

الجرائم الإلكترونية في ظل جائحة COVID-19 Cybercrime in light of the COVID-19 pandemic

تاريخ القبول: 2025/06/07

تاريخ الإرسال: 2025/03/15

COVID-19 في تصاعد هذه الجرائم، حيث أدى الاعتماد المتزايد على الإنترنت إلى خلق فرص جديدة للمجرمين لاستهداف قطاعات حيوية، مثل الصحة والتمويل والبنية التحتية الرقمية، ونتيجة لذلك ارتفعت معدلات الهجمات السيبرانية بشكل ملحوظ، مما دفع الدول والمنظمات إلى تبني استراتيجيات لمكافحةها.

وقد توصلت الدراسة إلى أن الجرائم الإلكترونية باتت أكثر تعقيدا بسبب التطور التكنولوجي، مما يستدعي تحديث التشريعات لمواكبة هذه التطورات، وتعزيز التعاون الدولي لمكافحة الجرائم السيبرانية العابرة للحدود.

الكلمات المفتاحية: الجريمة الإلكترونية؛ الفضاء السيبراني؛ اختراق؛ تحديات؛ كوفيد-19.

Abstract:

This study aims to shed light on cybercrimes as one of the growing security challenges in the digital age,

وغليسي أحلام*
جامعة سطيف 2
University of Setif 2
مخبر دراسات وأبحاث حول المجازر الاستعمارية
a.ouaghlici@univ-setif2.dz

ملخص:

تهدف هذه الدراسة إلى تسليط الضوء على الجرائم الإلكترونية باعتبارها أحد التحديات الأمنية المتنامية في العصر الرقمي، مع التركيز على تصاعدها خلال جائحة COVID-19، حيث أدى الاعتماد الواسع على التكنولوجيا في مختلف المجالات، مثل التعليم والعمل عن بُعد والخدمات المصرفية، إلى خلق بيئة خصبة لانتشارها، مما زاد من خطورتها على الأفراد والمؤسسات والدول.

استعرضت الدراسة مفهوم الجرائم الإلكترونية، والفرق بينها وبين الجرائم التقليدية، مع تسليط الضوء على تناميها في العصر الرقمي، كما ناقشت تأثير جائحة

with a particular focus on their surge during the COVID-19 pandemic. The widespread reliance on technology across various sectors, such as

*- المؤلف المراسل.

education, remote work, and banking services, has created a fertile environment for cybercrime to thrive, increasing its risks to individuals, institutions, and nations.

The study examines the concept of cybercrime and its distinction from traditional crimes, highlighting its rapid expansion in the digital era. It also explores the impact of COVID-19 on the rise of cybercrime, as increased internet dependence has provided new opportunities for criminals to target critical sectors such as healthcare, finance, and digital infrastructure. As a result, cyberattacks have significantly escalated, prompting governments

and organizations to adopt strategies to counter these threats.

The study concludes that cybercrimes have become increasingly complex due to technological advancements, necessitating the continuous updating of legal frameworks to keep pace with these developments. Additionally, it emphasizes the importance of strengthening international cooperation to combat cross-border cyber threats effectively.

Keywords: Cybercrime; Cyberspace; Hacking; Challenges; Covid-19

مقدمة:

أصبحت الجرائم الإلكترونية من القضايا التي تحظى باهتمام متزايد من قبل الدول، نظرا لتداعياتها الخطيرة على الأفراد والمؤسسات والبنى التحتية الرقمية، حيث باتت تشكل تهديدا للأمن الاقتصادي والاجتماعي وحتى الأمن القومي. ومع تفشي جائحة COVID-19، التي ظهرت لأول مرة في مدينة ووهان الصينية أواخر عام 2019، شهد العالم تحولا رقميا غير مسبوق، إذ اعتمدت الدول والأفراد بشكل مكثف على التكنولوجيا الحديثة في مختلف الأنشطة اليومية، مثل العمل والتعليم عن بُعد، والخدمات المصرفية، والتجارة الإلكترونية، مما أدى إلى زيادة هائلة في استخدام الإنترنت على المستوى العالمي.

وقد وُقر هذا التحول السريع بيئة مواتية لازدهار الجرائم الإلكترونية، حيث استغل المجرمون الرقميون هذا الاعتماد المتزايد على الفضاء السيبراني لشن هجمات واسعة النطاق، مستهدفين الأفراد والشركات وحتى الأنظمة الحكومية، كما شهدت هذه الفترة تطورا ملحوظا في أساليب الجريمة الإلكترونية، حيث أصبح بالإمكان



شراء مجموعة واسعة من الخدمات غير القانونية عبر مواقع الإنترنت العميق (*Dark Web*) ومنتديات القراصنة، مما سهل على المجرمين تنفيذ عملياتهم بسرية تامة بفضل تقنيات التشفير والتخفي، الأمر الذي زاد من صعوبة تعقبهم ومحاسبتهم. وفي ظل هذا التهديد المتنامي، أصبح تعزيز الأمن السيبراني أولوية قصوى، مما دفع الدول والمنظمات الدولية إلى تبني استراتيجيات متطورة لمكافحة الجرائم الإلكترونية.

- **إشكالية الدراسة:** عرفت الجرائم الإلكترونية ارتفاعا ملحوظا في ظل جائحة الوباء التي ضربت العالم عام 2019 (كوفيد-19)، وبناء على ذلك يمكن طرح الإشكالية التالية: **كيف ساهم فيروس كوفيد-19 في تنامي ظاهرة الجريمة الإلكترونية؟**

- **هدف الدراسة:** تهدف هذه الدراسة إلى تحديد مفهوم الجريمة الإلكترونية وأنواعها، كما تستهدف الدراسة الكشف عن القطاعات المتضررة بالجرائم الإلكترونية خلال أزمة كوفيد-19، والطريقة التي تعاملت بها الحكومات والمنظمات لمواجهة ذلك.

- **منهج الدراسة:** لدراسة الموضوع تم الاعتماد على المنهج الوصفي لوصف ظاهرة "الجريمة الإلكترونية" وتوضيح طبيعتها، كما تمت الاستعانة بالمنهج التحليلي لدراسة العلاقة التي تربط بين جائحة COVID-19 وتزايد الجرائم الإلكترونية، وتحليل القطاعات الأكثر استهدافا.

- **خطة الدراسة:** تم تقسيم الدراسة إلى محورين كآلاقي:

المحور الأول: ماهية الجريمة الإلكترونية

أولا: تعريف الجريمة الإلكترونية.

ثانيا: الفرق بين الجرائم التقليدية والجرائم الإلكترونية

ثالثا: أنواع الجريمة الإلكترونية.

المحور الثاني: الجريمة الإلكترونية في ظل COVID19

أولا: تنامي الجريمة الإلكترونية في ظل فيروس كوفيد-19.

ثانيا: القطاعات المستهدفة بالجريمة الإلكترونية في ظل فيروس كوفيد-19.
ثالثا: الاستجابات الدولية والمؤسسية لمكافحة الجريمة الإلكترونية خلال جائحة كوفيد-19.

