إلى صلاحية البيانات والمعلومات الموجودة بالحاسب لأن تكون محلاً للضبط، مستنداً في ذلك إلى إمكانية تسجيلها وتخزينها على وسائط مادية؛ فهذه البيانات المُعالجة إلكترونيا عبارة عن ذبذبات إلكترونية، أو موجات كهرومغناطيسية، تقبل التسجيل والحفظ والتخزين على وسائط مادية، أضف إلى ذلك إمكانية نقلها وبثها واستقبالها وإعادة إنتاجها، ومن ثم فإن وجودها المادي لا يمكن إنكاره. ويستند هذا الاتجاه إلى بعض النصوص التشريعية في القوانين المُقارنة كالقانون البلجيكي والكندي؛ ففي بلجيكا نصت المادة (٣٩) من قانون تحقيق الجنايات البلجيكي، المُضافة بالقانون الصادر في ٢٣ نوفمبر سنة ٢٠٠٠، على الحجز يتضمن الأشياء المادية والبيانات المعالجة إلكترونيا، أما في كندا فقد نصت المادة (٧/٢٩) من قانون الإثبات الكندي على أن تفتيش وضبط الدفاتر والسجلات الخاصة بمؤسسة مالية، يقتصر على تفتيش المكان بغرض تفقده و أخذ نسخة من المواد المكتوبة، يستوي في ذلك أن تكون السجلات مكتوبة أم في شكل إلكتروني[2]، ومن التشريعات العربية التي أجازت ضبط الأشياء المتعلقة بالجرائم المعلوماتية القانون الأردني، الذي نصت فيه المادة (١٣/ب) على أنه:"مع مراعاة حقوق الآخرين ذوي النية الحسنة وباستثناء المرخص لهم وفق أحكام قانون الاتصالات ممن لم يشتركوا بأي جريمة منصوص عليها في هذا القانون، يجوز لموظفي الضابطة العدلية ضبط الأجهزة والأدوات

---

(1) Spreutels (J.P.) : Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en belgique: rapp. Rev. Int. dr. pen. 1993. p. 161-170.

(2) Piragaff (D.K) : Computer crimes and others crimes aganiste information technology in the Canada., report, Rev. int. dr. pen. 1993, p.201-340; Meunier (C.): Art. Prec. P. 670.

والبرامج والأنظمة والوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون والأموال المتحصلة منها والتحفظ على المعلومات والبيانات المتعلقة بارتكاب أي منها".

المُشكلات العملية الخاصة بضبط البيانات والمعلومات: يثير إجراء ضبط البيانات المُعالجة إلكترونياً بعض الصعوبات العملية، المُتمثلة في كبر حجم الشبكات التي تحتوي على المعلومات المطلوب ضبطها، مثال البحث في نظام إلكتروني لشركة متعددة الجنسيات، وكذا مشكلة وجود هذه البيانات في شبكات أو أجهزة تابعة لدولة أجنبية، وهو ما يستدعي ضرورة تعاونها مع أجهزة العدالة في هذه الدول.

تساؤل: هل ضبط جهاز الحاسب الآلي يتطلب قرار من القاضي الجزئي كما هو الوضع في ضبط الخطابات أو الرسائل أو المطبوعات لدى مكاتب البريد: أجابت محكمة جنح مستأنف القاهرة الاقتصادية على هذا التساؤل، حينما قضت في أحد أحكامها أن ضبط جهاز الحاسب الآلي المستخدم في ارتكاب الجريمة لا يستلزم إذناً من القاضي الجزئي لكون محل الجريمة هو جهاز الحاسب الآلي وليس ضبط خطابات أو رسائل أو مطبوعات لدى مكتب البريد[١]، وهو ما أيده جانب من الفقه الجنائي[٢] مستنداً في ذلك إلى حكم المادة ٢٠٦ من قانون الإجراءات الجنائية التي لم تتطلب إذن القاضي الجزئي إلا في حالة ضبط الطرود والرسائل والمطبوعات لدي مكاتب البريد أو البرق،دون غيرها، وأن حالة الضبط من خلال الحاسب الآلي تختلف عن ضبط الرسائل والطرود بمكاتب البريد، فالأخيرة تفترض أن الخطابات المرسلة لم تصل للمرسل إليه، بخلاف

---

[١] انظر: حكم محكمة جنح مستأنف القاهرة الاقتصادية، جلسة ٢٠١٠/١١/٣، الدعوى رقم ٧٨٩ لسنة ٢٠١٠ جنح مستأنف والمقيدة برقم ١٥١٧ جنح القاهرة الاقتصادية، مشار إليها المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٢٢٤.

[٢] المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص ص٢٢٤، ٢٢٥.

حالة الضبط من خلال جهاز الحاسب الآلي، يكون الخطاب في حوزة المرسل للخطاب أو المرسل إليه حسب الأحوال، فضلاً عن عدم وجود نص تشريعي ينظم هذه المسألة، ومن ثم فإن ضبط الرسائل الإلكترونية المرسلة أو المستلمة من بريد إلكتروني إلي آخر لا يستلزم إذناً من القاضي الجزئي، باعتبار أنها تعد من قبيل الرسائل، وطالما أنها لم تكن موجودة لدي مكاتب البريد أو البرق، فإنه يكفي للاطلاع عليها أو ضبطها صدور إذن من النيابة العامة.

ويضيف الرأي السابق إلى أن بعض الرسائل الإلكترونية قد تكون في حوزة المتهم كما لو كان حائزاً لهاتفه الذكي الذي يحوي على الرسائل المذكورة، أو قد يكون في مسكنه، ومن ثم فإنه يتعين صدور الإذن الملائم الذي بموجبه يكون التفتيش صحيحاً، وهو ما ينطبق كذلك على حالات ذاكرات الهواتف النقالة والكاميرات ووسائط التخزين والأقراص المدمجة. ويتفق الرأي السابق مع قضاء محكمة النقض والتي ترى أن تفتيش جهاز الحاسب الآلي يدخل في اختصاص النيابة العامة التي تختص بإصدار الإذن بتفتيش الأشخاص والمنازل، دونما الاختصاص بتفتيش غير مسكن المتهم أو التنصت على المكالمات الإلكترونية أو مراقبة المحادثات السلكية واللاسلكية أو تسجيل محادثات تجري في مكان خاص والتي تتطلب صدور إذن من القاضي الجزئي[1].

الأمر بغلق البيانات: يمثل التفتيش والضبط أحياناً اعتداء على حقوق الغير، أو على حرمة حياته الخاصة، وهو ما يتطلب ضرورة اتخاذ الضمانات اللازمة لحماية هذه الحقوق والحريات، ومن التشريعات المُقارنة التي حرصت على تحقيق مثل هذه الضمانات للمُتهم في الإجراءات الجنائية، القانون البلجيكي؛ إذ أجاز للنيابة العامة

[1] انظر: الطعن الجنائي رقم ١٥٤٢ لسنة ٨٢ قضائية، جلسة ٢٠١٣/٧/٣، مشار إليه المستشار د.محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٢٢٥.

سلطة الأمر بغلق البيانات لمنع الوصول إليها، أو إلى النسخة المُستخرجة منها الموجودة لدى من يستعملون النظام، وذلك لضمان الحفاظ على البيانات محل البحث وضمان إمكانية مُقارنتها بالنسخة المُخرجة من الجهاز في حالة جحدها من المتهم (م ٢٩ مكررا /٣)، إلا أن المشرع المصري لم يشر لمثل هذا النوع من الأوامر في جرائم تقنية المعلومات.

المطلب الثالث

الإذن بالتفتيش في جرائم تقنية المعلومات

أجاز القانون إجراء التفتيش لغاية ضبط كل ما له علاقة بالجريمة، ويؤدي إلى ظهور الحقيقة سواء أكان هذا الشيء أدوات استعملت في ارتكاب الجريمة أو شيئاً نتج عنها أو غير ذلك[١]، ومن ثم يجوز أن يكون محلاً للضبط من قبل المُحقق الجنائي جميع الأشياء التي تفيد في كشف الحقيقة أو المُتعلقة بالجريمة[٢]، ويعُد التفتيش من إجراءات التحقيق التي يختص بها أصلاً سلطة التحقيق واستثناء مأموري الضبط القضائي، ولم يضع المشرع الجنائي تعريفاً مُحدداً للتفتيش كأحد الإجراءات الجنائية، إلا أن محكمة النقض المصرية قد عرفته بأنه:" البحث عن عناصر الحقيقة في مستودع السر"[٣]، بينما عرفه جانب من الفقه الجنائي[٤] بأنه:" إجراء من إجراءات التحقيق بمُقتضاه يقوم المُحقق أو من يأذن له من رجال الضبطية القضائية بالبحث في منزل شخص معين على أشياء مُتعلقة بجناية أو جنحة قامت قرائن قوية على حيازته لها".

---

[١] د. مأمون محمد سلامة، الإجراءات الجنائية، مرجع سابق، ص٦٨٩.

[٢] د. محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في الجرائم، مرجع سابق، ص١١.

[٣] مجموعة أحكام محكمة النقض: ١٢/١٧/ ١٩٦٢، س١٣، رقم ٢٠٥، ص٨٥٣.

[٤] د. مأمون محمد سلامة، الإجراءات الجنائية، مرجع سابق، ص٦٧٧.

فالتفتيش إجراء يهدف إلى البحث عن أشياء تتعلق بالجريمة، وكل ما يفيد بصفة عامة في كشف الحقيقة، سواء تعلق بالأشخاص أو الأماكن[١]،والتفتيش إجراءً ليس غاية في حد ذاته وإنما هو وسيلة لغاية، تتمثل فيما يمكن الوصول من خلاله إلى أدلة مادية تسهم في بيان وظهور الحقيقة، هذا وقد أشار قانون الإجراءات الجنائية المصري إلى إجراء تفتيش المنازل في نص المادة (٩١) إجراءات جنائية.

وقد عرف المجلس الأوروبي إجراء التفتيش في جرائم تقنية المعلومات بأنه:" الإجراء الذي يسمح بجمع الأدلة المُخزنة أو المُسجلة بشكل إلكتروني"[٢]، فهو الإجراء الذي يسمح باستخدام الوسائل الإلكترونية للبحث في أي مكان عن البيانات والأدلة المطلوبة[٣]، بينما يعرف البعض[٤] التفتيش الإلكتروني بأنه:" الاطلاع على المعلومات الإلكترونية بهدف ضبط أدلة الجريمة، وذلك إذا كانت هذه المعلومات محاطة بسياج من الحماية"، ومن ثم يخضع للضمانات التي يوجبها القانون.

التفتيش الإلكتروني في التشريع المصري: وقد أشارت المادة السادسة من القانون إلى اختصاص جهة التحقيق بأن تأمر بالبحث والتفتيش، والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقاً لغرض الضبط، ومن ثم فقد أناط القانون بسلطة التحقيق سواء أكانت النيابة العامة أو قاضي

---

[١] د. محمد أبو العلا عقيدة، شرح قانون الإجراءات الجنائية، ج١، ط١، ٢٠٠١، دار النهضة العربية،ص٤٣١ وما بعدها.

[2] Conseil de L'eurpe: Problemes de procedure penale lies a la technologie de l' information. Recommendation n. R (95) 13 et expose des motifs. Ed. Conseil de l'europe, 1996. p.28.

[3] Meunier (c): art. Prec. P. 663.

[٤] المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٢١٢.

التحقيق بإصدار الإذن بالتفتيش، ويشترط أن تكون سلطة التحقيق وفقاً لقواعد الاختصاص بإصدار الإذن، حيث نصت المادة المذكورة على أنه:"*الجهة التحقيق المختصة، بحسب الأحوال، أن تصدر أمراً مسبباً لمأموري الضبط القضائي المختصين، لمدة لا تزيد على ثلاثين يوماً قابلة للتجديد لمرة واحدة، متى كان لذلك فائدة في ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون، بواحد أو أكثر مما يأتي:-١ -... ٢ - البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقاً لغرض الضبط*" [١].

وقد انتقد جانب من الفقه الجنائي[٢] صياغة المادة السادسة من القانون، والتي أناطت بجهة التحقيق –دون غيرها- إصدار الإذن بتفتيش برامج الحاسب الآلي وقواعد البيانات وغيرها من النظم المعلوماتية تحقيقاً لغرض الضبط، بالنظر إلى أن هذا النص لم يراع مكان وجود الحاسب الآلي الذي قد يكون في مسكن للمتهم أو لغيره، حيث كان يتعين صدور الإذن في الحالة الأخيرة من القاضي الجزئي،ولو كانت النيابة العامة هي التي تباشر التحقيق، تطبيقاً للقواعد العامة المقررة في الإجراءات الجنائية.

---

[١] تتضمن معظم الصكوك الدولية متعددة الأطراف تحديداً للصلاحيات الخاصة بتفتيش النظم المعلوماتية أو وسائط تخزين البيانات، أو الوصول إليها بشكل مماثل، كما توفر تمهيداً لنطاق البحث لنظام حاسوبي آخر داخل إقليم الدولة في حالة إذا ثبت أن المعلومات المعنية غير موجودة في النظام الأصلي أو في الوسائط التي تم تفتيشها، ومن هذه الصكوك الاتفاقية العربية بشأن مكافحة جرائم تقنية المعلومات (م٢٦و٢٧)، واتفاقية بودابست (الاتفاقية الأوروبية) بشأن الجريمة الإلكترونية (م١٩)، ومشروع اتفاقية الاتحاد الأفريقي (م٣-٥٠ و٣-٥١)، ومشروع ميثاق الكوميسا (م٣٣ و٣٧). انظر: دراسة مكتب الأمم المتحدة المعني بالمخدرات والجريمة بشأن الجريمة السيبرانية، مرجع سابق، ص ص١٨١، ١٨٢.

[٢] المرجع السابق، ص٢٢٨.

ويضيف الرأي السابق انتقاداً آخر بشأن قصر الأحكام الخاصة بالتفتيش الإلكتروني على الجرائم الواردة في قانون مكافحة جرائم تقنية المعلومات فحسب دون غيرها من جرائم تقنية المعلومات الأخرى المعاقب عليها في قوانين أخرى كقانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣ وقانون تنظيم التوقيع الإلكتروني وهيئة صناعة تكنولوجيا المعلومات رقم ١٥ لسنة ٢٠٠٤ وغيرها من القوانين، وهو حكم غير مبرر بالنظر إلى أن وجوب توحيد المعاملة الإجرائية بين كافة جرائم تقنية المعلومات من خلال وضع قواعد عامة في الضبط والتفتيش فيما يتعلق بالأدلة الإلكترونية أو الرقمية، وبصرف النظر عن محل النص على القاعدة القانونية[١].

وتجدر الإشارة إلى اختلاف موقف التشريعات المقارنة بشأن تخويل سلطة الإذن بالتفتيش لسلطة التحقيق أم قضاء الموضوع؛ فإذ تتجه غالبية التشريعات المقارنة - ومنها التشريع المصري- إلى تخويل هذه السلطة لسلطة التحقيق، نجد أن جانب آخر من التشريعات كالتشريع الألماني يمنح هذه السلطة لقضاء الموضوع؛ إذ لا يجيز قانون الإجراءات الجنائية الألماني للنيابة العامة أن تأذن بتفتيش أجهزة الحاسب الآلي والأجهزة الإلكترونية والإطلاع على محتواها أو كشف المراسلات إلا بموجب أمر يصدر من قاضي وفقاً للضوابط والشروط المنصوص عليها في المواد ٩٨ و١٦٢ من قانون الإجراءات الجنائية الألماني[٢].

---

[١] الموضع السابق.

[٢] د. أشرف توفيق شمس الدين: مخاطر العملات الافتراضية في نظر السياسة الجنائية، مرجع سابق، ص٦٨٤.

شروط صحة إجراء التفتيش[1]: يشترط القانون لصدور إجراء التفتيش صحيحاً ضرورة توافر بعض الشروط الموضوعية وأخرى شكلية، وذلك على النحو التالي:-

أ) الشروط الموضوعية: تتمثل الشروط الموضوعية في أربعة شروط، يتمثل الشرط الأول فيها بسبب التفتيش، والثاني موضوعه، والثالث المكان الذي ينصب عليه التفتيش والرابع الغرض منه، وهي:-

١- أن يكون التفتيش مُتعلقاً بجريمة هي جناية أو جنحة قد وقعت فعلاً.

٢- أن يكون هناك اتهاماً موجهاً للشخص المُراد تفتيشه أو تفتيش مسكنه أو وجدت قرائن على حيازته لأشياء مُتعلقة بالجريمة.

٣- أن يكون التفتيش قد أنصب على مكان مُحدد أو قابل للتحديد على الأقل.

٤- أن يكون التفتيش بقصد ضبط أشياء مُتعلقة بالجريمة أو تفيد في كشف الحقيقة.

ب) الشروط الشكلية: تتمثل الشروط الشكلية في أمرين: (الأول) يتعلق بتسبيبه، والثاني يتعلق بتنفيذه، وهي:-

١- أن يكون الإذن بالتفتيش مُسبباً.

٢- أن يكون التفتيش بحضور المتهم أو من ينيبه عنه إن أمكن ذلك.

٣- تحرير محضر بإجراء التفتيش.

---

[1] د. محمد أبو العلا عقيدة: شرح قانون الإجراءات الجنائية، مرجع سابق، ص٤٣١ وما بعدها؛ د. محمد عبد اللطيف فرج: شرح قانون الإجراءات الجنائية، مرجع سابق، ص٢٨٦ وما بعدها.

جواز تفتيش الحاسب الآلي وملحقاته الكائنة في الأماكن الجائز تفتيشها قانوناً:يضيف الفقه الجنائي[١] إلى شروط صحة التفتيش في جرائم تقنية المعلومات أن يكون الدخول لمكان وجود الحاسب الآلي وملحقاته قد تم على نحوٍ صحيح، فإذا كان جهاز الحاسب الآلي وملحقاته في مسكن، فلا بد من الحصول على إذن من النيابة العامة للدخول إلى هذا المسكن، إما إذا كان التفتيش بناءً على توافر حالة التلبس، وكان الجهاز في مكان عام، كما لو كان في أحد المحال العامة، فمن حق مأمور الضبط القضائي إجراء التفتيش.

مدى صلاحية محل جرائم تقنية المعلومات للتفتيش: يشير الفقه الجنائي[٢] إلى أن طبيعة جرائم تقنية المعلومات، بل أن محلها (البيانات والبرامج) بصفة خاصة يصعب إجراء التفتيش عليها، فطبيعة التفتيش تقتضي التحفظ على أشياء مادية تتعلق بالجريمة، أو تفيد في كشف الحقيقة، وللوقوف على مدى صلاحية جرائم تقنية المعلومات للتفتيش عن أدلتها، يجب التمييز في هذا الصدد بين أمرين:-

أ) ارتكاب الجريمة على مكونات الحاسب: كمعدات الحاسب وكابلاته وشاشة العرض الخاصة ومفاتيح التشغيل، وذلك في حال سرقتها أو إتلافها أو اختلالها، ففي هذه الحالة لا نكون هناك مشكلة إجرائية في تنفيذ التفتيش؛ إذ تنطبق بصددها ذات القواعد التقليدية للتفتيش دون أدنى صعوبة أو عائق يحول دون ذلك.

---

[١] المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص ص٢٢٣، ٢٢٤.

[٢] ومن الفقه المصري، انظر: المستشار د. محمد سمير: المرجع السابق، ص٢٢٢؛ د. محمد الألفي: الجرائم المضرة بأمن الدولة عبر الإنترنت، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ٢٠١١، ص٣٦٦. ومن الفقه المقارن، انظر:

Brenner, S. W., Frederiksen, B.A., Computer Searches and Seizures: Some Unresolved Issues. Mich. Telecomm. Tech. L. Rev. 39(8), 2002; Kerr, O.S., Search Warrants in an Era of Digital Evidence. Mississippi Law Journal, 2005, pp. 75-85.

ب) ارتكاب الجريمة على برامج الحاسب وبياناته وشبكة الإنترنت: ففي هذه الحالة يتفق الفقه الجنائي إلى جواز أن يرد التفتيش على هذه البيانات غير المحسوسة عن طريق وسائط الحفظ أو التخزين الإلكترونية كالأسطوانات والأقراص المُمغنطة، ومخرجات الحاسب[١]، وهو ما أشارت إليه التشريعات الإجرائية المُقارنة التي أجازت إجراء التفتيش والضبط و التحفظ على البيانات المُعالجة إلكترونياً والمُخزنة بالحاسب الآلي أو الوسائط الإلكترونية التي سُجلت عليها هذه البيانات[٢].

محل التفتيش في جرائم تقنية المعلومات: يقتضى التفتيش عن البيانات المخزنة آلياً القيام بعملية ولوج للأنظمة المعلوماتية التي تحديدها لضبط ما يعد صالحاً كدليل أو قرينة لارتكاب جريمة ما، وهذا يقتضى من الشخص القائم بالتفتيش معرفة كيفية التعامل مع برامج وملفات البيانات المخزنة بالحاسب وكذا كلمة السر والمرور اللازمين للدخول للنظام[٣]، وتثير مسألة محل التفتيش مُشكلة خاصة بكيفية تنفيذ إذن التفتيش، والذي يشترط فيه أن يكون مُحدداً فيه نطاق وحدود تنفيذ الإذن بالتفتيش.

ويشير الفقه الجنائي[٤] إلى أن محل التفتيش في الجرائم المعلوماتية ينبغي أن يشمل البرامج أو الكيانات المنطقية، البيانات المُسجلة في ذاكرة الحاسب أو في مُخرجاته، السجلات المُثبتة لاستخدام نظام المُعالجة الآلية للبيانات، السجلات الخاصة

---

(1) Moherenschlager (M) :Computer crimes and others crimes aganiste information technology in the Germany. Rev. int. dr. pen. 1993, p.319. spec. 349.

(٢) د. محمد أبو العلا عقيدة: التحقيق وجمع الأدلة في الجرائم، مرجع سابق، ص٩.

(٣) د. عفيفى كامل عفيفى: جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، مكتبة الأهرام، القاهرة، ٢٠٠٠، ص٣٣٨.

(٤) د.أبو العلا عقيدة: التحقيق وجمع الأدلة في الجرائم الإلكترونية، الموضع السابق؛ د.هشام رستم، الجوانب الإجرائية للجرائم المعلوماتية، مرجع سابق، ص ص٧٧، ٧٨.

بعمليات الدخول إلى نظام المُعالجة الآلية للبيانات، وما يتعلق بها من سجلات كلمات السر ومفاتيح الدخول، ومفاتيح فك الشفرة.وقد أخذت الشرطة الكندية بذات الرأي السابق؛ إذ اعتمدت الشرطة التابعة لمركز المعلوماتية الكندي نموذجاً للإذن بالتفتيش، يتضمن التصريح بالبحث عن ضبط البرنامج أو كيان الحاسب المنطقي، والتي يدخل فيها برنامج التطبيق، ونظم التشغيل وما يتفرغ عنها من نظم، والبيانات المستخدمة بواسطة برنامج الحاسب، وأيضاً السجلات التي تثبت استخدام الأنظمة الآلية المعالجة للبيانات، والسجلات المستخدمة في عملية الولوج في النظام الآلي لمعالجة البيانات.

الضمانات القانونية للتفتيش في جرائم تقنية المعلومات: يشير الفقه الجنائي[١] إلى أن إجراء التفتيش بالنظر إلى كونه يتمثل في البحث في مستودع السر، يمثل مساساً بحرمة الحياة الخاصة، وتقييداً للحرية الفردية، وهو ما يتطلب ضرورة توافر الضمانات القانونية اللازمة لصحته، وهي ضمانات الكتابة، والتسبيب والاختصاص؛ أي أن يكون صدور الإذن بالتفتيش كتابة، وأن يكون بناءً على أمر قضائي مُسبب بشأنه، وأن يباشره الشخص أو الجهة المختصة قانوناً بذلك سواء أكانت النيابة العامة أو مأمور الضبط القضائي في حالة ندبه في غير حالات التلبس بالجريمة.

المشكلات الإجرائية الخاصة بالتفتيش في جرائم تقنية المعلومات: والتفتيش في الحاسب الآلي يعد عملية معقدة في الكثير من الأحيان، فالملفات المخزنة به تحتوي على عمليات إلكترونية معقدة، ويمكن تشفير الملفات، أو وضع بيانات مضللة عليها، ولذلك فإن القائم بالتفتيش يجب أن يكون لدية الخبرة الكافية بعلم الحاسب الآلي[٢]، وتكمن المُشكلات الإجرائية الخاصة بالتفتيش في الجرائم المعلوماتية - بصفة أساسية- في اختلاف الفقه الجنائي في عدة إشكاليات إجرائية، نذكر منها الحالات الخاصة بكيفية

---

[١] د. محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في الجرائم، الموضع السابق.

[٢] المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٢٢٧.

تنفيذ الإذن بالتفتيش في الشبكات المعلوماتية، وما يثيره من مُشكلة امتداد الإذن بالتفتيش، التفتيش العابر للحدود، وهو ما سوف نتناوله على النحو التالي:-

مشكلة امتداد الإذن بالتفتيش في الشبكات المعلوماتية: يشير الفقه الجنائي إلى مشكلة مُتعلقة بتنفيذ إذن التفتيش؛ فالأصل فيه أن يكون مُحدداً بنطاق مكاني مُعين؛ أي يشمل أماكن مُحددة، وهو ما يثير مشكلة مدى إمكانية البحث والتفتيش عن الأدلة في مكان آخر في نظام معلوماتي آخر غير الذي صدر بشأنه الإذن بالتفتيش، وخاصة أن طبيعة الجرائم المعلوماتية تُمكن الجناة من سهولة إخفاء بل وتدمير ومحو أدلة الجريمة خلال الفترة الزمنية التي تحتاجها سلطات التحري والاستدلال في الحصول على إذنٍ ثانٍ لتفتيش المكان الآخر، وما هو الإجراء الذي يمكن اتخاذه حال رفض صاحب المكان أو النظام الآخر السماح بمُباشرة التفتيش لديه؟وقد ذهب جانب من الفقه المُقارن[1] إلى سلطات التحقيق يمكنها أن تتغلب على هذه المشكلة عن طريق أن يتضمن الإذن بالتفتيش على الإذن بتفتيش أي نظام معلوماتي آخر يوجد في أي مكان غير مكان البحث، وهو ذات النهج الذي أخذت به بعض التشريعات المُقارنة، ونذكر منها القانون الهولندي الذي أجاز فيه مشروع قانون جريمة الحاسب الهولندي في المادة ٢٥ منه إمكانية امتداد تفتيش المسكن إلى تفتيش نظام آلى موجود في مكان آخر بغية التوصل إلى بيانات يمكن أن تفيد بشكل معقول في كشف الحقيقة وإذا ما وجدت هذه البيانات يجب تسليمها، هذا بالنسبة للتساؤل الأول.

أما بالنسبة للتساؤل الثاني، والخاص برفض الشخص صاحب الموقع أو النظام الإلكتروني الآخر الخضوع لإجراء التفتيش، فإن جانب من الفقه المُقارن[2] يرى في هذه الحالة عدم جواز التفتيش إلا برضاء الشخص بالتفتيش أو توافر حالة من

---

(1) Meunier (c): art. Prec. P. 664.

(2) Meunier (c): art. Prec. P. 665-668.

حالات التلبس بالجريمة التي تُجيز لسلطات الاستدلال والتحقيق التفتيش في النظام الإلكتروني دون تطلب صدور إذن بالتفتيش.

وأنه في هذه الحالة يجوز استصدار الأمر بامتداد التفتيش شفوياً من قاضي التحقيق لحين إصدار الإذن الكتابي، وفي جميع الأحوال ينبغي أن يكون الإذن مُسبباً، لتتمكن الجهة القضائية من مُراقبة مدى مشروعيته.

تساؤل بشأن حالة صدور إذن من النيابة العامة بتفتيش محل ليس به أجهزة حاسب آلي، وتبين بالانتقال والمعاينة قيام المتهم بأخذ وصلة إنترنت من هذا المحل إلى مسكنه: فهل يكون من حق مأمور الضبط القضائي الدلوف إلي المسكن المذكور؟ ويجيب جانب من الفقه الجنائي على هذا التساؤل بأن أحكام القضاء المصري استقرت على أنه لا يجوز لمأمور الضبط القضائي الدخول إلى المسكن الخاص إلا بعد الحصول على إذن من النيابة العامة بتفتيش المسكن أو برضاء من صاحبه، فإذا سمح لمأمور الضبط القضائي بالتفتيش، فإن هذا الرضاء يضفي على التفتيش أو الدخول إلى المسكن المشروعية، وهو ما يتفق مع أحكام القضاء المصري في هذا الشأن، فقد اعتبرت محكمة النقض دلوف مأموري الضبط القضائي إلي المسكن قد تم بعد سماح المتهم له بالدخول وهو ما يشكل معه الرضاء بدخول المسكن، ومؤدي ذلك أن الإذن الصادر بتفتيش وصلات الإنترنت خارج المسكن أو في إحدى المحلات لا يسوغ بذاته الدلوف إلي المسكن فإذا كان الإذن يشمل كافة الوصلات بيد أنه لا يبرر الدخول إلي المساكن إلا إذا نص على ذلك صراحة وعلى وجه محدد[1].

---

[1] انظر: حكم محكمة جنايات الإسكندرية، جلسة ٢٠١٥/٦/٥، الدعوى رقم ١٨٩٣٥ لسنة ٢٠١٥ جنايات قسم المنتزة ثان، المقيدة برقم ٢١٦٧ لسنة ٢٠١٥ كلي شرق الإسكندرية، والطعن الجنائي رقم ٢٩٩٥٣ لسنة ٨٦ق، جلسة ٢٠١٧/٤/٢٧، مشار إليهما المستشار د.محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص ص٢٢٥-٢٢٧.

موقف التشريعات المقارنة من تنظيم إجراء التفتيش في جرائم تقنية المعلومات:ومن التشريعات المُقارنة التي نظمت إجراءات التفتيش في مجال الجرائم المعلوماتية القانون البلجيكي؛ إذ نصت المادة (٨٨) من قانون تحقيق الجنايات البلجيكي المُضافة بالقانون الصادر في ٢٠٠٠/١١/٢٣ على أنه: " إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي، أو في جزء منه، فإن هذا البحث يمكن أن يمتد إلى نظام معلوماتي آخر يوجد في مكان آخر غير مكان البحث الأصلي، ويتم هذا الامتداد وفقا لضابطين: (أ) إذا كان ضرورياً لكشف الحقيقة بشأن الجريمة محل البحث. (ب) إذا وجدت مخاطر تتعلق بضياع بعض الأدلة، نظرا لسهولة عملية محو أو إتلاف، أو نقل البيانات محل البحث"، وهو ما يجيز لسلطات التحقيق الحصول على نسخة من البيانات التي يحتاجها، دون إذن الدولة التي توجد في نطاق إقليمها البيانات المطلوبة.

