الحماية الجنائية للخدمات
المقدمة للجمهور في عصر التحول الرقمي
دراسة في ضوء أحكام القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة تقنية المعلومات

إعـــداد

دكتـورة/ مـــي محمـد ممـدوح عبـدالله قايـد

دكتوراه في القانون الجنائي- جامعة القاهرة

مقـدمـــة

يشهد العالم تزايداً مطرداً في استخدام النظم المعلوماتية في كافة مناحي الحياة، سواء أكان على مستوى الأفراد أم مؤسسات الدولة، وإذا كان لتلك الثورة المعلوماتية العديد من الجوانب الإيجابية منها تقديم الخدمات الإلكترونية(١) من قبل مؤسسات الدولة، فإنها حملت في طياتها أيضاً بذور الشر، فقد أصبحت النظم المعلوماتية والشبكات المتصلة بها مصدراً خصباً للعديد من الجرائم المعلوماتية، كتدمير المواقع الإلكترونية، والاعتداء على حرمة الحياة الخاصة للمواطنين، وتدمير نظم المعلومات، وقرصنة البرمجيات واختراق البريد الإلكتروني، والسطو على أرقام البطاقات الائتمانية، مما يتسبب في تدمير البنية التحتية المعلوماتية للدولة، وتزداد فداحة وجسامة أضرار تلك الجرائم إذا وقعت على خدمات الدولة الجماهيرية؛ وتقاعست الدولة عن مكافحتها والحد من نطاقها.

وانطلاقاً من دور الدولة في مواجهة تلك الجرائم وإيماناً من المشرع الدستوري بأهمية حماية النظم المعلوماتية للدولة والأشخاص، فقد نص دستور جمهورية مصر العربية في المادة (٣١) على كفالة حماية أمن الفضاء المعلوماتي، باعتباره جزءاً أساسياً من منظومة الاقتصاد والأمن القومي، وأوجب الدستور على الدولة اتخاذ التدابير اللازمة للحفاظ عليه، وأحال المشرع الدستوري إلى القانون في اتخاذ كافة الإجراءات اللازمة لإقرار مفاهيم الأمن المعلوماتي، وذلك تأكيداً على واجب الحفاظ على الأمن القومي للدولة(٢).

كما ألزم المشرع الدستوري الدولة بوضع خطة شاملة للقضاء على الأمية الرقمية بين المواطنين(٣)، وحماية الأنشطة المعلوماتية باعتبارها مقومات أساسية للاقتصاد الوطني(٤)، وهذا ما دفع الدولة المصرية إلى اللجوء إلى التحول الرقمي في كافة القطاعات الحكومية وهو ما يتضح في خطة مصر لعام ٢٠٣٠.

---

(١) يقصد بمصطلح الخدمات الإلكترونية هي الخدمات الجماهيرية التي تقدمها الدولة للمواطنين ويكون من شأنها تلبية حاجاتهم وتحقيق رفاهيتهم، وقد يطلق عليها أيضاً الخدمات الرقمية، لذلك سيتم خلال دراستنا استخدام كلا المصطلحين.

(٢) المادة (٨٦) من الدستور المصري الصادر عام ٢٠١٤.

(٣) المادة (٢٥) من الدستور المصري الصادر عام ٢٠١٤.

(٤) المادة (٢٨) من الدستور المصري الصادر عام ٢٠١٤.

وقد أعلنت الحكومة أن هدف الدولة من رؤية "٢٠٣٠" هو تواجد الاقتصاد المصري بين أقوى ٣٠ اقتصاد على مستوى العالم بحلول عام ٢٠٣٠[١]، وهذا الهدف لن يتم إلا من خلال الإصلاح الاقتصادي والإداري للدولة، وأول خطوات هذا الإصلاح هو ميكنة الخدمات الجماهيرية.

فالإصلاح الإداري من أهم الملفات التي تسعى الدولة جاهدة إلى تحقيقه، ويُعد التحول الرقمي هو أساس هذا الإصلاح، فلم يعد رفاهية بل أصبح ضرورة ملحة، وذلك من خلال رقمنة الخدمات التي تقدمها الدولة.

وتعمل الحكومة المصرية على تنفيذ آليات التحول الرقمي، وذلك عن طريق تهيئة البيئة التشريعية ودعم البنية التحتية المعلوماتية لتوفير المُناخ الملائم للإصلاح الإداري للدولة، فأصدرت القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات بهدف حماية البنية المعلوماتية للدولة، مع التأكيد على حماية الحرية الشخصية أو حرمة الحياة الخاصة للمواطنين[٢]، وغيرها من الحقوق والحريات العامة التي يكفلها الدستور والقانون[٣].

أهمية البحث:

تنبع أهمية البحث من تزايد الدور الفعال للتحول الرقمي في خضم جائحة كوفيد –١٩، وبيان الدور الجوهري الذى تلعبه التكنولوجيا الحديثة في تغيير مفاهيم الإدارة الإلكترونية وتقديم خدماتها الإلكترونية للمواطنين، وتعزيز استخدام تكنولوجيا المعلومات بما يواكب مستحدثات العصر ومواجهة كافة الانتهاكات التي قد تتعرض لها تلك الخدمات

ونتيجة لتعدد التهديدات السيبرانية التي تتعرض لها الدولة المصرية؛ والتي قُدرت نحو ١٣ مليون هجمة سيبرانية على مصر خلال الربع الأول من عام ٢٠٢٣، وقد ركزت تلك الهجمات على الحسابات المصرفية وبيانات العملاء في القطاع المصرفي المصري بنسبة ١٨٦٪ خلال الربع الأول من العام ٢٠٢٣ مقارنة بنفس الفترة من عام ٢٠٢٢، بالإضافة إلى تعرض ما يقرب من ٧٥ ألف مستخدم في مصر خلال

(١) الترتيب الحالي لمصر (٤١) من إجمالي (١٩٢) في العالم، للمزيد أنظر.. استراتيجية التنمية المستدامة– رؤية مصر ٢٠٣٠، الصادرة عن وزارة التخطيط والمتابعة والإصلاح الإداري، ص ١٢.

(٢) تنص المادة (٥٩) من الدستور المصري الصادر عام ٢٠١٤ على أن "الحياة الآمنة حق لكل إنسان، وتلتزم الدولة بتوفير الأمن والطمأنينة لمواطنيها، ولكل مقيم على أراضيها"

(٣) المادة (٩٩) من الدستور المصري الصادر عام ٢٠١٤.

الربع الأول من عام ٢٠٢٣ لهجمات التصيد الاحتيالي عبر البريد الإلكتروني والرسائل النصية القصيرة، بالإضافة إلى تعرض بعض المؤسسات الحكومية المصرية لهجمات شنتها فرق قرصنة دولية في عام ٢٠٢٢ بهدف التجسس وسرقة بيانات العملاء(١)، ومن هنا كان لازماً الوقوف على الحماية الجنائية التي كفلها المشرع المصري لحماية الخدمات التي تقدمها مؤسسات الحكومة المصرية في البيئة الرقمية.

تساؤلات البحث:

١- ما هو مفهوم الخدمات الجماهيرية ؟

٢- ما المقصود بحقوق الإنسان الرقمية وما هي أنواعها؟

٣- ماذا يعني التحول الرقمي للخدمات الجماهيرية وما هي متطلباته؟

٤- ما هي الخدمات الرقمية التي تقدمها الحكومة المصرية؟

٥- ما هي سياسة الدولة المصرية في مواجهة الانتهاكات الرقمية؟

٦- ما هي أبرز النصوص القانونية التي تستهدف مواجهة انتهاكات الخدمات الإلكترونية؟

أهداف البحث:

- التعرف على مفهوم التحول الرقمي وتطبيقه على الخدمات الجماهيرية التي تقدمها الدولة.
- عرض سياسة الحكومة المصرية في منظومة التحول الرقمي لقطاعاتها المختلفة.
- إبراز مضمون الحماية الدستورية للنظم المعلوماتية، ومدى التزام الدولة بإنفاذ الأحكام الدستورية باتخاذ الإجراءات الكفيلة بضمان تأمين البنية التحتية للخدمات الجماهيرية، وإصدار القوانين اللازمة لإقرار مفاهيم الأمن المعلوماتي.
- دراسة النماذج الإجرامية المستحدثة والتي تسبب إعاقة تقديم الخدمات الرقمية في القانون ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات.. والعقوبات التي فرضها المشرع لكل جريمة، ومدى كفاية تلك النصوص التجريمية في مواجهة الجرائم المعلوماتية.

(١) Kaspersky tackles ١٣ million cyber attacks in Egypt during ١Q ٢٠٢٣, Daily News Egypt, last seen ٢٧/١٢/٢٠٢٣, https://www.dailynewsegypt.com/٢٠٢٣/٠٥/٠٨/kaspersky-tackles-١٣-million-cyber-attacks-in-egypt-during-١q-٢٠٢٣/.

مشكلة البحث:

أدت الثورة في مجال تكنولوجيا المعلومات والاتصالات إلى ازدياد المعوقات والصعوبات التي تواجه الدولة المصرية نتيجة كثرة التهديدات التي تواجه الحكومة المصرية خاصة عقب جائحة كوفيد-١٩ على الأمن القومي العالمي ومعوقات التنمية للدولة المصرية وتحقيق رؤية مصر لعام ٢٠٣٠، والتي من بينها التخوف من مخاطر أمن المعلومات الذي يمكن أن ينعكس على الأمن القومي المصري، ومدى كفاية النصوص التجريمية لمواجهة الجرائم المرتكبة على تلك الخدمات.

وفى ضوء تلك المخاوف تكمن إشكالية البحث المتمثلة في الوقوف على مدى كفاية الحماية القانونية التي كفلها مكافحة جرائم تقنية المعلومات في توفير الضمانات الكافية لحماية الخدمات الرقمية التي تقدمها الدولة للمواطنين، وفرض العقوبات الرادعة للجناة.

منهج البحث:

اعتمد البحث على المنهج الوصفي التحليلي في وصف وتشخيص موضوع البحث في مختلف جوانبه وأبعاده، كما يسعى إلى الوقوف على مدى كفاية السياسات الحالية لحماية الخدمات الجماهيرية من الجرائم المعلوماتية التي قد تتعرض لها، ومدى الحاجة إلى آليات جديدة لمنعها.

خطة البحث:

المبحث الأول: الخدمات الجماهيرية في عصر التحول الرقمي.

المطلب الأول: الخدمات الجماهيرية الرقمية.

المطلب الثاني: الخدمات الرقمية التي تقدمها الدولة المصرية.

الفرع الأول: تطبيقات التحول الرقمي في الحكومة المصرية.

الفرع الثاني: استراتيجية الدولة في مواجهة الانتهاكات الرقمية.

المبحث الثاني: السياسة الجنائية لمواجهة انتهاك الخدمات الإلكترونية.

المطلب الأول: الانتفاع بدون حق بخدمات الاتصالات والمعلومات.

المطلب الثاني: جريمة الدخول غير المشروع.

المطلب الثالث: الاحتيال على بطاقات البنوك والخدمات وأدوات الدفع الإلكتروني.

المبحث الثالث: مواجهة الدولة لجرائم الاعتداء على الشبكات المعلوماتية.

المطلب الأول: الاعتداء على أنظمة الدولة المعلوماتية.

المطلب الثاني: الاعتداء على سلامة الشبكة المعلوماتية.

المطلب الثالث: العبث بالأدلة الرقمية.

المبحث الأول
الخدمات الجماهيرية في عصر التحول الرقمي

تمهيد وتقسيم:

إن الخدمات الجماهيرية هي الخدمات التي تلبى الحاجات الضرورية للمواطن وتحقيق رفاهيته وتلتزم الحكومة بتقديمها لكل المواطنين على أن تكون مصلحة المجتمع ورفع مستوى المعيشة للمواطنين هي الهدف الرئيسي لهذه الخدمات، مثل (الخدمات الصحية وخدمات الأمن والخدمات الثقافية والتعليمية،...)، وهي مسئولية الدولة وليست موقوتة بزمن محدد، بل هي خدمات دائمة مستمرة ينبغي أن تخطط الدولة لتقديمها وتطويرها، وقد فرض التقدم الهائل في تكنولوجيا المعلومات والاتصالات على الحكومات والشعوب استخدام تقنياتها، وتحقيق الكثير من المتطلبات من خلالها والتي من أهمها تقديم خدمة جيدة للمواطنين، وتحقيق الشفافية الحكومية وتمكين المواطن من الحصول على خدماته بيسر وسهولة وأقل تكلفة.

ومع ارتباط الخدمات الجماهيرية بحقوق الإنسان والذي أصبح التقدم التكنولوجي يشكل انتهاك عليها وذلك عبر الوسائل التقنية الحديثة، مما أوجب على الدولة احترام تلك الحقوق والالتزام بحمايتها من كافة الانتهاكات غير المشروعة.

وتجدر الإشارة إلى أن مصر تدخل "المجموعة ب" التي تضم الدول ذات درجة "مرتفعة" في مؤشر التقنيات الحكومية لعام ٢٠٢٠، ويرتكز هذا المؤشر على أربعة مجالات وهي (أداء الخدمة العامة وهو يقيس مدى إتاحة الخدمات إلكترونياً– مشاركة المواطنين وهو يقيس مدي مشاركة المواطنين واستجابة الحكومة لمقترحاتهم– ممكنات الحكومة الرقمية وهو يقيس مدى توافر بيئة مناسبة لتقديم الخدمات الرقمية، الأنظمة الحكومية الرئيسية وهو يقيس الجوانب الرئيسية للنهج الحكومي مثل وجود مجال إلكتروني لتخزين البيانات)[١].

(١) يصنف المؤشر في ٤ مجموعات (المجموعة "أ" درجة مرتفعة للغاية، المجموعة "ب" درجة مرتفعة، المجموعة "ج" درجة متوسطة، المجموعة "د" درجة منخفضة)، وذلك بهدف قياس مدى تطور الدول في أربع مجالات رئيسية من خلال ٤٨ مؤشراً، للمزيد أنظر .. تقرير بعنوان "جهود على طريق التنمية– الرقمنة في مصر"، صادر عن مركز المعلومات ودعم اتخاذ القرار بمجلي الوزراء، يونيو ٢٠٢٢، ص ١٣ .

وفيما يلي سوف نتناول هذا المبحث من خلال المطلبين التاليين:

المطلب الأول: الخدمات الجماهيرية الرقمية.

المطلب الثاني: الخدمات الرقمية التي تقدمها الدولة المصرية.

المطلب الأول

الخدمات الجماهيرية الرقمية

يرتبط مفهوم الخدمة مرتبط ارتباطاً وثيقاً بحقوق الإنسان ومتطلباته، فالخدمة لها طرفان الأول مقدم الخدمة، والثاني مُتلقي الخدمة (طالب الخدمة)، ومن ثم يلزم أن يقوم الطرف الأول باحترام حقوق الطرف الثاني عند تقديم الخدمة، والعمل على توفير سبل الراحة والأمان والحماية له، ومع التقدم التكنولوجي ظهرت رغبة الحكومات والشعوب في دول العالم في الاستفادة من تقنيات هذا التقدم مع الحفاظ على حقوق الإنسان وصون حريته، وفي ضوء الحاجة لتطوير الخدمات الجماهيرية التي تقدمها الدولة، فقد رأت الدولة أن استخدام تكنولوجيا المعلومات هو أمر من شأنه إحداث طفرة كبيرة في أداء منظماتها الخدمية[١]، إلى جانب عدم المساس بحقوق الإنسان الدستورية والقانونية بل والعمل على حمايتها، وفيما يلي سوف نوضح ماهية الخدمات الجماهيرية التي تقدمها الدولة ونتبعها بمفهوم حقوق الإنسان الرقمية والتحول الرقمي لتلك الخدمات:

أولاً: الخدمات الجماهيرية:

تعرف الخدمة بأنها هي المنافع التي تقدمها الدولة أو المؤسسة "مُقدمة الخدمة" للجمهور سواء كانت حكومية أو غير حكومية، فهي سلسة من الأنشطة أو الإجراءات أو العمليات التي يوفرها مقدم الخدمة وتهدف إلى تلبية حاجة المواطنين، وذلك عبر قنوات تقديم الخدمات المختلفة وتكون مبنية على التفاعل من قبل الجمهور ومقدم الخدمة[٢]، مما يؤدي إلى زيادة الثقة بين الدولة والجمهور[٣].

---

(١) شريف صالح محمد، ورقة بحثية بعنوان "تطور مفهوم خدمات المواطنين وعلاقته بنظم المعلومات والاتصالات"، مصر، جامعة بورسعيد- كلية التجارة، ٢٠١٩، ص ٢٤١.

