جريمة اختراق الأمن السيبراني
وحماية استخدام البيانات والمعلومات
في القانون المصري

د. إسلام مصطفى جمعة مصطفى

دكتـوراه في القانون العام - كلية الحقـوق جامعة القاهرة

(ISSN: 2537 - 0758)

جريمة اختراق الأمن السيبراني
وحماية استخدام البيانات والمعلومات في القانون المصري

د. إسلام مصطفى جمعة مصطفى

ملخص البحث

تناول البحث التعريف بالأمن السيبراني ومدى أهميته ومميزاته والتهديدات التي يتعرض لها، وبيان ماهية الجريمة الإلكترونية وبوجه خاص التعرف على جريمة اختراق الحاسب الآلي من الناحية التقنية والطبيعة القانونية. مع إيضاح كيفية تصدي المشرع المصري لهذه الجريمة وبيان نص التجريم والعقاب وتوافر أركانها.

وما يترتب على حدوث تلك الجريمة من آثار عملية هامة، تتمثل في انتهاك حقوق الأفراد بما يشمل جرائم الاعتداء على حرمة الحياة الخاصة والتي يندرج منها جرائم استراق السمع أو نقله أو تسجيله، التقاط أو نقل صورة شخص، إذاعة أو استعمال تسجيل أو مستند أو التهديد بالإفشاء بمحتوياته، ربط معطيات شخصية للغير بمحتوى مناف للآداب العامة، الدخول غير المشروع أو الدخول بالخطأ والبقاء بدون وجه حق على موقع أو حساب خاص أو نظام معلوماتي، الاحتيال والاعتداء على بطاقات البنوك وأدوات الدفع الإلكترونية الخاصة بالأفراد، اصطناع ونسبة موقع بريد إلكتروني أو حساب خاص لشخص طبيعي.

أو ما يعد انتهاكًا لحقوق الدولة أو إحدى ومؤسساتها بما يشمل جرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة والتي يندرج منها جرائم الاعتداء على سلامة الشبكات المعلوماتية، اصطناع ونسبة موقع بريد إلكتروني أو حساب خاص لشخص اعتباري، إدارة أو استخدام موقع أو حساب خاص بهدف ارتكاب أو تسهيل ارتكاب جريمة، الاعتداء على بطاقات البنوك وأدوات الدفع الإلكترونية الخاصة بمؤسسات الدولة، وإلى غير ذلك من جرائم.

وبيان التفرقة بين تلك الآثار سواء تمثلت في الجرائم المضرة بأمن الدولة من جهة الداخل سواء كان اجتماعيًا أم سياسيًا أم اقتصاديًا أم كان يتعلق بنظام الحكم وإلى حماية الأمن والاستقرار الذي يتمتع به الأفراد، أم الاعتداء على أمن الدولة من جهة الخارج بهدف حماية استقلال الدولة وسيادتها.

Abstract

The academic research dealt with defining cyber security and its importance, features and threats to it, clarifying the nature of electronic crime, and identifying the crime of hacking a computer from a technical point of view and legal nature. With an explanation of how the Egyptian legislator tackled this crime and an explanation of the text of criminalization and punishment and the availability of its elements.

And the important practical consequences of the occurrence of that crime, represented in the violation of the rights of individuals, including crimes of assault on the sanctity of private life, which include the crimes of eavesdropping, transmitting or recording, taking or transmitting a person's picture, broadcasting or using a recording or document, or threatening to disclose With its contents, linking personal data of others with content contrary to public morals, illegal or mistaken entry and illegal stay on a website, private account or information system, fraud and attack on bank cards and electronic payment tools for individuals, fabricating and attributing an email site or private account to a person natural.

Also, considered a violation of the rights of the state or one of its institutions, including crimes of attacking the state's information systems, including crimes of attacking the integrity of information networks, fabricating and attributing an e-mail site or a private account to a legal person, managing or using a site or private account with the aim of committing or facilitating Committing a crime, attacking bank cards and electronic payment tools for state institutions, and other crimes.

And to clarify the distinction between those effects, whether they are crimes harmful to the security of the state from the inside, whether it is social, political, economic, or related to the system of government and to the protection of security and stability enjoyed by individuals, or attacks on state security from the outside to protect the independence and sovereignty of the state.

مقدمة وتقسيم

يشهد العالم العديد من الأحداث التي لم نعهد بها من قبل، حيث دعت منظمة الصحة العالمية إلى الإعلان عن وباء عالمي على أثر تفشي الفيروس الذي يسبب

(ISSN: 2537 - 0758)

مرض (كوفيد-١٩)، والذي ينحدر من سلالة فيروسات تُسمى كورونا أو الفيروسات التاجية. وذلك مع التوجه إلى ضرورة التعاون الدولي لتوحيد آليات الحد من انتشاره، وإقرار منظمة الصحة العالمية بأنه حتى وقتنا الراهن لا توجد أية أدوية مرخصة لعلاج هذا المرض أو الوقاية منه لعدم التوصل لاكتشاف لقاح آمن وفعال لتفادي إصابة العدوى به.

ووجدت دول العالم كافة مدى ضرورة الالتزام بمسئولية حماية الحياة الإنسانية باعتبارها أغلى ما يمكن للدول والحكومات والمجتمعات والمؤسسات المحافظة عليها. ومن جهة أخرى توجب عليها الموازنة بين الحفاظ على النفس البشرية بما يمثل اعتداء على حقوق وحريات الأفراد، وبين أخطار الأضرار الاقتصادية الناجمة عن الإغلاق الكامل أو الجزئي للبلاد لوقت غير معلوم. وما يترتب على ذلك من آثار يمكن أن تؤدي بدورها إلى انهيار اقتصاد بعض الدول، واختلال مراكز القوى في العالم تبعا لإمكانية صمود اقتصاد كل دولة على بصورة منفردة دون الاعتماد على غيرها من الدول.

وبناءً على تلك المعطيات واستنادا لحفظ النفس البشرية التي تعد أولى مقاصد الشريعة الإسلامية، وفي ضوء مواجهة تفشي هذا الفيروس، مما دعا إلى ضرورة التحول الرقمي في القطاع العام وتطوير الكوادر العاملة لديه لتقديم خدمات المواطنين لضمان استمرار حياة الفرد والكيانات والدولة مجتمعين. ومنها استكمال الدراسة لكافة المراحل التعليمية عن بعد، وخدمات العدالة الإلكترونية من رفع الدعوى والتقاضي والمحاكمة عن بعد، والمعاملات الخاصة بمصلحة الضرائب المصرية، وإنشاء موقع مصر الرقمية الذي يشمل خدمات الشهر العقاري والتوثيق والتموين، والمحاكم، والسجل التجاري والمرور. وعلى الصعيد الخاص لم تتوان الجهات والهيئات الخاصة عن مواكبة التطور للتحول الرقمي في شتى مجالات الحياة.

ولا شك باعتبارها طفرة للتحول تشمل ما لها من مميزات وما عليها من عيوب يكمن تداركها بالرؤية المستقلة بعيدة المدى للتعلم من أخطاء الآخرين. فماذا يحدث لو أصبح الحساب البنكي خاوي بدون أي مبررات، أو تم نشر كل ما نعرفه أو نمتلكه على الملاء، أو فقدان كافة الرموز السرية والبيانات والمعلومات للمواطنين أو الكيانات الخاصة والعامة للدولة؟

نعتقد أنه لا يوجد مصطلح قد يصف هذه الكارثة؟ وبسبب الطفرة التقنية التي يشهدها عصرنا أتمت الكثير من العمليات التي تطلبت أن تكون المعلومات إلكترونية،

وبسبب حداثة وجود المعلومات إلكترونيا لم تكن وسائل الحماية الإلكترونية قوية بما يكفي لحمايتها من المخترقين. وبعد كل عملية من عمليات الاختراق المؤثرة على أمن المعلومات يزداد الاهتمام بأمن المعلومات كما يزداد تطوّره وتزاد قوة وسائل حماية المعلومات.. ولكن أين كانت هذه المعلومات قبل وجود الإنترنت؟ أو فلنسأل سؤالاً آخر هل كانت توجد معلومات قبل وجود الإنترنت؟

بكل تأكيد كانت هذه المعلومات موجودة على الورق، مخزنة في مكاتب الأرشيف في كل مؤسسة أو شركة، وفي نفس الوقت كان للأرشيف وتنظيمه وحمايته أهمية قصوى، ألا تعتقد أن تأمين هذا الأرشيف كان مهما جدا للمؤسسات؟ ألم يكن فقدان إحدى الأوراق مؤثراً بقدر فقدان المعلومات الإلكترونية؟ أم لم يكن التعديل على هذه المعلومات وتزويرها مؤثرا بنفس قدر التعديل على المعلومات الإلكترونية؟ هذه الحقائق توصلك إلى أن المعلومات أينما وجدت إلكترونيا أو ورقيا تحتاج إلى حماية، لذا فإن الحديث عن أمن المعلومات لا يتوقف على حماية المعلومات إلكترونيا فقط، بل يتعداه إلى حمايتها في أنظمتها التقليدية أو أينما كانت.

وتتمثل أهمية الدراسة في التحديات الأمنية والتقنية والقانونية لاستخدامات تقنية المعلومات والحاسب الآلي أو أي جهاز متصل بشبكة الإنترنت (تابلت/ محمول ذكي)، مما يزيد من خطورة جريمة اختراق الأمن السيبراني على الأمن القومي ومؤسسات الدولة سواء القطاع العام أو الخاص والأفراد، وهل تنتفي مسئولية مقدم الخدمة أو البرنامج بمجرد موافقتنا على شروط الاستخدام؟ وسوف تقتصر الدراسة على كيفية محاولة حماية ومواكبة تطور التحول الرقمي دون معوقات أو على الأقل لمحاولة الحد منها، وبيان شرح جريمة اختراق الأمن السيبراني وأمن المعلومات في القانون المصري، من حيث بيان ماهيتها، ونص التجريم والعقاب، ومحاولة مشاركة فن القرصنة مع الجميع، والذي غالبًا ما يكون فهم تقنيات القرصنة أمرًا صعبًا لتطلبه كلاً من الاتساع وعمق المعرفة.

وعلى ما يبدو أن العديد من نصوص القرصنة مقصورة على فئة معينة ومربكة بسبب وجود فجوات قليلة في هذا التعليم. **ولذلك نقسم خطة البحث كما يلي:**

الفصل الأول: التعريف بالأمن السيبراني ومدى أهميته ومميزاته والتهديدات الموجه ضده

المبحث الأول: التعريف بالأمن السيبراني

المبحث الثاني: أهمية الأمن السيبراني والتهديدات الموجه ضده

الفصل الثاني: جريمة اختراق الأمن السيبراني في القانون المصري

(ISSN: 2537 - 0758)

المبحث الأول: ماهية الجريمة الإلكترونية.
المبحث الثاني: المفهوم التقني والطبيعة القانونية لجريمة الاختراق.

الفصل الأول
التعريف بالأمن السيبراني
ومدى أهميته ومميزاته والتهديدات الموجه ضده

للوهلة الأولى قد يستغرب البعض من قراءة أو سماع مصطلح الأمن السيبراني، وايضاحا لذلك نود أن نشير أن هذا المسمى يرادف في المعنى كل ما هو إلكتروني. ويختص هذا الأمن بكل ما يتعلق بالإلكترونيات، ومنها على سبيل المثال وليس الحصر أمن السيارة أو أجهزة المنزل أو حتى أمن الحواسب والبطاقات الأمنية وكلمات المرور. والإلكترونيات لها أنواع مختلفة، وهذا يقتضي بالتأكيد أن تكون طرق تأمين هذه الإلكترونيات مختلفة، فأمن الشبكات اللاسلكية مختلف عن أمن نظم المعلومات والذي يختلف بدوره عن أمن النظم وأمن إنترنت الأشياء بمختلف أنواعه، حيث يتعلق بالحماية الإلكترونية سواء تعلق الأمر بأمن المعلومات من عدمه.

وإن كنا نرى ضرورة التفرقة بين مجالي الأمن السيبراني وأمن المعلومات، وعدم استخدامهما كمصطلحين مترادفين، فالأمن السيبراني يختص بأمن كل ما يوجد في الفضاء الإلكتروني، ويشمل ذلك أمن المعلومات. بينما يهتم مجال أمن المعلومات بأمن المعلومات وإن كانت في الفضاء الإلكتروني. ونتناول في هذا الفصل التعريف بالأمن السيبراني، وماهية جرائم الاختراق أو القرصنة الإلكترونية.

المبحث الأول
التعريف بالأمن السيبراني
نبذة تعريفية عن الأمن السيبراني (Cyber Security)

يعد الأمن السيبراني أو ما يطلق عليه أمن المعلومات والحاسب الآلي، هو فرع من فروع التكنولوجيا المتخصصة بحماية الأنظمة والممتلكات والشبكات والبرامج من الهجمات الرقمية التي تهدف في الغالب إلى الوصول للمعلومات الحساسة، أو تغييرها، أو إتلافها أو ابتزاز المستخدمين للحصول على الخدمات أو الأموال أو السيطرة على العمليات التجارية.

وتعددت تعريفات الأمن السيبراني، حيث عرف بأنه مجموعة المسائل التي من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسب الآلي أو الشبكات، والتي تشمل الوسائل والأدوات المستخدمة في مواجهة الاختراق/القرصنة وكشف الفيروسات الرقمية ووقفها، وتوفير الاتصالات المشفرة(١).

