The Extent of the Need to Establish a Criminal Judiciary Specialized in Examining Technical Crimes A comparative study[#]

Dr. Abd Elraoof Hasan A. Elhaded [(1)*] Dr. Tarek Elsayed Mahmoud[(2)]

(1) Researcher,Assistant Professor Civil Law

(2) Researcher, Assistant Professor of Criminal Law.

Received: 1/2/2026

Accepted: 10/5/2026

Published: 23/7/2026

* *Corresponding Author:*
abdelraouf1969@gmail.com
Tarek.Mshmoud@uoa.edu.iq

DOI:
https://doi.org/10.59759/law.v5i2.1838

Abstract

The rapid and successive development in the field of information technology, and the successive development in the industry of artificial intelligence technologies, have led to the emergence of many patterns of criminal behavior that are completely different from the patterns of behavior in traditional crimes, as they are characterized by their ease and low cost. Additionally, their danger in some cases may exceed the danger of traditional crimes. Furthermore, this type of newly established crimes is not limited by geographical boundaries, as they cross borders. Therefore, legislators in various countries around the world have directed their efforts towards enacting special legislation and laws that aim to combat this type of crimes.

Undoubtedly, the distinction of this type of crime from traditional crimes requires that the concerned agencies responsible for investigating and detecting them possess technical capabilities and resources that qualify them for this responsibility. At the same time, it requires the existence of specialized judiciary with special abilities that enable them to deal with these crimes. This study aims to identify the different legislative plans regarding granting jurisdiction to specialized judges to consider

[#] A special issue for the Third International Conference, entitled: **Artificial Intelligence, A Legal Vision Towards a Sustainable Future**.

information technology crimes. The study focuses, through the comparative method, on identifying the legislative approach in some Arab and European countries in order to identify the most effective ways to combat this type of crime and achieve justice. To what extent is there a need to establish specialized courts to consider these crimes?

Keywords: Newly Established Crimes, Artificial Intelligence, Specialized Courts, Judicial Qualification, Comparative Studies.

"مدى الحاجة إلى انشاء قضاء جنائى متخصص بنظر الجرائم التقنية" دراسة مقارنة

عبدالرؤوف حسن أبو الحديد [1] طارق السيد محمود يوسف أبو عقيل [2]

(1) باحث، أستاذ مساعد قانوني

(2) باحث ، دكتوراه في القانون الجنائي

ملخص

أدى التطور السريع والمتلاحق في مجال تكنولوجيا المعلومات، والتطور المتلاحق في صناعة تقنيات الذكاء الاصطناعي إلى ظهور العديد من أنماط السلوك الإجرامي، وهي أنماط تختلف تمامًا عن أنماط السلوك في الجرائم التقليدية، لكونها تتميز بطابعها الخاص؛ فهي سهلة وغير مكلفة، كما أن خطورتها في بعض الحالات قد تتجاوز خطورة الجرائم التقليدية، فضلًا عن أن هذه النوعية من الجرائم المستحدثة لا تعوقها الحدود الجغرافية، فهي عابرة للحدود، ومن هنا فقد اتجه المشرع في مختلف دول العالم إلى سن تشريعات خاصة تستهدف التصدي لهذه النوعية من الجرائم.

ولا شك أن تميز هذه النوعية من الجرائم عن الجرائم التقليدية يستدعي أن تكون الأجهزة المعنية بالبحث والتحري عنها تمتلك قدرات وإمكانات ذات طابع تقني تؤهلها للقيام بهذه المسؤولية، كما تستدعي في ذات الوقت وجود قضاء متخصص يمتلك قدرات خاصة تمكنه من التعامل معها. وتأتي هذه الدراسة بهدف التعرف على خطة التشريعات المختلفة في شأن منح الاختصاص بالنظر في جرائم تقنية المعلومات، والتي قد تتركب بواسطة تقنيات الذكاء الاصطناعي، إلى قضاة متخصصين، وتتركز الدراسة من خلال استخدام المنهج المقارن على التعرف على مسلك المشرع في بعض الدول العربية والأوروبية، من أجل التعرف على أكثر الطرق فاعلية في التصدي لهذه النوعية من الجرائم، وتحقيق العدالة الناجزة، وإلى أي مدى أصبح هناك ضرورة تقتضي إنشاء محاكم مختصة بالنظر في هذه الجرائم.

الكلمات المفتاحيّة: تقنية المعلومات– الجرائم المستحدثة – الذكاء الاصطناعي – المحاكم الخاصة – التأهيل القضائي– الدراسات البينية.

المقدمة.