(٢) مرجع سابق، ص ٢٤١.

(٣) إن المواطنين الذين يشعرون بالرضا عن الخدمات العامة أكثر ميلاً إلى الثقة في أداء الحكومات إجمالاً بمقدار ٩ أضعاف مقارنة بغيرهم، استقصاء مرجعي حول رحلة القطاع العام، ٢٠١٨، مشار إليه بورقة بحثية بعنوان "الخدمات العامة الرقمية: سبل تحول سريع على نطاق واسع، ٢٠٢٠، ص ٢، أخر مطالعة بتاريخ ٢٠٢٣/١٢/٢٧،

ثانياً: حقوق الإنسان الرقمية:

إن الخدمات التي تقدمها الدولة للمواطنين ترتبط بحقوق الإنسان بصفة عامة، وحقوقه الرقمية بصفة خاصة، لذا يلزم علينا التعرف على ماهية حقوق الإنسان الرقمية التي يجب على الدولة مراعاتها عند تقديم خدماتها الرقمية، وعرف المركز العربي لتطوير الإعلام الاجتماعي "حملة" وجمعية الاتصالات التقدمية "APC" الحقوق الرقمية أو حقوق الإنترنت بأنها امتداد لحقوق الإنسان في العالم الواقعي، وهي حقوق معترف بها ومحمية ومروج لها بموجب القوانين والمعاهدات الدولية، حيث أن نفس الحقوق التي يتمتع بها الناس في العالم الواقعي يجب أن يتمتع بها في الواقع الافتراضي(١)، فهي بذلك تُعد امتداد لحقوق الإنسان المستمدة من الإعلان العالمي لحقوق الإنسان لعام ١٩٤٨ ومنسجمة مع مضامين العهد الدولي الخاص بالحقوق المدنية والسياسية لعام ١٩٦٦.

- **سمات حقوق الإنسان الرقمية:**

تتسم الحقوق الرقمية بعدة سمات تميزها عن غيرها من حقوق الإنسان؛ فهي (حقوق متطورة ومتجددة، مطلقة وليست مقيدة، حقوق متكاملة ومترابطة مع بعضها البعض، حقوق عامة وعالمية حيث إنها متاحة لجميع المستخدمين، حقوق ذاتية ونسبية ومتغيرة) (٢).

- **أنواع حقوق الإنسان الرقمية:** تتنوع وتتعدد حقوق الإنسان الرقمية، من أهمها ما يلي(٣):

١- الحق في الخصوصية الرقمية: يُعرف حق الخصوصية الرقمية بأنه وصف لحماية البيانات

للمزيد أنظر.. https://www.mckinsey.com/~/media/mckinsey/industries/public.

(١) د/ هاشم فتح الله عبدالرحمن عبدالعزيز، حقوق الإنسان الرقمية كمتطلب للتحول الرقمي الآمن، القاهرة، رابطة التربويين العرب، يوليو ٢٠٢١، العدد ١٨، ص ٤٦.

(٢) أ/ بيرم جمال، بحث بعنوان "حقوق الإنسان الرقمية"، موقع موسوعة ودق القانونية للأبحاث والدراسات والاستشارات القانونية الشاملة، منشور بتاريخ ٢٠٢١/١١/٤، أخر مطالعة بتاريخ ٢٠٢٣/٥/٢٤، https://wadaq.info.

(٣) مرجع سابق.

الشخصية للأفراد، والتي يتم نشرها وتداولها من خلال الوسائط الرقمية، وتتمثل البيانات الشخصية في البريد الإلكتروني والصور الشخصية والحسابات البنكية الرقمية وكافة البيانات الشخصية المتعلقة بالشخص، كما يشتمل على حماية شبكة الإنترنت وخصوصيتها وحماية المعلومات(١).

٢- الحق في التخفي الرقمي: يتجسد في حق كل فرد متواجد على الشبكة العنكبوتية في التخفي بحيث لا يكون مجبراً على الإفصاح عن هويته الرقمية بشرط أن لا يتعارض ذلك مع النظام العام أو حريات وحقوق الآخرين.

٣- الحق في النسيان الرقمي: يُقصد به أن يكون لكل فرد متواجد على شبكة الإنترنت الحق في تعديل أو تغيير أو مسح أو سحب كافة البيانات أو المعلومات التي تخصه عبر وسائط النقل الرقمية دون أن يتعارض ذلك مع حقوق الغير أو النظام العام، ويقتضي هذا الحق بالتزام الأشخاص المسؤولين عن المواقع الإلكترونية بعدم حفظ تلك البيانات لمدة تتجاوز الغاية التي جُمعت لأجلها وأن يحترموا حقوق الأفراد في نسيان بياناتهم الشخصية.

٤- الحق في التشفير: يعتبر أهم حق لحماية حرية الرأي والتعبير في العصر الرقمي، ويُقصد بالحق في التشفير أنه استخدام رموز أو إشارات غير متداولة فتصبح بمقتضاها المعلومات المرغوب في تحويرها أو إرسالها غير قابلة للفهم من جانب الغير، ويُعرَف التشفير في الأمن الإلكتروني بأنه تحويل البيانات من تنسيق قابل للقراءة إلى تنسيق مُشفر، فلا يمكن قراءة البيانات المشفرة أو معالجتها إلا بعد فك تشفيرها(٢).

٥- الحق في الأمن الإلكتروني: يشير حق الأمن الإلكتروني إلى مجموعة من التقنيات المستعملة لحماية سلامة الشبكات والبرامج والبيانات من الهجوم والضرر والولوج الغير

---

(١) د/ أمل فوزي أحمد عوض، الحقوق والحريات الرقمية (معالجات قانونية، تقنية، منظور الشريعة الإسلامية)، ألمانيا، برلين، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، يوليو ٢٠٢١، العدد الأول، ص ٤٧.

(٢) د/ بشير محمد حسين، أثر المراقبة الرقمية على الحريات العامة، الجائر، جامعة جيلالي اليابس، ٢٠١٧، ص ٦٥.

مصرح به[١]، ويُطلق على مصطلح الأمن الإلكتروني بالأمن السيبراني، ويُعرَف بأنه هو عملية حماية الأنظمة والشبكات والبرامج ضد الهجمات الرقمية.

ثالثاً: مفهوم التحول الرقمي للخدمات الجماهيرية:

يمثل التحول الرقمي للخدمات الجماهيرية تغيير جذري كبير في طريقة أو وسيلة تقديم تلك الخدمات، حيث يساعد على تحقيق الاستدامة، بالإضافة إلى بناء مجتمعات فعالة[٢]، ويشمل التحول الرقمي (Digital transformation) عملية تغيير المنتج أو طريقة تقديم الخدمة كلياً، فقد يكون استراتيجياً يتدخل في وظائف المؤسسة كلها، كما إنه يغير المكونات الأساسية للعمل من حيث البنية التحتية، وطرق التشغيل وكيفية الحصول على الخدمة[٣]، فالمستقبل الرقمي هو البديل العملي الوحيد المطروح أمامنا.

المطلب الثاني

الخدمات الرقمية التي تقدمها الدولة المصرية

تمهيد وتقسيم:

يُعد التحول الرقمي من أبرز، بل أهم الملفات التي طرحتها الحكومة المصرية في خطتها لعام ٢٠٣٠؛ حيث يسهم هذا التحول في تفّرد الدولة المصرية في القارة الإفريقية، والقضاء على الفساد، وذلك من خلال إتاحة الخدمات الرقمية لجميع المؤسسات والمواطنين بطرق بسيطة، وكذا تكلفة ملائمة في أي وقت وفي أي مكان، بجانب دعم الصناعات الرقمية والإبداع التكنولوجي، وإنشاء ممر مصر الرقمي؛ لضمان تحقيق الاستغلال الأمثل للموقع الجغرافي المصري لتصبح مركزاً عالمياً هاماً لخدمات الاتصال وتكنولوجيا المعلومات.

---

(١) Deloitte & Touche LLP, IT control objectives for Sarbanes Oxley", New Guidance on IT control and compliance, ٢٠٠٨, p١٠.

(٢) د/ عدنان مصطفى البار، التحول الرقمي كيف ولماذا؟، السعودية، جامعة الملك عبد العزيز، ٢٠١٩، ص ٢.

(٣) عباس بردان، ما هو التحول الرقمي وكيف تعرفه الشركات الرقمية ومحركات دفع التحول الرقمي والتكنولوجي، ٢٠١٩، الجزء الأول، ص ١٣.

وتعد مصر ضمن أسرع عشر دول نمواً في مجال الشمول الرقمي عام ٢٠٢٠، حيث أصبحت في المركز الثالث عالمياً في معدل تحسين الأداء في عام ٢٠٢٠[١]، كما أحرزت مصر تقدماً ملحوظاً في مؤشر جاهزية الشبكات في العالم لعام ٢٠٢١ لتصبح في الترتيب الـ(٧٧) من بين (١٣٠) دولة، في حين إنها كانت في الترتيب الـ(٨٨) من بين (١٣٤) دولة عام ٢٠٢٠[٢]، وفيما يلي سوف نتناول الخدمات الرقمية التي تقدمها الدولة المصرية للجمهور من خلال الفرعين التاليين:

الفرع الأول : تطبيقات التحول الرقمي في الحكومة المصرية.

الفرع الثاني : استراتيجية الدولة في مواجهة الانتهاكات الرقمية.

الفرع الأول

تطبيقات التحول الرقمي في الحكومة المصرية

تمضى الدولة قدماً في توجهها الاستراتيجي نحو بناء مصر الرقمية، حيث عملت على تعزيز وتطوير البنية التحتية لتكنولوجيا المعلومات والاتصالات، ووضع الخطط والاستراتيجيات الكفيلة بتحقيق أهدافها في الوصول إلى حكومة مترابطة ومتكاملة رقمياً، والتوسع في تقديم الخدمات المميكنة، مما يساهم في الارتقاء بمستوى حياة المواطنين عبر إتاحة خدمات إلكترونية متعددة توفر الوقت والجهد، فضلاً عن تطويع التكنولوجيا في إيجاد حلول للقضايا والتحديات التي تواجه المجتمع، وقد دشنت الحكومة المصرية العديد من تطبيقات التحول الرقمي؛ من أبرزها:

١ – بوابة مصر الرقمية:

- عبارة عن منصة تقدم الخدمات الحكومية إلكترونياً بشكل ميسر، حيث تقدم المنصة (١٦٨) خدمة من (٩) وزارات مختلفة، بلغ عدد مستخدمي البوابة (٧٥٧٩٥٨٦) مليون مواطن، وعدد الطلبات المقدمة (٤٠٠٧١٢٣٤) مليون طلب حتى ٢٠٢٣/٨/١٨[٣].

---

(١) تقرير بعنوان "جهود على طريق التنمية – الرقمنة في مصر"، مرجع سابق، ص ٢٨ .

(٢) يستهدف مؤشر جاهزية الشبكات تقييم البنية التحتية التكنولوجية للدول، واستخدامات الأفراد والحكومات للتكنولوجيا والاستثمار فيها، مرجع سابق، ص ٨ .

(٣) تجدر الإشارة إنه يتم تحديث البيانات على بوابة مصر الرقمية بشكل دوري، أخر مطالعة بتاريخ

٢- مجمع الإصدارات المؤمنة والذكية (قلعة مصر الرقمية):

- وهو أكبر وأحدث مجمع من نوعه في أفريقيا والشرق الأوسط، فقد صدر قرار رئيس الجمهورية بإنشاء جهاز بوزارة الدفاع يسمى "مجمع الإصدارات المؤمنة والذكية"، ويختص بتوفير الحلول التكنولوجية المتكاملة والمركزية في تصميم وتأمين وطباعة وإصدار كافة النماذج والإصدارات والمحررات الرسمية بأعلى مستويات التأمين، وقد أصدر المجمع أكثر من (٤٠٠) مليون إصدارة ذكية[١].

٣- خريطة مصر الخضراء:

- هي منصة إلكترونية على شبكة الإنترنت تختص باستعراض جهود الدولة المصرية لمجابهة التغيرات المناخية، تزامناً مع بدء فعاليات مؤتمر الدول الأطراف في اتفاقية الأمم المتحدة الإطارية بشأن تغيّر المناخ (COP٢٧)[٢].

٤- منصة الذكاء الاصطناعي:

- وهي أول منصة رقمية للذكاء الاصطناعي أُطلقت عام ٢٠٢١، حيث تضمن تحقيق نقلة نوعية كبرى في هذا المجال، الأمر الذي يدعم جهود الدولة في الاستفادة من هذه التكنولوجيا لتحقيق التحول الرقمي وبناء مصر الرقمية، بالإضافة إلى دورها في الترويج عن الدور الريادي لمصر باعتبارها طرفًا دوليًا فاعلًا في مجال الذكاء الاصطناعي[٣].

٢٠٢٣/٨/١٨، https://digital.gov.eg/ .

(١) تقرير بعنوان "جهود على طريق التنمية – الرقمنة في مصر"، مرجع سابق، ص ١٧.

(٢) كما أطلق المركز تطبيق "تبتا" وهو تطبيق لتكوين شبكة ضخمة من دعاة حماية البيئة والمهتمين بشئون البيئة والتعرف على أفضل الطرق للتعاون لحل أزمة المناخ وإنقاذ، موقع مركز المعلومات ودعم اتخاذ القرار، مجلس الوزراء، أخر مطالعة بتاريخ ٢٠٢٣/٥/٢٥، https://www.idsc.gov.eg/News/View/١٥٨١٩.

(٣) موقع وزارة الاتصالات وتكنولوجيا المعلومات، أخر مطالعة بتاريخ ٢٠٢٢/١١/٢٥، https://mcit.gov.eg/Ar/Media_Center/Press_Room/Press_Releases/٦٣٤٨٤ .

٥- منظومة النقل الذكي (ITS)[١]:

- تتكون المنظومة من (كاميرات مراقبة وحساسات على الطرق، بوابات تحصيل الرسوم، شبكة نقل البيانات، مراكز التشغيل والتحكم والدعم الفني، الدفع والتحصيل الإلكتروني،..)، وتهدف إلى تقليل نسب الحوادث وزيادة معدلات الأمان، وتحسين الكفاءة التشغيلية للطرق، بجانب خلق فرص استثمارية جديدة[٢].

الفرع الثاني
استراتيجية الدولة في مواجهة الانتهاكات الرقمية

تبنت الدولة المصرية استراتيجية متكاملة لمواجهة جرائم تقنية المعلومات وحماية منظومتها المعلوماتية، وفى حقيقة الأمر فإن مواجهة ذلك النوع من الجرائم يتطلب رجال يملكون الخبرة الفنية المعلوماتية[٣]، لذلك فقد نص قانون مكافحة جرائم تقنية المعلومات في مادته الخامسة على أنه: "يجوز بقرار من وزير العدل بالاتفاق مع الوزير المختص منح صفة الضبطية القضائية للعاملين بالجهاز القومي للاتصالات أو غيرهم ممن تحددهم جهات الأمن القومي بالنسبة إلى الجرائم التي تقع بالمخالفة لأحكام هذا القانون والمتعلقة بأعمال وظائفهم".

واتبعت الحكومة المصرية سياسة موحدة، تسعى إلي تعزيز حلول أمن البيانات والمعلومات لدى مختلف الجهات والهيئات، والتوسع في تقديم خدمات الحكومة الإلكترونية بشكل آمن[٤]، وتتجسد تلك السياسة حول محاور أربع رئيسية هي: (سبل تأمين شبكات البنية التحتية

(١) مرجع سابق، ص ٢٤.
(٢) تقرير بعنوان "جهود على طريق التنمية – الرقمنة في مصر"، مرجع سابق، ص٢٤.
(٣) د/ جميل الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، القاهرة، دار النهضة العربية، ٢٠٠١، ص ٨٩ وما بعدها.
(٤) تجدر الإشارة في هذا الصدد إلى تقدم مصر ٣ مراكز في مؤشر تطوير الحكومة الإلكترونية عام ٢٠٢٠، حيث انتقلت مصر من فئة "ذات الأداء المتوسط إلى فئة "ذات الأداء المرتفع"، تقرير بعنوان "جهود على طريق التنمية – الرقمنة في مصر"، مرجع سابق، ص ١٤ .

