الجرائم السيبرانية في عصر الثورة الصناعية الرابعة: الواقع والمأمول (دراسة وصفية تحليلية استشرافية في حقل القانون الجنائي)

الدكتور/ معاذ سليمان راشد الملا*

الملخص:

ورد لدى الخبير والباحث الأمريكي في مجال أمن المعلومات Donn B. Parker في مؤلفه Fighting Computer Crime عبارة مؤثرة وجديرة بأن نضعها في الاعتبار وهي أننا "بحاجة إلى معرفة أكبر قدر ممكن حول إساءة استخدام أجهزة الحاسب الآلي وآثارها لحماية معلوماتنا بشكل فعال. فمعرفة نقاط الضعف وحدها ليست كافية". وهذه العبارة فعلاً تكشف لنا واقع معرفتنا بالجرائم السيبرانية وأسبابها وآثارها المدمرة، ومع ذلك مازلنا عاجزين عن مواجهة تطورها المخيف على المجتمعات البشرية، لاسيما في عصر الثورة الصناعية الرابعة. فهذه الجرائم تعد من بين أهم التحديات التي سعت دول العالم بأسرها إلى مكافحتها والحد من آثارها المدمرة، إلا أن تجارب تلك الدول، والجهود التي بذلتها منذ ظهور هذه الجرائم في سبعينيات القرن الماضي حتى يومنا هذا تضعنا أمام واقع عدم كفاية منظومتها القانونية، وفاعلتها لمواجهة هذه الجرائم، بدلالة تطورها المستمر، وعدم استيعاب الأمم آثار هذا التطور الذي أدى إلى اتساع رقعة مخاطرها؛ بسبب تكنولوجيات عصر الثورة الصناعية الرابعة؛ كالذكاء الاصطناعي وإنترنت الأشياء والبيانات الضخمة والميتافيرس وغيرها من تكنولوجيات نقلت هذه الجرائم نقلة نوعية من حيث الأداء والآثار. لذلك؛ أردنا في هذه الورقة بيان ملامح تطور الجرائم السيبرانية والوقوف على تأثير تكنولوجيات الثورة الصناعية الرابعة على طبيعتها، وبيان التحديات الموضوعية والشكلية التي فرضت نفسها في الآونة الأخيرة. ومن أجل ذلك؛ ارتأينا اتباع منهج وصفي تحليلي نستشرف فيه واقع هذه الجرائم وتحدياتها أمام القانون الجنائي، وصولاً إلى نتائج وتوصيات تتضمن حلولاً لهذه المواجهة.

الكلمات المفتاحية: الجرائم السيبرانية – القانون الجنائي – تحديات – الثورة الصناعية الرابعة – الذكاء الاصطناعي.

---

* أستاذ القانون الجزائي المشارك – كلية القانون الكويتية العالمية – الكويت.

Cybercrime in the Fourth Industrial Revolution: Reality and Hope A Descriptive, Analytical, and Prospective Study In the Field of Criminal Law

Dr. Muath Sulaiman Rashid Al-Mulla*

Abstract:

In his book titled Fighting Computer Crime, the American expert and researcher in the field of information security, Donn B. Parker, mentioned an influential phrase that we should bear in mind, which is that "we need to know as much as possible about the misuse of computers and their effects in order to protect our information effectively; knowing the points of weakness alone is not sufficient." This phrase really reveals to us the reality of our knowledge of cybercrime, its causes, and it's devastating effects, yet we are still unable to confront its frightening development on human societies, especially in the era of the Fourth Industrial Revolution. These crimes are considered among the most important challenges that the countries of the world as a whole have sought to combat and limit their destructive effects. However, the experiences of those countries and the efforts they have made since the emergence of these crimes in the seventies of last century until the present day have put us before the reality of the inadequacy of their legal system and its effectiveness to confront these crimes. Its continuous development and the failure of nations to comprehend the effects of this development, which led to the widening of its risks due to the technologies of the era of the fourth industrial revolution, such as artificial intelligence, the Internet of things, big data, metaverse, and other technologies. These crimes conveyed a quantum leap in terms of performance and effects. So, in this paper, we wanted to show the features of the development of cybercrime, to stand on the impact of the technologies of the fourth industrial revolution on its nature, and to show the objective and formal challenges that have imposed themselves in recent times. For this purpose, we decided to follow a descriptive and analytical approach in which we explored the reality of these crimes and their challenges before the criminal law, to reach conclusions and recommendations that include solutions to this confrontation.

Keywords: Cybercrime - Criminal Law - Challenges - The Fourth Industrial Revolution - Artificial Intelligence.

---

* Associate Professor of Criminal Law, Kuwait International Law School, Kuwait.

المقدمـــة

قدمت التكنولوجيا الحديثة للإنسان مزايا كثيرة طورت مختلف مجالات حياته؛ حيث أعادت صياغة مفهوم التفاعل الإنساني، وانتقلت به من واقع التفاعل الحقيقي إلى واقع افتراضي لا يصطدم بحاجز الزمان أو المكان، كما تأثرت الحكومات ذاتها حيث استجابت لهذا الواقع، وتأقلمت مع معطياته، حتى أصبحنا أمام حكومات يُطلق عليها وصف إلكتروني أو حكومة إلكترونية أو حكومة رقمية[١].

والحقيقة أن تنافس شركات التكنولوجيا واستمراريتها وسرعتها في تطوير التطبيقات بدأنا –وبحق– نشعر بها حتى ضمن تحديث أجهزتنا، ففي كل يوم نسمع أخباراً عن اكتشافات واختراعات جديدة وهذه السرعة كانت بسبب ما أحدثته الثورة الصناعية الرابعة وتطبيقاتها المختلفة[٢]؛ كالذكاء الاصطناعي والبيانات الضخمة وإنترنت الأشياء والمركبات ذاتية القيادة والطائرات المسيرة والروبوتات والطباعة ثلاثية الأبعاد وتكنولوجيا الواقع الافتراضي، فهذه التطبيقات أحدثت نقلة نوعية في استخدام أدوات تقنية المعلومات من مجرد أدوات مؤتمتة تنفذ مهام محددة إلى أدوات ذكية قادرة على اتخاذ القرار دون تدخل من الإنسان.

---

[١] برزت فكرة الحكومة الإلكترونية أثناء حملة بيل كلينتون في انتخابات الرئاسة الأمريكية، حيث أعلن عن نيته بجعل طريق المعلومات السريع حجر الزاوية في البنية التحتية وتجسدت في أواخر التسعينيات. حول ذلك راجع د. داوود الباز، الحكومة الإلكترونية وأثرها على النظام القانوني للمرفق العام، منشأة المعارف، الإسكندرية، ٢٠٠٧، ص٢٦.

Grönlund, Åke and Horan, Thomas A. (2005) "Introducing e-Gov: History, Definitions, and Issues", Communications of the Association for Information Systems (AISeL): Vol. 15, 2004 Article 39. P713.
DOI: 10.17705/1CAIS.01539

[٢] د. محمد عبد الوهاب العزاوي، الثورة الصناعية الرابعة: رؤية عربية لتحديات المستقبل، الطبعة الأولى، ٢٠٢١م، المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، ص١٣.

ويعلم الجميع أن غريزة الشر في النفس البشرية وظفت التكنولوجيا في تحقيق المآرب الإجرامية؛ فظهرت العديد من المصطلحات والمفاهيم التي تدلل على طبيعة هذه الجرائم، وسوف نعتمد مصطلح الجرائم السيبرانية، فهذه الجرائم تعاظمت خطورتها مع توظيف تطبيقات الذكاء الاصطناعي، فالمشكلة أن المجتمع القانوني والأمني على وجه التحديد يعيان حجم خطورة هذه الجرائم وآثارها المدمرة على المقومات الأساسية للدول، وأن القوانين التي خُصصت لمواجهتها لم تكن كافية خصوصاً في ظل عدم وجود تعاون دولي حقيقي لمواجهة هذه الجرائم والحد من آثارها، فهذه القوانين غير قادرة على ملاحقة التطور السريع بسبب بطئها من ناحية وعدم استيعاب ما يخلفه التطور السريع من تحديات قانونية أكثر تعقيداً من قبل. هذا إلى جانب ضعف الأمان السيبراني، وعدم مواكبته تقنياً لحماية الأنظمة المختلفة من مخاطر تعرضه للهجمات المختلفة.