بدايةً من ظهور الإنترنت واتساع نطاق استخدامه، مرورًا بالدخول في العصر الرقمي، ووصولًا إلى تقنيات الذكاء الاصطناعي الفائق، وما ترتب على ذلك من ثورة تكنولوجية هائلة انعكست آثارها على كافة المجالات، ونتيجةً لحجم المكاسب والفوائد التي تحققت، فقد تخيل إنسان العصر الحديث أنه أسعد حظًا من الأجيال البشرية التي سبقته، وأنه قد بات المتحكم الوحيد في إدارة الكون على النحو الذي يرضي طموحه ويضمن له أعلى درجات الرفاهية.

وسرعان ما تبددت تلك الخيالات البشرية، بعد أن اصطدمت بالواقع المرير، ذلك الواقع الذي تكشف من خلاله الجانب المظلم للتطور التقني، فثبت بما لا يدع مجالًا للشك أن المخاطر الناجمة عن الغزو التكنولوجي لكافة المجالات لا تقل أبدًا عن حجم المنافع المتحصلة.

وتعد الجرائم التقنية واحدة من أصعب التحديات التي يشهدها العالم في الوقت الراهن، حيث لجأت العصابات الإجرامية إلى تكثيف جهود الاستعانة بالتطور التقني في تنفيذ مخططاتها الإجرامية، وأصبح الإنترنت ساحةً لأخطر أنواع الجرائم، كالإرهاب الإلكتروني، وغسيل الأموال باستخدام العملات الافتراضية، والاعتداء على البيانات الشخصية على منصات الويب المظلم، إلى جانب تجارة الأسلحة والرقيق والاعتداء على الأطفال، وسرعان ما دخل الذكاء الاصطناعي على هذا الخط، فتزايد حجم المخاطر، وتصاعدت الهجمات السيبرانية على البنى التحتية، وأصبح للمسيَّرات الكلمة العليا في إدارة الحروب، وتفاقمت الأزمة في ظل السباق الدولي نحو التسلح بالأسلحة الفتاكة ذاتية التشغيل من قبل الدول الكبرى، وعلى رأسها الولايات المتحدة وروسيا والصين، مع عجز المجتمع الدولي عن التوصل إلى اتفاقية عالمية للتصدي لمواجهة مخاطر الإجرام التقني.

وفي سبيل مواجهة تلك المخاطر، اتجهت معظم الدول إلى تبني خطة شاملة للتصدي للجرائم الإلكترونية، وبينما اتجهت بعض الدول، كالهند، إلى إجراء تعديل شامل على تشريعاتها الجنائية، اتجهت دول أخرى إلى سن تشريعات خاصة لمكافحة الإجرام التقني، وعلى صعيد إجراءات الملاحقة الجنائية تم تخصيص أجهزة خاصة لملاحقة هذه النوعية من الجرائم، أما فيما

يتعلق بالاختصاص بنظر القضايا المتعلقة بالجرائم التقنية، فقد اتجهت بعض الدول إلى منح الاختصاص في هذا الشأن إلى دوائر جنائية خاصة، بينما اتجهت دول أخرى إلى إنشاء محاكم خاصة عُهد إليها بالفصل في هذه الجرائم بهدف سرعة الفصل فيها.

ويأتي هذا البحث لإلقاء الضوء على مدى أهمية إنشاء محاكم خاصة لنظر الجرائم التقنية، ومدى كفاءة هذا النهج في مواجهة هذه النوعية من الجرائم.

أهمية موضوع البحث:

تتمثل أهمية البحث في كونه يتعرض لدراسة الجرائم الإلكترونية التي تعد واحدة من أكثر المخاطر العالمية تعقيدًا، كما أنه يأتي في الوقت الذي تكثف فيه الدول كافة الجهود في سبيل التصدي للجرائم التقنية، وخصوصًا تلك التي يتم الاستعانة في ارتكابها بتقنيات الذكاء الاصطناعي، في ظل غياب الأطر التشريعية التي تحكم استخدام هذه التقنيات.

إشكالية البحث:

تتمثل الاشكالية الرئيسية للبحث في محاولة التعرف على مدى فاعلية وجود قضاء جنائي متخصص بالنظر في الجرائم التقنية في الحد من هذه الجرائم وتحقيق الردع العام والخاص. وقد تفرع عن هذه الاشكالية عدة تساؤلات.