ويبرر الفقه البلجيكي[1] هذا النص بالقول بأن سلطة التحقيق يمكنها الدخول إلى النظام والإطلاع على البيانات المطلوبة دون أن تدرك أن هذه البيانات توجد من الناحية المادية خارج إقليم بلجيكا. والبديل لهذا النص، هو إرسال لجنة قضائية إلى الدولة المعنية وتطلب من السلطة المختصة بها أن تتحفظ على البيانات المكونة لمحل الجريمة، وتعطيها نسخة منها، وهذا يستغرق وقتا قد يدمر خلاله المتهم هذه البيانات. ومع ذلك يعترف الفقه بأن هذا النص يمثل اعتداء على سيادة الدولة.

ومن التشريعات العربية التي أجازت إجراء التفتيش في الجرائم المعلوماتية القانون الأردني الذي نصت فيه المادة (١٣/أ) على أنه:" مع مراعاة الشروط والأحكام المقررة في التشريعات ذات العلاقة، يجوز لموظفي الضابطة العدلية الدخول إلى أي مكان يشتبه باستخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج والأنظمة والوسائل المشتبه في

---

(1) IBIDEM.

استخدامها لارتكاب أي من تلك الجرائم، باستثناء بيوت السكن إلا بإذن من المدعي العام المختص قبل الدخول إليها، وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضرا بذلك ويقدمه إلى المدعي العام المختص".

ب) مُشكلة التفتيش في جرائم تقنية المعلومات العابرة للحدود: من المُشكلات الإجرائية التي تعيق أجهزة العدالة حالة إجراء التفتيش في الجرائم المعلوماتية العابرة للحدود، فالأصل أن الجرائم المعلوماتية قد تتم عبر الشبكات المعلوماتية، والتي تربط العديد من أجهزة الحاسب الآلي في العديد من الدول المختلفة، وعليه تثير إجراء التفتيش مشكلة إجرائه على جهاز حاسب آلي خارج النطاق الجغرافي للدولة التي أصدرت الإذن بالتفتيش، ومن ثم تثور مُشكلة شرعية هذا الإجراء ومساسه بسيادة الدولة الأخرى، ويرى الفقه الجنائي المُقارن[١] أن هذه المُشكلة الإجرائية يمكن تجاوزها من خلال تعزيز التعاون الدولي في مكافحة الجرائم المعلوماتية من خلال إبرام اتفاقيات ثنائية وجماعية تنظم مُباشرة هذا الإجراء، بينما ذهب جانب ثان[٢] إلى عدم إمكان إجراء التفتيش العابر للحدود بدون الحصول على إذن الدولة الأخرى أو وجود اتفاقية دولية تجيز إجراء ذلك، وقد أجازت المادة (٣٢) من اتفاقية بودابست إمكانية الدخول في أجهزة أو شبكات تابعة لدولة أخرى بغرض التفتيش والضبط دون إذنها في حالتين: (أ) إذا تعلق التفتيش بمعلومات أو بيانات مُباحة للجمهور (ب) إذا رضى صاحب أو حائز هذه البيانات بهذا التفتيش."، ومع ذلك فإن تطبيق هذا النص يمكن أن يثير مشكلات في التطبيق[٣].

---

(1) Podovo(Y.) : un apercu de la lutte contre la cybercriminalite en France. R.S.C. 2002, p. 765-778.

(2) Meunier (c): art. Prec. P. 676-677.

(٣) د. حسن صادق المرصفاوي: المرصفاوي في أصول الإجراءات الجنائية، منشأة دار المعارف، الإسكندرية، ٢٠٠٠، ص٤٦٠؛ د. محمد عبد اللطيف فرج: شرح قانون الإجراءات الجنائية، مرجع سابق، ص٣٠١.

المطلب الرابع

الأمر بتسليم المعلومات

أجاز القانون لسلطة التحقيق أن تأمر مقدم الخدمة بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتي أو جهاز تقنى موجودة تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمي خدمته وحركة الاتصالات التي تمت على ذلك النظام أو النظام التقني.

والأمر بالتسليم يكون موجهاً لمقدمي الخدمات، ومحله كافة البيانات أو المعلومات التي تتصل بارتكاب جريمة ما، ويشمل ذلك أيضاً بيانات مستخدمي الخدمة وحركة الاتصالات التي تمت، وهو إجراء يهدف إلى تمكين سلطات التحقيق من كشف الحقيقة وجمع الأدلة الرقمية ذات الصلة بجرائم تقنية المعلومات.

وقد حرصت العديد على المواثيق الدولية على تقرير الأمر بتسليم المعلومات لسلطات التحقيق، من أبرزها الاتفاقية الأوروبية في شأن الجرائم المعلوماتية (بودابست) والاتفاقية العربية لمكافحة جرائم تقنية المعلومات، فقد أجازت المادة (١٨) من اتفاقية بودابست إمكانية إصدار أمر لأي شخص لتقديم بيانات محددة موجودة على حاسب آلي بحوزته أو تحت سيطرته والمخزنة داخل نظام معلوماتي أو على أي وسيط تخزين بيانات آخر، فضلاً عن النص على إمكانية إصدار أمر لأي مُقدم خدمة يعرض خدماته في إقليم الدولة الطرف لتقديم معلومات للمشترك فيما يتعلق بتلك الخدمات الموجودة بحوزة أو تحت سيطرة مقدم الخدمة.

وكانت المادة (١٨) من الاتفاقية قد أشارت إلى أن مصطلح "معلومات المشترك" يعني به أية معلومات في صورة بيانات حاسب آلي أو أية صورة أخرى يتم حفظها من جانب مقدم الخدمة، والتي تتعلق بالمشتركين في الخدمات الخاصة به

بخلاف خط سير البيانات أو مضمونها والتي بموجبها يمكن التوصل إلى:

(أ) نوعية خدمة الاتصال المستخدمة، والشروط الفنية التي يتم اتخاذها في ذلك والفترة الزمنية للخدمة.

(ب) هوية المشترك وعنوانه البريدي أو الجغرافي، ورقم تليفونه وغير ذلك من أرقام الدخول الأخرى الخاصة به، والبيانات الخاصة بالفواتير والدفع المتاحة بموجب اتفاق الخدمة أو الترتيبات الخاصة بذلك.

(ج) أية معلومات أخرى خاصة بموقع تركيب أجهزة ومعدات اتصالات، والتي تتوافر بموجب اتفاق الخدمة أو الترتيبات الخاصة بذلك.

كما أجازت المادة (٢٥) من الاتفاقية العربية النص على إمكانية إصدار أمر لأي شخص لتسليم معلومات معينة في حيازته والمخزنة على تقنية معلومات أو وسيط تخزين معلومات، أو إصدار أمر لأي مزود خدمة يقدم خدماته في إقليم دولة طرف لتسليم معلومات المشترك المتعلقة بتلك الخدمات في حوزة مزود الخدمة أو تحت سيطرته.

المبحث الخامس

حجب المواقع الإلكترونية

أشار قانون مكافحة جرائم تقنية المعلومات إلى إجراء حجب المواقع الإلكترونية كأحد التدابير التي تقررها سلطة التحقيق في جرائم تقنية المعلومات، وهذا الإجراء ليس بجديد على المشرع المصري، فقد سبق النص عليه في قانون مكافحة الإرهاب ٩٤ لـ٢٠١٥ (م٤٩).

ويلاحظ وجود بعض الفوارق بين نص حجب المواقع الوارد في قانون مكافحة الإرهاب ونص الحجب الوارد في قانون مكافحة جرائم تقنية المعلومات؛ إذ أشار القانون الأخير إلى الرقابة القضائية على عمل جهة التحقيق بشأن امر الحجب، على خلاف قانون مكافحة الإرهاب الذي لم يشر إلى ذلك. بينما أشار قانون مكافحة الإرهاب إلى جواز أن يشمل الأمر بالحجب التحفظ على الأجهزة والمعدات المستخدمة في الجريمة، على خلاف قانون مكافحة جرائم تقنية المعلومات الذي لم يشر إلى ذلك.

وتبرز الإشارة إلى تشكيك البعض[1] في مدى إمكان تطبيق هذا الإجراء، مبرراً ذلك بأن تنفيذه مرهون بالتقدم التكنولوجي الذي تصل إليه الجهات الفنية المساعدة والمعنية بتنفيذ قرارات سلطة التحقيق، سيما وأن غالبية الخوادم الخاصة بالمواقع تبث من خارج القطر المصري، وهو ما قرره صراحة قانون مكافحة جرائم تقنية المعلومات حينما نص على عبارة "كلما أمكن تحقيق ذلك فنياً"، بالنظر إلى أنه في بعض الأحوال قد يصعب تنفيذ هذا الحجب.

---

[1] د. أحمد الضبع: إشكاليات مواجهة الإرهاب، مرجع سابق، ص ص١٩٨، ١٩٩.

وأخيراً تبرز الإشارة إلى أن قانون مكافحة الإرهاب أجاز للنيابة العامة أو سلطة التحقيق المختصة إصدار الأمر بالحجب، بينما فضل المشرع الجنائي في نص قانون مكافحة جرائم تقنية المعلومات استخدام مصطلح جهة التحقيق والذي يشمل بعينه كل من النيابة العامة وقاضي التحقيق، ومن ثم فلا خلاف بين النصين في ذلك.

وتبرز الإشارة إلى أهمية التمييز بين إجراء حجب المواقع وبين إجراءي الغلق والوقف؛ فحجب المواقع يقصد به استخدام سلطات الدولة لتقنيات أو أدوات فنية، تؤدي إلى منع ظهور أو السماح بالدخول لهذه المواقع داخل القطر المصري، فإجراء الحجب لا يفترض وقف الموقع أو إغلاقه، بينما يقصد بالوقف أو الإلغاء قيام الجهة أو الشركة مقدمة الخدمة "الخادم" التي تعمل على تشغيل الموقع باتخاذ إجراءات فنية بشأن وقفه أو إلغائه، والوقف يتضمن التعطيل المؤقت للموقع، بينما الإلغاء يشمل التعطيل الدائم للموقع وإنهاء وجوده مستقبلاً وجعله والعدم سواء.

وقد تطرق القانون للإجراءات الصادرة بشأن طلبات حجب المواقع، إذ منح لجهة التحقيق المختصة-سواء أكانت النيابة العامة أم قاضي التحقيق- أن تأمر بحجب موقع أو مواقع أو روابط أو محتوى محل البث، كلما أمكن تحقيق ذلك فنياً، حيث أوضحت المادة السابعة المعنونة بـ"الإجراءات والقرارات الصادرة بشأن طلبات حجب المواقع" هذه الأمور وأبانت جهة إصدارها وشروطها، وحالاتها، ومدتها، وأحوال إنهائها أو سقوطها؛ إذ تقضي المادة المذكورة بأنه:" *لجهة التحقيق المختصة متى قامت أدلة على قيام موقعُ يبث من داخل الدولة أو خارجها، بوضع أي عبارات أو أرقام أو صور أو أفلام، أو أي مواد دعائية أو ما في حكمها، بما يُعد جريمة من الجرائم المنصوص عليها في هذا القانون، ويشكل تهديداً للأمن القومي أو يعرض أمن البلاد أو اقتصادها القومي للخطر، أن تأمر بحجب الموقع أو المواقع محل البث، كلما أمكن تحقيق ذلك فنياً. وعلى جهة التحقيق عرض أمر الحجب على المحكمة المختصة، منعقدة في غرفة المشورة خلال أربع وعشرين ساعة مشفوعاً بمذكرة برأيها، وتصدر*

كمة قرارها في الأمر مسبباً إما بالقبول أو بالرفض، في مدة لا تجاوز اثنتين وسبعين ساعة من وقت عرضه عليها ".

الاعتبارات التي يقوم عليها قرار حجب المواقع: تطلب القانون أمرين لإجازة حجب المواقع الإلكترونية، وهما:-

١- وجود أدلة على قيام موقع بوضع أي عبارات أو أرقام أو صور أو أفلام أو أية مواد دعائية، أو ما في حكمها مما تعد جريمة من الجرائم المنصوص عليها بالقانون، ويستوي لدى القانون أن يكون الثمن داخل الدولة أو خارجها.

٢- أن يشكل هذا البث تهدياً للأمن القومي أو يعرض أمن البلاد أو اقتصادها القومي للخطر.

فهذا الإجراء يعد من التدابير الجنائية التي تتخذها جهات التحقيق للحد من مخاطر هذه المواقع في بث الشائعات والمساس بمقدرات الدولة، وهو ما عمل المشرع على تنظيمه من خلال وضع ضوابط ومحددات لهذه الجهات في إصدار أوامر الحجب.

ويعتقد الباحث أن القانون يشترط أن تكون الأدلة المتوافرة لدى جهات التحقيق على وقوع جريمة معلوماتية من الجرائم المنصوص عليها في القانون، أو توافر حالة من حالات تهديد الأمن القومي أو أمن البلاد أو اقتصادها القومي للخطر جدية، حتى يجوز لها عرض أمر الحجب على المحكمة، وتخضع تقدير هذه الأدلة ومدى جديتها لسلطة المحكمة وفقاً لظروف وملابسات الدعوى المعروضة أمامها.

الجهة المعنية بإصدار أمر الحجب: أشار القانون إلى الجهة المعنية بإصدار قرار الحجب وهي جهة التحقيق المختصة، ومن ثم تشمل كل من النيابة العامة وقاضي التحقيق، ويجب أن تكون هذه الجهة مختصة بتحقيق الدعوى وفقاً لقواعد الاختصاص المكاني المقررة في التشريع المصري، وهي مكان وقوع الجريمة أو مكان إقامة المتهم أو مكان ضبطه.

وتبرز الإشارة إلى أن البعض قد ذهب إلى أن المشرع لم يشترط درجة معينة فيمن يصدر هذا الأمر من جهة التحقيق إذا كان من أعضاء النيابة العامة، ومن ثم يجوز أن يصدره أي من أعضاء النيابة العامة، بمن فيهم مساعدوها، ولكن الرأي السابق يرى أن إجراء غلق أو حجب بعض أنواع المواقع الإلكترونية قد يكون له من الأثر ما يفوق غلق المقار والأماكن، وهو ما يستلزم في مصدر هذا الأمر قدراً من الخبرة لتقدير ما يعرض عليه، لذلك يفضل الرأي السابق أن تخول هذه السلطة لمن لا تقل درجته عن رئيس نيابة بالنسبة لأعضاء النيابة العامة[1]. إلا أن النص الحالي قد قصر هذه السلطة على القائم بالتحقيق من أعضاء النيابة العامة أيا كانت درجته، ومن ثم يجوز لمعاوني النيابة ومساعديها – من الناحية القانونية- إصدار الأمر بحجب المواقع الإلكترونية.

الجهة الفنية المعنية بتنفيذ أمر الحجب:تتولى النيابة العامة أو قاضي التحقيق بإخطار الجهاز القومي لتنظيم الاتصالات بقرارها بحجب الموقع الإلكتروني، والذي يقوم بدوره بإخطار مقدم الخدمة على الفور بقرار الحجب ليتولى تنفيذه، ومن ثم يجب أن يكون القرار محدداً لنطاق تطبيقه، ويترتب على إخلال مقدم الخدمة بتنفيذ الأوامر القضائية الخاصة بحجب المواقع تقرير مسئوليته الجنائية على النحو السالف الإشارة إليه سابقاً، ولا يعفي مقدم الخدمة من المسئولية الجنائية إلا استحالة تنفيذ قرار الحجب من الناحية الفنية على النحو الذي سبق أن أشار إليه القانون بأن يكون الحجب كلما أمكن تحقيق ذلك فنياً، ومن ثم قد تصدر النيابة العامة أو قاضي التحقيق أمراً بالحجب ولكن يتعذر للسلطات المصرية تنفيذه -كما سبق أن أشرنا- لوجود غالبية الخوادم الخاصة بهذه المواقع خارج الدولة.

إجراءات حجب المواقع في حالة الاستعجال:ويجوز في حالة الاستعجال لوجود خطر حال أو ضرر وشيك الوقوع من ارتكاب جريمة، أن تقوم جهات التحري والضبط،

---

[1] المرجع السابق، ص ١٩٩.

بإبلاغ الجهاز القومي لتنظيم الاتصالات، ليقوم بإخطار مقدم الخدمة على الفور بالحجب المؤقت، ويُلتزم بتنفيذ مضمون الإخطار فور وروده إليه، وعلى جهة التحري والضبط المبلغة أن تعرض محضرا تثبت فيه ما تم من إجراءات على سلطة التحقيق المختصة، خلال ٤٨ ساعة من تاريخ الإبلاغ الذي وجهته للجهاز، فإذا لم يعرض المحضر في الموعد المحدد، يعد الحجب الذي تم كأن لم يكن، وتعرض سلطة التحقيق أمر الحجب على المحكمة المختصة خلال ٢٤ ساعة مشفوعاً بمذكرة برأيها، على أن يصدر القرار في الطلب في مدة لا تجاوز ٧٢ ساعة من وقت عرضه عليها. ولمحكمة الموضوع أثناء نظر الدعوى أو بناء على طلب سلطة التحقيق أو الجهاز أو ذوى الشأن أن تأمر بإنهاء القرار الصادر بالحجب أو تعديل نطاقه[1].

ويسقط القرار الصادر بالحجب بصدور أمر بأن لا وجه لإقامة الدعوى الجنائية أو بصدور حكم بات فيها بالبراءة، حيث تنص المادة (السابعة/ فقرات٣حتى ٧) من القانون على أنه:" *ويجوز في حالة الاستعجال لوجود خطر حالّ، أو ضرر وشيك الوقوع، أن تقوم جهات التحرى والضبط المختصة بإبلاغ الجهاز، ليقوم بإخطار مقدم الخدمة على الفور بالحجب المؤقت للموقع أو المحتوى أو المواقع أو الروابط المذكورة في الفقرة الأولى من هذه المادة وفقاً لأحكامها. ويلتزم مقدم الخدمة بتنفيذ مضمون الإخطار فور وروده إليه. وعلى جهة التحرى والضبط التي قامت بالإبلاغ أن تحرر*

---

[1] من الجدير بالذكر أن مشروع قرار رئيس مجلس الوزراء بإصدار اللائحة التنفيذية للقانون رقم ١٧٥ لسنة ٢٠١٨ كان قد تضمن مادة برقم (٧) تنص على أنه:" يلتزم مقدم الخدمة بالاستجابة لطلبات الحجب الواردة طبقاً للمادة رقم ٧ من القانون، ولا يعد مسئولاً عن الآثار أو الأضرار المترتبة على هذه الطلبات في مواجهة الغير نتيجة استجابته لتلك الطلبات. ويجب في جميع الأحوال أن يكون الأمر، أو البلاغ، أو الإخطار الصادر بخصوص إجراءات الحجب، رسمياً ومكتوباً وموجهاً إلى الرئيس التنفيذي للجهاز. على أن يُخطر الجهاز مقدم أو مقدمي الخدمة بخطاب رسمي لتنفيذ الحجب. ويحق للجهاز التقدم إلى محكمة الموضوع أثناء نظرها الدعوى بطلب لإنهاء القرار الصادر بالحجب أو بتعديل نطاقه. وفي جميع الأحوال يُمثل الجهاز في الجلسة المحددة لنظر التظلم من الأمر أو القرار القضائي الصادر بالحجب أمام المحكمة المختصة وذلك بناء على إعلان له بالحضور".

حضراً تثبت فيه ما تم من إجراءات وفق أحكام الفقرة السابقة يُعرض على جهات التحقيق خلال ثمانٍ وأربعين ساعة من تاريخ الإبلاغ الذي وجهته للجهاز، وتتبع في شأن هذا المحضر ذات الإجراءات المبينة بالفقرة الثانية من هذه المادة. وتصدر كمة المختصة قرارها في هذه الحالة إما بتأييد ما تم من إجراءات حجب، أو بوقفها. فإذا لم يُعرض المحضر المشار إليه في الفقرة السابقة في الموعد المحدد، يعد الحجب الذي تم كأن لم يكن".

الجهة المخولة بإنهاء أمر الحجب او تعديله: أناط القانون بمحكمة الموضوع، من تلقاء نفسها، أو بناء على طلب جهة التحقيق، أو الجهاز القومي لتنظيم الاتصالات، أو ذوي الشأن، أن تأمر بإنهاء الأمر بالحجب أو تعديل نطاقه، حيث تقضي الفقرة الثالثة من المادة السابعة بأنه:" *ولمحكمة الموضوع أثناء نظر الدعوى، أو بناءً على طلب جهة التحقيق أو الجهاز أو ذوى الشأن أن تأمر بإنهاء القرار الصادر بالحجب، أو تعديل نطاقه*".

أحوال سقوط الأمر بالحجب: أشار القانون إلى أحوال سقوط الأمر بالحجب واعتباره كأن لم يكن، وتتمثل هذه الأحوال فيمايلي:-

١- عدم قيام جهة التحرى والضبط بعرض محضر الإجراءات الخاص بطلب الحجب المستعجل على جهة التحقيق المختصة خلال المدة الزمنية المقررة قانوناً (ثمانٍ وأربعين ساعة من تاريخ الإبلاغ الذي وجهته للجهاز القومي للاتصالات)، وفي هذه الحالة يعد الحجب الذي تم كأن لم يكن.

٢- صدور قرار من جهة التحقيق المختصة (النيابة العامة أو قاضي التحقيق) بألا وجه لإقامة الدعوى الجنائية، ويكون ذلك بعد تحقيق الدعوى من جانب جهة التحقيق، وتوافر سبب من أسباب الحفظ بالدعوى.

٣- صدور حكم محكمة الموضوع في الدعوى بالبراءة، وهو ما أشارت إليه الفقرة الأخيرة من المادة السابعة من أنه:"*وفى جميع الأحوال، يسقط القرار الصادر*

بالحجب بصدور أمر بألا وجه لإقامة الدعوى الجنائية، أو بصدور حكم نهائي فيها بالبراءة"، ومن ثم يشترط في هذا الحكم أن يكون باتاً؛ أي أن يكون مستنفذاً كافة طرق الطعن العادية وغير العادية، حتى يعتد به كعنوان للحقيقة[1].

التظلم من قرار الحجب: منح القانون للمتظلم الحق في تقديم تظلمه بعد انقضاء سبعة أيام من تاريخ القرار أو تاريخ تنفيذه، وإذا رُفض له أن يتقدم بآخر كلما انقضت ثلاثة أشهر من تاريخ الحكم بالرفض، وتفصل المحكمة في التظلمات خلال مدة لا تجاوز ٧ أيام من تقديمها، حيث بينت المادة الثامنة من القانون المعنونة بـ"التظلم من القرارات الصادرة بشأن طلبات حجب المواقع" مواعيد وإجراءات التظلم من القرارات القضائية الصادرة في طلبات حجب المواقع الإلكترونية، حيث تقضي المادة المذكورة بأنه:" *لكل من صدر ضده قرار قضائي من المنصوص عليها في المادة (٧) من هذا القانون، وللنيابة العامة ولجهة التحقيق المختصة ولكل ذى شأن، أن يتظلم منه أو من إجراءات تنفيذه أمام محكمة الجنايات المختصة بعد انقضاء سبعة أيام من تاريخ صدور الأمر أو من تاريخ تنفيذه بحسب الأحوال. فإذا رُفض تظلمه فله أن يتقدم بتظلم جديد كلما انقضت ثلاثة أشهر من تاريخ الحكم برفض التظلم. وفي جميع الأحوال، يكون التظلم بتقرير يودع قلم كتاب محكمة الجنايات المختصة، وعلى رئيس المحكمة أن يحدد جلسة لنظر التظلم يعلن بها المتظلم والجهاز وكل ذي شأن، وعلى المحكمة أن تفصل في التظلم خلال مدة لا تجاوز سبعة أيام من تاريخ التقرير به*"، ومن ثم يتضح من النص السابق مايلي:-

أ) صاحب الحق في التظلم: منح القانون الحق في التظلم لكل من صدر ضده قرار قضائي بحجب المواقع الإلكترونية الخاصة به، وللنيابة العامة أو لجهة التحقيق المختصة، كما لو كان المختص بالتحقيق في الدعوى أحد قضاة التحقيق، ولكل ذي شأن، ومن ثم يجوز للجهاز القومي للاتصالات التظلم من قرار الحجب، إذا كان لذلك

[1] د. مأمون سلامة: الإجراءات الجنائية، مرجع سابق، ص٣٢٦ ومابعدها.

مقتضى يرتبط بسلامة نظم المعلومات والبيانات، ويكون له التظلم من قرار الحجب ذاته أو من إجراءات تنفيذه.

ب) الجهة القضائية المعنية بنظر التظلم: حدد القانون الجهة القضائية المعنية بنظر التظلم وهي محكمة الجنايات المختصة.

ج) ميعاد التظلم: يحق لصاحب الحق في التظلم رفع تظلمه من قرار الحجب أو من إجراءات تنفيذه بعد انقضاء سبعة أيام من تاريخ صدور الأمر أو من تاريخ تنفيذه بحسب الأحوال، فإذا رُفض تظلمه فله أن يتقدم بتظلم جديد، كلما انقضت ثلاثة أشهر من تاريخ الحكم برفض التظلم.

د) إجراءات التظلم: يكون التظلم بتقرير يودع قلم كتاب محكمة الجنايات المختصة، وعلى رئيس المحكمة أن يحدد جلسة لنظر التظلم يعلن بها المتظلم والجهاز وكل ذي شأن، وعلى المحكمة أن تفصل في التظلم خلال مدة لا تجاوز سبعة أيام من تاريخ التقرير به.

المبحث السادس

المنـع من السفـر

وضعت المادة التاسعة من القانون حالات منع المتهمين من السفر، وإجراءات وجهة إصدار قرار المنع، ومدته وإجراءات التظلم منه، وإنهاءه، حيث أجاز القانون للنائب العام أو من يفوضه من المحامين العامين الأول بنيابات الاستئناف، عند الضرورة أو عند وجود أدله كافية على جدية الاتهام، أن يصدر أمر مسبب ولمدة محددة بمنع المتهم من السفر خارج البلاد ووضع اسمه على قوائم ترقب الوصول، حيث تقضي المادة المذكورة المعنونة بـ"المنع من السفر" بأنه:" *يجوز للنائب العام أو من يفوضه من المحامين العموم الأول بنيابات الاستئناف، ولجهات التحقيق المختصة، عند الضرورة أو عند وجود أدلة كافية على جدية الاتهام في ارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون أو الشروع في ارتكابها، أن يأمر بمنع المتهم من السفر خارج البلاد، أو بوضع اسمه على قوائم ترقب الوصول، بأمر مسبب لمدة محددة*".

أولاً- أحوال المنع من السفر: حدد القانون حالات المنع من السفر في الجرائم المعلوماتية والمتمثلة في وجود حالة الضرورة تتطلب منع الشخص من السفر، أو وجود أدلة كافية على اتهامه بارتكاب إحدى الجرائم المعلوماتية أو الشروع في ارتكابها، ويخضع تقدير مدى توافر الأدلة الكافية على صحة الاتهام الموجه للمتهم للسلطة التقديرية للنائب العام أو من يفوضه من المحامين العموم الأول بنيابات الاستئناف، وفي ضوء المعلومات المتوافرة لدى النيابة العامة على صحة الاتهامات الموجهة للمتهم.

ثانياً-إجراءات المنع من السفر وجهة إصداره: يكون المنع من السفر بقرار من النائب العام أو من يفوضه من المحامين العموم الأول بنيابات الاستئناف، أو بوضع اسمه على قوائم ترقب الوصول، على أن يكون قرار المنع أو ترقب الوصول مسبباً ومؤقتاً لمدة محددة.

ثالثاً-الطبيعة القانونية لأمر المنع: أبانت محكمة النقض المصرية في أحد أحكامها الطبيعة القانونية لأوامر المنع من التصرف، وترجع أهمية هذا التحديد للطبيعة القانونية، لبيان عما إذا كانت هذه الأوامر من طبيعة قضائية؟، ومن ثم تخضع لرقابة القضاء الجنائي، أم كانت من طبيعة إدارية؟، فتخضع لرقابة القضاء الإداري، وقد قضت محكمة النقض في أحد أحكامها بأن الأمر بالمنع من السفر من الإجراءات الجنائية التي تباشرها النيابة العامة باعتبارها سلطة تحقيق أو القاضي المختص عند ارتكاب جريمة، والتي ترمي إلى بقاء المتهم قريباً من السلطة التي تباشر التحقيق والمحافظة على أدلة الاتهام، وهي بهذه المثابة أعمال تحقيق لها طبيعة قضائية وقيام جهة الإدارة بتنفيذها لا ينظر إليه بمعزل عن هذا الأمر وليس من شأنه أن يغير وصفه باعتباره صادراً من السلطة القضائية[1].

وقد حذت المحكمة الدستورية العليا حذو محكمة النقض في اعتبار قرار المنع من السفر قراراً قضائياً يخضع لاختصاص القضاء العادي، وذلك في الدعوى التي أقيمت في تنازع الاختصاص السلبي بين جهتي القضاء العادي والإداري، حيث طالب المدعيان القضاء بتحديد الجهة القضائية المختصة بالفصل في النزاع على قرار النائب العام بمنعهما من السفر، بعد أن تسلبت كل من جهتي القضاء العادي والإداري من نظره. وقد قضت المحكمة الدستورية العليا في هذا الشأن بأنه:"وحيث إن إجراءات

[1] انظر: مجموعة أحكام محكمة النقض، جلسة ٢٠٠٩/٦/٤، الطعن رقم ٥٤١٠ لسنة ٦٦ ق، رقم ١١٠، ص٦٧٠.

التحقيق التي تتولاها النيابة العامة بمناسبة ارتكاب جريمة جنائية تتميز بأنها ذات طبيعة قضائية، بها تتحرك الدعوى الجنائية، ويتحدد بمقتضاها التصرف في هذه الدعوى، إما بإحالتها إلى المحكمة المختصة، أو بالأمر فيها بألا وجه لإقامتها، وكان القرار الصادر من النائب العام بمنع المتهمين من السفر -بمناسبة التحقيقات التي تجريها النيابة العامة معهم- يعد إجراءً قضائياً من الإجراءات الجنائية التي تباشرها النيابة العامة باعتبارها سلطة ناط بها القانون مهمة التحقيق عند ارتكاب جريمة، وكانت الغاية من إصدار ذلك القرار، هو بقاء المتهم قريباً من السلطة التي تباشر التحقيق والمحافظة على أدلة الاتهام، وهو بهذه المثابة يعد عملاً من أعمال التحقيق التي تتسم بالطبيعة القضائية، ومن ثم تكون جهة القضاء العادي، وقد ناط بها المشرع اختصاص الفصل في الدعوى الجنائية، هي المختصة بنظر المنازعات التي تثور بشأن تلك القرارات، ذلك أن هذه القرارات وقد صدرت من النيابة العامة في شأن منازعة جنائية، باعتبارها تتصل بجريمة من الجرائم التي تدخل في اختصاص جهة القضاء العادي، فإن هذه الجهة بحسبانها الجهة صاحبة الولاية العامة بالفصل في كافة المنازعات والجرائم -عدا ما تختص به محاكم مجلس الدولة- تكون هي المختصة بنظر الطعن على هذه القرارات.

