جرائم الإضرار بالنظم المعلوماتية الحكومية
في ضوء القانون الدولى

د. إسلام عبد ربه رمضان عبد ربه هديب
دكتوراه في القانون الدولى وماجستير بالأمن السيبرانى
عضو جمعية القانون الدولى

(ISSN: 2537- 0758)

جرائم الإضرار بالنظم المعلوماتية الحكومية في ضوء القانون الدولى

د. إسلام عبد ربه رمضان عبد ربه هديب

ملخص البحث:

إذا كان التقدم العلمي قد قدم للمجتمع كثير من الخدمات كعنصر إيجابي في المجتمع، فإنه قد حمل معه كأثر جانبي تطورا مقابلا كمياً ونوعيا في ظاهرة الجريمة، حيث استفادت هذه الظاهرة بدورها– كغيرها من الظواهر – من التقدم محاولة الوصول من خلاله إلى تحقيق الغايات والنتائج غير المشروعة.

والواقع أن أخطر اثار التقدم التقني واستفادة الجريمة من هذا التقدم هو استخدامه في الاعتداء على البنية الرقمية للدولة، والتي تتمثل في النظم المعلوماتية الحكومية، حيث بدأ هذا النوع من الجريمة في الانتشار اما طمعا في الحصول على مصلحة خاصة أو ميزة مالية، أو تبعا لأغراض سياسية تتمثل في استهداف الإضرار بالدولة بأي وسيلة كنوع من الحاق الخسائر بالممتلكات الحكومية.

ولقد انتبه المشرع الدولي والوطني إلى خطورة هذه الظاهرة الإجرامية، فبادروا إلى مواجهتها عن طريق إصدار الاتفاقيات والتشريعات الحديثة، والتي صدرت كي تلائم طبيعة هذه الجرائم والوسائل المستخدمة لارتكابها فتم ابرام اتفاقية بودابست، وصدر القانون رقم ١٤ لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية في قطر، والقانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة الجرائم الإلكترونية في مصر، وهي القوانين التي حاول من خلالها المشرع مكافحة أي اعتداء إلكتروني على النظم المعلوماتية، فأفرد موادا من شأنها التصدي لهذه المهمة وتوفير الحماية الجنائية للنظم المعلوماتية الحكومية.

وبرغم اتفاق هذه التشريعات في الهدف المرجو منها إلا أنها قد اختلفت في المعالجة التشريعية للظاهرة محل الدراسة، بحيث يمكن القول انها لم تكن على نفس القدر من الكفاية في مواجهة جريمة الإضرار بالنظم المعلوماتية الحكومية والحد من أثار هذه الجريمة.

Summary of research:

If scientific progress has provided society with many services as a positive element in society, it has carried with it as a side effect a corresponding quantitative and qualitative development in the phenomenon of crime, as this phenomenon in turn- like other phenomena- has benefited from progress in an attempt to achieve illegal ends and results.

In fact, the most serious effects of technological progress and the benefit of crime from this progress is its use in attacking the state's digital infrastructure, which is represented in government information systems, as this type of crime began to spread either in the ambition to obtain a private interest or financial advantage, or according to political purposes represented in the targeting of harming the state by any means as a type of damage to government property.

The international and national legislators have been alerted to the seriousness of this criminal phenomenon, so they took the initiative to confront it by issuing modern conventions and legislation, which were issued to suit the nature of these crimes and the means used to commit them. The Budapest Convention was concluded, and Law No. 14 of 2014 issuing the Law on Combating Electronic Crimes in Qatar, and Law No. 175 of 2018 on combating electronic crimes in Egypt, through which the legislator tried to combat any electronic attack on information systems, singling out articles that would address this task and provide criminal protection for governmental information systems.

Despite the agreement of these legislations in their desired goal, they differed in the legislative treatment of the phenomenon under study, so that it can be said that they were not equally adequate in confronting the crime of damaging governmental information systems and minimizing the effects of this crime.

(ISSN: 2537- 0758)

مقدمة

أصبح الحاسب الآلي والتقنيات المرتبطة به أحد أهم ركائز التطور العلمي خلال العقود الأخيرة، وذلك لارتباط هذه التقنيات بأغلب مجالات الحياة والأنشطة المختلفة التي يمارسها الأشخاص سواء الأنشطة العلمية أو الاقتصادية أو الاجتماعية، وإذا كان التقدم العلمي يؤدي خدمات غير محدودة للمجتمعات فإن هذا التقدم ذاته كثيرا ما يقترن بما يسمى التقدم السلبي، وهو التطور الذي يعود على المجتمع بالضرر، وأهم صوره التطور الإجرامي، والذي يضع العلم في خدمة الجريمة كأحد وسائل ارتكابها، أو يتسبب في ابتكار صور جديدة من الجرائم يحاول من خلالها المجرمون الاستفادة من هذا التطور، أو النهل من المغانم التي نتجت عن هذا التطور بصورة أو بأخرى.

وقد أدى الاستخدام المتصاعد للنظم المعلوماتية إلى ظهور ما اصطلح على تسميته بالجريمة المعلوماتية، والتي برزت في الآونة الأخيرة كنتيجة مرتبطة بالتقدم التقني المستحدث، وهو نوع من الاجرام يستهدف المعلوماتية ذاتها أو يرتكز عليها في استهدافه للأموال أو الأشخاص، ولم يكن التشريع والفقه بمعزل عن هذا النوع من التطور الإجرامي، حيث بدأ العاملون بالحقل القانوني عموما في وضع الاطار القانوني لهذا النوع من الجرائم بشكل واضح، حيث بدأ التمييز بين نوعين من الجرائم أو الاعتداء المعلوماتي، الأول هو استخدام تقنية المعلومات في ارتكاب أحد صور الجرائم التقليدية، مثل جرائم الاعتبار وجرائم الأموال، اي حالة أن تكون المعلوماتية وسيلة لارتكاب الجريمة[1]، اما النوع الثاني من جرائم المعلومات فهو حينما تكون تقنية المعلومات والاتصالات هي الهدف من ارتكاب الجريمة وغايتها، فنكون حينئذ امام أحد صور السلوك الاجرامي المستحدثة، والذي يرتبط بأمن وسلامة النظام المعلوماتي من ناحية وسرية وسلامة البيانات والمعلومات التي يتضمنها من ناحية أخرى، وهي الجرائم التي تترتب غالبا على الدخول غير المشروع إلى النظم المعلوماتية والتعرض لها وتهديد سلامتها وسلامة المعلومات التي تتضمنها[2].

---

[1] علي نعمة جواد الزرفي، **الجريمة المعلوماتية الماسة بالحياة الخاصة– دراسة مقارنة**، المكتب الجامعي الحديث، القاهرة ٢٠٢٠، ص ١٢

[2] نسرين عبد الحميد البيه، **الجريمة المعلوماتية والمجرم المعلوماتي**، منشأة المعارف، القاهرة ٢٠١٢، ص ٢٢

والواقع ان هذا النوع من الجرائم لم يقتصر في هدفه على استهداف النظم المعلوماتية الخاصة فحسب، وإنما تعدى هذا الوضع إلى استهداف النظم المعلوماتية الحكومية وتهديد المصلحة العامة، حيث يعمد الجناة في هذه الحالة إلى مهاجمة النظام المعلوماتي الحكومي، وذلك اما بهدف الإضرار به كتقنية ككل، وإما بهدف الإضرار بمحتوياته من معلومات عن طريق اتلافها أو محوها أو تعديلها أو سرقتها، وهي الجريمة التي يترتب عليها تهديد المصلحة العامة والإضرار بالنظام المعلوماتي الحكومي بصفة عامة[٣].

وإدراكا للمخاطر المتزايدة للجرائم التي تهدد النظم المعلوماتية، شرعت الأمم المتحدة في صياغة معاهدة دولية ملزمة قانونا لمواجهة هذا التهديد، بعد ان تطورت هذه الفئة من الجرائم بصورة تستعصى على المواجهة عن طريق الاتفاقيات التي اقرها المجتمع الدولي في العقود الأخيرة، وهي الجهود التي بدأت عام ٢٠١٩، وبعد مرور خمس سنوات، لا تزال المفاوضات مستمرة، مع عدم قدرة الأطراف على التوصل إلى توافق مقبول، ولم تفض اجتماعات أعضاء اللجنة المخصصة لوضع إتفاقية دولية شاملة لمكافحة استخدام تكنولوجيات المعلومات والاتصالات في الأغراض الإجرامية، إلى مشروع قانون متفق عليه، فيما لا تزال الدول مختلفة حول صياغة من شأنها تحقيق توازن بين ضمانات حقوق الإنسان والمخاوف الأمنية[٤].

وعلى صعيد القانون الوطني تصدى المشرع القطري لهذا النوع المستحدث من الجرائم عن طريق اصدار القانون رقم ١٤ لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية، والذي واجه الجريمة محل الدراسة عن طريق المادة ٢ من القانون، كما تصدى لها المشرع المصري بإصداره قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥

---

[٣] محمد ممدوح بدير، **مكافحة الجريمة المعلوماتية عبر شبكات الانترنت والاستدلال كوسيلة لإثبات الجريمة المرتكبة عبر الإنترنت– دراسة مقارنة**، مركز الدراسات العربية للنشر والتوزيع، القاهرة ٢٠١٩، ص ١٣

[٤] للاطلاع على مزيد من التفاصيل بخصوص مشروع المعاهدة العالمية للجرائم الإلكترونية راجع الموقع الرسمي للامم المتحدة

https://news.un.org/ar/story/2024/03/1128737

تاريخ الاطلاع: ٢٠٢٤/١٠/١٢

(ISSN: 2537- 0758)

لسنة ٢٠١٨، حيث خصص المادة ٢٠ من القانون لمواجهة جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة.

ويفيد الإجماع التشريعي على مواجهة هذه الجريمة مدى خطورتها وتأثيرها السلبي على المصلحة العامة، والتي تتمثل في سلطة الدولة في الاحتفاظ بالمعلومات والبيانات السرية والمعلنة على قواعد بيانات إلكترونية من خلال نظم معلوماتية مخصصة للتخزين والنشر وتداول المعلومات، الأمر الذي دفع المشرعين الدولي والوطني إلى تجريم الاعتداء على هذه النظم والمساس بها، وتشديد العقوبات في عدد من الحالات التي تضمنتها المعالجة التشريعية، بل واللجوء في بعض الأحيان إلى تضمين مواد العقاب عدد من العقوبات الفرعية التبعية والتكميلية.

مشكلة البحث:

تدور إشكالية الدراسة حول تحديد السياسة الدولية والوطنية الملائمة لمواجهة جريمة الإضرار بالنظم المعلوماتية الحكومية، والتي يمكن عن طريقها مكافحة هذه الجريمة والحد من آثارها، خاصة في ظل التطور المطرد في تقنية المعلومات والتي تفرز أنماط مستحدثة من السلوك الإجرامي، مما يضغط على المشرع في اتجاه التطوير المقابل لتجريم كافة صور السلوك المتصورة في هذه الجريمة، وهي المشكلة التي تدعو للتساؤل الرئيس المتمثل في: **ما مدى كفاية النصوص الدولية والوطنية لمواجهة جريمة الإضرار بالنظم المعلوماتية الحكومية؟** وهو التساؤل الذي يتفرع عنه عدد من التساؤلات الفرعية، وذلك على النحو التالي:

١. ماذا يعني مصطلح النظم المعلوماتية الحكومية؟ وما هي الأضرار التي تنجم عن المساس بها؟
٢. كيف واجه المشرع الدولي والمشرع الوطني هذه الجريمة؟
٣. ما هي السياسة العقابية المنتهجة حيال هذه الجريمة؟
٤. كيف استغل المشرع العقوبات الفرعية والتدابير الجنائية لدعم العقوبات المقررة لهذه الجريمة؟

أهمية البحث:

تبدو أهمية هذه الدراسة من زاويتين، الأولى الأهمية العلمية التي تتجسد في حداثة التشريعات الدولية والوطنية التي تتناولها، وهو ما يضع هذه الدراسة في مصاف

الدراسات الأولى التي تناولت الإطار القانوني لهذا السلوك الإجرامي المستحدث، اما الزاوية الثانية فهي الجانب التطبيقي للدراسة والذي يتضمن تقييم النصوص الجنائية المواجهة للجريمة محل الدراسة، وتحديد مدى كفايتها في تحقيق الحكمة التشريعية منها، سواء في الاتفاقيات الدولية أو الدول محل المقارنة.