تساؤلات البحث: تتمثل أهم التساؤلات التي يطرحها البحث في:

ما هو حجم المخاطر التي قد تترتب على انتشار الاجرام التقني، وما هي وسائل الحد منه؟

ما هي الخطط التي تتبناها الدول في مواجهة مخاطر الجرائم التقنية وما مدى فاعليتها؟

ما المقصود بالمحاكم الجنائية المتخصصة، وإلى أي مدى يسهم تواجدها في التصدي للإجرام التقني، وما هي أهم التجارب الدولية التي تبنت نهج إنشاء قضاء متخصص؟

منهجية البحث:

اعتمد البحث على المنهج التحليلي، حيث يتم تحليل النصوص القانونية والآراء الفقهية للوقوف على أهدافها وقياس مدى فاعليتها، كما تم الاعتماد على المنهج المقارن من خلال عرض بعض التجارب الدولية بشأن القضاء المتخصص بنظر الجرائم التقنية وذلك من أجل التعرف على مدى الحاجة للاستفادة من تلك التجارب.

خطة البحث:

تم تقسيم الدراسة إلى مبحثين، وذلك على النحو التالي:

المبحث الأول

الجرائم التقنية بين المخاطر وجهود المكافحة

وفقًا للتقرير الصادر عن المنتدى الاقتصادي العالمي حول المخاطر العالمية لعام 2025، فقد باتت المخاطر التقنية واحدة من أكبر المشكلات العالمية، حيث تطوّرت بوتيرة سريعة، من مجرد تهديدات بسيطة للأمن السيبراني إلى تحديات أعقد تتعلق بالذكاء الاصطناعي والتقنيات الحيوية[1] ، وفيما يخص المخاطر السيبرانية ألقى تقرير الآفاق العالمية للأمن السيبراني 2025 الضوء على واقع جديد يتميّز بتعقيد هائل في الفضاء السيبراني. وقد أسهمت التوترات الجيوسياسية والتطوّر التكنولوجي وصعود الهجمات السيبرانية المُعقّدة في توسيع نطاق المخاطر[2]. ولا تقتصر الآثار السلبية للجرائم التقنية على الجوانب الاقتصادية، بل انها تشكل تهديدًا للأمن المجتمعي والأمن القومي، خاصة في ظل تطور تقنيات الذكاء الاصطناعي في ظل غياب الأطر القانونية، وعياب الرقابة.

ونحاول من خلال هذا المبحث التعرف على ماهية الجرائم التقنية وما ينجم عنها من مخاطر، والجهود المبذولة لمكافحتها على الصعيدين الدولي والوطني، وذلك في مطلبين على النحو التالي:

المطلب الأول

ماهية الجرائم التقنية

أدى التطور التقني الهائل إلى ظهور أنماط جديدة من السلوك الإجرامي، وهو سلوك يشكل تهديدًا للفرد والمجتمع على حد سواء، حيث لا يقتصر الأثر السلبي للجرائم التقنية على مجال بعينه، بل يتعدى ذلك لتصبح تهديدًا للأمن الاقتصادي والاجتماعي والقومي، حتى أصبحت من أخطر التحديات التي يواجهها الإنسان المعاصر. وفي سبيل التعرف على ماهية الجرائم التقنية

---

(1) أنظر تقرير المخاطر العالمية لعام 2025، على الرابط التالي، تراريخ الزيارة 2025/3/30
https://encc-eg.org/pressroom/press.aspx?id=264

(2) الآفاق العالمية للأمن السيبراني 2025: دليل شامل لتعزيز القدرة التنافسية الرقمية في مصر، منور على الانترنت، الرابط التالي:
تاريخ الزيارة 2025/3/30 https://encc-eg.org/pressroom/press.aspx?id=267

سنحاول التعرض لمفهومها وبيان خصائصها، ثم التعرض لأهم التهديدات والمخاطر الناجمة عنها.

أولًا– مفهوم الجرائم التقنية:

تتعدد المصطلحات التي يطلقها الفقه لوصف الجرائم المرتبطة بالتطور التقني، حيث يطلق عليها البعض مصطلح الجرائم الإلكترونية[1]، بينما يفضل البعض الآخر تسميتها بجرائم الانترنت[2]، أو جرائم تقنية المعلومات[3]، كما يعد مصطلح الجرائم السيبرانية[4] من بين المصطلحات الشائعة لوصف السلوك الاجرامي المرتبط بالتطور التقني.

وهناك رأى في الفقه[5] يرى أن أساس اختلاف وجهات نظر الفقه حول المصطلح المستخدم يرجع في الأساس إلى تعدد الأسس التي يعتمد عليها في تحديد مفهوم تلك الجريمة، فبينما يتخذ

---

(1) د. ياسر سيد فهمي، المواجهة الجنائية للجريمة الإلكترونية ، دراسة تحليلية تأصيلية مقارنة، رسالة دكتوراة، كلية الحقوق ، جامعة القاهرة، 2021، ص12: 15.