وقد أسست المحكمة الدستورية العليا قضائها باختصاص القضاء العادي بنظر الطعن على أوامر المنع من السفر على عدة أمور أولهما كما سبق أن أشرنا إلى أن محكمتنا العليا أن قرار المنع من السفر من الإجراءات القضائية التي تباشرها النيابة العامة بمناسبة التحقيق في شأن منازعة تتصل بجريمة من جرائم القانون العام التي تدخل في اختصاص القضاء الجنائي، أضف إلى ذلك أمرين آخرين: الأول حيث اعتبرت محكمتنا العليا المحكمة المختصة بنظر أصل الموضوع تكون هي بذاتها الأجدر بنظر الأمور المتفرعة عنه، ومن ثم فإن الأمر بالمنع من السفر يتصل بإجراءات التحقيق الجنائي التي تباشرها النيابة العامة، إما الأمر الثاني يتصل بحسن إدارة العدالة

والمتمثل في عدم ضرورة تقطيع أواصر النزاع بين جهات قضائية مختلفة.

حيث قررت المحكمة أنه:" وحيث إن ما تقدم يؤكده أن القرار الصادر من النائب العام بمنع المتهمين من السفر- كما هو الحال في الدعوى الماثلة- إنما صدر بمناسبة تحقيقات تجريها النيابة العامة، والتي تنتهي بصدور قرار قضائي منها، إما بالأمر بألا وجه لإقامة الدعوى، أو بإحالتها إلى المحكمة الجنائية، بحسبانها المختصة بنظر الدعوى الجنائية والتعقيب على القرارات والأوامر التي تصدرها النيابة العامة في شأن التحقيقات الجنائية، وإذا كان مستقر هذه التحقيقات في الحالتين إلى المحاكم الجنائية، فإن تلك المحاكم تكون هي المختصة بنظر المنازعات التي يثيرها ذلك القرار، إعمالاً لقاعدتين -أولاهما- أن المحكمة المختصة بالفصل في أصل النزاع تكون هي المختصة بالتالي بنظر ما يتفرع عنه من منازعات، ثانيتهما- أن تحقيق العدالة تستوجب أن تكون المنازعة وما يتفرع عنها بيد جهة قضائية واحدة، جمعاً لأواصر تلك المنازعة، وحرصاً على عدم تقطيع أوصالها بين جهات قضائية مختلفة، إذ كان ما تقدم وكان القرار الصادر من النائب العام بمنع المدعيين من السفر قد صدر بمناسبة تحقيقات تجريها النيابة العامة معهما، ويتصل بجريمة من الجرائم الجنائية التي تدخل في اختصاص جهة القضاء العادي، ومن ثم تكون تلك الجهة هي المختصة بنظر الطعن على ذلك القرار.

وقد استطردت محكمتنا العليا في هذه المسألة، حيث أشارت إلى أنه:" وحيث إنه لا ينال مما تقدم القول، بأن القرارات التي يصدرها النائب العام بمنع المتهمين من السفر بمناسبة التحقيق معهم، يعوزها السند القانوني الذي ينظم هذه القرارات ويحدد إجراءات الطعن عليها، ذلك أن تقاعس المشرع العادي عن إصدار تشريع ينظم إجراءات المنع من السفر والسلطة المختصة بتقريره والجهة التي تختص بنظر الطعن عليها، لا يغير من الطبيعة القضائية لتلك القرارات، ولا يسوغ بحال إسناد الفصل في المنازعات التي تثيرها تلك القرارات لمحاكم مجلس الدولة، والتي حددت الدساتير

المصرية ابتداء بدستور ١٩٧١ وانتهاء بالدستور الحالي اختصاصه حصراً في المنازعات الإدارية باعتباره قاضيها الأصيل. وقد حكمت المحكمة بتعيين جهة القضاء العادي جهة مختصة بنظر التظلم من قرار النائب العام الصادر بالمنع من السفر[١].

رابعاً- التظلم من قرار المنع من السفر: أبان القانون أن للممنوع أو المدرج على القوائم، التظلم أمام المحكمة الجنائية المختصة خلال خمسة عشر يوما من تاريخ علمه به، وإذا رفضت تقدم بآخر كلما انقضت ثلاثة أشهر من تاريخ الحكم، وتفصل المحكمة في التظلمات خلال مدة لا تجاوز خمسة عشر يوما بحكم مسبب بعد سماع أقوال المتظلم وسلطة التحقيق المختصة، ويجوز للنيابة العامة فى كل وقت العدول عن الأمر الصادر منها، والتعديل فيه برفع الاسم لمدة محددة إذا دعت الضرورة لذلك.

وتقضي الفقرة الثانية من المادة التاسعة من القانون بأنه:"*ولمن صدر ضده أمر المنع من السفر أن يتظلم من هذا الأمر أمام محكمة الجنايات المختصة، خلال خمسة عشر يوماً من تاريخ علمه به. فإذا رفض تظلمه فله أن يتقدم بتظلم جديد كلما انقضت ثلاثة أشهر من تاريخ الحكم برفض التظلم.ويكون التظلم بتقرير يودع قلم كتاب محكمة الجنايات المختصة، وعلى رئيس المحكمة أن يحدد جلسة لنظر التظلم تُعلن بها النيابة العامة والمتظلم، وعلى المحكمة أن تفصل في التظلم خلال مدة لا تجاوز خمسة عشر يوماً من تاريخ التقرير به، بحكم مسبب بعد سماع أقوال المتظلم والنيابة العامة أو جهة التحقيق المختصة حسب الأحوال، ولها في سبيل ذلك أن تتخذ ما تراه من إجراءات أو تحقيقات ترى لزومها في هذا الشأن.ويجوز للنيابة العامة وجهات التحقيق المختصة في كل وقت العدول عن الأمر الصادر منها، كما يجوز لها التعديل فيه برفع الاسم من قوائم المنع من السفر أو ترقب الوصول لمدة محددة، إذا دعت الضرورة*

[١] انظر: حكم المحكمة الدستورية العليا في الدعوى رقم ٤٠ لسنة ٢٧ قضائية "تنازع"، جلسة ٢٠١٥/٦/١٣.

لذلك.وفى جميع الأحوال، ينتهي المنع من السفر بمرور سنة من تاريخ صدور الأمر، أو بصدور قرار بألا وجه لإقامة الدعوى الجنائية، أو بصدور حكم نهائي فيها بالبراءة، أيهما أقرب"، ويتضح من النص السابق مايلي:-

أ) ميعاد التظلم وجهة نظره: أجاز القانون لمن صدر ضده أمر المنع من السفر أن يتظلم منه أمام محكمة الجنايات المختصة، خلال خمسة عشر يوماً من تاريخ علمه به، فإذا رفض تظلمه، فله أن يتقدم بتظلم جديد، كلما انقضت ثلاثة أشهر من تاريخ الحكم برفض التظلم.

ب) إجراءات التظلم: يكون التظلم بتقرير يودع قلم كتاب محكمة الجنايات المختصة، وعلى رئيس المحكمة أن يحدد جلسة لنظر التظلم تُعلن بها النيابة العامة والمتظلم، وعلى المحكمة أن تفصل في التظلم خلال مدة لا تجاوز خمسة عشر يوماً من تاريخ التقرير به، بحكم مسبب بعد سماع أقوال المتظلم والنيابة العامة أو جهة التحقيق المختصة حسب الأحوال، ولها في سبيل ذلك أن تتخذ ما تراه من إجراءات أو تحقيقات ترى لزومها في هذا الشأن.

خامساً- العدول قرار المنع من السفر: أجاز القانون للنيابة العامة وجهات التحقيق المختصة في كل وقت العدول عن الأمر الصادر منها، كما يجوز لها التعديل فيه برفع الاسم من قوائم المنع من السفر أو ترقب الوصول لمدة محددة، إذا دعت الضرورة لذلك.

سادساً- أحوال إنهاء قرار المنع من السفر: أشار القانون إلى أحوال إنهاء المنع من السفر، حيث ينتهي المنع من السفر بمضي سنة من تاريخ صدور الأمر، أو بصدور قرار بألا وجه لإقامة الدعوى الجنائية من النيابة العامة أو قاضي التحقيق، أو بصدور حكم نهائي فيها من المحكمة الجنائية المختصة بالبراءة، أيهما أقرب.

المبحث السابع

الإثبات الجنائي في جرائم تقنية المعلومات

تلعب كل من الخبرة والأدلة الرقمية دوراً مهماً في إثبات جرائم تقنية المعلومات، وهو ما حرص المشرع على النص عليه، حيث نظمتا المادتان العاشرة والحادية عشرة من القانون عمل الخبراء المتخصصين في تطبيق أحكامه، وحجية وقوة الأدلة الرقمية في مجال الإثبات الجنائي، ونتناول فيمايلي الأحكام التي تضمنها القانون بشأن الخبراء والأدلة الرقمية، وذلك في مطلبين على النحو التالي:-

المطلب الأول

الخبرة في جرائم تقنية المعلومات

تعريف الخبرة: يقصد بالخبرة إبداء رأي فني من شخص مُختص فنياً في شأن واقعة ذات أهمية في الدعوى[١]، فهي وسيلة لتحديد التفسير الفني للأدلة أو الدلائل بالاستعانة بالمعلومات العلمية، وهي في حقيقتها ليست دليلاً مستقلاً عن الدليل القولي أو المادي، وإنما هي تقييم فني لهذا الدليل[٢].

وقد عرف قانون مكافحة جرائم تقنية المعلومات الخبرة في إطار هذه الجرائم بأنها: "كل عمل يتصل بتقديم الاستشارات أو الفحص أو المراجعة أو التقييم أو التحليل في مجالات تقنية المعلومات".

---

[١] د. محمود نجيب حسني: شرح قانون الإجراءات الجنائية، مرجع سابق، ص٥٣٠.

[٢] د. أحمد فتحي سرور: الوسيط في شرح قانون الإجراءات الجنائية، دار النهضة العربية، ط٧، ١٩٩٦، ص٥٨٨؛ د. محمد عبد اللطيف فرج: شرح قانون الإجراءات الجنائية، مرجع سابق، ص٢٧٧ وما بعدها.

التمييز بين الخبرة والشهادة: من الملاحظ أن القانون رقم ١٧٥ لـ٢٠١٨ لم يشر إلى أحكام خاصة بالخبرة أو الشهادة في جرائم تقنية المعلومات، وإنما أقتصر الأمر في شأن الخبرة على تحديد طوائف الخبراء في جرائم تقنية المعلومات، ومن ثم تنطبق في هذه الحالة القواعد العامة الواردة في قانون الإجراءات الجنائية في شأن كل من الشهادة والخبرة.

ويقصد بالشهادة تقرير يصدر عن شخص في شأن واقعة عاينها بحاسة من حواسه، ويرى البعض[1] أن الشهادة في الجرائم المعلوماتية ذات طابع خاص، وأن الشاهد في مثل هذا النوع من الجرائم هو الشخص الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب، والذي تكونت لديه معلومات جوهرية لازمة لولوج الحاسب الآلي والنظام المعلوماتي إذا كانت مصلحة التحقيق تقتضى التنقيب عن أدلة الجريمة داخله.

ويضيف الرأي السابق إلى هذا بأن قد يوجد عدد من الأشخاص بحكم وظيفتهم وخبرتهم واتصال عملهم بالتقنية والنظم المعلوماتية يمكن اعتبارهم كشهود معلوماتيون، بحيث يقع تحت بصرهم أو علمهم بعض المعلومات والأخبار التي تتصل بارتكاب جرائم معلوماتية، ومن أبرز هؤلاء الأشخاص عامل تشغيل الحاسب وهو الشخص المسئول عن تشغيل هذا الجهاز والمعدات المتصلة به، ومدخل البيانات، وهو من يقومون بنقل البيانات من الوثائق إلي وسط التخزين حتي تتم معالجتها بواسطة الحاسب، ومخطط البرامج والنظم المعلوماتية، ممن يقوم بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم، ثم يقوم بتحويلها إلى برامج دقيقة وموثقة

---

[1] انظر: د. هلالي عبد اللاه أحمد: التزام الشاهد بالإعلام في الجرائم المعلوماتية- دراسة مقارنة، بدون ناشر، ١٩٩٨، ص ص٢٣، ٢٤.

لتحقيق هذه المواصفات، واختيار وتعديل وتصحيح برامج نظام الحاسب الداخلية المعقدة. كما يوجد أيضاً محلل البيانات والنظم المعلوماتية، وهو من يقوم بتحليل الخطوات وتجميع بيانات نظام معين، ودراستها ثم تحليل النظام بتقسيمه إلى وحدات منفصلة واستنتاج العلاقات الوظيفية بين هذه الوحدات، وتتبع البيانات داخل النظام، واستنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسب.

كما يوجد أيضاً مهندسو الصيانة والاتصالات، وهم من يقوموا بأعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة به، ومديرو النظم، وهم من يوكل لهم أعمال الإدارة في النظم المعلوماتية، وكل هؤلاء الأشخاص أن يكون لديهم والخبرة والدراية الكافية في استخدام الحاسب الآلي والأجهزة التقنية، كذلك يتوافر لديهم كم من المعلومات المناسبة عن استخدام الحاسب الآلي والنظم المعلوماتية.

ويميز الفقه الجنائي بين كل من الخبرة والشهادة من حيث أن الأولى ترتكز على الرأي الفني للخبير في كشف الدلائل أو تحديد قيمتها التدليلية في الإثبات على خلاف الثانية، ومن ثم كانت الخبرة وقفاً على الأخصائيين من أهل العلم والتكنولوجيا لا بناء على مجرد مُشاهدتهم أو سماعهم، فالشاهد يدلي بأقواله عن الواقعة كما حدثت في مادياتها، أما الخبير فشهادته فنية؛ أي تنصرف إلى تقييمه الفني للواقعة محل الخبرة[١]، ونتيجة لذلك أجاز الفقه استبدال الخبير في الدعوى بغيره من الخبراء، وهو أمر غير مُتصور بالنسبة للشاهد لأن دوره في الدعوى قاصر عليه وحده[٢].

---

[١] د. مأمون محمد سلامة، الإجراءات الجنائية في التشريع المصري، مرجع سابق، ص٦٧٣.

[٢] د. آمال عبد الرحيم عثمان: الخبرة في المسائل الجنائية، رسالة دكتوراه، جامعة القاهرة، ١٩٦٤، ص ص٣٦-٩٥.

فالشاهد يقدم الى القاضي معلومات حصلها بالملاحظة الحسية، أما الخبير فيقدم الى القاضي تقارير وآراء توصل إليها بتطبيق قوانين علمية أو أصول فنية[١]، وقد يجمع الشخص بين صفتي الشاهد والخبير، كطبيب شهد ارتكاب جريمة قتل وحاول إسعاف المجني عليه قبل وفاته، فأتيح له بذلك معرفة أسباب وفاته[٢].

قواعد ندب الخبراء:هذا وقد نصت المادة (٨٥) إجراءات جنائية على إجراء ندب الخبراء كأحد إجراءات التحقيق في الدعوى الجنائية؛ إذ أجازت للمُحقق أن ينتدب خبيراً إذا ثارت أثناء التحقيق الابتدائي مشكلة فنية يتوقف على حسمها استمرار التحقيق وبلوغه غرضه في التنقيب عن أدلة الجريمة، وإذا كان الاستعانة بالخبرة أمراً جوازياً لجهة التحقيق والحكم، فقد استقر قضاء محكمة النقض المصرية على ضرورة استطلاع رأي أهل الخبرة في المسائل الفنية البحتة؛ إذ أوجبت المحكمة على القاضي الاستعانة بالخبير في المسائل الفنية البحتة، التي لا يمكنه أن يقطع فيها برأي، دون استطلاع رأي أهل الخبرة، فإذا تصدى القاضي للمسألة الفنية وفصل فيها دون تحقيقها بواسطة خبير، كان حكمه معيباً مُستوجباً نقضه[٣].

الإجراءات التي تخضع لها الخبرة: وقد نظم قانون الإجراءات الجنائية المصري الإجراءات التي يخضع لها الخبراء أمام سلطات التحقيق والمحاكم الجنائية، حيث يكون للمحكمة أن تقرر ندب الخبير من تلقاء نفسها أو بناء على طلب الخصوم، ولها أن تنتدب خبيراً واحداً أو أكثر، وعلى المحكمة أن تحدد له مهمته في وضوح ودقة قدر ما تسمح بذلك ظروف الدعوى، ولسلطات التحقيق والاستدلال ندب الخبير كذلك[٤].

---

[١] د. محمود نجيب حسني: شرح قانون الإجراءات الجنائية، المرجع السابق، ص٨٤٧.

[٢] د. جميل الصغير: الحاسب الآلي كوسيلة لإثبات الجريمة، مرجع سابق، ص٢٠.

[٣] مجموعة أحكام محكمة النقض: نقض ١٩٨٣/١/٤، س٣٤، رقم (٥)، ص(٥٢).

[٤] د. محمود نجيب حسني: شرح قانون الإجراءات الجنائية، مرجع سابق،ص٨٥١.

ويتعين على الخبير أن يحلف أمام القاضي يميناً قبل أدائه مهمته بأن يبدي رأيه بالذمة (م٨٦ إجراءات جنائية مصري)، ويكون حلف اليمين في مرحلتي المحاكمة والتحقيق الابتدائي دون مرحلة الاستدلال (م٢٩ إجراءات جنائية مصري)، ويجوز للخبير أن يؤدي مهمته في غير حضور الخصوم (م٨٥ إجراءات جنائية مصري)، ويجوز للخبير أن يستعين في تكوين رأيه بشخص آخر إذا قدر ملاءمة ذلك[١]، ولا يشترط أن يحلف هذا الأخير يميناً، إذ هو يعمل تحت إشراف الخبير المنتدب ويندمج عمله في مهمته ويعتبر أحد عناصرها[٢].

ويجوز لكل من الخصوم رد الخبير إذا وجدت أسباب قوية تدعو لذلك (م٨٩ إجراءات جنائية مصري)، ويقدم الخبير تقريره كتابة، وللمحكمة من تلقاء نفسها أو بناء على طلب الخصوم أن تأمر بإعلان الخبراء ليقدموا إيضاحات بالجلسة عن التقارير المقدمة منهم في التحقيق الابتدائي أو أمام المحكمة (م٢٩٣ إجراءات جنائية مصري)، ولا يلتزم الخبير قبل إدلائه بأقواله أمام المحكمة بحلف اليمين، وتقرير الخبير هو مجرد آراء في شأن دليل إثبات، للقاضي السلطة في تقدير قيمة هذا التقرير وفقاً لمبدأ الاقتناع القضائي[٣].

والقاعدة في قانون الإجراءات الجنائية أن للمحكمة تعيين خبير أو أكثر كلما رأت ذلك، وقد يكون ندبها للخبراء من تلقاء نفسها أو بناء على طلب الخصوم، والمحكمة غير ملزمة بإجابة طلب ندب الخبير مادامت قد رأت عدم جدوى ذلك الإجراء إزاء وضوح الواقعة موضوع طلب الخبرة والذي استظهرته من التحقيقات

---

(١) انظر: نقض جنائي ١٩٦٢/١١/٢٦، مجموعة أحكام محكمة النقض، س١٣، ص٧٧٥، مشار إليه د. محمود نجيب حسني: شرح قانون الإجراءات، مرجع سابق،ص٨٥٢.

(٢) د. محمود نجيب حسني: المرجع السابق،ص٨٥٢.

(٣) الموضع السابق.

والأوراق[١].

غير أنه يلاحظ أن المحكمة إذا اعترضتها واقعة فنية وإن كان لها أن تتخذ ما تراه بشأنها من وسائل لبحثها وفهمها مستعينة في ذلك بالحقائق العلمية الثابتة، إلا أنه يجب أن يكون استناد المحكمة إلى تلك الحقائق مبيناً على أسس علمية سليمة ثابتة بمصادر المعرفة بالمسألة موضوع البحث ثبوتاً لا يحتمل تفسيراً أو تأويلاً[٢]. فيجوز للمحكمة أن تستند إلى آراء علمية بخصوص المسألة موضوع البحث وردت بمؤلف علمي لا تحتمل ألفاظه التأويل أو التفسير[٣].

والمحكمة تكون ملزمة بندب خبير في جميع المسائل الفنية البحتة[٤]. وإذا رأت المحكمة عدم إجابة الخصم إلى طلب ندب خبير في تلك المسائل فعليها أن ترد على ذلك في أسباب حكمها استنادا إلى مصدر علمي قاطع في المسألة الفنية، وإلا كان حكمها معيباً بالقصور وبالإخلال بحق الدفاع[٥]. أما إذا رأت المحكمة ندب خبير فلها أن تندب واحد أو أكثر من الخبراء على أن يقدموا تقاريرهم كتابة بعد حلف اليمين القانونية أمام المحكمة قبل مباشرتهم أعمال الخبرة[٦].

سلطة المحكمة في تقدير الخبرة: القاعدة أن المحكمة هي الخبير الأعلى، ولذلك فتقارير الخبراء تخضع دائماً لتقديرها، فلها أن تطرحها كلية، ولها أن تأخذ برأي

---

[١] نقض ١٣ مايو ١٩٦٨، مجموعة الأحكام س١٩، رقم ١٠٧، ١٧ يونيو ١٩٦٨، مجموعة الأحكام س١٩، رقم ١٤٧.

[٢] نقض ٢٢ مايو ١٩٦٧، مجموعة الأحكام س١٨، رقم ١٣٤.

[٣] نقض ١١ ديسمبر ١٩٦٧، مجموعة الأحكام س١٨، رقم ٢٦٥.

[٤] نقض ٢١ أكتوبر ١٩٦٨، س١٩، رقم ١٦٨.

[٥] نقض ٢١ أكتوبر ١٩٤٦، مجموعة القواعد جـ٢، ٦٧٥، رقم ١٩٠.

[٦] د. مأمون سلامة، المرجع السابق.

خبير دون الآخر، كما أن للمحكمة سلطة الجزم في المسائل التي تتسق ووقائع الدعوى حتى ولو كان تقرير الخبير لم يجزم فيها برأي[١]. وإذا اختلف خبيران في الرأي فليست المحكمة ملزمة بمواجهتهما، وإنما تملك ترجيح أحداهما على الآخر وفقاً لاقتناعها وما تراه مؤيداً بوقائع الدعوى[٢]، وهي في ذلك غير ملزمة ببيان أسباب الترجيح كما أنما غير ملزمة بمناقشة التقارير الأخرى طالما لم ترى محلا لها، ولم يطلب الخصوم منها شيئاً من ذلك.

وتقضي السلطة التقديرية للمحكمة أيضاً أنها تملك الأخذ ببعض ما ورد بتقرير الخبير، وتطرح الجزء الآخر دون إبداء أسباب لذلك، اللهم إلا في المسائل الفنية فلا يجوز تفنيدها إلا بأسانيد فنية[٣]، ومتى اقتنعت المحكمة بتقرير الخبير، ورأت الاستناد إليه في حكمها، فيجب أن يكون ما ورد بالتقرير قد طرح للمناقشة بالجلسة، وإن كانت تلاوة التقرير غير لازمة[٤]، وحينما يكون استناد المحكمة إلى رأي الخبير لا يجافي المنطق والقانون فإنها تكون غير ملزمة بإجابة الخصم إلى طلبه في تعيين خبير آخر أو في إعادة المهمة إلى ذات الخبير، كما لا تكون ملزمة بالرد على ذلك في أسباب حكمها[٥].

أهمية الخبرة في جرائم تقنية المعلومات:تكمن أهمية عمل خبراء الأدلة الجنائية الرقمية في تعاملهم مع المعلومات المخزنة على الأجهزة الإلكترونية، بما في ذلك أجهزة الحاسب الآلي والهواتف المحمولة، وهي ذات طابع معنوي متغير ومتقلب

---

[١] نقض ١٩٧٦/٦/٢٦، مجموعة الأحكام س٢٧، ١٣٢، ٥٩٦.

[٢] نقض ١٨ أكتوبر ١٩٤٩، مجموعة القواعد جـ١، ٥٣٩، رقم٣١.

[٣] نقض ٢٧ نوفمبر ١٩٦٧، مجموعة الأحكام س١٨، رقم ٢٥١.

[٤] نقض ٨ يناير ١٩٦٨، مجموعة الأحكام س١٩، رقم ٦.

[٥] نقض ٨ يونيو ١٩٣٦، مجموعة القواعد جـ١، ٥٤٢، رقم ٥١.

ويسهل تغييرها والعبث بها أثناء التحقيقات، ومن ثم يسعى خبراء الأدلة الجنائية الرقمية في إطار عملهم في التحقيق في جرائم تقنية المعلومات إلى جمع الأدلة الرقمية من مسرح الجريمة، من خلال إيجاد صورة لأدلة جنائية رقمية غير مضطربة، أو نسخ مطابقة تماماً لجهاز التخزين، تحتوي على نسخة من الجهاز الأصلي مفصلة بقدر الإمكان، والعمل على الصورة بدلاً من الجهاز الأصلي، حتى يتمكن المحققون من فحص البيانات دون إلحاق أي اضطراب بالنسخة الأصلية، وهو ما يوفر حماية ضد أي تلاعب أو تزوير.

ويشير الفقه الجنائي[١] إلى أهمية الخبرة في كشف وتحقيق جرائم تقنية المعلومات؛ إذ تستعين أجهزة العدالة الجنائية (الشرطة والنيابة والقضاء) بأصحاب الخبرة الفنية المُتميزة في مجال تكنولوجيا المعلومات بُغية كشف غموض هذه الجرائم، وتجميع أدلتها والتحفظ عليها، ومُساعدة المُحققين فيها،واستجلاء غموضها خاصة في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق، فهذه الطائفة من الجرائم تتعلق بمسائل فنية غاية في التعقيد، فضلاً عن التطور السريع والمُتلاحق في وسائل ارتكابها، وهو ما يتطلب وجود خُبراء على درجة عالية من التخصص والخبرة، فضلاً عن أن الاستعانة بالخبراء المُتخصصين يضمن الحفاظ على أدلة الجريمة الرقمية، والتي قد تتسبب أجهزة العدالة (الشرطة والنيابة) – بسبب قلة الخبرة في التعامل معها– إلى إضاعتها أو العبث بها، ويضيف البعض[٢] إلى ذلك ضرورة توافر الخبرة العملية إلى جانب الكفاءة العلمية التخصصية؛ إذ يشترط في الخبير في جرائم تقنية المعلومات ضرورة توافر خبرة في تحقيق هذه الجرائم، وبصفة خاصة في جرائم التلاعب في البيانات وتزوير المُستندات.

---

[١] المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٢١٢.

[٢] د. محمد أبو العلا عقيدة، التحقيق وجمع الأدلة، مرجع سابق، ص ص٥،٦.

ويبرز البعض[1] أهمية الخبرة في جرائم تقنية المعلومات بقوله أن جرائم الإنترنت والحاسب الآلي إثباتها يعد من المسائل الفنية الدقيقة التي يلزم ندب خبير فيها يبين المسائل الفنية وكيفية ارتكاب الجريمة، فضلاً عن جرائم نسخ وتقليد المصنفات وبرامج الحاسب الآلي والأقراص الصلبة التي يلزم فحصها من قبل أحد الخبراء لبيان عما إذا كانت مقلدة او منسوخة من عدمه، وجريمة التزوير في المحررات الإلكترونية وإتلافها أو محو الوسائط الإلكترونية لا بد فيها من الفحص الفني وفي جريمة تمرير المكالمات الدولية للخبرة فيها أهمية قصوى لبيان الخسائر التي لحقت من جراء اقترافها.

وقد تضمنت المادة (١٠) من القانون رقم (١٧٥) لسنة ٢٠١٨م المعنونة بـ"الخبراء"، النص على إنشاء سجلين: الأول لقيد الخبراء التقنيين العاملين بالجهاز القومي لتنظيم الاتصالات، والثاني للخبراء التقنيين من خارج الجهاز؛ إذ تقضي المادة المذكورة على أنه:"*يُنشأ بالجهاز سجلان لقيد الخبراء، يقيد بأولهما الفنيون والتقنيون عاملون بالجهاز، ويقيد بالآخر الخبراء من الفنيين والتقنيين من غير العاملين به. وتطبق على الخبراء في ممارسة عملهم وتحديد التزاماتهم وحقوقهم القواعد والأحكام الخاصة بقواعد تنظيم الخبرة أمام جهات القضاء. واستثناء من تلك القواعد، تسرى على الخبراء المقيدين بالسجل الثاني القواعد والأحكام الخاصة بالمساءلة الإدارية والتأديبية الواردة بالقانون المنظم لعملهم إن وجد.وتحدد اللائحة التنفيذية لهذا القانون قواعد وشروط وإجراءات القيد في كل من السجلين*".

وقد أشارت المادة (٦) من اللائحة التنفيذية للقانون الصادرة بقرار رئيس مجلس الوزراء رقم ١٦٩٩ لسنة ٢٠٢٠ إلى أنه:" يقوم الخبراء وفقًا للمادتين رقمي

[1] المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص ص٢١٣،٢١٢.

(١)، (١٠) من القانون بتنفيذ المهام الفنية والتقنية التي يتم تكليفهم بها من جهات التحقيق أو الجهات القضائية المختصة أو من الجهات المعنية بمكافحة جرائم تقنية المعلومات بشأن الجرائم موضوع هذا القانون".

قواعد قيد الخبراء في السجل الأول: حددت المادة ٤ من اللائحة التنفيذية قواعد قيد الخبراء بالسجل الأول للخبراء، حيث تنص المادة المشار إليها على أنه:"يُنشأ بالجهاز سجلان لقيد الخبراء، يقيد بأولهما الفنيون والتقنيون العاملون بالجهاز، ويقيد بالآخر الخبراء من الفنيين والتقنيين من غير العاملين به. ويتم القيد فى السجل الأول الخاص بالعاملين بالجهاز بناءً على القواعد والشروط والإجراءات الآتية:

١- أن يكون حاصلاً على مؤهل علمي أو فني أو تقنى يتناسب ومجال الخبرة.

٢- أن يكون قد أمضى عام على الأقل في عمله بالجهاز.

٣- أن يجتاز الاختبارات الفنية التي يجريها الجهاز للمتقدم".

قواعد قيد الخبراء في السجل الثاني: حددت المادة ٥ من اللائحة التنفيذية قواعد قيد الخبراء بالسجل الأول للخبراء، حيث تنص المادة المشار إليها على أنه:" يُقيد الخبراء من الفنيين والتقنيين من غير العاملين بالجهاز بالسجل الثاني للخبراء طبقًا للقواعد والشروط الآتية:

١- أن يكون مصريًا متمتعًا بالأهلية المدنية الكاملة. ويجوز قيد الأجنبي على أن يتعهد كتابة بخضوعه للقوانين المصرية.