المحور الأول: ماهية الجريمة الإلكترونية:

أولا- تعريف الجريمة الإلكترونية:

لا يوجد اتفاق بين الباحثين في تقديم تعريف موحد للجريمة الإلكترونية، وذلك راجع إلى الأساس الفكري الذي ينطلقون منه، حيث تعتبر الجريمة الإلكترونية من بين الجرائم التي تباينت تسمياتها عبر مراحل زمنية لتطورها المرتبط بتقنية المعلومات، حيث بدأ تسميتها "بإساءة استخدام الكمبيوتر"، ثم احتيال الكمبيوتر، ثم الجريمة المعلوماتية، بعدها "جرائم الكمبيوتر" و"الجريمة المرتبطة بالكمبيوتر"، ثم الجرائم التقنية العالية، إلى "جرائم الهاكرز"، فجرائم الإنترنت، وأخيرا *Cyber crimes*⁽¹⁾، والملاحظ أن مصطلح الجريمة الإلكترونية *Cyber crimes* يتكون من مصطلحين⁽²⁾:

- الجريمة *Crime*: السلوكيات والأفعال الخارجة عن القانون.

- الإلكترونية *Cyber*: جزء من الحاسوب أو عصر المعلومات.

ويعرف أصحاب التوجه التقني الجريمة الإلكترونية على أنها: "نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود".

أما أصحاب القانون بصفة عامة فيعرفونها على أنها "أي فعل أو سلوك يتم إتيانه بواسطة الحواسيب ووسائل الاتصالات والأجهزة الرقمية الموصولة بالإنترنت، والجريمة الإلكترونية لها نفس عناصر الجريمة التقليدية، بحيث يكون المجرم أو الضحية شخصا طبيعيا أو شخصا معنويا أو اعتباريا أو حكما"⁽³⁾.



الجرائم الإلكترونية هي أفعال غير قانونية تُرتكب باستخدام الأجهزة الإلكترونية أو شبكة الإنترنت، وتتطلب معرفة متخصصة بتقنيات الحاسوب ونظم المعلومات؛ سواء لتنفيذها أو للتحقيق فيها وملاحقة مرتكبيها قضائياً.⁽⁴⁾

كما تعرف الجرائم الإلكترونية على أنها تلك الجرائم الناتجة عن استخدام المعلوماتية والتقنية الحديثة المتمثلة بالكمبيوتر والإنترنت، في أعمال وأنشطة إجرامية، بهدف أن تحقق عوائد مالية ضخمة عبر شبكة الإنترنت، أو تداول الأسهم وممارسة الأنشطة التجارية عبر هذه الشبكة، التي تحمل أرقاماً سرية بالشراء. وقد عرفها خبراء المنظمة الأوروبية للتعاون الاقتصادي بأنها "كل سلوك غير مشروع يرتبط بالمعالجة الآلية للبيانات أو نقلها".⁽⁵⁾

والجريمة الإلكترونية نوعان، فهي إما أن تكون جرائم موجهة ضد الحاسوب الآلي قصد إتلاف أو تدمير تقنية المعلومات والاتصالات، أو ممكن أن تستخدم هذه الأجهزة من أجل ارتكاب جرائم الاحتيال وسرقة الهويات والأرصدة المالية، وسرقة حقوق الملكية الفردية، والابتزاز والتحرش وغيرها.⁽⁶⁾

ويمكن تصنيف أبرز أساليب الجرائم الإلكترونية على النحو التالي:⁽⁷⁾

1- تخريب المعلومات وإساءة استخدامها: يشمل تدمير قواعد البيانات، وتمزيق الكتب، وتخريف المعلومات والسجلات الرسمية، مما يؤدي إلى فقدان البيانات أو تشويهها.

2- سرقة المعلومات: تتضمن بيع أو تخريب أو تدمير بيانات حساسة، مثل البحوث والدراسات المهمة ذات الصلة بالتطوير التقني أو الصناعي أو العسكري.

3- تزوير المعلومات: يشمل اختراق الأنظمة التعليمية وتغيير البيانات، مثل تعديل الدرجات الأكاديمية والتلاعب بالسجلات.

4- انتهاك الخصوصية: تتمثل في نشر معلومات شخصية عن الأفراد دون إذن، أو اختراق حساباتهم الإلكترونية وتسريب بياناتهم الخاصة.

- 5- **التنصت:** يتضمن الوصول غير المصرح به إلى قواعد البيانات، والتجسس على المحادثات الهاتفية، وسرقة الاتصالات الخاصة.
- 6- **التجسس:** يهدف إلى اعتراض المعلومات، وكشف تفاصيل أنشطة الأفراد بطرق غير مشروعة.
- 7- **التشهير:** يُستخدم لتشويه سمعة الأفراد، من خلال نشر معلومات شخصية أو ذات صلة بسلوكيات غير قانونية بهدف الإضرار بسمعتهم.
- 8- **السرقية العلمية:** تشمل الاستيلاء غير المشروع على الكتب والأبحاث الأكاديمية، خصوصاً تلك التي تتضمن تجارب علمية أو تطبيقية.
- 9- **سرقة الاختراعات:** يتمثل في الاستحواذ غير القانوني على الابتكارات العلمية بهدف بيعها أو استغلالها لأغراض تجارية أو بحثية.
- 10- **الاختراق غير القانوني للشبكات:** يتمثل في الوصول غير المصرح به إلى الأنظمة الإلكترونية بهدف التخريب، التجسس، أو سرقة المعلومات لتحقيق مكاسب غير مشروعة.
- 11- **قرصنة البرمجيات:** تشمل النسخ غير القانوني للبرامج، واستخدامها أو بيعها دون إذن من أصحاب الحقوق.
- 12- **سرقة البيانات والمعلومات:** تتضمن اعتراض البيانات الحساسة، مثل أرقام البطاقات الائتمانية، الحسابات المصرفية، وكلمات المرور، بهدف استغلالها أو بيعها.
- 13- **الاحتيال المالي عبر البطاقات:** يشمل الاستخدام غير المشروع لبطاقات التسوق المالية، والهاتف، إضافةً إلى سرقة أرقامها والمتاجرة بها، مثل استخدام أرقام بطاقات الائتمان في عمليات دولية غير قانونية.
- 14- **الإرهاب الإلكتروني (Cyber Terrorism):** يمارسه أفراد أو مجموعات تستهدف الحكومات أو المنظمات عبر الهجمات الإلكترونية على الأجهزة والشبكات، سعياً لتحقيق أهداف سياسية أو اجتماعية.⁽⁸⁾

ثانيا- الفرق بين الجرائم التقليدية والجرائم الإلكترونية:

مع تطور المجتمعات وتغير أساليب الجريمة، لم تعد التهديدات الأمنية تقتصر على الأفعال التقليدية مثل العنف السياسي، الفساد، والجريمة المنظمة، بل ظهرت جرائم جديدة تستغل التكنولوجيا لتحقيق أهدافها، فالجرائم التقليدية تعتمد على العنف المادي، بينما تستخدم الجرائم الإلكترونية أدوات رقمية مثل الهجمات السيبرانية، التجسس والتلاعب بالمعلومات، مما يجعلها أكثر تعقيدا وانتشارا.