وما نهدف إليه في سياق هذه الورقة هو ترجمة عنوانها، وهو بيان مدى تطور الجرائم السيبرانية في عصر الثورة الصناعية الرابعة، فاتبعنا منهجاً وصفياً تحليلياً حيث أردنا إيجاد تفسير لازدياد معدل هذه الجرائم وارتفاع خسائرها على الرغم من وجود قوانين مكافحة لها في معظم دول العالم إن لم يكن جميعها، وذلك كله بعد الوقوف على مفهومها، وعلاقتها ببعض المفاهيم الأخرى في البيئة ذاتها، محاولين الخروج ببعض المقترحات التي تستشرف حلولاً مناسبة تضمن آلية جدية لمواجهتها، وقمنا بتقسيم خطة البحث إلى ثلاثة مطالب وهي على النحو الآتي:

المطلب الأول: الجرائم السيبرانية: المفهوم والحقائق.

المطلب الثاني: مراحل تطور الجرائم السيبرانية: من التحكمية إلى الذكاء الآلي.

المطلب الثالث: التحديات التي فرضتها الثورة الصناعية الرابعة على قواعد القانون الجنائي.

المطلب الأول

الجرائم السيبرانية: المفهوم والحقائق

الجريمة –كما نعرفها– كل فعل أو امتناع يصدر من شخص مسؤول عن إتيانه بشكل يخالف قواعد القانون الذي يقرر عقوبة أو تدبيراً احترازياً له، ونعلم أيضاً أن الجريمة تطورت بفضل أدوات تكنولوجيا المعلومات التي عولمة أشكالها، وعظمت من خطورتها، حتى ظهرت مصطلحات ومفاهيم عدة للتدليل على طبيعة هذه الجرائم.

أولاً– مفهوم الجرائم السيبرانية:

لم يتفق الفقهاء على تحديد مصطلح ومفهوم يعبران عن الجرائم التي ترتبط بأدوات تقنية المعلومات، فالمتتبع لمراجع الفقه سوف يجد عمق الخلاف بينهم؛ حيث تعددت مصطلحاتها وتعريفاتها ضيقاً واتساعاً بسبب الاختلاف في رؤاهم التي اعتمدت على شكلية معينة، وقد قال بعضهم أن هناك أزمة في تحديد المصطلح والمفهوم[٣].

فالجهود الدولية المتعددة لمكافحة هذه الجرائم حاولت وضع مصطلح وتعريف لها، ففي إعلان فينا الخاص بالجريمة والعدالة في مواجهة تحديات القرن الحادي والعشرين الصادر عن مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في إبريل ٢٠٠٠ تم تبنى مصطلح الجريمة المعلوماتية، وعرفها بأنها: "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"[٤]، وهذا التعريف

---

[٣] أسامة أحمد المناعسة وجلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية – دراسة مقارنة، الطبعة الثانية، ٢٠١٤م، دار الثقافة للنشر والتوزيع، عمان، المملكة الأردنية الهاشمية، ص٦٦. د. عمار عباس الحسيني، جرائم الحاسوب والإنترنت– الجرائم المعلوماتية، الطبعة الأولى، ٢٠١٧م، منشورات زين الحقوقية، بيروت، ص٣٥ وما بعدها. وانظر أيضاً لدى:

Joanna Świątkowska, tackling cybercrime to unleash developing countries'digital potential, The European Cybersecurity Forum - CYBERSEC and AGH University of Science and Technology 2020, p7.

[٤] راجع الموقع الإلكتروني للإسكوا – الأمم المتحدة، على الرابط الآتي:

https://archive.unescwa.org/ar/tenth-united-nations-congress-prevention-crime-and-treatment-offenders

واسع في حقيقة الأمر، بل من أفضل التعريفات مقارنة بالتعريفات الدولية والإقليمية التي تلتها كتعريف خبراء منظمة التعاون الاقتصادي والتنمية التابعة للأمم المتحدة؛ حيث عرفوها بأنها: "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية الإلكترونية". وعرفتها المفوضية الأوروبية في الاستراتيجية الخاصة للأمن السيبراني لعام ٢٠١٣م بأنها: "مجموعة واسعة من الأنشطة الإجرامية المختلفة حيث يتم استخدام أجهزة الكمبيوتر وأنظمة المعلومات إما كأداة أساسية أو كهدف أساسي"[٥].

وهذا الخلاف انعكس على خطة المشرعين العرب الذين اتفقوا على إطلاق وصف مكافحة جرائم تقنية المعلومات في اتفاقية القاهرة الصادرة عام ٢٠١٠م، ولكن اختلفوا في تشريعاتهم الوطنية؛ فالمنظم السعودي أطلق عليها الجرائم المعلوماتية، والمشرع القطري أطلق عليها الجرائم الإلكترونية، وأطلق عليها المشرعان العماني والكويتي وصف جرائم تقنية المعلومات، وتبناه مسبقاً المشرع الإماراتي؛ إلا أنه غير المصطلح إلى مكافحة الشائعات والجرائم الإلكترونية، وهذا التفاوت شمل معظم قوانين الدول العربية الأخرى، وامتد إلى مسلك بعض التشريعات بتعريف هذه الجرائم؛ كالمنظم السعودي والقطري والكويتي وقوانين أخرى تركت مهمة التعريف للفقه؛ كالمشرع العماني الذي نص في المادة الأولى بند(ج) بأن جرائم تقنية المعلومات: "كل الجرائم المنصوص عليها في هذا القانون". والمشرع البحريني الذي لم يشر أبداً إلى تعريف هذه الجرائم.

ومن ناحيتنا نرى أن المصطلح الأنسب هو مصطلح جرائم تقنية المعلومات الذي استخدمته الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، أو مصطلح الجرائم السيبرانية إذا أردنا ترجمته من اللغة الإنجليزية Cybercrime كما هو الحال في اتفاقية بودابست الأوروبية الصادرة عام ٢٠٠١م؛ فقد تبنت كافة الدول الأوروبية مصطلح الجرائم السيبرانية.

أما تعريفات هذه الجرائم؛ فعلى الرغم من الجدل حول إيجاد تعريف جامع مانع، نجد أن التعريف الأشمل هو الذي يعرض أدوات تكنولوجيا المعلومات كوسائل أو أدوات لتنفيذ

---

(5) Joanna Świątkowska, op.cit, p.7.

النشاط الإجرامي عبرها أو هدفاً لها أو بيئة حاضنة للمحتوى الإجرامي[٦]. فهذا التعريف يجمع الأنشطة المستحدثة والأنشطة التقليدية[٧]، كما نرى أنه قادرٌ على استيعاب ما يقدمه المستقبل من نماذج أخرى، بما في ذلك الأنشطة الإجرامية عبر الذكاء الاصطناعي، والتطبيقات الأخرى.

وتجدر الإشارة إلى أن الجرائم السيبرانية عبارة عن أنشطة ماسة بالكيانات المعنوية، كونها ترتبط بالمحتوى المعلوماتي أياً كان شكله، وأياً كان الحق أو المصلحة المتصلة به، فقد يكون المحتوى يمس الحق في الخصوصية أو حق المؤلف أو أسرار أو غير ذلك. لذلك يمكن القول كلما كان المحتوى محمياً كلما قلت الهجمات السيبرانية، فالأمن السيبراني يسهم في مكافحة هذه الجرائم[٨]، وقد أكد الاتحاد الدولي للاتصالات في دراسة صدرت عنه عام ٢٠١٢م أن وضع استراتيجية لمكافحة الجرائم السيبرانية يشكل عنصراً لا يتجزأ من استراتيجية الأمن السيبراني[٩].

ثانياً- الجرائم السيبرانية والحقائق:

مما لا شك فيه أن معدلات الجرائم السيبرانية تزداد يومياً بعد يوم حالياً، لاسيما مع اعتماد أدوات التكنولوجيا على خوارزميات الذكاء الاصطناعي، ويقول رئيس تحرير مجلة Cybersecurity Ventures ستيف مورجان في تقرير الجرائم السيبرانية الصادر لعام ٢٠٢٢م أنه: "إذا اعتبرنا الجرائم السيبرانية دولة، فإنها ستكون أكبر اقتصاد في العالم

---

[٦] د. أيمن عبد الله فكري، جرائم نظم المعلومات – دراسة مقارنة، ٢٠٠٧م، دار الجامعة الجديدة، الإسكندرية، ص٨٢. وانظر أيضاً:

Jonathan Clough, Principles of Cybercrime, 2 edition, 2015, Cambridge University Press, UK, P.10-11.

(7) Joanna Świątkowska, op.cit, p.8.