٢- أن يكون محمود السيرة حسن السمعة.

٣- ألا يكون قد سبق الحكم عليه بحكم نهائي بالإدانة في جريمة مخلة بالشرف.

٤- أن يكون لديه سيرة ذاتية تتضمن خبرة عملية مناسبة.

٥- موافقة الجهات المعنية من جهات الأمن القومي على القيد بالسجل. ويترتب على تخلف أي شرط من الشروط السابقة الشطب من السجل بقرار من الجهاز".

وقد أشارت المادة (٧) من اللائحة التنفيذية إلى التزام الجهاز القومي لتنظيم الاتصالات بالحفاظ على سرية بيانات الخبراء، وعدم الإفصاح عنها، حيث نصت المادة المشار إليها إلى أنه:" يُراعى الجهاز الحفاظ على سرية البيانات الواردة بسجلات قيد الخبراء وعدم الإفصاح عنها إلا بموجب أمر قضائي".

التمييز بين خبراء الجهاز القومي لتنظيم الاتصالات وغيرهم من الخبراء: ميز المشرع المصري بين خبراء الجهاز القومي لتنظيم الاتصالات وغيرهم من الخبراء، حيث أشار إلى سريان القواعد والأحكام الخاصة بالمساءلة الإدارية والتأديبية الواردة بالقانون المنظم لعملهم إن وجد، وذلك اتساقاً مع القواعد العامة في هذا الشأن، وبالنظر إلى أن هؤلاء الخبراء قد ينظم عملهم ومساءلتهم إدارياً أو تأديبياً قوانين خاصة تنظم عملهم.

تقدير موقف المشرع المصري بشأن الخبراء: وحسناً فعل المشرع المصري باستحداث سجلين للخبراء الذين يمكن لجهات التحقيق والمحاكمة الاستعانة بهم في الجرائم المعلوماتية، حيث يجوز للمحكمة أن جهات التحقيق أن تندب أحد خبراء الجهاز القومي لتنظيم الاتصالات أو أحد خبراء المعلوماتية ممن مشهود لهم بالكفاءة والخبرة في هذا المجال المستحدث، وبما يواجه مشكلة عدم توافر العدد المناسب من الخبراء لدى الجهاز القومي لتنظيم الاتصالات في ضوء ضخامة الأعداد المتوقع نظرها من هذه القضايا أمام القضاء الجنائي.

إجراءات قيد الخبراء في السجلات: أشارت المـادة (٨) من اللائحة التنفيذية إلى إجراءات قيد الخبراء، حيث نصت المادة المشار إليها على أنه:"يتعين على من يرغب في قيد اسمه في السجل الثاني للخبراء أن يتقدم للرئيس التنفيذي للجهاز بطلب كتابي بذلك موضحًا فيه التخصص الذي يرغب العمل فيه كخبير، وأن يرفق بالطلب صور الشهادات والمستندات المؤيدة لطلبه. ويمكن للجهاز أن يطلب منه خلال ثلاثون يومًا من تاريخ تقديم الطلب معلومات إضافية قبل الفصل في الطلب، ويعتبر عدم الرد على الطلب لمدة ستين يومًا من تاريخ تقديمه رفضًا له. وفى حال رفض الجهاز الطلب، يحق للمتقدم التظلم بالإجراءات المقررة قانونًا".

قواعد تنظيم الخبرة أمام القضاء: تبرز الإشارة إلى أن قانون مكافحة جرائم تقنية المعلومات قد أشار إلى أنه تطبق على الخبراء في ممارسة عملهم وتحديد التزاماتهم وحقوقهم القواعد والأحكام الخاصة بقواعد تنظيم الخبرة أمام جهات القضاء، وهذه القواعد أوردها المرسوم بقانون رقم (٩٦) لسنة ١٩٥٢ بشأن تنظيم الخبرة أمام جهات القضاء، والذي تضمن قواعد اختيار وعمل وتأديب الخبراء المقيدون في جداول المحاكم وخبراء وزارة العدل ومصلحة الطب الشرعي والمصالح الأخرى التي يعهد إليها بأعمال الخبرة، وكل من ترى جهات القضاء عند الضرورة الاستعانة برأيهم الفني من غير من ذكروا، ومن ثم ينطبق هذا القانون على خبراء المعلوماتية الذين تنتدبهم المحكمة أو سلطات التحقيق لإبداء الرأي الفني في مثل هذه الجرائم.

موقف التشريعات المُقارنة: ومن التشريعات المُقارنة التي أوردت تنظيماً لأعمال الخبرة في الجرائم المعلوماتية القانون البلجيكي الصادر في ٢٠٠٠/١١/٢٣؛ إذ تضمن النص على جواز استعانة مأمور الضبط القضائي وقاضي التحقيق بخبير ليقدم المعلومات والأدلة التي تُعين المحقق في إثبات وقوع الجريمة، كما يجيز لسلطة

التحقيق أن تطلب من الخبير تشغيل النظام أو البحث فيه أو عمل نسخة من البيانات المطلوبة للتحقيق أو سحب البيانات المُخزنة أو المُحولة أو المنقولة[١]، ويشير البعض إلى أن مهمة الخبير في الجرائم المعلوماتية تقتصر على مهمة تشغيل النظام، وتقديم البيانات المطلوبة حسب الطريقة التي تريدها جهة التحقيق، فقد يُطلب من الخبير تقديم هذه البيانات مسجلة على قرص مُمغنط (ديسك أو سي دي) أو على ورق، ويكون هذا الحق في الاستعانة بالخبرة لقاضي التحقيق بصفة أصلية، ويجوز للنيابة العامة في حالة التلبس بالجريمة على سبيل الاستثناء، أو عند رضاء المُتهم بالتفتيش[٢].

طبيعة عمل الخبير في جرائم تقنية المعلومات:ثار تساؤل حول طبيعة التزام الخبير في الجرائم المعلوماتية، وهل هو التزام ببذل عناية أم بتحقيق نتيجة، وقد ذهب البعض[٣] إلى أن التزام الخبير يكون ببذل عناية، فلا يُسأل إذا لم يصل إلى النتيجة المطلوبة نتيجة ضعف خبرته أو بسبب العقبات التي واجهته أثناء مُباشرته لمُهمته، ويمكن أن تثور مسئوليته الجنائية إذا رفض القيام بالمُهمة المُكلف بها، أو أتلف عمداً البيانات المطلوب منه التعامل معها أو حفظها، هذا إلى جانب التزام الخبير بالمُحافظة على السر المهني، فإذا أفشى الخبير أية معلومة أو بيان مُتعلق بالجريمة المُكلف بالعمل فبها، فإنه يعاقب بالعقوبة المُقررة لهذه الجريمة.

---

(١) نصت المادة (٨٨) من قانون تحقيق الجنايات البلجيكي على أنه: "يجوز لقاضي التحقيق، وللشرطة القضائية أن يستعينا بخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام، وكيفية الدخول فيه، أو الدخول للبيانات المخزونة أو المعالجة أو المنقولة بواسطته، ويعطي القانون كذلك لسلطة للتحقيق أن تطلب من الخبير تشغيل النظام، أو البحث فيه، أو عمل نسخة من البيانات المطلوبة للتحقيق، أو سحب البيانات المخزنة أو المحولة أو المنقولة، على أن يتم ذلك بالطريقة التي تريدها جهة التحقيق".

(2) Meunier (c): art. Prec. P. 682-683.

(3) Meunier (c): art. Prec. P. 683-684.

ومن التشريعات العربية التي نصت على جواز استعانة أجهزة التحقيق والادعاء بأعمال الخبرة النظام السعودي، والذي نص على أن:"تتولى هيئة الاتصالات وتقنية المعلومات وفقا لاختصاصها تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة"(م١٤).

المطلب الثاني

حجية الدليل الرقمي في الإثبات الجنائي

تحتوي بيانات الحاسب الآلي والاتصالات الإلكترونية -التي يحتمل أن تكون ذات صلة بجرم ما- على العديد من الصور والفيديوهات ورسائل البريد الإلكتروني وسجلات المحادثات وبيانات النظام، ويواجه المحققون في سبيل جمع الأدلة الرقمية ذات الصلة بجرم ما بعض التحديات المتمثلة في كبر كم هذه البيانات، والتي يستغرق فحصها وقت طويل، فضلاً عن تباين أشكال الملفات المحتملة ونظام التشغيل والبرمجيات التطبيقية وتفاصيل الأجهزة، وهو ما قد يشكل تعقيدات عملية بشأن تحديد المعلومات ذات الصلة بالجريمة، ولا شك في أن هذه البيانات والمعلومات تشكل بنسبة كبيرة أدلة رقمية، إذا ما تم التعامل معها من جانب الخبراء التقنيون.

إلا أنه في إطار القانون الجنائي، فقد ثار التساؤل عما إذا كانت هذه الأدلة الرقمية المستحدثة تتمتع بالحجية القانونية ذاتها التي تتمتع بها الأدلة التقليدية في إثبات الجريمة على الرغم من الطبيعة المعنوية لهذه الأدلة والتي تختلف عن الأدلة التقليدية ذات الطبيعة المادية؟

وقد أجاب المشرع عن هذا التساؤل في قانون مكافحة جرائم تقنية المعلومات، من خلال إضفائه الحجية القانونية المقررة للدليل المادي التقليدي على الدليل الرقمي ذي الطابع المعنوي في الإثبات الجنائي، حينما قرر في المادة (١١)من القانون على

أنـه: "*يكـون للأدلـة المـستمدة أو المـستخرجة مـن الأجهـزة أو المعـدات أو الوسـائط أو الدعامات الإلكترونية أو من النظام المعلوماتي أو من برامج الحاسب، أو من أي وسيلة تقنيـة المعلومـات ذات قيمـة وحجيـة الأدلـة الجنائيـة الماديـة فـي الإثبـات الجنـائي متـى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية لهذا القانون*".

العلة من تقرير الحجية القانونية للدليل الرقمي: ترجع أهمية هذا النص فيما يقرره من قيمة ثبوتية وحجية قانونية في الإثبات الجنائي للدليل الرقمي كتلك المقررة للدليل التقليدي، وهو من الأهمية بمكان في مجال الإثبات الجنائي، بغية الاستفادة من هذه الطائفة من الأدلة في إثبات الجرائم ونسبتها إلى مرتكبيها، فمن المعلوم أن وثائق الحاسب الآلي ورسائل البريد الإلكتروني والرسائل النصية والفورية، والمعاملات، والصور وتواريخ الإنترنت هي أمثلة على المعلومات التي يمكن جمعها من الأجهزة الإلكترونية واستخدامها بشكل فعال جداً كدليل جنائي.

أهمية الدليل الرقمي في الإثبات الجنائي: ترجع أهمية الدليل الرقمي في مجال الإثبات الجنائي إلى ذيوع استخدام التكنولوجيا في مناحي الحياة بالشكل الذي أصبح فيه من غير المتصور وقوع جريمة سواء أكانت جريمة مستحدثة أم تقليدية دونما أن يتخلف عنها أدلة رقمية يمكن التوصل من خلالها إلى تحديد مرتكب الجريمة، وهو ما يتطلب ضرورة إجراء تغييرات جذرية في طرق جمع الأدلة وآليات التعاون الدولي في المسائل الجنائية تتناسب وطبيعة هذه النوعية المستحدثة من الأدلة الجنائية.

التعريف التشريعي للدليل الرقمي: عرف المشرع المصري الدليل الرقمي بأنه: "*أي معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها، ويمكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة*"، ويلاحظ أن

التعريف التشريعي حرص على إبراز جوهر الدليل الرقمي وهي المعلومات المستخرجة من الأجهزة التقنية سواء أكانت أجهزة الحاسب الآلي أو شبكات المعلومات وما في حكمها.

التعريف الفقهي للدليل الرقمي: اهتم الفقه بوضع تعريف للدليل الرقمي، حيث عرفه البعض[١] بأنه الدليل المأخوذ من أجهزة الكمبيوتر، ويكون فى شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا، ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء، وهو مكون رقمى لتقديم معلومات فى أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم، وذلك من أجل اعتماده أمام الجهات القضائية لاستعماله فى الإثبات.

بينما عرفها جانب آخر[٢] بأنه:" الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية، وأجهزة ومعدات وأدوات الحاسب الآلي، أو شبكات الاتصالات من خلال إجراءات قانونية وفنية، لتقديمها للقضاء بعد تحليلها علمياً أو تفسيرها في شكل نصوص مكتوبة، أو رسومات أو صور وأشكال وأصوات، لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها"، ويعرفها جانب ثالث[٣] بأنه:" معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي

---

(١) د. ممدوح عبد الحميد عبد المطلب: البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، القاهرة، ٢٠٠٦، ص٨٨

(٢) عبد الناصر محمد محمود فرغلي وآخر: الإثبات الجنائي، مرجع سابق، ص١٣.

(٣) د. محمد الأمين البشري: التحقيق في الجرائم المستحدثة، مطبوعات جامعة نايف العربية للعلوم الأمنية، الرياض، ط١، ٢٠٠٤، ص٢٣٤.

وملحقاتها وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جانٍ أو مجني عليه".

ويتضح لنا من التعاريف السابقة أنه بينما ركز التعريف التشريعي على جوهر الدليل ومضمونه، بينما نجد التعاريف الفقهية ركزت على عدة جوانب موضوعية وفنية وقانونية في تعريف الدليل الرقمي، وهو نهج محمود من جانب الفقه، حيث يحسب له تصديه لمسألة التعريف بالدليل الرقمي في وقت تأخر فيه المشرع المصري عن إصدار هذا القانون، ومن ثم تأخره في بيان ماهية وطبيعة هذه النوعية المستحدثة من الأدلة الجنائية وحجيتها القانونية.

والدليل الرقمي قد يكون من الوضوح حينما يتخذ صور معينة، مثل مطبوعات رسائل البريد الإلكتروني المتوفرة بسهولة التي يرسلها مرتكب الجريمة، أو سجلات اتصال بروتوكول الإنترنت التي يبلغ عنها مباشرة من قبل موفر خدمة الإنترنت، وقد يتطلب في أحوال أخرى استعمال تقنيات متطورة من أجل التوصل إليه عن طريق استخدام تقنيات أو أدوات لاستعادة الآثار أو البيانات التي يتم الحصول عليها من الحاسب الآلي والنظم المعلوماتية والشبكات والتي من شأنها أن تقدم أدلة على وقوع جرم ما، ومن ثم يأتي دور خبراء وتقنيات الأدلة الجنائية الرقمية في استعادة وتحليل المواد التي تم الحصول عليها من أجهزة الحاسب والشبكات والنظم المعلوماتية، والاستفادة من قابلية الحواسب لتخزين وتسجيل وحفظ البيانات عن أغلب أنشطة مستخدموها، في جمع وتعقب الآثار الرقمية[1].

[1] انظر: دراسة مكتب الأمم المتحدة، مرجع سابق، ص٢٣٠.

الأثر الرقمي والدليل الرقمي:يقصد بالأثر الرقمي كل ما ينتج عن تفاعل المستخدم مع وسائل تقنية المعلومات وأجهزة الحاسب الآلي، حيث ينتج عن هذا التفاعل مجموعة كبيرة من الآثار الرقمية (يطلق عليها أحياناً البصمات الرقمية أو الأشياء الاصطناعية)، إلا أن هذا الأثر يتحول إلى دليل رقمي إذا نجح الخبراء التقنيون باستخدام الأجهزة والتطبيقات التكنولوجية الخاصة في الربط بينه وبين الجريمة المرتكبة، ومن ثم إثبات الصلة بينه وبين مرتكب الجريمة، ويذهب جانب من الفقه الجنائي[١] إلى وجوب التزام مأمورو الضبط القضائي أو الخبراء بالضمانات التي توفر الثقة في الأدلة المادية، بمعنى الالتزام بالشرعية في كل إجراء يتخذه أو كل خطوة يخطوها، وإلا كان البطلان للإجراء، وعدم الأخذ بالدليل المستمد من ذلك الإجراء الباطل[٢].

الشروط الواجب توافرها لتقرير حجية الدليل الرقمي: وقد حددت المادة (٩) من اللائحة التنفيذية للقانون الجوانب والشروط الفنية بشأن التعامل مع هذه النوعية من الأدلة الجنائية، حيث تقضي المادة المشار إليها بأنه:"تحوز الأدلة الرقمية ذات القيمة والحجية للأدلة الجنائية المادية في الإثبات الجنائي إذا توافرت فيها الشروط والضوابط الآتية:

١- أن تتم عملية جمع أو الحصول أو استخراج أو استنباط الأدلة الرقمية محل الواقعة باستخدام التقنيات التي تضمن عدم تغيير أو تحديث أو محو أو تحريف للكتابة أو البيانات والمعلومات، أو أي تغيير أو تحديث أو إتلاف للأجهزة أو المعدات أو

---

[١] د. أحمد فتحي سرور: الوسيط في قانون الإجراءات الجنائية، طبعة مطبعة جامعة القاهرة، ١٩٧٩، ج١، ص٣٧٥.

[٢] د. حسين إبراهيم: الإثبات الجنائي، مطبعة كلية الشرطة، القاهرة، ٢٠٠٢، ص٢١.

البيانات والمعلومات، أو أنظمة المعلومات أو البرامج أو الدعامات الالكترونية وغيرها. ومنها على الأخص تقنيةDigital Images Hash، Write Blocker، وغيرها من التقنيات المماثلة.

٢- أن تكون الأدلة الرقمية ذات صلة بالواقعة وفى إطار الموضوع المطلوب إثباته أو نفيه وفقًا لنطاق قرار جهة التحقيق أو المحكمة المختصة.

٣- أن يتم جمع الدليل الرقمي واستخراجه وحفظه وتحريزه بمعرفة مأموري الضبط القضائي المخول لهم التعامل في هذه النوعية من الأدلة، أو الخبراء أو المتخصصين المنتدبين من جهات التحقيق أو المحاكمة، على أن يبين فى محاضر الضبط، أو التقارير الفنية على نوع ومواصفات البرامج والأدوات والأجهزة والمعدات التي تم استخدامها، مع توثيق كود وخوارزم Hash الناتج عن استخراج نسخ مماثلة ومطابقة للأصل من الدليل الرقمي بمحضر الضبط أو تقرير الفحص الفني، مع ضمان استمرار الحفاظ على الأصل دون عبث به.

٤- فى حالة تعذر فحص نسخة الدليل الرقمي وعدم إمكانية التحفظ على الأجهزة محل الفحص لأي سبب يتم فحص الأصل ويثبت ذلك كله فى محضر الضبط أو تقرير الفحص والتحليل.

٥- أن يتم توثيق الأدلة الرقمية بمحضر إجراءات من قبل المختص قبل عمليات الفحص والتحليل له وكذا توثيق مكان ضبطه ومكان حفظه ومكان التعامل معه ومواصفاته".

توثيق الدليل الرقمي: حددت المادة (١٠) من اللائحة التنفيذية للقانون كيفية توثيق الدليل الرقمي، حيث نصت المادة المشار إليها على أنه:" يتم توصيف وتوثيق الدليل الرقمي من خلال طباعة نسخ من الملفات المخزن عليها أو تصويرها بأي

وسيلة مرئية أو رقمية، واعتمادها من الأشخاص القائمين على جمع أو استخراج أو الحصول أو التحليل للأدلة الرقمية، مع تدوين البيانات التالية على كل منها:

١ ـ تاريخ ووقت الطباعة والتصوير.

٢ ـ اسم وتوقيع الشخص الذى قام بالطباعة والتصوير.

٣ ـ اسم أو نوع نظام التشغيل ورقم الإصدار الخاص به.

٤ ـ اسم البرنامج ونوع الإصدار أو الأوامر المستعملة لإعداد النسخ.

٥ ـ البيانات والمعلومات الخاصة بمحتوى الدليل المضبوط.

٦ ـ بيانات الأجهزة والمعدات والبرامج والأدوات المستخدمة".

أدوات توثيق الدليل الرقمي: يستعين خبراء الأدلة الجنائية الرقمية ـفي إطار عملهم التقنيـ بأدوات أو برمجيات أو أجهزة تقنية تساعد على إيجاد صورة للدليل الرقمي، من أبرز هذه الأجهزة جهاز مانع الكتابة والذي من شأنه منع إلحاق أي تغييرات على البيانات الأصلية[١]، وبرامج "نحت البيانات أو الملفات" والتي من شأنها استعادة الملفات المحذوفة أو التالفة من بقايا البيانات الأولية التي تبقى على أجهزة التخزين حتى بعد زوال الملف الأصلي[٢]، والعمل على إيجاد نسخة "خطوة بخطوة" للمعلومات المخزنة. وفي بعض الأحيان يستعين خبراء الأدلة الجنائية الرقمية بأدوات تحليل تجزئات التشفير للتعامل مع الملفات المشفرة؛ إذ أن أي تغيير بسيط للبيانات، ينتج عنه حدوث تشفير مختلف.

---

[١] انظر: المعهد الأمريكي الوطني للمعايير والتكنولوجيا، ٢٠٠٤، جهاز مانع الكتابة (HWB) مواصفات، الإصدار 2.0، مشار إليه دراسة مكتب الأمم المتحدة، مرجع سابق، ص٢٣١.

[٢] انظر: غوتمان بي: الحذف الآمن للبيانات من الذاكرة المغنطيسية وذاكرة الحالة الصلبة، وقائع الندوة الأمنية السادسة لاتحاد الحوسبة التقنية المتقدمة، ١٩٩٦، مشار إليه دراسة مكتب الأمم المتحدة، الموضع السابق.

ومن الجدير بالذكر أن الأجهزة والبرمجيات والأدوات التقنية المستخدمة من قبل الخبراء لجمع الأدلة الرقمية تختلف بحسب نوعية الوسائط التقنية المستخدمة، كما أنها تتطلب تقنيات مختلفة لتحقيق هذه الأدلة الرقمية، فأجهزة المحمول تختلف أدوات فحصها عن تلك المستخدمة في فحص جهاز حاسب مكتبي أو خادم شبكة، فقد تشتمل عملية جمع الأدلة الرقمية على إجراء فحص وتحليل الأجهزة الإلكترونية وأجهزة الحاسب المكتبي والمحمول الكائنة في المنازل وأماكن العمل، والتي عادةً ما تحتوي على أقراص صلبة ذات سعة كبيرة من شأنها تخزين كمية كبيرة من المعلومات، بما في ذلك الصور ومقاطع الفيديو، فضلاً عن تواريخ تصفح المواقع الإلكترونية، ورسائل البريد الإلكتروني ومعلومات التراسل الفوري، والتي عادةً ما تقوم بتشغيل عدد صغير من أنظمة لتشغيل كالويندوز والماك أو أس ولينوكس، بينما تشمل عملية فحص أجهزة المحمول أجهزة محمولة صغيرة الحجم تعمل بطاقة منخفضة، وذات سعة تخزين أقل، وببرامج أبسط لتسهيل المكالمات الهاتفية وتصفح الإنترنت[١].

وتبرز الإشارة إلى أن أجهزة المحمول والأجهزة اللوحية -والتي غالباً ما تكون بمثابة نسخ مطورة من أجهزة المحمول- قد تشكل بالنسبة للمحققين كنزاً هائلاً من المعلومات ذات الصلة بارتكاب الجرائم، بالنظر لما تتسم به من سمات مميزة، أبرزها: قابليتها على التنقل، ووجودها بصحبة مالكها في كل الأوقات، واتصالها المستمر بشبكات الاتصالات، مما يساعد على الحصول على مراقبة دقيقة للموقع الجغرافي إلى حد معقول، علاوة على ما تحتويه من قائمة جهات الاتصال وسجلات المكالمات، فضلاً عن تدفق جميع المعلومات والبيانات عبر شبكات مقدمي خدمات الإنترنت المحمول[٢].

---

[١] انظر: دراسة مكتب الأمم المتحدة، مرجع سابق، ص٢٣٢.

[٢] الموضع السابق.

كما تحظى تقنيات الأدلة الجنائية الخاصة بالشبكات المعلوماتية بأهمية كبيرة، من خلال ارتباطها بالهواتف المحمولة وأجهزة الحاسب الآلي، واستخدامها في خدمات الإنترنت والتخزين السحابي، حيث يتم تخزين البيانات على الإنترنت من خلال مراكز بيانات، بدلاً من تخزينها على جهاز المستخدم، الأمر الذي يدعو إلى استخدام نظم لتحليل المعلومات على هذه الشبكات للتوصل إلى كمية من المعلومات التي يمكن تجميعها، ويتعين للحصول على معلومات مفصلة بخصوص الأنشطة التي تجرى في الشبكة وتخزينها، أن يكون جمع البيانات بصورة نشطة وتخزينها للتحليل لاحقاً، ويمكن أن تشمل هذه العملية تحليلاً لملفات السجلات من أجهزة الشبكة مثل جدران الحماية وكشف التسلل، فضلاً عن نظم الوقاية، وكذلك تحليل محتوى نقل بيانات الشبكة المسجلة في حال توفرها[١].

غني عن البيان أنه في الحالات التي يتمكن فيها الجاني من الدخول غير المشروع والتسلل لأحد نظم الحاسب، فإن البيانات الموجودة على هذا الحاسب تصبح معرضة للخطر من طرف المهاجم، ولا يعتد بملفات السجلات لنشاط هذا النظام، ومن ثم لا تمثل التحقيقات الجنائية للشبكة الصيغة الوحيدة المتاحة لأي محلل؛ إذ يكمن التحدي الأساسي في هذه الحالة في إعادة القيام بالإجراءات التي اتخذت على أي شبكة من بيانات السجلات المحدودة المتاحة، واستخدام ذلك في تحديد محاولات التسلل والدخول غير المشروع للنظم المعلوماتية ومحاولات قطع الخدمة، إضافة إلى البيانات الخاصة بأي الموارد التي وصل إليها الأفراد في أي وقت[٢].

---

(1) Chappell, L., 2012. Wireshark Network Analysis (Second Edition): The Official Wireshark Certified Network AnalystStudy Guide. Laura Chappell University.

(٢) انظر: دراسة مكتب الأمم المتحدة، مرجع سابق، ص٢٣٣.

خصائص الدليل الرقمي: يتسم الدليل الرقمي بعدد من الخصائص التي تميزه على الدليل الجنائي التقليدي، وفيما يلي نتناول هذه الخصائص على النحو التالي:-

أ): الطبيعة المعنوية للدليل الرقمي: يتكون الدليل الرقمي من بيانات ومعلومات ذات هيئة إلكترونية غير ملموسة، لا تدرك بالحواس العادية، بل يتطلب إدراكها الاستعانة بأجهزة ومعدات وأدوات الحاسبات الآلية HARDWARE، واستخدام نظم برامجية حاسوبية SOFTWARE[١].

ب): الطابع الافتراضي للدليل الرقمي: فالأدلة الرقمية ليست أقل مادية من الدليل المادي فحسب، بل تصل إلى درجة التخيلية في شكلها وحجمها ومكان تواجدها غير المعلن، فالدليل الرقمي يشمل كافة أشكال وأنواع البيانات الرقمية الممكن تداولها، بحيث يكون بينها وبين الجريمة رابطة من نوع ما، وتتصل بالضحية على النحو الذي يحقق هذه الرابطة بينها وبين الجاني[٢].

ج): إمكانية نسخ الدليل الرقمي بشكل مطابق: يمكن استخراج نسخ من الأدلة الرقمية مطابقة للأصل ولها ذات القيمة العلمية والحجية الثبوتية، وهذا الأمر لا يتوافر في الأدلة التقليدية، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد والتلف والتغيير، عن طريق نسخ طبق الأصل من الدليل[٣].

د): صعوبة التخلص من الدليل الرقمي: إن الأدلة الرقمية يمكن استرجاعها بعد محوها، وإصلاحها بعد إتلافها، وإظهارها بعد إخفائها، مما يؤدي إلى صعوبة الخلاص منها، وهي خصيصة من أهم خصائص الدليل الرقمي، بالمقارنة بالدليل

---

[١] عبد الناصر محمد محمود فرغلي وآخر: الإثبات الجنائي، مرجع سابق، ص١٤.

[٢] د. عمر محمد بن يونس: مذكرات في الإثبات الجنائي عبر الإنترنت، مرجع سابق، ص١٤.

[٣] عبد الناصر محمد محمود فرغلي وآخر: الإثبات الجنائي، مرجع سابق، ص١٥.

التقليدي، ويتم ذلك من خلال استخدام العديد من البرامج الحاسوبية التي وظيفتها استعادة البيانات التي تم حذفها أو إلغائها، سواء تم ذلك عن طريق حذف البيانات أو المعلومات، أو تم عمل إعادة تهيئة أو تشكيل للقرص الصلب، مما يعني صعوبة إخفاء الجاني لجريمته عن أعين رجال العدالة الجنائية[١].

هـ): الطابع الديناميكي للدليل الرقمي: الأدلة الرقمية ذات طابع ديناميكي فائق السرعة، تنتقل من مكان لآخر عبر شبكات الاتصال متعدية لحدود الزمان والمكان[٢].

و): الدليل الرقمي يكشف عن شخصية المجرم: يمكن من خلال الدليل الرقمي رصد المعلومات عن الجاني وتحليلها في ذات الوقت، كما يمكن للدليل الرقمي تسجيل تحركات الفرد وعاداته وسلوكياته وبعض الأمور الشخصية عنه[٣].

أوجه التمييز بين الدليل التقليدي والدليل الرقمي: يتسم الدليل الرقمي بعدد من السمات التي تميزه عن غيره من الأدلة التقليدية، ومن أبرزها أنه سريع الزوال والتغيير، وهو ما يثير إشكالية حفظ الدليل والحصول عليه، علاوة على صعوبة الوصول إليه حينما يستخدم المشتبه فيهم نظاماً للتشفير[٤]، مما يجعل الحصول عليه

---

(١) الموضع السابق.

(٢) الموضع السابق.

(٣) د. ممدوح عبد الحميد عبد المطلب: استخدام بروتوكول TCP IP في بحث وتحقيق الجرائم على الكمبيوتر، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية الذي نظمه، مركز البحوث والدراسات بأكاديمية شرطة دبي، خلال الفترة (٢٦-٢٠٠٣/٤/٢٨)، إمارة دبي، دولة الإمارات العربية المتحدة، ص ص٦٤٩، ٦٥٠.