وفيما يلي أبرز الفروقات بين الجرائم التقليدية والجرائم الإلكترونية:

المجال	الجرائم التقليدية	الجرائم الإلكترونية
من حيث المكان والزمان	تُرتكب في بيئة مادية محددة، ما يستلزم حضورا للمجرم في موقع الجريمة أثناء تنفيذها.	يمكن تنفيذها من أي مكان في العالم، وفي أي وقت عبر الإنترنت، دون حاجة إلى الحضور المادي.
من حيث التكلفة الاقتصادية	تُحدث خسائر مالية تُقدَّر بحوالي 71. تريليون دولار سنويا، وتشمل هذه الخسائر ما ينتج عن السرقة، الاحتيال المادي، وتدمير الممتلكات.	قدّرت خسائرها بأكثر من 6 تريليونات دولار سنويا، وتشمل هجمات الفدية، تسريبات البيانات، وتعطيل البنى التحتية الرقمية.
من حيث شخصية المجرم	المجرم التقليدي هو شخص يرتكب أفعالا مجرّمة باستخدام وسائل مادية في حيز مكاني وزماني محدد، مدفوعا غالبا بعوامل اجتماعية أو اقتصادية. وقد يكون فردا أو جزءا من جماعة إجرامية أو إرهابية تستخدم أدوات تقليدية.	المجرم الإلكتروني يمتلك مهارات تقنية متقدمة، وقد يعمل ضمن شبكات منظمة دولية، أو حتى برعاية جهات رسمية في بعض الحالات، وغالبا ما يكون مجهول الهوية.
من حيث الوسائل المستخدمة	تعتمد الجريمة التقليدية على وسائل مادية ملموسة (الأسلحة وأدوات الكسر والاقتحام).	تُرتكب باستخدام أدوات رقمية غير مادية، مثل البرمجيات الخبيثة، رسائل التصيد، أدوات التجسس، وبرمجيات التحكم عن بعد.
من حيث الإطار التشريعي	تخضع لمنظومات قانونية واضحة منذ عقود، وتوجد اتفاقات دولية تنظم ملاحقتها، مثل قوانين العقوبات الجنائية الموحدة.	لا تزال مواجعتها القانونية تواجه صعوبات كبيرة، أبرزها تأخر التشريعات عن مواكبة التطور الرقمي، وضعف التنسيق الدولي.

المصدر: من إعداد الباحثة بالاعتماد على:

-Yar, M: *Cybercrime and Society, A Journal of Policy and Practice*,



مجلة الباحث للدراسات الأكاديمية — المجلد 12 - العدد 02 - جوان 2025

EISSN: 2588-2368

ISSN: 2352-975X

Volume 8, Issue 3, September 2014, <https://doi.org/10.1093/police/pau024>

-Wall, D: *Cybercrime: The Transformation of Crime in the Information Age*, <https://www.researchgate.net>, date the site was viewed: (23.05.2025)

- ENISA: *Threat Landscape Report 2022*, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022> date the site was viewed: (23.05.2025).

- Siegel, L. J: *Criminology: Theories, Patterns, and Typologies*, (11th ed), Cengage Learning, 2015.

يكشف الجدول المقارن بين الجرائم التقليدية والجرائم الإلكترونية عن تحول نوعي في مصادر التهديد الأمني، حيث أن الأولى تُصنف ضمن التهديدات الملموسة المباشرة التي تستهدف الأفراد والممتلكات، بينما تمثل الثانية تهديداً غير مرئي ومعقداً، يضرب في عمق البنية المعلوماتية للدول، وهذا التمايز لا يُعد فقط شكلياً، بل يُعبر عن تحول بنيوي في مفهوم الأمن القومي المعاصر.

فبينما ترتبط الجرائم التقليدية غالباً بالعنف المادي والاضطرابات الاجتماعية، فإن الجرائم الإلكترونية تستهدف نظم المعلومات والبيانات الحساسة، ما يجعل آثارها غير مرئية فوراً لكنها عميقة، فاستهداف منظومة صحية أو مالية من خلال هجمات سببرانية لا يؤدي فقط إلى خسائر اقتصادية، بل قد يُربك وظائف الدولة ويقوض ثقة المواطن في المؤسسات.

وفي هذا الإطار، يكتسب الأمن السببراني بعداً سيادياً، لا يقل أهمية عن الأمن العسكري أو الاقتصادي، إذ أصبحت حماية الفضاء الرقمي ضرورة وطنية لضمان استمرار عمل مؤسسات الدولة، وتأمين خصوصية الأفراد، وحماية البنية التحتية الرقمية، خاصة بعد اتساع الاعتماد عليها في ظل جائحة كورونا وما بعدها. هذا التغير يفرض على الدول مراجعة منظوماتها الأمنية، بحيث لا تقتصر على حماية الحدود البرية أو الجوية، بل تمتد لتشمل الفضاء الرقمي، كما يقتضي تطوير تشريعات سببرانية قادرة على مواكبة هذا النوع من التهديدات، إلى جانب تعزيز



التعاون الدولي.

ثالثاً- أنواع الجرائم الإلكترونية:

1- جرائم تسبب الأذى للأفراد: تتضمن هذه الجرائم استهداف أفراد معينين، بهدف الحصول على معلومات حساسة، سواء المتعلقة بحساباتهم البنكية أو بياناتهم الشخصية على الإنترنت، وتشمل:

أ- انتحال الشخصية: يقوم المجرم باستدراج الضحية بطرق غير مباشرة لاستخلاص معلومات خاصة، ثم يستغلها لتحقيق مكاسب مادية أو لتشويه السمعة، مما قد يؤدي إلى الإضرار بالعلاقات الاجتماعية أو المهنية للضحية.

ب- تهديد الأفراد: يتمكن المجرم من الوصول إلى معلومات شخصية وحساسة للضحية عبر القرصنة وسرقة البيانات، ثم يستخدمها للابتزاز بغرض الحصول على الأموال أو إجبار الضحية على القيام بأفعال غير قانونية، مما قد يعرضه للخطر أو الأذى.

ت- تشويه السمعة: يستغل المجرم البيانات المسروقة، ويضيف إليها معلومات مغلوطة، ثم ينشرها عبر وسائل التواصل الاجتماعي أو يرسلها عبر البريد الإلكتروني، بهدف الإضرار بسمعة الضحية وإلحاق أذى نفسي بها.

ث- تحريض على أعمال غير مشروعة: يستغل المجرم المعلومات المسروقة لابتزاز الضحايا وإجبارهم على الانخراط في أنشطة غير قانونية، مثل الدعارة، وتجارة المخدرات، وغسيل الأموال، بالإضافة إلى جرائم إلكترونية أخرى، مما يعرضهم لمخاطر قانونية وأخلاقية جسيمة.