(2) د. محمود محمد صفاء الدين علي، الجهود الدولية والتشريعية لمكافحة جرائم الانترنت، مجلة البحوث القانونية والاقتصادية، المجلد54، العدد 3، كلية الحقوق، جامعة المنوفية، اكتوبر 2021، ص528 وما بعدها؛ د. حرز الله محمد لخضر، جرائم الأنترنت وتحديات الأمن السايبراني: دراسة في متغيرات الجريمة ومقارباتها العلاجية.، مجلة المفكر، المجلد18، العدد1، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر 2023، ص510

(3) د. نايف شافي المظافرة، جرائم تقنية المعلومات فى التشريع الأمريكى مقارنة بالتشريعات العربية، مجلة البحوث القانونية والاقتصادية، المجلد13، العدد83، كلية الحقوق، جامعة المنصورة، ص 337: 340

(4) د. محمد محمود فيالة، القانون الدولي والتحديات المعاصرة الجريمة السيبرانية نموذجا، مجلة الحقوق للبحوث القانونية، المجلد 2، العدد1، كلية الحقوق، جامعة الإسكندرية، 2024، ص815: 816؛ وانظر:

Krishna Kumar & Praveen Gupta, A Study About Cyber Crimes And Cyber Law In India, JETIR May 2019, Volume 6, Issue 5,pp131: 134 https://www.jetir.org/papers/JETIRBW06027.pdf

(5) Ramadan, S.A., Qasim, A., Abdullah, A.F. (2024). Legal Liability Arising from Information Crimes in UAE Law. In: Alareeni, B., Elgedawy, I. (eds) Opportunities and Risks in AI for Business Development. Studies in Systems, Decision and Control, vol 545. Springer,p.785 https://link.springer.com/chapter/10.1007/978-3-031-65203-5_67

البعض الوسيلة المستخدمة أساسًا لتعريف الجريمة، يتجه آخر إلى تبني محل الجريمة كأساس للتعريف، كما يجمع البعض بين الوسيلة المستخدمة في ارتكاب الجريمة وبين موضوعها، وكذلك هناك من يركز على الخصائص الشخصية لمرتكبي هذه النوعية من الجرائم.

وفي رأينا أنه على الرغم من تعدد الأسس التي اتخذها الفقه لتقديم مدلول محدد للجرائم المتصلة بالتطور التقني إلا أنها جميعًا تؤدى إلى ذات المعنى، فهذه النوعية من السلوك الإجرامي ترتبط ارتباطًا وثيقًا بالثورة التكنولوجية، فهي في كل الحالات سلوكًا غير مشروع. وقد عرفها البعض بأنها: "كل فعل أو امتناع يتعلق بالاعتداء على الأموال المادية أو المعنوية ويكون استخدام التقنية المعلوماتية فيه أمرًا ضروريًا سواء تم ذلك بشكل مباشر أو غير مباشر"[1] بينما ذهب البعض إلى أنها سلوك غير مشروع ينطوي على الاستخدام السيئ للإنترنت."[2]

وقد اتجه رأى في الفقه[3] إلى أن هناك أربعة أسس يتم استخدامها في وضع تعريف للجرائم التقنية، وتتمثل في الوسيلة المستخدمة في ارتكاب الجريمة، موضوع الجريمة، المام الفاعل بتقنية المعلومات، وأخيرًا الاعتماد على أكثر من معيار في توضيح المفهوم، وينتهي هذا الرأي إلى تعريف الجرائم التقنية بأنها: "كل فعل أو امتناع من شأنه الاعتداء على الأموال المعنوية (معطيات الحاسب) يكون ناتجًا بطريقة مباشرة وغير مباشرة لتدخل التقنية المعلوماتية" معتبرًا أنه تضمن اعتماد المفهوم لأكثر من معيار. وفي رأينا أن هذا المفهوم يفتقد إلى الدقة، إذ لا تقتصر الجرائم التقنية على الاعتداء على معطيات الحاسب.

وعلى الرغم من عزوف المشرع في معظم الدول عن تبني تعريف محدد للجرائم التقنية، إلا أن المشرع في كل من الكويت والسعودية قد خالف هذا النهج، حيث عرفها المشرع الكويتي بأنها "كل فعل يرتكب باستخدام الحاسب الآلي، أو الشبكة المعلوماتية أو غيرها من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون[4]"، بينما اتجه المنظم السعودي إلى تعريفها بأنها" أي فعل

---

(1) د. محمد محمود فيالة، القانون الدولي والتحديات المعاصرة الجريمة السيبرانية، مرجع سابق، ص816

(2) د. حرز الله محمد لخضر، جرائم الأنترنت وتحديات الأمن السايبراني، مرجع سابق، ص510

(3) سعد فهد سعد ادبيس المطيري، مفهوم الجرائم الالكترونية وسماتها، المجلة القانونية، المجلد16، العدد5، كلية الحقوق ، جامعة القاهرة، فرع الخرطوم، مايو 2023،ص1247

(4) القانون 63 لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات الكويتي.