(٤) عرفت المادة الأولى من اللائحة التنفيذية للقانون رقم (١٧٥) لسنة ٢٠١٨ كلاً من التشفير ومفتاح التشفير، بأن التشفيرEncryption: منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونيًا بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة، بينما مفتاح التشفيرEncryption Key: أرقام أو رموز أو حروف ذات طول محدد تستخدم في عمليات =

بدون رمز التشفير أمراً صعباً ويستغرق وقتاً طويلاً، فضلاً عن وجوده في أماكن جغرافية متعددة، ومن ثم صعوبة الحصول عليه خارج نطاق الولاية القضائية للدول، بالإضافة إلى العديد من الاشكاليات التي تخص مدى مقبوليته أمام القضاء الجنائي. وتتبلور أبرز ملامح التمييز بين كل من الدليلين، فيما يلي:-

١- الدليل التقليدي دعامته ورق ملموس، بعكس الدليل الرقمي، فإن دعامته برامج الحاسب الآلي، أو أي وسائط تقنية حديثة، ومن ثم يحتاج الدليل الرقمي إلي وسائط تقنية لقراءته، بينما يمكن قراءة الدليل المادي بسهولة ومباشرة من دعامته الورقية.

٢- الدليل الرقمي يسهل البحث عنه وإدارته، والتعديل فيه، وتخزينه واسترجاعه، وتبويبه، باستعمال بعض خصائص البرمجة الإلكترونية، بعكس الدليل المادي الذي يثبت علي حاله التي أعد بها.

٣- الدليل الرقمي ووفقاً لدعامته الإلكترونية التي تستوعب معلومات كبيرة تبعاً لحجم الوسيط ومقدار المعلومة، فإن ذلك يتيح الفرصة لعرض عدد غير محدود من المستندات، في مساحة صغيرة من الوسيط الإلكتروني.

تقسيمات الدليل الرقمي: تتباين صور الدليل الرقمي، وقد قسمها البعض[1] إلى ثلاثة أقسام رئيسية: (الأول) أدلة رقمية تخص أجهزة الحاسب الآلي وشبكاتها،

=

التشفير وفك التشفير. ويستخدم نفس المفتاح في التشفير وفك التشفير ويسمى التشفير المتماثل، ويجب الحفاظ على سرية المفتاح. ويستخدم زوج من المفاتيح مترابطين بعلاقة رياضية بحيث يستخدم أحدهما في التشفير والآخر في فك التشفير ويسمى التشفير غير المتماثل، ويجب الحفاظ على سرية أحد المفاتيح بينما يعلن عن الآخر بشروط ومعايير محددة.

[1] د. ممدوح عبد الحميد عبد المطلب: البحث والتحقيق الجنائي الرقمي، مرجع سابق، ص٨٨.

و(الثاني) أدلة رقمية تخص شبكة المعلومات الدولية "الإنترنت"، و(الثالث) أدلة رقمية تخص بروتوكولات تبادل المعلومات بين أجهزة شبكة الإنترنت.

بينما يشير البعض الآخر إلى تقسيم ثانٍ قررته وزارة العدل الأمريكية سنة ٢٠٠٢، إلى ثلاث مجموعات، تشمل[١]: (الأولى) السجلات المحفوظة في الحاسب الآلي، كالوثائق المكتوبة والمحفوظة مثل رسائل البريد الإلكتروني وملفات النصوص المكتوبة كالوورد ورسائل غرف المحادثات عبر الإنترنت، و(الثانية)السجلات التي تم إنشاؤها بواسطة الحاسب الآلي، وتعتبر مخرجات برامج الحاسب الآلي التي لم يتدخل فيها الإنسان، كسجلات الهاتف وفواتير السحب الآلي ATM، و(الثالثة) السجلات التي جزء منها تم حفظه بالإدخال والجزء الآخر تم إنشاؤها بواسطة الحاسب الآلي، ومن أمثلتها أوراق العمل المالية التي تحتوي على مدخلات تم معالجتها من خلال برامج أوراق العمل مثل EXCEL بإجراء العمليات الحسابية عليها.

ومن ثم يفترض التنوع في صور الدليل الرقمي، تنوع وتعدد وسائل التحصل عليه من أجهزة الحاسب الآلي والشبكات المعلوماتية، ومن ثم يرى البعض أن مسألة استخلاص الدليل الرقمي من مخرجات الحاسب الآلي والشبكات المعلوماتية أن الدليل المستمد منها يظل رقمياً، حتى وإن اتخذ هيئة أخرى، ويكون اعتراف القانون بهذه الهيئة الأخرى مؤسساً على طابع افتراضي مبناه أهمية الدليل الرقمي ذاته وضرورته في عملية الإثبات الجنائي في جرائم تقنية المعلومات، ومن ثم يلزم اتخاذ مسلك الافتراض من حيث اعتباره دليلاً أصلياً[٢].

---

[١] عبد الناصر محمد محمود فرغلي وآخر: الإثبات الجنائي، مرجع سابق، ص١٤.

[٢] د. عمر محمد بن يونس: مذكرات في الإثبات الجنائي عبر الإنترنت، مرجع سابق، ص١٢.

القواعد الواجب مُراعاتها في إثبات الأدلة الرقمية: يتسم الدليل الرقمي بطبيعة خاصة، وهي قابليته للتعديل، ومن ثم فإن هذا الدليل غالباً ما يتسم بطبيعة مُتقلبة[١]، وهو ما يتطلب سرعة التحقيق في جرائم تقنية المعلومات، واتخاذ الإجراءات القانونية اللازمة لضبط وتفتيش أو التحفظ على هذه الأدلة الرقمية، ولذلك ترتكز خطة التحقيق في هذه الفئة من الجرائم على عدة عوامل من أبرزها:-

١) فحص طبيعة بيئة المعالجة الآلية للبيانات التي سيمارس المحقق في إطارها عمله وتحديد نوعية وكيفية تعامله معها وتأثيرها في طبيعة ونطاق إجراءاته وتوقيتها.

٢) حصر المواقع والأماكن الحساسة بمبنى معالجة أو نقل البيانات كمكتبة الوثائق وأماكن تخزين الأشرطة والأقراص الممغنطة، وتحديد المسئولين عن أمنها.

٣) الوقوف على قواعد تشغيل نظام الحاسب، وكيفية تنظيم دورة المعالجة الإلكترونية للبيانات ومدى مركزية المهام والمعرفة في هذا الصدد.

٤) تحديد أساليب التدقيق والمعالجة وغيرها من العمليات الممكن إجرائها بمساعدة الجهة المجني عليها، وتلك التي يلزم إجراءها عن طريق حاسب آخر غيره.

٥) مراعاة أمن المعلومات التي قد يستلزم التحقيق الحصول عليها من نظام المعالجة الإلكترونية للبيانات يمكن أن تكون متاحة فقط لفترة زمنية محدودة داخل دائرة معالجة البيانات، ويقتضي ذلك أن يبادر المحقق بتقييم البيانات التي يتطلبها التحقيق والحصول عليها فوراً لتخزينها في دعائم مأمونة.

---

[١] كينجي ميانيشي: شبكة الربط بين النقاط المرجعية الوطنية، المؤتمر الدولي السادس للجرائم المعلوماتية،١٣-١٥/٤/٢٠٠٥، إصدار مركز بحوث الشرطة، القاهرة، ص ص٩٥-٩٨.

٦) فحص الاحتمالات المختلفة لنمط الدعامة أو الوعاء المتبقي استخدامه للحصول على الدليل وصيانته (ورق، ميكروفيش، أوعية أو وسائط ممغنطة).

٧) إعداد قائمة بالأشخاص المتعين سؤالهم، وتحديد النقاط التي يجب استيضاحهم بشأنها[١].

مشروعية الدليل الرقمي: يستلزم الدليل الرقمي أن تكون وسيلة التحصل عليه كانت مشروعة، وهو ما يتحقق من خلال ما يلي:-

١) إجراءات التحصل على الدليل تمت وفق القانون: أي ضرورة ارتكان الدليل على إجراءات مشروعة، سواء أكانت تلك الإجراءات قد صدرت من قبل القاضي بصورة مباشرة أو غير مباشرة، أو من قبل المتهم واعترافه واستجوابه، أو من قبل الغير بعد القيام بالقبض عليه أو تفتيشه أو تفتيش مسكنه أو ممارسة أي عمل من أعمال الخبرة الفنية.

٢) التوصل إلى الدليل عن طريق إرادة حرة: بمعنى الحصول عليه قد تم دون أي اعتداء على إرادة المتهم أو إرادة الغير، بحيث يكون طريقة العثور عليه خالية من أي عيب تشوب تلك الإرادة.

ومن التطبيقات القضائية حول مشروعية إجراءات التحصل على الدليل ما قررت إحدى المحاكم الأمريكية بشأن مشروعية قيام أجهزة إنفاذ القانون بجمع معلومات بشأن وقوع جريمة ما من بين المعلومات والبيانات التي يتشاركها المتهم مع أصدقائه على مواقع التواصل الاجتماعي، حيث دفع المتهم ببطلان الدليل الذي تم الحصول عليه من حسابه الشخصي على فيسبوك على سند من القول إن أجهزة

[١] د. هشام محمد فريد رستم، المرجع السابق، ص٣٤ وما بعدها.

الشرطة قد انتهكت حقوقه المنصوص عليها في التعديل الرابع على الدستور الأمريكي، وكان المتهم قد قام بضبط إعدادات الخصوصية الخاصة بحسابه الشخص على موقع التواصل الاجتماعي (فيسبوك) بصورة يمكن معها "للأصدقاء" فقط رؤية ما يقوم بإرساله على حسابه من مراسلات.

وتمكنت أجهزة الشرطة من الحصول على دليل يجرم المتهم من خلال أحد الأشخاص (الشهود)، وقد صادف أن يكون هذا الشاهد أحد" أصدقاء" المتهم على موقع التواصل الاجتماعي، وقد رفضت المحكمة الدفع وقضت بأنه:" إذا كانت إعدادات الضبط المتعلقة بالخصوصية على موقع التواصل الاجتماعي (فيسبوك) تسمح برؤية المراسلات من قبل" الأصدقاء"، فتستطيع أجهزة الدولة الولوج إلى هذه المعلومات من خلال تعاون أحد الأشخاص من "أصدقاء" المتهم على موقع التواصل الاجتماعي دون أن يُشكّل ذلك انتهاكًا للتعديل الرابع. بينما يعتقد المتهم -بدون أدنى شك- أن حسابه لن تتم مشاركته من قبل سلطات إنفاذ القانون، ليس هناك أي مبرر للتوقع بأن" الأصدقاء" سيحافظون على سرية الحساب. وكلما اتسعت دائرة "الأصدقاء"، زاد الاحتمال بأن مراسلات المتّهم ستتم رؤيتها من قبل شخص غير متوقع أن يراها. توقعات المتهم المشروعة في الحفاظ على خصوصيته تنتهى عندما ينشر مراسلاته إلى "أصدقائه"؛ لأن هؤلاء "الأصدقاء" يملكون الحرية في استخدام هذه المعلومات كيفما يشاؤون بما في ذلك مشاركة هذه المعلومات مع أجهزة الدولة"[1].

---

[1] انظر: حكم صادر من محكمة المقاطعة الجنوبية بنيويورك بالولايات المتحدة الأمريكية بتاريخ ١٠ من أغسطس عام ٢٠١٢ في قضية:

United States v. Meregildo, No. 11 Cr. 576(WHP), 2012 WL 3264501, at *2 (S.D.N.Y. Aug. 10, 2012)..

بينما في قضية أخرى، قضت محكمة النقض الفرنسية في حكم لها أن: "التسجيل الهاتفي الذي يجريه أحد الأطراف بدون علم صاحب الأقوال المسجلة يشكل طريقة غير مشروعة تؤدي إلى عدم قبوله برهاناً، وقد نقضت بذلك حكم محكمة الاستئناف بباريس الذي أخذ بالتسجيل"[١].

مقبولية الدليل الرقمي أمام القضاء الجنائي: سبق أن أشرنا إلى أن الدليل الرقمي هو أية مادة تتخذ الشكل الإلكتروني أو الرقمي، ونظراً للخصائص التي يتمتع بها الدليل الرقمي والتي من أبرزها الطابع المعنوي المتغير لهذه الدليل وقابليته للتغير والتعديل، وأهميته في الإثبات الجنائي والارتكان عليه في تقرير المسئولية الجنائية للأشخاص وإدانتهم بناءً على هذه الأدلة، فقد اتجه القضاء الجنائي في بعض الدول إلى وضع بعض القواعد أو المعايير لتقدير مدى قبول الأدلة الرقمية والتأكد من موثوقيتها وبحث مدى إمكان الإرتكان عليها في الإجراءات القضائية، وتتبلور أبرز القواعد لتقرير مقبولية الدليل الرقمي أمام القضاء الجنائي في ضرورة تيقن المحكمة من سلامة الدليل الرقمي وصحته وعدم تعرضه لأي محاولة للعبث به، ومن ثم يقع على

---

[١] ذهبت محكمة النقض الفرنسية (الغرفة التجارية) إلى أن تسجيل مكالمة هاتفية من قبل أحد الأطراف دون علم صاحب الأقوال يشكل وسيلة ماكرة، مما يمنع قبول تقديمه كدليل، حيث بنت محكمة النقض حكمها بنقض حكم محكمة استئناف باريس الصادر في ٢٠٠٧/٦/١٩ على مخالفة ذلك لأحكام الفقرة الأولى من المادة السادسة من الاتفاقية الأوروبية لحقوق الإنسان وحرياته الأساسية، وكانت محكمة الاستئناف بباريس قد قررت أن تسجيلات المكالمات الهاتفية المقدمة من الطرف الرافع للدعوى وليس من المحققين أو من المقرر، لا يمكن رفضها بمجرد علة الحصول عليها بصورة ماكرة، وبأنها تعتبر مقبولة متى خضعت للمناقضة، حيث يعود للمحكمة تقدير قيمتها الثبوتية. انظر:

Cass. Com. 3 Juin 2008, No. 07-1714707-17196, bull. 4, 2008,no.112.

قارن كذلك: حكم محكمة النقض الفرنسية (الدائرة الجنائية)

Cass. Crim. 31 Jan 2007, No. 383-82-06, bull. Crim., 2007,no.27.

عاتق سلطة الاتهام إثبات أن هذا الدليل بداءةً قد تم التحصل عليه بطريق مشروع، وثانياً إثبات ما يسمى باستمرارية الدليل؛ أي أن حالة المعلومات الرقمية كدليل لم يطرأ عليها أي تعديل أو تغيير يشكك من مصداقيتها في كشف وقائع الجريمة طوال فترة الإجراءات القضائية منذ تاريخ التحفظ عليه وحتى صدور حكم في الدعوى.

وتمثل إمكانية تعديل الأشياء الاصطناعية الخاصة بالحاسب أو الكتابة فوقها أو حذفها بسهولة تحدياً يتعلق بمصداقية هذا الدليل أمام المحكمة ووجوب التحقق من مصادر المعلومات الرقمية، ومن ثم تتطلب عملية جمع الآثار الرقمية بمسرح جريمة تقنية المعلومات خبراء متخصصين في مجال المعلوماتية، وهم من يناط بهم استخلاص وجمع الأدلة الرقمية من أجهزة الحاسب الآلي والنظم المعلوماتية والشبكات المعلوماتية ومن وسائل تقنية المعلومات المختلفة، ويقع على عاتقهم مهمة جمع الدليل وحفظه بالصورة التي عليها، وبما يمنع أي محاولة للعبث به أو تعديله أو تغييره.

ويجب على القائمين على جمع الأدلة الرقمية من مسرح الجريمة اتخاذ الإجراءات اللازمة للحفاظ على سلامة الدليل الرقمي بدءاً من لحظة إنشائه ووصولاً لمرحلة تقديمه أمام المحكمة، وهو ما يعرف باستمرارية الدليل وثبات حالته وعدم تعرضه للتعديل أو التحريف أو العبث به، حيث يجب عليهم الحفاظ على استمرارية الأدلة على كل من الأجهزة المادية التي تحتوي على البيانات (عند تلقيها أو الاستيلاء عليها)، والبيانات المخزنة الموجودة على الأجهزة[1].

---

[1] انظر: الأدلة الرقمية الموجودة في حجرة المحكمة، دليل لإنفاذ القانون والمدعيين العامين، وزارة العدل الأمريكية، معهد العدالة الوطني، ٢٠٠٧، ص١٦، مشار إليه دراسة مكتب الأمم المتحدة، مرجع سابق، ص٢٢٨.

ويجب على سلطة التحقيق أن تعرض على المحكمة الإجراءات المطبقة للحفاظ على سلامة الدليل الرقمي، وتبيان الآلية المطبقة لحفظ الدليل وتوثيق التاريخ الزمني له، وأنه لم يطرأ عليه أي تغيير، ولم يتم العبث به، فيجب على النيابة العامة أن تعرض على المحكمة أن المعلومات الرقمية التي تم الحصول عليها من الجهاز هي بمثابة تمثيل حقيقي وسليم للبيانات الأصلية التي يتضمنها الجهاز (الصحة)، وأن الجهاز والبيانات المراد تقديمها كأدلة هي ذاتها التي تم اكتشافها في الأصل، وتم حفظها وتوثيق التاريخ الزمني لها (السلامة)، لما في ذلك من تأثير مباشر على المحكمة في ترجيح فكرة موثوقية الدليل الرقمي وجدارته بالثقة من جانبها[1]، ومن ثم مقبوليته أمام القضاء الجنائي، وللمحكمة في تحقيقها للدعوى بالجلسة سماع الشهود والخبراء ممن قاموا بجمع واستخلاص الأدلة الرقمية ومناقشتهم فيما أثبتوه بتقاريرهم للتثبت من صحتها وسلامتها وأن الوصول إليها قد تم بطريق مشروع.

وتبرز أهمية تناول موضوع موثوقية الدليل الرقمي أمام القضاء الجنائي في سابقة الطعن أمام إحدى المحاكم الأمريكية في موثوقية المعلومات المتولدة من الحاسب الآلي وتلك المخزنة على الحاسب على أساس الثغرات الأمنية الموجودة في أنظمة التشغيل والبرامج التي يمكن أن تؤدي إلى طرح تهديدات على سلامة المعلومات الرقمية، حيث نظرت المحكمة في مسألة قابلية المعلومات الرقمية للتعرض للتلاعب أثناء تقديم الدلائل الإلكترونية، وتم تسليط الضوء على الحاجة لتبيان صحة الحاسب

---

(١) انظر: مارسيلا الإبن أيه جيه، غرينفيلد أر أس (محرران): الأدلة الجنائية الإلكترونية، الدليل الميداني لجمع ودراسة وحفظ أدلة جرائم الحاسب، ط٢، ٢٠٠٢، بوكا راتون، مطبعة سي أر سي، ص١٣٦، مشار إليه دراسة مكتب الأمم المتحدة، مرجع سابق، ص٢٢٩.

الآلي فيما يخص قدرته على الاحتفاظ بالمعلومات موضوع القضية واستعادتها[١]، حيث قضى بأن مقبولية المعلومات المتولدة من الحاسب الآلي (مثل سجلات ملف التسجيل) تعطي تفاصيل عن الأنشطة الخاصة بالحاسب الآلي والشبكة وغيرها من الأجهزة التي يمكن أن تكون عرضة للطعن في حال كان النظام الذي يقوم بتوليد المعلومات لا يحتوي على ضوابط أمنية قوية[٢].

مدى الحجية القانونية للدليل الرقمي في الإثبات الجنائي: يتمثل جوهر العملية الإثباتية في تحويل تلك الواقعة المتنازع عليها إلى أمر مقبول لكافة ومسلم به دون تنازع فيه، أي تحويل حالة الشك في الواقعة التي يراد إثباتها إلى حالة من التيقن بحدوثها، وذلك من خلال التوصل إلى إقناع القاضي بحقيقة ذلك عن طريق ما يقدم في الدعوى من وسائل قادرة على ذلك.

ويتبع التشريع المصري نظام الإثبات الحر أو نظام الأدلة المعنوية وفى هذا النظام لا يرسم القانون طرقاً محددة للإثبات يتقيد بها القاضي الجنائي، بل ترك حرية الإثبات لأطراف الخصومة في أن يقدموا ما يرون أنه مناسب لاقتناع القاضي الذي يتلمس تكوين عقيدته أي دليل يطرح أمامه، وله أن يقدر القيمة الاقناعية لكل منهما، حسبما تتكشف لوجدانه، حيث لا سلطان عليه في ذلك إلا ضميره، وهو ما يعرف بمبدأ قضاء القاضي باقتناعه.

---

(١) انظر: ري فيي فينهي، قضية شركة ديبتور أمريكان إكسبريس ترافلريلاند سيرفيس ضد شركة فيي فينهي، جلسة١٦/١٢/٢٠٠٦، ص١٨، مشار إليه دراسة مكتب الأمم المتحدة، مرجع سابق، ص٢٢٩.

(٢) انظر: تشايكين دي: تحقيقات الشبكة حول الهجمات الإلكترونية- حدود الأدلة الرقمية، الجريمة والقانون والتغير الاجتماعي، ٢٠٠٦، ص ص ٢٣٩-٢٦٥، مشار إليه دراسة مكتب الأمم المتحدة، مرجع سابق، ص٢٢٩.

وهكذا يتضح أن القاضي له مطلق الحرية في أن يستعين بكافة طرق الإثبات للبحث عن الحقيقة والكشف عنها طالما كانت هذه الطرق مشروعة، ويقوم بتقدير كل دليل طرح أمامه لأن مبدأ الحرية والاقتناع لدى القاضي في تقدير قيمة الأدلة قائم، وله أن يستمدها من أي مصدر يطمئن إليه، دون أن يملى عليه المشرع حجية معينة أو يلزمه بإتباع وسائل محددة للكشف عن الحقيقة كقاعدة عامة.

وقد استقر قضاء محكمة النقض على أن ما تحويه الأوراق إن هي إلا عناصر إثبات تخضع في جميع الأحوال لتقدير القاضي الجنائي وتحتمل الجدال والمناقشة كسائر الأدلة، وللخصوم أن يفندوها دون أن يكونوا ملزمين بسلوك سبيل الطعن بالتزوير[١]. ويبين القاضي الأدلة التي أعتمد عليها وكانت مصدراً لاقتناعه فإذا كان تقديره لا يخضع لرقابة محكمة النقض، إذ ليس لها أن تراقبه في تقديره إلا أن لها أن تراقب صحة الأسباب التي أستدل بها على هذا الاقتناع[٢]،ويُرجع الفقه الجنائي إقرار القانون الجنائي لهذا المبدأ في استخدام الدليل العلمي في الإثبات مثل تلك الأدلة المستمدة من الطب الشرعي والتحاليل، وتحقيق الشخصية ومضاهاة الخطوط، وغيرها من الأدلة العملية، وهي أمور لا تقبل أي قيود لدى تعويل القاضي عليها لتكوين عقيدته، ولذلك ترك القانون للقاضي الحرية في تقدير تلك الأدلة وملاءمتها.

فالقانون لم يرسم في المواد الجنائية طريقاً يسلكه القاضي في تحري الأدلة[٣]، ولا يخرج عن هذه القاعدة إلا ما استثناه القانون وجعل له قوة إثبات خاصة بحيث يعتبر المحضر حجة بما ورد فيه إلى أن يثبت ما ينفيه تارة بالطعن بالتزوير كما هي الحال

---

[١] انظر: نقض ٢٠١٢/١٢/٢٣، مجموعة أحكام محكمة النقض، س٦٣، ص٨٦٤.

[٢] د. محمود نجيب حسنى: شرح قانون الإجراءات الجنائية، مرجع سابق، ص٤٠٥ وما بعدها.

[٣] انظر: الطعن رقم (١٨٦٣٧) لسنة ٨٤ق، جلسة ٢٠١٥/٤/١٤، مشار إليه المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٢٥٠.

في محاضر الجلسات والأحكام وتارة أخرى بالطعن بالطرق العادية كمحاضر المخالفات بالنسبة إلى الوقائع التي يثبتها المأمورون المختصون إلى أن يثبت ما ينفيها[١].

ويذهب جانب من الفقه الجنائي[٢]-وبحق- إلى أن تطبيق القواعد العامة في الإثبات الجنائي تفترض أن تكون الأدلة الرقمية مطروحة على بساط البحث أمام المحكمة، فإذا ما أطمأنت إليها عولت عليها، وإذا لم ترتاح لها طرحتها ولا تعتد بها، فملاك الأمر إلى وجدانها وعقيدتها، كما هو الحال في سائر الأدلة الأخرى.

كما أن الوقائع الجنائية لا يمكن تحديدها مسبقاً كما في القانون المدني؛ فهي ليس مما يحرر بها عقود أو يمكن الحصول من الجاني على اعتراف مكتوب بها، ولذلك كان الدليل المستمد من أجهزة الحاسب الآلي ما هو إلا أحد تطبيقات الدليل العلمي بما يتميز به من موضوعية وحياد وكفاءة في إقناع القاضي الجنائي.

موقف القضاء المصري من الاعتداد بالدليل الرقمي: تبرز الإشارة إلى أن القضاء المصري قد اعتد بالدليل الرقمي المتحصل من جرائم تقنية المعلومات، إذ عولت إحدى دوائر الجنايات على الإثبات الناتج عن دليل مستمد من محادثة إلكترونية عبر شبكة الإنترنت، وأقرتها محكمة النقض على ذلك[٣]، كما اعتد القضاء بتقديم الدليل

---

(١) انظر: نقض ١٩٦٧/٦/١٢، مجموعة أحكام محكمة النقض، س١٨، ص٧٩٧.

(٢) انظر: المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٢٥١.

(٣) قضت محكمة النقض في أحد أحكامها الحديثة بأنه:" لما كان ذلك، وكان ما أثبته الحكم في بيانه للواقعة ومضمون ما شهد به ضابطها من أنه إذ سمع مضمون نسخة المحادثة التي أجراها المتهم الطاعن على شبكة المعلومات الدولية وتبينه ما احتوت عليه من عبارات تثبت حيازته لمواد مفرقعة وقنابل وأسلحة نارية وذخائر دون ترخيص، وإقراره له باعتناقه لأفكار "جهادية" متطرفة بتكفير مؤسسات الدولة وبحيازة المضبوطات التي أشار إليها الحكم، وكان من المقرر أن القول بتوافر حالة التلبس أو عدم توافرها من المسائل الموضوعية التي تستقل بتقديرها محكمة الموضوع بغير معقب، ما دامت قد أقامت قضاءها على أسباب سائغة، وكان ما أورده الحكم تدليلا على قيام حالة التلبس وردا على دفع الطاعن كافيا وسائغا ويتفق وصحيح القانون، فإن ما أثاره =

من المجنى عليه، سواء كان هاتفه المحمول، أو جهاز الحاسب الخاص به، أو من خلال ضبطه من جهاز المتهم، وذلك على النحو التالي:-

(الفرض الأول) تقديم الدليل من جهاز المجني عليه: إما بالنسبة للفرض الأول، فقد اعتد به القضاء في حالة تقديمه من المجنى عليه، واعتد به دون إذن، لأنه هاتف المجنى عليه الذى قدمه برضائه الكامل، حتى ولو كان به تسجيل للمتهم، حيث قضت محكمة النقض بأن: (المشرع تطلب مباشرة الإجراءات المبينة بالمادة المراد ذكرها، كي يوضع تحت المراقبة التليفون الذى استعان به الجاني في توجيه ألفاظ السب والقذف إلى المجنى عليه، بحسب أن تلك الإجراءات فرضت ضمانة لحماية الحياة الخاصة والأحاديث الشخصية للمتهم.

ومن ثم فلا تسرى تلك الإجراءات على تسجيل ألفاظ السب والقذف من تليفون المجنى عليه الذى يكون له بإرادته وحدها، ودون حاجة إلى الحصول على إذن من رئيس المحكمة الابتدائية لتسجيلها، بغير أن يعد ذلك اعتداء على الحياة الخاصة لأحد، ومن ثم فلا جناح على المدعين بالحقوق المدنية إذا وضعا على خط التليفون الخاص بهما جهاز تسجيل، لضبط ألفاظ السباب الموجهة إليهم، توصلا إلى التعرف على شخص من اعتاد على توجيه ألفاظ السباب والقذف إليهما عن طريق الهاتف.

ولما كان ذلك، وكان الحكم المطعون فيه قد انتهى إلى بطلان الدليل المستمد من الشريط المسجل بمعرفة المدعين بالحقوق المدنية من جهاز التليفون الخاص بهما،

=

الطاعن ينحل إلى جدل موضوعي لا تجوز إثارته أمام محكمة النقض". انظر: الطعن الجنائي رقم (٣١٣٣٠) لسنة ٨٣ ق، جلسة ٢٠١٥/٥/٥، مشار إليه المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص١٢٤.

فإنه يكون قد أخطا فى تطبيق القانون بما يعيبه ويوجب نقضه والإعادة)[١].

(الفرض الثاني) التحصل على الدليل من جهاز المتهم: إما الفرض الثاني أن تتم المطالبة بالتحصل علي الدليل بضبطه من جهاز المتهم أو مراقبته، وهو ما يحتاج إلى إذن من الجهات القضائية المختصة لعمل ذلك، ولقد كان قانون العقوبات يحوى عددًا كبيرًا من قرائن الإثبات ضد المتهم، إلى أن قضت المحكمة الدستورية العليا بعدم دستوريتها لإخلالها بمبدأ الأصل فى المتهم البراءة، ومنها القرينة التي كانت تضعها المادة ١٩٥ عقوبات، والتي افترضت علم رئيس التحرير بكافة ما تنشره الجريدة التي يشرف عليها، وعدم جواز نفى هذه القرينة إلا من خلال وسائل محددة نصت عليها المادة ١٩٥ عقوبات ذاتها، لذلك، فإنه يجب إثبات وقوع الجريمة من المتهم دون افتراض ذلك، أو إقامة قرينة ضده.

ولقد صدرت أحكام عديدة من القضاء المصري تفيد بأنه قد أعتد بالدليل الرقمي دون الوقوف فى موقف متحجر، وتطلب أن يتم فى شكل تقليدي كمحرر أو شهادة شاهد، ومن القضايا الشهيرة قضية حرق المجمع العلمي، حيث اعتدت المحكمة بالأسطوانات المدمجة والتسجيلات المثبتة لمرتكب الجريمة والتى اطمأنت إليها، وكذلك فى واقعة رشوة عرضت على القضاء استنادًا لتسجيلات، حيث قضت محكمة النقض بأن: (لما كان الثابت من مدونات الحكم المطعون فيه أن المحكمة عولت فى إدانة الطاعن على تسجيلات اللقاءين اللذين تما بين المبلغ والطاعن يومى ٢٦ و٢٨ نوفمبر ١٩٩٦، وأفصح الحكم عن اطمئنانه إليها ثم أردف بقوله، إنه على فرض بطلان التسجيلات، فلا يوجد ما يمنع المحكمة من اعتبارها عنصرًا من عناصر الإثبات فى الدعوى فى منزلة تظاهر الأدلة.

ويبين مما أورده الحكم أن المحكمة لم تبن قضاءها بصفة أصلية على تلك

[١] انظر: الطعن الجنائي رقم (٢٢٣٤٠) لسنة ٦٢ ق، جلسة ٢٠٠٠/٥/١٨، مجموعة أحكام محكمة النقض، س٥١، ص٤٨١.