2- جرائم تسبب الأذى للمؤسسات: وتشمل⁽⁹⁾:

أ- اختراق الأنظمة: تتسبب الهجمات السيبرانية في أضرار كبيرة للمؤسسات، تشمل خسائر مالية، واختراق بيانات حساسة، وتعطيل الأنظمة التشغيلية، حيث يستغل المهاجمون هذه الثغرات لسرقة المعلومات واستغلالها في عمليات احتيالية،

أو تدمير البنية الرقمية للمؤسسة لتحقيق مكاسب مادية أو سياسية. كما تشمل هذه الجرائم ابتزاز الموظفين واستخدام برامج التجسس لاختراق الشبكات والسيطرة عليها، وهذه الهجمات تمثل تهديدا مباشرا للاقتصاد والأمن القومي، خاصة عند استهداف مواقع رسمية لنشر معلومات مضللة أو التحريض على أنشطة غير قانونية، مما يستدعي تعزيز تدابير الحماية السيبرانية بشكل مستمر.

ب- تدمير النظم: يتم تنفيذ هذا النوع من الهجمات باستخدام الفيروسات الإلكترونية، التي تنتشر داخل الأنظمة وتؤدي إلى اضطراب كبير وتعطيل العمليات التشغيلية. يتسبب ذلك في خسائر فادحة، خاصة عند استهداف ملفات حساسة تُعد ضرورية لإدارة وتنظيم الشركات والمؤسسات.

كما يمكن أن يشمل التدمير اختراق الخادم الرئيسي للمؤسسة، حيث يقوم المهاجمون بالوصول إلى حسابات الموظفين واستغلالها للدخول إلى الشبكة بأكملها في وقت واحد، مما يؤدي إلى شلل كامل في النظام وتعطل العمليات، مما ينعكس سلباً على سير الأعمال واستقرار المؤسسات.

3- جرائم الأموال: وتشمل: (10)

أ- الاستيلاء على حسابات البنوك: تتضمن هذه الجريمة اختراق الحسابات المصرفية للأفراد والشركات، بالإضافة إلى الحسابات الخاصة بمؤسسات الدولة والجهات الخاصة، كما تشمل سرقة بيانات البطاقات الائتمانية واستخدامها بطرق غير مشروعة للاستيلاء على الأرصدة المالية.

ب- انتهاك حقوق الملكية الفكرية والأدبية: يتمثل هذا الانتهاك في إنشاء نسخ غير قانونية من البرامج والتطبيقات وملفات الوسائط المتعددة (الملتيميديا)، ثم نشرها عبر الإنترنت دون إذن أصحابها الأصليين، مما يؤدي إلى خسائر مالية كبيرة لشركات البرمجيات وصناعة المحتوى الصوتي والمرئي.



4- الجرائم التي تستهدف أمن الدولة: وتشمل:⁽¹¹⁾

أ- برامج التجسس: تُعد برامج التجسس من أخطر التهديدات الإلكترونية التي تستهدف أمن الدولة، حيث تُستخدم لأغراض سياسية تهدد استقرار البلاد وسلامتها، حيث يقوم المجرمون بزرع هذه البرامج داخل الأنظمة الإلكترونية للمؤسسات الحيوية، مما يسمح لأعداء الوطن باختراق الأنظمة والاطلاع على معلومات حساسة، بما في ذلك المخططات العسكرية، مما يشكل تهديدا خطيرا للأمن القومي.

ب- استخدام المنظمات الإرهابية لأسلوب التضليل: تعتمد الجماعات الإرهابية على وسائل الاتصال الحديثة وشبكة الإنترنت لنشر معلومات مضللة، تهدف إلى زعزعة الاستقرار وإثارة الفوضى، لتحقيق أجندات سياسية وتنفيذ مخططات إرهابية، كما تستغل هذه المنظمات الفضاء الرقمي للتلاعب بعقول الشباب، بهدف تجنيدهم أو توجيههم نحو مصالح تخدم أجنداتها التخريبية.

المحور الثاني: الجريمة الإلكترونية في ظل COVID-19

فرض وباء كورونا الذي اجتاحت العديد من دول العالم تحديا أمنيا مرتبطا بالأمن السيبراني، فقد شهدت العديد من دول العالم هجمات إلكترونية شكلت تهديدا لأمن واستقرار الدول.

أولا- تنامي الجريمة الإلكترونية في ظل فيروس كوفيد-19:

أدى انتشار جائحة كوفيد-19 إلى إحداث تحولات جذرية في مختلف جوانب الحياة، حيث فرضت الدول تدابير احترازية مشددة، شملت الإغلاق العام والانتقال المكثف إلى البيئات الرقمية لمواصلة الأنشطة الاقتصادية والتعليمية والإدارية، ومع هذا التحول السريع برز الفضاء السيبراني كبيئة رئيسية للتفاعل، مما وفر للمجرمين الإلكترونيين فرصا غير مسبوقة لاستغلال الثغرات الأمنية، واستهداف الأفراد والمؤسسات على نطاق واسع.⁽¹²⁾

لقد شهدت الجرائم السيبرانية تصاعدا ملحوظا خلال الجائحة نتيجة لعدة عوامل، أبرزها التوسع الكبير في العمل عن بُعد، والاعتماد المتزايد على الخدمات الإلكترونية، إلى جانب ضعف تدابير الحماية الرقمية لدى العديد من الأفراد والمؤسسات، وقد استغل القراصنة حالة الخوف والارتباك التي سادت خلال الأزمة، لتنفيذ هجمات تصيد احتيالي (Phishing)، ونشر برمجيات خبيثة (Malware)، وارتكاب عمليات احتيال مالي، بالإضافة إلى شن هجمات الفدية (Ransomware) التي استهدفت قطاعات حيوية، مثل الرعاية الصحية، والمؤسسات المالية، والهيئات الحكومية.

وقد سجل عام 2020 أرقاما قياسية غير مسبوقة في حجم البيانات المخترقة والخسائر الناتجة عن الهجمات السيبرانية، حيث أفادت تقارير صادرة عن منظمات دولية، مثل الإنتربول والاتحاد الدولي للاتصالات، بأن الجرائم الإلكترونية تضاعفت بشكل ملحوظ، مع تصاعد عمليات الابتزاز الإلكتروني وسرقة الهويات الرقمية، كما أظهرت بيانات من شركات الأمن السيبراني أن معدلات الهجمات زادت بنسبة تجاوزت 300% مقارنة بالسنوات السابقة، ما شكل تهديدا متزايدا للأمن الرقمي العالمي.⁽¹³⁾

إن تسارع رقمنة الأنشطة الاقتصادية والاجتماعية دون تعزيز إجراءات الحماية الإلكترونية، جعل الفضاء السيبراني ساحة خصبة لجرائم معقدة تتجاوز الحدود الجغرافية، مما يفرض على الدول والمنظمات تكثيف الجهود لتعزيز الأمن السيبراني، من خلال تطوير البنية التحتية الرقمية، ورفع الوعي المجتمعي حول أساليب الحماية، وتعزيز التعاون الدولي لمكافحة الجرائم الإلكترونية المتزايدة.