إن الأمن السيبراني هو مجموعة من الأدوات والسياسات ومفاهيم الأمن الإلكتروني وضمانات الأمان والمبادئ التوجيهية وأساليب إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والضمانات والتقنيات التي يمكن استخدامها لحماية البيئة الإلكترونية والمنظمات وأصول المستخدم(٢).

ويعد مجموعة التقنيات والعمليات والممارسات وتدابير الاستجابة والتخفيف المصممة لحماية الشبكات وأجهزة الحاسوب والبرامج والبيانات من الهجوم أو التلف أو الوصول غير المصرح به لضمان السرية والنزاهة والتوافر (٣).

حيث يتكون الأمن السيبراني إلى حد كبير من الأساليب الدفاعية المستخدمة لاكتشاف الدخلاء المحتملين واحباطهم(٤). وهو فن ضمان وجود واستمرارية مجتمع المعلومات لدولة ما، وضمان وحماية المعلومات والمجموعات والبنية التحتية الحيوية في الفضاء السيبراني(٥).

(1) "Cyber Security involves reducing the risk of malicious attack to software, computers and networks. This includes tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, enable encrypted communications, and on and on" (Cyber security, Edward Amoroso 2007).
(2) "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets." (ITU 2009).
(3) "The body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability" (Public safety Canada, 2014).
(4) "Cybersecurity consists largely of defensive methods used to detect and thwart would-be intruders" (Kemmerer, 2003).
(5) "The art of ensuring the existence and continuity of the information society of a nation, guaranteeing and protecting, in Cyberspace, its information, as-sets and critical infrastructure" (Canongia & Man-Darino, 2014).

(ISSN: 2537 - 0758)

وهو حالة الحماية من الاستخدام الإجرامي أو غير المصرح به للبيانات الإلكترونية، أو الإجراءات المتخذة لتحقيق ذلك[٦]. ويستلزم الأمن السيبراني حماية شبكات الحاسب والمعلومات التي تحتويها من الاختراق والتلف أو الاضطراب[٧]. والقدرة على الحماية أو الدفاع عن استخدام الفضاء الإلكتروني من الهجمات الإلكترونية[٨].

ويشار إليه بأنه النشاط أو العملية أو القدرة أو الحالة التي يتم بموجبها حماية أنظمة المعلومات والاتصالات والمعلومات الواردة فيها، أو الدفاع ضد الضرر أو الاستخدام غير المصرح به أو التعديل أو الاستغلال[٩].

وإن كنا نرى صعوبة تحديد تعريف شامل للأمن السيبراني، باعتباره مصطلح متغير ينظم ويجمع كافة الموارد والعمليات والهياكل المستخدمة لحماية الفضاء الإلكتروني والأنظمة التي تدعم الفضاء الإلكتروني من الأحداث التي لا تتماشى بحكم القانون مع حقوق الملكية الفعلية.

مصطلحات مرتبطة بالأمن السيبراني

يتبع الأمن السيبراني نهجا محددا يتكون من عدة طبقات للحماية تثبت في أجهزة الحاسب أو الشبكات أو البرامج أو البيانات التي ينوي المستخدم حمايتها. وتوجد من المصطلحات المرتبطة بالأمن السيبراني نذكر منها:

أ) الفضاء السيبراني (Cyber Space)

عبارة عن بيئة تفاعلية رقمية تشمل عناصر مادية وغير مادية مكونة من مجموعة من الأجهزة الرقمية وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشتغلين أو مستعملين ويطلق عليه (الذراع الرابعة للجيوش الحديثة).

---

(6) "The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this" (Oxford University Press, 2014).

(7) "Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption" (Lewis, 2006).

(8) "The ability to protect or defend the use of cyber-space from cyber-attacks" (CNSS, 2010).

(9) "The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation" (DHS, 2014).

ب) الردع السيبراني (Cyber Deterrence)

يعرف على أنه منع الأعمال الضارة ضد الأصول الوطنية في الفضاء الرقمي والأصول التي تدعم العمليات الفضائية.

ج) الهجمات السيبرانية (Cyber Attacks)

أي فعل يقوض من قدرات ووظائف شبكة الحاسوب لغرض شخصي أو سياسي، من خلال استغلال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام.

د) الجريمة السيبرانية (Cyber Crime)

مجموعة من الأفعال والأعمال غير القانونية التي عبر معدات أو أجهزة إلكترونية عبر شبكة الإنترنت، وتتطلب حكما خاصا بتقنيات الحاسوب ونظم المعلومات لارتكابها أو التحقيق فيها أو مقاضاة فاعليها. وهي التي سوف نتناولها بالتفصيل في هذه الدراسة.

المبحث الثاني
أهمية الأمن السيبراني والتهديدات الموجه ضده

يستفيد الجميع من برامج الدفاع الإلكتروني المتقدمة على المستوى الفردي. ويمكن أن يُسفر هجوم الأمن الإلكتروني عن الكثير من الأشياء ومنها سرقة الهوية، ومحاولات الابتزاز، وفقدان البيانات المهمة. حيث يعتمد الجميع على بنية أساسية حيوية مثل محطات الطاقة والمستشفيات وشركات الخدمات المالية، ويعد تأمين هذه المؤسسات وغيرها هو أمر ضروري للحفاظ على سير عمل المجتمع لدينا.

ونعرض للمفاهيم الثلاثة التي تؤدي بدورها لأهداف الحفاظ على سلامة موارد نظام المعلومات وتوافرها وسريتها (بما في ذلك الأجهزة والبرامج الثابتة والمعلومات أو البيانات والاتصالات[١٠]:

أ) **السرية** (Confidentiality)

وهي التحكم في الولوج إلى البيانات وإتاحتها لمن يسمح لهم فقط. ويتضمن هذا المصطلح مفهومين مترابطين، وهما **سرية البيانات** بما يضمن عدم إتاحة المعلومات الخاصة أو السرية أو الكشف عنها للأفراد غير المصرح لهم. و**الخصوصية** التي تضمن أن يتحكم الأفراد في المعلومات المتعلقة بهم أو يؤثرون عليها والتي يمكن جمعها وتخزينها ومن قبل من، ومن قد يتم الكشف عن هذه المعلومات.

---

(10) Cryptography and Network Security, William Strallings, global seventh edition 2017, chapter 1, page 21.

(ISSN: 2537 - 0758)

ب) النزاهة (Integrity)

وهي الحفاظ على سلامة البيانات والمعلومات وحمايتها من الهجمات التخريبية أو السرقة. ويشمل هذا المصطلح مفهومين مرتبطين، وهما تكامل البيانات بما يضمن أن المعلومات المخزنة والبرامج يتم تغييرها فقط بطريقة محددة ومصرح بها. وتكامل النظام يضمن يؤدي وظيفته المقصودة بطريقة سليمة وخالية من التلاعب غير المصرح به المتعمد أو غير المقصود للنظام.

ج) الجاهزية (Availability)

وهي جاهزية جميع الأنظمة والخدمات والمعلومات واتاحتها حسب طلب الشركة أو عملائها. وذلك بما يضمن عمل الأنظمة على الفور وعدم رفض الخدمة للمستخدمين المصرح لهم.

مميزات الأمن السيبراني

حماية الشبكات والبيانات من الدخول غير المصرح به، وتحسين مستوى حماية المعلومات وضمان استمرارية الأعمال، وتعزيز ثقة المساهمين وأصحاب المصلحة في الشركة، واسترداد البيانات المسربة في وقت أسرع في حالة حدوث خرق للنظام الأمني السيبراني.

أنواع تهديدات الأمن السيبراني

تصيد المعلومات هو عملية إرسال رسائل بريد إلكتروني احتيالية تشبه رسائل البريد الإلكتروني من المصادر الموثوقة. والهدف هو سرقة المعلومات الحساسة مثل أرقام بطاقة الائتمان ومعلومات تسجيل الدخول. وهو أكثر أنواع الهجمات الإلكترونية شيوعًا. يمكنك المساعدة في حماية نفسك من خلال التثقيف أو استخدام الحلول التقنية التي تعمل على تصفية رسائل البريد الإلكتروني الضارة.

برامج الفدية هي نوع من البرامج الضارة مصممة بهدف ابتزاز المال عن طريق منع الوصول إلى الملفات أو نظام الحاسوب حتى يتم دفع الفدية. ولا يضمن دفع الفدية استرداد الملفات أو استعادة النظام.

البرامج الضارة هي نوع من البرامج المصممة للوصول غير المصرح به إلى جهاز الحاسوب أو إلحاق الضرر به.

التحايل باستخدام الهندسة الاجتماعية هي أسلوب يستخدمه الخصوم لاستدراجك إلى الكشف عن المعلومات الحساسة. يمكنهم طلب الحصول على دفع نقدي أو

الوصول إلى بياناتك السرية. ويمكن دمج الهندسة الاجتماعية مع أي من التهديدات المذكورة سابقًا لزيادة فرصتك في النقر على الروابط أو تنزيل البرامج الضارة أو الوثوق بمصدر ضار.

الفصل الثاني
جريمة اختراق الأمن السيبراني في القانون المصري

أسهم دخول التقنيات الحديثة في مجال الاتصالات وتكنولوجيا المعلومات وشبكة الإنترنت إلى إفراز أنماط مستحدثة من الجرائم لم يكن للبشرية سابق عهد بها، وتتميز هذه النوعية من الجرائم بأنها معقدة في طرق ارتكابها، ووسائل كشفها، كما أنها ذات طابع دولي، لذلك أصبحت تمثل خطرا داهما يؤرق دول العالم بأسره. وسنحاول في هذا المبحث التعرف على الجريمة الإلكترونية، وجريمة اختراق الأمن السيبراني في القانون المصري، وذلك من حيث ماهيتها، وخصائصها، وطبيعتها القانونية.

المبحث الأول
ماهية الجريمة الإلكترونية

بالتمعن في دراسة النظم القانونية المختلفة والتشريعات الإقليمية والدولية في محاولة تعريف محدد للجريمة الإلكترونية، نجد أن هناك تفاوت في تحديد مفهومها، فالبعض عرف الجريمة الإلكترونية والبعض الآخر لم يتطرق لتعريفها مكتفياً ببيان الأفعال التي يجرمها ووضع لها العقوبات التي يراها تتناسب مع الجرم. وسوف نعرض لكلٍ من التعريف التقني الفني والقانوني:

تعريف الأمم المتحدة: أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية.

تعريف مجلس أوروبا: عرفت اتفاقية مجلس أوروبا المبرمة في بودابست لعام ٢٠٠١، الجريمة الإلكترونية في الفصل الثاني منها، بأنها الجرائم ضد السرية والنزاهة وتوافر البيانات وأنظمة الحاسب الآلي،

وتعريف الدخول غير المشروع والاعتراض القانوني والتدخل في البيانات والنظام وإساءة استخدام الأجهزة. وذلك مع تفرد الاتفاقية في تقسيم الجرائم الإلكترونية إلى جرائم ذات الصلة بالحاسب الآلي، والتزوير، والمحتوى المتعلق بالمواد الإباحية للأطفال،

(ISSN: 2537 - 0758)

وانتهاك حقوق المؤلف والجرائم المجاورة لها، والمحاولة والمساعدة والتحريض والمسؤولية المؤسسية[١١].

تعريف مشروع القانون العربي: النموذجي في شأن مكافحة جرائم الحاسوب والإنترنت الذي صيغ في جامعة الدول العربية بين مجلس وزراء الداخلية العرب ومجلس وزراء العدل العرب في ٢٢ مايو ٢٠٠٣، والذي تم إقراره قد عرف الجريمة الإلكترونية في المادة الأولى منه بأنها كل فعل مؤثم يتم ارتكابه عبر أي وسيط إلكتروني[١٢].

المشرع السعودي: أي فعل يرتكب متضمنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخافة لأحكام هذا النظام (ف٨م١ المرسوم الملكي م/١٧).

المشرع القطري: أي فعل ينطوي على استخدام وسيلة تقنية المعلومات أو النظام أو الشبكة المعلوماتية بالطريقة غير مشروعة بما يخالف أحكام القانون (قانون رقم ١٤ لسنة ٢٠١٤).

أما عن **المشرع المصري** في القانون رقم ١٧٥ لسنة ٢٠١٨ ولائحته التنفيذية، والمشرع الإماراتي في المرسوم الاتحادي رقم ٥ لسنة ٢٠١٢، والمشرع العماني في المرسوم رقم ١٢ لسنة ٢٠١١، والمشرع البحريني في القانون رقم ٦٠ لسنة ٢٠١٤، فقد اكتفى التشريع بشأن مكافحة جرائم تقنية المعلومات بوضع نص التجريم الأفعال المكونة للجريمة الإلكترونية دون التطرق لتعريفها.

وننوه عن قرار رئيس جمهورية مصر العربية رقم ٢٧٦ لسنة ٢٠١٤ بشأن انضمام مصر إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بتاريخ ٢١ ديسمبر ٢٠١٠ مع التحفظ بشأن شرط التصديق.

تعريف الجريمة الإلكترونية في التشريع المصري

نتناول بالبحث التعرف على مفهوم الجريمة الإلكترونية في التشريع المصري، وذلك بعرض نصوص التجريم والعقاب قبل وبعد صدور قانون رقم ١٧٥ لسنة ٢٠١٨ الخاص بشأن مكافحة جرائم تقنية المعلومات.

---

(11) www.gocsi.com

(١٢) الجرائم الاقتصادية الشائعة الجزء٢، بهاء المري، الطبعة الثانية ٢٠١٩، ص١٨.