أهداف البحث:

١. بيان ماهية الأضرار التي تهدد النظم المعلوماتية الحكومية.
٢. توضيح أركان جريمة الإضرار بالنظم المعلوماتية الحكومية في القانون الدولي والوطني.
٣. تحديد السياسة العقابية المتخذة في مواجهة الجريمة محل الدراسة.

منهج البحث:

انتهج الباحث في الدراسة الماثلة عددا من المناهج البحثية منها المنهج الوصفي وذلك من خلال وصف جريمة الإضرار بالنظم المعلوماتية الحكومية محل الدراسة فى القانون الدولي والوطني، وانتهج المنهج التحليلي من خلال تحليل نصوص الاتفاقيات الدولية، والتشريعات الوطنية وأحكام المحاكم العليا الخاصة بالجريمة، كما لجأ لاستخدام المنهج المقارن وذلك لتوضيح أوجه الاتفاق والاختلاف بين نصوص التشريعات المقارنة التي تناولت هذه الجريمة، وذلك في النظم القانونية محل المقارنة.

خطة البحث:

المبحث التمهيدي: مفهوم الإضرار بالنظم المعلوماتية الحكومية.

المطلب الأول: تعريف الإضرار بالنظم المعلوماتية الحكومية.

المطلب الثاني: صور الإضرار بالنظم المعلوماتية الحكومية.

المبحث الأول: البنيان القانوني لجريمة الإضرار بالنظم المعلوماتية الحكومية.

المطلب الأول: الركن المادي فى الجريمة.

المطلب الثاني: الركن المعنوي فى الجريمة.

المبحث الثاني: الأحكام العقابية الخاصة بجريمة الإضرار بالنظم المعلوماتية الحكومية.

المطلب الأول: العقوبات الأصلية والفرعية.

المطلب الثاني: التدابير الجنائية المقررة للجريمة.

خاتمة ونتائج وتوصيات.

(ISSN: 2537- 0758)

المبحث التمهيدي
مفهوم الإضرار بالنظم المعلوماتية الحكومية

تمهيد وتقسيم:

تعد النظم المعلوماتية أحد التطورات التطبيقية لعلوم الحاسب الآلي، حيث تدمج هذه النظم بين كل تقنية المعلومات وعلوم الحاسبات، وتستهدف المساهمة في بناء أنظمة الحاسب الآلي التي تعتمد على التكنولوجيا، وتقديم الخدمة للمنظمات الإدارية، كما تدعم هذه النظم وحدات الإدارة الحكومية فتقدم لها المساعدة في إنجاز الأنشطة والأعمال المختلفة من خلال مجموعة من مهام الحاسب الآلي، والتي تتضمن تخزين المعلومات ومعالجتها وتداولها[٥].

وتحتوي نظم المعلومات الخاصة بالجهات الحكومية على نوعين من المعلومات، الأول هو المعلومات المتاحة للكافة والتي يمكن الاطلاع عليها وتداولها بشكل مشروع دون مخالفة قانونية، والثاني هو المعلومات التي لا يجوز الوصول إليها والأطلاع عليها إلا بموجب تصريح مسبق من الجهات المختصة، وهي ما اصطلح على تسميته بالمعلومات السرية، حيث يعد مجرد الوصول لها دون ترخيص بمثابة اعتداء على سلامة النظام المعلوماتي لان هذا الاطلاع يتضمن اختراق للنظام المعلوماتي الحكومي وهو التصرف الذي يعرض فاعله للمسئولية الجنائية.

من خلال هذا التمهيد تنقسم الدراسة في هذا المبحث إلى مطلبين، حيث يتناول الأول توضيح ماهية الإضرار بالنظم المعلوماتية بينما يتناول الثاني توضيح صوره.

المطلب الأول: تعريف الإضرار بالنظم المعلوماتية الحكومية.

المطلب الثاني: صور الإضرار بالنظم المعلوماتية الحكومية.

---

[٥] أشرف نجيب الدريني، **جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات– دراسة مقارنة**، بحث منشور في مجلة روح القوانين، مجلد ٩٥ عدد ٩٥، كلية الحقوق جامعة طنطا، القاهرة ٢٠٢١، ص ٢٤١

المطلب الأول
تعريف الإضرار بالنظم المعلوماتية الحكومية

تعد جريمة الإضرار بالنظم المعلوماتية الحكومية وما تتضمنها هذه النظم من شبكات إلكترونية برامج حاسوبية ومعلومات من مظاهر التطور السلبي للتقدم الإلكتروني، حيث تمثل هذه الجريمة تهديدا لكل من الوعاء والمحتوى المعلوماتي الحكومي، كما تهدد الأجهزة والبرمجيات الحكومية التي تستخدم في عمل هذه النظم، مما يعني الإضرار بالنشاط الإلكتروني الحكومي بصفة عامة، وقد اجتهد كثير من الفقه القانوني في محاولة وضع تعريف لجريمة الإضرار بالنظم المعلوماتية الحكومية، وذلك في سبيل تحديد وصف دقيق لهذه الظاهرة الإجرامية الحديثة والتي ترتكب من خلال وسائل تقنية المعلومات، حيث اتجه البعض لتعريفها من حيث وسائل إرتكابها بينما اتجه فريق آخر إلى تعريفها من خلال النتيجة الإجرامية المترتبة عليها.

فاتجه بعض الفقه إلى أن جريمة الإضرار بالنظم المعلوماتية هي الجريمة التي يقدم فيها الجاني على استخدام وسائل تقنية المعلومات أو علوم الحاسب الآلي في الحصول على أو تغيير المحتوى المعلوماتي الإلكتروني[٦]، وعرفها فقه آخر بإنها جريمة تهدد النظام المعلوماتي ويتم ارتكابها عن طريق وسائل إلكترونية[٧]، بينما عبر فقه ثالث عن تعريفه لهذه الجريمة بإنها أحد أنواع الجرائم التي يستخدم فيها الجاني وسائل إلكترونية لتهديد النظام المعلوماتي أو المحتوى الذي يتضمنه[٨].

ومن ناحية اخرى رأى فريق من الفقه تعريف جريمة الإضرار بالنظم المعلوماتية من زاوية النتيجة الإجرامية، فرأى بعض هذا الفقه تعريف هذا النوع من الجرائم بإنه الاعتداء

---

[٦] معتوق عبد اللطيف، **الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن**، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة العقيد الحاج لخضر باتنة، الجزائر ٢٠١٢، ص ٣٦

[٧] محمود رجب فتح الله، **شرح قانون مكافحة جرائم تقنية المعلومات وفقا للقانون المصري الحديث**، دار الجامعة الجديدة للنشر، القاهرة ٢٠١٩، ص ٢٩

[٨] مشتاق طالب وهيب النعيمي، **تزوير المعلومات كأحد صور الجرائم المعلوماتية**، منشورات الحلبي الحقوقية، بيروت ٢٠١٨، ص ٢٨

(ISSN: 2537- 0758)

على النظام المعلوماتي والذي يتضمن الإضرار بالنظام الحاوي للمعلومات أو الإضرار بالمعلومات ذاتها أو الإضرار بكلاهما[٩]، أو هي الجرائم الماسة بالمواد المعلوماتية المخزنة في الأنظمة الإلكترونية سواء كان هذا التخزين على سبيل الحفظ أو المعالجة[١٠].

والواقع أن كلا من هاتين الفئتين للتعريفات تعد مكملة للأخرى، بحيث لا يجوز الذهاب إلى كفاية أحدهما عن الآخر، فمن ناحية تفرض طبيعة النظم المعلوماتية أن يكون الإضرار بها عن طريق وسائل تقنية المعلومات، حيث أن الإضرار المادي وإن كان متصورا في تحطيم أجهزة الحاسب الآلي أو قطع الوصلات السلكية إلا أن هذا النوع من الإضرار يعد غير مؤثر في النظام المعلوماتي ومحتواه من المعلومات، والتي يتم تخزينها إلكترونيا بحيث لا تؤثر فيها الأعطاب المادية، ومن ناحية أخرى فإن الإضرار بالنظام المعلوماتي يستوجب أن يكون هذا النظام هو محل الاعتداء، سواء كان الاعتداء على الوعاء الإلكتروني أو المحتوى، وهو الاعتداء الذي يتمثل في اختراق النظام المعلوماتي أو التجسس عليه أو إتلاف المحتوى المعلوماتي أو تغيير مضمونه أو التعرض لنظم الاتصالات الحكومية التي تتم عن طريق نظم المعلومات.

وبالإضافة إلى ما قدمه الفقه من تعريف لهذا النوع من الجرائم فإن المشرع بدوره كان له بعض الإسهامات في وضع تعريفات، سواء كانت هذه التعريفات عن طريق المشرع الدولي أو الوطني أو المشرع المقارن، ذلك أن الجهود الفقهية عادة ما تقدم للمشرع السبيل لاستكمالها عن طريق النصوص التشريعية التي تحاول وضع أطر محددة للسلوك الإجرامي حرصا على تحقيق مبدأ شرعية الجرائم.

حيث قدمت الأمم المتحدة تعريفا للجرائم الواقعة على النظم المعلوماتية يتمثل في إنها الجريمة التي ترتكب إما بواسطة نظام إلكتروني أو باستخدام شبكة إلكترونية أو تقع

---

[٩] محمد عبيد الكعبي، **الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت**، دار النهضة العربية، القاهرة ٢٠١٠، ص ٨٩

[١٠] محمد علي سويلم، **شرح قانون جرائم تقنية المعلومات– القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات– دراسة مقارنة**، دار المطبوعات الجامعية للتوزيع، القاهرة ٢٠١٩، ص ١٠٢

على نظام إلكتروني، أي أنها جريمة تمس في ارتكابها وسط إلكتروني أي كان صلتها بهذا الوسط سواء وقعت عليه أو من خلاله أو بإستخدامه، وهو التعريف الذي يشمل وسيلة ارتكاب الجريمة ومحلها، وذلك في المسلك التعريفي الذي أشار إليه الباحث، والذي يجمع بين الوسيلة المستخدمة في ارتكاب الجريمة والنتيجة الإجرامية المترتبة عليها[١١].

كما قدم المشرع الدولي عن طريق الاتفاقيات الإقليمية ممثلة في الاتفاقية الأوروبية للجرائم السيبرانية تعريفا لجرائم الاعتداء على النظم المعلوماتية تجسد في إنها الأفعال التي تشكل نشاطا غير مشروعا يرتبط بالحواسب الآلية وشبكة الإنترنت، وعمد المشرع الأوروبي من خلال هذه الاتفاقية إلى تقسيم هذا النوع من الجرائم بحسب محل الجريمة أو النتيجة الإجرامية التي تترتب عليها، وذلك إلى عدد من الفئات منها الجرائم التي تستهدف الخصوصية وسلامة المحتوى المعلوماتي، والجرائم ذات الصلة بالحواسب الآلية، والجرائم التي تستهدف الإضرار بالمحتوى المعلوماتي، والجرائم الماسة بالعلامة التجارية والملكية الفكرية والصناعية[١٢].