التسجيلات، وإنما استندت إليها كقرينة تعزز بها أدلة الثبوت التى أوردتها، ولا يعد ذلك منها تناقضًا أو اضطرابًا فى الحكم)[١]، ومن ثم يتضح أن القضاء قد سبق وأن اعتد بالدليل الرقمي في عدد من القضايا في تاريخ سابق عن صدور قانون مكافحة جرائم تقنية المعلومات وهذا نهج محمود للقضاء المصري الذي أرسى هذه القواعد في وقت غاب فيه التنظيم القانوني لهذه المسألة.

حجية التصوير بكاميرات المراقبة التليفزيونية: انتشر استخدام كاميرات المراقبة التليفزيونية في كافة مناحي الحياة، نتيجة لانتشار الجرائم، حيث عملت الكثير من الدول على تزويد الطرق العامة والميادين وغيرها من الأماكن العامة والمؤسسات والأسواق الكبري والفنادق والمدارس وبعض المساكن بكاميرات المراقبة التليفزيونية الحديثة، وتلعب هذه الكاميرات دوراً فاعلاً في كشف غموض الكثير من الجرائم، حيث تتمكن من تسجيل وتصوير ما يدور في المكان على مدار اليوم، وقد يتصادف أن تسجل الكاميرات المذكورة وقائع إجرامية أو يبين منها شخص المشتبه به أو أن الجريمة قد ارتكبت على نحو معين.

ويقر جانب من الفقه الجنائي[٢] بمشروعية الدليل المتحصل من الكاميرات المذكورة؛ شريطة وجود هذه الكاميرات في أماكن عامة، وتسجيلها وقائع الجريمة في هذه الأماكن أيضاً، وكذلك إذا كانت موضوعة في مكان خاص كمسكن وكانت تسجل ما يحدث في مكان عام، فإذا التقطت شخصاً يرتكب جريمة، فلا تثريب في التعويل على الدليل المستمد منها، أما إذا كانت الكاميرات مثبتة في مكان خاص كمسكن، وسجلت الكاميرات ما يحدث بهذا المكان من جرائم، فإن الدليل المتحصل في هذه الحالة يفتقر إلي المشروعية، ومع ذلك فإن الدليل غير المشروع المذكور قد يقود مأمور الضبط

---

[١] انظر: الطعن الجنائي رقم (١٦١٣٧) لسنة ٦٧ ق، جلسة ١٩٩٨/٣/١٤، مجموعة أحكام محكمة النقض، س٤٩، ص٥٦٣.

[٢] المستشار د. محمد سمير: قانون العقوبات الاقتصادي، مرجع سابق، ص٢٣١.

القضائي إلي أدلة أخرى مشروعة.

ويرى الرأي السابق أن المحاكم الجنائية لم تتردد في التعويل على الأدلة المتحصلة من الكاميرات، كما أن محكمة النقض لم تجد حرجاً في ذلك[١]، على الرغم من وجود أعطال في كاميرات المراقبة في بعض الأحيان مما يؤدي إلى التأثير على وضوح أو جودة بعض مقاطع الصورة والصوت المسجل عليها[٢].

خلاصة القول أن إجراءات وتقنيات وأدوات جمع الأدلة الرقمية كان من المتوجب تناولها بشكل أكثر تفصيلاً باللائحة التنفيذية للقانون، بما يحقق تنظيماً تفصيلياً متكاملاً لإجراءات جمع وتوثيق الأدلة الرقمية، وهي من الأدلة المستحدثة التي تتطلب ضرورة تنظيم أحكام التعامل معها بشكل مفصل، بالشكل الذي حقق موثوقيتها أمام القضاء الجنائي، ومن ثم تعزيز الاستفادة منها في مجال الإثبات الجنائي.

---

(١) الموضع السابق، حيث استرشد سيادته بأحكام النقض: الطعن رقم (٢١٨١٩) لسنة ٨٥ق، جلسة ٢٠١٥/١٢/٣؛ نقض ٢٠١٠/٣/٤، مجموعة أحكام محكمة النقض، س٦١، ص٢١٥.

(٢) سبق لمحكمة النقض التصدي لهذه المسألة، فقضت بأنه "لما كان الطاعن لم يدفع أمام محكمة الموضوع ببطلان الدليل المستمد من كاميرات المراقبة على الأساس الذي يتحدث عنه في وجه طعنه – أى لوجود أعطال بأجزاء في بعض مقاطع الصورة والصوت المسجل عليها – فإن هذا الوجه من النعي غير مقبول، لما هو مقرر أن الدفع ببطلان إجراء من الإجراءات السابقة على المحكمة من الأخذ بهذه التسجيلات – علي فرض بطلانها– على أنها عنصر من عناصر الاستدلال مادام أنه كان مطروحاً على بساط البحث وتناوله الدفاع بالمناقشة". انظر: الطعن رقم (٣٢٤١٨) لسنة ٨٥ ق، جلسة ٢٠١٧/٧/٣١، مشار إليه المستشار د/ محمد سمير، مرجع سابق، ص٢٣٢.

المبحث الثامن

الصلح والتصالح في جرائم تقنية المعلومات

أخذ قانون مكافحة جرائم تقنية المعلوماتي بنظامي الصلح مع المجني عليه والتصالح مع الدولة من خلال الجهاز القومي لتنظيم الاتصالات، وحيث جاءت المادة الثانية عشرة من القانون المعنونة بـ"الصلح والتصالح"[1]، لتحديد حالات وإجراءات وآثار التصالح في بعض الجرائم المنصوص عليها في القانون، وهو ما سوف نتناوله في مطلبين على النحو التالي:-

المطلب الأول

الصلح مع المجني عليه

أشارت الفقرتين الأولى والثانية من المادة (٤٢) من القانون على أنه:" *يجوز تهم في أية حالة كانت عليها الدعوى الجنائية، وقبل صيرورة الحكم باتاً، إثبات الصلح من المجني عليه أو وكيله الخاص أو خلفه العام، أمام النيابة العامة أو المحكمة المختصة بحسب الأحوال، وذلك في الجنح المنصوص عليها في المواد (١٤، ١٥، ١٦، ١٧، ١٨، ١٩، ٢٣، ٢٦، ٢٨، ٣٠، ٣١) من هذا القانون. ولا ينتج إقرار المجني عليه بالصلح المنصوص عليه بالفقرة السابقة أثره إلا باعتماده من الجهاز بالنسبة*

---

[1] تبرز الإشارة إلى أن مشروع القانون المقدم من الحكومة كان يشير في عنوان المادة إلى التصالح فقط دون الصلح، إلا أن مجلس النواب قد صحح هذا العنوان ليصبح الصلح والتصالح، نظراً للتمييز الواضح بين الصلح الذي يكون بين الجاني أو وكيله الخاص والمجني عليه أو ورثته أو وكيله الخاص، والتصالح الذي يتم بين المتهم والدولة أو الجهة الإدارية المعتدى عليها مقابل غرامة التصالح. انظر: مضبطة مجلس النواب المصري، الجلسة السادسة والخمسين، المعقودة في ٢٠١٨/٥/١٤م، مرجع سابق، ص ١١٨ ومابعدها.

للجنح المنصوص عليها بالمواد (١٤، ١٧، ١٨، ٢٣) من هذا القانون"، بينما أشارت الفقرة الأخيرة من المادة المذكورة بأنه:" *ويترتب على الصلح انقضاء الدعوى الجنائية، ولا أثر للصلح على حقوق المضرور من الجريمة أو على الدعوى المدنية* "، ونتناول فيما يلي أحكام الصلح مع المجني عليه في الجرائم المعلوماتية، وذلك على النحو التالي:-

أولاً- نطاق الصلح مع المجني عليه في الجرائم المعلوماتية: أبان نطاق تطبيق الصلح مع المجني عليه في الجرائم المعلوماتية من الجنح المنصوص عليها في المواد ١٤، ١٥، ١٦، ١٧، ١٨، ١٩، ٢٣، ٢٦، ٢٨، ٣٠، ٣١ من هذا القانون، وهي جرائم: الدخول غير المشروع (م١٤)، تجاوز حدود الحق في الدخول(م١٥)، والاعتراض غير المشروع(م١٦)، والاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية(م١٧)، والاعتداء على البريد الإلكتروني أو المواقع والحسابات الخاصة(م١٨)، والاعتداء على تصميم موقع(م١٩)، جرائم الاحتيال والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الإلكتروني (م٢٣)، التشهير بالغير(م٢٦)، العبث بالأدلة الرقمية (م٢٨)، الامتناع عن التبليغ في الجرائم المعلوماتية(م٣٠)، إفشاء البيانات المحفوظة لدى مقدم الخدمة(م٣١)، ويتفق هذا النهج التشريعي طبيعة التصالح كاستثناء على حق الدولة في العقاب على الجرائم، والذي يجب أن يكون محدداً، ويلاحظ أن المشرع أشار إلى أن نطاق الصلح يشمل جرائم الجنح المحددة في القانون، ومن ثم لا يمتد التصالح في الأحوال التي يتوافر في الجريمة ظرف مشدد يغير من وصف الجريمة من الجنحة إلى الجناية، فلا صلح في الجنايات، بالنظر إلى خطورة الأخيرة، وتطلب القانون من جهات التحقيق مباشرة إجراءات التحقيق فيها، وإحالتها للقضاء.

ثانياً- أطراف الصلح في جرائم تقنية المعلومات:يتمثل النطاق الشخصي للصلح في أطرافه، وأطراف الصُلح الجنائي هم المتهم والمجني عليه، أضف إلى ذلك النيابة العامة أو المحكمة، وهما الجهتين القضائيتين المُخول لأطراف الصُلح إثبات وقوع الصُلح بينهما أمامهما، وقد نص المشرع المصري على السماح لكل من للمُتهم أو وكليه الخاص[١] إثبات الصُلح مع المجني عليه أو وكيله الخاص أو خلفه العام؛ أي ورثته أمام النيابة أو المحكمة في أي مرحلة من مراحل الدعوى الجنائية، حتى وبعد صيرورة الحكم باتاً[٢]، والواقع أن الحكمة التشريعية من إقرار الصلح حتى صيرورة الحكم الجنائي باتاً هو تشجيع الأفراد على التسوية الودية في مثل هذه القضايا[٣].

وقد أضاف القانون الجهاز القومي لتنظيم الاتصالات كأحد أطراف الصلح، حينما تطلب في جرائم بعينها اعتماد الصلح مع المجني عليه من الجهاز، وهي: الدخول غير المشروع (م١٤)، والاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية(م١٧)، والاعتداء على البريد الإلكتروني أو المواقع والحسابات

---

[١] يلاحظ من صياغة نص المادة (١٨ مكرراً "أ") إجراءات جنائية- قبل تعديلها الأخير- كانت تقصر الحق في إثبات الصلح في المجني عليه أو وكيله الخاص، إلا أن التعديلات الأخيرة لنظام الصلح أجازت لورثة المجني عليه أو وكيلهم الخاص إثبات الصلح مع المتهم، ولاشك أن هذا التعديل قد عالج مشكلة وفاة المجني عليه، فالنظر إلى اعتبار أن هذا الحق في الصلح حق شخصي، يقتصر على المجني عليه أو من يوكله، فإن هذا الحق يسقط بوفاة المجني عليه، ومن ثم لا يجوز إعمال نظام الصلح، إلا أن التعديلات الأخيرة والتي أجازت لورثة المجني عليه أو وكيلهم الخاص إثبات الصلح مع المتهم قد وسعت في إعمال نظام الصلح الجنائي، وبصفة خاصة في حالة وفاة المجني عليه، كما أن قصر الحق في الصلح على المجني عليه في جريمة القتل الخطأ (إحدى الجرائم التي أجاز المشرع الجنائي الصلح فيها) يصبح منتفياً منذ البداية، ومن ثم أضحى إقرار هذا الحق لورثة المجني عليه من الأمور اللازمة للقول بجواز إعمال نظام الصلح الجنائي في هذه الجريمة.

[٢] د. مأمون محمد سلامة: الإجراءات الجنائية، مرجع سابق، ص٣٢٥.

[٣] قارن: الكتاب الدوري رقم (١٢) لسنة ٢٠٠٦ والخاص بتعليمات النائب العام بشأن نظام الصلح في بعض الجرائم متضمناً بعض التعليمات للسادة أعضاء النيابة.

الخاصة(م١٨)، جرائم الاحتيال والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الإلكتروني (م٢٣).

وقد حددت المادة ١٢ من اللائحة التنفيذية كيفية اعتماد الجهاز القومي لتنظيم الاتصالات إقرار المجني عليه بالصلح، حيث تقضي المادة المشار إليها بأنه:"يشترط لاعتماد الجهاز إقرار المجني عليه بالصلح طبقا للمادة رقم ٤٢ من القانون، فى الجرائم المنصوص عليها في المواد (١٤، ١٧، ١٨، ٢٣) استيفاء وتقديم ما يلى:

١- شهادة صادرة من النيابة أو المحكمة المختصة بحسب الأحوال بالقيد والوصف للجريمة محل الصلح.

٢- صورة طبق الأصل من المحضر أو الوثيقة التي أثبت فيها الصلح بين المتهم والمجني أو وكيله الخاص أو خلفه العام أمام النيابة أو المحكمة المختصة والمتضمنة إقرار المجني عليه بهذا الصلح.

٣- شهادة صادرة من النيابة المختصة تفيد عدم صدور حكم نهائي في الدعوى الجنائية.

٤- طلب باسم الرئيس التنفيذي للجهاز لاعتماد المحضر أو الوثيقة المتضمنة إقرار المجني عليه بالصلح يقدم من المتهم أو من وكيله أو من خلفه العام".

ثالثاً- شروط تطبيق الصلح الجنائي:يشترط لتطبيق الصُلح الجنائي في القانون المصري ضرورة توافر شرطين: (الأول): أن تكون الجريمة من الجرائم التي أجاز المشرع الصلح فيها، وذلك على سبيل الحصر، وبذلك يخرج من نطاق الصُلح الجرائم التي لم يرد النص عليه في القانون[1]، و(الثاني) ضرورة إثبات الصُلح أمام النيابة

[1] قارن: للباحث: بدائل الدعوى الجنائية في القانون المصري في ضوء أحدث التعديلات التشريعية، مجلة كلية التدريب والتنمية، القاهرة، العدد (٢٤)، مارس٢٠١١، ص٤٠٢.

العامة أو المحكمة، حيث يشترط القانون لإعمال أثر الصُلح في انقضاء الدعوى أن يتم إثبات الصُلح من المجني عليه أو وكيله الخاص أو خلفه العام أمام السلطة القضائية المختصة سواء أكانت النيابة العامة أو في محضر الجلسة أمام المحكمة في أي مرحلة كانت عليها الدعوى ولو بعد صيرورة الحكم باتاً أو أثناء تنفيذ العقوبة، وإذا قدم الصُلح من غير المجني عليه أو خلفه العام أو المُتهم، فيجب أن يكون هناك توكيل خاص يبيح له ذلك، ولا يشترط تقديم الصُلح أو صورة منه، كما لا يشترط إثبات بنود الصُلح في محضر الجلسة، وإنما الذي يشترط فقط إثبات أن المجني عليه قد تصالح مع المُتهم، ولا يشترط في اتفاق الصُلح أن يكون معلقاً على شرط، فالصُلح المعلق على شرط لا ينتج أثره في انقضاء الدعوى الجنائية[١].

رابعاً- إجراءات الصُلح الجنائي: لم يرد في قانون الإجراءات الجنائية أي تنظيم لإجراءات الصلح الجنائي، ومن هذا المنطلق أشار الفقه الجنائي إلى تحديد إجراءات الصلح الجنائي في تقديم ما يفيد الصُلح إلى الجهات القضائية المختصة من جانب الأشخاص الذين يجوز لهم التمسك بوقوع الصُلح، فلا يتحقق الصُلح الجنائي بوقوع الاتفاق بين المُتهم والمجني عليه أو وكيله الخاص أو خلفه العام على إنهاء الإجراءات القضائية بشكل ودي، وإنما يجب تقديم طلباً لإثبات الصُلح من جانب المجني عليه أو وكيله الخاص أو ورثة المجني عليه أو وكيلهم الخاص أو من المتهم أو وكيله الخاص إلى السلطة القضائية المختصة (النيابة العامة أو المحكمة المختصة)[٢]، ويفترض فيمن يتقدم بطلب إثبات الصُلح أن تتوافر لديه الأهلية لمُباشرة التصرفات

---

[١] د. مأمون محمد سلامة: الإجراءات الجنائية، مرجع سابق، ص٣٢٥؛ رائد. د. جاسم محمد العنتلي: الصلح في قانون الإجراءات الجزائية الاتحادي، دورية الفكر الشرطي، المجلد (١٨)، العدد (٧١)، ٢٠٠٩، مركز بحوث الشارقة، الإمارات العربية المتحدة، ص١٢٧.

[٢] انظر للباحث: بدائل الدعوى الجنائية في القانون المصري، مرجع سابق، ص٤٠٦.

القانونية، فإذا كان المجني عليه أو أحد خلفه العام أو المتهم قاصراً – وهذا الفرض لم يتعرض له التنظيم التشريعي للصُلح الجنائي – ففي هذه الحالة يلزم تقديم طلب إثبات الصلح ممن له ولاية عليه[١]، وهذا ما يأخذ به قضاء النقض[٢]، ويتطلب القانون ضرورة تقديم طلب إثبات الصُلح للجهة القضائية المختصة بنظر الدعوى سواء أكانت النيابة العامة أو المحكمة المختصة، فإذا كانت الدعوى في حوزة النيابة؛ أي قبل إحالتها للمحكمة المختصة في مرحلتي الاستدلال أو التحقيق الابتدائي، فإنه يتم تقديم طلب إثبات الصلح للنيابة العامة، أما إذا كانت النيابة العامة قد أحالت القضية للمحكمة، فإن طلب إثبات الصُلح يقدم للمحكمة المختصة[٣]، وإذا قُدم طلب إثبات الصُلح من غير الأشخاص المنصوص عليهم في القانون، فإن هذا الإجراء يكون غير مقبولاً، لتقديمه من غير ذي صفة، وإذا حكمت المحكمة بناءً على طلب قُدم من غير الأشخاص الذين حددهم المُشرع، يكون حكمها باطلاً، وإذا لم يقدم طلب إثبات الصُلح للنيابة أو المحكمة، فإنه لا يجوز لها أن تقضي بانقضاء الدعوى الجنائية بالصُلح من تلقاء نفسها[٤].

---

(١) يشير البعض إلى أن القاعدة الإجرائية المنصوص عليها في المادة (٥) من قانون الإجراءات الجنائية تقضي بأنه في حالة تقديم الشكوى عندما يكون المجني عليه لم يبلغ خمسة عشر سنة كاملة، أو كان مصابا بعاهة في عقله أن يتم تقديم الشكوى ممن له الولاية عليه، وإذا كانت الجريمة واقعة على المال تقبل الشكوى من الوصي أو القيم، فإنه يمكن تطبيق هذه القاعدة على الصلح على سبيل القياس.

(٢) ذهبت محكمة النقض في أحد أحكامها إلى أن:" ولى القاصر هو وكيل جبري عنه بحكم القانون، ينظر في القليل والجليل من شئونه الخاصة بالنفس والمال". نقض ١٩٩٠/١/٢، س٤١، رقم ٣، ص٣٨؛ نقض ١٩٩٠/٥/٨، س٤١، رقم ١٢٠، ص٦٩٦.

(٣) انظر للباحث: بدائل الدعوى الجنائية، مرجع سابق، ص٤٠٦.

(٤) د. عبد الله أحمد الشيخ: التصالح والصلح في المنازعات الجنائية وأثرهما في استقرار الأمن العام، رسالة دكتوراه، كلية الدراسات العليا بأكاديمية الشرطة، القاهرة، ٢٠٠٩، ص ص١٢٠، ١٢١.

خامساً- الآثار القانونية للصلح الجنائي: يرتبط الأثر القانوني لنظام ما بطبيعته القانونية، وقد اختلف الفقه الجنائي حول الطبيعة القانونية لنظام الصلح الجنائي، فمنهم من ذهب إلى أن الصلح ليس إلا عقداً مدنياً بين المتهم والنيابة العامة أو المجني عليه ومن ثم فهو أمر غريب في المسائل الجنائية[١]، بينما ذهب جانب آخر من الفقه إلى أن الصلح له طابع جنائي، فمنهم من ذهب على أن غرامة الصلح ذات طبيعة مختلطة تجمع بين عنصري التعويض والعقاب كما في الغرامة الضريبية[٢]، ومنهم من ذهب إلى أن غرامة التصالح هي عقوبة مالية بديلة يتوقف تنفيذها على رضاء المجني عليه[٣]، إلا أن الباحث يفضل اعتبار الصلح من بدائل الدعوى الجنائية أو من أسباب انقضاء الدعوى الجنائية، والذي يستهدف تجنيب المتهم الخضوع للعقوبة، ويترتب على تحققه انقضاء الدعوى الجنائية سواء أكان ذلك بمقابل أو بدون مقابل، ومن ثم فمقابل الصلح ليس بعقوبة، وتتمثل الآثار القانونية للصُلح في تناول أثره على كلٍ من الدعويين الجنائية والمدنية المرفوعة أمام المحكمة الجنائية، فضلاً عن تناول أثر الصلح على العقوبة الجنائية، فبالنسبة للدعوى الجنائية، يترتب على إتمام الصلح الجنائي في القانون المصري انقضاء الدعوى الجنائية، وهو ما أشار إليه نص المادة (١٨مكرراً "أ" إجراءات جنائية)؛ إذ نصت الفقرة الأخيرة من المادة ٤٢ من القانون على أنه:" ويترتب على الصُلح انقضاء الدعوى الجنائية..."، فإذا قُدم الصلح – كما

---

(١) د. عوض محمد عوض: المبادئ العامة لقانون الإجراءات الجنائية، دار المطبوعات الجامعية، ١٩٩٩، ص١٣٩ وما بعدها؛ د. مدحت عبد الحليم رمضان: الإجراءات الجنائية الموجزة لإنهاء الدعوى الجنائية، دار النهضة العربية، ٢٠٠٠، ص٨٤ وما بعدها؛ د. عبد الرءوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، ط٢، ١٩٩٦، ج١، ص٧٢٠.

(٢) د. أحمد فتحي سرور: القانون الجنائي الدستوري، مرجع سابق، ص٣٤٨.

(٣) د. محمد حكيم حسين الحكيم: النظرية العامة للصلح في المواد الجنائية وتطبيقاتها، مرجع سابق، ص١٤٦ وما بعدها؛ د. إبراهيم حامد طنطاوي: الصلح الجنائي في نطاق المادتين ١٨مكرر و١٨مكرر أ- دراسة مقارنة، دار النهضة العربية، ٢٠٠٠، ص٣١.

سبق أن أشرنا- أمام النيابة العامة أمرت بألا وجه لإقامة الدعوى الجنائية لانقضائها بالصلح، إما إذا قدم الصلح أمام المحكمة المختصة، حكمت بانقضاء الدعوى الجنائية بالصلح[١]، ويقتصر أثر الصلح الجنائي على طرفيه فحسب، ومن ثم لا يمتد إلى غيرهم إعمالاً لمبدأ نسبية أثر الصلح الجنائي، ومن ثم لا يمتد أثر الصلح إلى المضرور من الجريمة غير المجني عليه[٢].

أما بالنسبة للعقوبة الجنائية، فإنه وفقاً للقواعد العامة في قانون الإجراءات الجنائية الواردة في المادة ١٨ مكرر (أ) إجراءات جنائية، تأمر النيابة العامة بوقف تنفيذ العقوبة إذا حصل الصُلح أثناء تنفيذها، ويتضح من النص السابق أن الصُلح لا يتم إلا بتوافق إرادتي المُتهم والمجني عليه، وأنه يجوز إبرامه في كافة مراحل الدعوى الجنائية حتى لو صدر فيها حكم بات. ويترتب على الصُلح بالنسبة للمتهم الإفراج عنه إذا كان محبوساً، أو وقف تنفيذ العقوبة إذا كان المُتهم يقضي فترة الحبس[٣]، أما بالنسبة للدعوى المدنية، فقد نصت الفقرة الأخيرة من المادة ٤٢ من القانون على أن:"لا أثر للصلح على حقوق المضرور من الجريمة أو على الدعوى المدنية"، هو ما

---

(١) ومن الجدير بالذكر أن مشروع تعديل قانون الإجراءات الجنائية لعام ٢٠١٧ تضمن تعديلاً للفقرة الأخيرة من المادة (١٨مكرراً أ) والتي تقضي بأنه: "وتقضي المحكمة بانقضاء الدعوى الجنائية بالصلح ولو كانت مرفوعة بطريق الادعاء المباشر، وتأمر النيابة العامة بوقف تنفيذ العقوبة إذا حصل الصلح أثناء تنفيذها، ولا أثر للصلح على حقوق المضرور من الجريمة"، كما استحدث مادة جديدة برقم (١٨مكرراً "أ"/٢) تقضي بأنه:" وفي جميع الأحوال التي يتم فيها الصلح وفقاً للمواد السابقة يترتب على انقضاء الدعوى الجنائية بالصلح انسحاب أثره على جميع الوقائع محل الصلح بجميع كيوفها وأوصافها، ويمتد أثره إلى جميع المتهمين في الواقعة محل الصلح، ولو تعددت الأوصاف القانونية للاتهام".

(٢) د. هدى حامد قشقوش: الصلح في نطاق قانون الإجراءات الجنائية رقم ١٧٤ لسنة ١٩٩٨ مع التعليق على أحدث الأحكام، دار النهضة العربية، القاهرة، ص٧١ ومابعدها.

(٣) الطعن رقم ٢١٨٦٤ لسنة٦٢ق، جلسة ٢٠٠١/١١/٢١، مجموعة المكتب الفني لهيئة قضايا الدولة، سنة ٢٠٠٣، ص٨٠٤.

يتفق مع نص المادة (٢٥٩) إجراءات جنائية[١]، ويبرر جانب مهم من الفقه الجنائي[٢] – وبحق- عدم تأثير نظام الصلح على الدعوى الجنائية في أن نظامي الصلح والتصالح لا يتمتعا بحجية إيجابية فيما يتعلق بثبوت التهمة أو نفيها ومن ثم فلا حجية له أمام القضاء المدني، ويقتصر أثرهما على الحجية السلبية المتمثلة في انقضاء الدعوى الجنائية ولهذا فإن مبلغ الصلح لا يعد عقوبة، ولا تسري عليه أحكامها[٣].

المطلب الثاني

التصالح مع الجهاز القومي لتنظيم الاتصالات

أجاز القانون التصالح بين المتهم والجهاز القومي لتنظيم الاتصالات، حيث أشارت الفقرات الثالثة والرابعة والخامسة من المادة (١٢) إلى أنه:" ***كما لا يُقبل التصالح إلا من خلال الجهاز بخصوص الجنح المنصوص عليها بالمادتين (٢٩ ، ٣٥) من هذا القانون. ولا يسقط حق المتهم في التصالح برفع الدعوى الجنائية إلى المحكمة المختصة إذا دفع ثلثي الحد الأقصى للغرامة المقررة للجريمة أو قيمة الحد الأدنى أيهما أكثر، وذلك قبل صدور حكم نهائي في الموضوع. وفى جميع الأحوال يجب على المتهم الذي يرغب في التصالح أن يسدد قبل رفع الدعوى الجنائية مبلغاً يعادل ضعف الحد***

---

[١] نصت المادة ٢٥٩ إجراءات جنائية على أن:" إذا انقضت الدعوى الجنائية بعد رفعها لسبب من الأسباب الخاصة بها فلا تأثير لذلك في سير الدعوى المدنية المرفوعة معها".

[٢] د. أحمد فتحي سرور: القانون الجنائي الدستوري، مرجع سابق، ص٣٤٦.

[٣] على خلاف الرأي السابق، يذهب جانب من الفقه إلى اعتبار أن غرامة الصلح هي عقوبة، وأن الدولة قد تحصل على سلطتها في العقاب كما في الصلح دون الحاجة إلى دعوى جنائية، وأن سداد المتهم لغرامة الصلح يعد من قبيل التنفيذ الاختياري وليس الإجباري للعقوبة. إلا أن هذا الرأي مردود عليه بأن الصلح أجازه القانون لعلة خاصة تتعلق بتيسير الإجراءات الجنائية وإعطاء قيمة قانونية لعفو المجني عليه في جرائم معينة. أنظر: د. أحمد فتحي سرور: القانون الجنائي الدستوري، مرجع سابق، ص٣٤٧.

***الأقصى للغرامة المقررة للجريمة. ويكون السداد إلى خزانة المحكمة المختصة أو النيابة العامة، بحسب الأحوال"*.**

أولاً- نطاق التصالح مع الجهاز القومي لتنظيم الاتصالات في جرائم تقنية المعلوماتية: أوضح القانون نطاق التصالح في الجرائم المعلوماتية بنصه على أنه:"*لا يُقبل التصالح إلا من خلال الجهاز بخصوص الجنح المنصوص عليها بالمادتين ٢٩، ٣٥ من هذا القانون*"، ومن ثم يقتصر نطاق التصالح في الجرائم المعلوماتية على جريمتي تعريض المواقع والحسابات الخاصة والبريد الإلكتروني والنظم المعلوماتية لخطر الجرائم المعلوماتية، وتعريض المواقع والحسابات الخاصة والبريد الإلكتروني والنظم المعلوماتية للأشخاص الاعتبارية لخطر الجرائم المعلوماتية.

ثانياً- شروط تطبيق التصالح الجنائي: يشترط لتطبيق التصالح ضرورة توافر شروط ثلاثة: (الأول)، أن تكون الجريمة محل التصالح من الجرائم المحددة قانوناً، (والثاني) أن يقوم المُتهم بدفع مبلغاً يعادل ضعف الحد الأقصى للغرامة المُقرر للجريمة، واشترط القانون أن يكون دفع مبلغ الغرامة قبل رفع الدعوى، ويكون الدفع إلى خزانة المحكمة أو إلى النيابة العامة أو إلى أي موظف عام يرخص له في ذلك من وزير العدل، ولا يسقط حق المُتهم في التصالح برفع الدعوى إلى المحكمة المختصة، إلا إذا دفع المُتهم ثلثي الحد الأقصى للغرامة المُقررة أو قيمة الحد الأدنى المُقرر لها أيهما أكثر[1]، (والثالث) أن يطلب المتهم من الجهاز القومي لتنظيم الاتصالات الصلح في الجرائم المحددة قانوناً، مقدماً الأوراق والشهادات التي تثبت دفع غرامة التصالح، (والرابع) قبول الجهاز القومي لتنظيم الاتصالات للتصالح مع المتهم.

---

[1] د. مأمون محمد سلامة: الإجراءات الجنائية، مرجع سابق، ص٣٢٥.