الوضع قبل صدور قانون رقم ١٧٥ لسنة ٢٠١٨ الخاص بشأن مكافحة جرائم تقنية المعلومات

نصت المادة ٣١ من الدستور المصري الصادر عام ٢٠١٤ جاءت نصا دستوريا صريحا يشير إلى وجوب الحفاظ على المعلومات والبيانات الالكترونية، إذ جرى نصها على أن أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون.

وتوجد بعض النصوص القانونية المتناثرة في قوانين مختلفة تتحدث عن بعض العقوبات المرتبطة ببعض الجرائم الإلكترونية منها قانون الاحوال المدنية المصري رقم ١٤٣ لسنة ١٩٩٤ والذي نظم في عدد من مواده تجريم تعديل بيانات الأحوال الشخصية للمواطنين المسجلة على الحاسب الآلي أو الوسائط الالكترونية الموجودة بمصلحة الأحوال المدنية التابعة لوزارة الداخلية بالتزوير أو الاتلاف أو الاطلاع عليها دون وجه حق، وذلك في عدد من المواد منها المادة ٧٢ من القانون والتي جاءت تنص على أن" في تطبيق أحكام هذا القانون وقانون العقوبات تعتبر البيانات المسجلة بالحاسبات الآلية وملحقاتها بمراكز معلومات الأحوال المدنية ومحطات الإصدار الخاصة بها المستخدمة في إصدار الوثائق وبطاقات تحقيق الشخصية بيانات واردة في محررات رسمية.

فإذا وقع تزوير في المحررات السابقة أو في غيرها من المحررات الرسمية، تكون العقوبة الأشغال الشاقة المؤقتة أو السجن لمدة لا تقل عن خمس سنوات، والمادة ٧٤ من القانون والتي جاء في نصها مع عدم الإخلال بأية عقوبة شديدة منصوص عليها في قانون العقوبات أو في غيره من القوانين، كأن يعاقب بالحبس مدة لا تجاوز ستة أشهر وبغرامة لا تزيد عن خمسمائة جنيه أو بإحدى هاتين العقوبتين كل من اطلع أو شرع في الاطلاع أو حصل أو شرع في الحصول على البيانات أو المعلومات التي تحتويها السجلات أو الحاسبات الآلية أو وسائط التخزين الملحقة بها أو قام بتغييرها بالإضافة أو بالحذف أو بالإلغاء أو بالتدمير أو بالمساس بها بأي صورة من الصور أو أذاعها أو أفشاها في غير الأحوال التي نص عليها القانون ووفقا للإجراءات المنصوص عليها فيه، فإذا وقعت الجريمة على البيانات أو المعلومات أو الإحصاءات المجمعة تكون العقوبة السجن.

والمادة ٧٥ من القانون التي تنص على أنه يعاقب بالحبس مدة لا تجاوز ستة أشهر وغرامة لا تقل عن مائتي جنيه ولا تزيد على خمسمائة جنيه أو بإحدى هاتين العقوبتين كل من عطل أو أتلف الشبكة الناقلة لمعلومات الأحوال المدنية، أو جزءا منها وكان

(ISSN: 2537 - 0758)

ذلك ناشئا عن إهماله، أو رعونته، أو عدم احترازه، أو عدم مراعاته للقوانين واللوائح والأنظمة.

فإذا وقع الفعل عمدا تكون العقوبة السجن مع عدم الإخلال بحق التعويض في الحالتين. أما المادة ٧٦ من القانون فنصت بأنه يعاقب بالأشغال الشاقة المؤقتة كل من اخترق أو حاول اختراق سرية البيانات أو المعلومات أو الإحصاءات المجمعة بأية صورة من الصور وتكون العقوبة الأشغال الشاقة المؤيدة إذا وقعت الجريمة في زمن الحرب.

وقرر قانون حماية الملكية الفكرية رقم ٨٢ لسنة ٢٠٠٢ في بعض مواده حماية السرقات الأدبية عبر شبكة الإنترنت فجاء نص المادة ١٤٠ منه للحديث عن نوعية من جرائم الإنترنت فنص على أنه تتمتع بحماية هذا القانون حقوق المؤلفين على مصنفاتهم الأدبية والفنية، وبوجه خاص المصنفات الآتية:

الكتب والكتيبات والمقالات والنشرات من الحاسب الآلي أو من غيره. من برامج الحاسب الآلي وقواعد البيانات سواء أكانت مقروءة من الحاسب الآلي أو من غيره من المحاضرات، والخطب، والمواعظ، وأية مصنفات شفوية أخرى إذا كانت مسجلة.

وجاء نص المادة ١٨١ في البند الرابع والسادس، ناصا على العقوبة وجرى على أن مع عدم الإخلال في أية عقوبة أشد في أي قانون آخر، يعاقب بالحبس مدة لا تقل عن شهر وبغرامة لا تقل عن خمسة آلف جنيه ولا تجاوز عشرة آلاف جنيه أو بإحدى هاتين العقوبتين، وكل من أرتكب أحد الأفعال الآتية:

نشر مصنف، أو تسجيل صوتي، أو برنامج إذاعي، أو أداء محمي طبقاً لأحكام هذا القانون عبر أجهزة الحاسب الآلي، أو شبكات الإنترنت، أو شبكات المعلومات، أو شبكات الاتصال، أو غيرها من الوسائل دون إذن كتابي مسبق من المؤلف أو صاحب لحق المجاور.

والإزالة أو التعطيل أو التعييب بسوء نية بأية حماية تقنية يستخدمها المؤلف أو صاحب الحق المجاور كالتشفير أو غيره.... وفي حالة العود تكون العقوبة الحبس مدة لا تقل عن ثلاثة أشهر والغرامة التي لا تقل عن عشرة آلاف جنيه ولا تجاوز خمسين آلف جنيه. وفي جميع الأحوال تقضي لمحكمة بمصادرة النسخ محل الجريمة أو المتحصلة منها وكذلك المعدات والأدوات المستخدمة في ارتكابها. ويجوز للمحكمة عند الحكم بالإدانة أن تقضي بغلق المنشأة التي استغلها المحكوم عليه في ارتكاب الجريمة

مدة لا تزيد عن ستة أشهر، ويكون الغلق وجوبيا في حالة العود في الجرائم المنصوص عليها في البندين ثانياً وثالثاً من هذه لمادة. وتقضي المنشأة بنشر ملخص الحكم بالإدانة في جريدة يومية أو أكثر على نفقة المحكوم عليه.

كما نظم قانون تنظيم الاتصالات ١٠ لسنة ٢٠٠٣ بعض جرائم الإنترنت فنص في المادة ٧٣ منه على أن يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز خمسين ألف جنيه أو بإحدى هاتين العقوبتين، كل من قام أثناء تأدية وظيفته في مجال الاتصالات أو بسببها بأحد الأفعال الآتية:

١) إذاعة أو نشر أو تسجيل لمضمون رسالة اتصالات أو لجزء منها دون أن يكون له سند قانونيا في ذلك.
٢) إخفاء، أو تغيير، أو إعاقة، أو تحوير أية رسالة اتصالات أو لجزء منها تكون قد وصلت إليه.
٣) الامتناع عمداً عن إرسال رسالة اتصالات بعد تكليفه بإرسالها.
٤) إفشاء أية معلومات خاصة بمستخدمي شبكات الاتصال أو عما يجرونه أو ما يتلقونه من اتصالات وذلك دون وجه حق، كما نصت المادة ٧٥ منه على أن يعاقب بالحبس وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائه ألف جنيه أو بإحدى هاتين العقوبتين، كل من قام بإفشاء أو نشر أو إذاعة أية معلومات حصل عليها بحكم وظيفته أو بسببها عن منشأة عاملة في مجال الاتصالات متى كان من شأن ذلك أن يؤدى إلى قيام منافسة غير مشروعة بين المنشآت العاملة في هذا المجال.

وجاء قانون التوقيع الالكتروني رقم ١٥ لسنة ٢٠٠٤، لينظم بعض صور الجرائم الالكترونية فنص في المادة ٢٣ منه، على أنه مع عدم الإخلال بأية عقوبة اشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مئة ألف جنيه أو بإحدى هاتين العقوبتين كل من:

أ) أصدر شهادة تصديق الكتروني دون الحصول على ترخيص بمزاولة النشاط من الهيئة.
ب) أتلف أو عيّب توقيعا أو وسيطا أو محررا إلكترونيا، أو زوّر شيئا من ذلك بطريق الاصطناع، أو التعديل، أو التحوير، أو بأي طريق آخر.
ج) استعمل توقيعا، أو وسيطا، أو محررا إلكترونيا معيبا، أو مزورا مع علمه بذلك.

(ISSN: 2537 - 0758)

د) خالف أيّا من أحكام المادتين (١٩)، (٢١) من هذا القانون.

هـ) توصّل بأية وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر إلكتروني او اخترق هذا الوسيط أو اعترضه أو عطله عن أداء وظيفته، وتكون العقوبة على مخالفة المادة (١٣) من هذا القانون، الغرامة التي لا تقل عن خمسة ألاف جنيه ولا تجاوز خمسين ألف جنيه.

وفي حالة العود تزاد بمقدار المثل المقررة، العقوبة المقررة لهذه الجرائم في حديها الأدنى والأقصى. وفي جميع الأحوال يحكم نشر حكم الإدانة في جريدتين يوميتين واسعتي الانتشار، وعلى شبكات المعلومات الالكترونية المفتوحة على نفقة المحكوم عليه.

كما تناول قانون الطفل المعدل بالقانون رقم ١٢٦ لسنة ٢٠٠٨ في المادة ١١٦ مكرر (أ) منه الاستغلال الجنسي للأطفال عبر شبكة الإنترنت والذي جاء نصها بأن يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن عشرة آلاف جنيه، ولا تجاوز خمسين ألف جنيه كل من استورد أو صدر أو أنتج أو أعد أو عرض أو طبع أو روج أو حاز أو بث أي أعمال إباحية يشارك فيها أطفال أو تتعلق بالاستغلال الجنسي للطفل، ويحكم بمصادرة الأدوات والآلات المستخدمة في ارتكاب الجريمة والأموال المتحصلة منها، وغلق الأماكن محل ارتكابها مدة لا تقل عن ستة أشهر، وذلك كله مع عدم الإخلال بحقوق الغير حسن النية. ومع عدم الإخلال بأي عقوبة أشد ينص عليها في قانون آخر، يعاقب بذات العقوبة كل من:

استخدم الحاسب الآلي، أو الإنترنت، أو شبكات المعلومات، أو الرسوم المتحركة لإعداد، أو لحفظ، أو لمعالجة، أو لعرض، أو لطابعة، أو لنشر، أو لترويج أنشطة، أو أعمال إباحية تتعلق بتحريض الأطفال أو استغلالهم في الدعارة والأعمال الإباحية أو التشهير بهم أو بيعهم.

استخدام الحاسب الآلي، أو الإنترنت، أو شبكات المعلومات، أو الرسوم المتحركة لتحريض الأطفال على الانحراف أو لتسخيرهم في ارتكاب جريمة أو على القيام بأنشطة أو أعمال غير مشروعة أو منافية للآداب، ولو لم تقع الجريمة فعلا.

الوضع بعد صدور قانون رقم ١٧٥ لسنة ٢٠١٨ الخاص بشأن مكافحة جرائم تقنية المعلومات، ولائحته التنفيذية الصادرة بقرار رئيس الوزراء رقم ١٦٩٩ لسنة

٢٠٢٠[١٣]: لا يسعنا القول بمدى تناول تقنين جرائم مكافحة تقنية المعلومات بوجه عام بعد صدور قانون رقم ١٧٥ لسنة ٢٠١٨ الخاص بشأن مكافحة جرائم تقنية المعلومات، ولائحته التنفيذية الصادرة بقرار رئيس الوزراء رقم ١٦٩٩ لسنة ٢٠٢٠. وإن كان ينصب البحث الدراسة على تناول جريمة اختراق الأمن السيبراني بوجه خاص.

المبحث الثاني
المفهوم التقني والطبيعة القانونية لجريمة الاختراق

لاحظنا أثناء هذا الوباء العالمي مدى انتقلنا للتحول الرقمي باستخدام الحاسب الآلي والهواتف الذكية. ولكن الأمر الأكثر غرابة هو الشعور بأن هناك من يساعدنا في أفكارنا، فتتحدث مع أسرتك أو اصدقائك على شيء بداخلك أو يعجبك، فتتفاجئي أثناء استخدام حاسبك أو هاتفك بالرد على السؤال قبل كتابته أو بظهور فيديو يدعم الفكرة أو يحث عليها!! فهل دفعنا ثمن التطور مقابل انتهاك خصوصيتنا؟ وإن كان فهل يعد هذا جريمة اختراق لخدمة هدف تجاري؟ وهل توجد أي أهداف أخرى لجريمة الاختراق منها ما يتعلق بالأمن القومي؟ وهل تنتفي مسئولية مقدم الخدمة أو البرنامج بمجرد موافقتنا على شروط الاستخدام؟

وإن كانت تلك الجريمة تتعدد آثارها وفقا للغرض الذي شرعت من أجله، فمنها ما يقتصر على انتهاك حرمة الحياة الخاصة للأفراد، ومنها ما يتعدى ذلك ليشمل التعدي على أمن الدولة الداخلي أو الخارجي.