(8) Australian Government, Attorney General's Department, National Plan to Combat Cybercrime, 18. P.6.
http://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Documents/National%20Plan%20to%20Combat%20Cybercrime.pdf

(9) Marco Gercke, Understanding Cybercrime: Phenomena, Challenges and Legal Response, ITU, September 2012, p. 97 19

بعد الولايات المتحدة الأمريكية والصين"[١٠]، وسوف نحاول رصد أهم الإحصائيات التي توضح مدى ارتفاع معدلات الجرائم السيبرانية بالحقائق والأرقام التي أظهرتها المراكز البحثية المختلفة عبر تقاريرها حول هذه الجرائم:

١. أشار تقرير Cybersecurity Ventures لعام ٢٠٢٢م إلى أن نمو تكاليف الأضرار الناجمة عن الجرائم الإلكترونية تقدر بـ ٣ تريليون دولار أمريكي في عام ٢٠١٥م، ومن المتوقع أن تصل الأضرار إلى ١٠,٥ تريليون دولار بحلول عام ٢٠٢٥. وبيَن التقرير أن تكلفة أضرار برامج الفدية Ransomware damages الواقعة على الأفراد والمؤسسات كل ثانيتين زادت ٥٧ مرة منذ عام ٢٠١٥م حتى عام ٢٠٢١م بمقدار ٢٠ مليار دولار، ويتوقع أن هذه التكلفة سوف تزداد سنوياً إلى ما يقارب ٢٦٥ مليار دولار بحلول عام ٢٠٣١م. كما بين أن الأضرار الناجمة عن الهجمات المتعلقة بالعملات المشفرة تقدر ٧,٧ مليار دولار أمريكي.

٢. أظهر تقرير Mimecast's لعام ٢٠٢٣م نتائج إحدى الدراسات البحثية، وكشفت هذه الدراسة عن توقعها سرقة ٣٣ مليار سجل إلكتروني في عام ٢٠٢٣م، وبمعدل زيادة ١٧٥% عن عام ٢٠١٨م؛ حيث تم سرقة ١٢ مليار سجل في هذه الفترة[١١].

٣. كشف منتدى دافوس الاقتصادي المنعقد في ١ يوليو عام ٢٠٢٢م[١٢] أن فرق الأمن السيبراني في كافة دول العالم تعرضت للإرباك أثناء فترة جائحة كورونا؛ حيث استغل المجرمون انتقال بيئات العمل المختلفة بما في ذلك الشركات إلى العمل عن بعد،

---

[١٠] راجع الموقع الإلكتروني للمجلة على الرابط التالي:
https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

[١١] راجع التقرير على الرابط التالي:
https://www.mimecast.com/resources/ebooks/the-state-of-email-security-2023/download/

[١٢] للمزيد من التفاصيل راجع الموقع الإلكتروني للمنتدى على الرابط التالي:
https://www.weforum.org/agenda/2022/07/global-cybersecurity-outlook-davos-2022/

الذي أصبح أمراً أساسياً لسير الأعمال، وقد أظهر أن الهجمات السيبرانية زادت ١٢٥% على مستوى العالم حتى عام ٢٠٢١م، واستمرت في ازدياد إلى عام ٢٠٢٢م.

٤. بينت شركة IBM في تقريرها الصادر عام ٢٠٢٢م أن متوسط الوقت الذي تستغرقه الشركات لتحديد الهجوم السيبراني، واحتوائه والرد عليه هو ٢٧٧ يوماً، وهو أقل بثلاثة أيام عن المتوسط في عام ٢٠٢٠م، وقدرت أنه كلما زاد الوقت الذي يستغرقه تحديد الهجوم السيبراني واحتوائه، زادت تكلفة الرد، وهذه التكلفة وفق تقديرها هي ١,١٢ مليون دولار أمريكي. كما أظهر التقرير أن متوسط كلفة اختراقات أنظمة الشركات وانتهاك البيانات تصل إلى ٤,٣٥ مليون دولار أمريكي. كذلك تناول التقرير أعلى تكلفة اختراق تقع في أنظمة الرعاية الصحة؛ حيث بلغت الخسائر ١٠,١٠ مليون دولار أمريكي[١٣].

٥. أجرت A Clark School دراسة عبر ميشيل كوكير في محاولة للتعرف على قراصنة "القوة الغاشمة"، أظهرت فيها أن الهجمات تحدث طوال الوقت على أجهزة الحواسيب المتصلة بشبكة الإنترنت بمتوسط ٢٢٤٤ محاولة يوميًا وتصل إلى هجوم واحد كل ٣٩ ثانية. وبينت أن هذه الهجمات ليست جميعها ناجحة؛ إلا أن معظمها يحاول الوصول إلى أسماء المستخدمين وكلمات المرور[١٤].

٦. وفقًا لدراسات أجراها مركز Statista أن آثار الجرائم الإلكترونية واختراق البيانات واسعة النطاق وعالمية، وقد بينت أن هناك ١٨٠٢ حالة من حالات اختراق البيانات الخاصة بأفراد أمريكيين في عام ٢٠٢٢م، وتأثر ٤٢٢ مليون فرد من قبل جهات التهديد[١٥].

---

[١٣] للمزيد من التفاصيل راجع التقرير، على الرابط التالي:
https://www.ibm.com/reports/data-breach

[١٤] راجع الموقع الإلكتروني، على الرابط التالي:
https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

[١٥] للمزيد من التفاصيل راجع الموقع الإلكتروني للمركز، على الرابط التالي:
https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

٧. بين تقرير SoSafe's Cyber Trends عام ٢٠٢٣م أن (٩٠ %) من الخروقات الأمنية في الشركات تكون نتيجة لهجمات التصيد الاحتيالي، إذ بات من السهل مع دخول الذكاء الاصطناعي في تطوير خداع المستخدمين والموظفين، وأن العلامات التجارية أصبحت في مرمى هذه الأنشطة خصوصاً العلامات التجارية الكبرى [١٦].

٨. وفقًا لدراسة نشرتها شركة Next Move Strategy Consulting، أظهرت فيها أن قيمة حجم سوق الأمن السيبراني العالمي ما يقرب من ٢٢٢ مليار دولار أمريكي في عام ٢٠٢٢م، ومن المتوقع أن يتجاوز السوق ٦٥٠ مليار دولار أمريكي ويزداد بنمو سنوي يقدر بنسبة (١٢,٨٪) من عام ٢٠٢٢م إلى عام ٢٠٣٠م[١٧].

٩. أظهر مركز أبحاث التنمر الإلكتروني الذي يقوم بجمع البيانات منذ عام ٢٠٠٧م حتى الآن، أن نسبة الذين تعرضوا للتنمر الإلكتروني (٢٩,٣%) من طلاب المدارس المتوسطة والثانوية. وتشكل زيادة بنسبة ١,٥ بالمائة منذ عام ٢٠٢٢م. وهناك عدة دراسات تظهر مدى خطورة هذه النوعية من الاعتداءات خصوصاً على الأطفال في المدارس [١٨].

مما تقدم نجد أن لغة الأرقام التي تتبعناها من عدة إحصائيات مختلفة، قامت بإعدادها مراكز متخصصة في مجال تقنية المعلومات، تكشف عن حقيقة ارتفاع مستمر لمعدلات الجرائم السيبرانية، وازدياد في تكاليف الخسائر الناجمة عنها، فضلاً عن الجرائم الأخرى، فعلى الرغم من التدابير المتخذة على المستويين الدولي والإقليمي لمكافحتها؛ إلا أن هناك صعوبة حقيقية لمواجهتها.

---

[١٦] راجع التقرير على الموقع الإلكتروني التالي:
https://sosafe-awareness.com/resources/reports/cybercrime-trends-2023/

[17] Next Move Strategy Consulting, New York, Jan. 30, 2023.
https://www.nextmsc.com/report/cyber-security-market

[١٨] للاطلاع على الدراسات راجع الرابط الإلكتروني التالي:
https://www.comparitech.com/internet-providers/cyberbullying-statistics/

المطلب الثاني

أثر تكنولوجيات الثورة الصناعية الرابعة

على تطور الجرائم السيبرانية

ندرك تماماً أن مصدر الجريمة هو الإنسان ذاته، وما زال حتى يومنا هذا يستغل ذكاءه في تطوير أساليبه التي اعتمدت على الابتكار في مجال تكنولوجيا المعلومات؛ فظهرت جرائم مرتبطة بها وهي الجرائم السيبرانية التي تنال من الجميع بدون استثناء سواء كانوا متصلين في شبكة الإنترنت أو لم يتصلوا بها[١٩]، ولقد خصصنا هذا المطلب لبيان ملامح تطور هذه الجرائم في مرحلتين اثنتين الأولى: مرحلة السيطرة والتحكم البشري، والثانية مرحلة أتمتة الجريمة وذكاء الآلة.