وتطبيقات التحكم الصناعي، مستقبل الهجمات السيبرانية وتأثيرها على الأمن القومي[١]، المستجدات التشريعية وانعكاسها على آليات التعامل مع جرائم تقنية المعلومات، أفضل الممارسات لتأمين منظومة الخدمات الإلكترونية)[٢]، وفيما يلى نتناول أهم جهود سياسة الحكومة المصرية في رقمنة خدماتها الجماهيرية وحمايتها[٣]:

١- المجلس الوطني للذكاء الاصطناعي[٤]:

يختص المجلس بوضع الاستراتيجية الوطنية للذكاء الاصطناعي، والإشراف على تنفيذها، ومتابعتها، وتحديثها تماشياً مع التطورات الدولية في هذا المجال، ويقوم المجلس بالعديد من المهام منها (وضع السياسات والتوصيات المتعلقة بالأطر الفنية والقانونية والاقتصادية المتعلقة بتطبيقات الذكاء الاصطناعي، التعاون والتنسيق مع الجهات الإقليمية والدولية ذات الصلة لتبادل الخبرات والمعارف واختيار أفضل تطبيقات الذكاء الاصطناعي، إعداد التوصيات الخاصة بالتشريعات ذات الصلة بمجالات الذكاء الاصطناعي).

٢- المجلس الأعلى للمجتمع الرقمي[٥]:

تم تشكيل المجلس الأعلى للمجتمع الرقمي ليكون برئاسة مجلس الوزراء، ويختص المجلس الأعلى للمجتمع الرقمي بالعديد من المهام أهمها (إقرار الاستراتيجية القومية لبناء

---

(١) تجدر الإشارة إلى أن ترتيب مصر في مؤشر الأمن السيبراني في عام ٢٠٢٠ (٢٣) عالمياً من بين (١٩٤) دولة، تقرير بعنوان "جهود على طريق التنمية– الرقمنة في مصر"، مرجع سابق، ص ١٠.

(٢) د/ وليد سمير المعداوي، مكافحة جرائم تقنية المعلومات والإرهاب الإلكتروني وفقاً لأحدث التشريعات المصرية، الإمارات، القيادة العامة لشرطة الشارقة، مركز بحوث الشرطة، مجلة الفكر الشرطي، يوليو ٢٠٢٠، العدد ٣، المجلد ٢٩، ص ٢٤٩.

(٣) الإشارة السابقة، ص ٢٥٠.

(٤) قرار رئيس مجلس الوزراء رقم ٢٨٨٩ لسنة ٢٠١٩ بشأن إنشاء مجلس وطني للذكاء الاصطناعي.

(٥) صدر قرار رئيس الجمهورية رقم ٥٠١ لسنة ٢٠١٧ بشأن إنشاء مجلس أعلى للمجتمع الرقمي، منشور بالجريدة الرسمية، العدد ٤٠ تابع (أ)، في ٢٠١٧/١٠/٧، والذي تم إعادة تشكيله بموجب قرار رئيس الجمهورية رقم ٥١١ لسنة ٢٠٢٢، المنشور بالجريدة الرسمية ، العدد ٤١ مكرر (أ)، في ٢٠٢٢/١٠/٢٤.

دولة رقمية متكاملة، اعتماد السياسات والإجراءات والآليات الخاصة اللازمة لبناء مجتمع رقمي، إقرار سياسات تقديم الخدمات الحكومية الرقمية).

٣- الاستراتيجية الوطنية للأمن السيبراني ٢٠٢٢- ٢٠٢٦[١]:

تهدف الاستراتيجية إلى تأمين البنية التحتية للاتصالات والمعلومات بشكل متكامل لتوفير البيئة الآمنة لمختلف القطاعات لتقديم الخدمات الإلكترونية المتكاملة، بالإضافة إلى توحيد الرؤى الوطنية من أجل التصدي للهجمات السيبرانية، وتعزيز الوعى المجتمعي والمؤسسي بالأمن السيبراني، والارتقاء بالبحث العلمي وتعزيز الابتكار.

٤- المركز المصري للاستجابة لطوارئ الحاسب الآلي (EG CERT) [٢]:

قام الجهاز القومي لتنظيم الاتصالات بتأسيس المركز المصري للاستجابة لطوارئ الحاسب الآلي (سيرت) في إبريل ٢٠٠٩، وتتركز مهمة المركز حول توفير نظام للإنذار المبكر ضد البرمجيات الخبيثة والهجمات الإلكترونية التي تنتشر على نطاق واسع ضد البنية التحتية الحيوية للمعلومات المصرية.

٥- المجلس الأعلى للأمن السيبراني في مصر[٣]:

يهدف إلى حماية المعلومات والبيانات لدى كافة جهات الدولة، والتأكد من توافر التمويل لتنفيذ منظومة الأمن المعلوماتي، ووضوح الإطار التشريعي له، ويختص المجلس بالعديد من المهام، أهمها (اعتماد استراتيجيات تأمين البنية التحتية للاتصالات والمعلومات لقطاعات الدولة، التعاون والتنسيق وتبادل المعلومات دولياً وإقليمياً في مجال الأمن المعلوماتي، اقتراح

---

(١) الاستراتيجية الوطنية للأمن السيبراني ٢٠٢٢-٢٠٢٦، الموقع الرسمي لوزارة الاتصالات وتكنولوجيا المعلومات، أخر مطالعة بتاريخ ٢٠٢٣/٦/٥، https://mcit.gov.eg/ar/Media_Center/Press_Room/Press_Releases/٦٤٨٥١.

(٢) أنظر الموقع الرسمي لوزارة الاتصالات وتكنولوجيا المعلومات، آخر مطالعة ٢٠٢٣/٦/٨، https://mcit.gov.eg/ar/TeleCommunications/Industry/Cyber_Security .

(٣) قرار رئيس مجلس الوزراء رقم ٢٢٥٩ لسنة ٢٠١٤ بشأن إنشاء المجلس الأعلى للأمن السيبراني.

التعديلات التشريعية اللازمة في مجال أمن المعلومات، وضع آليات رصد المخاطر والمتابعة الدورية للهجمات السيبرانية، وضع آليات تأمين وحماية المواقع الحكومية على الإنترنت)[١].

٦- اللجنة الوطنية المعنية بالاستخدام الآمن للإنترنت للأطفال[٢]:

بدأت اللجنة عملها في يونيو ٢٠١٣، هي تعتبر استكمالا لجهود فريق العمل الوطني المعني بالاستخدام الآمن للإنترنت الذي كان مشكلاً في الفترة من أكتوبر ٢٠٠٩ إلى يناير ٢٠١٢، بهدف وضع وتفعيل استراتيجية قومية لحماية الأطفال على الإنترنت وتمكينهم من استخدامه[٣].

المبحث الثاني

السياسة الجنائية لمواجهة انتهاك الخدمات الإلكترونية

تمهيد وتقسيم:

أكد المشرع المصري على أهمية مكافحة الجرائم التي تمثل انتهاكاً للخدمات الرقمية عبر شبكة المعلومات الدولية، حيث قرر دستور عام ٢٠١٤ حماية خاصة للفضاء المعلوماتي بموجب المادة (٣١) والتي نصت على أن "أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون"، كما أكد على حماية الحياة الخاصة للمواطنين بالمادة (٥٧) من الدستور والذي تضمنت أنها مصونة لا تمس وللمراسلات البريدية، والإلكترونية حرمة، وألزمت الدولة بحماية حق المواطنين في

(١) قرار رئيس مجلس الوزراء رقم ١٦٣٠ لسنة ٢٠١٦ بشأن اختصاصات المجلس الأعلى للأمن السيبراني.

(٢) الموقع الرسمي لوزارة الاتصالات وتكنولوجيا المعلومات، أخر مطالعة بتاريخ ٢٠٢٣/٦/٨، https://mcit.gov.eg/Ar/Media_Center/Latest_News/News/٣٤١٥ .

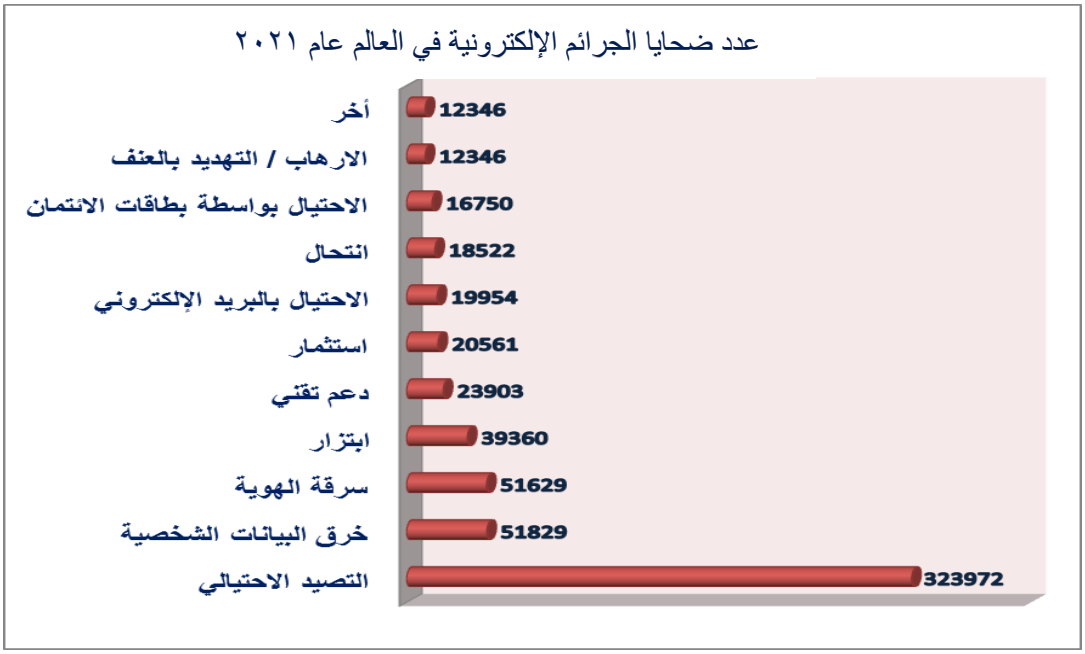
(٣) ورقة مفاهيمية بعنوان "اللجنة الوطنية المعنية بالاستخدام الآمن للإنترنت للأطفال"، صادرة عن وزارة الاتصالات وتكنولوجيا المعلومات، أخر مطالعة بتاريخ ٢٠٢٣/١٢/٢٧، للمزيد أنظر.. https://www.itu.int/en/ITUD/RegionalPresence/ArabStates/Documents/events/٢٠١٥/COP/NationalCOPCommitteeconceptPaper-ar.pdf

استخدام وسائل الاتصال بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، وترك للقانون تنظيم ذلك.

وتنبع أهمية مواجهة تلك الانتهاكات من التطور المستمر في نظم معالجة البيانات والمعلومات الإلكترونية وتخزينها وتبادلها، وتعدد المواقع والحسابات الخاصة والاتساع في استخدام البريد الإلكتروني وأجهزة تقنية المعلومات، بجانب تطور وسائل الاتصال الإلكترونية، مما يلزم الدولة بضرورة مواجهتها لتحقيق الحماية الجنائية التي يكفلها الدستور والمحافظة على المعلومات وكفالة سريتها وعدم إفشائها.

وفيما يلي إحصائية بعدد ضحايا أبرز الجرائم الإلكترونية في العالم خلال عام ٢٠٢١، والتي توضح أنه ما يقرب من ٣٢٤ ألف فرد قد تأثر من جراء جرائم التصيد الاحتيالي، يليها جرائم خرق البيانات الشخصية والتي يقترب عدد ضحاياها من ٥٢ ألف حالة[١].

(١) إحصائية بعنوان "أكثر أنواع الجرائم الإلكترونية التي يتم الإبلاغ عنها شيوعًا في عام ٢٠٢١"، أخر مطالعة بتاريخ ٢٠٢٣/٦/١٨، https://www.statista.com/statistics/١٨٤٠٨٣/commonly-reported-types-of-cyber-crime/ .



وفيما يلي سوف نتناول الجرائم الواردة بقانون مكافحة جرائم تقنية المعلومات والتي تمثل انتهاكاً للخدمات التي تقدمها الدولة للجمهور، وذلك على النحو التالي:

المطلب الأول: الانتفاع بدون حق بخدمات الاتصالات والمعلومات.

المطلب الثاني: جريمة الدخول غير المشروع.

المطلب الثالث: الاحتيال على بطاقات البنوك والخدمات وأدوات الدفع الإلكتروني.

المطلب الأول

الانتفاع بدون حق بخدمات الاتصالات والمعلومات

عاقب المشرع في قانون مكافحة جرائم تقنية المعلومات على الانتفاع بدون حق بخدمات الاتصالات والمعلومات وتقنيتها، حيث نصت المادة (١٣) على أن "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".

المصلحة محل الحماية القانونية:

تقوم المصلحة محل الحماية القانونية في هذه الجريمة على توفير الحماية اللازمة لأصحاب خدمات الاتصالات وخدمات البث المرئي أو المسموع من الأضرار المادية الواقعة عليهم من أعمال السرقة أو القرصنة الإلكترونية.

وسوف نتناول ركني الجريمة المادي والمعنوي بالإضافة إلى الشرط المفترض، ونتبعهم بالعقوبة المقررة لها، وذلك على النحو التالي:

أولاً: الشرط المفترض:

يتعلق الشرط المفترض في هذه الجريمة في محلها، حيث تطلب المشرع أن يقع الانتفاع على خدمة من خدمات الاتصالات أو خدمات قنوات البث المرئي أو المسموع حتى تتحقق الجريمة، ومن أمثلة الاعتداء على تلك الخدمات قيام الجاني باستخدام خدمات شبكة الإنترنت باستخدام برامج خاصة عبر الأقمار الصناعية، أو قيامه بنقل القنوات التليفزيونية أو الإذاعية المشفرة.

ثانياً: الركن المادي:

يتمثل الركن المادي في هذه الجريمة في كل فعل إيجابي يصدر عن الجاني من شأنه الحصول على منفعة، ولم يتطلب المشرع أن يكون الجاني قد حصل على المنفعة لنفسه وإنما تتحقق الجريمة في حقه حتى لو كانت للغير.

ولم يحدد المشرع الوسائل التي يتم الانتفاع بها فهي كثيرة لا حصر لها، وإنما حدد محل الانتفاع بالخدمات على سبيل الحصر وليس المثال وهي إحدى وسائل شبكة النظام المعلوماتي أو إحدى وسائل تقنية المعلومات المتعلقة بخدمة اتصالات[١] أو خدمة من

(١) ولما كان المستقر عليه فقهاً أنه "يقصد بتقديم خدمة الاتصالات هو توفير إمكانية الاتصال بأي وسيلة، ومن أهم هذه الخدمات خدمة نقل الصوت والصورة عبر الأجهزة المعدة لذلك، كما أن المشرع جرم فعل تقديم خدمات

خدمات قنوات البث المسموع أو المرئي، ومن ثم تتحقق الجريمة إذا استخدم الجاني برامج لفك التشفير الخاص بإحدى القنوات التليفزيونية بغرض الحصول على خدمات البث التليفزيوني.

كما اشترط المشرع لتحقق الركن المادي للجريمة أن يكون هذا الانتفاع قد تم بدون وجه حق، ويعرف الانتفاع بأنه هو تحقيق أكبر قدر من الاستفادة سواء أكانت استفادة مادية أو معنوية أو أدبية، وقد اعتبر المشرع أن هذا الانتفاع أو الاستغلال واستخدام هذه التقنية دون حق مشروع من قبيل الأفعال غير المشروعة المجرمة أو القرصنة التي تستوجب العقاب، بل اعتبرها جريمة تشبه إلى حد كبير جريمة السرقة، وقد عرفها المشرع بأنها كل انتفاع يتم بدون وجه حق عن طريق شبكة النظام المعلوماتي أو إحدى وسائل تقنية المعلومات بخدمة اتصالات أو خدمة من خدمات قنوات البث المسموع أو المرئي[١]، ويكون الانتفاع قد تم بدون وجه حق إذا كان مخالفاً لشروط توفير تلك الخدمات، أو المخالفة للحقوق الاقتصادية لأصحابها[٢].

ثالثاً: الركن المعنوي:

تعد هذه الجريمة من الجرائم العمدية التي لا يتصور ارتكابها بطريق الخطأ، فلابد أن

الاتصالات للغير دون الحصول على ترخيص بذلك من الجهاز القومي لتنظيم الاتصالات ويستلزم الأمر لتحديد الركن المادي لهذه الجريمة معرفة المقصود بخدمه أو خدمات الاتصالات التي يحظر تقديمها بدون هذا الترخيص، وأطلق المشرع لفظ تقديم خدمات الاتصالات دون تحديد لطريقة أو أسلوب هذا التقديم للخدمة ودون تحديد لشخص من يقدمها"، حكم محكمة القاهرة الاقتصادية في القضية رقم ٣٠٣٧ لسنة ٢٠٠٩، جلسة ٢١-١-٢٠١٠.