لقد عرفت فترة جائحة كورونا العديد من الهجمات الإلكترونية، ففي إيران قامت مجاميع للقرصنة بشن العديد من الهجمات الإلكترونية على منظمة الصحة العالمية، ومراكز أبحاث بريطانية وأمريكية تسعى لإنتاج لقاحات لعلاج فيروس كورونا، حيث



قام قراصنة إلكترونيون يعملون لصالح الحكومة الإيرانية باختراق حسابات البريد الإلكتروني الشخصية لموظفين من منظمة الصحة العالمية. هذا وقد نشرت استشارية المركز الوطني للأمن السيبراني NCSC في المملكة المتحدة تفاصيل حول نشاط مجموعة تعرف باسم "APT29"، تستهدف العديد من مراكز الأبحاث في المملكة المتحدة وكندا والولايات المتحدة⁽¹⁴⁾، وتعمل بشكل شبه مؤكد كجزء من خدمات المخابرات الروسية، كما تعتمد على مجموعة من الأدوات منها البرامج الضارة المخصصة المعروفة باسم WellMess و WellMail⁽¹⁵⁾، كما ذكرت شرطة مدينة لندن في جانفي 2020 أنها فقدت أكثر من 11 مليون جنيه إسترليني في عمليات احتيال⁽¹⁶⁾.

ومن بين الهجمات الأكثر شهرة خلال الوباء هو اختراق Twitter في 15 جويلية، حيث اخترق المهاجم حسابات أشخاص مثل Apple و BILL وأوباما، ووفقا لتقرير نشرته وول ستريت جورنال، فقد تم تنفيذ الهجوم من قبل الجاني باستخدام مزيج من القرصنة التقليدية، مثل مواقع التصيد، والهندسة الاجتماعية⁽¹⁷⁾.

ومما سبق يتضح أن أزمة فيروس كورونا ساهمت في تغيير طبيعة هذه الهجمات الإلكترونية، وزيادة أعدادها، فمن المتوقع أن تزيد حدة الصراعات بين الدول، فقد سعت الدول إلى شن العديد من الهجمات الإلكترونية، وذلك بهدف التهيب أو التأثير في الدول المستهدفة، والقضاء على بنيتها التحتية ومؤسساتها الحيوية، وكذا الضغط على قادة حكومات الدول، كما قد تضطر الدول إلى خفض انفاقها الأمني خاصة في ظل بروز مفهوم جديد للأمن القومي، والذي أصبح يتضمن عناصر ومكونات جديدة تتمثل في توفير مخزون سلمي ومنشآت طبية مزودة بالآلات وكوادر طبية قادرة على التعامل مع الأزمة، مع تفعيل دور القطاع الخاص ليشترك حكومات الدول في النهوض باقتصاديات الدول.

وتجدر الإشارة أن الدول وجهت مواردها إلى معالجة المشكلات الاجتماعية والاقتصادية والأمنية التي تواجهها، وذلك باستثمار هذه الموارد في القطاعات الحيوية ومراكز الأبحاث ومؤسسات الأمن السيبراني، وغيرها من القطاعات التي تعتبر بمثابة خط الصد الأول في مواجهة هذا الوباء، فقد ضاعف انتشار وباء فيروس كورونا أهمية أمن الفضاء السيبراني، والذي أصبح من أهم الأدوات التي تعتمد عليها الدول في مواجهة تداعيات هذا الفيروس، حيث قام مكتب الاتصالات الحكومية البريطانية بالتعاون مع دوائر الاستخبارات البريطانية بتأمين التطبيقات الرقمية لمؤسسات الصحة العامة، وبينما تمكنت عدد من حكومات الدول، مثل الولايات المتحدة الأمريكية والمملكة المتحدة والصين وروسيا واليابان وكندا وغيرها من الدول، من أن تمتلك بنية تحتية جيدة، وأن تضع خططاً طارئة لحماية فضاءاتها الرقمية ضد التهديدات المحتملة، فهناك دول مازالت تفتقر إلى بنية تحتية وكوادر مدربة قادرة على مواجهة التهديدات المصاحبة لأزمة فيروس كورونا.⁽¹⁸⁾

ثانياً- القطاعات المستهدفة بالجريمة الإلكترونية في ظل فيروس كوفيد-19:

1- القطاع الصحي: يعد قطاع الرعاية الصحية أكثر القطاعات تعرضاً للهجمات الإلكترونية خلال فترة فيروس كورونا "كوفيد-19"، حيث تم استهداف المستشفيات والمراكز الطبية والمؤسسات العامة في مختلف أرجاء العالم، من خلال برامج الفدية بصورة أساسية، فنظراً لحاجة أطقم الرعاية الصحية إلى بنية تحتية رقمية لمواجهة أزمة كورونا، عمل المخترقون على استغلال هذه الثغرة، ظناً منهم أن المؤسسات الصحية ستضطر إلى الدفع لاستعادة أنظمتها، هذا وقد انتهز المخترقون الأزمة لبيع أدوات طبية مزيفة، والترويج لتوصلها لاكتشافات جديدة عن فيروس كورونا "كوفيد-19".⁽¹⁹⁾

هذا وقد تعرضت وكالة الصحة الأمريكية في 16 مارس 2020 لهجوم سيبراني أدى إلى تعطل شبكتها الداخلية، كما أفاد مستشفى برنو الجامعي في جمهورية



التشيك أنه تعرض لهجوم سيبراني (برمجيات الفدية)، ترتب عليه إلغاء العديد من العمليات الجراحية، وتحويل المرضى الجدد إلى مستشفيات قريبة⁽²⁰⁾. وتجدر الإشارة أن المكتب الوطني للاستخبارات الاحتياطية في المملكة المتحدة أبلغ عن خسائر بقيمة 1.6 مليون جنيه إسترليني بسبب الاحتيال المرتبط بفيروس كورونا، حيث دفعت ضحية واحدة 15 000 جنيه إسترليني لشراء أقنعة وهمية. هذا وقد أشارت منظمة الصحة العالمية في عدة تقارير صادرة عنها في 2020، إلى تزايد الهجمات الإلكترونية المرتبطة بفيروس كورونا، والتي كانت عرضة لها، وقد تركزت هذه الهجمات فيما يأتي:

أ- الهجوم على البنية المعلوماتية للمنظمة.

ب- اختراق الحسابات الإلكترونية للعاملين في مجال مكافحة فيروس كوفيد-19 من أطباء وصيادلة وأفراد وباحثين بيولوجيين ومسؤولين في شركات أدوية.