ثالثاً- إجراءات التصالح الجنائي: تتمثل إجراءات التصالح في عرض التصالح والوفاء بمبلغ الغرامة، وفيما يلي نتناول إجراءات التصالح الجنائي على النحو التالي:-

أ) الوفاء بمبلغ الغرامة: ينبغي علي المتهم الراغب في التصالح في جرائم تقنية المعلومات أن يدفع - قبل رفع الدعوى الجنائية- مبلغاً يعادل ضعف الحد الأقصى للغرامة المُقرر للجريمة بغض النظر عن الحد الأدنى للغرامة. أما إذا تم إحالة الدعوى الجنائية للمحكمة، فإن ذلك لا يسقط حق المُتهم في التصالح، وإنما يترتب على ذلك زيادة مبلغ التصالح؛ إذ يلتزم المُتهم - في هذه الحالة– بدفع مبلغاً يعادل ثلثي الحد الأقصى للغرامة المُقررة للجريمة أو قيمة الحد الأدنى المُقرر لها أيهما أكثر، فالمُشرع المصري حدد مقدار غرامة التصالح بنسبة محددة، ويتم الدفع إلى خزانة المحكمة أو النيابة العامة، بحسب الأحوال.

ب) موافقة الجهاز القومي لتنظيم الاتصالات على التصالح: حددت المادة ١٣من اللائحة التنفيذية كيفية قبول التصالح من جانب الجهاز القومي لتنظيم الاتصالات وفق المادة ٤٢ من القانون، حيث نصت المادة المشار إليها على أنه:" يكون تصالح المتهم طبقًا للمادة رقم (٤٢) من القانون، في الجرائم المنصوص عليها بالمادتين (٢٩، ٣٥) من القانون من خلال الجهاز باستيفاء وتقديم ما يلى:

شهادة صادرة من النيابة أو المحكمة المختصة بحسب الأحوال بالقيد والوصف للجريمة موضوع التصالح.

شهادة صادرة من النيابة المختصة تفيد عدم صدور حكم نهائي فى موضوع الجريمة محل طلب التصالح.

أن يقدم المتهم الراغب في التصالح أو وكيله قبل رفع الدعوى الجنائية الإيصال الدال على سداده مبلغًا يعادل ضعف الحد الأقصى للغرامة المقررة للجريمة.

أن يقدم المتهم الراغب في التصالح أو وكيله بعد رفع الدعوى الجنائية الإيصال الدال على سداده ثلثي الحد الأقصى للغرامة المقررة للجريمة أو قيمة الحد الأدنى للغرامة أيهما أكثر قبل صدور حكم نهائي في الموضوع".

ج) مخاطبة الجهاز القومي لتنظيم الاتصالات للجهة القضائية لإثبات التصالح مع المتهم: في حال قبول الجهاز الأوراق المقدمة من المتهم للتصالح في جرائم تقنية المعلومات المحددة بالقانون، فإن الجهاز يخاطب الجهة القضائية المعنية، وهي النيابة العامة أو المحكمة المختصة للتصرف في الدعوى في ضوء التصالح مع المتهم.

رابعاً- أثر التصالح على الدعوى الجنائية: يرتبط الأثر القانوني لنظام ما – كما سبق أن أشرت- بطبيعته القانونية، وقد اختلف الفقه الجنائي حول الطبيعة القانونية لنظام التصالح الجنائي في جرائم القانون العام، فمنهم من ذهب - كما سبق الإشارة في نظام الصلح – إلى اعتبار نظام التصالح عقداً مدنياً[١]، ومنهم من ذهب إلى اعتباره ذا طبيعة إدارية[٢]، ومنهم من اعتبره عقد جنائي تعويضي[٣]، ومنهم من اعتبره عملاً قانونياً[٤]، إلا أن الباحث يفضل اعتبار نظام التصالح الجنائي من بدائل الدعوى الجنائية أو من أسباب انقضائها على النحو السابق الإشارة إليه في نظام الصلح الجنائي، ويتفق الباحث مع الفقه الجنائي[٥] الذي يرى أن التصالح إذا تم قبل الدعوى الجنائية، فإنه يعد بديلاً لها، وإن تم بعد هذا التحريك اعتبر سبباً لاحقاً لانقضائها.

---

[١] د. سر الختم عثمان إدريس: النظرية العامة للصلح في القانون الجنائي، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ١٩٧٩، ص١٧٢.

[2] Merle (R.), et Vitu (A.), traite de droit criminel, procédure pénale, CUJAS, 5ed. 2001, no.65.p.84.

[3] DOBKIN (M.): La transaction en matière pénale, D. 1994, Chron, P. 139.

[٤] د. أحمد فتحي سرور: الصلح في الجرائم الضريبية، مجلة إدارة قضايا الحكومة، س٢٨، يوليو- سبتمبر ١٩٨٤،ع٣، ص١٢٩.

[٥] د. أحمد فتحي سرور: الوسيط في قانون الإجراءات الجنائية، مرجع سابق، ص٢٦٥.

وعرض التصالح على المُتهم لا يرتب أثره في انقضاء الدعوى الجنائية إلا بدفع مبلغ التصالح، فإذا دفع المُتهم مبلغ التصالح، فإنه تنقضي الدعوى الجنائية بالتصالح، وينبغي أن يصدر عضو النيابة العامة قراراً بحفظ الأوراق أو الأمر بألا وجه – بحسب الأحوال- لانقضاء الدعوى بهذا السبب[١]، وعلى المحكمة حين تقضي بانقضاء الدعوى الجنائية بالتصالح أن تبين فحوى التصالح وتستظهر مدى توافر شروطه، وإلا كان حكمها معيباً بالقصور في التسبيب[٢]، وهو أمر متعلق بالنظام العام يجب على المحكمة أن تقضي به من تلقاء نفسها، ولو بغير دفع من الطاعن، وإلا كان حكمها معيباً بمخالفة القانون[٣]، فإذا أثار المتهم دفاعاً بشأن وقوع التصالح، والتفتت المحكمة عن هذا الدفاع ولم تقسطه حقه ولم تقم بتمحيصه بلوغاً إلى غاية الأمر فيه، فإن حكمها يكون فوق ما ران عليه من القصور قد جاء مشوباً بالإخلال بحق المتهم في الدفاع[٤]. أما بالنسبة للدعوى المدنية، فلا يترتب على انقضاء الدعوى الجنائية بالتصالح أثر على الدعوى المدنية الناشئة عن الواقعة موضوع الجريمة التي تم التصالح فيها[٥]، فإذا تم التصالح قبل رفع الدعوى الجنائية، فلا يجوز رفع الدعوى المدنية أمام المحكمة الجنائية، لأنها لا تختص بها إلا بصفة تبعية، وحيث أن الدعوى الجنائية لم يتم رفعها، فإنه لا يجوز نظر الدعوى المدنية أمام المحكمة الجنائية، وإذا تم

---

[١] انظر للباحث: بدائل الدعوى الجنائية، مرجع سابق، ص٤١٩.

[٢] انظر: الطعن رقم (٩٠) لسنة ٤٥ ق، جلسة ١٩٧٥/٣/٣، س٢٦، ج١، ص٢٠٥؛ الطعن رقم (١٧٥٣) لسنة ٦٢ق، جلسة ١٩٩٤/١٢/١١، س٤٥، ج١، ص١١١٩.

[٣] انظر: الطعن رقم (٢٦١٨) لسنة ٥١ ق، جلسة ١٩٨٢/١/١٩، س٣٣، ج١، ص٤٦؛ الطعن رقم (٢٧٠٧٩) لسنة ٦٧ق،جلسة٢٠٠٧/٧/١ ،لم ينشر بعد.

[٤] انظر: الطعن رقم (٢٦٢٥) لسنة ٥١ق، جلسة ١٩٨٢/١/١٩، س٣٣، ج١، ص٤٦؛ الطعن رقم (٦٧٣٦) لسنة ٥٩ق، جلسة ١٩٩٢/١/٢٣، س٤٣،ج١، ص١٧٦.

[٥] أنظر: تعليمات النائب العام السابق الإشارة إليها.

التصالح بعد رفع الدعوى، فإنه لا أثر له على الدعوى المدنية والتي يتعين على المحكمة الجنائية الاستمرار في نظرها تطبيقاً لنص المادة (٢٥٩) إجراءات جنائية[١].

[١] د. إبراهيم حامد طنطاوي: الصلح الجنائي، مرجع سابق، ص١٤٢؛ د. مدحت محمد عبد العزيز: الصلح والتصالح، مرجع سابق، ص١٩٤؛ د.عبد الله الشيخ: التصالح والصلح، مرجع سابق، ص١٣٩.

المبحث التاسع

التعاون الدولي لمكافحة جرائم تقنية المعلومات

تبرز أهمية التعاون الدولي في المسائل الجنائية ذات الصلة بجرائم تقنية المعلومات، بالنظر إلى الطابع عبر الوطني الذي تتسم به هذه الجرائم والتي تستخدم في ارتكابها في أغلب الأحوال شبكة الإنترنت، ومن ثم تتحقق عناصر الركن المادي للجريمة وآثارها في الغالب في دولة أو أكثر، وهو ما يتطلب ضرورة وجود قواعد قانونية تنظم مسائل التعاون بين جهات إنفاذ القانون بين الدول، علاوة على أن الأدلة الرقمية المتخلفة عن هذه الجرائم قد توجد في أكثر من دولة، وهو ما يتطلب تفعيل أحكام التعاون الدولي القضائي في هذا الشأن.

وقد بينت المادة الرابعة من القانون أحوال وشروط التعاون الدولي في مجال مكافحة الجرائم المعلوماتية، وقد جاءت هذه الأحكام في نص عام، تضمن آليات تبادل المعلومات والمساعدة القضائية، حيث أشارت المادة المذكورة إلى أنه:" *تعمل السلطات المصرية المختصة على تيسير التعاون مع نظيراتها بالبلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصدق عليها، أو تطبيقاً لمبدأ المعاملة بالمثل، دل المعلومات بما من شأنه أن يكفل تفادى ارتكاب جرائم تقنية المعلومات، والمساعدة على التحقيق فيها، وتتبع مرتكبيها. على أن يكون المركز الوطني للاستعداد لطوارئ الحاسب والشبكات بالجهاز هو النقطة الفنية المعتمدة في هذا الشأن*".

وقد حدد المشرع المصري الأغراض التي يتوخاها من التعاون الدولي في مجال جرائم تقنية المعلومات، والمتمثلة فيما يلي:-

١- تفادي ارتكاب جرائم تقنية المعلومات، وهذا هو هدف التعاون الدولي الأمني.

٢ـ المساعدة على التحقيق فيها وتتبع مرتكبيها، وهذا هو هدف التعاون القضائي الدولي.

وقد أشار القانون إلى اعتبار المركز الوطني للاستعداد لطوارئ الحاسب والشبكات بالجهاز القومي لتنظيم الاتصالات هو النقطة الفنية المعتمدة في هذا الشأن، ويكون ذلك في إطار الاتفاقيات الدولية والإقليمية والثنائية المصادق عليها، أو تطبيق مبدأ المعاملة بالمثل.

ويرى الباحث أنه كان من الأولى بالمشرع أن يتضمن تفصيلاً أكثر فيما يتصل بمسائل التعاون الدولي في مكافحة جرائم تقنية المعلومات من خلال تقرير نصوص بشأن تسليم المجرمين والمساعدة القضائية، وبالشكل الذي يحدد شروط وإجراءات التسليم وشروط وإجراءات المساعدة القضائية المتبادلة إلى غير ذلك من آليات التعاون القضائي الدولي.

وفي هذا الإطار تبرز الإشارة إلى أن مكتب الأمم المتحدة المعني بالمخدرات والجريمة ـ في إحدى دراساته حول الجريمة السيبرانية- يرى وبحق أن الاعتماد على الوسائل التقليدية للتعاون الدولي الرسمي في مسائل جرائم تقنية المعلومات لا يكفي حالياً للاستجابة في الوقت المناسب لمقتضيات الحصول على أدلة رقمية سريعة الزوال والتغير، توجد في أمكان جغرافية متعددة، وهو ما سيشكل مشكلة إجرائية بشأن كافة الجرائم وليس الجرائم المعلوماتية فحسب[١].

وفيما يلي نتناول أبرز آليات التعاون الدولي التي أشار إليها القانون، متمثلة في تبادل المعلومات والمساعدة القضائية، وذلك على النحو التالي:-

---

[١] انظر: دراسة مكتب الأمم المتحدة المعني بالمخدرات والجريمة بعنوان:" دراسة شاملة عن الجريمة السيبرانية"، مرجع سابق، صxv.

أهمية التعاون الدولي في مجال جرائم تقنية المعلومات: نظراً للطابع عبر الوطني لجرائم تقنية المعلومات، استلزمت إجراءات مُكافحتها ضرورة تضافر الجهود الدولية وتعزيز التعاون الدولي بين دول العالم في مجال مواجهة هذه الجرائم، ولاشك في أن المواجهة الفعالة لهذه الجرائم تتحقق من خلال تفعيل التعاون الدولي في المسائل الجنائية[١]، وترجع أهمية التعاون الدولي في مكافحة جرائم تقنية المعلومات إلى الطبيعة الخاصة لجريمة تقنية المعلومات كجريمة عبر وطنية، تتطلب تحقيقات سريعة تتسم بالخبرة والتعاون غير المسبوق، وهو ما يتطلب ضرورة تعاون أجهزة إنفاذ القانون بصورة سريعة وفعالة عبر الحدود الوطنية[٢].

علاوة على اقتصار نطاق انطباق القواعد الجنائية على إقليم الدولة (مبدأ إقليمية القاعدة الجنائية)، وهو ما يترتب عليه صعوبات إجرائية في مواجهة هذه الجرائم، تتمثل في عدم إمكانية السلطات القضائية بالدولة مباشرة بعض الأعمال القضائية الإجرائية داخل أقاليم الدول الأخرى كإجراءات التفتيش والضبط إلى غير ذلك من الإجراءات الجنائية[٣]، فغالباً ما تتضمن معظم الاتفاقيات الدولية نصوصاً تقتضي ضرورة اللجوء إلى المُساعدة القضائية المُتبادلة بهدف تحقيق السرعة والفعالية في إجراءات الملاحقة للجناة[٤].

---

[١] أنظر: ديباجة الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية، بودابست، ٢٠٠١/١١/٢٣.

[٢] كريستوفر بينتر: التهديد الذي تفرضه الجريمة المعلوماتية والحاجة إلى التعاون الدولي، مرجع سابق، ص٦٦.

[٣] المستشار. البشري الشوربجي: أفاق وآليات التعاون الدولي ضد الجريمة، مجلة القضاة الفصلية، السنة ٥٣، ٢٠٠٣، نادي القضاة المصري، القاهرة، ص١٠.

[٤] د. جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، مرجع سابق، ص٧٩.

ويمكن التمييز في مسائل التعاون الدولي بين التعاون الدولي الأمني والذي يشمل تبادل المعلومات بين جهات إنفاذ القانون، والتعاون الدولي القضائي بين جهات التحقيق والمحاكمة، وهو ما سنتناوله على النحو التالي:-

أولاً- التعاون الدولي في مجال تبادل المعلومات: يعد تبادل المعلومات في مجال جرائم تقنية المعلومات من أبرز صور التعاون الدولي في مواجهتها، وهو قد يتم بشكل ثنائي أو متعدد الأطراف، من خلال المنظمة الدولية للشرطة الجنائية أو غيرها من الأجهزة النظيرة على الصعيد الإقليمي كاليوروبول والأفريبول والمكتب العربي لمكافحة الجريمة، ويقصد بتبادل المعلومات التعاون الدولي الأمني، والذي يتم من خلال تبادل المعلومات بين الأجهزة الأمنية حول الأنشطة الإجرامية التي يباشرها مجرمو المعلوماتية، بهدف تحقيق تعاون أمني فعال في مواجهتها.

وبالنظر إلى الطبيعة الخاصة للجرائم المعلوماتية، فإن التعاون الدولي في مكافحتها لا ينبغي أن يقتصر على التعاون الدولي الأمني في مجال تبادل المعلومات، والتعاون الدولي القضائي في مجال الإنابة القضائية وتسليم المجرمين، وإنما يتطلب الأمر التعاون الدولي في مجال تدريب الكوادر الأمنية والقضائية على كشف وتحقيق جرائم تقنية المعلومات، وقد اهتم المجتمع الدولي بتفعيل التعاون الدولي في مجال مكافحة هذه الطائفة من الجرائم من خلال عدة حلول، أبرزها: اتفاقية بودابست، والقرار الإطاري الخاص بالاتحاد الأوروبي، والأنشطة التشريعية وأنشطة بناء القدرات في مجال المكافحة، والتي تدعمها بعض المنظمات الدولية الإقليمية كمنظمة الدول الأمريكية، ومجموعة دول أسيا والباسيفيك، فضلاً عن جهود مجموعة العمل الدولية المعنية بالتدريب على الجريمة المعلوماتية، وجهود المنظمة الدولية للشرطة الجنائية "الإنتربول"[1].

[1] كريستوفر بينتر: مرجع سابق، ص٦٦.

ثانياً- التعاون القضائي الدولي في جرائم تقنية المعلومات: يتمثل التعاون القضائي الدولي في مجموعة الوسائل القانونية، والتي بواسطتها تقدم إحدى الدول معاونة سلطتها العامة أو مؤسساتها القضائية إلى سلطة التحقيق أو الحكم أو التنفيذ في دولة أخرى[١]، أو ما يعرف بالمُساعدة القضائية والتي تعد كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم[٢]، ومن أبرز صور المساعدة القضائية الدولية في جرائم تقنية المعلومات الإنابة القضائية وتسليم المجرمين[٣]، وذلك على النحو التالي:-

١) الإنابة القضائية: تُعد الإنابة القضائية إحدى صور المُساعدة القضائية للتعاون الدولي، فهي تؤدي إلى تمكين دولة ما من الاستفادة من السلطات العامة أو الهيئات القضائية لدولة أخرى، إذا ما حالت الحدود الإقليمية دون نفاذ قانونها تجاه الجاني[٤]، ويعرف الفقه الجنائي الإنابة القضائية بأنها طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية، تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها لضرورة ذلك للفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة، ويتعذر عليها القيام به بنفسها[٥]، فالإنابة القضائية تعد من الإجراءات المسهلة لمباشرة الإجراءات الجنائية في النطاق الدولي، والتي تساعد على التغلب على عقبة السيادة الإقليمية، بما يكفل إنهاء إجراءات التحقيق والمحاكمة في الدعوى الجنائية.

---

[١] د. حسنين عبيد: القضاء الجنائي الدولي، دار النهضة العربية، القاهرة، ١٩٧٧، ص ص٩٩، ١٠٠.

[٢] المرجع السابق، ص١٤٠.

[٣] يعرف القانون الجنائي العديد من آليات التعاون الدولي من أبرزها تسليم المجرمين، والمساعدة القضائية المتبادلة ونقل الإجراءات الجنائية ونقل المحكوم عليهم.

[٤] د. عبد الرحيم صدقي: التعاون الدولي في الفكر المُعاصر، مجلة القانون والاقتصاد، مطبعة جامعة القاهرة، ١٩٨٣، ص٢٤٩.

[٥] د. عبد الرؤوف مهدي: شرح القواعد العامة للإجراءات، مرجع سابق، ص١٠٢.

شروط تطبيق الإنابة القضائية: يشترط لتنفيذ الإنابات القضائية بين الدول عدة شروط، من أبرزها:-

١- وجود اتفاقيات دولية ثنائية أو جماعية، تجيز اتخاذ السلطات القضائية لإجراءات الإنابة القضائية.

٢- قيام السلطات القضائية المختصة بإرسال الملف الخاص بالدعوى الجنائية بمرفقاته من مستندات ووثائق ومحاضر تحقيق، والتي تم إجرائها بمعرفة السلطة القضائية في الدولة المطلوب فيها اتخاذ بعض إجراءات التحقيق، وهي تتشابه في ذلك مع إجراءات ندب مأموري الضبط القضائي بإجراء من إجراءات التحقيق نيابةً عن المحقق وبناءً على طلبه[١].

الإطار الدولي للإنابة القضائية في جرائم تقنية المعلومات: يلاحظ الفقه الجنائي خلو القانون المصري من تنظيم لمسألة إجراءات الإنابة القضائية، إذ يعتمد الأمر فحسب على الأحكام الخاصة بالاتفاقيات الدولية ذات الشأن التي انضمت إليها مصر، وبموجب هذه الاتفاقيات، فإن الدولة المطلوب منها الإنابة تتولى طبقاً لتشريعها تنفيذ الإنابة القضائية المتعلقة بالقضايا الجنائية، حيث يتم إرسال طلبات الإنابة القضائية إلى الدولة المطلوب إليها بطريقين: من خلال مكتب التعاون الدولي بوزارة العدل أو عن الطريق الدبلوماسي[٢]، وفيما يلي نتناول أحكام الإنابة القضائية في إطار اتفاقيتي بودابست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات بالإيجاز التالي:-

---

[١] د. سالم محمد سليمان الأوجلي: أحكام المسئولية الجنائية عن الجرائم الدولية في التشريعات الوطنية- دراسة مقارنة، رسالة دكتوراه، جامعة عين شمس، ١٩٩٧، ص٢٤٩.

[٢] د. جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، مرجع سابق، ص٨٤.

أ) المساعدة المتبادلة في اتفاقية بودابست (الأوروبية): تخضع المساعدة المتبادلة لقانون الدولة المطلوب منها المساعدة أو اتفاقية المساعدة واجبة التطبيق، ولا يجوز رفض المساعدة على أساس أن الجريمة تعتبر جريمة مالية، ويعتبر هذا الشرط مستوفى في حالة وجود جريمة مزدوجة، ويجوز لأطراف هذه الاتفاقية إخطار الأطراف الأخرى، في حالة وجود أو بسبب تحقيق يجرى، بمعلومات قد يساعده في البدء بالتحقيق أو اتخاذ إجراءات بصدد جرائم تتعلق بهذه الاتفاقية، وعلى الطرف المتلقي الحفاظ على سرية هذه المعلومات، وفي حالة العكس عليه إخطار الطرف المعطى للمعلومات لكي يقرر ما إذا كان ينبغي تقديم هذه المعلومات من عدمه، وقد أفردت المادة (٢٧) من الاتفاقية الإجراءات المتعلقة بالمساعدة القضائية في حالة عدم وجود اتفاقية دولية واجبة التطبيق بشأن الطلبات المساعدة المتبادلة، ذكرت فيها بعض أسباب الرفض مثل إذا ما تعلق الطلب بجريمة سياسية، أو أن تنفيذ الطلب يمس السيادة أو الأمن أو النظام العام.

ب) المساعدة المتبادلة في الاتفاقية العربية: أشارت نصوص الاتفاقية العربية إلى أحكام المساعدة المتبادلة في نطاق جرائم تقنية المعلومات، حيث نصت المادة (٣٢) على حث الدول الأطراف على تقديم المساعدة المتبادلة لغايات التحقيق، وجمع الأدلة في الجرائم المعلوماتية، وقد اشترطت المادة ضرورة تقديم طلب خطي للمساعدة المتبادلة على أن تخضع شروط المساعدة لقانون الدولة المطلوب منها المساعدة، كما نصت المادة (٣٣) على جواز إعطاء أية معلومات حصلت عليها الدولة أثناء التحقيقات إلى دولة أخرى طرف في الاتفاقية، بالإضافة إلى اتخاذ الإجراءات الخاصة بتحديد سلطة محددة تختص بإجراءات المساعدة المتبادلة، كما أشارت الاتفاقية إلى حق الدولة في رفض المساعدة في حالة الجرائم ذات الطابع السياسي أو إذا كانت المساعدة تمثل انتهاكاً لأمن هذه الدولة (م٣٥).

٢) تسليم المجرمين: عرف الفقه الجنائي تسليم المجرمين بأنه:" تخلي دولة لأخرى عن شخص ارتكب جريمة لكي تحاكمه عنها أو لتنفذ فيه الحكم الذي أصدرته عليه محاكمها، وذلك باعتبار أن الدولة طالبة التسليم هي صاحبة الاختصاص الطبيعي أو الأولى بمحاكمته وعقابه"[١]،ويتم التسليم وفق الشروط المتفق عليها في الاتفاقيات بين الدول، وفي حدود القوانين الداخلية التي تنظم إجراءات التسليم، فإن لم توجد معاهدة تسليم أو نص في القانون الداخلي أتبع في التسليم ما استقر عليه العرف الدولي، ويبقى التسليم دوماً اختيارياً إذا لم يكن بين الدولتين معاهدة أو اتفاق دولي، وإن شاءت نصت على شرط المعاملة بالمثل[٢].

ويقدم طلب التسليم بين حكومتين – وفقاً للمجرى العادي للأمور– بالطريق الدبلوماسي ماعدا الحالات الاستثنائية يمكن تقديمه من خلال السلطات القضائية في الدولة الطالبة إلى السلطات المعنية في الدولة المطلوب إليها، ويعقب تقديم الطلب أن تصدر الدولة المطلوب إليها أمراً بحبس الشخص المطلوب احتياطياً لحين البت في الطلب وعلى الدولة الطالبة أن تقدم الأدلة والمستندات التي تؤيد طلبها[٣].

أ) تسليم المجرمين في اتفاقية بودابست (الأوروبية): نصت الاتفاقية على انطباقها في حالة إذا ما كانت الجرائم المنصوص عليها في هذه الاتفاقية معاقب عليها بموجب قوانين كلا من الطرفين المعنيين بعقوبة مقيدة للحرية لمدة سنة على الأقل أو

---

[١] د. عمر السعيد رمضان: شرح قانون العقوبات- القسم العام، دار النهضة العربية، القاهرة، ص١٢١؛ د. عبد الفتاح محمد سراج: النظرية العامة لتسليم المجرمين- دراسة تحليلية تأصيلية، رسالة دكتوراه، جامعة المنصورة، ١٩٩٩، ص٦٥.

[٢] د. إيهاب محمد يوسف: إشكاليات تسليم المتهمين بانتهاك مبادئ القانون الدولي الإنساني (اتجاهات التنظير– مقترحات المواجهة)، مجلة كلية الدراسات العليا، العدد (١١)، يوليو ٢٠٠٤، ص١٦٦.

[٣] المرجع السابق، ص١٦٨.

بعقوبة أشد، وتطبق العقوبة الأقل فى حالة إذا ما كان توجد تشريعات موحدة، أو متبادلة بالمثل، أو بموجب اتفاقية تسليم. وقد اعتبرت الاتفاقية الجرائم المنصوص عليها فى (المواد٢-١٣) من الجرائم التى يجب تسليم المجرمين فيها، إذا ما وجدت اتفاقية لتسليم المجرمين بين الأطراف. وفى حالة عدم وجود اتفاقية تسليم مجرمين بين الأطراف، يجوز اعتبار هذه الاتفاقية الأساس القانوني لعملية التسليم، وبالنسبة للدول التي لا تجعل تسليم المجرمين مشروط على اتفاقية تسليم فإنهم بانضمامهم لهذه الاتفاقية يعتمدون الجرائم المنصوص عليها في الاتفاقية كجرائم يجوز فيها تسليم المجرمين، ويخضع تسليم المجرمين لقانون الدولة المطلوب منها التسليم أو اتفاقية تسليم المجرمين واجبة التطبيق.وفى حالة الرفض بسبب الجنسية أو الاختصاص القضائي، فإن الدولة المراد التسليم منها أن تحيل الدعوى لسلطاتها المختصة، وإبلاغ النتيجة للطرف للدولة الطالبة، وعلى الدول عند التوقيع أن تخطر السكرتير العام لمجلس أوروبا باسم السلطة المسئولة عن طلبات التسليم.

ب) تسليم المجرمين في الاتفاقية العربية: نصت الاتفاقية العربية على إجراء تسليم المجرمين، وقد أشارت المادة (٣١) من الاتفاقية إلى جواز الاعتداد بالاتفاقية كأساس قانوني بين الدول الأطراف في مسألة تسليم المجرمين، وحددت شروط التسليم بألا تكون الجريمة المطلوب فيها التسليم لا تقل عقوبتها عن عقوبة سالبة للحرية لمدة سنة أو أكثر، فضلاً عن خضوع التسليم للشروط المنصوص عليها في الدولة التي يقدم إليها طلب التسليم، مع تقرير حق الدول الأطراف في رفض طلب التسليم مع التعهد بتوجيه الاتهام للجناة الذين يرتكبون جرائم معاقب عليها وفقا لقانون الدولتين بعقوبة لا تقل عن سنة أو بعقوبة أشد لدى أي من الدولتين.

الخاتمـة

استعرضنا خلال السطور السابقة موضوع رؤية تحليلية لأحكام قانون مكافحة جرائم تقنية المعلومات المصري رقم (١٧٥) لسنة ٢٠١٨، والذي تناولنا فيه في مطلب تمهيدي وثلاثة مباحث: موقف التشريع المصري والمقارن من مكافحة الجرائم المعلوماتية، والأحكام العامة والموضوعية والإجرائية لقانون مكافحة جرائم تقنية المعلومات، وقد تمخضت الدراسة عن عدد من النتائج والتوصيات على النحو التالي:-

أولاً- النتائج: تتبلور أبرز النتائج التي انتهى إليها البحث، فيمايلي:-

١- تأخر المشرع المصري في إصدار قانون مكافحة الجرائم المعلوماتية.

٢- حسناً فعل المشرع المصري بإصدار القانون رقم (١٧٥) لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات والذي يمثل الغطاء التشريعي لمواجهة الجرائم المعلوماتية.

٣- تضمن القانون لعدد من الأحكام العامة والموضوعية والإجرائية ذات الصلة بمكافحة الجرائم المعلوماتية.

٤- وجوب الوضع في الاعتبار تطبيقات ونظم الذكاء الاصطناعي والعمل على توافق قواعد القانون الجنائي مع مثل هذه التطبيقات المستحدثة وبصفة خاصة قواعد المسئولية الجنائية المرتبة على الأخطاء الناجمة عن هذه التطبيقات والنظم.

ثانياً- التوصيات: تتمثل أبرز التوصيات التي يقترحها الباحث فيمايلي:-

١- وجوب سعي المجتمع الدولي إلى صياغة صك دولي أممي لمواجهة جرائم تقنية المعلومات على غرار الصكوك الدولية النظيرة لمكافحة الجريمة المنظمة والفساد.

٢- توجيه نظر المشرع المصري نحو إضافة تعاريف لكل من الجريمة المعلوماتية والجماعة الإجرامية المنظمة والجريمة عبر الوطنية ضمن التعاريف الواردة بقانون مكافحة جرائم تقنية المعلومات.

٣- توجيه نظر المشرع المصري نحو تعديل قانون مكافحة جرائم تقنية المعلومات بإضافة نص يجيز تجريم تعديل بيانات المرضى عبر شبكة المعلومات الدولية.

٤- توجيه نظر المشرع المصري نحو تعديل قانون مكافحة جرائم تقنية المعلومات بإضافة نص يجيز تجريم عمليات التزوير الإلكتروني.