(١) د/ حاتم أحمد محمد بطيخ، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات "دراسة تحليلية مقارنة"، القاهرة، جامعة مدينة السادات – كلية الحقوق، مجلة الدراسات القانونية والاقتصادية، أغسطس ٢٠٢١، العدد ١، المجلد ٧، ص ٣٨.

(٢) لم يشترط القانون لثبوت جريمتي إنشاء وتشغيل شبكة اتصالات خاصة بالبث الإذاعي المسموع والمرئي– دون الحصول على ترخيص من الجهة الإدارية– قيام أدلة معينة بل للمحكمة أن تكون اعتقادها بالإدانة في هاتين الجريمتين من كل ما تطمئن إليه من ظروف الدعوى وقرائنها، حكم محكمة النقض في الطعن رقم ٦٥ لسنة ٨٢ ق، جلسة ٢٠١٢/٦/١١.

يتوافر القصد الجنائي العام بعنصرية العلم والإرادة[١]، فيجب أن يكون الجاني على علم بأنه يقوم بفعل من شأنه الانتفاع أو الحصول على خدمة غير مسموح له بالحصول عليها، وأنه يقوم بهذا الانتفاع بدون وجه حق، كما يجب أن تتجه إرادته الحرة الواعية إلى استخدام تلك الوسائل والتقنيات في الحصول على هذه الخدمة أو المنفعة، ولا عبرة بالباعث على ارتكاب الجريمة حتى ولو كان الباعث على ذلك نبيلاً[٢][٣].

رابعاً: العقوبة:

عاقب المشرع مرتكب هذه الجريمة بعقوبة الحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين.

المطلب الثاني

جريمة الدخول غير المشروع

جرم المشرع في قانون مكافحة جرائم تقنية المعلومات جريمة الدخول غير المشروع عبر تجريم أفعال الدخول والبقاء غير المشروع لموقع أو حساب أو نظام معلوماتي، فنصت المادة (١٤) على أن "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

(١) إن القانون لا يتطلب عادة قصداً خاصاً في الجرائم الاقتصادية بل أنه يفترض غالباً القصد العام من مجرد وقوع المخالفة، حكم محكمة القاهرة الاقتصادية في القضية رقم ٥٠٢ لسنة ٢٠١٠، جلسة ٣-٣-٢٠١٠.

(٢) د/ رامي متولي القاضي، شرح قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ (مقارناً بالتشريعات والمقارنة والمواثيق الدولية)، القاهرة، مركز الدراسات العربية، ٢٠٢٠، الطبعة الأولى، ص ٨٩.

(٣) كما ذهبت محكمة القاهرة الاقتصادية إلى أنه "يتمثل الركن المادي في جريمة نشر مصنفاً محمياً عبر أجهزة الحاسب الآلي بدون إذن كتابي في عنصرين الأول إتيان المتهم لفعل النشر عن طريق الأجهزة الإلكترونية والثاني أن يكون مقارفة المتهم للواقعة المادية دون إذن مسبق من المؤلف أو صاحب الحق المجاور، أما الركن المعنوي يتمثل في توافر العلم والإرادة لدى المتهم من أنه يعلم بأنه ينشر المصنف بإحدى الوسائل الإلكترونية أو غيرها، لأن المشرع لم يحصر تلك الوسائل وأن يكون ذلك النشر بدون إذن المؤلف أو صاحب الحق المجاور وأن تتوافر لدية إرادة تحقيق ذلك، القضية رقم ٥٧٣ لسنة ٢٠١٠، جلسة ٤-٣-٢٠١٠.

محظور الدخول عليه. فإذا نتج عن ذلك الدخول 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".

المصلحة محل الحماية القانونية:

قرر قانون العقوبات المصري مصلحة واجبة الحماية في كل جريمة تستوجب العقاب، وذهبت كافة القوانين العقابية الأخرى على ذات النهج، والتي من بينها الجرائم التي تنطوي على المساس بالحقوق والحريات الأساسية للأفراد– أو أي مصلحة عامة أخرى– فهي تعد إهداراً لمصلحة الدولة في سلامة أمنها وأمن أفرادها(١)، وتقوم المصلحة على عنصرين: الأول الباعث؛ وهو الحاجة إلى حماية الحق محل الحماية القانونية، والثاني الغاية؛ وهو المصلحة الناتجة عن تحقيق حماية القانون للحق المعتدي عليه(٢).

وتقوم المصلحة محل الحماية هنا على مواجهة حالات الاعتداء غير المشروع على الأنظمة المعلوماتية والمواقع الإلكترونية والحسابات الشخصية، وحمايتها عبر إضفاء الحماية القانونية عليها، ولمواجهة أفعال الاختراق المعلوماتي، وفيما يلي سوف نُبين أركان هذه الجريمة بالإضافة إلى الشرط المفترض لها، وذلك على النحو التالي:

أولاً: الشرط المفترض:

يلزم أن يتوافر الشرط المفترض وقت مباشرة الفاعل لنشاطه الإجرامي، وهو يعتبر عنصر سابق على السلوك الذي يلزم وجوده كي يثبت لهذا السلوك صفته الإجرامية، فهو يسبق ارتكاب الجاني لنشاطه الإجرامي كما إنه مستقل عن هذا النشاط، على اعتبار أنه

---

(١) تُعرف المصلحة بأنها هي "العلاقة بين شخص ومال أو هي الحكم التقييمي الذي يسبغه صاحب الحاجة على الوسيلة التي تكفل إشباعها بصورة مشروعة، للمزيد، أنظر. د/ حسنين إبراهيم صالح عبيد، فكرة المصلحة في قانون العقوبات، القاهرة، المجلة الجنائية القومية، يوليو ١٩٧٤، العدد الثاني، المجلد ١٧، ص ص٢٤٠–٢٤١.

(٢) د/ مي ممدوح قايد، السياسة الجنائية لمواجهة الإرهاب المعاصر، القاهرة، دار النهضة العربية، ٢٠٢٢، ص ١٤٧.

المجال الذي تقع فيه الجريمة، كما أنه لازم لتحقق الجريمة[١].

ويتحقق الشرط المفترض هنا في محل الجريمة والمتمثل في المواقع الإلكترونية والنظم المعلوماتية والحسابات الخاصة، ولا يمتد ليشمل المعلومات التي يشملها الموقع أو الحساب أو النظام المعلوماتي، وقد عُرف الموقع بأنه مجال أو مكان افتراضي له عنوان محدد على شبكة معلوماتية، يهدف إلى إتاحة البيانات والمعلومات للعامة أو الخاصة[٢].

كما عُرف الحساب الخاص بأنه 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، بينما يعُرف النظام المعلوماتي بأنه مجموعة برامج وأدوات معدة لغرض إدارة ومعالجة البيانات والمعلومات أو تقديم خدمة معلوماتية[٣].

ثانياً: الركن المادي:

يتمثل الركن المادي في هذه الجريمة في السلوك الإجرامي الذي يتحقق بتوافر أحد الأفعال التي تقوم على اختراق المواقع الإلكترونية أو الحسابات الخاصة أو الأنظمة المعلوماتية والوصول إليها أو البقاء فيها بدون وجه حق، فهي جريمة شكلية تتحقق حتى ولو لم يترتب عليها تحقق النتيجة الإجرامية المترتبة عليها، وقد حدد المشرع صور السلوك الإجرامي على سبيل الحصر وهي[٤]:

---

(١) للمزيد أنظر: د. عبد العظيم مرسي وزير، الشروط المفترضة في الجريمة، القاهرة، دار النهضة العربية، ١٩٨٣، ص ٧٧.

(٢) المادة (١) من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨، تجدر الإشارة إلى إنه تم نشر أول موقع في العالم في ٦ أغسطس عام ١٩٩١ من قبل الفيزيائي البريطاني تيم بيرنرز لي، كما يلغ عدد المواقع المستخدمة حتى عام ٢٠٢١ قرابة الاثنين مليار موقع، وذلك وفقاً لتقرير إحصائيات الإنترنت والحقائق لعام ٢٠٢٢، أخر مطالعة بتاريخ ٢٠٢٣/٦/١٨، https://www.websiterating.com.

(٣) المادة (١) من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨.

(٤) ذهبت المحكمة الاقتصادية بالقاهرة في الجنحة رقم ٦٢٨ لسنة ٢٠٢١ الصادر بجلسة ٢٠٢١/٥/٢٦ إلى أنه قد ثبت أن "المتهم قام باختراق الموقع الخاص بحكومة رأس الخيمة، وقد توافقت جميع الأدلة الفنية مع ما قرره المتهم من أنه قام بالدخول للموقع عبر

١- **الدخول العمدي:** وهو الدخول غير المشروع؛ ويتحقق بفعل إيجابي من شأنه أن يؤدي إلى الدخول أو اختراق موقع إلكتروني أو حساب خاص أو نظام معلوماتي، ولم يتطلب المشرع طريقة معينة للدخول أو الاختراق، كما لم يتطلب صفة خاصة فيمن يقوم بهذا الفعل(١)، بينما اشترط أن يتم الدخول على موقع محظور الدخول عليه، وهذا يعني إنه إذا كان الموقع أو الحساب أو النظام مصرح الدخول إليه فلا تتحقق الجريمة؛ إلا إذا كان هذا الدخول بدون وجه حق من الجاني(٢).

٢- **الدخول غير العمدي:** وقد يحدث هذا الدخول عن طريق الإهمال أو عدم الاحتراز أو نتيجة إخلال الجاني بواجباته، كما إنه يتحقق فعل الدخول بطريق الخطأ حين لم يراعي الجاني التعليمات والقواعد الخاصة بأمن المعلومات الواجب اتباعها(٣)، كما يلزم أن يكون الدخول قد تم لموقع أو حساب أو نظام محظور الدخول عليه.

ثالثاً: الركن المعنوي:

تقنيه GETBYQUERY وهو ما توافق مع تقارير الفحص الخاصة بحكومة رأس الخيمة وتقرير فحص الجهاز القومي للاتصالات، وحيث أن المتهم قد بين أنه بهذه التقنية تمكن من الحصول على أسماء جداول قواعد البيانات وجداول أسماء المستخدمين وهو الأمر الغير متاح للمستخدمين العاديين للموقع ، كما قررت المحكمة أن وجود ثغرة ما بنظام من الأنظمة لا يعطي الحق لمن يحوز علوم تلك التقنيات من أن يقوم باختراقها، لأنه لا يوجد أي نظام مؤمن بشكل كامل وأن أي نظام إلكتروني موجود يحوى ثغرات باختلاف طبيعتها وكيفية اختراقها".

(١) د/ حسنى الجندي، قانون مكافحة جرائم تقنية المعلومات في دولة الإمارات العربية المتحدة، دولة الإمارات العربية المتحدة، الشارقة، أكاديمية العلوم الشرطية، ٢٠٠٩، الجزء الثالث، ص ٧٦.

(٢) قرر المشرع العقاب على جريمة تجاوز الحق في الدخول واعتبرها جريمة مستقلة، بموجب المادة (١٥) من قانون مكافحة جرائم تقنية المعلومات حيث نصت على أن "يعاقب 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 مستخدما حقا مخولا له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول"، ونرى أن المشرع قد ساوى بين دخول الجاني بطريق مشروع أو غير مشروع، فقد يدخل الجاني بطريق مشروع ولكنه تجاوز حدود الحق في الدخول لمدة من الزمن، ونرى أن جريمة الدخول هي جريمة وقتية وإنما جريمة التجاوز فهي جريمة مستمرة تستغرق وقتاً من الزمن.

(٣) د/ رامي متولي القاضي، مرجع سابق، ص ٩٥.

يلزم أن يتوافر القصد الجنائي العام بعنصرية العلم والإرادة، حتى تتحقق هذه الجريمة في الصورة العمدية أو غير العمدية، ففي الصورة العمدية يجب أن يكون الجاني على علم بأنه يقوم بدخول موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه، كما يلزم أن تتجه إرادته الحرة إلى تحقيق هذا الدخول والبقاء فيه(١)، بينما يتحقق الركن المعنوي في الصورة غير العمدية حينما تتجه إرادة الجاني إلى فعل الدخول دون النظر إلى النتيجة، ودون مراعاته قواعد أمن المعلومات المقررة.

رابعاً: العقوبة:

عاقب المشرع كل من دخل عمداً أو بطريق الخطأ غير العمدي وبقى بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه بعقوبة أصلية وهي الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين(٢).

كما حدد حالات تشديد العقاب على سبيل الحصر، وذلك دون الإخلال بحق المحكمة في توقيع العقوبات التبعية التي يمكن الحكم بها وهو ما سنوضحه فيما يلي:

١- **حالات تشديد العقوبة**، وهي:

(أ) إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على الموقع أو الحساب الخاص أو النظام المعلوماتي: شدد المشرع العقوبة لتصبح الحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين؛ وذلك إذا نتج عن الدخول أي من الأفعال المشار إليها(٣).

(ب) الإخلال بالنظام العام: قرر المشرع تشديد العقاب إذا ارتكب الجاني الجريمة بغرض

---

(١) ذهبت المحكمة الاقتصادية بالقاهرة في الجنحة رقم ٦٢٨ لسنة ٢٠٢١ الصادر بجلسة ٢٠٢١/٥/٢٦ إلى أنه "قد ثبت بإقرار المتهم اختراقه للنظام بشكل غير قانوني وتواجده على النظام طوال ثلاث ساعات كامله حتى سقوط وإتلاف النظام، مما يثبت معه قيام المتهم بارتكاب تلك الجرائم وتسببه بأضرار ماليه وأدبيه كبيره لدخوله لنظام غير مصرح له بالدخول إليه بتلك الطريقة والاستيلاء على بياناته وإتلافها".

(٢) المادة (١/١٤) من قانون مكافحة جرائم تقنية المعلومات.

(٣) المادة (٢/١٤) من قانون مكافحة جرائم تقنية المعلومات.

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، وذلك بهدف حفظ كيان الدولة وأمنها القومي من ناحية، وحفظ المبادئ والقيم الأسرية في المجتمع المصري وحرمة الحياة الخاصة للمواطنين من ناحية أخرى، وجعل العقوبة السجن المشدد في هذه الحالة[١].

٢- **العقوبات التبعية:** حدد قانون مكافحة جرائم تقنية المعلومات العقوبات التبعية التي تُوقع على مرتكبيها وهي[٢]:

(أ) المصادرة: منح المشرع للمحكمة في حالة الحكم بالإدانة أن تقضي بمصادرة الأدوات والآلات والمعدات والأجهزة مما لا يجوز حيازتها قانوناً، أو غيرها مما يكون قد استخدم في ارتكاب الجريمة، أو سهل أو ساهم في ارتكابها، وذلك دون الإخلال بحقوق الغير حسني النية.

(ب) غلق المقر: أجاز المشرع الحكم بغلق المقر أو الموقع الخاص بالشخص الاعتباري، إذا لم يكن حاصلاً على ترخيص بمزاولة النشاط من إحدى الجهات الحكومية المصرح لها بذلك.

(ج) العزل: للمحكمة إذا قضت بالإدانة على أحد الموظفين العموميين، لارتكابه جريمة من الجرائم المنصوص عليها في هذا القانون، أثناء وبسبب تأديته لوظيفته، أن تقضي بعزله مؤقتاً من وظيفته، إلا إذا كان الغرض من ارتكاب الجريمة الإخلال بالنظام العام أو تعريض

---

(١) ذهبت المحكمة الإدارية العليا إلى إن "المشرع قرر في قانون تقنية المعلومات عقوبات تتسم بالشدة لحفظ كيان الدولة وأمنها القومي من ناحية، وحفظ المبادئ والقيم الأسرية في المجتمع المصري وحرمة الحياة الخاصة للمواطنين من ناحية أخرى، بل إن المشرع شدد العقوبة بالمادة (٣٤) منه إذا وقعت أي الجريمة 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"، الطعن رقم ٤٣١٨١ لسنة ٦٥ق.ع- بتاريخ ٢٠٢١/٦/١٩.

(٢) تجدر الإشارة إلى أن المشرع حدد العقوبات التبعية التي توقع على مرتكبي أي من الجرائم الواردة بقانون مكافحة جرائم تقنية المعلومات بالمادتين (٣٨، ٣٩)، وهي تنطبق على كافة الجرائم الواردة بالقانون لذا نكتفي بالتعرض لها في هذا المحل منعاً للتكرار.

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 فيكون العزل وجوبياً.