يرتكب متضمنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام"[1] وهو مسلك منتقد من جانب الفقه نظرًا لما شابهما من قصور وعدم الدقة . كما أنه ليس من بين اختصاصات المشرع وضع تعاريف للجرائم، فهو عمل من اختصاص الفقه والقضاء[2].

ويرى الباحث أنه على الرغم من تعدد التعاريف التي تبناها الفقه لتحديد مفهوم الجرائم التقنية إلا أن أقربها إلى الشمول هو تعريف الجرائم التقنية على أنها:" كل سلوك غير مشروع ويشكل مخالفة للتشريعات المنظمة لتقنية المعلومات والذكاء الاصطناعي"[3] فمن مزايا هذا التعريف أنه اشتمل على كافة أنواع السلوك التي تخالف التشريعات المنظمة لتقنية المعلومات كما يتسع ليشمل الجرائم التي قد تنجم عن استخدام تقنيات الذكاء الاصطناعي.

ثانيا- أبرز خصائص الجرائم التقنية:

يتفق الفقه[4] على مجموعة معينة من الخصائص التي تتميز بها الجرائم التقنية عن الجرائم التقليدية، وتتمثل أهم تلك الخصائص فيما يلي:

1-جرائم عابرة للحدود:

---

(1) المادة 8/1 من نظام مكافحة جرائم المعلوماتية السعودي.

(2) د. حاتم أحمد محمد بطيخ، تطور السياسة التشريعية فى مجال مكافحة جرائم تقنية المعلومات، دراسة مقارنة، مجلة الدراسات القانونية، المجلد7، العدد1، كلية الحقوق، جامعة مدينة السادات، ملحق يوليو – اغسطس 2021، ص16

(3) د. طارق السيد محمود أبوعقيل، دور الدراسات البيئية فى ارساء قواعد القانون الجنائي التقني، مجلة الباحث للعلوم القانونية، المجلد 5، العدد2، كلية القانون جامعة الفلوجة، 2024، ص104

(4) د. عبد الإله محمد النوايسة، جرائم تكنولوجيا المعلومات، ط1، دار وائل للنشر والتوزيع، عمان، االأردن ، 2017، ص87؛ د. أحمد محمد براك، شرح قانون الجرائم الإلكترونية، دار الثقافة للنشر والتوزيع، عمان، الاردن، 2024، ص32 وما بعدها؛ د.محمد البلى العتوم، جرائم تكنولوجيا المعلومات، النظرية العامة للجرائم الالكترونية، دار الثقافة للنشر والتوزيع، عمان ، الأردن، 2023، ص26: 35؛ د. وفاء نعيم، المؤتمر الدولي الثانى للعلوم الانسانية والاجتماعية، البحث العلمى فى مواجهة المخاطر العالمية، الواقع والتحديات ورى المستقبل، المجلة الجنائية القومية، المجلد67، العدد 2، المركز القومى للبحوث الحنائية، القاهرة، 2024، ص123: 124؛ د. ذياب موسى البداينة، الجرائم الالكترونية ، المفهوم والاسباب، ورقة مقدمة في الملتقى العلمي الجرائم المستحدثة في ظل التغيرات والتحولات الاقليمية والدولية ، عمان ، الاردن، 2-2014/9/4، ص19: 20

تتسم الجريمة الالكترونية في غالب الأحيان بالطابع العابر للحدود، وذلك بالنظر للطابع العالمي لشبكة الانترنيت، فعولمة هذه الجرائم يؤدي إلى تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم؛ وتعد صورة صادقة من صور العولمة؛ فمن حيث المكان يمكن ارتكاب هذه الجرائم عن بُعد وقد يتعدد هذا المكان بين أكثر من دولة؛ فلا تقتصر آثارها على حدود دولة بعينها، وغالبًا لا يتواجد الفاعل على مسرح الجريمة، ومن الناحية الزمنية تختلف المواقيت بين الدول؛ الأمر الذي يثير التساؤل حول تحديد القانون الواجب التطبيق على هذه الجريمة.[1]

2- صعوبة الإثبات والملاحقة:

من أدق خصائص الجرائم التقنية أن إثباتها أمر بالغ الصعوبة، ويرجع ذلك إلى تعدد المعوقات التي تحول دون سرعة التوصل لمرتكب الجريمة[2]، كما أن الدليل في الجرائم التقنية عادة غير ملموس ويحتاج إلى امكانيات تقنية فائقة الدقة، أضف إلى ذلك وجود مساحة على شبكة المعلومات الدولية تمكن مستخدميها من إخفاء الهوية، تعريف بالويب المظلم[3] والذي يعد ساحة لممارسة كافة أنواع الجرائم. كما أن ضخامة البيانات تعد إحدى معوقات سرعة الحصول على الأدلة، كما أن سهولة محو الأدلة تزيد الأمر تعقيدًا، أضف إلى ذلك انعدام خبرة الأجهزة المعنية بالملاحقة والتحقيق[4] قد يؤدى إلى إفلات الجناة من العقاب.

---

(1) فعالية التشريعات العقابية في مكافحة الجرائم الإلكترونية، مجلة دراسات وابحاث، المجلد1، العدد1، جامعة زيان عاشور، الجلفة، الجزائر 2009، ص428؛ د. سعد فهد سعد، مفهوم الجرائم الالكترونية، مرجع سابق، ص1258

(2) د. منصور فهيد سعد الحارثى، معوقات اثبات الجرائم المتعلقة بتقنية المعلومات، المجلة القانونية، المجلد 15، العدد4، كلية الحقوق، جامعة القاهرة، فرع الخرطوم، فبراير 2023، ص 1054 وما بعدا

(3) Hemdani, M.G.K. (2025). Cryptocurrencies and the Dark Web: A Gateway to Money Laundering. In: Chawki, M., Abraham, A. (eds) Cybercrime Unveiled: Technologies for Analysing Legal Complexity. Studies in Computational Intelligence, vol 1181. Springer,pp.217: 224

(4) Jain, R., Sonowal, B. (2025). Analyzing the Procedure for Investigation in Cybercrime and Admissibility of Electronic Evidence. In: Chawki, M., Abraham, A. (eds) Cybercrime Unveiled: Technologies for Analysing Legal Complexity. Studies in Computational Intelligence, vol 1181.

3- **جرائم ناعمة:**

مرتكب الجرائم التقنية في الغالب الأعم شخص يمتلك الخبرة والمهارات التقنية التي تجعله قادرًا على تنفيذ جريمته بدقة، ولذا يطلق عليها جرائم الياقات البيضاء[1]، كما أنها جرائم ناعمة إذ أنها على عكس بعض الجرائم التقليدية لا تتطلب العنف[2]، فسرقة البيانات، والسطو على حسابات البنوك، والهجمات السيبرانية، والابتزاز الإلكتروني، وغيرها من مختلف أنماط السلوك الإجرامي على الفضاء الإلكتروني يتم دون الحاجة إلى أي مجهود عضلي. وحتى جرائم الاعتداء على الأشخاص التي ترتكب عبر الأجهزة التقنية لا تحتاج إلى أي جهد أو عنف، فاختراق حاسوب بإحدى المستشفيات والتلاعب بجدول مواعيد الدواء تمهيدًا للقضاء على حياة أحد المرضى لا يستلزم العنف، كما أن تسير إحدى الطائرات المسيرة لتفجير مؤسسة لا يحتاج لأي مجهود.

4- **تتطلب مهارات ودراية بالجوانب التقنية:**

على اعتبار أن الجرائم التقنية غالبًا ما تقع في بيئة المعالجة الآلية للبيانات، ويتطلب ارتكابها التعامل مع مجموعة ضخمة من البيانات، كما تتطلب الدخول إلى النظام المعلوماتي، وهو ما يتطلب فهم الجاني واحاطته بالمعلومات التقنية وعلوم الحاسب، واحتراف استخدام الانترنت، وفي الغالب الأعم فإن الجرائم التقنية ترتكب من قبل أشخاص على قدر عال من الاحتراف في مجال تكنولوجيا المعلومات والحاسب الآلي[3].

Springer, Cham. ,pp265-278 https://doi.org/10.1007/978-3-031-80557-8_12

(1) د. عصام حسنى الأطرش، تأثير جرائم ذوى الياقات البيضاءعلى الأمن القومي الفلسطيني، من وجهة نظر ذوى الاختصاص، مجلة ،جامعة الشارقة للعلوم القانونية، المجلد21، العدد3، الامارات، سبتمبر 2024ص370 وما بعدها