أما المشرع القطري فقد عرف النظام المعلوماتي من خلال المادة ١ من القانون رقم ١٤ لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية على إنه مجموعة برامج

---

[١١] إعلان فيينا بشأن الجريمة والعدالة– مواجهة تحديات القرن الحادي والعشرين، صدر عن مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين المنعقد في فينا من ١٠ إلي ١٧ أبريل ٢٠٠٠، للاطلاع على النص الكامل للإعلان راجع الموقع الرسمي لمكتبة حقوق الإنسان، جامعة مينيسوتا

http://hrlibrary.umn.edu/arab/vi2000.html

تاريخ الاطلاع: ٢٠٢٤/١٠/١٢

[١٢] للاطلاع على النص الكامل للاتفاقية الأوربية لمكافحة الجرائم المعلوماتية المنعقدة في بودابست في ٢٠٠١/١١/١٣، راجع الموقع الرسمي للأمم المتحدة

https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Report/UNODC_CCPCJ_EG.4_2019_2_A.pdf

تاريخ الاطلاع ٢٠٢٤/١٠/١٢

(ISSN: 2537- 0758)

وأجهزة، تستخدم لإنشاء أو استخراج المعلومات، أو إرسالها، أو استلامها، أو عرضها، أو معالجتها، أو تخزينها، كما عرف الأفعال التي تشكل السلوك الإجرامي المكون لجريمة الإضرار بها من خلال المادة ٣ من ذات القانون والتي حددت الإضرار في تدمير أو إيقاف أو تعطيل النظام، أو تغييره أو الغائه أو تعديل محتوياته أو تصميماته أو طريقة استخدامه أو انتحال شخصية ماله أو القائم على إدارته، الأمر الذي يشير لتوسع المشرع القطري في تجريم الأفعال التي تقع على النظم المعلوماتية وتلحق بها أضرارا أو تهدد بإلحاق هذه الأضرار[١٣].

وأخيرا واجه المشرع المصري جريمة الإضرار بالنظم المعلوماتية من خلال قانون مكافحة الجرائم الإلكترونية رقم ١٧٥ لسنة ٢٠١٨، حيث عرّف النظم المعلوماتية من خلال المادة ١ من القانون بإنها مجموعة من الأدوات والبرامج المعدة لإدارة ومعالجة المعلومات والبيانات وتقديم الخدمات المعلوماتية، كما تصدى لتعريف الإضرار بالنظم المعلوماتية الحكومية من خلال المادة ٢٠ من القانون بإنها الدخول العمدي أو البقاء العمدي عقب الدخول بالخطأ أو تجاوز حد الدخول المرخص به، أو الاختراق، أو الاعتراض أو الحصول على المعلومات والبيانات من النظام المعلوماتي، أو الإتلاف أو التشويه أو التغيير أو النسخ أو الإلغاء الذي يرد على المحتوى المعلوماتي للنظام[١٤].

ويلاحظ على تعريف المشرع المصري محاولته حصر أكبر عدد من صور السلوك الإجرامي الذي يمثل إضرارا بالنظم المعلوماتية الحكومية، وهو ما يمكن تفسيره بالعمل على توفير أقصى نطاق من الحماية الجنائية لهذه النظم، وذلك لتحقيق الردع بنوعيه العام والخاص تجاه ارتكاب هذا النوع من الجرائم، الأمر الذي يضع كثير من الأفعال تحت طائلة القانون رقم ١٧٥ لسنة ٢٠١٨[١٥].

---

[١٣] عبد الله محمد الحضري الكثيري، **جريمة الدخول بغير وجه حق الي المواقع الإلكترونية والنظم المعلوماتية العامة في القانون القطرى- دراسة تحليلية**، دار النهضة العربية للنشر والتوزيع، القاهرة ٢٠٢١، ص ٤٤

[١٤] ضياء الحق بهادر اليمني، **التنظيم القانوني لتقنية المعلومات وأثرها على النظام العام**، رسالة دكتوراه، كلية الحقوق جامعة أسيوط، القاهرة ٢٠٢٠، ص ٤٣

[١٥] محمد علي سويلم، **مرجع سابق**، ص ١٣٢

وعلى هذا يمكن الذهاب إلى أن التشريعات برغم اتفاقها على تجريم الاعتداء على النظم المعلوماتية الحكومية والإضرار بها، إلا انها اختلفت في نطاق هذا التجريم، حيث نجد أن المشرع القطري قد توسط بين كلا من المشرعين الدولي الذي ضيق من هذا النطاق، والمشرع المصري الذي توسع فيه إلى درجة كبيرة، ذلك التوسع الذي يؤيده الباحث ويتضامن بناء عليه مع المسلك التشريعي المصري في هذا الصدد.

المطلب الثاني
صور الإضرار بالنظم المعلوماتية الحكومية

حرص المشرع الدولي والمشرع الوطني على تحديد صور جريمة الإضرار بالنظم المعلوماتية الحكومية، وذلك لتوضيح معالم هذه الجريمة من ناحية، ولطبيعتها الفنية من ناحية أخرى، حيث تستلزم هذه الطبيعة أن يكون الإطار القانوني للجريمة متصفا بوضوح الصياغة التشريعية وذلك للتيسير على القضاء في نظر الدعاوى الجنائية المقامة استنادا لإرتكاب هذا النوع من الجرائم.

وبالرغم من اختلاف صور هذه الجريمة بين القانون الدولي والتشريعات محل المقارنة إلا أن الإمعان في المصطلحات المستخدمة في هذه التشريعات لتحديد صور الجريمة تنبئ عن إمكانية استيعاب كافة الصور في أي منها، فبينما لجأ تعريف لجنة خبراء منظمة التعاون الاقتصادي للتنمية للتعميم فحدد هذه الإضرار بأنها نتيجة كل سلوك غير مشروع يتعلق بالمعالجة الآلية للبيانات، ونجد أن المجلس الاوروبي في تقريره المتعلق بجرائم الحاسب الآلي يحدد هذه الأضرار بانها تغيير بيانات الحاسب الالي أو محوها، كما حددها مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين بانها جميع الجرائم التي يمكن إرتكابها في البيئة الإلكترونية[١٦]، بينما نجد أن القانون القطري رقم ١٤ لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية، قد حدد صور هذه الجريمة في التدمير والايقاف والتعطيل والتغير والإلغاء والتعديل، في الوقت الذي حددها المشرع المصري من خلال قانون مكافحة الجرائم الإلكترونية رقم ١٧٥

[١٦] سليمان ابو نمر، **مكافحة الجريمة المعلوماتية في إطار القانون الدولي**، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، الجزائر ٢٠٢١، ص ٧

(ISSN: 2537- 0758)

لسنة ٢٠١٨ في إتلاف المحتوى الإلكتروني، أو تدميره أو تشويهه أو تغييره أو تغيير تصميم النظام المعلوماتي، أو إلغاء النظام المعلوماتي كلياً أو جزئياً[١٧].

وعلى هذا واستنادا لنصوص القانون الدولي والقوانين محل المقارنة يمكن تحديد صور جريمة الإضرار بالنظم المعلوماتية الحكومية على النحو التالي:

أولاً: تدمير النظام المعلوماتي

يعني تدمير النظام المعلوماتي تعطيله بصورة نهائية ودائمة، بحيث تنتفي القدرة على الاستفادة منه، وتنعدم الفرصة في تأديته للمهام المنشودة من وجوده، فالتدمير يعني الانتهاء المادي لوجود النظام المعلوماتي بصورة كاملة، وهو ما يعني خروجه من الخدمة نهائيا، ومحو المعلومات والبيانات التي يتضمنها، وإستحالة استعادتها مرة أخرى، الأمر الذي يعني تعطل كافة الوظائف التي يقوم بها، وتأكيد عدم إمكانية قيامه بها[١٨].

ثانياً: إيقاف النظام المعلوماتي

ويعني الإيقاف تعطل النظام المعلوماتي عن العمل بصورة مؤقتة، وهو التعطل الذي قد يحدث بأي صورة، فيتصور توقف بعض وظائفه دون الأخرى، كأن يتيح النظام في هذه الحالة الإطلاع على محتواه المعلوماتي دون إمكانية تناوله بالحذف أو الإضافة أو التعديل، وقد يعني الإيقاف تعطل وظائف الارسال والاستقبال من وإلى النظام المعلوماتي، أو ظهور بعض محتوياته دون الأخرى، كما قد يتصور تعطله بصورة كلية عن العمل، إلا أن كافة هذه الصور هي رهينة بعدم القدرة على الاستفادة من النظام المعلوماتي بصورة مؤقتة، وإلا استحال الإيقاف إلى تدمير البيانات إذا كان العطل نهائي لا يرجى إصلاحه، أو استحال إلى تعطيل إذا كان في المستطاع الاستفادة من النظام المعلوماتي جزئيا[١٩].

---

[١٧] لمزيد من المعلومات راجع: أشرف نجيب الدريني، **مرجع سابق**، ص ٢٥٢، عبد الله محمد الحضري الكثيري، **مرجع سابق**، ص ٦٠، وأيضا محمد علي سويلم، **مرجع سابق**، ص ١٤٣

[١٨] زينات طلعت شحادة، **الأعمال الجرمية التي تستهدف الأنظمة المعلوماتية**، دار المنشورات الحقوقية صادر، بيروت ٢٠١٧، ص ١٦٣

[١٩] طه السيد أحمد الرشيدى، **الطبيعة الخاصة لجرائم تقنية المعلومات**، دار الكتب والدراسات العربية، القاهرة ٢٠١٦، ص ٦٦

ثالثاً: **تعطيل النظام المعلوماتي**

في هذه الصورة تتعطل بعض وظائف النظام المعلوماتي بصورة مؤقتة إلا أن هذا التعطل لا يمنع الاستفادة من النظام المعلوماتي بصورة جزئية، كما يتسم التعطل بكونه حالة عارضة تصيب النظام المعلوماتي لفترة مؤقتة، حيث تتوقف بعض الخصائص عن العمل بينما يستمر النظام في العمل الجزئي عن طريق باقي خصائصه، وغالبا ما يصيب العطل الوظائف غير الأساسية أو غير المرتبطة ببعضها، مما يمنح مستخدمي النظام المعلوماتي الفرصة للإستفادة منه ولو بصورة جزئية، ويتسم التعطيل كأحد صور الإضرار بالنظام المعلوماتي بكونه أحد العيوب غير الرئيسة وغير الدائمة والتي تصيب النظام فتقصر الاستفادة منه لفترة مؤقتة على وظائف معينة دون غيرها[٢٠].

رابعاً: **التغيير والإلغاء والتعديل**

تتحقق هذه الصورة بوقوع الجريمة على المحتوى المعلوماتي الذي يتضمنه النظام المعلوماتي الحكومي، ففي هذه الصورة لا ينال السلوك الإجرامي من انتظام عمل النظم المعلوماتية، وإنما محل الجريمة هو المعلومات والبيانات التي تشملها النظم، حيث ينتج عن هذا السلوك نتيجة إجرامية هي تغيير المعلومات والبيانات أو إلغائها تماما، بحيث يصبح النظام المعلوماتي خاليا من المحتوى محل الاعتداء، أو متضمنا لمحتوى مصطنع يضمّنه الجاني ضمن هذا النظام، وهي إحدى الصور المنتشرة للإضرار بالنظم المعلوماتية الحكومية والتي يعمد خلالها الجاني إلى اخفاء نوع معين من المعلومات بصورة دائمة أو استبداله بمعلومات زائفة مختلفة عن البيانات والمعلومات الأصلية التي وضعتها الجهات الرسمية بالنظام[٢١].