أولاً- مرحلة السيطرة والتحكم البشري:

اعتمدت هذه المرحلة على قدرة الإنسان في توظيف أدوات تكنولوجيا المعلومات في ارتكاب الجريمة، التي تغيرت شيئاً فشيئاً تبعاً للتطور التكنولوجي، الذي بدأت معالمه تظهر في عصر المعلومات، أي العصر الذي انتقلت فيه القوة من شخص يمتلك رأس المال لإنشاء المصانع ودفع أجور العمال إلى شخص يسيطر على تقنيات الاتصالات والمعلومات، ويمتلك المعرفة التقنية والبرمجية، حتى أُسبغ عليه وصف الذكاء؛ لاعتماده على تلك الأدوات في ارتكاب هذه النوعية من الجرائم؛ فأُطلق عليه مصطلح المجرم المعلوماتي أو المجرم السيبراني، وإلى غير ذلك من مسميات تجعله في ميزان التفرقة أخطر وأذكى من المجرم التقليدي.

وقد درج إطلاق مسمى الهاكرز أو المخترقين للإشارة إلى النموذج المحترف أو الأذكى من بين الطوائف الإجرامية الأخرى في هذه البيئة[٢٠]، ويتفق فقهاء القانون فيما بينهم

---

(19) David Sutton, Cyber Security: A practitioner's guide, 2007 BCS Learning & Development Ltd, UK, P12.

(٢٠) حول ذلك راجع أسامة أحمد المناعسة وجلال محمد الزعبي، المرجع السابق، ص٧٦ وما بعدها. ود. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت – دراسة مقارنة، الطبعة الأولى ٢٠٠٩م، دار النهضة العربية، القاهرة، ص٦١. وفي الفقه الأجنبي راجع:

على أن هناك سمات شخصية له، أولها أن المجرمين يتمتعون بمؤهلات فنية تخصصية في مجال تقنية المعلومات، أما الصفة الثانية فتتمثل في ذكاء من لديه خبرة ومهارة عالية سواء كانت لديه مؤهلات أم كانت بسبب اكتسابه الخبرة والمهارة التي تمكنه من التعامل بهذه الأدوات، ويضيف البعض سمات أخرى كالسن والمكانة والخبرة[٢١]، وهذه الصفات في مجملها مكنت المجرمين من توظيف أدوات تقنية المعلومات في إتمام الأنشطة الإجرامية في الفضاء السيبراني، وما يفسر لجؤهم إليها خصوصاً الجماعات الإجرامية المنظمة هو الخصائص التي تميزت بها عن الجرائم التقليدية من حيث الأداء ومن حيث الأثر، فمن حيث الأداء تميزت هذه الجرائم بأنها تتم بلا عنف وبكبسة زر، وتتم أيضاً دون مواجهة مع المجني عليه، كما أنها جرائم عابرة للحدود الوطنية، أما من حيث النتيجة فقد تميزت هذه الجرائم بدقة وسرعة في التنفيذ، كما أن أثارها خطيرة جداً على المقومات الأساسية للدول، لاسيما مع اعتماد كياناتها على التقنية الحديثة[٢٢].

ويمكن القول بأنه مع تغلغل هذه الأدوات في حياتنا جعل صفة الذكاء متفاوتة، فجريمة الدخول غير المشروع على سبيل المثال تختلف عن جريمة القذف والسب التي تعد جريمة تقليدية، ولكن الأدلة المستخدمة فيها حدثت طريقتها، والخطورة في الأمر أن المجرمين استطاعوا نقل خبرتهم الإجرامية على شبكة الإنترنت بتحميل المحتويات غير المشروعة، وفهرستها في المواقع الإلكترونية التي تتضمن طرق صناعة الفيروسات الخبيثة، وغير

Don B. Parker, Fighting Computer Crime – A New Framework for Protecting Information, 1998, Wiley, USA, P159.

Thomas J.Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar, Cybercrime and Digital Forensics, 2015, Routledge, UK, P40.

[٢١] راجع د. أيمن عبد الله فكري، المرجع السابق، ص١٠٦ وما بعدها. ود. حسين بن سعيد الغافري، المرجع السابق، ص٦٢.

Don B. Parker, Op, cit, P136 -P162.

[٢٢] حول ذلك راجع أسامة أحمد المناعسة وجلال محمد الزعبي، المرجع السابق، ص٧٦ وما بعدها. و د. أيمن عبد الله فكري، المرجع السابق، ص٩٦ وما بعدها وانظر إلى هذه الخصائص لدى:

Jonathan Clough, Op, cit, P15-23.

ذلك. وهذا ما قصدناه أن بيئة الإنترنت أصبحت حاضنة للمحتوى الإجرامي، بحيث يُمَكِن المستخدمين من إجراء البحث عبر محركات البحث العادية؛ كغوغل وبينغ وغيرها.

وليس ذلك فحسب؛ بل هناك مواقع غير مرئية توجد أسفل المواقع العادية يطلق عليها بمواقع الويب العميق أو الديب ويب المواقع وقواعد البيانات غير المكتشفة في شبكة الإنترنت تتضمن أشكالاً من المحتوى المعلوماتي كالمجلات الأكاديمية، وشبكات الإنترنت التجارية، وأرشيف الويب، والخدمات المصرفية عبر الإنترنت وصولاً إلى المواقع الإلكترونية المحمية بكلمة مرور وغيرها. وهذا المحتوى لا يمكن الوصول إليه من خلال محركات البحث العادية؛ لأنه غير مفهرس والطريقة الوحيدة للوصول إليه هي من خلال امتلاك عنوان الموقع، كما أن هناك ما هو أعمق وأخطر من هذه البيئة، والذي يُطلق عليه الويب المظلم أو الدارك ويب وهو جزء صغير من الديب ويب، وهو مكان يضم مواقع إلكترونية لا يمكن تتبع مصدرها ولا يمكن التعرف فيها على المستخدمين الذين يبقون هوياتهم مجهولة بشكل كامل من خلال أدوات (برنامج I2P أو Tor) لإخفاء عناوين بروتوكولية الـ IP كما لا يمكن لأحد الوصول إليه بالطرق العادية، سوى أشخاص محددين وعبر بوابات محددة كما بينا، وقد عُرفت هذه البيئة بأنها منطلق للأنشطة غير القانونية؛ كالاتجار بالمخدرات والإتجار بالبشر وإلى غير ذلك من جرائم خطيرة لا يمكن تعقب مرتكبيها[٢٣]، وقد انضمت إليها مواقع إلكترونية شهيرة؛ كموقع فيسبوك بغاية تقديم خدمات بعيدة عن الرقابة، وأيضاً موقع ويكليكس لقبول تسريبات من مصادر مجهولة.

---

[٢٣] د. وليد بن صالح، الإنترنت المظلم والعملات الافتراضية: التحديات الجديدة للقانون الجنائي، مجلة كلية القانون الكويتية العالمية، العدد رقم ٣ الجزء الثاني- أكتوبر ٢٠١٨م، الكويت، ص٣٩٠ وما بعدها. ود. رامي متولي القاضي، مكافحة الإجرام المنظم عبر شبكة الإنترنت المظلمة، بحث منشور في المجلة الجنائية القومية، المجلد ٦٤ العدد ٣، نوفمبر ٢٠٢١م، ص٤٧.
https://ncj.journals.ekb.eg/issue_29391_32360.html

وراجع حول ذلك أيضاً لدى:
Kristin Finklea, Dark Web, Congressional Research Service, March 10, 2017, USA, P5. And Debarati Halder, Cyber Victimology- Decoding Cyber-crime Victimisation, 2022, Routledge, UK, P.49.

ولم تستطع قوى العالم حتى يومنا هذا مواجهة الأنشطة الإجرامية الصادرة من هاتين البيئتين.

ثانياً- مرحلة أتمتة الجريمة وذكاء الآلة:

وهي المرحلة التي تعبر عن نتائج اعتكاف المطورين في وادي السيلكون على تحسين وظائف التكنولوجيا، قاصدين بذلك خدمة الإنسان وتحقيق رفاهيته، حتى بلغ التطوير ذروته في عصر الثورة الصناعية الرابعة، التي نهضت تكنولوجياتها على تقنية المعلومات؛ كالذكاء الاصطناعي وإنترنت الأشياء والبيانات الضخمة وغيرها[٢٤]، فأضفت صفة الذكاء على الآلة أو الروبوت، وذلك عن طريق أتمتة وظائفها ببرامج تتضمن لغة تفهمها الآلة للقيام بأعمال أو خدمات للبشر بشكل تلقائي أو آلي وبشكل كلي أو جزئي، وتلعب خوارزميات الذكاء الاصطناعي والبيانات الضخمة دوراً كبيراً في ذلك؛ حيث جعلت الآلة أكثر ذكاءً. فالأتمتة تتطلب نظام آلي متمثل في جهاز الحاسوب الذي يتحكم بها، وأيضاً برنامج مكتوب بلغة برمجية معينة، بحيث تفهمها الآلة لتكتسب مهارة التعلم والتدرب من محيطها، وتؤدي الأعمال بناء على الخبرة التي من حصيلة البيانات التي قامت بجمعها لتنفذ تلك الأعمال بذكاء ودقة، وبأقل الأخطار، وقد تتفوق فيها على الإنسان في بعض المهام الصعبة إنجازها في أوقات قصيرة[٢٥].