ت- تزوير حسابات إلكترونية باسم الصندوق التضامني للاستجابة ضد فيروس كوفيد-19، ويمثل الهدف من ذلك في الحصول على معلومات بشأن الفيروس أو الأدوية التي تعالج أعراضه، أو اللقاءات المحتملة للقضاء عليه، ومن ثم يمكن لهؤلاء المخترقين بيع هذه المعلومات لدول وأجهزة مخابرات وشركات كبرى، التي تتسابق فيما بينها للحصول على اللقاح.⁽²¹⁾

2- القطاع الاقتصادي: وفقا لدراسة جديدة من شركة الحوسبة السحابية Iomart، زادت خروقات البيانات واسعة النطاق بنسبة 237% في الربع الأول من عام 2020، مقارنة بالفترة نفسها من عام 2019، والسبب في ذلك زيادة الأعمال المصرفية والتجارة الإلكترونية في زمن كوفيد-19 عبر الإنترنت، فقد دفعت تلك الجائحة الشركات إلى التحول المفاجئ لمعظم الموظفين العاملين لديها إلى العمل من المنزل، مما اضطر الكثيرون إلى اتباع بعض الاختصارات الأمنية، وقد قدرت تلك

الدراسة حجم الخسائر الاقتصادية لقطاع الشركات الناجمة عن خرق البيانات على النحو التالي: (22)

أ- ينتج عن خرق البيانات النموذجي لشركة كبيرة فقدان البيانات ما بين 10 ملايين و99 مليون سجل، ويخفض قيمة الشركة بنسبة 7.27%، وبالنسبة للشركات الصغيرة يمكن أن يكون خرق البيانات كارثيا.

ب- ووفقا لتقرير حديث صادر عن شركة VMware، فقد ارتفع برنامج الفدية بنسبة 90%، بقيام المجرم السيبراني بتشفير الملفات، ثم يطلب فدية لاستعادة الوصول، فقد حدث في شركة صناعة السيارات اليابانية (هوندا) أن برامج الفدية أصابت الخوادم الداخلية للشركة بما في ذلك أنظمة الإنتاج، مما أجبرها على تعليق بعض إنتاجها من السيارات والدراجات النارية، كما دفعت شركة التكنولوجيا المالية الإسرائيلية Sapiens فدية بقيمة 250 ألف دولار في شكل عملة "بتكوين" بعد أن هدد المتسللون بإغلاق شبكة الشركة، كما تم استهداف الوكالات الحكومية والحكومات المحلية في الولايات المتحدة الأمريكية، فمدينة ألاباما دفعت ما يقارب 300.000 ألف دولار من عملة البتكوين بعد هجوم إلكتروني على نظام شبكة الحاسوب الخاص بها في يونيو 2020، وفي كاليفورنيا تعرضت مدينة Torrance تورانس لهجوم من برمجيات الفدية، أدى إلى تعطيل موقعها الإلكتروني والبريد الإلكتروني ونظامها المالي، وطلب المهاجمون 100 بتكوين بقيمة حوالي 70.000 دولار. (23)

هذا وقد تضمن تقرير شركة PhishLabs، أن بورصات العملات المشفرة شهدت زيادة بمقدار 10 أضعاف في الهجمات في النصف الأول من العام 2021 مقارنة بالفترة نفسها من العام السابق 2020، وأنه تم تنظيم غالبية هجمات العملات المشفرة عبر وسائل التواصل الاجتماعي، كما توقع التقرير استمرار استهداف شركات العملات المشفرة بقوة من قبل الجهات الفاعلة المهددة عبر وسائل التواصل



الاجتماعي في المستقبل، فقد تم ارتكاب أكبر عملية سرقة للعملات المشفرة في 10 أغسطس، حيث تم سرقة 613 مليون دولار من العملات الرقمية من منصة *Poly Network* لتبادل الرموز، فقط لإعادة توكنات (*tokens*) قيمتها 260 مليون دولار بعد أقل من 24 ساعة.⁽²⁴⁾

3- القطاع المالي: خلال جائحة *COVID-19*، تعرضت الأنظمة العالمية للهجوم وفقدت ملايين الدولارات من خلال الجرائم الإلكترونية، فقد تأثرت أسواق الأسهم في جميع أنحاء العالم، حيث تعرضت صناعة الخدمات المالية للهجوم من خلال التصيد والبرامج الضارة وبرامج الفدية وعمليات الخداع الاحتيالي، (مثل الاتصالات الزائفة التي يُزعم أنها من مصدر معروف وموثوق به، والتي تطلب معلومات سرية كتسجيل الدخول أو كلمة المرور أو المعلومات المصرفية)، من قبل المتسللين⁽²⁵⁾. بين فيفري وأبريل 2020، زادت الهجمات الإلكترونية والتهديدات على المؤسسات المالية بأكثر من 238٪ على مستوى العالم، في وقت كان الاقتصاد العالمي يعمل بلا كلل لمكافحة عدوى *COVID-19*، خلقت أزمة *COVID-19* مناخا مثاليا لمجرمي الإنترنت، حيث نمت هجمات برامج الفدية تسعة أضعاف في هذه الفترة، مع رسائل البريد الإلكتروني المخادعة كمصدر أساسي، وقد تزايدت الهجمات الإلكترونية والتهديدات بشكل كبير؛ لأن المجرمين الإلكترونيين (الدكاء البشري) لديهم معرفة أفضل بسياسات وإجراءات المؤسسات المالية، وبالتالي يمكنهم بسهولة تحديد النقاط العمياء للمؤسسة المالية⁽²⁶⁾.

4- خدمات مؤتمرات الفيديو والاجتماعات: خاصة فيما يتعلق بمنصات المؤتمرات والاجتماعات ومحادثات الفيديو كانت من بين الأهداف المفضلة للمخترقين خلال أزمة كوفيد-19، إذ ظهرت فيها بعض الثغرات الأمنية، مثل منصة زوم - *Zoom*، التي شهدت انضمام بعض الأشخاص عشوائيا إلى اجتماعات الفيديو وتعطيله بمحتوى غير مرغوب به، أو نشر فيديوهات مسجلة لم يتم حفظها في مساحات تخزين

سحابية آمنة، وتم نشرها بعد ذلك على شبكة الانترنت، وشمل ذلك اجتماعات عمل خاصة، ومحادثات شخصية بين عائلات وأصدقاء.⁽²⁷⁾

ثالثاً- الاستجابات الدولية والمؤسسية لمكافحة الجريمة الإلكترونية خلال جائحة

Covid-19:

دفع تزايد عدد الجرائم والهجمات الإلكترونية خلال أزمة كوفيد-19 الصحية، العديد من الدول والمنظمات والشركات إلى الإعلان عن جملة من الإجراءات والجهود التي ستتخذها وتبذلها لمواجهة الجريمة الإلكترونية، وكبحها في ظل استمرار هذه الأزمة.

1- الولايات المتحدة الأمريكية: استثمرت الولايات المتحدة بشكل مكثف في تعزيز أنظمة الحماية الإلكترونية وتطوير استراتيجيات وطنية شاملة لمكافحة الجرائم الإلكترونية، مع التركيز على حماية البيانات الشخصية وتعزيز الأمن السيبراني، حيث أعلن مجلس الشيوخ الأمريكي عن تقديم مشروع قانون جديد يهدف إلى تنظيم جمع واستخدام البيانات التي يتم الحصول عليها عبر التطبيقات الخاصة، بتتبع التلاقي بين الأفراد خلال أزمة كوفيد-19.