خامساً: **إتلاف المحتوى الإلكتروني**

يتبين نوع هذا السلوك من مفهومه الاصطلاحي حيث يرد على محتوى النظام المعلوماتي من معلومات وبيانات وتطبيقات وغيرها من محتويات النظام، وهي المعلومات التي تحرص السلطة المختصة على اتاحتها للجمهور أو الاحتفاظ بها سرا للاطلاع بموجب ترخيص مسبق ولفئات وظيفية معينة دون غيرها، ويتجسد السلوك

---

[٢٠] محمد عبيد الكعبي، **مرجع سابق**، ص ١١٣

[٢١] مدحت محمد عبد العزيز ابراهيم، **الجرائم المعلوماتية الواقعة علي النظام المعلوماتي– دراسة مقارنة**، دار النهضة العربية، القاهرة ٢٠١٩، ص ٨١

(ISSN: 2537- 0758)

الاجرامي في هذه الجريمة في محو المعلومات والبيانات كليا أو جزئيا، أو التشويش على هذه البيانات والمعلومات بحيث تبدو غير ظاهرة لمستخدمي النظام أو المنتفعين به، أو تغيير نظم الولوج والاطلاع، الأمر الذي يترتب عليه عدم إمكانية الاستفادة من المحتوى المعلوماتي ذاته رغم سير النظام المعلوماتي واطراده، ودون تأثير على الخصائص الفنية التي يتمتع بها، أو طريقة إدارته، أو اساليب العمل الإداري[٢٢].

سادساً: تغيير تصميم النظام المعلوماتي

وهي الصورة التي انفرد بتجريمها المشرع المصري من خلال المادة ٢٠ من قانون مكافحة الجرائم الإلكترونية رقم ١٧٥ لسنة ٢٠١٨، حيث تقع هذه الجريمة بولوج الجاني للنظام المعلوماتي وتعديل المظهر الخارجي للنظام دون أن يمس طريقة عمله أو المحتوى المعلوماتي الذي يتضمنه، فهي جريمة تقع على الشكل دون المضمون، بحيث لا يؤثر ارتكابها على كفاءة أداء النظام أو المحتوى العلوماتي له.

والحكمة من تجريم هذا السلوك تكمن في اقدام الجاني على الولوج للنظام المعلوماتي دون ترخيص مسبق، وتلاعبه في الطراز المظهري بصورة قد لا تمكن مستخدمي النظام من الوصول إليه من ناحية، كما أن من يملك تعديل المظهر يملك تعديل المضمون لذا فقد أتى تجريم هذا السلوك على سبيل تحقيق الردع العام والردع الخاص، وحماية النظم المعلوماتية الحكومية من أي مساس بها باعتبارها نظم إلكترونية رسمية لا يجوز التعرض لها أو المساس بها بأي صورة[٢٣].

وعلى هذا يمكن القول أن جرائم الإضرار بالنظم المعلوماتية الحكومية لا تقتصر في محلها على النظام المعلوماتي ذاته، وإنما يتصور أن ترد على المحتوى الذي يتضمنه النظام المعلوماتي، كما أن اختلاف التشريعات المقارنة في تجريم أنماط السلوك برغم وجوده في النصوص التشريعية إلا أنه لا يجد له أثرا في الوقائع المادية، حيث تجرم التشريعات كافة صور المساس بالنظم المعلوماتية سواء ورد الاعتداء على النظام أو محتواه، كما أن الخلاف الاصطلاحي لم ينتج عنه اختلاف في مضمون المفاهيم مما يمكن معه الذهاب في النهاية إلى وحدة السلوك التشريعي بين التشريع الإماراتي والتشريعات محل المقارنة.

---

[٢٢] فرج علي خضير، **نظرات في سياسية التجريم في قانون جرائم تقنية المعلومات**، بحث منشور في مجلة المحاماة، العدد ١، القاهرة ٢٠٢١، ص ٥٠

[٢٣] محمد علي سويلم، **مرجع سابق**، ص ١٥٢

المبحث الأول
البنيان القانوني لجريمة الإضرار بالنظم المعلوماتية الحكومية

تمهيد وتقسيم:

يشكل الإضرار بالنظم المعلوماتية الحكومية هاجسا للقانون الدولي على المستوى الأممي والأقليمي، لاسيما بعد تطور الهجمات السيبرانية على المواقع الرسمية الحكومية، وأصبحت الجرائم الإلكترونية تؤثر على امن واستقرار الدول، مما يستدعى ضرورة التعاون القانوني الدولي لابرام إتفاقيات لتنظيم الجرائم الإلكترونية التي تقع على النظم المعلوماتية الحكومية، وفرض القوانين والعقوبات على مرتكبي هذه الجرائم التي تحتمل عديد من أنماط السلوك الإجرامي، وذلك في ظل خلاف دولي حول إسناد قواعد المسؤولية الدولية في عمليات الاعتداء على المواقع الإلكترونية الحكومية ونظمها المعلوماتية، خاصة جرائم التجسس الإلكتروني بين الدول، وتبادل الاتهامات حول اختراق لسيادة الدول الإلكترونية، وهي النتيجة الطبيعية لتعداد أنماط وصور إرتكاب هذه الجريمة والتي وردت في الاتفاقيات الدولية والقانون القطري رقم ١٤ لسنة ٢٠١٤، والقانون المصري رقم ١٧٥ لسنة ٢٠١٨.

حيث حرصت هذه التشريعات على تناول السلوك المجرم بالتعداد لا التعريف المجرد، وهو ما ترتب عليه تعدد صور السلوك الإجرامي، بالإضافة لاختلاف الركن المعنوي وما إذا كان يتمثل في القصد الجنائي العام أو الخاص، وذلك بتباين السلوك الإجرامي المنصوص عليه سواء في القانون الدولي أو القوانين محل المقارنة.

المطلب الأول: الركن المادي فى الجريمة.

المطلب الثاني: الركن المعنوي فى الجريمة.

المطلب الأول
الركن المادي فى الجريمة

يتضح الركن المادي في جريمة الإضرار بالنظم المعلوماتية الحكومية من زاويتين، أولهما نمط السلوك الذي يقدم عليه الجاني في هذا النوع من الجرائم، والثاني محل وقوع هذه الجريمة أو النتيجة الإجرامية المترتبة عليها، وهو ما يتبين من نصوص التجريم في القانون الإماراتي والقوانين محل المقارنة، وذلك على النحو التالي:

(ISSN: 2537- 0758)

أولاً: الركن المادي في القانون الدولي

يمثل القانون الدولي في هذا المجال إتفاقية بودابست لمكافحة الجرائم المعلوماتية ٢٠٠١[٢٤]، والتي حددت السلوك الإجرامي في مجموعة من الجرائم حيث تشمل قائمة الجرائم المدرجة حداً أدنى من التوافق لم يستبعد توسع نطاق القانون الوطني، وشملت هذه الصور اختراق النظام المعلوماتي الذي يترتب عليه الإضرار بالنظام أو تدميره أو إيقافه عن العمل أو تعطيله، كما تناولت الإضرار بالمحتوى المعلوماتي الناجم عن اختراق النظام والذي يؤدي إلى حذف أو تدمير أو إتلاف البيانات والمعلومات التي يتضمنها النظام المعلوماتي، أو فقدان السرية المفترضة في المعلومات والبيانات غير المتاحة للتداول.

وقد عبرت الاتفاقية عن الاختراق باصطلاح النفاذ غير القانوني من خلال المادة ٢ من الاتفاقية فعرفته بإنه التسلل غير المرخص للنظام المعلوماتي أو البقاء غير المشروع في النظام بعد انتهاء الحدود المرخص بها للدخول، وعلى ذلك يتصور أن يتم الاختراق في حالة الدخول المشروع إذا تجاوز الجاني الحدود المقررة له في هذا الدخول، ويحدث هذا حينما يخالف القواعد الزمنية للدخول، أو يتجاوز النطاق المكاني المقرر، أو يستخدم صلاحيات غير مخولة له[٢٥].

ويشمل هذا النفاذ الدخول الكامل أو الجزئي إلى نظام الكمبيوتر (المعدات، والمكونات والبيانات المخزنة في النظام المثبت، والدلائل، وبيانات الحركة، والبيانات ذات الصلة بالمحتوى)، ومع ذلك، لا يتضمن مجرد إرسال رسالة عن طريق البريد الإلكتروني أو ملف إلى هذا النظام، ويشمل النفاذ الدخول إلى نظام كمبيوتر آخر، حيث يتم ربطه عبر شبكات الاتصالات العامة، أو بنظام كمبيوتر على نفس الشبكة، فمناط التجريم في المادة هو افضاء السلوك لتدمير أو إيقاف أو تعطيل النظام المعلوماتي الحكومي، بغض النظر عن نمط هذا السلوك والذي يرجع للقانون الوطني تحديده

---

[٢٤] اعتمدت الاتفاقية من لجنة وزراء مجلس أوروبا في ٨ نوفمبر ٢٠٠١، وفتح باب التوقيع عليها في ٢٣ نوفمبر ٢٠٠١، بمناسبة المؤتمر الدولي حول الجريمة الإلكترونية.

[٢٥] محمود على احمد المردني، **مرجع سابق**، ص ١٥٢

وتكييف الواقع واعطاء وصفه القانوني الصحيح[٢٦].

اما المادة ٣ فقد جرمت الاعتراض غير القانوني للبيانات والمعلومات، حيث هدفت إلى حماية الحق في خصوصية نقل البيانات، وتمثل الجريمة نفس الانتهاك لخصوصية الاتصالات مثل التنصت والتسجيل التقليديين للمحادثات الهاتفية الشفوية[٢٧]، وتطبق الجريمة المنصوص عليها في المادة ٣ هذا المبدأ على جميع أشكال نقل البيانات الإلكترونية، سواء عن طريق الهاتف أو الفاكس أو البريد الإلكتروني أو نقل الملفات، ونطوي الاعتراض بواسطة الوسائل الفنية على التنصت على محتوى الاتصالات أو رصده أو مراقبته، أو شراء محتوى البيانات سواء بطريقة مباشرة من خلال الولوج إلى نظام الكمبيوتر واستخدامه، أو عن طريق استخدام أجهزة اختلاس السمع أو التنصت الإلكترونية، ويمكن أن ينطوي الاعتراض أيضا على التسجيل، وتشمل الوسائل الفنية الأجهزة التقنية المثبتة على خطوط النقل وكذلك أجهزة جمع وتسجيل الاتصالات اللاسلكية. ويمكن أن تشمل استخدام البرمجيات وكلمات المرور والرموز.

كما جرما المادة (٤) من الإتفاقية حالات الإضرار بالنظام المعلوماتي، كتجريم يتوقف على النتيجة الإجرامية بصرف النظر عن السلوك، فحددت صور هذا الاضرار بإنها التغيير السلبي في سلامة البيانات والبرامج أو محتواها الإعلامي، كما اعتبرت ان حذف البيانات يتساوى مع التدمير، حيث يتم تدمير البيانات وجعلها غير قابلة للتعرف، كما عرفت إتلاف بيانات الكمبيوتر بانه أي عمل يمنع أو ينهي توافر البيانات للشخص الذي لديه حق النفاذ إلى الكمبيوتر أو لوسيلة حفظ البيانات التي تم تخزين البيانات عليها، وعرفت التغيير بأنه تعديل البيانات القائمة، وبالتالي فإن إدخال رموز خبيثة مثل الفيروسات وأحصنة طروادة تعد من الأضرار التي تشملها هذه الفقرة، كما هو الحال بالنسبة للتعديل الناجم عن التلاعب في البيانات[٢٨].