المطلب الثالث

الاحتيال على بطاقات البنوك والخدمات وأدوات الدفع الإلكتروني

تعتبر التطورات العلمية والتحولات الاقتصادية والثقافية العالمية والمحلية من أهم العوامل التي أثرت بل ساهمت في ظهور هذه الجرائم التقنية والتي قد تمثل انتهاكاً لخدمات المجتمع الرقمية، وانتشارها بصورة سريعة ومرعبة مما جعلها تجتاح العالم بأسره[١].

فعدم وجود التشريع المناسب والعقوبة الرادعة كان من أخطر هذه العوامل وأهمها؛ نظراً لحداثة هذه الطائفة من الجرائم والمجرمين، واعتماد أغلب الدول على التشريعات التقليدية القديمة التي أصبحت لا تتناسب مع خطورة هذه الطائفة من الجرائم المعلوماتية[٢].

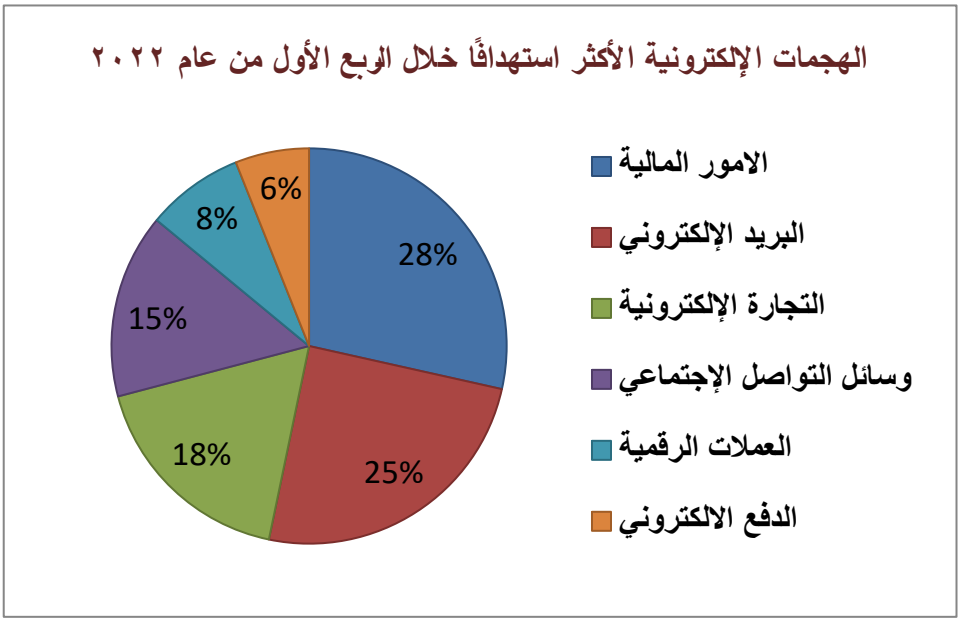
وهناك إحصائيات توضح تصنيف الهجمات الإلكترونية حسب وسيلة ارتكابها، وقد أبرزت أن المعاملات المالية هي التي كانت عرضة أكثر للهجمات الإلكترونية خلال الربع الأول من عام ٢٠٢٢ على مستوى العالم، حيث بلغت الهجمات الإلكترونية نحو المؤسسات المالية في العالم نحو (٢٣.٦٪)[٣].

---

(١) د/ صالح سليمان عبد العظيم، الأبعاد والتأثيرات الاجتماعية المرتبطة باستخدام الإنترنت على الأسرة العربية، دراسة ميدانية على عينة من طالبات جامعة الإمارات العربية، ورقة مقدمة إلى مؤتمر واقع الأسرة في المجتمع، تشخيص للمشكلات واستكشاف لسياسات المواجهة، المنعقد بدار الضيافة، جامعة عين شمس، في الفترة من ٢٦– ٢٨ سبتمبر ٢٠٠٤، ص٢٥ وما بعدها.

(٢) د/ حاتم أحمد محمد بطيخ، مرجع سابق، ص ٥.

(٣) إحصائية بعنوان الصناعات عبر الإنترنت الكثر استهدافاً بهجمات التصيد اعتباراً من الربع الأول من عام ٢٠٢٢، منشورة بتاريخ ٢٠٢٢/٧/٧، أخر مطالعة بتاريخ ٢٠٢٣/٥/٢٣، https://www.statista.com/statistics/٢٦٦١٦١/websites-most-affected-by-phishing/.



وتعد جرائم الاحتيال الإلكتروني من أهم الجرائم المعلوماتية وأكثرها انتشاراً في الوقت الراهن، وتتحقق جرائم الاحتيال الإلكتروني بالاعتداء على الخدمات التي تقدمها الجهات المصرفية بالدولة للمواطنين، لذا نصت المادة (٢٣) من قانون مكافحة جرائم تقنية المعلومات على أن "يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة 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 أو بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الإلكترونية. فإن قصد من ذلك استخدامها في الحصول على أموال الغير أو ما تتيحه من خدمات يعاقب 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، وبغرامة 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".

وتختلف مفاهيم الاحتيال الإلكتروني فيذهب رأي إلى إنه سلوك احتيالي ينتهج منهج

الحوسبة بنية الحصول على امتياز مالي، كما ذهب اتجاه أخر إلى أنه التلاعب العمدي بمعلومات وبيانات تمثل قيماً مادية يختزنها نظام الحاسب الآلي، أو الإدخال غير المصرح به لمعلومات وبيانات صحيحة، أو التلاعب في الأوامر والتعليمات التي تحكم عملية البرمجة، أو أية وسيلة أخرى من شأنها التأثير على الحاسب الآلي، حتى يقوم بعملياته بناءً على هذه البيانات أو الأوامر أو التعليمات، من أجل الحصول على ربح غير مشروع وإلحاق الضرر بالغير[١].

ونأخذ على المشرع إنه لم يضع تعريف محدد لجرائم الاحتيال الإلكتروني ضمن التعريفات الواردة بالقانون، لذا نرى إنه يلزم تعريف "الاحتيال الإلكتروني بأنه: كل فعل يؤدي إلى التأثير على نظام إلكتروني أو نظام معلوماتي أو شبكة معلوماتية أو أية وسيلة تقنية معلوماتية أو جهاز حاسب آلي أو توقيع إلكتروني أو معلومات إلكترونية وذلك عن طريق البرمجة أو الحصول أو الإفصاح أو النقل أو النشر لرقم أو كلمة أو رمز سري أو بيانات سرية أو خاصة أخرى، بقصد الحصول على منفعة دون وجه حق أو للإضرار بالغير"[٢].

وقد أسفرت جهود الحكومة المصرية خلال الأسبوع الأول من عام ٢٠٢٣ إلى ضبط متهم ارتكب واقعة في مجال (الاحتيال المصرفي والاستيلاء على بيانات البطاقات البنكية) مما مكن الدولة من استرداد مبالغ مالية بلغت (٢٥ مليون جنيه)، بينما تم ضبط عدد (٢٤) قضية خلال شهر ديسمبر عام ٢٠٢٢[٣]، كما يقع عدد(٢,٢٤٤) هجوماً إلكترونياً يومياً، أي ما يعادل أكثر من (٨٠٠,٠٠٠) هجوم سنوياً، هذا ما يقرب من هجوم واحد كل ٣٩ ثانية[٤].

وقد بلغ عدد جرائم الاحتيال بالبريد الإلكتروني (BEC) قد بلغ (١٩٩٥٤) جريمة، في

---

(١) د/ محمد طارق، جريمة الاحتيال عبر الإنترنت، مصر، منشورات الحلبي الحقوقية، الطبعة الأولى، ٢٠١١، ص٣٧.

(٢) وذلك على غرار التشريع الكويتي الصادر بالقانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات.

(٣) الموقع الرسمي لوزارة الداخلية، أخر مطالعة بتاريخ ١٩-٥-٢٠٢٣، https://www.moi.gov.eg/news/GetDetails٣.

(٤) تقرير بعنوان "إحصائيات وحقائق واتجاهات الأمن السيبراني لعام ٢٠٢٣"، أخر مطالعة بتاريخ ٢٠٢٣/٨/٢٢، https://www.websiterating.com/ar/research/cybersecurity-statistics-facts/.

حين إنه بلغ عدد جرائم الاحتيال بواسطة بطاقات الائتمان (١٦٧٥٠) جريمة على مستوى العالم خلال عام ٢٠٢١[١].

المصلحة محل الحماية القانونية:

تتمثل المصلحة في تجريم جرائم الاحتيال والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الإلكتروني في تحقيق الاستقرار وضمان أمن المجتمع ورعاية مصالح مواطنيه المالية، وذلك بمواجهة صور الاعتداء على الأموال من خلال ارتكاب عمليات الاحتيال عبر شبكة الإنترنت والاستخدام غير المشروع لبطاقات الدفع الإلكتروني مع توفير الحماية لتلك الوسائل.

وفيما يلي نقوم بإيضاح أركان هذه الجريمة بالإضافة للشرط المفترض، والعقوبة المقررة لمرتكبها؛ وذلك على النحو التالي:

أولاً: الشرط المفترض:

يتحقق الشرط المفترض في هذه الجريمة في محلها والذي يتمثل في الشبكات الإلكترونية أو أدوات الدفع الإلكتروني التي تشمل البطاقات البنكية وبطاقات الخدمات، وقد ذكر المشرع هذه البطاقات على سبيل المثال وليس الحصر، بحيث يتسع النص ليشمل كافة أنواع الوسائل والبطاقات التي قد تُستحدث مُستقبلاً.

ويؤخذ على المشرع المصري إنه لم يتعرض لتعريف بطاقات الدفع الإلكتروني، ونرى إنه يمكن تعريفها بأنها هي "البطاقة الإلكترونية التي تحتوي على شريط ممغنط أو شريحة ذكية أو غيرها من وسائل تقنية المعلومات والتي تحتوي على بيانات أو معلومات إلكترونية والتي تصدرها الجهات المرخص لها بذلك"[٢].

---

(١) حيث يقوم المجرمون باختراق أنظمة البريد الإلكتروني للحصول على معلومات عن أنظمة الدفع الخاصة بالأشخاص أو الشركات، وتحويل الأموال إلى حسابهم المصرفي، إحصائية بعنوان "أكثر أنواع الجرائم الإلكترونية التي يتم الإبلاغ عنها شيوعًا في عام ٢٠٢١"، مرجع سابق، أخر مطالعة بتاريخ ٢٠٢٣/٥/١٥.

(٢) وذلك على غرار التشريع القطري الصادر بالقانون رقم ١٤ لسنة ٢٠١٤ بشأن مكافحة جرائم تقنية المعلومات، والتشريع العماني الصادر مرسوم سلطاني رقم ٢٠١١/١٢ بإصدار قانون مكافحة جرائم تقنية المعلومات.

ثانياً: الركن المادي:

تعد هذه الجريمة من الجرائم الشكلية التي يكفي لتحققها ارتكاب الجاني السلوك الإجرامي دون أن يتوقف على تحقق النتيجة الإجرامية المترتبة على هذا السلوك، ويقوم السلوك الإجرامي لهذه الجريمة 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(١).

ثالثاً: الركن المعنوي:

يتحقق الركن المعنوي لهذه الجريمة بتوافر القصد الجنائي الذي يُعد شرطاً ضرورياً لكى تقوم المُساءلة الجنائية في حق الجاني، وقد يتخذ صوراً متنوعة منها: القصد العام والقصد الخاص، وأساس التمييز بينهما؛ هو النظر إلي ما إذا كان الشارع يتطلب في الجريمة حصول نتيجة إجرامية معينة، أو وقوعها بباعث خاص(٢)، حيث تعد هذه الجريمة من الجرائم العمدية التي لا يتصور ارتكابها بصورة غير عمدية.

فيجب أن يتوافر القصد الجنائي العام بعنصريه العلم والإرادة، وذلك بأن يكون الجاني على علم بأنه يستخدم أو يستعمل الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول إلى أرقام أو بيانات بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الإلكترونية وذلك دون وجه حق أي بشكل غير مشروع، كما يلزم أن تتجه إرادته إلى القيام بهذا

---

(١) وكانت جريمة النصب تتطلب لتوافرها أن يكون ثمة احتيال وقع من المتهم على المجني عليه بقصد خداعة والاستيلاء على ماله فيقع المجنى عليه ضحية الاحتيال الذي يتوافر باستعمال طرق احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة أو بالتصرف في مال الغير ممن لا يملك التصرف، وقد نص القانون على أن الطرق الاحتيالية في جريمة النصب يجب أن يكون من شأنه الإيهام بوجود مشروع كاذب أو واقعة مزورة أو إحداث الأمل بحصول ربح وهمي أو غير ذلك، حكم محكمة النقض في الطعن رقم ١٤٤٦٧ لسنة ٨٩ ق– بتاريخ ٢٤/ ٢٠٢٢/٥.

(٢) د/ مي ممدوح قايد، مرجع سابق، ص ٢٧٤.

الاحتيال[١]، كما يتطلب المشرع قصداً خاصاً في هذه الجريمة إلى جانب القصد العام، فلا قيام للقصد الخاص بغير قصد عام، ومن ثم فالبحث في توافر القصد الخاص مفترضاً ثبوت توافر القصد العام[٢]، ويتحقق القصد الخاص لهذه الجريمة متى كان الهدف هو من ارتكابها الحصول على أموال الغير أو غير ذلك من خدمات.

رابعاً: العقوبة:

عاقب المشرع كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أو بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الإلكترونية بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن ثلاثين ألف جنيه، ولا تجاوز خمسين ألف جنيه أو بإحدى هاتين العقوبتين.

كما شدد المشرع العقاب في حالات معينة على سبيل الحصر وهي:

- **استخدام البطاقات في الحصول على أموال الغير أو غيرها من الخدمات:** شدد المشرع العقوبة لتصبح الحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين.
- **الاستيلاء للنفس أو للغير على تلك الخدمات أو الأموال:** شدد المشرع العقاب لتصبح العقوبة الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو إحدى هاتين العقوبتين.

---

(١) يقصد بالركن المعنوي الحالة النفسية التي كان عليها الجاني أثناء ارتكابه للجريمة وهو يتخذ صورتين هما: صورة الخطأ العمدي (القصد الجنائي)، وصورة الخطأ غير العمدي (الإهمال وعدم الاحتياط)، ويعرف القصد الجنائي بأنه: هو انصراف إرادة الجاني إلى ارتكاب الجريمة مع العلم بأركانها القانونية، لذا فإنه يجب توافر عنصري العلم والإرادة، للمزيد أنظر.. د. حاتم عبدالرحمن منصور الشحات، الضوابط القضائية للركن المعنوي في جرائم العنف، الكويت، جامعة الكويت، مجلة الحقوق، ديسمبر ٢٠١٢، العدد ٤.

(٢) د/عبدالولى أحمد صالح المرهبي، مكافحة جرائم خطف الأشخاص، القاهرة، أكاديمية الشرطة،٢٠٠٩، ص٢٠٩.

المبحث الثالث

مواجهة الدولة لجرائم الاعتداء على الشبكات المعلوماتية

تمهيد وتقسيم:

في إطار مكافحة الاستخدام غير المشروع للحاسبات وشبكات وتقنيات المعلومات، وما يرتبط بها من جرائم، فقد جرم المشرع في قانون مكافحة تقنية المعلومات الأفعال التي قد تمثل اعتداء عليها، وذلك مع التزام المشرع بالدقة في تحديد تلك الأفعال، وتجنب التعبيرات الغامضة بوضع تعاريف دقيقة لها، وتحديد عناصر الأفعال المجرمة بكثير من العناية، دون الإخلال بالاعتبارات الشخصية للمجنى عليهم، والاعتبارات المتعلقة بالمصلحة العامة وحماية الأمن والاقتصاد القوميين.

فقد قرر المشرع حماية خاصة لحماية البيانات والمعلومات الإلكترونية الخاصة بالدولة أو أحد الأشخاص الاعتبارية العامة وذلك نظراً لطبيعتها الخاصة وتعلقها بمصالح المجتمع العليا، من خطر الاعتراض أو الاختراق أو العبث بها أو إتلافها أو تعطيلها بأي صورة كانت؛ وفيما يلي سوف نتناول الجرائم التي تمثل اعتداء على الخدمات التي تقدمها الدولة للمواطنين من خلال ما يلي:

المطلب الأول: الاعتداء على أنظمة الدولة المعلوماتية.

المطلب الثاني: الاعتداء على سلامة الشبكة المعلوماتية.

المطلب الثالث: العبث بالأدلة الرقمية.