وبموجب "قانون حماية بيانات المستهلك خلال أزمة كوفيد-19"، ستلزم الشركات والمؤسسات الرقمية بتوفير مستويات أعلى من الشفافية حول كيفية جمع البيانات، وأماكن تخزينها، والأغراض التي تُستخدم من أجلها، مع فرض قيود مشددة على مشاركة هذه المعلومات مع جهات خارجية دون موافقة المستخدمين، وذلك بهدف تعزيز خصوصية الأفراد وحماية حقوقهم الرقمية في ظل التوسع المتزايد في تقنيات التتبع والذكاء الاصطناعي.⁽²⁸⁾

2- الاتحاد الأوروبي: كشفت المفوضية الأوروبية في 2020 عن الاستراتيجية التي سيعتمد عليها الاتحاد الأوروبي على المستويين الداخلي والخارجي لفترة 2020-2025، ولقد كان ملف الأمن السيبراني من بين أهم الأولويات، حيث أعلنت

المفوضية زيادة جهودها في التعامل مع العدد المتزايد للهجمات الإلكترونية،⁽²⁹⁾ كما أكدت مفوضة الشؤون الداخلية الأوروبية *Johansson Ylva* على الحاجة الملحة لتكثيف جهود الاتحاد الأوروبي لمكافحة الجريمة الإلكترونية، والدور الأساسي لليوروبول في هذه الجهود في ظل تزايد عدد الجرائم الإلكترونية بفعل فيروس كورونا⁽³⁰⁾.

3. دول الشرق الأوسط وإفريقيا: خلال جائحة كوفيد-19، عززت دول الشرق الأوسط استراتيجياتها لمكافحة الجرائم الإلكترونية عبر إنشاء وحدات متخصصة، وتحسين مستوى الأمن السيبراني، ففي الإمارات العربية المتحدة أطلقت الهيئة العامة لتنظيم قطاع الاتصالات وحدة الأمن السيبراني، بهدف حماية الأفراد والشركات من التهديدات السيبرانية، مثل التصيد الاحتيالي والهجمات على الأنظمة الحكومية.⁽³¹⁾

أما في المملكة العربية السعودية، فقد عززت الهيئة الوطنية للأمن السيبراني من إجراءات الحماية، وأصدرت تحذيرات دورية لمنع عمليات الاختيال الإلكتروني التي استهدفت الشركات والمواطنين أثناء الجائحة.

بالإضافة إلى ذلك شددت دول المنطقة الرقابة على منصات التواصل الاجتماعي والمواقع الإلكترونية بهدف الحد من انتشار المعلومات المضللة حول فيروس كورونا، حيث قامت مصر والأردن بفرض عقوبات صارمة على ناشري الأخبار المزيفة، التي استُخدمت كوسيلة للاختيال وسرقة البيانات⁽³²⁾، كما حرصت بعض الدول مثل قطر والكويت، على حماية البنية التحتية الحيوية من الهجمات الإلكترونية، عبر تطوير مراكز عمليات أمنية متقدمة، تراقب النشاطات المشبوهة في القطاعات الحساسة، كالصحة والتعليم والقطاع المصرفي.

أما في إفريقيا فقد برزت جهود الاتحاد الأفريقي من خلال إطلاق مبادرات لدعم الدول الأعضاء في تطوير سياسات وتشريعات قوية لمكافحة الجرائم الإلكترونية،

خاصة بعد تصاعد الهجمات التي استهدفت الأنظمة الصحية والبنية التحتية الحيوية، حيث أصدر الاتحاد الإفريقي القرار رقم 473 لعام 2021، والذي تناول تأثيرات الذكاء الاصطناعي والروبوتات والتقنيات الحديثة على حقوق الإنسان والشعوب الإفريقية، ودعا القرار المنظمات الإقليمية الفرعية في إفريقيا إلى تطوير أطر قانونية واضحة لضبط استخدام هذه التقنيات، محذرا من مخاطر الجرائم الإلكترونية، مثل التضليل الإعلامي ونشر الأخبار الكاذبة، التي تفاقمت خلال الجائحة وأسهمت في عرقلة الجهود الصحية وزعزعة الاستقرار الاجتماعي، كما أكد الاتحاد الإفريقي على ضرورة تعميق البحث العلمي في مجال الذكاء الاصطناعي وتأثيره على إفريقيا، لضمان حماية حقوق الشعوب وحرياتهما في ظل التحولات الرقمية المتسارعة التي فرضتها الأزمة الصحية العالمية.⁽³³⁾

4- منظمة الصحة العالمية: أعلنت منظمة الصحة العالمية عن اتخاذ تدابير تقنية متقدمة لتعزيز أمنها السيبراني، حيث يعمل خبراءها على تقليل الهجمات الإلكترونية التي تستهدف أنظمتها الرقمية، من خلال تطوير آليات دفاع متقدمة وتحليل التهديدات السيبرانية في الوقت المناسب، كما باشرت المنظمة في تحديث شامل لنظام المعلومات الخاص بها، بهدف تحسين مستوى الأمان وضمان حماية البيانات الحساسة المتعلقة بالصحة العامة والبحوث الطبية.

بالإضافة إلى ذلك أطلقت المنظمة عبر موقعها الرسمي حملة توعوية لمساعدة المستخدمين في تجنب عمليات الاحتيال والخداع الإلكتروني، حيث قدمت مجموعة من الإرشادات حول كيفية التعرف على محاولات التصيد الاحتيالي، وتأمين الحسابات الشخصية، وحماية البيانات الصحية من الاستغلال غير المشروع.⁽³⁴⁾

5- مؤسسات الخدمات المالية: تبنت مؤسسات الخدمات المالية تقنيات الذكاء الاصطناعي وتحليل البيانات، لتطوير نظام إنذار مبكر يكشف الاحتيال في معاملات بطاقات الائتمان، مما مكّنها من رصد الأنماط غير الطبيعية واكتشاف

الأنشطة المشبوهة بسرعة فائقة، وقد أثبت هذا النظام فعاليته بشكل خاص خلال فترة تفشي فيروس كوفيد-19، حيث شهدت المؤسسات المالية زيادة في مستوى الحماية من الاحتيال بنسبة 40%، مقارنة بالفترة السابقة، وذلك بفضل التحليل التنبئي واتخاذ القرارات الاستباقية للحد من المخاطر المالية وتعزيز ثقة العملاء.⁽³⁵⁾

خاتمة:

تمثل الجرائم الإلكترونية تحديا بارزا في العصر الرقمي، وقد ازدادت خطورتها بشكل ملحوظ خلال جائحة COVID-19، حيث استهدفت الأفراد والمؤسسات والقطاعات الحيوية، فقد وفرت ظروف الجائحة التي فرضت التباعد الاجتماعي والاعتماد المكثف على الوسائل الرقمية في مختلف جوانب الحياة، بيئة مواتية لارتفاع معدلات الجرائم الإلكترونية، وهو ما استدعى تبني تدابير صارمة للحد من انتشار هذه الجرائم، وتعزيز الأمن السيبراني على جميع المستويات لحماية البيانات والأنظمة من التهديدات المتزايدة.