---

[٢٦] سليمان ابو نمر، مرجع سابق، ص ٣٣

[٢٧] عيسى سليم داود الزيدي، **جرائم القرصنة الالكترونية**، دار الكتب القانونية للتوزيع، القاهرة ٢٠٢٢، ص ١١٦

[٢٨] جمال محمد خلفان، **التعاون الوطني والدولي في الجرائم الإلكترونية– المشكلات والحلول**، بحث منشور في مجلة المعهد العالي للدراسات النوعية، مجلد ٣ عدد ١٦، يوليو ٢٠٢٣، ص٥٤٦٨

(ISSN: 2537- 0758)

وقد حرص المشرع الدولي من خلال هذه الاتفاقية على إيضاح أن هذه الأفعال لا تدخل ضمن نطاق التجريم إلا إذا وقعت دون وجه حق، فالترخيص الممنوح للموظف العام بالتعامل مع النظام المعلوماتي الحكومي من خارج الدولة، كموظفي البعثات الدبلوماسية أو غيرهم من العاملين بالخارج لا تخضع جرائمهم لهذه الاتفاقية طالما كان هناك ترخيص ممنوح لهم بالتعامل مع النظام المعلوماتي الحكومي للدولة، وهو ما أكدت عليه المادة ٤ من الاتفاقية[٢٩].

ثانياً: الركن المادي في قانون مكافحة الجرائم الإلكترونية القطري رقم ١٤ لسنة ٢٠١٤:

لم يهتم المشرع القطري بالتمييز بين الإضرار بالنظم المعلوماتية الحكومية والنظم المعلوماتية الخاصة، حيث سوى في العقوبة المفروضة للجريمة في الحالتين بموجب المادتين ٢، ٣ من القانون رقم ١٤[٣٠]، وعلى هذا جمع بين الإضرار بالنظام المعلوماتي

---

[٢٩] حيث نصت هذه المادة على ان "لا يعاقب على الأفعال المذكورة أعلاه إلا إذا ارتكبت بدون حق"، وهو ما يعني ان ارتكابها بموجب ترخيص من الجهات المختصة يخرج عن إطار الاتفاقية.

[٣٠] **مادة ٢:** عاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (٥٠٠,٠٠٠) خمسمائة ألف ريال، كل من تمكن عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، بغير وجه حق، من الدخول إلى موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها.

وتُضاعف العقوبة المنصوص عليها في الفقرة السابقة، إذا ترتب على الدخول الحصول على بيانات أو معلومات إلكترونية، أو الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني أو أية بيانات حكومية سرية بطبيعتها أو بمقتضى تعليمات صادرة بذلك، أو إلغاء تلك البيانات والمعلومات الإلكترونية أو إتلافها أو تدميرها أو نشرها، أو إلحاق الضرر بالمستفيدين أو المستخدمين، أو الحصول على أموال أو خدمات أو مزايا غير مستحقة.

مادة ٣: يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (٥٠٠,٠٠٠) خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من دخل عمداً، دون وجه حق، بأي

المعلوماتي والإضرار بالمحتوى المعلوماتي من خلال المادة ٣، والتي حددت السلوك الإجرامي للجريمة بداية في الدخول غير المشروع– دون أن يتطرق للإضرار المترتب على الدخول المشروع– والذي يترتب عليه إلغاء أو حذف أو إضافة أو إفشاء أو إتلاف أو تغيير أو نقل أو التقاط أو نسخ أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية مخزنه في النظام المعلوماتي، أو إلحاق ضرر بالمستخدمين أو المستفيدين، أو تدمير أو إيقاف أو تعطيل الموقع الإلكتروني أو النظام المعلوماتي أو الشبكة المعلوماتية، أو تغيير الموقع الإلكتروني أو إلغائه أو تعديل محتوياته أو تصميماته أو طريقة استخدامه أو انتحال شخصية ماله أو القائم على إدارته.

ويتضح من خلال نصوص المادتين ٢، ٣ أن المشرع القطري سوى في التناول بين الإضرار بالنظم المعلوماتية الحكومية والخاصة في ذات الركن المادي وهو ارتكاب أي تصرف من شأنه ترتب أحد أو بعض أو كل النتائج سالفة الذكر، بينما اختص النظم المعلوماتية الحكومية بنوع من الأضرار هو ما ورد في عجز المادة ٢ من القانون والمتمثل في حصول الجاني على معلومات أو بيانات لها علاقة بالأمن الداخلي أو الخارجي، أو الاقتصاد الوطني، أو أي معلومات سرية، أو الإضرار بالمحتوى المعلوماتي الحكومي، أو الإضرار بالمستفيدين من هذا المحتوى، أو الاستفادة غير المستحقة سواء كانت استفادة مالية أو عن طريق الحصول على مزايا أو خدمات.

كما يلاحظ على المسلك التشريعي للمشرع القطري اغفاله للنص على تجريم الإضرار بالنظم المعلوماتية الحكومية في حالة الدخول المشروع للنظام المعلوماتي، وهو

وسيلة، موقعاً إلكترونياً، أو نظاماً معلوماتياً، أو شبكة معلوماتية، أو وسيلة تقنية معلومات أو جزء منها، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك.

وتُضاعف العقوبة المنصوص عليها في الفقرة السابقة، إذا ترتب على الدخول إلغاء أو حذف أو إضافة أو إفشاء أو إتلاف أو تغيير أو نقل أو التقاط أو نسخ أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية مخزنه في النظام المعلوماتي، أو إلحاق ضرر بالمستخدمين أو المستفيدين، أو تدمير أو إيقاف أو تعطيل الموقع الإلكتروني أو النظام المعلوماتي أو الشبكة المعلوماتية، أو تغيير الموقع الإلكتروني أو إلغائه أو تعديل محتوياته أو تصميماته أو طريقة استخدامه أو انتحال شخصية ماله أو القائم على إدارته.

(ISSN: 2537- 0758)

ما يثير التساؤل حول ارتكاب هذا الفعل من قبل موظف عام يتمتع بحق الولوج للنظام المعلوماتي دون أن يتعدى الحدود القانونية للدخول سواء كانت حدود زمنية أو مكانية أو شخصية[٣١]، الأمر الذي يخلق إشكالية تتصل بمبدأ شرعية الجرائم حيث يلاحظ أن المشرع القطري قد ضمّن كلا من المادتين ٢، ٣ من القانون رقم ١٤ لسنة ٢٠١٤ عبارة " كل من تمكن ... بغير وجه حق من الدخول ....."، وعبارة " كل من دخل عمداً، دون وجه حق ...".

وهو ما يوحي بأن الدخول المرخص غير مجرم مهما تبعه من أضرار، وهو ما **يراه الباحث** مشكلة في الصياغة التشريعية تفتح الباب أمام التذرع بمبدأ شرعية الجرائم للافلات من العقاب، ولذا كان الأجدر بالمشرع القطري أن يعدل الصياغة بحيث يشمل بالتجريم كافة السلوكيات التي تؤدي للإضرار بالنظام المعلوماتي بغض النظر عما سبق هذا الإضرار من اسلوب الولوج للنظام المعلوماتي الحكومي

ثالثاً: الركن المادي في قانون مكافحة الجرائم الإلكترونية رقم ١٧٥ لسنة ٢٠١٨:

أفرد المشرع المصري المادة ٢٠ من القانون[٣٢] لتنظيم جريمة الاعتداء على

---

[٣١] عبد الله محمد الحضري الكثيري، **مرجع سابق**، ص ٩١

[٣٢] مادة ٢٠: 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 عمدا، أو بخطأ غير عمدي وبقي بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعا أو بريدا إلكترونيا أو حسابا خاصا أو نظاما معلوماتيا يدار بمعرفه 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 كليا أو جزئيا، بأي وسيلة كانت، تكون العقوبة السجن، والغرامة التي لا تقل عن مليون جنيه ولا تجاوز خمسة ملايين جنيه.

الأنظمة المعلوماتية الخاصة بالدولة، حيث حدد من خلال هذه المادة صور السلوك الإجرامي في هذه الجريمة، والتي لجأ إلى التوسع في تعددها بحيث تشمل كافة أنماط السلوك الذي يمثل اعتداء على النظم المعلوماتية الحكومية، وقد حدد المشرع المصري هذا السلوك في إتلاف النظام المعلوماتي أو المعلومات أو البيانات أو الموقع الإلكتروني أو الحساب أو البريد الإلكتروني، أو تدمير أحد هذه العناصر أو تشويهه أو تغييره أو تغيير التصميم الخاص به أو نسخ البيانات أو المعلومات أو تسجيلها أو تعديل مسارها أو إعادة نشرها، أو إلغائها[٣٣].

ويلاحظ على مسلك المشرع المصري في تجريم هذه الأنماط من السلوك الاجرامي انه قد جمع في نص التجريم بين الأفعال الماسة بالنظام المعلوماتي الحكومي والأفعال الماسة بالمحتوى المعلوماتي لهذا النظام، حيث اتت الصياغة شاملة أي تصرف من شأنه الإضرار بالنظام أو المعلومات، دون أن يحدد طبيعة الفعل المجرم أو صورة السلوك الإجرامي ومعتمدا على النتيجة الاجرامية المترتبة على هذا السلوك والتي تتمثل في الإضرار بالنظام أو المعلومات، وعلى سلطة القضاء في تكييف التهمة[٣٤]، مع ملاحظة ربطه لهذه النتيجة بالتواجد دون وجه حق في النظام المعلوماتي[٣٥].

كما قرن المشرع المصري بدوره مثل المشرع القطري بين الدخول غير المصرح به أو تجاوز تصريح الدخول وبين فعل الإضرار بالنظام المعلوماتي، فلم يضمّن القانون ١٧٥ لسنة ٢٠١٨ حكما يخص الإضرار نتيجة للدخول المشروع إلى النظام، وهو ما يتصور عند إتيان أحد أو بعض الأفعال التي يترتب عليها الاضرار بالنظام المعلوماتي الحكومي من قبل موظف عام يملك حق الدخول ودون أن يتجاوز حدود التصريح بحكم وظيفته، أو بمناسبة الوظيفة[٣٦].

---

[٣٣] محمد علي سويلم، **مكافحة الجرائم الإلكترونية– دراسة مقارنة بالتشريعات العربية والأجنبية والاتفاقيات الدولية**، دار المطبوعات الجامعية، القاهرة ٢٠٢٠، ص ١٣٣

[٣٤] حكم محكمة النقض المصرية، **الطعن رقم ٢٧ لسنة ٨٧ قضائية**، جلسة ٢٠١٩/٢/٦

[٣٥] سيد علي السيد محمد، **الجرائم الإلكترونية– ماهيتها، صورها، إثباتها، مكافحتها**، دار التعليم الجامعى، القاهرة ٢٠٢٠، ص ٨٠

[٣٦] محمد علي سويلم، **مرجع سابق**، ص ١٣٨

(ISSN: 2537- 0758)

وهو الأمر الذي يمكن معه الحكم على التشريع المصري ذات الحكم على التشريع القطري، والذي اتسم بالقصور حيال مواجهة هذه الجريمة إذا تم ارتكابها من قبل من يحق له الدخول إلى النظام المعلوماتي، حيث تنبئ صياغة كلا من التشريعين أن هذا التجريم لم يقرره المشرع إلا في حالة الإضرار بالنظام المعلوماتي المترتب على اختراق إو بقاء غير مشروع في النظام المعلوماتي.