---

[٢٤] إيهاب خليفة، مجتمع ما بعد المعلومات – تأثير الثورة الصناعية الرابعة على الأمن القومي، مركز المستقبل للأبحاث والدراسات المتقدمة، الطبعة الأولى، ٢٠١٩م، العربي للنشر والتوزيع، القاهرة. ص٢١ وما بعدها. وانظر أيضاً:

Klaus Schwab, The Fourth Industrial Revolution, 2016, Geneva, Switzerland, P11. Mark Skilton and Felix Hovsepian, the 4th Industrial Revolution Responding to the Impact of Artificial Intelligence on Business, 2018, Palgrave Macmillan, Switzerland, P.4.

[٢٥] حول ذلك راجع إيهاب خليفة، المرجع السابق، ص٤٣ وما بعدها. ود. سوسن طه ضليمي ود. ماجد محمد أبو شرحه، استخدام نماذج الذكاء الاصطناعي في تطبيقات إدارة المعرفة، الطبعة الأولى، ٢٠٢١م، القاهرة، ص٣١ وما بعدها. وانظر أيضاً:

Jerry Kaplan, Artificial Intelligence: What Everyone Needs to Know, Oxford University Press; 1st edition – 2016, USA, P.7. And Flynn Coleman: A Human

وقد استفاد المجرمون من إرهاصات هذه الثورة في ارتكاب جرائمهم دون تدخل منهم، فقد أصبحوا أكثر ابتكاراً بسبب الذكاء الاصطناعي الذي يمكن استخدامه في أدوات عدة؛ كاستخدامهم الطائرات بدون طيار لتنفيذ بعض الأنشطة الإجرامية كنقل المواد المتفجرة أو المخدرات أو غير ذلك، أو برمجة الآلة لتزييف الحقيقة عبر التطبيقات الإلكترونية وهو ما أطلق عليه وصف التزييف العميق، وقد استخدمت لتنفيذ عمليات غير مشروعة أبرزها انتحال صفات أو شخصيات الغير لخداع آخرين وجني أرباح طائلة من وراء تلك العمليات، أو استخدامها في التأثير على سير عملية الانتخابات أو الإضرار بسمعة الآخرين.

وتجدر الإشارة إلى أنه بعد إعلان المدير التنفيذي لشركة فيسبوك مارك زوكربيرغ في ٢٨ أكتوبر ٢٠٢١م عن تغيير مسماها إلى ميتا، فقد عبر في هذا الإعلان عن نيته تطوير هذه الخدمة من خلال إدماج الحياة الواقعية مع الواقع الافتراضي والواقع المعزز، ويقال عنها بالواقع الهجين أو المختلط، بمعنى أن تعاملنا مع التكنولوجيا لن يكون من خلال الضغط على الأزرار؛ بل سوف ننتقل بأنفسنا إلى هذا العالم عبر صورة رمزية تعبر عن هوية المستخدم، وقد عرفت باسم أفاتار (Avatar)، وهي ضرورية للتعبير عن المستخدم، ليكون في مساحات افتراضية ثلاثية الأبعاد يستطيع الأشخاص من خلالها الالتقاء والاجتماع، كما يستطيعون شراء وبيع السلع والعقار عبر العملات الافتراضية[٢٦].

Algorithm: How Artificial Intelligence Is Redefining Who We Are Hardcover – October 1, 2019, Counterpoint, USA, P11.

[٢٦] حول ذلك تفصيلاً راجع د. أشرف محمد زيدان ود. سيف السويدي، العالم ما وراء التقليدي "ميتافيرس"، الطبعة الثانية، ٢٠٢٢م، دار الأصالة للنشر والتوزيع، الجمهورية التركية – إسطنبول، ص٣٤. ود. خالد ممدوح إبراهيم، التنظيم القانوني لتقنية الميتافيرس، الطبعة الأولى، ٢٠٢٣م، دار الفكر الجامعي، الإسكندرية، ص٤٤.

Melodena Stephens, METAVERSE AND ITS GOVERNANCE, The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue, New York, June 2022. United States of America. P10.
https://standards.ieee.org/wp-content/uploads/2022/06/XR_Metaverse_Governance.pdf

وبذلك نجد أن الجرائم السيبرانية في عصر الثورة الصناعية الرابعة أصبحت أكثر خطورة كونها ذكية بفضل خوارزميات الذكاء الاصطناعي، أي أننا أصبحنا أمام مفهوم جديد انتقلت فيها الجرائم السيبرانية من مجرد جرائم يتحكم فيها البشر إلى جرائم ترتكبها الآلة الذكية.

المطلب الثالث

التحديات التي فرضتها الثورة الصناعية الرابعة

على قواعد القانون الجنائي

إن طبيعة الجرائم السيبرانية، وتطور أساليبها وتطبيقاتها دون ضوابط من ناحية، وتباطؤ عجلة القانون في مزامنة التطور التكنولوجي أسهم ذلك في إثارة إشكاليات حقيقية أمام تطبيق أحكام قواعد القانون الجنائي، تحديداً بشقيه الموضوعي والإجرائي. وسوف نعرض هذه الإشكاليات وفقاً لهذا التقسيم.

أولاً- الإشكاليات الموضوعية:

فرضت الجرائم السيبرانية إشكاليات حقيقية تتعلق بمدى إمكانية تطبيق أحكام القانون على بعض الأفعال الإجرامية في بيئة الفضاء السيبراني، وهذه الإشكاليات:

١. **عدم ملائمة النصوص الجنائية لبعض الوقائع في العالم السيبراني:** نجم عن التطوير المستمر للتكنولوجيا ظهور أنماط إجرامية يصعب القول بإمكانية تطبيق النصوص التقليدية على وقائعها أو حتى القوانين المتعلقة بمكافحة الجرائم السيبرانية في بعض الدول، والتي تحتاج إلى مرونة وتحديث، بحيث توائم التطور في هذه البيئة، ومن أهم النماذج التي ظهرت مؤخراً الجرائم في بيئة الميتافيرس؛ فقد تعرضت باحثة تجسدت عبر صورة أنثى (أفاتار) للتحرش اللفظي والجنسي من أربع أفاتارات ذكور، وتم بشكل رقمي اغتصاب الأفاتار الخاص بها جماعياً، والتُقطت لها صور[٢٧].

---

(27) Brenda K. Wiederhold, Sexual Harassment in the Metaverse, CYBERPSYCHOLOGY, BEHAVIOR, AND SOCIAL NETWORKING Volume 25, Number 8, 2022, Mary Ann Liebert, Inc. P479. https://DOI: 10.1089/cyber.2022.29253.editorial.

كذلك يرى البعض أن هذه البيئة ممكن أن تكون مسرحاً لنمو الأنشطة الاحتيالية، خصوصاً مع استخدام العملات الافتراضية في العديد من التعاملات في هذه البيئة [٢٨]. وبالتالي فإن عدم ملاءمة النصوص لمثل هذه الوقائع سوف يضع القاضي أمام صعوبة تكييف الواقعة، لاسيما مع القواعد التي تحكم تفسير النص الجنائي على وجه التحديد.

٢. تحديد المسؤول جزائياً عن الأنشطة الإجرامية وتطبيق العقوبات: في العالم السيبراني تعد مشكلة تحديد المسؤول جزائياً من المسائل الشائكة، كون المستخدم يستطيع أن يختبئ وراء شبكات ال VPN على سبيل المثال، أو يتخذ صورة رمزية في بيئة الميتافيرس أو غير ذلك من الوسائل التي قد يصعب فيها تحديد هوية المستخدم، خصوصاً مع اتجاه بعض الفقهاء إلى إمكانية مساءلة الآلة الذكية أو الروبوتات[٢٩].

والرأي الذي نراه صواباً أنه لابد من مساءلة الإنسان عن الأخطاء التي تقع من الآلة جنائياً أو حتى مدنياً، إذ إن سيطرة الإنسان مهمة جداً، وإلا لا معنى للتفكير بالمسؤولية بشكل مستقل عنه[٣٠]، لذلك هناك ضرورة الاعتراف بالشخصية القانونية للكيانات الآلية الذكية تماماً كما هو الحال لمسؤولية الشخص الاعتباري أو المعنوي الذي أصبح من الشخصيات القانونية التي يسند إليها الاتهام في المخالفات التي تقع لحسابها أو باسمها.