ومن خلال ما تم عرضه نستنتج أن:

- 1- الجرائم الإلكترونية من أكثر الجرائم المعاصرة انتشارا التي باتت تهدد أمن الفرد والدولة معا.
- 2- تُعد أزمة فيروس كورونا من أبرز التحديات التي واجهت دول العالم، فقد خلقت هذه الأزمة نوعا جديدا من التهديدات تجسدت في هجمات الفضاء السيبراني، كما فرضت حالة من الارتباك بشأن آليات التعامل مع هذه الهجمات.
- 3- أدت الإجراءات الاحترازية من الفيروس (التباعد الاجتماعي) إلى الاعتماد على الانترنت بشكل كلي، وهو الأمر الذي أدى إلى ارتفاع نسبة الجرائم الإلكترونية.
- 4- إن مكافحة الجرائم الإلكترونية تتطلب تكاتف الجهود الوطنية والدولية في سبيل التقليل منها.

- الاقتراحات:

- 1- تعزيز التشريعات الوطنية والدولية لمكافحة الجرائم الإلكترونية، وتحديث القوانين لتواكب التطورات التكنولوجية.
- 2- تكثيف التعاون الدولي في مجال الأمن السيبراني لمواجهة التهديدات العابرة للحدود.
- 3- رفع الوعي المجتمعي حول أساليب الاحتيال الإلكتروني، وتعزيز الثقافة السيبرانية بين الأفراد والمؤسسات.

الهوامش والمراجع:

- (1)- لمياء مجدوب: الجريمة الإلكترونية، مجلة الحكمة للدراسات الإعلامية والاتصالية، العدد 13، 2018، ص 97.
- (2)- ذياب موسى البداينة: الجرائم الإلكترونية: المفهوم والأسباب، الملتقى الدولي حول: الجرائم المستحدثة في ظل المتغيرات والتحول الإقليمي والدولية، عمان، المملكة الأردنية الهاشمية، 2014، ص 3.
- (3) مصطفى إبراهيم سلمان الشمري: الجرائم الإلكترونية وتأثيرها على العراق، العراق بعد عام 2003: الدولة، المجتمع، الاقتصاد، القانون، العلاقات الخارجية، التحديات والفرص، المحرر: لقمان عمر محمود النعيمي: دار نون للطباعة والنشر والتوزيع، تكريت، 2021، ص 121.
- (4)- لمياء مجدوب: مرجع سبق ذكره، ص 98.
- (5)- مفتاح ميلاد الهديف: الجرائم الإلكترونية، مجلة التربوي، العدد 20، جانفي 2022، ص 143.
- (6)- جمال دقيش: واقع الجريمة الإلكترونية في الجزائر: دراسة تحليلية خلال الفترة 2013-2017، الملتقى الوطني حول: واقع الجريمة الإلكترونية بين مبادئ الحرية وضوابط المسؤولية، ص 4.
- (7)- ذياب موسى البداينة: مرجع سبق ذكره، ص ص 15-20.
- (8)- الجرائم الإلكترونية. احذر حاسوبك، <https://www.aljazeera.net> تاريخ التصفح: (16 نوفمبر 2022).
- (9)- "ماهي الجرائم الإلكترونية؟ أنواعها؟ كيفية تنفيذها وطرق مواجهتها" <https://www.it-pillars.com>، تاريخ التصفح: (10 مارس 2025).
- (10)- سورية ديش: أنواع الجرائم الإلكترونية وإجراءات مكافحتها، <https://democraticac.de>، تاريخ التصفح: (16 نوفمبر 2022).
- (11)- ماهي الجرائم الإلكترونية؟ أنواعها؟ كيفية تنفيذها وطرق مواجهتها، مرجع سبق ذكره.
- (12)- عماد الدين عبد الحميد: الجرائم السيبرانية في زمن كورونا وآثارها على الأمن القومي الاقتصادي، <https://www.aliqtisadalislami.net> تاريخ التصفح: (18 نوفمبر 2022).
- (13)- نفس المرجع.



(14)- *Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic*, <https://www.prnewswire.com>, 17(/ 11/ 2022).

(15)- ياسمين أحمد صالح: مرجع سبق ذكره، ص 80.

(16)- *Impact of COVID-19 on Cybersecurity*: <https://www2.deloitte.com>, At 16(/11/2022).

(17)- *Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic*, Opcit.

(18)- نفس المرجع، ص 81-82.

(19)- رضا سيف الدين جلولي: النشاط الإجرامي في ظل فيروس كورونا كوفيد-19 (تناهي ظاهرة الجريمة الإلكترونية أمودجا، مجلة العلوم الإنسانية لجامعة أم البواقي، المجلد 8، العدد 3، ديسمبر 2021، ص 279.

(20)- ياسمين أحمد صالح: مرجع سبق ذكره، ص 80.

(21)- رضا سيف الدين جلولي: مرجع سبق ذكره، ص 279.

(22)- عماد الدين عبد الحميد: مرجع سبق ذكره.

(23)- نفس المرجع.

(24)- نفس المرجع.

(25)- Joël Chigada and Rujeko Madzinga, *Cyberattaques et menaces pendant la COVID-19: une revue systématique de la littérature*, *Journal sud-africain de la gestion de l'information*, vol.23 n.1, 2021, in: <http://www.scielo.org.za>.

(26)- Ibid.

(27)- رضا سيف الدين جلولي: مرجع سبق ذكره، ص 280.

(28)- *Dubai future foundation, LIFE AFTER COVID 19: CYBERSECURITY*, p. 9. At: <https://www.dubaifuture.ae>

(29)- Nicolás, E, *EU Five-Year Security Plan to Focus on Critical Infrastructure*, At: <https://euobserver.com>, 2020(, July 27).

(30)- *Europol, Covid-19 Sparks Upward Trend in Cybercrime*, At: <https://www.europol.europa.eu>, (2020, October 05).

(31)- وكالة أنباء الإمارات، خبراء الجريمة السيبرانية يناقشون التحديات والإجراءات المستقبلية، <https://www.wam.ae/ar/details/1395302871603>، تاريخ التصفح: (8 مارس 2025).

(32)- حسينة بن رقية: انتشار الأخبار الزائفة حول فيروس كورونا على مواقع التواصل الاجتماعي بين الفراغ القانوني وتفاقم الأزمة: مقارنة نظرية تحليلية، <https://aleph.edinum.org/8803> تاريخ التصفح: (8 مارس 2025).

(33)- رباب حداداة: الجرائم الإلكترونية والأمن الرقمي في إفريقيا، <https://ciessm.org>، تاريخ التصفح: (10 مارس 2025).

(34)- رضا سيف الدين جلولي: مرجع سبق ذكره، ص 280.

(35)- نفس المرجع، ص 280.