المطلب الثاني

الركن المعنوي فى الجريمة

لا يمكن دراسة المسئولية الجنائية عن فعل مجرم اكتفاء بالركن المادي فحسب، وإنما يتدخل القصد الجنائي في تقرير هذا النوع من المسئولية فيتحكم فيها بالإقرار أو التشديد أو التخفيف أو الاعفاء، وعلى هذا فان تحديد نطاق المسئولية عن جريمة الإضرار بالنظم المعلوماتية الحكومية قد تدخل فيه دور القصد الجنائي بصورة كبيرة، إما بسبب القواعد العامة في المسئولية الجنائية، وإما عن طريق الصياغة التشريعية في مواد التجريم والتي صرحت مباشرة بدور القصد الجنائي في التجريم والعقاب في كل من القانون الاتحادي والقوانين محل المقارنة.

أولاً: الركن المعنوي في القانون الدولي

اتى النص على الصورة العمدية لجريمة الإضرار بالنظم المعلوماتية الحكومية صريحا في إتفاقية بودابست من خلال نص المادة ٣ من الاتفاقية، والتي نصت على أن "لإلحاق المسؤولية الجنائية يجب أن يرتكب الاعتراض غير المشروع عمدا"، وهي ذات الصياغة المستخدمة في المادة ٤ التي نصت على ان "بالإضافة إلى ذلك يجب أن يكون الجاني قد تصرف عمدا" وهو ما يعني عدم تصور ارتكاب هذه الجريمة عن طريق الخطأ الأمر الذي يعفي الجاني من المسئولية الجنائية في هذه الحالة، حيث تشير هذه المواد إلى وجوب توافر صفة العمد في السلوك الإجرامي المرتكب في هذه الجريمة، وعدم قيام المسئولية عنها حال ارتكابها على سبيل الخطأ.

وأكتفى المشرع الدولي حيال هذه الجرائم بالقصد الجنائي العام والذي يتمثل في علم الجاني بالعناصر التي تتكون منها الجريمة والمتمثلة في السلوك الاجرامي والنتيجة

الاجرامية المترتبة عليه[٣٧]، وإرادته التي تتجه لارتكاب هذا السلوك رغم علمه بما يفضي إليه من إضرار بالنظام المعلوماتي الحكومي، إلا أن هذا لا يتضمن وجوب علم الجاني بتجريم التصرف الذي يقدم عليه، لان هذا العلم يعني علم بالقانون وهو ما يفترض في كل الأحوال اتباعا لقاعدة عدم جواز الاعتذار بالجهل بالقانون.

ويلاحظ على مسلك المشرع الدولي مداومته على الاكتفاء بالقصد الجنائي العام حيال هذه الجريمة، وهو المسلك الذي يفرضه لزوم المنطق القانوني إزاء الجرائم التي تتسم نتائجها الإجرامية بالخطر بحيث يضمن المشرع عن طريق هذا المسلك إقرار العقاب لمرتكبي هذه الجرائم دون إمكانية التذرع بعدم توافر قصد جنائي خاص، والتوسع في نطاق التجريم ليشمل كل إقدام على هذه التصرفات بغض النظر عن الهدف من هذه التصرفات[٣٨].

والواقع أن الاكتفاء بالقصد الجنائي العام هو مسلك المشرع حينما يتشدد في الحماية الجنائية للمصلحة محل الحماية، إذ يحاول من خلال هذا المسلك إزالة كافة العقبات التي من شأنها أن تحول دون توفير هذه الحماية أو تتعارض معها، وهو ما يبرز أهمية هذه المصلحة واعتداد المشرع بها وحرصه عليها، وهو ما يتجسد في حماية النظم المعلوماتية الحكومية وما تتضمنه من بيانات ومعلومات تتسم بالحساسية والخطورة، كما تعني حمايتها حماية المصلحة العامة، الأمر الذي دفع المشرع الدولي الى هذا المسلك التشريعي المحمود.

ثانياً: الركن المعنوي في قانون مكافحة الجرائم الإلكترونية القطري رقم ١٤ لسنة ٢٠١٤:

اتبع المشرع القطري ذات النهج الذي اتبعه المشرع الاتحادي، حيث اشترط توافر العمد في حق الجاني في جرائم الإضرار بالنظم المعلوماتية الحكومية، وهو ما يتبين من نص المادة ٢ والتي نصت على أن " كل من تمكن..."، كما يتبين من نص المادة ٣ والتي ورد بها عبارة " كل من دخل عمداً ..."، فلم يعرف التشريع الجنائي القطري ارتكاب هذا النوع من الجرائم على سبيل الخطأ، إذ ترتبط المسئولية الجنائية عنها

---

[٣٧] ربيع محمود الصغير، **القصد الجنائي في الجرائم المتعلقة بالانترنت والمعلوماتية- دراسة تطبيقية مقارنة**، مركز الدراسات العربية للنشر والتوزيع، القاهرة ٢٠١٦، ص ٢٢

[٣٨] محمود على احمد المردني، **مرجع سابق**، ص ١٥١

(ISSN: 2537- 0758)

بإتيانها عمدا من قبل الجاني[٣٩].

واستمرارا في اتباع النهج ذاته لم يشترط المشرع القطري توافر قصد خاص في هذه الجريمة، حيث اكتفى بضرورة توافر القصد الجنائي العام بعنصريه العلم والإرادة، وذلك لذات الحكمة التشريعية السالف ذكرها، والتي تقتضي عدم تقييد القضاء عند نظر الدعاوى الجنائية المقامة بخصوص هذا النوع من الجرائم بتحري توافر أي من صور القصد الجنائي الخاص، الأمر الذي يترتب عليه افتراض توافر عناصر الجريمة بصورة كاملة حال اقدام الجاني على ارتكابها عمد مع علمه بأن ما يرتكبه هو أحد التصرفات التي يترتب عليها الإضرار بالنظام المعلوماتي الحكومي على إحدى الصور التي أوردها المشرع في القانون رقم ١٤ لسنة ٢٠١٤.

ويتجلى عدم اشتراط توافر اي من القصود الخاصة من خلال المادة ٢ والتي قررت قيام المسئولية الجنائية في حالة ترتب على الدخول غير المشروع الحصول على أي من المعلومات والبيانات التي تتصف بالسرية، إذ قرر المشرع قيام الجريمة بمجرد الحصول على أي من هذه المعلومات حتى لو لم يكن الجاني يهدف من دخوله إلى الحصول عليها أو انتهاك سريتها[٤٠].

ثالثاً: الركن المعنوي في قانون مكافحة الجرائم الإلكترونية رقم ١٧٥ لسنة ٢٠١٨

تثير صياغة المشرع المصري من خلال المادة ٢٠ من القانون بعض الالتباس بسبب استهلاله المادة ٢٠ بعبارة "كل من دخل عمدا، أو بخطأ غير عمدي وبقى بدون وجه حق ..."، حيث عد البعض هذه العبارة بمثابة تصريح تشريعي بتصور ارتكاب هذه الجريمة على سبيل الخطأ، وخاصة أن المشرع كان في غنى عن ذكرها لو اراد الاكتفاء بالصورة العمدية للجريمة، إلا أن التمعن في الصياغة التشريعية للمادة يفيد ان الدخول بخطأ غير عمدي لا يجرم إلا في حالة اقترانه بالبقاء في النظام المعلوماتي الحكومي دون وجه حق، وهو ما لا يتصور إلا على سبيل العمد[٤١].

---

[٣٩] عبد الله محمد الحضري الكثيري، **مرجع سابق**، ص ١٤٠

[٤٠] ضرغام جابر عطوش آل مواش، **جريمة التجسس المعلوماتي– دراسة مقارنة**، المركز العربي للنشر والتوزيع، القاهرة ٢٠١٧، ص ٦٦

[٤١] خالد حسن أحمد لطفى، **الأدلة الجنائية الحديثة فى إثبات الجريمة الإلكترونية**، دار الفكر الجامعي، القاهرة ٢٠٢١، ص ٥٢

وعلى هذا لا يجوز القول بأن هذه الجريمة يتصور ارتكابها في التشريع المصري على سبيل الخطأ، إذ اشترط المشرع توافر ركن العمد لقيامها، إلا أن ما اتسم به التشريع المصري بحق هو عدم توحيد نظرته تجاه هذه الجريمة، ذلك انه اكتفى بضرورة توافر القصد الجنائي العام احيانا، بينما اشترط توافر القصد الجنائي الخاص في أحوال أخرى.

فمن ناحية اكتفى المشرع المصري بالقصد الجنائي العام في حالة ان ترتب على الدخول غير المشروع تحقق أحد الأضرار المنصوص عليها في المادة ٢٠ من القانون رقم ١٧٥ لسنة ٢٠١٨، ففي هذه الحالة اشترط المشرع توافر القصد الجنائي العام بعنصريه العلم والإرادة كمناط لقيام المسئولية الجنائية في حق مرتكب جريمة الإضرار بالنظام المعلوماتي الحكومي، بينما اشترط توافر قصدا جنائيا خاصا في حالة تضمن هذا الإضرار حصول الجاني على معلومات أو بيانات حكومية، حيث اشترطت المادة ٢٠ أن يكون بقصد الاعتراض أو الحصول على المعلومات وذلك لقيام المسئولية الجنائية، فإن تم الحصول على المعلومات عرضا بمناسبة الدخول غير المشروع أو بسببه دون توافر قصد الاعتراض أو الحصول على المعلومات، تقتصر المسئولية الجنائية على جريمة الدخول غير المشروع أو البقاء غير المصرح به[٤٢].

مما سبق يتبين أن الاتجاه التشريعي تجاه جريمة الإضرار بالنظم المعلوماتية الحكومية اتسم دائما باتساع نطاق التجريم، والذي يتحقق بمجرد اتيان الجاني لأي فعل يترتب عليه الإضرار بالنظام المعلوماتي على أي صورة من الصور الوارد ذكرها في كل من إتفاقية بودابست والقانون القطري رقم ١٤ لسنة ٢٠١٤، والقانون المصري رقم ١٧٥ لسنة ٢٠١٨، شريطة أن يقوم الجاني بارتكاب السلوك الاجرامي على سبيل العمد مع تحقق عنصري العلم والإرادة المكونين للقصد الجنائي العام، وذلك رغبة من المشرع في تحقيق الحماية الجنائية بمفهومها الشامل للنظم المعلوماتية الحكومية، وتحقيق الردعين العام والخاص حيال هذا النوع من الجرائم بمختلف صوره.

---

[٤٢] عرفت المادة ١ من القانون رقم ١٧٥ لسنة ٢٠١٨ الاعتراض بإنه " 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".

(ISSN: 2537- 0758)

المبحث الثاني
الأحكام العقابية الخاصة بجريمة الإضرار بالنظم المعلوماتية الحكومية

تمهيد وتقسيم:

تعد العقوبة هي الترجمة التطبيقية لرغبة المشرع في توفير الحماية الجنائية للمصلحة، حيث تعتبر السياسة العقابية والاتجاه للتشديد أو التخفيف هو ما يعكس مدى حرص المشرع على مواجهة الجريمة، وهو ما يتبين حيال الجريمة محل الدراسة من خلال العقوبات المقررة لها في القانون الدولي والتشريعات محل المقارنة، وهي العقوبات التي تبرز نظرة المشرع للنظم المعلوماتية الحكومية وأهميتها في النظام القانوني للدولة.