ويراد بالجرائم المضرة بأمن الدولة من جهة الداخل تلك الجرائم التي تنطوي على اعتداء على النظام الداخلي للدولة والمساس بالأمن والاستقرار الذي يتمتع به الناس. ومن هنا يتضح أن المصلحة المحمية بهذا التجريم تختلف عن المصلحة في جرائم الاعتداء على أمن الدولة من جهة الخارج. فبينما يهدف هذا التجريم إلى حماية نظام الدولة الداخلي سواء كان اجتماعيًا أم سياسيًا أم اقتصاديًا أم كان يتعلق بنظام الحكم وإلى حماية أمن الناس واستقرارهم، فإن تجريم الاعتداء على أمن الدولة من جهة الخارج يهدف إلى حماية استقلال الدولة وسيادتها. وإن كان الواقع يدل على أن كيان الدولة من جهة الداخل والخارج وحدة واحدة وكلا لا يتجزأ[١٤].

---

[١٣] الجريدة الرسمية– العدد ٣٢ مكرر (ج) نشر بتاريخ أغسطس ٢٠١٨.

[١٤] الجرائم الإرهابية في القانون المصري وفقا للمعايير الدولية، أحمد فتحي سرور، الهيئة المصرية العامة للكتاب، طبعة ٢٠١٨ ص٩.

(ISSN: 2537 - 0758)

وبمحاولة البحث نعرض التعريف التقني والقانوني بجريمة اختراق الأمن السيبراني، ونص تجريمها، وأركانها، وذلك باعتبارها أساس لكل الجرائم المتعلقة بانتهاك الخصوصية، سوء تمثل ذلك انتهاكا لحرية الأفراد أو أمن الدولة الداخلي أو الخارجي.

الجريمة بوجه عام: عُرفت الجريمة من قديم الأزل منذ قتل قابيل أخوه هابيل، وذلك في قول الله تعالى وَاتْلُ عَلَيْهِمْ نَبَأَ ابْنَيْ آَدَمَ بِالْحَقِّ إِذْ قَرَّبَا قُرْبَانًا فَتُقُبِّلَ مِنْ أَحَدِهِمَا وَلَمْ يُتَقَبَّلْ مِنَ الْآَخَرِ قَالَ لَأَقْتُلَنَّكَ قَالَ إِنَّمَا يَتَقَبَّلُ اللَّهُ مِنَ الْمُتَّقِينَ (٢٧) لَئِنْ بَسَطْتَ إِلَيَّ يَدَكَ لِتَقْتُلَنِي مَا أَنَا بِبَاسِطٍ يَدِيَ إِلَيْكَ لِأَقْتُلَكَ إِنِّي أَخَافُ اللَّهَ رَبَّ الْعَالَمِينَ (٢٨) إِنِّي أُرِيدُ أَنْ تَبُوءَ بِإِثْمِي وَإِثْمِكَ فَتَكُونَ مِنْ أَصْحَابِ النَّارِ وَذَلِكَ جَزَاءُ الظَّالِمِينَ (٢٩) فَطَوَّعَتْ لَهُ نَفْسُهُ قَتْلَ أَخِيهِ فَقَتَلَهُ فَأَصْبَحَ مِنَ الْخَاسِرِينَ (٣٠) فَبَعَثَ اللَّهُ غُرَابًا يَبْحَثُ فِي الْأَرْضِ لِيُرِيَهُ كَيْفَ يُوَارِي سَوْءَةَ أَخِيهِ قَالَ يَا وَيْلَتَى أَعَجَزْتُ أَنْ أَكُونَ مِثْلَ هَذَا الْغُرَابِ فَأُوَارِيَ سَوْأَةَ أَخِي فَأَصْبَحَ مِنَ النَّادِمِينَ (٣١) مِنْ أَجْلِ ذَلِكَ كَتَبْنَا عَلَى بَنِي إِسْرَائِيلَ أَنَّهُ مَنْ قَتَلَ نَفْسًا بِغَيْرِ نَفْسٍ أَوْ فَسَادٍ فِي الْأَرْضِ فَكَأَنَّمَا قَتَلَ النَّاسَ جَمِيعًا وَمَنْ أَحْيَاهَا فَكَأَنَّمَا أَحْيَا النَّاسَ جَمِيعًا وَلَقَدْ جَاءَتْهُمْ رُسُلُنَا بِالْبَيِّنَاتِ ثُمَّ إِنَّ كَثِيرًا مِنْهُمْ بَعْدَ ذَلِكَ فِي الْأَرْضِ لَمُسْرِفُونَ (٣٢). سورة المائدة

اختلفت مدارس علم الاجتماع في تعريف الجريمة، وقد أدى هذا الاختلاف إلى ظهور عدد من التعريفات ذات الاتجاه الاجتماعي، ومن أشهرها تعريف سالن Sallin أن الجريمة هي انتهاك للمعايير الاجتماعية. وتأتي شهرة هذا التعريف من كونه جمع كثيرا من الاعتبارات الاجتماعية في عبارة قصيرة، فالعادات والتقاليد والأعراف والقانون كلها معايير اجتماعية، ومن أهم الانتقادات الموجهة إلى هذا التعريف أن المعايير الاجتماعية تختلف من مجتمع إلى آخر، ولعل ذلك هو ما دفع العالم Rafaele Garofalo إلى تصنيف الجرائم إلى جرائم طبيعية وجرائم مصطنعة، الأمر الذي أظهر تعريفSallin، وكأنه تعريف يخص مجتمعا واحدا، فقد قسم جاروفالو الجريمة إلى نوعين جريمة طبيعية، وجريمة مصطنعة.

فالجريمة الطبيعية هي ذلك الفعل الذي لا يختلف شعور الناس تجاهه بأنه جريمة مهما اختلفت المجتمعات والأزمنة، كالاعتداء المادي أو المعنوي على الأفراد، والاعتداء على الأموال والممتلكات.

أما **الجريمة المصطنعة** فهي الأفعال المنتهكة لمكونات ثقافية مصطنعة، أو ما يسمى بالعواطف غير الثابتة كالديانات والعادات والتقاليد.

ولعل نظرية جاروفالو من أكثر النظريات انسجاما مع الواقع الثقافي المعاصر، ذلك أنه لا يمكن بحكم هذا الواقع أن يتم الحصول على تعريف اجتماعي واحد يكون مقبولا تمامًا في كل المجتمعات، أو على الأقل عند كل علماء الاجتماع.

وعلى هذا الأساس فإن النقد الموجه لهذه النظرية من زاوية عدم تشابه عاطفتي الشفقة والأمانة لدى كل المجتمعات، وهو نقد جاء به العالم (Durkheim)، نقد ضعيف لأنه لم يأخذ في الاعتبار أن الشعوب والثقافات، قد لا تتفق على تعريف آخر أكثر من اتفاقها على هذا التعريف في هذا العصر بالذات، ثم أنه يؤخذ على هذا النقد أن العواطف تتشابه لدى كل المجتمعات لكنها لا تتطابق تماما، والأخذ بمسألة واحدة تتشابه عواطف كل الشعوب تجاهها، خير من تركها حتى يتحقق التطابق العاطفي التام.

هناك مبدأ أصيل في القانون المصري، أنه لا جريمة ولا عقوبة إلا بنص قانوني، ومن ثم طالما غاب نص التجريم بالقانون فلا يمكن وصف أي فعل خارج عن تأثيم القانون بوصفه بالجريمة.

وتأسيًا على ذلك تناول الفقه القانوني تعريف الجريمة بأنها هي الواقعة التي ترتكب إضرارًا بمصلحة حماها المشرع ورتب عليها أثرًا جنائيًا متمثلًا في العقوبة.

ويتبين من هذا التعريف أنها واقعة قانونية غير مشروعة، فهى واقعة قانونية نظرًا لأن القانون يرتب عليها أثرًا قانونيًا، وهي غير مشروعة باعتبار أنها تقع بالمخالفة لأوامر المشرع ونواهيه. وأما الضابط الوحيد الذي يصلح للتمييز فهو الأثر القانوني المقرر للجريمة، ألا وهو العقوبة الجنائية[١٥].

قانون العقوبات: هو فرع من فروع القانون تحدد به الدولة الأفعال البشرية المعتبرة جرائم، لما تنطوي عليه من أحداث اضطراب في المجتمع نتيجة لإضرارها أو تهديدها للمصالح العامة للمجتمع أو الأفراد، وتحدد به العقوبات المقررة لمن يرتكب هذه الأفعال[١٦]. كما عرف بأنه مجموعة القواعد القانونية التي تفرضها الدولة لتنظيم التجريم والعقاب، وهو ينطوي على الوقائع التي يمتنع على الأفراد تحقيقها بالتهديد بتوقيع عقوبة معينة كأثر قانوني لمخالفة أوامر المشرع ونواهيه. والوقائع المنهي عنها بواسطة قواعد

[١٥] قانون العقوبات– القسم العام، مأمون محمد سلامة، طبعة ٢٠٢٠ ص١٠١.

[١٦] شرح القواعد العامة لقانون العقوبات، عبد الرؤوف مهدي، طبعة ٢٠١١ ص١٤.

(ISSN: 2537 - 0758)

قانون العقوبات هي التي يطلق عليها الجرائم، بينما الأثر القانوني المترتب على ارتكابها هو العقوبة[١٧].

قانون الإجراءات الجنائية: هو ذلك الفرع من فروع القانون الذي تنظم الدولة بموجبه كيفية مباشرتها لسلطتها في العقاب، أي كيفية تطبيقها لقانون العقوبات[١٨].

العلاقة بين قانون الإجراءات الجنائية وقانون العقوبات: يهدف كلٍ من القانونين إلى حماية الحقوق والحريات التي تعد أساسًا للقواعد الموضوعية، وإذا كان قانون الإجراءات الجنائية يهتم بتنظيم إجراءات الخصومة الجنائية، متوخيًا في ذلك تطبيق قانون العقوبات، لكنه لا يجوز أن نغفل أن الشرعية الدستورية لكلا القانونين تقوم على الحماية التي يوفرها كل منهما للحقوق والحريات التي كفلها الدستور، وأنه بدون وجود قانون الإجراءات الجنائية لن يتم تطبيق قانون العقوبات، باعتبار الأول هو الطريق الواجب اتباعه للانتقال من التجريم للعقاب[١٩].

التعريف التقني لجريمة الاختراق

الاختراق أو ما يطلق عليها عملية القرصنة، هي تقنية اكتشاف الروابط أو الثغرات الضعيفة في أنظمة الحاسوب أو الشبكات واستغلالها للوصول غير المصرح به إلى البيانات أو لتغيير ميزات أنظمة الحاسوب المستهدفة أو الشبكات. ويصف القرصنة التعديل في أجهزة الحاسوب أو البرامج أو الشبكات لتحقيق أهداف معينة لا تتماشى مع أهداف المستخدم. في المقابل، يُطلق عليه أيضًا اختراق أمان شخص ما وسرقة بياناته الشخصية أو السرية مثل أرقام الهواتف وتفاصيل بطاقة الائتمان والعناوين وكلمات المرور المصرفية عبر الإنترنت وإلى ما غير ذلك[٢٠].

وعرف باعتباره التقنية التي يستخدمها الأشخاص، الذين يطلق عليهم مسمى قراصنة، أو متسللين أو مهاجمين، فهم جميعًا متطفلين يحاولون اختراق الشبكات

---

[١٧] قانون العقوبات– القسم العام، مأمون محمد سلامة، طبعة ٢٠٢٠ ص٧.

[١٨] شرح قانون الإجراءات الجنائية، محمود نجيب حسني، الطبعة الرابعة ٢٠١١ الجزء الأول ص٣. شرح القواعد العامة للإجراءات الجنائية، عبد الرؤوف مهدي، طبعة ٢٠٢٠ ص٢٥.

[١٩] الوسيط في قانون الإجراءات الجنائية، أحمد فتحي سرور، الطبعة الحادية عشر ٢٠٢٠ ص١٦.

[20] International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 6 Issue 4 April 2017, Page No. 21042-21050 Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i4.42 Aman Gupta, IJECS Volume 6 Issue 4 April, 2017 Page No. 21042-21050 Page 21042 Ethical Hacking and Hacking Attacks Aman Gupta, Abhineet Anand.

والأنظمة. ويرجع هدف البعض منهم من أجل المتعة أو الربح أو تعطيل العمليات والابتزاز. وذلك مع وجود العامل المشترك لديهم في محاولة الكشف عن ضعف في أي نظام لاستغلاله[٢١].

وعلى الصعيد الآخر عرف البعض الاختراق أو القرصنة على الرغم من أنها قد تستحضر أشكال متعددة من التخريب الإلكتروني والتجسس والضرر التقني، وربطها بخرق القانون بافتراض أن كل من يشارك في أنشطة القرصنة هو مجرم. إلا أن القرصنة قد تتعدى أكثر من ذلك، بوصفها تتعلق باتباع القانون أكثر من خرقه باعتبارها فن حل المشكلات الإبداعي سوء تمثل ذلك في ايجاد حل غير تقليدي للمشكلة أو استغلال الثغرات في البرمجة غير الدقيقة، حيث يتمثل جوهرها في العثور على استخدامات غير مقصودة أو تم التغاضي عنها لقوانين وخصائص حالة معينة، ومن ثم تطبيقها بطرق جديدة ومبتكرة لحل مشكلة ما[٢٢].

ولا سيما يُعد أكبر تحدي لاستخدام التكنولوجيا والذكاء الاصطناعي هو افتقارها للحتمية المطلقة. وإن كان في الغالب يستخدم التطور التكنولوجي في حالة الاستقرار والرخاء، وعلى الرغم من ذلك فإن مدى تقييم صلابة وتفاعل نظام الذكاء الاصطناعي لا يحدث إلا حال وجود الأزمات. ولذلك ينبغي أن يبين الذكاء الاصطناعي مدى فاعلية أداؤه في ظروف الأزمة قبل أن يتم دمجه في خوارزميات لا يمكن أن يتم إيقافه، وانطباق ذات الأمر في التعامل مع بيئة عمل الأسواق ذات السيولة المنخفضة[٢٣].