---

(28) Simon Mackenzie, Criminology Towards the Metaverse: Cryptocurrency Scams, Grey Economy and the Technosocial, The British Journal of Criminology, 2022, 62, P1545.
https://doi.org/10.1093/bjc/azab118

(٢٩) للمزيد من التفاصيل راجع في الآراء لدى د. يحيى إبراهيم دهشان، المسؤولية الجنائية عن جرائم الذكاء الاصطناعي، مجلة الشريعة والقانون، كلية القانون، جامعة الإمارات العربية المتحدة، العدد ٨٢، إبريل ٢٠٢٠م، ص٢٠. ود. أيمن محمد الأسيوطي، الجوانب القانونية لتطبيق الذكاء الاصطناعي، الطبعة الأولى ٢٠٢٠م، دار مصر للنشر والتوزيع، القاهرة، ص١٣٩. وانظر حول ذلك أيضاً:
Gabriel hallevy, Liability for Crimes Involving Artificial Intelligence Systems, Springer, Switzerland, P14. John. Kingston, Artificial Intelligence and Legal Liability, International Conference on Innovative Techniques and Applications of Artificial Intelligence SGAI 2016: Research and Development in Intelligent Systems XXXIII, P270.

(30) Radutniy Oleksander Eduardovich , Criminal Liability of the Artificial Intelligence, Problems of Legality, 2017, Issue 138, P139.

فالآلة الذكية ممكن أن تصبح محلاً للمساءلة، طالما كانت قادرة على اكتساب السلوكيات المحيطة بها أو فهم وحل المشكلات المعرفية أو غير ذلك من تصرفات يمكن القول بأن الآلة عالمة بها، ولكن يصعب تصور الإرادة فيها، وهي الأساس في قيام المسؤولية الجنائية، كما يصعب فرض العقوبة على الآلة لتحقيق فكرة الردع بشقيه العام والخاص.

٣. **تحديد الولاية القضائية والقانون الواجب التطبيق:** الجرائم السيبرانية –كما بينا سابقاً– جرائم ذات طابع دولي؛ حيث تخطت أبعادها قدرة القوانين الجزائية على مواجهة الجرائم التي تقع من الخارج، فهذه القوانين تضع سيادتها في إقليم الدولة فقط، فلا تثور أي مشكلة إذا وقعت الجريمة داخل إقليم الدولة، أي إذا كانت الجريمة المرتكبة قد وقعت داخل إقليم الدولة بصرف النظر عن جنسية الأطراف الموجودين داخل الإقليم، حيث يكون القانون الواجب تطبيقه هو القانون الوطني، كما أن القضاء الوطني يكون أيضاً مختصاً في النظر في ملابسات الواقعة.

ولكن تبدو الصعوبة فيما لو ارتكبت الجريمة من خارج إقليم الدولة، وتحققت آثارها في الداخل أو العكس ارتكبت خارج إقليم الدولة، ووقعت آثارها داخل الإقليم، فقد يكون السلوك جريمة في بلد، ولا يكون كذلك –أي أنه مباح– في بلد آخر، وهذا الأمر من شأنه أن يعيق حتى العمل القضائي[٣١]، فهذه المسألة تحتاج إلى معالجة قانونية حقيقية على المستوى الدولي أولاً، ثم بعد ذلك معالجة القوانين الداخلية أو الوطنية، وفقاً لما يتم الاتفاق عليه.

---

[٣١] مسعد علي الصباحي الكندي، القانون الواجب التطبيق على الجريمة الإلكترونية، الطبعة الأولى، ٢٠١٩م، أوراق للنشر والتوزيع، دولة الإمارات العربية المتحدة، ص١٣. وانظر حول ذلك أيضاً:

Calderoni, Francesco, The European legal framework on cybercrime: striving for an effective implementation. Crime, Law and Social Change, 54(5), 339-357.
https://doi.org/10.1007/s10611-010-9261-6

ثانياً- الإشكاليات الإجرائية:

واجهت دول العالم إشكاليات إجرائية للحد من الجرائم السيبرانية بوصفها البسيط، ومما لا شك فيه سوف تواجه صعوبة أكثر لمواجهتها بعد توظيف خوارزميات الذكاء الاصطناعي فيها، ويمكن إجمال هذه الإشكالات على النحو الآتي:

١. إثبات الأدلة المتحصلة في الجرائم السيبرانية وحجيتها أمام القضاء: مع اعتماد الدول على التكنولوجيا الحديثة في معظم التعاملات وتطور آليات إنجازها والحاجة إلى استمرار تدفق البيانات التي يتم معالجتها رقمياً عبر الأنظمة الرقمية، يمكن القول بأنه أصبح من السهل الحصول على الأدلة لإثبات بعض الوقائع الإجرامية التي يرتكبها الجناة في الفضاء السيبراني؛ كالصور والمقاطع والنصوص، وإلى غير ذلك من محتوى رقمي يمكن تقديمه للقضاء كأدلة لها حجية لإثبات الواقعة الإجرامية تماماً كالدليل التقليدي.

إلا أن التطور التكنولوجي أوجد مشكلة حقيقية تتمثل في القدرة على التلاعب في المحتوى الرقمي من خلال تطبيقات التزييف العميق التي أشرنا إليها سابقاً، فهذه التطبيقات وبفضل تكنولوجيا الذكاء الاصطناعي أصبح من الممكن جعل المحتوى المزيف سواء كان صورة أو صوتاً أو مقطعاً يتشابه تماماً مع المحتوى الحقيقي[٣٢]، الأمر الذي يمكن الجناة من ارتكاب جرائم عديدة عبر هذه التطبيقات؛ كانتحال شخصية الغير أو التشهير بقصد الإساءة للغير أو نشر الأخبار المزيفة أو الشائعات بقصد التأثير على الرأي العام في قضايا معينة.

وعلى الرغم من خطورة هذه التطبيقات؛ إلا أنها ما زالت مباحة، ويمكن تحميل برامجها من المواقع الإلكترونية المختلفة. وقد اعتمدت بعض الدول على قوانينها في مواجهة هذه

---

(32) Bobby Chesney, and Danielle Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, California Law Review, Volume 107, Issue 6, P.1758.
https://doi.org/10.15779/Z38RV0D15J

السلوكيات كالقانون الإماراتي والهندي على سبيل المثال، وهناك دول خُصصت قوانين لمكافحة هذه الأنشطة كالولايات المتحدة الأمريكية والصين[٣٣].

٢. **تعامل سلطات الضبط في مسرح الجريمة السيبرانية:** يختلف مسرح الجريمة بمفهومه التقليدي عن مسرح الجريمة السيبرانية، فالأخيرة مسرحها إما أن يكون الآلة ذاتها ولا إشكال في هذه الحالة إذ أنها تشابه المسرح التقليدي، إذ يتم ضبط الأدلة التي يمكن تحصيلها في الآلة، وبالتالي فإن الانتقال والمعاينة أمران ضروريان في هذا الإجراء، أو مسرحاً افتراضياً وهذا المسرح لا يتطلب الانتقال والمعاينة بل أن هذه الإجراءات يمكن أن تتخذ في المكان الذي يكون فيه عضو الضبط، وبالتالي فهو يتعامل مع بيئة شبكة الإنترنت ومحتوى رقمي مخزن فيه لا يمكن قراءته أو استدعاؤه إلا من خلال أدوات تقنية المعلومات، أي أننا أمام أدلة ذات طبيعة غير مادية[٣٤].

وبالتالي يجب على سلطات الضبط مراعاة طبيعة هذه الأدلة عند قيامهم بأعمالهم المتمثلة بالتفتيش وتحصيل الأدلة، وذلك لضمان عدم إخفائها أو طمسها، وأيضاً لضمان عدم التلاعب فيها على النحو السابق ذكره، ويفترض ذلك سرعة اتخاذ الإجراءات.

٣. **ملاحقة مرتكبي الجرائم السيبرانية:** إن ملاحقة مرتكبي الجرائم السيبرانية تكون بناء ما يستدل من محتوى معلوماتي يمكن بموجبه التعرف على هويتهم؛ كالعنوان البروتوكولي (IP Addresse)، أي أن التحقق من هوية الجاني يكون من خلال المعرف الرقمي، وهذا الأمر بالنسبة إلى الجرائم التي تقع من المستخدمين العاديين، أما الفئة الإجرامية الأخرى والذين عرف عنهم ذكاؤهم ومهارتهم وقدرتهم على التخفي باتخاذ تدابير واقية مثل التشفير فيصعب على أجهزة الضبط ملاحقتهم أو التعرف على هويتهم، لاسيما إذا كان منطلق الاعتداءات في بيئة الإنترنت المظلم. وكما هو الحال في البند السابق

---

(33) Julia Chen, deepfakes, September 2020.
https://asiasociety.org/sites/default/files/inline-files/Final%20Deepfake%20PDF.pdf

[٣٤] للمزيد من التفاصيل راجع د. عادل حماد عثمان، ضبط الأدلة في الجريمة المعلوماتية، رابطة الأدب الحديث، المجلد رقم ١١٣، يونيو، ٢٠١٧م، مصر، ص١٣٨.