ولا يمكن النظر للعقوبات كوحدة واحدة، حيث اعتاد المسلك التشريعي على فرض نوعين من العقوبات هي العقوبات الأصلية والعقوبات الفرعية، والتي يلجأ لها لتعزيز الحماية الجنائية للمصلحة محل الحماية، او يضمن من خلالها عدم تكرار وقوع الجريمة سواء من نفس الجاني أو غيره، كما تقرر التشريعات عادة حيال الجرائم ذات الصبغة الفنية عدد من التدابير الجنائية التي تواجه بها الخطورة الإجرامية للجاني، والتي يراعى من خلالها طبيعة الجريمة، **وهو ما نفصله في هذا الجزء من الدراسة على النحو التالي:**

المطلب الأول: العقوبات الأصلية والفرعية.

المطلب الثاني: التدابير الجنائية المقررة للجريمة.

المطلب الأول
العقوبات الأصلية والفرعية

يعد إقرار العقوبات هو رد الفعل الطبيعي من قبل المشرع حيال ظاهرة الجريمة، وهو المسلك الذي يجب أن يتسم بالتلائم مع فداحة الجريمة ودرجة خطورتها على المجتمع، بالإضافة لقيمة المصلحة التي يتغيأ المشرع حمايتها من خلال السياسة العقابية المفروضة.

أولاً: العقوبات الأصلية والفرعية في القانون الدولي

لم يحدد المشرع الدولي عقوبات بعينها على جريمة الإضرار بالنظم المعلوماتية الحكومية من خلال إتفاقية بودابست، وانما حدد ضوابط قيام المسئولية الجنائية، تاركا

للمشرع الوطني تحديد العقوبة التي تتسم بالشدة الملائمة لأهمية المصلحة المحمية بموجب هذه الاتفاقية، وهي النظام المعلوماتي التابع للدولة ممثلة في أحد مؤسساتها أو مرافقها الحيوية، حيث تتضمن هذه النظم كثير من المعلومات والبيانات الاستراتيجية، بالإضافة لتحكم هذه النظم في سير العمل بهذه المؤسسات والمرافق، الأمر الذي يبرز مدى أهميتها بالنسبة للدولة والمجتمع، بما يعكسه ذلك من رغبة تشريعية في توفير أقصى قدر من الحماية لها، وتحقيق الردع بنوعيه بخصوص الجرائم الماسة بها[٤٣].

حيث جرمت المادة ١١ الشروع والمساهمة الجنائية، فنصت في الفقرة ١ منها على تجريم المساعدة أو التحريض على ارتكاب أي جريمة من الجرائم المنصوص عليها في المواد ٣، ٤ من الاتفاقية، كما جرمت المادة ٢ الشروع في هذه الجرائم، مع الوضع في الاعتبار ان تحقق صفة العمدية في المساهمة الجنائية أو الشروع هو مناط التجريم في هذه الحالات، اتفاقا مع اشتراط صفة العمدية في تصرف الفاعل في هذه الجرائم في حالات وقوعها بصورة تامة.

وتناولت المادة ١٢ من الاتفاقية المسئولية الجنائية للشخص المعنوي عن هذه الجرائم، تماشيا مع التوجه القانوني المعاصر للاعتراف بالمسئولية الجنائية للأشخاص الاعتبارية، ويتلخص الغرض من ذلك في فرض المسؤولية على الشركات والجمعيات والأشخاص الاعتبارية بصفة عامة عن الأفعال المجرّمة التي يقوم بها شخص في منصب قيادي داخل المؤسسة، عندما يتم ارتكابها لصالح أو لحساب الشخص الاعتباري، وتنص المادة ١٢ أيضا على المسؤولية في حال عدم قيام ذلك الشخص بدوره المنوط به في الرقابة والإشراف على العاملين بالشخص الاعتباري، بحيث يؤدي الاهمال في الرقابة إلى ارتكاب أي من موظفي الشخص المعنوي لأحد الجرائم المنصوص عليها في الاتفاقية[٤٤].

---

[٤٣] محمد الشبلي العتوم، **جرائم تكنولوجيا المعلومات في القانون الدولي- النظرية العامة للجرائم الإلكترونية**، دار الثقافة للنشر والتوزيع، عمان ٢٠٢١، ص ٥٠١

[٤٤] عبد العزيز لطفي جاد الله، **أمن المجتمع الإلكتروني بين سياسة السوق الإلكترونية والتعاون الدولي في إطار مواجهة الجرائم الإلكترونية**، دار الوفاء لدنيا الطباعة والنشر، القاهرة ٢٠٢٤، ص ١١٩

(ISSN: 2537- 0758)

ثانياً: العقوبات الأصلية والفرعية في القانون القطري

قرر المشرع القطري العقوبة الأصلية على هذه الجريمة من خلال المادتين ٢، ٣ من القانون رقم ١٤ لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية، واللتان قررتا عقوبة الحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كعقاب على سلوك الإضرار بالنظم المعلوماتية الحكومية، كما تنص المادة ٤٩ من القانون على العقاب على الاشتراك بطريق الاتفاق أو التحريض أو المساعدة في ارتكاب هذه الجريمة بذات العقوبات المقررة للفاعل الأصلي، حيث حرص المشرع القطري على المساواة في العقاب بين الفاعل والشريك في الجرائم المنصوص عليها في هذا القانون[٤٥].

وقد تناول المشرع القطري العقوبات الفرعية من خلال المادة ٥٣ والتي نصت على إلزام المحكمة بالقضاء بمصادرة الأجهزة والبرامج والوسائل التي استخدمها الجاني في ارتكاب الجريمة، دون اخلال بحقوق الغير حسن النية، كما تلتزم المحكمة باغلاق المحل الذي تمت من خلاله هذه الجريمة.

وإذا كان التشريع القطري قد تنبه لخطورة المساهمة الجنائية في هذه الجريمة فعاقب الشريك بذات العقوبة المقررة للفاعل، إلا أن السياسة العقابية القطرية عموما حيال هذه الجريمة لا يمكن وصفها بالسياسة المشددة، حيث تعامل المشرع القطري مع هذه الجريمة كجنحة برغم فداحة الجريمة والخطورة الاجرامية التي يعكسها تصرف الجاني، وكذلك خطورة النتائج الإجرامية المترتبة عليها.

ثالثاً: العقوبات الأصلية والفرعية في القانون المصري

قررت المادة ٢٠ من قانون مكافحة الجرائم الإلكترونية رقم ١٧٥ لسنة ٢٠١٨ عقوبة السجن، والغرامة التي تتراوح بين مليون جنيه وخمسة ملايين جنيه، وذلك على جريمة إتيان أي تصرف من شأنه الإضرار بالنظم المعلوماتية الحكومية، كما نصت المادتان ٣٨، ٣٩ على العقوبات الفرعية حيث نصت المادة ٣٨ على إلزام المحكمة بالقضاء بمصادرة الالات والمعدات والادوات والأجهزة التي استخدمت في ارتكاب

[٤٥] عبد الله محمد الحضري الكثيري، **مرجع سابق**، ص ١٥٩

الجريمة أو سهلت ارتكابها، كما قررت وجوب الحكم بغلق الشخص الاعتباري المدان في ارتكاب هذه الجريمة إذا كان غير حاصل على الترخيص بممارسة النشاط.

كما قضت المادة ٣٩ بعزل الموظف العام الذي يحكم بإدانته في هذه الجريمة لمدة مؤقتة تحددها المحكمة، أو عزلا دائما في حالة ارتكاب 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 أو تعطيل أحكام الدستور أو القوانين أو اللوائح أو الإضرار بالوحدة الوطنية والسلام الاجتماعي، تكون العقوبة السجن المشدد"[٤٦]، وهي الحالة التي لم يتطرق لها المشرع الدولي والقطري.

يتبين مما سبق أن المشرع المصري قد واجه جريمة الإضرار بالنظم المعلوماتية الحكومية بعقوبات تعد مشددة بالنسبة للمسلك التشريعي الجنائي، بعكس المشرع القطري الذي لم يول هذه الجريمة الاهتمام الذي يلائمها كأحدى الجرائم التي تمثل خطورة بالغة على المصلحة العامة والمجتمع مكتفيا بتوصيفها على انها جنحة.

كما يتبين اشتراك التشريعات محل الدراسة في تقرير المصادرة كعقوبة فرعية وجوبية، حيث الزم المشرع القضاء بالحكم بمصادرة ما تم استخدامه لارتكاب الجريمة من معدات وادوات وبرامج، دون الاخلال بحقوق الغير حسن النية، مع انفراد المشرع المصري بالحكم بعزل الموظف العام المدان في هذا النوع من الجرائم.

المطلب الثاني
التدابير الجنائية المقررة للجريمة

لا يكتفي المشرع عادة بالعقوبات المقررة في حالة تعامله مع الجرائم التي تحمل في ملابساتها درجة من الخطورة الإجرامية لدى الجاني، أو التي يترتب عليها نتائج إجرامية فادحة، وهو ما اتبعته التشريعات محل الدراسة ازاء جريمة الإضرار بالنظم المعلوماتية الحكومية، وهو مل يتضح على النحو التالي:

---

[٤٦] محمد كمال محمد الدسوقى، **الحماية الدولية لسرية المعلومات الإلكترونية– دراسة مقارنة**، دار الفكر والقانون، القاهرة ٢٠٢١، ص ١٨٨

(ISSN: 2537- 0758)

أولاً: التدابير الجنائية في القانون الدولي

نظم المشرع الدولي التدابير الجنائية من خلال المادة ١٣ من إتفاقية بودابست، حيث ارسى مبدأ امكاني توقيع هذا النوع من التدابير على الأشخاص الطبيعية والاعتبارية، على أساس تحقيق القدر الملائم من الردع والذي قد لا يتحقق عن تطبيق العقوبة بمفردها، حيث تركت المادة الباب مفتوحا أمام إمكانية فرض عقوبات أو تدابير أخرى لمواجهة خطورة هذه الجرائم، وعلى سبيل المثال، يمكن أن تشمل التدابير إصدار حكم يتضمن مصادرة الأشياء والأموال المضبوطة، والتي استخدمت أو تحصلت عن الجريمة، كما تركت للأطراف السلطة التقديرية لإنشاء نظام للجرائم والعقوبات الجنائية يتوافق مع أنظمتها القانونية الوطنية القائمة(٤٧).

وعلى الرغم من عدم نص الاتفاقية على تدابير محددة على سبيل الحصر، إلا أن النص على إمكانية القضاء بأي من التدابير الملائمة كان له الأثر الأكبر في اتجاه التشريعات الوطنية لإقرار نظام التدابير، والنص على التدابير التي تلائم طبيعة هذه الجرائم وطبيعة المجتمع الذي ترتكب فيه(٤٨).

ثانياً: التدابير الجنائية في التشريع القطري

لم يرد في القانون القطري رقم ١٤ لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية إلا تدبير وحيد، هو ما نصت عليه المادة ٥٢ من جواز ابعاد المدان من الدولة وذلك في حالة كونه غير حامل للجنسية القطرية، ويأتي تقرير هذا التدبير في سياق سلسلة من التعامل المخفف الذي درج عليه المشرع القطري حيال جريمة الإضرار بالنظم المعلوماتية الحكومية(٤٩).

ثالثاً: التدابير الجنائية في القانون المصري

برغم وجود التدابير الجنائية في النظام التشريعي الجنائي المصري، إلا أن احكام القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة الجرائم الإلكترونية قد خلت من النص

---

(٤٧) عبد العزيز لطفي جاد الله، **مرجع سابق**، ص ١٨٨

(٤٨) محمد علي سويلم، **مرجع سابق**، ص ٢٢٦

(٤٩) عبد الله محمد الحضري الكثيري، **مرجع سابق**، ص ١٦٦

على أي من التدابير الجنائية، مكتفية بالعقوبات الأصلية والتبعية المنصوص عليها من خلال مواد القانون.