المطلب الأول

الاعتداء على أنظمة الدولة المعلوماتية

حفاظاً على صون هيبة الدولة وسرية بياناتها، قرر المشرع عقوبة رادعة لجريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة، حيث نصت المادة (٢٠) من قانون مكافحة تقنية المعلومات على أن "يعاقب 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 بخطأ غير عمدي وبقى بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعاً أو بريداً إلكترونياً أو حساباً خاصاً أو نظاماً معلوماتياً يدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكا 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. وفي جميع الأحوال، إذا ترتب على أي من الأفعال السابقة إتلاف تلك البيانات أو المعلومات 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 إلغائها كلياً أو جزئياً، بأي وسيلة كانت، تكون العقوبة السجن، والغرامة التي لا تقل عن مليون جنيه ولا تجاوز خمسة ملايين جنيه".

تجدر الإشارة إلى أنه من أبرز وقائع الاعتداء على الأنظمة المعلوماتية للدولة ما تم الإعلان عنه من قِبل قراصنة إيرانيون يطلق عليها أسم "بلاك ريوارد" أو "المكافأة السوداء" بتاريخ ٢٢ أكتوبر ٢٠٢٢، أنهم اخترقوا نظام البريد الإلكتروني الداخلي لشركة إنتاج وتطوير الطاقة النووية الإيرانية، وأنها ستنشر البيانات التي حصلت عليها في غضون ٢٤ ساعة، ما لم تفرج السلطات عن جميع السجناء السياسيين والمتظاهرين[١].

المصلحة محل الحماية القانونية:

تتمثل المصلحة هنا في حماية الأنظمة المعلوماتية للدولة وما تحتويه من بيانات ومعلومات إلكترونية متعلقة بها أو أحد سلطاتها أو أجهزتها أو وحداتها أو الهيئات العامة أو الهيئات المستقلة أو الأجهزة الرقابية أو هيئاتها العامة الخدمية أو الاقتصادية وغيرها من الأشخاص الاعتبارية العامة أو ما في حكمها المتاحة على الشبكة المعلوماتية أو أي نظام

(١) جدير بالذكر أن تلك المجموعة قامت بالعديد من حوادث الاختراق الإلكتروني للأنظمة الإيرانية، أخر مطالعة بتاريخ ٢٠٢٣/٥/١٨، . https://www.skynewsarabia.com/world/١٥٦٤٩٣٧-%D٩٪٨٢

معلوماتي أو حاسب خاص بها من الاعتداءات[١]، لكونها تعوق سلطات الدولة في القيام بواجباتها وتهدد بناء المجتمع واستقراره، كما إنها تهدد الاقتصاد القومي وتؤثر على جميع أنشطة الدولة[٢].

وسوف نتناول فيما يلي دراسة هذه الجريمة من خلال توضيح أركانها؛ وذلك على النحو التالي:

أولاً: الشرط المفترض:

يتمثل في محل الجريمة وهو البريد أو الموقع الإلكتروني أو الحساب أو النظام المعلوماتي الذي يدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكا لها، أو يخصها.

ثانياً: الركن المادي:

يتحقق بمجرد قيام الجاني بارتكاب أي من الأفعال التي تمثل السلوك الإجرامي لهذه الجريمة، وهي (الدخول العمدي، الدخول غير العمدي "بخطأ" مع البقاء بدون وجه حق، تجاوز حدود الحق من حيث الزمان أو مستوى الدخول، أو الاختراق[٣])، على بريد أو موقع إلكتروني أو حساب مملوك للدولة أو أحد الأشخاص الاعتبارية العامة أو يدار بمعرفتها أو لحسابها أو

---

(١) قرر المشرع حماية خاصة لأسرار الدولة والبيانات والمعلومات الإلكترونية المتعلقة بها أو أحد سلطاتها أو أجهزتها، وحدد 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 والصور والأصوات، وما في حكمها، وأن البرنامج المعلوماتي عبارة عن 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 شكلها الأصلي أو في أي شكل آخر تظهر فيه من خلال حاسب آلي أو نظام معلوماتي، حكم المحكمة الإدارية العليا في الطعن رقم ٥٩٥٦٨ لسنة ٦٤ ق.ع- بتاريخ ٢٠٢٠/٦/١٣.

(٢) د/ ميادة مصطفي محمد المحروقي، المواجهة الجنائية الموضوعية للتنظيمات الإرهابية، المنصورة، كلية الحقوق- جامعة المنصورة، مجلة البحوث القانونية والاقتصادية، أغسطس ٢٠١٧، العدد ٦٣، الجزء الأول، ص ٥٠٦.

(٣) الاختراق يشتمل على 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، حكم المحكمة الإدارية العليا في الطعن رقم ٥٩٥٦٨ لسنة ٦٤ ق.ع- بتاريخ ٢٠٢٠/٦/١٣.

يخصها[١]، لذا تعد هذه الجريمة من الجرائم الشكلية فيكفي لتحققها ارتكاب الجاني السلوك الإجرامي دون أن يتوقف على تحقق النتيجة.

ثالثاً: الركن المعنوي:

يتحقق بتوافر القصد الجنائي العام بعنصريه العلم والإرادة، وقد يقوم بصورة عمدية وبصورة الخطأ غير العمدي، ففي الصورة العمدية لابد أن يكون الجاني على علم بدخوله بدون وجه حق موقع أو بريد إلكتروني أو حساب خاص مملوك للدولة أو لأحد الأشخاص الاعتبارية العامة وبقاءه عليه أو تجاوز حدود هذا الحق، أو قام باستخدام أية برامج لاختراقها، كما يجب أن تتجه إرادته الحرة الواعية إلى تحقيق ذلك، بينما في صورة الخطأ غير العمدي فإرادة الجاني لا تتجه إلى الدخول غير المشروع لتلك المواقع أو الحسابات وإنما يتحقق الدخول بفعل الجاني نتيجة عدم مراعاته لقواعد أمن الحسابات والنظم المعلوماتية[٢].

رابعاً: العقوبة:

عاقب المشرع كل من دخل عمداً، أو بخطأ غير عمدي وبقى بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعاً أو بريداً إلكترونياً أو حساباً خاصاً أو نظاماً معلوماتياً يدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكاً لها، أو يخصها؛ بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن

---

(١) ومن حيث أن ما نُسب إلى الطاعن من أنه أخترق أجهزة الحاسب الآلي بالهيئة العامة للرقابة المالية مما تسبب في انتهاك سرية البيانات الموجودة عليها ومحاولة نسخها، مما يشكل في حقه خروجاً جسيماً على قواعد قانون مكافحة جرائم تقنية المعلومات وعدواناً أثيماً على الأنظمة المعلوماتية الخاصة بالدولة متجاوزاً حدود الحق المخول له من حيث الزمان أو مستوى الدخول مخترقاً نظامًا معلوماتيًا يُدار لحساب الدولة ممثلاً في أحد الأشخاص الاعتبارية العامة– الهيئة العامة للرقابة المالية– مما يستوجب مساءلته عنه تأديبياً مع أخذه بالشدة الرادعة، كما أن عملية الاختراق لأجهزة الحاسب الآلي بالهيئة ثابت في حقه عن طريق الدليل الرقمي وليس الورقي بحسبان أن الأدلة الرقمية هي السبيل لكشف مكافحة جرائم تقنية المعلومات، حكم المحكمة الإدارية العليا في الطعن رقم ٦٠١٦٩ لسنة ٦٤ ق.ع– بتاريخ٢٠٢٠/٦/١٣.

(٢) إن الأدلة في المواد الجنائية متساندة يكمل بعضها بعضاً ومنها مجتمعة تتكون عقيدة القاضي فلا ينظر إلى دليل بعينه لمناقشته على حده دون باقي الأدلة، كما لا يشترط في الدليل أن يكون صريحاً دالاً بنفسه على الواقعة المراد إثباتها بل يكفى أن يكون استخلاص ثبوتها عن طريق الاستنتاج"، حكم محكمة النقض في الطعن رقم ١٣٦٨ لسنة ٩١ ق– بتاريخ ٢٠٢٢/٢/١٠.

خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين.

كما شدد المشرع العقاب في بعض الحالات نظراً لخطورة هذه الجريمة وهي:

- **الدخول بقصد الاعتراض[١] أو الحصول بدون وجه حق على بيانات أو معلومات حكومية[٢]:** شدد المشرع العقاب لتصبح العقوبة السجن، والغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه.
- **إتلاف تلك البيانات أو المعلومات أو الموقع إتلافاً كلياً أو جزئياً:** شدد المشرع العقاب إذا ترتب على أي من الأفعال السابقة إتلاف تلك البيانات أو المعلومات 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 إلغائها كليا أو جزئيا، بأي وسيلة كانت لتصبح العقوبة السجن، والغرامة التي لا تقل عن مليون جنيه ولا تجاوز خمسة ملايين جنيه.

المطلب الثاني

الاعتداء على سلامة الشبكة المعلوماتية

جرم قانون مكافحة جرائم تقنية المعلومات الاعتداء على الشبكة معلوماتية بأي صورة من الصور فقررت المادة (٢١) أن "يعاقب 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 متعمدا 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. ويعاقب

---

(١) عرفت المادة (١) من قانون مكافحة جرائم تقنية المعلومات الاعتراض بأنه هو "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".

(٢) عرفت المادة (١) من قانون مكافحة جرائم تقنية المعلومات البيانات الحكومية بأنها هي "بيانات متعلقة 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".

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".

وقد عرف القانون الشبكة المعلوماتية بأنها هي مجموعة من الأجهزة أو نظم المعلومات تكون مرتبطة معاً، ويمكنها تبادل المعلومات والاتصالات فيما بينها وتبادل الخدمات الإلكترونية وتيسير سبل تقديمها للمواطنين، ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية، والتطبيقات المستخدمة عليها[١]، ونظراً لأهميتها سواء للأفراد أو الدولة أو الأشخاص الاعتبارية العامة قرر المشرع لها حماية قانونية خاصة.

المصلحة محل الحماية القانونية:

تتمثل المصلحة في حرص المشرع على حماية الشبكة المعلوماتية من محاولات العبث والنيل بها، مع ضمان تأدية وظيفتها على أكمل وجه، وحفاظاً على الأجهزة والمعلومات والبيانات المدونة عليها من أعمال التخريب التي يسبب مخاطر لمستخدميها، وشدد المشرع الحماية بالنسبة للشبكات التابعة للدولة أو الأشخاص الاعتبارية العامة نظراً لخطورتها ولكونها تعرض مصالح المواطنين وأمنهم للخطر؛ وفيما يلي سوف نقوم بإيضاح أركان الجريمة، والعقوبة المقررة لها؛ وذلك على النحو التالي:

أولاً: الشرط المفترض:

يتمثل الشرط المفترض في محل الجريمة وهو الشبكة المعلوماتية، وهي تشمل على مكونات مادية مثل الحاسب الآلي والأجهزة المادية والمعدات، كما تشمل على مكونات معنوية وتتمثل في البرامج والبيانات والمعلومات ونظم تشغيل الشبكات[٢].

تجدر الإشارة إلى أن شبكة المعلومات الدولية (Internet) تعد من أبرز الشبكات

(١) المادة (١) من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨.

(٢) د/ حسنى الجندي، مرجع سابق، ص ١١٧.

المعلوماتية في العالم وهي شبكة حواسيب ضخمة متصلة مع بعضها البعض[١].

ثانياً: الركن المادي:

يقوم الركن المادي لهذه الجريمة على السلوك الإجرامي الذي قد يتخذ الصورة العمدية أو الخطأ، فتتحقق الجريمة في صورتها العمدية متى قام الجاني بفعل إيجابي من شأنه أن يتسبب 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[٢].

أما في صورة الخطأ غير العمدي فيتحقق الركن المادي فيها متى قام الجاني بسلوك غير عمدي تسبب خطأ في إيقاف عمل الشبكة المعلوماتية أو تعطيلها أو التشويش عليها أو الحد من كفاءتها، وقد يتخذ هذا الخطأ صورة الإهمال أو التقصير أو الإخلال بالواجبات، وينبغي أن تتوافر علاقة السببية بين فعل الجاني وما يترتب عليها من إيقاف عمل الشبكة المعلوماتية أو تعطيلها أو التشويش عليها[٣].

---

(١) وتعكس الإحصائيات العالمية لعدد مستخدمي الإنترنت بين ٢٠١٩ والربع الأول من عام ٢٠٢٣ هذا الأمر عبر القفزة التي حققتها، ففي ٢٠١٩ كان ٤.١ مليار شخص وهو ما يعادل (٥٤٪) من سكان العالم يستخدمون الإنترنت، ثم ارتفع عدد المستخدمين ليصل إلى حوالي ٥.١٨ مليار شخص يستخدمون الإنترنت في العالم، أي حوالي (٦٤.٦٪) من سكان العالم، كما أظهرت الإحصائيات أن النمو في أعداد مستخدمي الإنترنت في الدول العربية واضحاً بشكل كبير، https://١-a١٠٧٢.azureedge.net/blogs، مقال بعنوان "أرقام في حياتنا"، منشور بتاريخ ٢٠٢٣/٥/٧، أخر مطالعة بتاريخ ٢٠٢٣/٨/٢٢.

(٢) عرف قانون تقنية المعلومات في المادة (١) منه المعالجة الإلكترونية بأنها هي "أي عملية إلكترونية أو تقنية تتم كليًا أو جزئيًا 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 البيانان والمعلومات الإلكترونية، وذلك باستخدام أي وسيط من الوسائط أو الحاسبات أو الأجهزة الأخرى الإلكترونية أو المغناطيسية أو الضوئية أو ما يُستحدث من تقنيات أو وسائط أخرى".

(٣) تعد علاقة السببية في المواد الجنائية علاقة مادية تبدأ بالفعل الذي اقترفه الجاني، وترتبط من الناحية المعنوية بما يجب أن يتوقعه من النتائج المألوفة لفعله إذا ما أتاه عمداً، وهذه العلاقة موضوعية ينفرد قاضي الموضوع

ثالثاً: الركن المعنوي:

يقوم الركن المعنوي لها على توافر القصد الجنائي العام بعنصرية العلم والإرادة، سواء ارتكبت الجريمة بصورة عمدية أو بطريق الخطأ، ففي الصورة العمدية يجب أن يكون الجاني على علم بأنه يقوم بفعل ينصب على شبكة معلوماتية وأن من شأن هذا الفعل تعطيل أو إيقاف أو التشويش عليها أو الحد من كفاءتها، كما يجب أن تتجه إرادة الجاني الحرة إلى ارتكاب هذا الفعل وإحداث النتيجة المترتبة عليه وذلك بالنسبة للصورة العمدية، أما في صورة الخطأ لم يتطلب المشرع أن تتجه إرادة الجاني إلى إحداث النتيجة الإجرامية، أي إنه يكتفي بعلمه بأنه يقوم بعمل على الشبكة المعلوماتية من دون أن يتخذ إجراءات الحيطة والحذر اللازمين لحماية الشبكة.

رابعاً: العقوبة:

عاقب المشرع 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 بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، وقد حدد المشرع حالات تشديد العقاب لهذه الجريمة، كما جعل من حالة ارتكاب الجريمة بطريق الخطأ ظرفاً مخففاً للعقوبة وهو ما سنوضحه فيما يلي:

١- **العقوبة المشددة:** شدد المشرع العقوبة إذا وقعت الجريمة على شبكة معلوماتية تخص الدولة أو أحد الأشخاص الاعتبارية العامة أو تمتلكها أو تدار بمعرفتها لتصبح السجن المشدد والغرامة التي لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه.

٢- **العقوبة المخففة:** جعل المشرع ارتكاب الجريمة بطريق الخطأ ظرفاً مخففاً للجاني حيث خفف العقوبة لتصبح الحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن خمسين ألف

بتقديرها ومتى فصل فيها إثباتاً أو نفياً فلا رقابة لمحكمة النقض، حكم محكمة النقض في الطعن رقم ١٢٧٥٤ لسنة ٨٢ ق – جلسة ٢٠١٤/٤/٢، موقع محكمة النقض، www.cc.gov.eg.

جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين وذلك لكل من تسبب بخطئه 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، ونرى إنه يمكن أن **يُستخدم هذا التخفيف بصورة خاطئة، فإذا لم يثبت ركن التعمد في حق الجاني يجب أن يتم توقيع العقوبة المقررة دون تخفيف، كما قد يكون هذا الخطأ تم بصورة الإهمال أو عدم اتباع الواجبات وهذا لا يستوجب تخفيف العقاب وإنما على العكس يستلزم تشديد العقوبة، لذا نقترح عدم التفرقة في العقاب بين مرتكبي الجريمة بصورة عمدية أو بطريق الخطأ لتحقيق الردع العام والخاص لأفراد المجتمع.**

المطلب الثالث

العبث بالأدلة الرقمية

حرص المشرع على قيام الجهات الرسمية بعملها، حيث تقوم هذه الجهات بإصدار بعض الخدمات الإلكترونية للمواطنين التي قد تستخدم دليلاً لأفراد أو الجهات ذاتها لإثبات تقديم الخدمة للمواطن والتي قد يترتب عليها تقاضي المواطن للجهة أو العكس، فقد قرر العقاب على كل ما من شأنه أن يعوقها في مباشرة مهامها ومن ذلك العبث بالخدمات الجماهيرية الرقمية وأدلتها، وذلك بتقرير عقوبة منفردة للقائم بذلك، فقد نصت المادة (٢٨) على أن "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 إلكتروني 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".