(2) د. ذياب موسى البداينة، الجرائم الالكترونية، مرجع سابق، ص20

(3) د. يوسف نفيد، المكافحة التشريعية لبعض صور الجرائم المعلوماتية وأصناف المجرم المعلوماتي، المجلة العربية للدراسات الأمنية، المجلد38، العدد2، أكاديمية نايف العربيوة للعلوم الأمنية، ديسمبر 2022، ص139؛ د. هنادي محمود توفيق صالح، غسل الأموال عبر المتجر الإلكتروني، دراسة في التشريع الأردني، المجلة الأردنية في القانون والعلوم السياسية، المجلد16، العدد1، 2024، ص75: 76

ثالثًا- مخاطر الجرائم التقنية:

تتعدد أنماط الجرائم الإلكترونية إلى درجة وجود نموذج تقني لكافة أشكال الجرائم التقليدية، بما فيها جرائم الاعتداء على الأشخاص وجرائم الاعتداء على الأموال، وكذلك الجرائم المتصلة بالأمن القومي والسياسة الاقتصادية، بمعني أن مخاطر هذه النوعية من الجرائم المستحدثة تتخطي بمراحل تلك المخاطر الناجمة عن الجرائم التقليدية، لهذا اتجه رأى في الفقه[1] إلى ضرورة إرساء قواعد موضوعية وإجرائية خاصة بفرع جديد من فروع القانون هو القانون الجنائي التقني. وذهب رأى آخر[2] إلى ضرورة مراجعة التشريعات القائمة، وعلى العموم يمكن ذكر بعض المخاطر على النحو التالي:

1-المخاطر الاجتماعية:

تتعدد مخاطر الجرائم التقنية التي تنعكس بالسلب على الفرد والمجتمع، فعلى المستوى الفردي يؤدى تنامى العلاقات غير المشروعة على وسائل التواصل الاجتماعي إلى التشتت الذهني، وتشكل تهديدًا للخصوصية [3] وتفكك الأسرة كما أن توجيه بعض الجرائم الالكترونية ضد الأطفال[4] من شأنه أن يؤدى إلى الاضرار بصحتهم النفسية.

2-المخاطر الاقتصادية:

---

(1) د. طارق السيد محمود، دور الدراسات البينية في ارساء قواعد القانون الجنائي التقني، مرجع سابق، ص294 وما بعدها.

(2) AL-Mulla, M.S. (2025). Cybercrime from Controllability to Subjectivity: A Serious Call for Legislative Review. In: Chawki, M., Abraham, A. (eds) Cybercrime Unveiled: Technologies for Analysing Legal Complexity. Studies in Computational Intelligence, vol 1181. Springer, Cham, pp134: 148 at:. https://doi.org/10.1007/978-3-031-80557-8_6

(3) د. كهينة علواش، مخاطر الجريمة الإلكترونية عبر مواقع التواصل الاجتماعي بين اختراق الخصوصية وآليات المواجهة، مجلة دراسات، المجلد 11، العدد2، الجزائر، نوفمبر 2022، ص93.

(4) تهاني محمد بن سويد، حماية الأطفال من الجرائم الإلكترونية مسؤولية مجتمعية، مجلة مستقبل العلوم الاجتماعية، المجلد 18، العدد3، الجمعية العامة العربية للتنمية البشرية والبيئية، يوليو 2024، ص197: 210

تتسبب الجرائم الإلكترونية بخسائر كبيرة للمؤسسات والشركات المتمثلة في خسائر مادية وأخرى تتعلق بالنظم، بحيث يقوم المجرم باختراق أنظمة الشبكات الخاصة بالمؤسسات والشركات والحصول على معلومات قيمة وخاصة بأنظمة الشركات، ومن ثم يقوم باستخدام المعلومات من أجل خدمة مصالحه الشخصية والتي تتمثل في سرقة الأموال وتدمير أنظمة الشركة الداعمة في عملية الإدارة مما يسبب خسائر جسيمة للشركة أو المؤسسة. كما يمكن سرقة المعلومات الخاصة بموظفين المؤسسات والشركات وتحريضهم وابتزازهم من أجل تدمير الأنظمة الداخلية للمؤسسات، وتثبيت أجهزة التجسس على الحسابات والأنظمة والسعي لاختراقها والسيطرة عليها لتحقيق مكاسب مادية وسياسية[1].