ويرى الباحث ان هذا المسلك التشريعي لا يعد غريبا على المشرع المصري الذي لا يكترث عادة لفرض التدابير الجنائية إلا في حالات بعينها أهمها جرائم الأحداث، ومواجهة حالات إجرام فاقدي أو ناقصي الأهلية، فالنظام الجنائي المصري بصورة عامة يقوم على العقوبات بأنواعها الأصلية والتكميلية والتبعية، بصورة أكبر من الاعتماد على التدابير الجنائية.

الخاتمة

إذا كان التقدم العلمي قد قدم للمجتمع كثير من الخدمات كعنصر إيجابي في المجتمع، فإنه قد حمل معه كأثر جانبي تطورا مقابلا كمياً ونوعيا في ظاهرة الجريمة، حيث استفادت هذه الظاهرة بدورها– كغيرها من الظواهر– من التقدم محاولة الوصول من خلاله إلى تحقيق الغايات والنتائج غير المشروعة.

والواقع أن أخطر اثار التقدم التقني واستفادة الجريمة من هذا التقدم هو استخدامه في الاعتداء على البنية الرقمية للدولة، والتي تتمثل في النظم المعلوماتية الحكومية، حيث بدأ هذا النوع من الجريمة في الانتشار اما طمعا في الحصول على مصلحة خاصة أو ميزة مالية، أو تبعا لأغراض سياسية تتمثل في استهداف الإضرار بالدولة بأي وسيلة كنوع من الحاق الخسائر بالممتلكات الحكومية.

ولقد انتبه المشرع الدولي والوطني إلى خطورة هذه الظاهرة الإجرامية، فبادروا إلى مواجهتها عن طريق إصدار الاتفاقيات والتشريعات الحديثة، والتي صدرت كي تلائم طبيعة هذه الجرائم والوسائل المستخدمة لارتكابها فتم ابرام إتفاقية بودابست، وصدر القانون رقم ١٤ لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية في قطر، والقانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة الجرائم الإلكترونية في مصر، وهي القوانين التي حاول من خلالها المشرع مكافحة أي اعتداء إلكتروني على النظم المعلوماتية، فأفرد موادا من شأنها التصدي لهذه المهمة وتوفير الحماية الجنائية للنظم المعلوماتية الحكومية.

(ISSN: 2537- 0758)

وبرغم اتفاق هذه التشريعات في الهدف المرجو منها إلا أنها قد أختلفت في المعالجة التشريعية للظاهرة محل الدراسة، بحيث يمكن القول انها لم تكن على نفس القدر من الكفاية في مواجهة جريمة الإضرار بالنظم المعلوماتية الحكومية والحد من أثار هذه الجريمة.

النتائج:

١. رغم اتفاق التشريعات محل الدراسة على تجريم الإضرار بالنظم المعلوماتية الحكومية، إلا أنها اختلفت في نطاق هذا التجريم، حيث يأتي المشرع المصري في الصدارة من ناحية التوسع في هذا النطاق، يليه المشرع القطري ثم المشرع الدولي.
٢. لا يقتصر محل جرائم الإضرار بالنظم المعلوماتية الحكومية على النظام المعلوماتي فحسب، وإنما ترد هذه الجريمة على المحتوى المعلوماتي الذي يتضمنه النظام، والواقع ان التشريعات كافة تجرم صور المساس بالنظم المعلوماتية سواء وقع الضرر على النظام أو محتواه.
٣. رغبة من المشرع الدولي في تحقيق الحماية الجنائية بمفهومها الشامل للنظم المعلوماتية الحكومية، وتحقيق الردعين العام والخاص حيال هذا النوع من الجرائم بمختلف صوره حاول دائما التوسع في نطاق التجريم من خلال عمومية صور الاعتداء، والسماح للمشرع الوطني بفرض العقوبات والتدابير الجنائية دون تحديدها، تاركا للقانون الوطني تحديدها بحسب السياسة الجنائية الوطنية.
٤. تشدد المشرع المصري في مواجهة جريمة الإضرار بالنظم المعلوماتية الحكومية وذلك عن طريق فرض عقوبات تعد مشددة بالنسبة للمسلك التشريعي الجنائي المصري، بعكس المشرع القطري الذي جاءت العقوبات التي فرضها عقوبات تتسم بالضعف والهزل، حيث تعامل مع جريمة الإضرار بالنظم المعلوماتية الحكومية على انها جنحة، رغم الخطورة الإجرامية التي يتسم بها مرتكبها، والنتائج الإجرامية الفادحة المترتبة عليها.

التوصيات:

١. العمل على سرعة إبرام المعاهدة العالمية للجرائم الإلكترونية، حيث ان إتفاقية بودابست لم تعد نظاما قانونيا ملائما لمواجهة هذه الجرائم بعد مرور ما يقارب ربع قرن على اصدارها تطورت فيها هذه الجريمة بدرجة كبيرة تتطلب العمل على تحديث المسلك التشريعي الدولي في مواجهتها.

٢. تعديل قانون مكافحة الجرائم الإلكترونية المصري رقم ١٧٥ لسنة ٢٠١٨، بحيث تضاف مادة تجرم الإضرار بالنظم المعلوماتية الحكومية في حالة ترتب هذا الإضرار عن دخول أو بقاء مصرح بهم للنظام المعلوماتي الحكومي وذلك بصورة صريحة.

٣. اعتبار كافة الجرائم التي تقع على النظم المعلوماتية الحكومية من الجرائم الماسة بأمن الدولة في كل الأحوال، حيث تشكل هذه الجرائم اعتداء على مصلحة الدولة العليا المتمثلة في استقرار تداول المعلومات وسلامة البنية التحتية الرقمية للدولة، والحفاظ على المعلومات والبيانات السرية.

٤. تشديد العقوبة الفرعية في حالة ارتكاب الجريمة من قبل موظف عام بسبب أو بمناسبة ادائه للوظيفة العامة إلى العزل النهائي من الوظيفة على سبيل الوجوب في حالة الحكم بإدانته حيث ان الجاني في هذه الحالة مؤتمن على اسرار الدولة ونظمها الإلكترونية ما يضاعف المسئولية في حقه.

(ISSN: 2537- 0758)

قائمة المراجع

أولاً: المراجع العربية

١. حسين ابراهيم خليل، تطبيقات قضائية على جريمة الإزعاج المتعمد عن طريق وسائل الاتصالات الحديثة، دار الفكر والقانون، القاهرة ٢٠١٥.

٢. خالد حسن أحمد لطفى، الأدلة الجنائية الحديثة فى إثبات الجريمة الإلكترونية، دار الفكر الجامعي، القاهرة ٢٠٢١.

٣. ربيع محمود الصغير، القصد الجنائي في الجرائم المتعلقة بالإنترنت والمعلوماتية– دراسة تطبيقية مقارنة، مركز الدراسات العربية للنشر والتوزيع، القاهرة ٢٠١٦.

٤. رضا السيد عبد العاطي، الظروف المشددة والمخففة في قانون العقوبات– دراسة قضائية مقارنة، دار مصر للنشر والتوزيع، القاهرة ٢٠٢٠.

٥. زينات طلعت شحادة، الأعمال الجرمية التي تستهدف الأنظمة المعلوماتية، دار المنشورات الحقوقية صادر، بيروت ٢٠١٧.

٦. سيد علي السيد محمد، الجرائم الإلكترونية– ماهيتها، صورها، إثباتها، مكافحتها، دار التعليم الجامعى، القاهرة ٢٠٢٠.

٧. ضرغام جابر عطوش آل مواش، جريمة التجسس المعلوماتي– دراسة مقارنة، المركز العربي للنشر والتوزيع، القاهرة ٢٠١٧.

٨. ضياء الحق بهادر اليمني، التنظيم القانوني لتقنية المعلومات وأثرها على النظام العام، رسالة دكتوراه، كلية الحقوق جامعة أسيوط، القاهرة ٢٠٢٠.

٩. طه السيد أحمد الرشيدى، الطبيعة الخاصة لجرائم تقنية المعلومات، دار الكتب والدراسات العربية، القاهرة ٢٠١٦.

١٠. عبد الله محمد الحضري الكثيري، جريمة الدخول بغير وجه حق إلي المواقع الإلكترونية والنظم المعلوماتية العامة في القانون القطرى– دراسة تحليلية، دار النهضة العربية للنشر والتوزيع، القاهرة ٢٠٢١.

١١. عيسى سليم داود الزيدي، جرائم القرصنة الإلكترونية، دار الكتب القانونية للتوزيع، القاهرة ٢٠٢٢.

١٢. محمد الشبلي العتوم، جرائم تكنولوجيا المعلومات- النظرية العامة للجرائم الإلكترونية، دار الثقافة للنشر والتوزيع، عمان ٢٠٢١.
١٣. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة ٢٠١٠.
١٤. محمد علي سويلم، مكافحة الجرائم الإلكترونية- دراسة مقارنة بالتشريعات العربية والأجنبية والاتفاقيات الدولية، دار المطبوعات الجامعية، القاهرة ٢٠٢٠.
١٥. محمد علي سويلم، شرح قانون جرائم تقنية المعلومات- القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات- دراسة مقارنة، دار المطبوعات الجامعية للتوزيع، القاهرة ٢٠١٩.
١٦. محمد كمال محمد الدسوقى، الحماية الجنائية لسرية المعلومات الإلكترونية- دراسة مقارنة، دار الفكر والقانون، القاهرة ٢٠٢١.
١٧. محمد ممدوح بدير، مكافحة الجريمة المعلوماتية عبر شبكات الإنترنت والاستدلال كوسيلة لإثبات الجريمة المرتكبة عبر الإنترنت- دراسة مقارنة، مركز الدراسات العربية للنشر والتوزيع، القاهرة ٢٠١٩.
١٨. محمود رجب فتح الله، شرح قانون مكافحة جرائم تقنية المعلومات وفقا للقانون المصري الحديث، دار الجامعة الجديدة للنشر، القاهرة ٢٠١٩.
١٩. محمود على احمد المردني، النظام القانوني للجريمة الإلكترونية المعلوماتية- دراسة مقارنة، دار العلم والإيمان للنشر والتوزيع، القاهرة ٢٠٢٢.
٢٠. مدحت محمد عبد العزيز ابراهيم، الجرائم المعلوماتية الواقعة علي النظام المعلوماتي- دراسة مقارنة، دار النهضة العربية، القاهرة ٢٠١٩.
٢١. مشتاق طالب وهيب النعيمي، تزوير المعلومات كأحد صور الجرائم المعلوماتية، منشورات الحلبي الحقوقية، بيروت ٢٠١٨.
٢٢. نسرين عبد الحميد البيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، القاهرة ٢٠١٢.

(ISSN: 2537- 0758)

ثانياً: الدراسات السابقة والبحوث

١. أشرف نجيب الدريني، جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات– دراسة مقارنة، بحث منشور في مجلة روح القوانين، مجلد ٩٥ عدد ٩٥، كلية الحقوق جامعة طنطا، القاهرة ٢٠٢١.

٢. فرج علي خضير، نظرات في سياسية التجريم في قانون جرائم تقنية المعلومات، بحث منشور في مجلة المحاماة، العدد ١، القاهرة ٢٠٢١.

٣. سليمان ابو نمر، مكافحة الجريمة المعلوماتية في إطار القانون الدولي، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، الجزائر ٢٠٢١.

٤. معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة ماجستير جامعة العقيد الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية، الجزائر ٢٠١٢.