المصلحة محل الحماية القانونية:

تتمثل المصلحة هنا في حرص المشرع على قيام الجهات الرسمية بعملها على الوجه الأكمل وتوفير المُناخ الملائم لهم، وذلك بتوفير كافة الأدلة والمستندات اللازمة لإثبات الفعل المخالف للقانون، بغرض مجابهة كافة المحاولات في إخفاء أو العبث بالأدلة الرقمية، مما يشكله هذا الفعل من مساعدة الجاني للهروب من المسائلة القانونية، فضلاً عما يمثله الدليل الرقمي من أهمية في الإثبات الجنائي للجرائم المعلوماتية باعتباره الوسيلة الوحيدة لإثبات هذه الجرائم، وفيما يلي سوف نستعرض أركان هذه الجريمة على النحو التالي:

أولاً: الشرط المفترض:

يتمثل الشرط المفترض في هذه الجريمة في عنصرين أساسين لتوافرهما في حق الجاني وهما[١]:

١- **صفة الجاني:** اشترط المشرع في مرتكب هذه الجريمة أن يكون شخصاً مسئولاً عن إدارة الموقع أو الحساب الخاص أو البريد الإلكتروني أو النظام المعلوماتي، فإذا صدر الفعل من شخص غير مسئول لا تتحقق في حقه هذه الجريمة وإنما يخضع لنص عقابي أخر.

٢- **محل الجريمة:** تطلب المشرع أيضاً توافر شرط أخر في هذه الجريمة حتى تتحقق في حق مرتكبها، وهو يتمثل في محلها والمتمثل في الأدلة الرقمية[٢]، وهو ما يعني إنه يلزم أن يكون الفعل الذي يرتكبه الجاني يقع على دليل رقمي يتعلق بأي من الجرائم الواردة بقانون مكافحة جرائم تقنية المعلومات.

---

(١) إذا اشترط القانون توافر شرط معين سواء في صفة الجاني أو محل الجريمة وهو ما يسمى بالشرط المفترض، فالجهل أو الغلط في هذا الشرط ينفي القصد الجنائي لدى المتهم، وبذلك تنعدم الجريمة في حقه، د/ أحمد فتحي سرور، الوسيط في قانون العقوبات- القسم العام، القاهرة، دار النهضة العربية، ٢٠١٥، الطبعة السادسة، ص ٦٧٤.

(٢) عرفت المادة (١) من قانون تقنية المعلومات 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".

ثانياً: الركن المادي:

يتمثل الركن المادي في هذه الجريمة في كل فعل إيجابي يصدر عن المسئول عن إدارة الموقع أو الحساب أو البريد الإلكتروني من شأنه أن يمثل إخفاء أو عبث بأي دليل من الأدلة الرقمية المتصلة بالجرائم الواردة بالقانون(١)، وفيما يلي سوف نوضح صور السلوك الإجرامي لهذه الجريمة:

١- **الإخفاء:** ويقصد بالإخفاء ستر الشيء عن أعين الناس وعدم إظهاره، وهو يؤدي إلى إعادة السلطات المختصة وعرقلتها عن القيام بمهامها في الوصول إلى الحقيقة، ولإخفاء الأدلة عدة صور منها المسح أو الإلغاء، كما إنه يجب أن ينصب هذا الإخفاء على دليل رقمي متصل بجريمة ارتكبت بالفعل(٢).

٢- **العبث:** هو قيام الجاني بفعل من شأنه تغيير طبيعة الدليل أو عناصره، مما يؤدي إلى صعوبة الوصول إلى الجاني، وللعبث عدة صور منها تعديل مضمون الدليل أو مساره أو شكله أو طبيعته.

ثالثاً: الركن المعنوي:

تعتبر هذه الجريمة من الجرائم العمدية التي لا يتصور ارتكابها بصورة غير عمدية، وذلك نظراً لقيام الجاني بفعل إيجابي يؤدي إلى ضياع أو إخفاء الدليل الرقمي، ويقوم الركن المعنوي هنا على القصد الجنائي العام بعنصرية العلم والإرادة، فيجب أن يكون الجاني على علم بأنه يقوم بفعل من شأنه إخفاء الدليل الرقمي أو العبث به وضياعه، كما يجب أن تتجه إرادته إلى تحقيق ذلك الفعل وما قد يترتب عليه من آثار.

---

(١) استقرت أحكام المحكمة الإدارية العليا على أن "المشرع استلزم في جرائم تقنية المعلومات توافر الدليل الرقمي وقرر أن يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط الدعامات الإلكترونية، أو النظام المعلوماتي أو من برامج الحاسب، أو من أي وسيلة لتقنية المعلومات ذات قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائي متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية للقانون المشار إليه وبغير توافر هذا الدليل الرقمي فلا يمكن معاقبة المواطن على جريمة خالية من دليل الإدانة"، الطعن رقم٤٣١٨١ لسنة ٦٥ ق.ع- بتاريخ ٢٠٢١/٦/١٩.

(٢) إسراء محمد على سالم- منى عبد العالي موسي، جريمة إخفاء المال الضائع (دراسة مقارنة)، العراق، جامعة بابل، ٢٠١٤، ص ١٢٨٨، وما بعدها.

كما تطلب المشرع في هذه الجريمة توافر قصد جنائي خاص؛ ويتمثل القصد الخاص هنا في رغبة الجاني في قصد إعاقة عمل الجهات الرسمية المختصة عن القيام بعملها، ويقصد بالسلطات الرسمية هنا السلطات المعنية بمكافحة جرائم تقنية المعلومات.

رابعاً: العقوبة:

عاقب المشرع المسئول عن إدارة موقع أو حساب خاص أو بريد إلكتروني أو نظام معلوماتي، إذا قام بإخفاء دليل رقمي أو عبث به، وكان هذا الدليل متصلاً بإحدى الجرائم المنصوص عليها في قانون مكافحة تقنية المعلومات ووقعت على موقع أو حساب أو بريد إلكتروني بقصد إعاقة عمل الجهات الرسمية المختصة بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين[1].

(١) تجدر الإشارة إلى أن المشرع عاقب المسئول عن إدارة الموقع أو الحساب الخاص أو البريد الإلكتروني أو النظام المعلوماتي الذي يعرض أيا منها لإحدى الجرائم الواردة بالقانون بعقوبة الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين، كما خفف العقوبة حال إنه تسبب بإهماله في تعرض أي منها لإحدى الجرائم المنصوص عليها في القانون، وكان ذلك بعدم اتخاذه التدابير والاحتياطيات التأمينية الواردة في اللائحة التنفيذية بعقوبة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين.. أنظر المادة (٢٩) من قانون مكافحة جرائم تقنية المعلومات.

الخاتمة

أدرك العالم منذ ما يقارب من ربع قرن أهمية تقنية المعلومات والتي تمثل اليوم العمود الفقري لأغلب المؤسسات العامة والخاصة، حيث تدخل التقنية في أدق تفاصيل حياتنا ويكاد من المستحيل أن يمر يوم بدون أن نستخدم إحدى وسائل تقنية المعلومات.

لذا يُعد التحول الرقمي من أبرز الملفات التي طرحتها الحكومة المصرية والتي تسهم في القضاء على الفساد من خلال مشروع التحول الرقمي لمجتمع رقمي، يهدف إلى إتاحة الخدمات الرقمية بطرق بسيطة وتكلفة ملائمة في أي وقت وأي مكان لجميع مؤسسات الدولة والمواطنين من خلال تطوير منظومة رقمية متكاملة مؤمنة على المستوى القومي، فإدخال التكنولوجيا والميكنة إلى الجهات الحكومية سوف يسهم في التحول الرقمي للمجتمع، ويعمل على تقليل معدلات الفساد والبيروقراطية والعمل على خلق اقتصاد قوي، فالتحول الرقمي هو مسئولية الجميع؛ سواء أكان الدولة أو المواطنين، للحصول على مستوى معيشة أفضل، في مجتمع آمن في ظل التغيرات العالمية التي توجب علينا عملية التحول لمواجهة التحديات العالمية وتغيراته.

وبطبيعة الحال، فقد كان للتطور المستمر في نظم معالجة البيانات والمعلومات الآلية وتخزينها وتبادلها وتخليقها وتطويرها– وتعدد المواقع والحسابات الخاصة، والاتساع المُطرد في استخدام البريد الإلكتروني، والأجهزة والمعدات التقنية، إلى جانب التطور المذهل في وسائل الاتصال المعلوماتي– انعكاسات حتمية في تقنيات المعلومات بحيث ترتكب جرائم بواسطة تلك الأنظمة والتقنيات باعتبارها من وسائلها وأدواتها، وهى ما يطلق عليها الآن جرائم تقنية المعلومات، التي تكون المعلومات محلاً للجرائم أو أداة في ارتكابها.

وبناءً على ما سبق فقد صدر القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، يهدف إلى مكافحة الاستخدام غير المشروع للحاسبات وشبكات المعلومات، ووضع القواعد والأحكام والتدابير اللازم اتباعها من قبل مقدمي الخدمة لتأمين خدمة تزويد المستخدمين بخدمات التواصل بواسطة تقنية المعلومات، وحماية البيانات والمعلومات الحكومية

والمعلومات الشخصية.

نتائج وتوصيات الدراسة

أولاً: النتائج:

نستخلص من بحثنا للحماية الجنائية للخدمات المقدمة للجمهور في عصر التحول الرقمي العديد من النتائج أهمها:

١- تعرف الخدمات الجماهيرية بأنها الخدمات التي تلبى الحاجات الضرورية للمواطن وتحقيق رفاهيته وتلتزم الحكومة بتقديمها لكل المواطنين سواء كانت حكومية أو غير حكومية، فهي سلسة من الأنشطة أو الإجراءات أو العمليات التي يجب على الدولة توفيرها وتهدف إلى تلبية حاجة المواطنين.

٢- تُعد حقوق الإنسان الرقمية إمداد لحقوق الإنسان في العالم الواقعي بصفة عامة، فهي تمثل ذات الحقوق التي يتمتع بها الفرد في العالم الواقعي.

٣- يُعد التحول الرقمي من أبرز الملفات التي طرحتها الحكومة المصرية في خطتها لعام ٢٠٣٠؛ حيث يسهم في تفّرد الدولة المصرية في القارة الإفريقية، والقضاء على الفساد، وذلك من خلال إتاحة الخدمات الرقمية لجميع المؤسسات والمواطنين بطرق بسيطة، حيث تعد مصر ضمن أسرع عشر دول نمواً في مجال الشمول الرقمي عام ٢٠٢٠، حيث أصبحت في المركز الثالث عالمياً في معدل تحسين الأداء الحكومي في عام ٢٠٢٠.

٤- تسعى الحكومة المصرية إلي تعزيز حلول أمن البيانات والمعلومات لدى كافة جهات ومؤسسات الدولة، والتوسع في تقديم خدمات الحكومة الإلكترونية بشكل آمن، من خلال أربع محاور رئيسية هي (سبل تأمين شبكات البنية التحتية وتطبيقات التحكم الصناعي، مستقبل الهجمات السيبرانية وتأثيرها على الأمن القومي، المستجدات التشريعية وانعكاسها على آليات التعامل مع جرائم تقنية المعلومات، أفضل

الممارسات لتأمين منظومة الخدمات الإلكترونية).

٥- تعزيز وتطوير الحكومة المصرية للبنية التحتية لتكنولوجيا المعلومات والاتصالات، ووضع الخطط والاستراتيجيات الكفيلة بتحقيق أهدافها في الوصول إلى حكومة مترابطة ومتكاملة رقمياً، والتوسع في تقديم الخدمات المميكنة، بما يضمن تحسين بيئة العمل والتأسيس لمجتمع المعرفة ورفع مستوى الأداء داخل مؤسسات الدولة المختلفة.

٦- تطبيقات وسائل تكنولوجيا المعلومات والاتصالات مثل الحكومة الإلكترونية والذكية من أهم وسائل الإصلاح الإداري والتحول للإدارة العامة الحديثة.

٧- وعى المواطنين وكفاءة وتدريب الموظفين وتوفير البنية التقنية والتكنولوجية تعد عوامل رئيسية في عملية الإصلاح وتطوير الأداء الحكومي لخدمات المواطنين.

٨- حَرص المُشرع الدستوري على كفالة الحماية الدستورية للنُظم المعلوماتية واعتبر أن أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وألزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه.

٩- إن المشرع وضع مصر على خريطة العالم الرقمي وذلك بصدور القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، حيث جاءت نصوصه كاشفة عن أنه قانون عقابي للمجرم المعلوماتي وليس رقابياً، فهو قانون احترازي لا اختراقي.

١٠- يمنح القانون للمواطنين الحرية في الفضاء الإلكتروني أيا كانت وسائله سواء (الفيسبوك أو غيره) طالما كانت تلك الحرية تُمارس في إطار القانون دون المساس بالأمن القومي للبلاد أو بسمعة المواطنين أو خرق حياتهم الخاصة بما يسئ إليهم، وحفاظاً على سمعتهم.

١١-تضمن القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات عدداً من القواعد الموضوعية غير التقليدية لمواجهة النماذج الإجرامية المستحدثة في النطاق المعلوماتي من أهمها (جرائم الاعتداء على أنظمة وشبكات الدولة المعلوماتية، جرائم الاحتيال على بطاقات البنوك، الانتفاع بدون حق بخدمات

الاتصالات والمعلومات).

ثانياً: التوصيات:

١- يؤخذ على المشرع في قانون مكافحة تقنية المعلومات عدم وضع بعض التعاريف التي يلزم تحديدها لتطبيق القانون ولكونها جرائم العصر الحديث، لذا نقترح ضرورة إجراء تعديل تشريعي، **نظراً لأهميتها وأسوة ببعض التشريعات العربية كالتشريع البحريني والكويتي والقطري**، وهي كالتالي:

- **الاحتيال الإلكتروني:** كل فعل يؤدي إلى التأثير على نظام إلكتروني أو نظام معلوماتي أو شبكة معلوماتية أو أية وسيلة تقنية معلوماتية أو جهاز حاسب آلي أو توقيع إلكتروني أو معلومات إلكترونية وذلك عن طريق البرمجة أو الحصول أو الإفصاح أو النقل أو النشر لرقم أو كلمة أو رمز سري أو بيانات سرية أو خاصة أخرى، بقصد الحصول على منفعة دون وجه حق أو للإضرار بالغير.
- **الابتزاز الإلكتروني:** كل فعل من شأنه أن يمثل أسلوب من أساليب الضغط أو الإكراه على شخص أخر بهدف تحقيق مقاصد إجرامية.
- **بطاقات الدفع الإلكتروني:** البطاقة الإلكترونية التي تحتوي على شريط ممغنط أو شريحة ذكية أو غيرها من وسائل تقنية المعلومات والتي تحتوي على بيانات أو معلومات إلكترونية والتي تصدرها الجهات المرخص لها بذلك.
- **المعطيات الشخصية:** هي كل معلومة يمكن أن تدل على شخص طبيعي معرفاً أو قابلاً للتعريف بطريق مباشر أو عن طريق معالجتها أو تحليلها سواء كانت ورقية أو إلكترونية أو غيرها ما عدا تلك المعلومات المتعلقة بالحياة العامة.

٢- ضرورة إجراء تعديل تشريعي لجريمة الاعتداء على سلامة الشبكة المعلوماتية، حيث جعل المشرع من الخطأ ظرفاً مخففاً للعقوبة، ونرى إنه يمكن أن يُستخدم هذا التخفيف بصورة خاطئة، فإذا لم يثبت ركن التعمد في حق الجاني يجب أن يتم توقيع العقوبة المقررة دون تخفيف، كما قد يكون هذا الخطأ تم بصورة الإهمال أو

عدم اتباع الواجبات وهذا لا يستوجب تخفيف العقاب وإنما على العكس يستلزم تشديد العقوبة، لذا نقترح عدم التفرقة في العقاب بين مرتكبي الجريمة بصورة عمدية أو بطريق الخطأ لتحقيق الردع العام والخاص لأفراد المجتمع.