قد يتبن لسلطات الضبط أن الجريمة وقعت من خارج إقليم الدولة، وبالتالي فإن ملاحقة الجناة وتحديد هويتهم وتعقبهم وتقديمهم للعدالة يتعارض مع مبدأ سيادة الدول.

ومما لا شك فيه أن متطلبات العدالة الجنائية تقضي تحمل الأجهزة الحكومية مسؤوليتها تجاه اكتشاف الجرائم[٣٥]، وهذا لا يتأتى إلا من خلال أمرين اثنين أولهما أن تسعى إلى تحقيق فكرة التعاون بين الدول سواء باتفاقيات دولية أو إقليمية وتفعيل أدوات المساعدة القانونية أو الأمنية بموجبها فلا يمكن مواجهة هذه الجرائم إلا من خلال تحقيق التعاون بين دول العالم. وأما الثاني أن يكون لدى سلطات الضبط مهارة كافية في التعامل مع التكنولوجيا[٣٦].

يتضح لنا مما سبق أن التطور الهائل والسريع في العالم التكنولوجي أدى إلى عجز القواعد القانونية عن مواجهة سوء استخدام أدواته؛ بسبب عدم استيعاب معظم التشريعات في دول العالم لأهمية وضع ضوابط لتطور الأدوات المختلفة، ونرى أن ذلك هو ما يفسر سبب ارتفاع الهجمات السيبرانية على النحو الذي عرضناه في مقدمة هذه الدراسة؛ حيث استغل المجرمون إمكانيات هذا التطور، لذلك نرى بأنه من الضروري فضلاً عن تحديث القواعد القانونية بما يتوافق مع التطور أن تتخذ منهجية جديدة استباقية لمواجهة هذه الجرائم، والارتقاء في مستوى الأمن السيبراني، إذ يجب التفكير والتصرف بمستوى المجرمين ذاته؛ فالدفاع فقط لم يعد الأسلوب الفعال للمواجهة، بل لابد من المبادرة في الرد على تلك الهجمات.

---

[٣٥] راجع مهيوب يوسف، وفريحة رشيد، التحري الجنائي في مسرح الجريمة الإلكترونية، مجلة القدس المفتوحة للأبحاث والدراسات، ٤٢، ٢٠١٧م، ص٥٨.

[36] Susan W. Brenner & Joseph J. Schwerha IV, Transnational Evidence Gathering and Local Prosecution of International Cybercrime, 20 J. Marshall J. Computer & Info. L. 347 (2002).

الخاتمـــة

بما أن فترة ظهور الجرائم السيبرانية تعتبر طويلة نسبياً فقد كان بإمكان المجتمع الدولي الحد من خطورتها إلا أنه وقف عاجزاً عن مواجهتها والحد من آثارها التي نالت من أمن الأفراد والدول على حد سواء، وإن عدم استيعابه الحاجة الماسة إلى تحقيق فكرة التعاون دولياً وإقليمياً هو ما أدى إلى فقد السيطرة تماماً على عجلة تطور أساليب هذه الجرائم، وارتفاع نسب الهجمات، وازديادها بشكل مخيف بفضل تكنولوجيا الذكاء الاصطناعي، التي جعلت منها جرائم ذكية ترتكب بواسطة روبوتات آلية تستطيع اتخاذ قراراتها دون أي تدخل من البشر، حتى أصبحنا أمام فوضى تكنولوجية اختلقتها الشركات التي ما زالت حتى يومنا هذا تطور وتبتكر دون أن تضع ضوابط أخلاقية لهذا التطوير، فإن عدم قدرة المجتمع الدولي على ضبط سرعة هذا التطور فضلاً عن عدم قدرة القوانين الوطنية على مواجهة تلك الجرائم لاسيما إذا وقعت خارج نطاق إقليم الدولة هو ما جعل بعض الدول تأخذ قوانينها الجنائية بمبدأ الاختصاص الجنائي العالمي، لمواجهة الجرائم التي تقع خارج إقليمها، لتمتد إلى خارج إقليم الدولة؛ كالولايات المتحدة الأمريكية وكندا وكذلك التشريعات الأوروبية كالقانون الفرنسي والسويسري[٣٧].

وأما الدول العربية فلم تكن بالمستوى الذي يحقق الطموح في مواجهة هذه الجرائم على الرغم من وجود اتفاقية عربية تعني بمكافحتها، فالجهود العربية متفرقة حيث اقتصرت على المواجهة الوطنية في بعض الدول من خلال تعديل قواعدها القانونية مع العجز الواضح على المستوى الدولي والإقليمي أيضاً.

لذلك نرى من الضروري مواجهة هذه الجرائم بقانون دولي موحد فمهما بلغت القوانين الوطنية من تطور لقواعدها لن تكون قادرة على مواجهة هذه الجرائم بشكل فعال لاسيما مع اعتماد الدول على الرقمنة في بنيتها التحتية لأنها سوف تتعرض –بطبيعة الحال–

---

[٣٧] للمزيد من التفاصيل راجع لحبيب النعيمي، العدالة الجنائية الدولية والسيادة الوطنية بالإشارة إلى الحالة العربية، الطبعة ١ ٢٠٢٢، دراسات الوحدة العربية، بيروت، ص٢١٧.

للتهديدات السيبرانية كفايروس الفدية على سبيل المثال الذي وُصف بالكارثة الإلكترونية حيث اجتمعت دولٌ لمواجهة خطورته على أمنها الرقمي(٣٨).

لذلك يجب أن يكون هناك فهماً واستيعاباً أكثر للربط بين الجرائم السيبرانية والحاجة إلى تطوير القواعد القانونية ومنظومة الأمن السيبراني، ومن هذا المنطلق نوصي بالآتي:

١- أن يكون هناك قانون دولي موحد لمواجهة الجرائم السيبرانية لعل ذلك يسهم في تعزيز فكرة التعاون الدولي والإقليمي لمكافحتها ويوحد سياسة المواجهة.

٢- دراسة مدى إمكانية منح المحكمة الجنائية الدولية اختصاص النظر في الجرائم التي تقع خارج إقليم الدول، فلعل ذلك يضمن معالجة مبدأ الاختصاص من ناحية، ويكمل وجهة نظرنا في تبني قانون موحد لمكافحة هذه الجرائم من ناحية أخرى.

٣- أن تقوم الجهات الدولية والإقليمية بإيجاد الحلول الضامنة لمعالجة فوضى عمليات التطوير التكنولوجي المستمر دون ضوابط مما جعل الأمر صعباً على الأدوات القانونية والأمنية.

٤- أن تساير الدول العربية ما قامت به الدول الأوروبية من جهود واضحة نظمت فيها أوجه التعاملات في البيئة السيبرانية من خلال وضع ضوابط ولوائح تبين سياسة التعامل في هذه البيئة، وأهمها على الإطلاق لائحة البيانات الشخصية والقانون المدني للروبوتات والذكاء الاصطناعي.

٥- تغير منهجية الأمن السيبراني من أسلوب الدفاع إلى المبادرة بالرد على الهجمات، فالمنهجية القديمة لم تعد فعالة، إذ يمكن أيضاً استغلال الذكاء الاصطناعي في هذه المواجهة.