وفي كلتا الحالتين لا يسعنا القول، إلا بالسؤال عن ماهية الآثار الناتجة عن اختراق الأمن السيبراني والجرائم المتعلقة به؟ سواء تمثل ذلك في أوقات الاستقرار أو الأزمات، وفي كل الأحوال على صعيد الجرائم المتعلقة الناشئة عن حدوثه على صعيد انتهاك حقوق الأفراد أو حقوق الدول ومؤسساتها التي تمثلها.

---

(21) Study Of Ethical Hacking Bhawana Sahare1, Ankit Naik2, Shashikala Khandey, International Journal of Computer Science Trends and Technology (IJCST) Volume 2 Issue 4, Nov-Dec 2014

(22) Hacking- The Art of Exploitation, Jon Erickson, 2nd Edition 2008, p478.

(٢٣) تطورات الاستخدام الاقتصادي للذكاء الاصطناعي، عبد السلام محمد، دار الأهرام للنشر والتوزيع، طبعة ٢٠٢٢، ص٨٧.

(ISSN: 2537 - 0758)

تعريف جريمة الاختراق في التشريع المصري

عرف القانون رقم ١٧٥ لسنة ٢٠١٨ الخاص بشأن مكافحة جرائم تقنية المعلومات في المادة رقم (١) منه، **الاختراق** على أنه 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.

كما عرف **الاعتراض** بأنه مشاهدة البيانات أو المعلومات أو الحصول عليها بغرض التنصت، أو التعطيل، أو التخزين، أو النسخ، أو التسجيل، أو تغيير المحتوى أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه. وذلك لأسباب غير مشروعة ودون وجه حق.

وذلك مع ملاحظة تعريف القانون في ذات المادة **البيانات والمعلومات الإلكترونية** بأنها كل ما يمكن إنشاؤه، أو تخزينه، أو معالجته، أو تخليقه، أو نقله، أو مشاركته، أو نسخه، بواسطة تقنية المعلومات، كالأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور والأصوات، وما في حكمها.

وتقسيم البيانات إلى **بيانات شخصية** وهي أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى. و**بيانات حكومية** وهي 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.

النصوص القانونية لجريمة الاختراق والجرائم المتعلقة بها

تناول قانون ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات الباب الثالث منه الجرائم والعقوبات، حيث خصص الفصل الأول في المواد من ١٢ حتى ٢٢ نص التجريم بكل ما يتعلق بجريمة الاختراق والجرائم المتعلقة بها، ومنها الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات، والانتفاع بدون حق بخدمات الاتصالات والمعلومات وتقنيتها، والدخول غير المشروع، وتجاوز حدود الحق في الدخول، والاعتراض غير المشروع، والاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية، والاعتداء على البريد الإلكتروني أو الموقع أو الحسابات الخاصة، والاعتداء على تصميم الموقع، الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة،

والاعتداء على سلامة الشبكة المعلوماتية، والبرامج والأجهزة والمعدات المستخدمة في ارتكاب جرائم تقنية المعلومات.

كما تناول الفصل الثاني في المادتين ٢٣، ٢٤ الجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات الخاصة بجرائم الاحتيال والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الإلكتروني. وتطرق الفصل الثالث في المادتين ٢٥، ٢٦ الجرائم المتعلقة بالاعتداء على الحياة الخاصة والمحتوى المعلوماتي غير المشروع.

والفصل الرابع والخامس في المواد من ٢٧ إلى ٣٣ الجرائم المرتكبة من مدير الموقع والمسئولية الجنائية لمقدمي الخدمة.

والفصل السادس في المادة ٣٤ الظروف المشددة للجريمة حال إذا وقعت أي جريمة من الجرائم المنصوص عليها في هذا القانون بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر أو الإضرار بالأمن القومي للبلاد، أو بمركزها الاقتصادي، أو منع أو عرقلة ممارسة السلطات العامة لأعمالها أو تعطيل أحكام الدستور أو القوانين أو اللوائح أو الإضرار بالوحدة الوطنية والسلام الاجتماعي، تكون العقوبة السجن المشدد.

والفصل السابع في المواد ٣٥ إلى ٣٧ بشأن المسئولية الجنائية للشخص الاعتباري. والفصل الثامن في المادتين ٣٨، ٣٩ بشأن العقوبات التبعية، والتي تشمل مصادرة الأدوات والآلات والمعدات والأجهزة أو غيرها مما استخدم أو سهل أو ساهم في ارتكابها، كما تعرض لعقوبة الغلق للشخص الاعتباري والعزل حال الإدانة لأحد الموظفين العموميين.

وأخيرًا الفصل التاسع في المادتين ٤٠، ٤١ تعرض لفعل الشروع في الجريمة بالعقاب بنصف الحد الأقصى للعقوبة المقررة للجريمة، والإعفاء قبل بدء التنفيذ الجريمة وكشفها في حالة إبلاغ السلطات العامة أو القضائية، وجواز سلطة المحكمة التقديرية للإعفاء أو تخفيف العقوبة إذا حصل البلاغ بعد كشف الجريمة وقبل التصرف في التحقيق فيها إذا مكن الجاني أو الشريك أثناء التحقيق السلطات المختصة من القبض على مرتكبي الجريمة الآخرين أو ضبط الأموال موضوع الجريمة أو أعان أثناء البحث والتحقيق على كشف الحقيقة فيها أو القبض على مرتكبي جريمة اخرى مماثلة لها في النوع والخطورة. ومراعاة وجوب القضاء برد الأموال المتحصلة من الجرائم المنصوص عليها في هذا القانون.

(ISSN: 2537 - 0758)

أما عن نصوص مواد اللائحة التنفيذية لقانون رقم ١٧٥ لسنة ٢٠١٨ الخاص بشأن مكافحة جرائم تقنية المعلومات، والصادرة بقرار رئيس مجلس الوزراء رقم ١٦٩٩ لسنة ٢٠٢٠، فمن الملاحظ أنها صيغت بمثابة التخصص الفني التقني من مصطلحات التشفير Encryption، ومفتاحه، والبنية التحتية الحرجة، ونظام التحكم الصناعي، وتعريف نقاط الضعف Vulnerabilities، باعتبارها خلل أو ثغرة في نظام التشغيل أو تطبيقات أو شبكات المعلومات أو العمليات أو السياسيات الخاصة بتأمين المعلومات أو في بيئة تقنية المعلومات أو الاتصالات، والتي يمكن استغلالها في عمليات الاختراق أو الهجوم أو الاتلاف أو التجسس أو أي عمل غير مشروع.

وتناولت المادتين ٢، ٣ من اللائحة التنفيذية مدى التزام مقدمو خدمات تقنية المعلومات باتخاذ الإجراءات التقنية والتنظيمية لحماية الأمن السيبراني وتفادي محاولات الاختراق والاعتراض، وذلك من خلال تشفير البيانات والمعلومات بما يحافظ على سريتها، وعدم اختراقها باستخدام نظام تشفير قياسي متماثل أو غير متماثل مع مسئوليته بالحفاظ على سرية وأمان مفتاح التشفير، وتنصيب واستخدام نظم وبرامج ومعدات

مكافحة البرمجيات والهجمات الخبيثة والتأكد من صلاحيتها وتحديثها، واستخدام بروتوكولات آمنة، ووضع صلاحيات بالشبكات والملفات وقواعد البيانات وتحديد المسئولين، لضمان حماية الوصول المنطقي إلى الأصول المعلوماتية والتقنية لمنع الوصول غير المصرح به.

وإعداد قائمة بالأجهزة والمعدات وأرقامها المميزة والمسلسلة وطرازاتها وكذا بيان بالنظم والبرامج والتطبيقات وقواعد البيانات المستخدمة ومواصفاتها، وتطبيق أفضل الممارسات والضوابط عند اختيار مواصفات كلمات السر أو المرور، وتوثيق إجراءات التنصيب والتشغيل الخاصة بالأنظمة، وضمان تنفيذ وتشغيل وصيانة الأنظمة وإلزام الأطراف المتعاقد معها بإبرام اتفاقيات تحدد مستوى تقديم الخدمة مع الجهة وحدود مسئولية كل جهة.

واتخاذ إجراءات التحديثات الخاصة بالنظم والبرامج والتطبيقات بشكل دوري وإتمام الاختبارات اللازمة قبل إجراء التحديثات، وإجراء اختبار سنوي للكشف عن الاختراقات أو المخاطر الأمنية، واستخدام معدات وأجهزة ونظم وبرمجيات الجدران النارية لحماية الشبكات والنظم.

وتناولت المادة ٣ من اللائحة التنفيذية مدى التزام وامتثال مقدمو خدمات تقنية المعلومات والاتصالات التي تمتلك أو تدير أو تشغل البنية التحتية المعلوماتية الحرجة

المخاطبين بأحكام هذا القانون ولائحته، باتخاذ الإجراءات التقنية والتنظيمية من حيث إعداد سياسة أمن معلومات واعتمادها من الإدارة العليا للبنية التحتية المعلوماتية الحرجة وضمان مراجعتها كل عام لضمان استمرار ملائمة وكفاية وفاعلية تلك السياسة، واستخدام شهادات تصديق إلكتروني صادرة من جهة من جهات إصدار شهادات التوقيع الإلكتروني، ومنع الوصول المادي لغير المخول أو المصرح لهم الدخول أو الوصول لمقار وأجهزة ومعدات أنظمة البنية التحتية المعلوماتية الحرجة.

والالتزام باستخدام ضوابط نفاذ قوية وفعالة، وتوثيق إجراءات التنصيب والتشغيل الخاصة بنظم البنية التحتية المعلوماتية الحرجة، وإتاحتها للمستخدمين المخول لهم ذلك عند حاجتهم إليها، وإلزام الموردين بتزويد الجهة بكامل الوثائق الخاصة بالإجراءات التشغيلية، وضمان تنفيذ وتشغيل وصيانة أنظمة البنية التحتية المعلوماتية الحرجة وإلزام الأطراف المتعاقد معها بإبرام اتفاقيات تحدد مستوى تقديم الخدمة مع الجهة.

وإجراء التحديثات الخاصة بالنظم والبرامج والتطبيقات بشكل دوري، ومسح سنوي لأنظمة التحكم الصناعي للكشف عن الثغرات ونقاط الضعف واتخاذ الإجراءات اللازمة للتعامل معها، واختبار سنوي للكشف عن الاختراقات أو المخاطر الأمنية وتثبيت أجهزة المنع والكشف عن الاختراقات، واتخاذ الإجراءات الملائمة للتعامل مع الثغرات الفنية للأجهزة وللنظم والبرامج والتطبيقات عند العلم بها، وأخذ نسخ احتياطية شهرية للبيانات والمعلومات، والاحتفاظ بها وتخزينها مشفرة في موقع آخر، وإعداد قائمة بالأجهزة والمعدات وأرقامها المميزة والمسلسلة وطرازاتها وكذا بيان بالنظم والبرامج والتطبيقات وقواعد البيانات المستخدمة ومواصفاتها.

وتحديد مسئوليات الإدارة العليا ومسئولي تكنولوجيا المعلومات وأمن المعلومات بشكل واضح وصلاحيات وسلطات وواجبات والتزامات كل منهم، مع ضرورة اتساق ذلك مع ما تقوم به غدارات الموارد البشرية وشئون العاملين من إعداد للهياكل، والتوصيف الوظيفي، والأنشطة التدريبية وغيرها من أنشطة وعمليات تلك الإدارات.

وإبلاغ المركز الوطني للاستعداد لطوارئ الحاسب والشبكات بالجهاز عن أي حوادث أو اختراقات فور العلم بحدوثها، ووضع خطة استمرارية العمل والبدائل المقترحة حال حدوث أي أخطار أو أزمات تتعلق بتقديم الخدمة أو انقطاعها، والقدرة على استعادتها.

(ISSN: 2537 - 0758)

أركان جريمة اختراق الأمن السيبراني

الجريمة الإلكترونية هي الجريمة ذات طابع مادي، تتمثل في كل فعل أو سلوك غير مشروع مرتبط بأية جهة أو شكل بالحاسب الآلي وشبكة الإنترنت، مما يتسبب في تحميل أو إمكان تحميل المجنى عليه خسارة، وحصول أو إمكان حصول مرتكبه على أي مكسب. وفي الغالب ما تهدف هذه الجرائم إلى سرقة المعلومات الموجودة في أجهزة الحاسب أو تهدف على نحو غير مباشر إلى الأشخاص والجهات المعنية بتلك المعلومات.

والجريمة من هذا النوع لها مسميات عديدة، منها جرائم الحاسب والإنترنت computer crime جرائم التقنية العالية hi-tech crime الجريمة الإلكترونية e-crime الجريمة السيبرانية Cyber crime جرائم أصحاب الياقات البيضاء white collar، وغالبا ما تكون الاعتداءات على الكيانات المعنوية المتعلقة بقيمتها الاستراتيجية، كمخازن المعلومات، وهذا أهم ما يميز الجرائم الإلكترونية عن غيرها من الجرائم؛ فهى تتعلق بالكيانات المعنوية ذات القيمة المادية أو القيمة المعنوية البحتة أو كليهما معا، وهذا هو أساسها الذي لا يمكن تصور وجود جريمة إلكترونية بدونها، فلولا هذا الأساس لكانت من الجرائم العادية التي تخضع للقانون الجنائي التقليدي. إضافةً إلى هذا فهى تتكون من أساسين هما عناصر الجريمة والسلوك ووصفه الإجرامي، والنص القانوني على تجريم السلوك وإيقاع العقوبة، والذي يعد من أساسيات الجرائم العادية.