٣- إجراء تعديل تشريعي لجريمة تجاوز الحق في الدخول، حيث أن المشرع ساوى بين دخول الجاني بطريق مشروع أو غير مشروع، فقد يدخل الجاني بطريق مشروع ولكنه يتجاوز حدود الحق في الدخول لمدة من الزمن، لذا نرى أن جريمة الدخول هي جريمة وقتية وإنما جريمة التجاوز فهي جريمة مستمرة تستغرق وقتاً من الزمن لذا يجب التفرقة بين تلك الجريمتين في العقاب.

٤- تركيز كافة مؤسسات الدولة على الخدمات الأكثر احتياجاً للمواطنين عند تطبيق الحكومة الإلكترونية، بحيث تحل لهم المشكلات السابقة في الإدارة التقليدية حتى تُحقق لهم الإشباع والرضا مما يساهم بشكل كبير في زيادة الوعى ومشاركة الجميع في عملية التحول الرقمي.

المراجع

أولاً: الكتب والأبحاث القانونية:

١- أحمد فتحي سرور، الوسيط في قانون العقوبات- القسم العام، القاهرة، دار النهضة العربية، ٢٠١٥، الطبعة السادسة.

٢- أحمد كاظم- ورود قاسم جبر، "تكنولوجيا التحول الرقمي وتأثيراها في تحسين الأداء الاستراتيجي للمصرف، العراق، جامعة كربلاء، المجلة العراقية للعلوم الإدارية، ٢٠٢٠، العدد ٦٥، المجلد ١٦.

٣- إسراء محمد على سالم- منى عبد العالي موسي، جريمة إخفاء المال الضائع (دراسة مقارنة)، العراق، جامعة بابل، ٢٠١٤.

٤- أكمل يوسف، قوائم الكيانات الإرهابية والإرهابيين في ضوء الشرعية الدستورية والجنائية، القاهرة، مركز الدراسات العربية للنشر والتوزيع، ٢٠٢٠.

٥- أمل فوزي أحمد عوض، الحقوق والحريات الرقمية (معالجات قانونية، تقنية، منظور الشريعة الإسلامية)، ألمانيا، برلين، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، يوليو ٢٠٢١، العدد الأول.

٦- إيهاب المير، متطلبات تنمية الموارد البشرية لتطبيق الإدارة الإلكترونية: دراسة تطبيقية بالإدارة العامة للمرور بوزارة الداخلية، البحرين، جامعة نايف العربية للعلوم الأمنية، ٢٠٠٧.

٧- بشير محمد حسين، أثر المراقبة الرقمية على الحريات العامة، الجائر، جامعة جيلالي اليابس، ٢٠١٧.

٨- جميل الصغير، الإنترنت والقانون الجنائي، القاهرة، دار النهضة العربية، ٢٠٠٢.

٩- جميل الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، القاهرة، دار النهضة العربية،٢٠٠١.

١٠-حاتم أحمد محمد بطيخ، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات (دراسة تحليلية مقارنة)، مصر، جامعة مدينة السادات، مجلة الدراسات

القانونية والاقتصادية، أغسطس ٢٠٢١، العدد ١، المجلد ٧.
١١-حاتم عبدالرحمن منصور الشحات، الضوابط القضائية للركن المعنوي في جرائم العنف، الكويت، جامعة الكويت، مجلة الحقوق، ديسمبر ٢٠١٢، العدد ٤.
١٢-حسن عفيف العريشي، واقع نظام الرقابة الإدارية الإلكترونية وسبل تطويره في وزارة الداخلية الفلسطينية الشق المدني، فلسطين، جامعة الأقصى، ٢٠١٥.
١٣-حسنى الجندي، قانون مكافحة جرائم تقنية المعلومات في دولة الإمارات العربية المتحدة، دولة الإمارات العربية المتحدة، الشارقة، أكاديمية العلوم الشرطية، ٢٠٠٩، الجزء الثالث.
١٤-حسنين إبراهيم صالح عبيد، فكرة المصلحة في قانون العقوبات، القاهرة، المجلة الجنائية القومية، يوليو ١٩٧٤، العدد الثاني، المجلد ١٧.
١٥-رامي متولي القاضي، شرح قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ (مقارناً بالتشريعات والمقارنة والمواثيق الدولية)، القاهرة، مركز الدراسات العربية، ٢٠٢٠، الطبعة الأولى.
١٦-سيد أحمد محمدين، حلم مصر ٢٠٣٠ حكومة بلا ورق التحول الرقمي نقلة نوعية تحرر مصر من البيروقراطية والفساد الإداري، القاهرة، مجلة المال والتجارة، مايو ٢٠٢١، العدد ٦٢٥.
١٧-شريف صالح محمد، ورقة بحثية بعنوان "تطور مفهوم خدمات المواطنين وعلاقته بنظم المعلومات والاتصالات"، مصر، جامعة بورسعيد- كلية التجارة، ٢٠١٩.
١٨-صالح سليمان عبد العظيم، الأبعاد والتأثيرات الاجتماعية المرتبطة باستخدام الإنترنت على الأسرة العربية، دراسة ميدانية على عينة من طالبات جامعة الإمارات العربية، ورقة مقدمة إلى مؤتمر واقع الأسرة في المجتمع، تشخيص للمشكلات واستكشاف لسياسات المواجهة، المنعقد بدار الضيافة، جامعة عين شمس، في الفترة من ٢٦- ٢٨ سبتمبر ٢٠٠٤.
١٩-عاشور عبدالكريم، دور الإدارة الإلكترونية في ترشيد الخدمة العمومية في الولايات المتحدة الأمريكية والجزائر، الجزائر، جامعة منتوري – قسنطينة، ٢٠١٠.

٢٠-عباس بردان، ما هو التحول الرقمي وكيف تعرفه الشركات الرقمية ومحركات دفع التحول الرقمي والتكنولوجي، ٢٠١٩، الجزء الأول.
٢١- عبد العظيم مرسي وزير، الشروط المفترضة في الجريمة، القاهرة، دار النهضة العربية، ١٩٨٣.
٢٢-عبدالله العمري، جريمة ابتزاز النساء، الرياض، مكتبة العبيكان، ٢٠٠٩.
٢٣- عبدالولى أحمد صالح المرهبي، مكافحة جرائم خطف الأشخاص، القاهرة، أكاديمية الشرطة، ٢٠٠٩.
٢٤-عدنان مصطفى البار، التحول الرقمي كيف ولماذا؟، السعودية، جامعة الملك عبد العزيز، ٢٠١٩.
٢٥-عدنان مصطفى البار، تقنيات التحول الرقمي، السعودية، جامعة الملك عبد العزيز، ٢٠٢١.
٢٦-عيدوني كافية- بن حجوبة حميد، الإدارة الإلكترونية في العالم وسبل تطبيقها (واقع وأفاق)، الجزائر، جامعة عباس الغرور، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، مجلة الأصيل للبحوث الاقتصادية والإدارية، ديسمبر ٢٠١٧، العدد الثاني.
٢٧-محمد طارق، جريمة الاحتيال عبر الإنترنت، مصر، منشورات الحلبي الحقوقية، الطبعة الأولى، ٢٠١١.
٢٨-مصطفى محمد على شديد، تأثير التحول الرقمي على مستوى أداء الخدمة المقدمة بالتطبيق على موظفي الإدارة العامة للمرور بمحافظة القاهرة، القاهرة، جامعة القاهرة – كلية الاقتصاد والعلوم السياسية، أكتوبر ٢٠٢١، العدد الرابع، المجلد ٢٢.
٢٩-موسى عبدالناصر- محمد قريشي، مساهمة الإدارة الإلكترونية في تطوير العمل الإداري بمؤسسات التعليم العالي، الجزائر، جامعة بسكرة، مجلة الباحث، ٢٠١١، العدد ٩.
٣٠-مي ممدوح قايد، السياسة الجنائية لمواجهة الإرهاب المعاصر، القاهرة، دار النهضة العربية، ٢٠٢٢.
٣١-ميادة مصطفي محمد المحروقي، المواجهة الجنائية الموضوعية للتنظيمات الإرهابية، المنصورة، كلية الحقوق- جامعة المنصورة، مجلة البحوث القانونية والاقتصادية، أغسطس ٢٠١٧، العدد ٦٣، الجزء الأول.
٣٢-هاشم فتح الله عبدالرحمن عبدالعزيز، حقوق الإنسان الرقمية كمتطلب للتحول الرقمي الآمن، القاهرة، رابطة التربويين العرب، يوليو ٢٠٢١، العدد ١٨.

٣٣-وليد سمير المعداوي، مكافحة جرائم تقنية المعلومات والإرهاب الإلكتروني وفقاً لأحدث التشريعات المصرية، الإمارات، القيادة العامة لشرطة الشارقة، مركز بحوث الشرطة، مجلة الفكر الشرطي، يوليو ٢٠٢٠، العدد ٣، المجلد ٢٩.

ثانياً: التشريعات:

١- الدستور المصري الصادر عام ٢٠١٤.

٢- قانون العقوبات رقم ٥٨ لسنة ١٩٣٧.

٣- قانون مكافحة جرائم تقنية المعلومات ١٧٥ لسنة ٢٠١٨.

٤- التشريع الكويتي الصادر بالقانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات.

٥- التشريع القطري الصادر بالقانون رقم ١٤ لسنة ٢٠١٤ بشأن مكافحة جرائم تقنية المعلومات.

٦- التشريع العماني الصادر مرسوم سلطاني رقم ٢٠١١/١٢ بإصدار قانون مكافحة جرائم تقنية المعلومات.

ثالثا: التقارير:

١- استراتيجية التنمية المستدامة- رؤية مصر ٢٠٣٠، الصادرة عن وزارة التخطيط والمتابعة والإصلاح الإداري.

الاستراتيجية الوطنية للأمن السيبراني ٢٠٢٢-٢٠٢٦، الموقع الرسمي لوزارة الاتصالات وتكنولوجيا المعلومات، https://mcit.gov.eg/ar/Media_Center/Press_Room/Press_Releases/٦٤٨٥١

٢- تقرير بعنوان "جهود على طريق التنمية- الرقمنة في مصر"، صادر عن مركز المعلومات ودعم اتخاذ القرار بمجلي الوزراء، يونيو ٢٠٢٢.

رابعا: المواقع الإلكترونية:

١- إحصائية بعنوان "أكثر أنواع الجرائم الإلكترونية التي يتم الإبلاغ عنها شيوعًا في عام ٢٠٢١"، https://www.statista.com/statistics/١٨٤٠٨٣/commonly-reported-types-of-cyber-crime/

٢- إحصائية بعنوان الصناعات عبر الإنترنت الكثر استهدافاً بهجمات التصيد اعتباراً من الربع الأول من عام ٢٠٢٢،
https://www.statista.com/statistics/٢٦٦١٦١/websites-most-affected-by-phishing/ .
٣- بوابة مصر الرقمية بشكل دوري، https://digital.gov.eg/ .
٤- بيرم جمال، بحث بعنوان "حقوق الإنسان الرقمية"، موقع موسوعة ودق القانونية للأبحاث والدراسات والاستشارات القانونية الشاملة، منشور بتاريخ ٢٠٢١/١١/٤، https://wadaq.info.
٥- دراسة برلمانية صادرة عن لجنة الاتصالات وتكنولوجيا المعلومات بمجلس النواب، https://www.parlmany.com/News/
٦- ما هي البيروقراطية، https://www.lazemtefham.com/٢٠١٥/١٢/blog-post_٢٦.html .
٧- الموقع الرسمي لوزارة الداخلية المصرية، https://moi.gov.eg/home/contact
٨- موقع مركز المعلومات ودعم اتخاذ القرار، مجلس الوزراء المصري، https://www.idsc.gov.eg/News/View/١٥٨١٩ .
٩- ورقة بحثية بعنوان "الخدمات العامة الرقمية: سبل تحول سريع على نطاق واسع، ٢٠٢٠، https://www.mckinsey.com/~/media/mckinsey/industries/public.
١٠- ورقة مفاهيمية بعنوان "اللجنة الوطنية المعنية بالاستخدام الآمن للإنترنت للأطفال"، صادرة عن وزارة الاتصالات وتكنولوجيا المعلومات، https://www.itu.int/en/ITU-D/RegionalPresence/ArabStates/Documents/events/٢٠١٥/COP/NationalCOPCommitteeconceptPaper-ar.pdf

خامسا: المراجع الأجنبية:

١- Catala (Pierre), “Les Transformations de droit par l’informatique“, in Bensoussan (Alain), Linamt de Bellefonds (Xavier), Maisl (Herbert) (eds.) emergences du droit de l’Informatique , ١٩٨٣ .

٢- Deloitte & Touche LLP, IT control objectives for Sarbanes Oxley", New Guidance on IT control and compliance, ٢٠٠٨.

الملخص

تعد الحقوق الرقمية إحدى سمات وخصائص العصر الحالي والتي برزت نتيجة الثورة المعلوماتية المعاصرة والقائمة على التكنولوجيا الحديثة والتقنية المتطورة، فيجب أن تحرص الدولة على توافرها عند تقديم الخدمات الرقمية للمواطنين، والتي ساعدت في نقل المعلومات ومعالجتها حتى أصبحت عاملاً رئيسياً ومؤثراً في كافة مناحي الحياة الاجتماعية والاقتصادية والثقافية والعلمية والقانونية، وعنصراً مؤثراً في أنماط التفكير وحل المشكلات على مستوى الفرد والجماعة.

ويعتبر التحول الرقمي من أبرز، بل أهم الملفات التي طرحتها الحكومة المصرية في خطتها لعام ٢٠٣٠؛ حيث يسهم هذا التحول في تفّرد الدولة المصرية في القارة الإفريقية، والقضاء على الفساد والبيروقراطية، لضمان تحقيق الاستغلال الأمثل للموقع الجغرافي المصري لتصبح مركزاً عالمياً هاماً لخدمات الاتصال وتكنولوجيا المعلومات.

وقد أدت الثورة المعلوماتية إلى ظهور من يسيء استخدام الأنظمة المعلوماتية بشكل غير مشروع والذي قد يعرض خدمات المجتمع الجماهيرية للخطر، وهو ما أدى إلى ظهور الجرائم الإلكترونية المعلوماتية الأمر الذي يؤثر على حقوق الإنسان عامةً والحقوق الرقمية على وجه الخصوص، وللجدير بالذكر إلى أن حقوق الإنسان الرقمية حظيت باهتمام عالمي المستوى؛ وذلك بعد ذيوع وانتشار شبكة الإنترنت منذ تسعينات القرن الماضي وتحديداً عام ١٩٩١، حيث حدثت نقلة نوعية سريعة في مجال تكنولوجيا المعلومات بعد أن كان الإنترنت مقتصراً على بعض المؤسسات الموثوقة كالجامعات لغايات إجراء الدراسات والأبحاث العلمية إلى أن أصبح الإنترنت واسع النطاق والعالمية.

لذا تعمل الحكومة المصرية على تهيئة البيئة التشريعية ودعم البنية التحتية المعلوماتية، فأصدرت القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات بهدف حماية البنية المعلوماتية للدولة، مع التأكيد على حماية الحرية الشخصية أو حرمة الحياة الخاصة للمواطنين، وغيرها من الحقوق والحريات العامة التي يكفلها الدستور والقانون.

الكلمات المختصرة: (الحقوق الرقمية، التحول الرقمي، جرائم تقنية المعلومات، انتهاك الخدمات الإلكترونية، الأنظمة المعلوماتية).

The summary

Digital rights are one of the features and characteristics of the current era, which emerged as a result of the contemporary information revolution based on advanced technology, the state must ensure their availability when providing digital services to citizens. it has helped in the transfer and processing of information to become a major and influential factor in all aspects of life and an influential element in the patterns of thinking and problem solving at the level of the individual and the group.

Digital transformation is one of the most prominent and even most important files presented by the Egyptian Government in its ٢٠٣٠ plan.

The information revolution has led to the emergence of an illicit misuse of information systems that could jeopardize mass society's services, resulting in cybercrime, affecting human rights in general and digital rights in particular, and it is worth noting that digital human rights have received world-class attention; After the spread of the Internet.

The Egyptian Government is therefore working to create a legislative environment and support information infrastructure, It promulgated Law No. ١٧٥ of ٢٠١٨ on combating information technology offences with a view to protecting the State's information infrastructure, with emphasis on protecting the personal freedom or privacy of citizens and other public rights and freedoms guaranteed by the Constitution and the law.

Short words: (digital rights, digital transformation, IT crimes, violation of electronic services, information systems).