٥- توجيه نظر المشرع المصري نحو تعديل قانون مكافحة جرائم تقنية المعلومات بإضافة نص يجيز تجريم استعمال البيانات الإلكترونية المزورة.

٦- توجيه نظر المشرع المصري نحو تعديل قانون مكافحة جرائم تقنية المعلومات بإضافة نص يجيز تجريم الاحتيال المعلوماتي.

٧- توجيه نظر المشرع المصري نحو تعديل قانون مكافحة جرائم تقنية المعلومات بإضافة نص يجيز تجريم التحريض على ممارسة الدعارة والفجور عبر الشبكة المعلوماتية.

٨- توجيه نظر المشرع المصري نحو تعديل قانون مكافحة جرائم تقنية المعلومات بإضافة نص يجيز تجريم اصطناع أو حيازة صور أو رسوم مخلة بالآداب العامة.

٩- توجيه نظر المشرع المصري نحو تعديل قانون مكافحة جرائم تقنية المعلومات بإضافة نص يجيز تجريم توفير أو تسهيل الوصول لمواد مخلة بالحياء أو النظام العام والآداب.

١٠- توجيه نظر المشرع المصري نحو تعديل قانون مكافحة جرائم تقنية المعلومات بإضافة نص يجيز تجريم نشر المصنفات الفكرية عبر شبكة الإنترنت بدون تصريح من صاحب الحق فيها.

١١- توجيه نظر المشرع المصري نحو تعديل قانون مكافحة جرائم تقنية المعلومات بإضافة نص يجيز تجريم عدم الإبلاغ عن جرائم تقنية المعلومات.

١٢- توجيه نظر المشرع المصري نحو تعديل قانون مكافحة جرائم تقنية المعلومات بإضافة نص يجيز تجريم عمليات غسل الأموال عبر شبكة الإنترنت.

١٣- توجيه نظر المشرع المصري نحو تعديل قانون مكافحة جرائم تقنية المعلومات بإفراد نص منفصل بكل من جريمة انتهاك حرمة الحياة الخاصة وجريمة إغراق البريد الإلكتروني للمجني عليه بالرسائل وبجريمة الاعتداء على المبادئ والقيم الأسرية، فصلاً للنص التجريمي الواحد، لتمايز كل صورة إجرامية عن النموذج القانوني للجريمة الأخرى.

١٤- توجيه نظر المشرع المصري نحو تضمين تعريف لجريمة تقنية المعلومات والجماعة الإجرامية المنظمة والجريمة ذات الطابع عبر الوطني ضمن التعاريف الواردة بالقانون، بالنظر إلى ذيوع استخدام جماعات الجريمة المنظمة للتقنيات المستحدثة في ارتكاب أنشطتها الإجرامية لاسيما جرائم تقنية المعلومات.

ملحق

مشروع قانون ( ) لسنة

بتعديل بعض أحكام القانون رقم (١٧٥) لسنة ٢٠١٨م

المادة الأولى- يضاف إلى نصوص القانون ١٧٥ لسنة ٢٠١٨م المواد التالية:-

مادة (١): تعاريف

جرائم تقنية المعلومات: الجرائم التي تكون المعلومات إما محلاً لها أو أداة في ارتكابها.

الجماعة الإجرامية المنظمة: الجماعة المؤلفة وفق تنظيم معين من ثلاثة أشخاص علي الأقل للعمل بصفة مستمرة أو لمدة من الزمن بهدف ارتكاب جريمة محددة أو أكثر من بينها الجرائم المنصوص عليها في هذا القانون وذلك من أجل الحصول بشكل مباشر أو غير مباشر علي منفعة مادية أو معنوية.

الجريمة ذات الطابع عبر الوطني: أية جريمة ارتكبت في أكثر من دولة، أو ارتكبت في دولة واحدة وتم الإعداد أو التخطيط لها أو التوجيه أو الإشراف عليها أو تمويلها في دولة أخرى أو بواسطتها، أو ارتكبت في دولة واحدة عن طريق جماعة إجرامية منظمة تمارس أنشطة إجرامية في أكثر من دولة، أو ارتكبت في دولة واحدة وكانت لها آثار في دولة أخرى.

مادة (٢): يعاقب بالحبس الذي لا تقل مدته عن سنتين كل من عدل أو أتلف الفحوص الطبية، أو التشخيص الطبي، أو العلاج الطبي، أو الرعاية الطبية، أو سهل للغير فعل ذلك، أو مكنه منه، باستعمال الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.

مادة (٣): يعاقب بالحبس مدة لا تقل عن ثلاث سنوات والغرامة التي لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز سبعمائة ألف جنيه أو بإحدى هاتين العقوبتين، كل من ارتكب تزويراً مادياً أو معنوياً بأية وسيلة كانت في البيانات والمعلومات الإلكترونية المخزنة في نظام المعلومات الإلكتروني أو المسجلة على اسطوانات أو شرائط ممغنطة، وذلك بقصد تغيير الحقيقة فيها إضراراً بالشخص المعني أو المتحكم في البيانات والمعلومات الإلكترونية أو المتحكم في نظام المعلومات الإلكتروني. وتكون العقوبة الحبس والغرامة، إذا وقع التزوير من المتحكم في البيانات والمعلومات الإلكترونية أو المتحكم في نظام المعلومات الإلكتروني. وتكون العقوبة السجن والغرامة إذا كان التزوير في البيانات والمعلومات الإلكترونية التي تتعلق بأمن الدولة أو بمصلحة اقتصادية عامة أو بأي مصلحة عامة أخرى.

مادة (٤): يعاقب بذات العقوبات المنصوص عليها في المادة السابقة، كل من استخدم البيانات والمعلومات الإلكترونية المزورة أو استفاد منها بأي طريقة وهو عالم بتزويرها.

مادة (٥): يعاقب بالحبس مدة لا تقل عن سنتين أو بالغرامة التي لا يقل حدها الأدنى عن عشرين ألف جنيه ولا تجاوز مائتي ألف جنيه أو بالعقوبتين معاً، كل من توصل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات أو ما في حكمها إلى الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه.

مادة (٦): يعاقب بالحبس مدة لا تقل عن سنة ولا تزيد عن ثلاث سنوات والغرامة التي لا يقل مقدارها عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه، من

حرض شخصاً أو أغواه لارتكاب الدعارة أو الفجور أو ساعده على ذلك باستخدام الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو ما في حكمها. فإن كان المجني عليه حدثاً كانت العقوبة الحبس الذي لا تقل مدته عن سنتين والغرامة التي لا يقل مقدارها عن عشرين ألف جنيه ولا تجاوز مائتي ألف جنيه.

مادة (٧): يعاقب بالحبس والغرامة التي لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه أو بإحدى هاتين العقوبتين، كل من اصطنع أو قلد أو حصل أو حاز بقصد العرض أو التوزيع أو النشر أو البيع صوراً أو رسوماً مُعالجة إلكترونياً مخلة بالآداب العامة، أو أدار مكاناً لذلك. وتكون العقوبة الحبس الذي لا تقل مدته عن سنة ولا تجاوز خمس سنوات والغرامة التي لا تقل عن سبعمائة ألف جنيه ولا تجاوز مليون جنيه أو بإحدى هاتين العقوبتين، إذا كانت الرسوم لأطفال عراه أو في أوضاع جنسية.

مادة (٨): يعاقب بالحبس والغرامة التي لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه، كل من وفر أو سهل عمداً أو بإهمال عن طريق شبكة المعلومات أو أحد أجهزة الحاسب الآلي أو ما في حكمها للوصول لمحتوى مخل بالحياء أو منافٍ للنظام العام أو الآداب. وإذا وجه الفعل المشار إليه إلى حدث، يعاقب مرتكبها بالحبس الذي لا تقل مدته عن سنتين، والغرامة التي لا يقل مقدارها عن عشرين ألف جنيه ولا تجاوز مائتي ألف جنيه.

مادة (٩): مع مراعاة الأحكام المنصوص عليها في قانون حماية الملكية الفكرية، يعاقب بالحبس أو الغرامة أو بالعقوبتين معاً، كل من نشر أو نسخ دون وجه حق عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو ما في حكمها أي مصنفات فكرية أو أدبية أو أبحاث علمية أو ما في حكمها بدون إذن أو تصريح من صاحب الحق فيها. فإذا كان النشر أو النسخ بقصد التسويق أو الربح تكون العقوبة

الحبس الذي لا تقل مدته عن سنة واحدة والغرامة التي لا يقل حدها الأدنى عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه.

مادة (١٠): يُعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز عشرين ألف جنيه أو بإحدى هاتين العقوبتين، كلمن علم بارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو بالشروع فيها ولم يبلغ السلطات المختصة بذلك، فإذا كان الجاني موظفاً عاماً ووقعت الجريمة إخلالاً بواجبات وظيفته كان الحد الأقصى للحبس خمس سنوات. وللمحكمة الإعفاء من العقاب إذا كان المتخلف عن الإبلاغ زوجاً للجاني أو كان من أحد أصوله أو فروعه أو إخوته أو أخواته.

مادة (١١): مع مراعاة الأحكام المنصوص عليها في قانون غسل الأموال، يعاقب بالسجن مدة لا تقل عن خمس سنوات أو بالغرامة التي لا يقل مقدارها عن مائة ألف جنيه أو بالعقوبتين معاً، كل من قام بتحويل الأموال غير المشروعة أو نقلها أو تمويه المصدر غير المشروع لها أو إخفائه أو قام باستخدام أو اكتساب وحيازة الأموال مع العلم بأنها مستمدة من مصدر غير مشروع أو بتحويل الموارد أو الممتلكات مع العلم بمصدرها غير المشروع، وذلك عن طريق استخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد إضفاء الصفة المشروعة على تلك الأموال أو أنشأ أو نشر معلومات أو موقعاً لارتكاب أي من هذه الأفعال.

قائمة المراجع

أولاً- باللغة العربية

١) المراجع العامة

- **أحمد فتحي سرور: الوسيط في شرح قانون الإجراءات الجنائية، دار النهضة العربية، ط٧، ١٩٩٦.**
- **حسن صادق المرصفاوى: أصول الإجراءات الجنائية، منشأة المعارف، الإسكندرية، ١٩٨٢.**
- **حسنين عبيد: شرح قانون العقوبات- القسم الخاص، دار النهضة العربية، القاهرة، ط٩، ٢٠٠٩.**
- **عبد الرؤوف مهدي: شرح القواعد العامة للإجراءات الجنائية وفقاً لآخر التعديلات، دار النهضة العربية،٢٠٠٨.**
- **عبد العظيم وزير: شرح قانون العقوبات- القسم العام، النظرية العامة للجريمة- الجزء الأول، دار النهضة العربية، القاهرة.**
- **عمر السعيد رمضان: شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، ١٩٨٦.**
- **مأمون محمد سلامة: " الإجراءات الجنائية في التشريع المصري"، دار النهضة العربية، القاهرة،٢٠٠٣.**

- محمد أبو العلا عقيدة: - شرح قانون الإجراءات الجنائية، ج١، ط١، دار النهضة العربية، ٢٠٠١.

- شرح قانون الإجراءات الجنائية، ج٢، دار النهضة العربية، ٢٠٠٠.

- محمد زكى أبو عامر: الإجراءات الجنائية، دار منشأة المعارف، الإسكندرية، غير مذكورة سنة النشر، الطبعة الثانية.

- محمد عبد اللطيف فرج: - شرح قانون الإجراءات الجنائية وفقاً لأحدث التعديلات التشريعية، ج١، ط٣، ٢٠١١.

- شرح قانون الإجراءات الجنائية في جمع الاستدلالات والتحقيق الابتدائي، ط٢، القاهرة، ٢٠١٠.

- محمود نجيب حسنى: شرح قانون الإجراءات الجنائية، دار النهضة العربية الطبعة الثانية، ١٩٨٨.

٢)- المراجع المتخصصة

- آمال عبد الرحيم عثمان: الخبرة في المسائل الجنائية، رسالة دكتوراه، جامعة القاهرة، ١٩٦٤.

- أحمد محمود محمد مصطفى: الجريمة المعلوماتية وسبل مُكافحتها، ورقة عمل مقدمة ندوة الواقع الأمني مسئوليات – إنجازات، مركز بحوث الشرطة- أكاديمية الشرطة، ورشة العمل الرابعة، يوم ٢٠١١/١/٩، ص١.

- أر. بنيـــدجامين و بـــي جلادمـــان و بـــي رانـــدل: حمايـة أنظمـة تكنولوجيـا المعلومـات ضـد الجريمـة المعلوماتيـة، ورقـة عمـل مقدمـة للمـؤتمر الـدولي السادس حول الجريمة المعلوماتية، القاهرة،١٣-١٥ أبريل٢٠٠٥، ترجمة مركز بحوث الشرطة.

- إســماعيل عبــد النبــي شاهين: أمن المعلومات في الإنترنت بين الشريعة والقانون، مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية،٢٠٠٠.

- أشــرف توفيــق شــمس الدين: مخـاطر العمـلات الافتراضـية فـي نظـر الـسياسة الجنائية، بحث مقدم للمؤتمر الدولي الخامس عشر لكلية الشريعة والدراسات الإسلامية بجامعة الشارقة بعنوان (العملات الافتراضية في الميزان)، الشارقة، دولة الإمارات العربية المتحدة.

- إيمـــان شـــريف قائـــد: الجريمـة المعلوماتيـة وأبعادهـا أحـد أنمـاط الجـرائم المستحدثة، ورقة عمل مقدمة لندوة الواقع الأمني مسئوليات- إنجازات، مركز بحوث الشرطة بأكاديمية الشرطة، القاهرة،٢٠١١/١/٩.

- أيمـــن عبـــد الحفـــيظ: إستراتيجية مكافحة الجرائم الناشئة عن استخدام الحاسب الآلي، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة.

- إيهاب محمد يوسف: إشكاليات تسليم المتهمين بانتهاك مبادئ القانون الدولي الإنساني (اتجاهات التنظير – مقترحات المواجهة)، مجلة كلية الدراسات العليا، العدد (١١)، يوليو ٢٠٠٤.

- باسكال هتيز شولدت: إنشاء مركز وطني يختص بجرائم التقنية الفائقة، المؤتمر الدولي السادس للجرائم المعلوماتية، ترجمة مركز بحوث الشرطة، ٢٠٠٥.

- باسم منصور: الآليات الأمنية لمواجهة جرائم الحاسب والإنترنت، مجلة مركز بحوث الشرطة، عدد (٣٥)، يناير ٢٠٠٩.

- تامر الدمياطي: صور الجرائم المضرة بسلامة التوقيع والمحرر الإلكتروني، ورقة عمل مقدمة لندوة المواجهة الأمنية للجرائم المعلوماتية التي عقدت بمركز بحوث الشرطة، أكاديمية الشرطة، القاهرة،٧أبريل ٢٠٠٩.

- جان ميشيل لوبوتان: كلمة المنظمة الدولية للإنتربول أثناء المؤتمر الدولي السادس للجرائم المعلوماتية، ١٣-٢٠٠٥/٤/١٥، القاهرة، إصدارات مركز بحوث الشرطة.

- جمال توفيق وآخرون: دراسة مركز بحوث الشرطة حول الجرائم المعلوماتية وطرق مواجهتها، مركز بحوث الشرطة، أكاديمية الشرطة، الإصدار الثالث، يونيو ٢٠٠٥، القاهرة.

- جميل عبد الباقي الصغير: - الحماية الجنائية لبطاقات الائتمان الممغنطة، دراسة تطبيقية في القضاء الفرنسي والمصري، دار النهضة العربية،١٩٩٢.

- الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ١٩٩٩.

- الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية،٢٠٠٢.

-القانون الجنائي والإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٢.

- حسني الجندي: التشريعات الجنائية الخاصة في دولة الإمارات العربية المتحدة، الكتاب الثالث- قانون مكافحة جرائم تقنية المعلومات في دولة الإمارات العربية المتحدة، ط١، ٢٠٠٩.

- حسنين عبيد: القضاء الجنائي الدولي، دار النهضة العربية، القاهرة، ١٩٧٧.

- رأفت رضوان: عالم التجارة الإلكترونية، المنظمة العربية للعلوم الإدارية، القاهرة، ١٩٩٩.

- رامي متولي القاضي: - الجرائم المعلوماتية وطرق مواجهتها، ورقة عمل مُقدمة لمؤتمر الجرائم المُستحدثة – كيفية إثباتها

ومواجهتها، المركز القومي للبحوث الاجتماعية والجنائية، يومي ١٥-١٦/١٢/٢٠١٠.

- دور وزارة الداخلية في مكافحة الجرائم المعلوماتية، ورقة عمل مُقدمة لندوة الواقع الأمني مسئوليات-إنجازات، مركز بحوث الشرطة- أكاديمية الشرطة، ورشة العمل الرابعة، القاهرة، يوم ٢٠١١/١/٩.

- رانجان راجيش: تعليق حول التوصيات الصادرة عن المؤتمر السابق،ورقة عمل مقدمة للمؤتمر الدولي السادس للجرائم المعلوماتية، إصدارات مركز بحوث الشرطة،١٣-١٥/٤/٢٠٠٥،القاهرة،٢٠٠٥.

- ساتو تاكاشي جارسيا: مقترح بإجراء التحقيق الدولي المشترك، المؤتمر الدولي السادس للجرائم المعلوماتية، ترجمة مركز بحوث الشرطة، ٢٠٠٥.

- سالم محمد سليمان الأوجلي: أحكام المسئولية الجنائية عن الجرائم الدولية في التشريعات الوطنية – دراسة مقارنة، رسالة دكتوراه، جامعة عين شمس، ١٩٩٧.

- سليمان أحمد فضل: البعد الدولي للجرائم المعلوماتية وطرق مواجهتها، ورقة عمل مقدمة لندوة الواقع الأمني مسئوليات – إنجازات، مركز بحوث الشرطة بأكاديمية الشرطة،

القاهرة، ٢٠١١/١/٩.

- سيـــــــسيليا فانـــــــت: مـشروع "نـيكس"- مـشروع إسـتخبار عمليـاتي سويدي يركز على عمليات الاتجار في المخدرات عبر شـبكة الإنترنـت، المـؤتمر الـدولي الـسادس للجـرائم المعلوماتية، ترجمة مركز بحوث الشرطة، ٢٠٠٥.

- عبـــد الـــرحيم صـــدقي: التعـاون الـدولي فـي الفكـر المُعاصـر، مجلـة القـانون والاقتصاد، مطبعة جامعة القاهرة، ١٩٨٣.

- عبـد الفتـاح محمـد سـراج: النظريـة العامـة لتـسليم المجـرمين- دراسـة تحليليـة تأصيلية، رسالة دكتوراه، جامعة المنصورة، ١٩٩٩.

ج

- عفيفـــى كامـــل عفيفـــى: جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، مكتبة الأهرام، القاهرة، ٢٠٠٠.

- على عبد القادر القهوجي: الحمايـة الجنائيـة لبـرامج الحاسـب، دار الجامعـة الجديدة للنشر، الإسكندرية، ١٩٩٧.

- غنـــام محمـــد غنـــام: عدم ملائمـة القواعـد التقليديـة فـي قـانون العقوبـات لمكافحة جرائم الكمبيوتر، مؤتمر القـانون والكمبيـوتر والإنترنت، كليـة الـشريعة والقـانون، جامعـة الإمـارات العربية المتحدة، سنة ٢٠٠٠.

- فـــــــؤاد جمـــــــال: جـرائم الحاسـبات والإنترنـت – الجـرائم المعلوماتيـة، ورقـة عمـل مقدمـة لنـدوة المواجهـة الأمنيـة للجريمـة

المعلوماتية، مركز بحوث الشرطة، أكاديمية الشرطة بالقاهرة، ٢٠٠٩/٤/٧.

- فلينت ووترز: ـ مدخل للتعاون الإقليمي في مجال التحقيقات في جرائم استغلال الأطفال، المؤتمر الدولي السادس حول الجريمة المعلوماتية، القاهرة،١٣ـ١٥ أبريل٢٠٠٥، ترجمة مركز بحوث الشرطة.

ـ العملية متكافئة الدقة ـ ملاحقة تطور الجريمة ـ تطور التحقيقات السرية المتكافئة، ورقة عمل بذات المؤتمر.

- كارولين بووفي: البوت نتس ـ تهديد متنامي، تقرير من المملكة المتحدة، المؤتمر الدولي السادس للجرائم المعلوماتية، ترجمة مركز بحوث الشرطة، ٢٠٠٥.

- كريستوفر بينتر: التهديد الذي تفرضه الجريمة المعلوماتية والحاجة إلى التعاون الدولي، ورقة عمل مقدمة للمؤتمر الدولي السادس للجرائم المعلوماتية الذي نظمته المنظمة الدولية للشرطة الجنائية "الإنتربول"، القاهرة، ١٣ـ١٥/٤/٢٠٠٥، ترجمة مركز بحوث الشرطة.

- كينجي ميانيشي: شبكة الربط بين النقاط المرجعية الوطنية، ورقة عمل مقدمة للمؤتمر الدولي السادس للجرائم المعلوماتية،١٣ـ١٥/٤/٢٠٠٥، إصدار مركز بحوث

الشرطة، أكاديمية الشرطة، القاهرة.

- لـــــــويس ماتمـــــــان: حتمية المشاركة، ورقة عمل مقدمة للمؤتمر الدولي الســادس للجــرائم المعلوماتيـــة، القـــاهرة، ١٣-١٥/٤/٢٠٠٥، ترجمة مركز بحوث الشرطة.

- مـــاهر محمـــود أحمـــد الصالحى: " الجرائم المرتكبة عبر شبكة المعلومات الدولية " ورقة عمل مقدمة إلى ندوة " الأمن والإنترنت " التى نظمها مركز بحوث الشرطة بأكاديمية الشرطة بتاريخ ١٥/٦/٢٠٠٣م.

- مـــــــدحت زعتـــــــر: نحو إستراتيجية دولية لمكافحة الجرائم المعلوماتية، مجلة مركز بحوث الشرطة، بأكاديمية الشرطة، العدد التاسع، يناير ١٩٩٦.

- محـــــسن العبـــــودي: "المواجهة الأمنية لجرائم الإنترنت"، ورقة عمل منشورة على شبكة الإنترنت.

- محفـــوظ عبـــد الحكـــيم محفوظ: الجريمة المعلوماتية وأبعادها ومظاهرها الحديثة وما تشكله من أبعاد مستحدثة للجريمة بصفة عامة، ورقة عمـل مقدمـة نـدوة الواقـع الأمنـي مـسئوليات – إنجازات، مركز بحوث الشرطة- أكاديمية الشرطة، ورشة العمل الرابعة، يوم ٩/١/٢٠١١.

- محمـد أبـو العـلا عقيـدة: التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، ورقـة عمـل مقدمـة للمـؤتمر العلمـي الأول حـول

الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، ٢٦-٢٨ /٤/ ٢٠٠٣، دبي- الامارات العربية المتحدة.

- محمد سمير قانون العقوبات الاقتصادي، طبعة نادي القضاة، ٢٠١٩.

- محمد يوسف: التحديات التى تواجه التحقيقات فى الجرائم المعلوماتية وسبل مواجهتها، ورقة عمل مقدمة لندوة المواجهة الأمنية للجريمة المعلوماتية التي عقدت بمركز بحوث الشرطة، أكاديمية الشرطة بالقاهرة، ٧أبريل ٢٠٠٩.

- محمود على الركايبي: "دور الشرطة في مصر" (القاهرة – مكتبه ومطبعة مصطفى البابي الحلبي وأولاده – الطبعة الأولى ١٩٦٦م).

- مصطفى طاهر: المواجهة التشريعية لظاهرة غسل الأموال، مطابع الشرطة،القاهرة، ٢٠٠٢.

- ممدوح عبد الحميد عبد المطلب: جرائم استخدام شبكة المعلومات العالمية – الجريمة عبر الإنترنت، مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية، ٢٠٠٠.

- نائلة عادل محمد فريد جرائم الحاسب الاقتصادية - دراسة نظرية وتطبيقية،

قورة: دار النهضة العربية، القاهرة، ٢٠٠٤.

- نبيل عبد المنعم جاد: التحقيق والبحث الجنائي في جرائم الحاسب، مجلة كلية التدريب والتنمية، بأكاديمية الشرطة، العدد الأول، يوليو ١٩٩٩.

- نيجل جونز: ورقة عمل مقدمة إلى المؤتمر الدولى السادس حول الجريمة المعلوماتية، القاهرة من ١٣ – ١٥ إبريل ٢٠٠٥.

- هشام محمد توفيق: وسائل حماية المجتمع المدني من الجرائم المعلوماتية، ورقة عمل مقدمة لندوة المواجهة الأمنية للجرائم المعلوماتية.

- هشام محمد فريد رستم: -الجرائم المعلوماتية- أصول التحقيق الجنائي الفني، ورقة عمل مقدمة إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، مجلد٢.

- الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، ١٩٩٤.

- هدى حامد قشقوش: جرائم الحاسب الإلكتروني والتشريع المقارن، دار النهضة العربية،١٩٩٢.

- وليد سمير المعداوي: دور الشرطة في حماية الحياة الخاصة من أخطار المعلوماتية، رسالة دكتوراه، كلية الدراسات العليا،

٢٠١١.

- وليـــــد عـــــالكوم: مفهوم وظاهرة الإجرام المعلوماتي، مؤتمر"القانون والكمبيوتر والإنترنت"، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، مجلد٢.

- وليـــد نبيـــل طـــه: الجرائم الإلكترونية طبقاً لاتفاقية بودابست، ورقة عمل مقدمة لندوة الواقع الأمني مسئوليات – إنجازات، مركز بحوث الشرطة بأكاديمية الشرطة، القاهرة، ٢٠١١/١/٩، ورشة العمل الرابعة.

- يـــاب فـــان أوس: التهديدات الموجهة للبنية التحتية للمعلومات، ورقة عمل مقدمة للمؤتمر السادس للجرائم المعلوماتية، القاهرة، ١٣-١٥/٤/٢٠٠٥، ترجمة مركز بحوث الشرطة.

ثانياً- المراجع باللغة الإنجليزية

- Arthur L. Bowker & Leonard N. Drinkarde: " Downloading using computer software as investigative tool " . F.B.I Law Enforcement Bulletin Dune, 1996.

- Brenner, S. W., Frederiksen, B.A.: Computer Searches and Seizures: Some Unresolved Issues. Mich. Telecomm. Tech. L. Rev. 39(8); Kerr, O.S., 2005.

	Search Warrants in an Era of Digital Evidence. Mississippi Law Journal,2002.
- Brown, I.	**Communications Data Retention in an Evolving Internet. International Journal of Law and Information Technology, 19(2):107, 2010.**
- Fallmann, H., Wondracek, G. and Platzer, C.	**Covertly probing underground economy marketplaces. Vienna University of Technology,2010.**
- Feigenbaum et al.	**A Model of Onion Routing with Provable Anonymity. Financial Cryptography and Data Security Lecture Notes in Computer Science.2007.**
- Chappell, L.	**Wireshark Network Analysis (Second Edition): The Official Wireshark Certified Network Analyst Study Guide, Laura Chappell University,2012.**
- James W Oldenburg, Richard H. Ward	**Criminal Investigation, New York, 1992.**
- Kaspersen	**Computer crimes and others crimes**

(H.W.K)	aganiste information technology in the Netherlands. Rev. int. dr. pen. 1993.
- Moherenschlager (M)	Computer crimes and others crimes aganiste information technology in the Germany. Rev. int. dr. pen. 1993
- Orin S. KERR	Search warrants in an era of digital evidence, Mississippi Law Journal, Vol. 75, 2005.
- Piragaff (D.K)	Computer crimes and others crimes aganiste information technology in the Canada., report, Rev. int. dr. pen. 1993.
- SeiberUlrich	• Computer crimes & other crimes related to information technology, 1991. • Mastering complexity in the global cyberspace: The harmonization of computer-related criminal law.
- Stone-Gross, B., et al.	Your Botnet is My Botnet: Analysis of a Botnet Takeover,2009.
- Walden, I.	Accessing Data in the Cloud: The Long

Arm of the Law Enforcement Agent. Privacy and Security for Cloud Computing. Computer Communications and Networks 2013.

ثالثاً- الاتفاقيات والمواثيق الدولية باللغة الانجليزية

- **Convention on Cyber Crime-Explanatory Report, adopted on 8 Nov.2001.**
- **European Convention on Cyber Crime, adopted in Budapest on 23 Nov.2001.**

رابعاً- الدراسات المنشورة باللغة الانجليزية

- **Comprehensive Study on Cybercrime, United Nations Office of Drugs And Crime, Draft February 2013, Published by UNODC, New York,2013.**
- **Europol, 2011. Threat assessment (abridged). Internet facilitated organised crime. iOCTA. File No.: 2530–264. The Hague. 7 January. Available at: https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf**
- **NATO Cooperative Cyber Defence Centre of Excellence and ENISA, 2012. : Legal Implications of Countering Botnets.**

- OECD, 2008. Malicious Software (Malware). A Security Threat to the Internet Economy. DSTI/ICCP/REG(2007)5/FINAL. 28 April 2008; Hogben, G. (ed.) 2011. Botnets: Detection, Measurement, Disinfection and Defence. European Network and Information Security Agency(ENISA).
- UNODC calculations based on Microsoft, 2010. Microsoft Security Intelligence Report. Volume 9. Figure as of first half 2010. This estimate is of the same order of magnitude as that of Symantec, 2011. Internet Security Threat Report. 2011. Volume 17 (estimate of 4.5 million for 2010); Acohido, B., 2010. Are there 6.8 million –or 24 million– botted PCs on the Internet? The Last Watchdog. : Available at: http://lastwatchdog.com/6-8-million-24-million-botted-pcs-internet/

خامساً- المراجع باللغة الفرنسية

- DOBKIN (M.) La transaction en matière pénale, D. 1994, Chron
- GASSIN (R.) Fraud informatique, Dalloz,1995.
- Merle (R.), et Vitu (A.) Traite de droit criminel, procédure pénale, CUJAS, 5ed. 2001.

- Meunier (c) La loi du 28 November 2000 relative a la criminalite informatique. Rev. dr. pen. Crim. 2002.

- Podovo(Y.) Un apercu de la lutte contre la cybercriminalite en France. R.S.C. 2002.

- Sedallion (Valerie) Droit de L'Internet.Reg lamentation Responsobilite's, Contrats Collection Aui ,Paris, 1997.

- Spreutels (J.P.) Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en belgique: rapp. Rev. Int. dr. pen. 1993.

- VERGUCHT (Pascal) La repression des délits informatiques dans une perspective internationnale, Thése, Montpellier 1, 1996:

سادساً- وثائق المجلس الأوروبي باللغة الفرنسية

- Conseil de L'eurpe: Problemes de procedure penale lies a la technologie de l' information. Recommendation n. R (95) 13 et expose des motifs. Ed. Conseil de l'europe, 1996.