ولم يقم المصري بوضع تشريع فاصل ومحدد للجريمة بوجه عام، ولكن اكتفى بإيضاح تعريفها من خلال تقسيمها من حيث نوعها وعقوبتها. وترك الأمر للفقه خوفًا من أن يضع تعريفًا للجريمة لا يشمل كافة النشاط الإجرامي.

حيث عرفها الفقيه فرانسوا كرارا الجريمة، بأنها كل عمل خارجي لا يبرره استعمال حق أو أداء واجب يقوم به الإنسان مخالفًا بذلك قانونًا للدولة يعاقب عليه. كما عرفها جارو، بأنها فعل أي حركة جسمانية تهدف إلى إحداث تغيير في العالم الملموس. وعرفها كوشى، بأنها كل عمل أو امتناع يحظره القانون ويفرض له عقاب.

ولا ننسى بأن هناك مبدأ أصيل فى القانون المصري، أنه لا جريمة ولا عقوبة إلا بنص قانوني، ومن ثم طالما غاب نص التجريم بالقانون فلا يمكن وصف أي فعل خارج عن تأثيم القانون بوصفه بالجريمة.

وتأسيًا على ذلك تناول الفقه القانوني تعريف **الجريمة** بأنها هي الواقعة التي ترتكب إضرارًا بمصلحة حماها المشرع ورتب عليها أثرًا جنائيًا متمثلًا في العقوبة. ويتبين من هذا التعريف أنها واقعة قانونية غير مشروعة، فهى واقعة قانونية نظرًا لأن القانون يرتب عليها أثرًا قانونيًا، وهي غير مشروعة باعتبار أنها تقع بالمخالفة لأوامر المشرع ونواهيه. وأما الضابط الوحيد الذي يصلح للتمييز فهو الأثر القانوني المقرر للجريمة، ألا وهو العقوبة الجنائية[٢٤].

وعرفت بأنها فعل غير مشروع صادر عن إرادة جنائية يقدر له القانون عقوبة أو تدبيرًا احترازيًا[٢٥]. كما عرفت بأنها نوع من السلوك البشري، يفصله قانون العقوبات عن مجموع الأنشطة البشرية لإهداره أو تهديده مصلحة للمجتمع يراها جديرة بالحماية، فيحظر اتيانه ويقرر لمن يرتكبه عقابًا[٢٦].

وتنازع الفقه في تعريف الجريمة من الناحية القانونية إلى اتجاهين، أحدهما المادي والآخر شخصي. حيث يهتم الاتجاه المادي بالفعل المادي، أما الاتجاه الشخصي فأنه يقيس الجريمة بالنظر إلى الإرادة الآثمة لمرتكبها ومدى خطورة صاحبها على المجتمع. وفي واقع الأمر يلاحظ أن الجريمة لا تقوم بغير فعل مادي وإرادة آثمة، فلا تقوم الجريمة بغيرهما معا. فالجريمة ليست محض فعل مادي مخالف للقانون، وإنما هي تجمع بين الاثنين ولا قيام لها بدونهما[٢٧].

وتأسيًا على ما سبق يتحقق الركن المادي لجريمة الاختراق على سلوك مادي قوامه تصدي الجاني لأية معلومة أو بيانات أو كل ما هو متداول عن طريق شبكة المعلومات أو أحد أجهزة الحاسب الآلي وما في حكمها، حيث يتم الاختراق أو الاعتراض باستخدام وسائل فنية تمكن الجاني من خلالها بالتجسس المعلوماتي من خلال مشاهدة البيانات أو

---

[٢٤] قانون العقوبات القسم العام، مأمون محمد سلامة، طبعة ٢٠٢٠ ص١٠١.

[٢٥] شرح قانون العقوبات القسم العام، محمود نجيب حسني، دار المطبوعات الجامعية، طبعة ٢٠١٨ ص٤٥.

[٢٦] شرح القواعد العامة لقانون العقوبات، عبد الرؤوف مهدي، دار النهضة العربية، طبعة ٢٠١١ ص٣٣٢.

[٢٧] الوسيط في قانون العقوبات القسم العام، أحمد فتحي سرور، دار الأهرام للنشر والتوزيع والإصدارات القانونية، طبعة ٢٠٢٠ ص٣١٣.

(ISSN: 2537 - 0758)

المعلومان أو التصنت أو التحكم أو مراقبة ما هو متداول من خلال الولوج داخل النظام واستخدامه بشكل مباشر أو غير مباشر.

أما عن الركن المعنوي لجريمة الاختراق، فلا ينفك أن يتماثل مع الركن المعنوي للجرائم العمدية. والتي يقوم ركنها المعنوي على القصد الجنائي العام المتحقق بعنصريه وهما العلم والإرادة. وذلك بعلمه بأن ما يقوم به يعد اختراق بدون وجه حق لأي بيانات أو معلومات، وبالرغم من هذا العلم المتحقق تتجه إرادته إلى إتيان هذا السلوك المادي المكون للجريمة طوعيًة.

تطبيقات قضائية للجرائم الناشئة عن اختراق الأمن السيبراني

المادة ٢٥ من القانون ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات. مفادها؟ المرجع في تعرف حقيقة المعلومات والأخبار ومدى تعلقها بالحياة الخاصة للمجني عليه وانتهاكها لخصوصيته دون رضاه. موضوعي. حد ذلك؟ تحري حقيقة الأخبار ومدى تعلقها بالحياة الخاصة للمجني عليه. تكييف قانوني يخضع لرقابة محكمة النقض. علة ذلك؟ عدم تضمن المنشور المنسوب إلى الطاعن كتابته ووضعه على موقع الفيس بوك ما من شأنه أن يمس الحياة الخاصة للمجني عليه أو ينتهك خصوصيته دون رضاه ومصادفته واقعة حرر بشأنها محضر. أثره: عدم تأثيمه بالمادة ٢٥ من القانون ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات. مخالفة الحكم هذا النظر. خطأ في تطبيق القانون. يوجب نقضه والقضاء بالبراءة[٢٨].

---

[٢٨] الطعن رقم ١٥٨٠٢ لسنة ٩٠ القضائية الدوائر الجنائية جلسة الثلاثاء الموافق ٨ يونية سنة ٢٠٢١. لما كان الحكم الابتدائي المؤيد لأسبابه بالحكم المطعون فيه أنه حصَّل واقعة الدعوى بما مفاده أن المجني عليه تقدم ببلاغ للإدارة العامة لتكنولوجيا المعلومات – فرع.... يتضرر من القائم على إدارة الحساب الشخصي على موقع الفيس بوك المسمى ".... " لقيامه بعمل مشاركات تتضمن عبارات من شأنها الإساءة لسمعته والتشهير به، والذي تبين من التحريات أنه مفعل عن طريق الهاتف المحمول رقم.... المسجل باسم/.... وأنه مرتكب الواقعة محل الفحص، وباستجوابه أقر بارتكابه الواقعة بقصد توثيق واقعة تعدي الشاكي على والده بقاعة المحكمة لخلافات بينهما، وبمطالعة المحكمة للصورة الضوئية المرفقة بالمحضر لصفحة الفيس بوك تبين وجود المنشور محل الواقعة ونصه (المتهم.... يتعدى على الأستاذ/.... المحامي بقاعة جلسة الجنح المستأنفة.... في وجود جمهور المتقاضين والمحامين وغياب أمن المحكمة شير وأنا أحد شهود الواقعة). لما كان ذلك، وكانت المادة ٢٥ من القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات والتي دين الطاعن بمقتضاها قد نصت على أن: (يُعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من اعتدى على أي من المبادئ أو القيم الأسرية

لما كانت جناية التهديد المنصوص عليها في الفقرة الأولى من المادة ٣٢٧ من قانون العقوبات تتوافر إذا وقع التهديد كتابة بارتكاب جريمة ضد النفس أو المال، وكان التهديد مصحوباً بطلب أو تكليف بأمر وكان الحكم قد أورد بأسبابه قيام الطاعن بتهديد المجني عليهما عبر مواقع التواصل الاجتماعي، وتمكن من خدعاهما وتحصل منهما على صور ومقاطع مرئية في أوضاع مخلة بالحياء وهددهما بنشرها، وإذ كان مصطلح الكتابة قد ورد في المادة ٣٢٧ سالفة الذكر على سبيل البيان في صيغة عامة لتشمل كافة وسائل الكتابة المختلفة سواء كانت بالطرق التقليدية أو بإحدى الوسائل الإلكترونية الحديثة، فإذا أثبت الحكم على الطاعن إرساله عبارات التهديد عن طريق الوسائط الإلكترونية الحديثة– وهي لوحة المفاتيح– بقصد إيقاع الخوف في نفس المجني عليهما لحملهما على أداء ما هو مطلوب، فإنه يكون قد استظهر أركان جريمة التهديد كما هي معرفة به في القانون، ويضحى منعى الطاعن في هذا الشأن على غير أساس[٢٩].

في المجتمع المصري أو انتهك حرمة الحياة الخاصة، أو أرسل بكثافة العديد من الرسائل الالكترونية لشخص معين دون موافقته، أو منح بيانات شخصيته إلى نظام أو موقع الكتروني لترويج السلع والخدمات دون موافقته، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخباراً أو صوراً وما في حكمها تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة)، وكان من المقرر أنه وإن كان المرجع في تعرف حقيقة المعلومات والأخبار ومدى تعلقها بالحياة الخاصة للمجني عليه وانتهاكها لخصوصيته دون رضاه هو بما يطمئن إليه قاضي الموضوع في تحصيله لفهم الواقع في الدعوى، إلا أن حد ذلك ألا يخطئ في تطبيق القانون على الواقعة كما صار إثباتها في الحكم أو يمنح دلالة للمعلومات والأخبار بما يحيلها عن معناها، كما أن تحري حقيقة تلك الأخبار ومدى تعلقها بالحياة الخاصة للمجني عليه هو من التكييف القانوني الذي يخضع لرقابة محكمة النقض باعتبارها الجهة التي تهيمن على الاستخلاص المنطقي الذي يتأذى إليه الحكم من مقوماته المسلمة. لما كان ذلك، وكان ما تضمنه المنشور المنسوب إلى الطاعن كتابته ووضعه على موقع الفيس بوك فضلاً عن أنه– وعلى ما يبين من المفردات المضمومة– قد صادف واقعة حرر بشأنها محضر من والد الطاعن ضد المجني عليه، ليس من شأنه أن يمس الحياة الخاصة للمجني عليه أو ينتهك خصوصيتها دون رضاه، ومن ثم فهو لا يقع تحت نص المادة ٢٥ من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، فإن الحكم المطعون فيه وقد خالف هذا النظر وقضى بمعاقبة الطاعن عن تلك الجريمة ودانه بمقتضاها يكون قد بني على خطأ في تأويل القانون، مما يتعين معه على المحكمة نقض الحكم المطعون بالنسبة لتلك التهمة، والقضاء ببراءة الطاعن منها عملاً بالمادة ٣٠٤ من قانون الإجراءات الجنائية.

[٢٩] طعن رقم ٢٢٦٢٠ لسنة ٨٨ قضائية الدائرة الجنائية جلسة ٩ من يوليه سنة ٢٠٢٠ المكتب الفني ص١١٨. من حيث إن الطاعن ينعى على الحكم المطعون فيه أنه إذ دانه بجرائم التهديد بإفشاء أمور

(ISSN: 2537 - 0758)

خادشه بالشرف والحياء بنشر مقاطع مرئية مسجلة عبر مواقع التواصل الاجتماعي واستعمالها في غير علانية والاعتداء على حرمة الحياة الخاصة للمجني عليهما وتعمد إزعاج الغير باستخدام إحدى وسائل الاتصالات قد شابه القصور في التسبيب والفساد في الاستدلال وانطوى على إخلال بحق الدفاع ذلك أنه خلا من بيان واقعة الدعوى بياناً تتحقق به أركان الجرائم التي دانه بها والظروف التي وقعت فيها، وقضى بمعاقبته رغم عدم توافر الركن المادي والمعنوي لجريمة التهديد الآثمة بالمادة ٣٢٧ من قانون العقوبات سيما وأن المجني عليهما قاما بإرسال مقاطع الفيديو بإرادتهما كما دفع ببطلان الاعتراف المنسوب للطاعن لأنه وليد إكراه مادي ومعنوي، وببطلان تفتيش الهاتف الشخصي لشقيق الطاعن لتجاوز القائم به الغرض المخصص بالإذن إلا أن الحكم رد على الدفعين بما لا يسوغ، وأخيراً فإن المحكمة قضت بإلزامه بالدعوى المدنية رغم عدم إعلانه بها وسداد الرسم المقرر لها مما يعيب الحكم ويستوجب نقضه.