---

(38) Jenna McLaughlin, White House brings together 30 nations to combat ransomware, October 13, 2021.
https://www.npr.org/2021/10/13/1045248842/white-house-brings-together-30-nations-to-combat-ransomware

المراجـــع

أولاً- مراجع باللغة العربية:

- أسامة أحمد المناعسة وجلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية- دراسة مقارنة، الطبعة الثانية، ٢٠١٤م، دار الثقافة للنشر والتوزيع، عمان، المملكة الأردنية الهاشمية.
- أشرف محمد زيدان وسيف السويدي، العالم ما وراء التقليدي "ميتافيرس"، الطبعة الثانية، ٢٠٢٢م، دار الأصالة للنشر والتوزيع، الجمهورية التركية – إسطنبول.
- أيمن عبد الله فكري، جرائم نظم المعلومات – دراسة مقارنة، ٢٠٠٧م، دار الجامعة الجديدة، الإسكندرية.
- أيمن محمد الأسيوطي، الجوانب القانونية لتطبيق الذكاء الاصطناعي، الطبعة الأولى ٢٠٢٠م، دار مصر للنشر والتوزيع، القاهرة.
- إيهاب خليفة، مجتمع ما بعد المعلومات- تأثير الثورة الصناعية الرابعة على الأمن القومي، مركز المستقبل للأبحاث والدراسات المتقدمة، الطبعة الأولى، ٢٠١٩م، العربي للنشر والتوزيع، القاهرة.
- حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت – دراسة مقارنة، الطبعة الأولى ٢٠٠٩، دار النهضة العربية، القاهرة.
- خالد ممدوح إبراهيم، التنظيم القانوني لتقنية الميتافيرس، الطبعة الأولى، ٢٠٢٣م، دار الفكر الجامعي، الإسكندرية.
- عادل حماد عثمان، ضبط الأدلة في الجريمة المعلوماتية، رابطة الأدب الحديث، المجلد رقم ١١٣، يونيو، ٢٠١٧م، مصر.
- عمار عباس الحسيني، جرائم الحاسوب والإنترنت – الجرائم المعلوماتية، الطبعة الأولى، ٢٠١٧م، منشورات زين الحقوقية، بيروت.
- رامي متولي القاضي، مكافحة الإجرام المنظم عبر شبكة الإنترنت المظلمة، بحث منشور في المجلة الجنائية القومية، المجلد ٦٤، العدد ٣، نوفمبر ٢٠٢١م.

- سوسن طه ضليمي ود. ماجد محمد أبو شرحة، استخدام نماذج الذكاء الاصطناعي في تطبيقات إدارة المعرفة، الطبعة الأولى، ٢٠٢١م، القاهرة.
- لحبيب النعيمي، العدالة الجنائية الدولية والسيادة الوطنية بالإشارة إلى الحالة العربية، الطبعة ١، ٢٠٢٢م، دراسات الوحدة العربية، بيروت.
- محمد عبد الوهاب العزاوي، الثورة الصناعية الرابعة: رؤية عربية لتحديات المستقبل، الطبعة الأولى، ٢٠٢١م، المنظمة العربية للتنمية الإدارية، جامعة الدول العربية.
- مسعد علي الصباحي الكندي، القانون الواجب التطبيق على الجريمة الإلكترونية، الطبعة الأولى، ٢٠١٩م، أوراق للنشر والتوزيع، دولة الإمارات العربية المتحدة.
- مهيوب يوسف، وفريحة رشيد، التحري الجنائي في مسرح الجريمة الإلكترونية، مجلة القدس المفتوحة للأبحاث والدراسات، ٤٢، ٢٠١٧م.
- داوود الباز، الحكومة الإلكترونية وأثرها على النظام القانوني للمرفق العام، منشأة المعارف، الإسكندرية، ٢٠٠٧م.
- وليد بن صالح، الإنترنت المظلم والعملات الافتراضية: التحديات الجديدة للقانون الجنائي، مجلة كلية القانون الكويتية العالمية، العدد رقم ٣ الجزء الثاني– أكتوبر ٢٠١٨م، الكويت.
- يحيى إبراهيم دهشان، المسؤولية الجنائية عن جرائم الذكاء الاصطناعي، مجلة الشريعة والقانون، كلية القانون، جامعة الإمارات العربية المتحدة، العدد ٨٢، إبريل ٢٠٢٠م.

ثانياً– مراجع باللغة الإنجليزية:

- Joanna Świątkowska, Tackling cybercrime to unleash developing countries'digital potential, The European Cybersecurity Forum - CYBERSEC and AGH University of Science and Technology 2020.
- Jonathan Clough, Principles of Cybercrime, 2 edition, 2015, Cambridge University Press, UK.
- Marco Gercke, Understanding Cybercrime: Phenomena, Challenges and Legal Response, ITU, September 2012.19

- David Sutton, Cyber Security: A practitioner's guide, 2007 BCS Learning & Development Ltd, UK.
- Don B. Parker, Fighting Computer Crime – A New Framework for Protecting Information, 1998, Wiley, USA.
- Debarati Halder, Cyber Victimology- Decoding Cyber-crime Victimisation, 2022, Routledge, UK.
- Thomas J.Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar, Cybercrime and Digital Forensics, 2015, Routledge, UK.
- Kristin Finklea, Dark Web, Congressional Research Service, March 10, 2017, USA.
- Klaus Schwab, The Fourth Industrial Revolution, 2016, Geneva, Switzerland.
- Mark Skilton and Felix Hovsepian, the 4th Industrial Revolution Responding to the Impact of Artificial Intelligence on Business, 2018, Palgrave Macmillan, Switzerland.
- Jerry Kaplan, Artificial Intelligence: What Everyone Needs to Know, Oxford University Press; 1st edition – 2016, USA.
- Flynn Coleman: A Human Algorithm: How Artificial Intelligence Is Redefining Who We Are Hardcover – October 1, 2019, Counterpoint, USA.
- Susan W. Brenner & Joseph J. Schwerha IV, Transnational Evidence Gathering and Local Prosecution of International Cybercrime, 20 J. Marshall J. Computer & Info. L. 347 (2002).
- Melodena Stephens, METAVERSE AND ITS GOVERNANCE, The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue, New York, June 2022. United States of America.
- Brenda K. Wiederhold, Sexual Harassment in the Metaverse, CYBERPSYCHOLOGY, BEHAVIOR, AND SOCIAL NETWORKING Volume 25, Number 8, 2022, Mary Ann Liebert, Inc. https://DOI: 10.1089/cyber.2022.29253.editorial.
- Simon Mackenzie, Criminology Towards the Metaverse: Cryptocurrency Scams, Grey Economy and the Technosocial, The British Journal of Criminology, 2022, 62. https://doi.org/10.1093/bjc/azab118

- Gabriel hallevy, Liability for Crimes Involving Artificial Intelligence Systems, Springer, Switzerland.
- John. Kingston, Artificial Intelligence and Legal Liability, International Conference on Innovative Techniques and Applications of Artificial Intelligence SGAI 2016: Research and Development in Intelligent Systems XXXIII.
- Radutniy Oleksander Eduardovich, Criminal Liability of the Artificial Intelligence, Problems of Legality, 2017, Issue 138.
- Grönlund, Åke and Horan, Thomas A. (2005) "Introducing e-Gov: History, Definitions, and Issues," Communications of the Association for Information Systems (AISeL): Vol. 15, 2004 Article 39. DOI: 10.17705/1CAIS.01539
- Calderoni, Francesco, The European legal framework on cybercrime: striving for an effective implementation. Crime, Law and Social Change, 54(5). https://doi.org/10.1007/s10611-010-9261-6
- Bobby Chesney, and Danielle Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, California Law Review, Volume 107, Issue 6. https://doi.org/10.15779/Z38RV0D15J
- Julia Chen, deepfakes, September 2020. https://asiasociety.org/sites/default/files/inline-files/Final%20Deepfake%20PDF.pdf
- Jenna McLaughlin, White House brings together 30 nations to combat ransomware, October 13, 2021. https://www.npr.org/2021/10/13/1045248842/white-house-brings-together-30-nations-to-combat-ransomware

ثالثاً– مصادر أخرى:

- الموقع الإلكتروني للإسكوا – الأمم المتحدة على الرابط الآتي:

https://archive.unescwa.org/ar/tenth-united-nations-congress-prevention-crime-and-treatment-offenders

- الموقع الإلكتروني مجلة ventures cybersecurity:

https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

- تقرير شركة mimecast:

https://www.mimecast.com/resources/ebooks/the-state-of-email-/security-2023/download

- موقع منتدى الاقتصادي العالمي:

https://www.weforum.org/agenda/2022/07/global-cybersecurity-outlook-davos-2022/

- تقرير شركة IBM:

https://www.ibm.com/reports/data-breach

- الموقع الإلكتروني A. James Clark School of Engineering جامعة ميرلاند:

https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

- الموقع الإلكتروني لمركز Statista للأبحاث:

https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

- تقرير على الموقع الإلكتروني التوعوي sosafe-awareness

https://sosafe-awareness.com/resources/reports/cybercrime-trends-2023/

- الموقع الإلكتروني لشركة Comparitech:

https://www.comparitech.com/internet-providers/cyberbullying-statistics/

- Australian Government, Attorney General's Department, National Plan to Combat Cybercrime, 18. http://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Documents/National%20Plan%20to%20Combat%20Cybercrime.pdf,
- Next Move Strategy Consulting, New York, Jan. 30, 2023. https://www.nextmsc.com/report/cyber-security-market