وحيث إن الحكم المطعون فيه بين واقعة الدعوى بما تتوافر به كافة العناصر القانونية للجرائم التي دان الطاعن بها وأقام على ثبوتها في حقه أدلة سائغة من شأنها أن تؤدي إلى ما رتبه الحكم عليها مستمدة من أقوال شهود الإثبات وما ثبت بالتقرير الفني لإدارة مكافحة جرائم المعلومات. لما كان ذلك، وكان من المقرر أن القانون لم يرسم شكلاً خاصاً يصوغ فيه الحكم بيان الواقعة المستوجبة للعقوبة والظروف التي وقعت فيها، فمتى كان مجموع ما أورده الحكم – كما هو الحال في الدعوى المطروحة – كافياً في تفهم الواقعة بأركانها وظروفها حسبما استخلصته المحكمة كان ذلك محققاً لحكم القانون ويكون منعي الطاعن بقالة القصور غير سديد. لما كان ذلك، وكانت جناية التهديد المنصوص عليها في الفقرة الأولى من المادة ٣٢٧ من قانون العقوبات تتوافر إذا وقع التهديد كتابة بارتكاب جريمة ضد النفس أو المال وكان التهديد مصحوباً بطلب أو تكليف بأمر، وكان الحكم قد أورد بأسبابه قيام الطاعن بتهديد المجني عليهما عبر مواقع التواصل الاجتماعي وتمكن من خدعاهما وتحصل منهما على صور ومقاطع مرئية في أوضاع مخلة بالحياء وهددهما بنشرها وإذ كان مصطلح الكتابة قد ورد في المادة ٣٢٧ سالفة الذكر على سبيل البيان في صيغة عامة لتشمل كافة وسائل الكتابة المختلفة سواء كانت بالطرق التقليدية أو بإحدى الوسائل الإلكترونية الحديثة فإذا أثبت الحكم على الطاعن إرساله عبارات التهديد عن طريق الوسائط الإلكترونية الحديثة– وهي لوحة المفاتيح– بقصد إيقاع الخوف في نفس المجني عليهن لحملهن على أداء ما هو مطلوب فإنه يكون قد استظهر أركان جريمة التهديد كما هي معرفة به في القانون ويضحى منعى الطاعن في هذا الشأن على غير أساس. لما كان ذلك، وكان من المقرر أن القصد الجنائي في جريمة التهديد يتوافر متى ثبت للمحكمة أن الجاني ارتكب التهديد وهو يدرك أثره من حيث إيقاع الرعب في نفس المجني عليه وأنه يريد تحقيق ذلك الأثر بما قد يترتب عليه من أن يذعن راغماً إلى إجابة الطلب، ولا يلزم التحدث استقلالاً عن هذا الركن بل يكفي أن يكون مفهوماً من عبارات الحكم وصراحة عبارات التهديد وظروف الواقعة كما أوردها ومن ثم يكون النعي بالقصور في هذا الشأن على غير أساس. لما كان ذلك، وكانت المادة سالفة الذكر إذ لم توجب بصيغتها العامة أن تكون عبارات التهديد دالة بذاتها على أن الجاني سوف يقوم بارتكاب الجريمة إذا لم يجب إلى طلبه بل يكفي أن يكون الجاني

قد وجه التهديد كتابة إلى المجني عليه وهو يدرك أثره من حيث إيقاع الرعب في نفسه وأنه يريد تحقيق ذلك الأثر بما قد يترتب عليه أن يذعن المجني عليه راغماً إلى إجابة الطلب، فإذا كانت المحكمة قد استخلصت من عبارات التهديد وظروف الواقعة وملابساتها أن الطاعن رمي إلى إثارة الرعب والفزع في نفس المجني عليهما وهو ما حملهما على إرسال صور ومقاطع الفيديو لهما في أوضاع مخله بالحياء والشرف بما يعدم إرادتهما حين أرسلا تلك الصور ومقاطع الفيديو ومن ثم يكون النعي في هذا الصدد في غير محله. لما كان ذلك، وكان الاعتراف في المسائل الجنائية من عناصر الاستدلال التي تملك محكمة الموضوع كامل الحرية في تقدير صحتها وقيمتها في الإثبات ولها أن تأخذ به متى اطمأنت إلى صدقه ومطابقته للحقيقة والوقع كما أن لها أن تقدر عدم صحة ما يدعيه المتهم من أن الاعتراف المعزو إليه انتزع منه بطريق الإكراه أو صدر منه على أثر إجراء باطل بغير معقب عليها ما دامت تقيم تقديرها على أسباب سائغة وكانت المحكمة قد خلصت في استدلال سائغ إلى سلامة الدليل المستمد من اعتراف الطاعن أمام النيابة لما ارتأته من مطابقته للحقيقة والواقع الذي أظهرته من باقي عناصر الدعوى وأدلتها ومن خلوه مما يشوبه وصدوره عن طواعية واختيار فإن ما يثيره الطاعن من مجادلة في هذا الشأن ينحل إلى جدل موضوعي في سلطة المحكمة في تقدير الأدلة مما لا يجوز الخوض فيه أمام محكمة النقض. لما كان ذلك، وكان الحكم قد عرض لدفاع الطاعن بتجاوز الضابط للإذن واطرحه في قوله: (وكان الثابت بالأوراق صدور إذناً من النيابة العامة بالتفتيش لمسكن المتحري عنه شقيق المتهم– ذات مسكن المتهم– ونفاذاً لذلك الإذن توجه ضابط الواقعة إلى مسكن المأذون بتفتيشه وتقابل مع المتهم ووالدته وحال تفتيش المسكن عثر على هاتف محمول ماركة (infinix) متصل بشبكة الانترنت هوائياً عن طريق رواتر متصل بخط التليفون الأرضي رقم "....." وبفحص الهاتف مبدئياً تبين أنه يفتح تلقائياً على الحساب محل الواقعة المسمى (.....) وأقر له المتهم بأنه خاص به وأنه هو منشئ ذلك الحساب وأدلى له ببيانات البريد الإلكتروني وكلمة المرور الخاصين به وعثر على المحادثات والصور والمقاطع المرئية المسجلة بمحل الواقعة فتم اصطحابه للقسم لتحرير محضر بالواقعة وكانت المحكمة تطمئن إلى شهادة ضابط الواقعة وصحة ما أدلى به ومن ثم يكون ما أتاه ضابط الواقعة من إجراءات تفتيش وضبط تمت وفقاً لصحيح القانون وفي حدود إذن النيابة العامة الصادر له، ويضحى بالتالي الدليل المستمد من تلك الإجراءات صحيحاً، وتعول عليه المحكمة كدليل صحيح في الدعوى مع باقي الأدلة فيها، إذ أن الأدلة في المواد الجنائية متساندة يكمل بعضها بعضاً ومنها مجتمعة تتكون عقيدة القاضي فلا ينظر إلى دليل بعينه لمناقشته على حدة دون باقي الأدلة بل يكفي أن تكون الأدلة في مجموعها كوحدة مؤدية إلى ما قصده الحكم منها ومنتجة في اكتمال اقتناع المحكمة واطمئنانها إلى ما انتهت إليه الأمر الذي يضحى معه هذا الدفع في غير محله لقيامه على سند صحيح من الواقع والقانون والمحكمة تلتفت عنه). وكان الحكم قد رد عليه رداً كافياً ويستقيم به اطراحه، وكان من المقرر أن الأمر الذي تصدره النيابة العامة بتفتيش شخص معين ومن قد يكون موجوداً معه وقت التفتيش على مظنة اشتراكه معه في الجريمة التي صدر أمر التفتيش من أجلها يكون صحيحاً في القانون، وكان الثابت من مدونات الحكم المطعون فيه أن الأمر الصادر من النيابة العامة بضبط وتفتيش شخص ومسكن

(ISSN: 2537 - 0758)

من المقرر أن الإزعاج وفقاً لنص المادة ١٦٦ مكرراً من قانون العقوبات لا يقتصر على السب والقذف، لأن المشرع قد عالجها بالمادة ٣٠٨ مكرراً بل يتسع لكل قول أو فعل تعمده الجاني يضيق به صدر المواطن، وكان البيّن من مطالعة مدونات الحكم المطعون فيه أن محكمة الموضوع قد اطمأنت إلى قيام الطاعنة باستخدام خط ال ADSL المتصل بهاتف شقيقتها في إرسال الرسالتين اللتين تضمنتا عبارات تنطوي على سب المجني عليه ومضايقته وهي عبارات شائنة وألفاظ تخدش الاعتبار وتم توجيهها عن طريق البريد الإلكتروني الذي توافر باستخدامه ركن العلانية وقصد من توجيهها خدش اعتبار المجني عليه وهذه العبارات الشائنة بذاتها تزعج أي إنسان ويضيق بها صدر أي شخص، وإذ تعمدت الطاعنة إتيان ذلك الفعل واتجهت إرادتها إلى إزعاج المجني عليه مما أرسلته من تلك العبارات الجارحة الأمر الذي يتحقق به أركان الجريمة موضوع الدعوى، ويضحى ما تنعاه الطاعنة في هذا المنحى غير مقبول[٣٠].

المتحري عنه شقيق الطاعن وهو ذات مسكن الأخير قد تضمن سريانه على من يتواجد معه بالمسكن، فإن التفتيش الواقع تنفيذاً له يكون ولا مخالفة فيه للقانون ويكون أخذه بنتيجته صحيحاً ولا يصح الطعن عليه بأن ما تم فيه تجاوز للأمر الصادر لمأمور الضبط ما دام هو لم يقم بأي عمل إيجابي بقصد البحث عن جريمة أخرى غير التي صدر من أجلها الأمر، فمن البداهة أن الإجراء المشروع لا يتولد عن تنفيذه في حدوده عمل باطل وكان ما أورده الحكم رداً على ما دفع به الطاعن من بطلان القبض والتفتيش كافياً وسائغاً في الرد ويتفق وصحيح القانون فإن ما يثيره الطاعن في هذا الوجه ينحل إلى جدل موضوعي لا يجوز إثارته أمام محكمة النقض. لما كان ذلك، وكان يبين من الحكم المطعون فيه أنه قد أثبت به أنه تم إعلان الطاعن بالدعوى المدنية في المواجهة وإذ كانت ورقة الحكم تعتبر متممة لمحضر الجلسة في شأن إثبات إجراءات المحاكمة وكان الأصل في الإجراءات أنها روعي، ومتى أثبت الحكم إعلان الطاعن بالدعوى المدنية في المواجهة فلا يجوز للطاعن أن يجحد ما أثبته الحكم من تمام هذا الإجراء إلا بالطعن بالتزوير وهو ما لم يفعله، فإن النعي على الحكم بدعوى البطلان لا يكون له محل. لما كان ذلك، وكان عدم سداد رسم الدعوى المدنية- بفرض صحته- لا يتعلق بإجراءات المحاكمة من حيث صحتها أو بطلانها ومن ثم فإن ما ينعاه الطاعن في هذا الشأن يكون غير سديد. لما كان ما تقدم، فإن الطعن برمته يكون على غير أساس متعيناً رفضه موضوعاً.

[٣٠] طعن رقم ٣٩١٤٤ لسنة ٨٥ قضائية الدوائر الجنائية جلسة ٢١ مايو ٢٠٢١ المكتب الفني سنة ٦٧ قاعدة ٦٣ صفحة ٥٦٠. لما كان الحكم الابتدائي المؤيد لأسبابه والمكمل بالحكم المطعون فيه قد بيّن واقعة الدعوى بما تتوافر به كافة العناصر القانونية للجريمة التي دان الطاعنة بها وأورد على ثبوتها في حقها أدلة استمدها من أقوال المجني عليه، ومما ثبت من تقرير الفحص الفني وما قدم من مستندات وأورد مؤداها في بيان كاف يتفق ويواءم مع ما أورده في بيانه لواقعة الدعوى، وهي أدلة سائغة من شأنها أن تؤدي إلى ما رتبه الحكم عليها. لما كان ذلك، وكان من المقرر أن القانون لم يرسم شكلاً خاصاً

يصوغ فيه الحكم بيان الواقعة المستوجبة للعقوبة والظروف التي وقعت فيها فمتى كان مجموع ما أورده كافياً في تفهم الواقعة بأركانها وظروفها حسبما استخلصته المحكمة– كما هو الحال في الدعوى المطروحة– فإنه ينحسر عن الحكم قاله القصور. ومن المقرر أن الإزعاج وفقاً لنص المادة ١٦٦ مكرراً من قانون العقوبات لا يقتصر على السب والقذف ؛ لأن المشرع قد عالجها بالمادة ٣٠٨ مكرراً بل يتسع لكل قول أو فعل تعمده الجاني يضيق به صدر المواطن، وكان البيّن من مطالعة مدونات الحكم المطعون فيه أن محكمة الموضوع قد اطمأنت إلى قيام الطاعنة باستخدام خط الـ ADSL المتصل بهاتف شقيقتها في إرسال الرسالتين اللتين تضمنتا عبارات تنطوي على سب المجني عليه ومضايقته وهي عبارات شائنة وألفاظ تخدش الاعتبار وتم توجيهها عن طريق البريد الإلكتروني الذي توافر باستخدامه ركن العلانية وقصد من توجيهها خدش اعتبار المجني عليه وهذه العبارات الشائنة بذاتها تزعج أي إنسان ويضيق بها صدر أي شخص، وإذ تعمدت الطاعنة إتيان ذلك الفعل واتجهت إرادتها إلى إزعاج المجني عليه مما أرسلته من تلك العبارات الجارحة الأمر الذي يتحقق به أركان الجريمة موضوع الدعوى، ويضحى ما تنعاه الطاعنة في هذا المنحى غير مقبول. و لما كان ما تثيره الطاعنة من قيامها بجحد صور الرسائل محل الاتهام، فإن ذلك مردود بأن ما جاء في القانون من حجية المحررات وإثبات صحتها إنما محله أحكام الإثبات في المواد المدنية والتجارية حيث عينت أدلة ووضعت أحكاماً لها وألزم القاضي بأن يجرى في أحكامه على مقتضاها، وليس في القانون ما يجبر المحاكم الجنائية على ترسمه ؛ لأنها في الأصل حرة في انتهاج السبيل الموصل لاقتناعها ولم يرسم القانون في المواد الجنائية طريقاً خاصاً يسلكه القاضي في تحري الأدلة، وكانت أوجه الدفاع المبينة بوجه الطعن في هذا الشأن من أوجه الدفاع القانونية الظاهرة البطلان مما لا تلتزم محكمة الموضوع أصلاً بالرد عليها ولا يعتبر سكوتها عنها إخلالاً بحق الدفاع ولا قصوراً في حكمها، ومن ثم فإن ما تثيره الطاعنة في هذا الصدد يكون غير سديد. لما كان الحكم المطعون فيه قد رد على دفاع الطاعنة القائم على التمسك بالحق في الشكوى كسبب من أسباب الإباحة في قوله ".... أن ذلك مردود بأن حق الشكوى لا يمكن أن يمتد بحال من الأحوال إلى ارتكاب الجرائم كما أن هذا الحق مكفول للكافة إذا ما كان تقديم الشكوى إلى الجهات المختصة التي خصها القانون بتلقي الشكاوى والتبليغات وفحص واتخاذ اللازم قانوناً حيالها". وهو رد سائغ يتفق مع صريح نص القانون، ويضحى ما تثيره في هذا الخصوص غير سديد. وكانت محكمة الموضوع قد اطمأنت إلى أقوال المدعي بالحق المدني وصحة تصويره للواقعة، فإنه لا محل للنعي على المحكمة عدم إجابتها طلب التصريح للطاعنة باستخراج المستندات الواردة بمذكرة أسبابها ما دام أن هذا الطلب لا يتجه إلى نفي الفعل المكون للجريمة ولا إلى إثبات استحالة حصول الواقعة بل المقصود منه إثارة الشبهة في الدليل الذي اطمأنت إليه المحكمة، مما يعد دفاعاً موضوعياً لا تلتزم المحكمة بإجابته.

(ISSN: 2537 - 0758)

إن جريمة استعمال أجهزة الاتصالات لا تقتصر على الازعاج فقط. اتساعها لكل قول أو فعل تعمده الجاني يضيق به صدر المواطن، وأياً كان نوع أجهزة الاتصالات المستعملة أو الوسيلة المستخدمة[٣١].

إرشادات تقنية لمواجهة اختراق الأمن السيبراني[٣٢]

- استخدام جدار حماية للأجهزة أو البرامج التي تمنع المتسللين من الوصول إلى بياناتك الشخصية أو بيانات شركتك.
- استخدام برامج مكافحة الفيروسات لفحص أجهزة الحاسب الآلي/ اللوح أو الهاتف الذكي من البرامج الضارة وحذفها.
- استخدام أحدث البرامج وتصحيحات/تحديثات الأمان.
- تأمين مستعرض صفحات الويب ونظام التشغيل.
- الاتصال بشبكة لاسلكية محددة عن طريق معرِّف الشبكة.
- SSID استخدام تعطيل البث.

يضيف حاجز إضافي لاكتشاف الشبكة ويوفر حد أدنى من الأمان.

- تشفير الاتصال اللاسلكي.

تمكين أمان الشبكة اللاسلكية واستخدام ميزة التشفير .WPA2

- Wi-fi مراعاة عدم الاتصال من نقطة اتصال عامة.

موقع عام لتصفح الإنترنت، ويفضل ألا يتم الوصول إليه/ مشاركة أي معلومات شخصية حساسة من خلاله.

- (VPN) استخدام شبكة افتراضية خاصة مشفرة

اتصال مشفر بين جهاز الحاسب الآلي وجهاز خادم. VPN لمنع اعتراض البيانات

- استخدام مدير كلمات المرور ببرنامج أو خدمة تقوم بتخزين كلمات المرور المختلفة والمعقدة وتشفيرها للاستخدام عبر حسابات على الإنترنت.
- إنشاء كلمات مرور غير كلمات القاموس أو الأسماء الموجودة في أي لغة/ ولا الكلمات المشتملة على أخطاء إملائية شائعة/ ولا تستخدم أسماء أجهزة الحاسوب أو أسماء الحسابات. ويفضل استخدم الأحرف الخاصة إن أمكن، وكلمة مرور مكونة من عشرة أحرف على الأقل.

---

[٣١] طعن رقم ٢٢٨٤ لسنة ٨٩ قضائية الدوائر الجنائية جلسة ١٠ يونية ٢٠٢٠.

[32] Cisco introduction to cybersecurity course, May 2021.

- التشفير بتحويل المعلومات إلى صيغة يتعذر على أي طرف غير مصرح له قراءتها النسخ الاحتياطي للبيانات. وذلك يمنع فقدان البيانات غير القابلة للاستبدال من خلال حل التخزين الداخلي.
- جعل الملفات غير قابلة للاسترداد بتدمير محرك الأقراص الثابت أو جهاز التخزين بشكل مادي.
- تفعيل المصادقة ثنائية العامل بالإضافة إلى اسم المستخدم وكلمة المرور، فتوجد متطلبات لرموز أخرى، مثل بطاقة الائتمان أو رقم الهاتف، للتحقق من بيانات اعتماد المستخدم.
- التصفح الآمن عن طريق الترخيص المفتوح، وهو بروتوكول معياري مفتوح يسمح للمستخدم النهائي بالوصول إلى التطبيقات الخارجية دون الكشف عن كلمة مرور المستخدم، Microsoft Internet Explorer: InPrivate و Google Chrome: Incognito و Mozilla Firefox: صفحة فرعية خاصة/ النوافذ الخاصة و Safari: Private: التصفح الخاص

جميعها أساليب للحفاظ على خصوصية محفوظات الاستعراض عن طريق تعطيل ملفات تعريف الارتباط تلقائيًا وحذف ملفات الإنترنت المؤقتة وإزالة محفوظات الاستعراض بعد غلق النافذة أو البرنامج.

الخاتمة

تناول البحث التعريف بالأمن السيبراني أهميته ومميزاته والتهديدات التي يتعرض لها، وبيان ماهية الجريمة الإلكترونية وبوجه خاص التعرف على جريمة الاختراق من الناحية التقنية والطبيعة القانونية. وذلك مع إيضاح كيفية تصدي المشرع المصري لهذه الجريمة وبيان نص التجريم والعقاب وتوافر أركانها.

وما يترتب على حدوث تلك الجريمة من آثار عملية هامة، تتمثل في انتهاك حقوق الأفراد بما يشمل جرائم الاعتداء على حرمة الحياة الخاصة والتي يندرج منها جرائم استراق السمع أو نقله أو تسجيله، التقاط أو نقل صورة شخص، إذاعة أو استعمال تسجيل أو مستند أو التهديد بالإفشاء بمحتوياته، ربط معطيات شخصية للغير بمحتوى مناف للآداب العامة، الدخول غير المشروع أو الدخول بالخطأ والبقاء بدون وجه حق على موقع أو حساب خاص أو نظام معلوماتي، الاحتيال والاعتداء على بطاقات البنوك

(ISSN: 2537 - 0758)

وأدوات الدفع الإلكترونية الخاصة بالأفراد، اصطناع ونسبة موقع بريد إلكتروني أو حساب خاص لشخص طبيعي.

أو ما يعد انتهاكًا لحقوق الدولة أو إحدى ومؤسساتها بما يشمل جرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة والتي يندرج منها جرائم الاعتداء على سلامة الشبكات المعلوماتية، اصطناع ونسبة موقع بريد إلكتروني أو حساب خاص لشخص اعتباري، إدارة أو استخدام موقع أو حساب خاص بهدف ارتكاب أو تسهيل ارتكاب جريمة، الاعتداء على بطاقات البنوك وأدوات الدفع الإلكترونية الخاصة بمؤسسات الدولة، وإلى غير ذلك من جرائم.

وبيان التفرقة بين تلك الآثار سواء تمثلت في الجرائم المضرة بأمن الدولة من جهة الداخل سواء كان اجتماعيًا أم سياسيًا أم اقتصاديًا أم كان يتعلق بنظام الحكم وإلى حماية الأمن والاستقرار الذي يتمتع به الأفراد، أم الاعتداء على أمن الدولة من جهة الخارج بهدف حماية استقلال الدولة وسيادتها. وذلك مع الوضع بعين الاعتبار أن كيان أمن الدولة من جهة الداخل والخارج يمثل وحدة واحدة وكلا لا يتجزأ.

التوصيات

ويلاحظ مما توصلنا إليه من خلال البحث، أن الجهد المبذول في حماية اختراق الأمن السيبراني والجرائم الناشئة عنه يوفر الكثير من عناء حدوثه وما يترتب على ذلك من أضرار. وهو في واقع الأمر حماية لحرمة الحياة الخاصة بالأفراد، وحماية للأمن القومي للدولة من جهة الداخل والخارج. **وإن كنا نود عرض بعض المقترحات على سبيل التوصيات:**

- المطالبة بالتدخل التشريعي لمواكبة تطور الجريمة الإلكترونية المعاصرة وسرعة انتشارها.
- ضرورة التعاون الإقليمي والدولي لوضع قيود يتم من خلالها ملاحقة مجرمين القرصنة الإلكترونية.
- تفعيل سياسات وقائية دفاعية في صورة تدبير وقائي يتمثل في حماية البيانات الشخصية لمستخدمي الوسائل التكنولوجية. ومن جهة أخرى اتخاذ تدبير دفاعي لمواجهة حماية الأمن السيبراني من الاختراق.
- تدريب السلطات التشريعية والقضائية والتنفيذية على اكتساب الخبرة التقنية، للتعامل مع الجرائم الإلكترونية نظرا لما تتطلبه طبيعة هذه الجرائم من تقنية لاكتشافها والبحث عنها.

قائمة المراجع

المراجع العربية:

١). الجرائم الاقتصادية الشائعة الجزء الثاني، بهاء المري، دار روائع القانون، الطبعة الثانية ٢٠١٩.
٢). الجريدة الرسمية، العدد ٣٢ مكرر (ج) نشر بتاريخ أغسطس ٢٠١٨.
٣). قانون العقوبات، القسم العام، مأمون محمد سلامة، سلامة للنشر والتوزيع، طبعة ٢٠٢٠.
٤). شرح قانون الإجراءات الجنائية الجزء الأول، محمود نجيب حسني، دار النهضة العربية، الطبعة الرابعة ٢٠١١.
٥). شرح القواعد العامة للإجراءات الجنائية، عبد الرؤوف مهدي، دار الأهرام للنشر والتوزيع، طبعة ٢٠٢٠.
٦). الوسيط في قانون الإجراءات الجنائية، أحمد فتحي سرور، دار الأهرام للنشر والتوزيع، الطبعة الحادية عشر ٢٠٢٠.
٧). تطورات الاستخدام الاقتصادي للذكاء الاصطناعي، عبد السلام محمد، دار الأهرام للنشر والتوزيع، طبعة ٢٠٢٢.
٨). شرح قانون العقوبات القسم العام، محمود نجيب حسني، دار المطبوعات الجامعية، طبعة ٢٠١٨.
٩). شرح القواعد العامة لقانون العقوبات، عبد الرؤوف مهدي، دار النهضة، طبعة ٢٠١١.
١٠). الوسيط في قانون العقوبات القسم العام، أحمد فتحي سرور، دار الأهرام للنشر والتوزيع، طبعة ٢٠٢٠.
١١). الموقع الرسمي لجامعة الدول العربية www.gocsi.com
١٢). الجرائم الإرهابية في القانون المصري وفقا للمعايير الدولية، أحمد فتحي سرور، الهيئة المصرية للكتاب، طبعة ٢٠١٨.
١٣). شرح جرائم تقنية المعلومات، بهاء المري، منشأة المعارف، طبعة ٢٠١٩.
١٤). المستحدث من المبادئ الصادرة من الدوائر الجنائية بمحكمة النقض، المكتب الفني المجموعة الجنائية ٢٠١٩/٢٠٢٠.
١٥). المستحدث من المبادئ الصادرة من الدوائر الجنائية بمحكمة النقض، المكتب الفني المجموعة الجنائية ٢٠٢٠/٢٠٢١.

المراجع الأجنبية:

1). Cyber Security involves reducing the risk of malicious attack to software, computers and networks. This includes tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, enable encrypted communications, and on and on" (Cyber security, Edward Amoroso 2007).

(ISSN: 2537 - 0758)

2). Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets." (ITU 2009).
3). The body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access to ensure confidentiality, integrity and availability" (Public safety Canada, 2014).
4). Cybersecurity consists largely of defensive methods used to detect and thwart would-be intruders" (Kemmerer, 2003).
5). The art of ensuring the existence and continuity of the information society of a nation, guaranteeing and protecting, in Cyberspace, its information, as-sets and critical infrastructure" (Canongia & Man-Darino, 2014).
6). The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this" (Oxford University Press, 2014).
7). Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption" (Lewis, 2006).
8). The ability to protect or defend the use of cyber-space from cyber-attacks" (CNSS, 2010).
9). The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation" (DHS, 2014).
10). Cryptography and Network Security, William Strallings, global seventh edition 2017, chapter 1, page 21.
11). 19-7242 Volume 6 Issue 4 April 2017, Page No. 21042-21050 Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i4.42 Aman Gupta, IJECS Volume 6 Issue 4 April, 2017 Page No. 21042-21050 Page 21042 Ethical Hacking and Hacking Attacks Aman Gupta, Abhineet Anand.
12). International Journal Of Engineering And Computer Science ISSN:23
13). Study Of Ethical Hacking Bhawana Sahare1, Ankit Naik2, Shashikala Khandey, International Journal of Computer Science Trends and Technology (IJCST) Volume 2 Issue 4, Nov-Dec 2014
14). Hacking- The Art of Exploitation, Jon Erickson, 2nd Edition 2008, p478.