3- المخاطر الأمنية:

هناك مجموعة من الجرائم التقنية تكون الدولة فيها هي المجني عليه، ويكون الجاني قد دخل أو اخترق موقعًا أو بريدًا إلكترونيًا أو حسابًا خاصًا أو نظامًا معلوماتيًا يُدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة أو مملوكًا لها، أو يخصها على سبيل مثال جرائم التجسس أو التحريض على الإرهاب ضد مصلحة الوطن باستخدام معلومات قد تم سحبها من ملفات أجهزة الدولة. ومن قبيل الجرائم التي تشكل تهديدًا لأمن الدولة اختراق المواقع الإلكترونية والسيطرة عليها، ومن ثم توظيفها لتخدم مصالح كيانات خطيرة تهدف إلى زعزعة الأمن بالبلاد والسيطرة على عقول الشباب وتحريضهم للقيام بأعمال غير مشروعة [2]، وقد تستعين العصابات الاجرامية بتقنيات الذكاء الاصطناعي لشن الهجمات السيبرانية ضد البنية التحتية، وارتكاب جرائم الارهاب الإلكتروني، أو استخدام تقنيات التزييف العميق ومن ثم اشاعة الفوضى بنشر أخبار

---

(1) أبو بكر أحمد همام، الآثار الاقتصادية للجرائم المعلوماتية وسبل مكافحتها، مجلة جامعة جنوب الوادي الدولية للعلوم القانونية، المجلد 6، العدد6، 2021، ص347وما بعدها.

(2) الجرائم الإلكترونية تدق ناقوس الخطر وتهدد أمن الدول والشعوب، مقال منور على الانترنت، فبراير 2022، على الرابط التالي، وتاريخ الزيارة 2025/3/30
https://draya-eg.org/2022/02/24

وصور مزيفة، وقد يصل الأمر إلى التلاعب في القرارات السياسية ونتائج الانتخابات واسقاط الأنظمة الحاكمة[1].

المطلب الثاني

جهود مكافحة الجرائم التقنية

أولًا- الجهود على الصعيدين الدولي والاقليمي:

أظهر تقرير حديث أن التكاليف العالمية للجرائم الإلكترونية تنمو بنسبة 15% سنويًا، وأشار التقرير إلى أن المخاطر الناجمة عن جرائم التقنية خلال عام 2024 ستتجاوز 9.5 تريليون دولار أميريكي وهو ما يوازي اقتصاد ثالث دولة في العالم بعد الولايات المتحدة والصين[2]، ومع تعاظم حجم مخاطر الجرائم التقنية وتخطي آثارها الحدود الاقليمية على نحو يشكل تهديدًا دوليًا، بدأت المنظمات الدولية في السعي نحو مواجهة هذه النوعية من الجرائم، كذلك على المستوى الاقليمي تم اقرار المعاهدات بهدف التصدى لمخاطر الإجرام التقني.

1- على الصعيد الدولي:

هناك العديد من القرارات التي صدرت عن مؤتمرات دولية استهدفت التأكيد على ضرورة التصدي للجرائم الإلكترونية، ومنها القرار الصادر عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء بهافانا 1990 بشأن الجرائم المتصلة بالكمبيوتر، وحث القرار كافة الدول على تكثيف جهودها لمكافحة الجرائم التقنية، تلي ذلك التوصيات الصادرة عن المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات بالبرازيل 1994 بشأن جرائم الكمبيوتر، ونص على بعض الأفعال المجرمة، وتضمن النص على بعض القواعد الاجرائية[3].

---

(1) Abel Yeboah-Ofori, Jamal-Deen Abdulai, Ferdinand Katsriku, Cybercrime and Risks for Cyber Physical Systems, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 8(1):2019, 43-57.

(2) Steve Morgan, 2024 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics,Jun 24,2024, https://cybersecurityventures.com/cybersecurity-almanac-2024/ الزيارة بتاريخ 2025/4/2.

(3) ليندا شرابشة ، السياسة الدولية و الإقليمية في مجال مكافحة الجريمة الالكترونية. الاتجاهات الدولية في مكافحة الجريمة الالكترونية، مجلة دراسات وأبحاث، المجلد 1، العدد1، جامعة زيان عاشور، الجزائر 2009، ص245 : 246

أما فيما يخص منظمة الأمم المتحدة فتتمثل أهم الجهود في مجموعة القرارات الصادرة عن الجمعية العامة ومنها القرار 63/55 والذى تحدد من خلاله بعض التدابير الالزامية لمنع اساءة استخدام التكنولوجيا[1]. ثم القرار 121/56 لعام 2002، وقد سلط الضوء على جهود المنظمات الدولية والاقليمية في مجال مكافحة الجرائم التقنية[2]. كذلك انعقدت العديد من المؤتمرات[3] وفي مقدمتها مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية لعام 2010، تلاه المؤتمر الثالث عشر عام 2015.

وعلى الرغم من حجم الجهود إلا أنه وحتى مطلع عام 2024 ظل المجتمع الدولي عاجزًا عن ابرام اتفاقية عالمية لمواجهة الإجرام التقني، إلا أنه في أواخر ذات العام انبعث الأمل من جديد بعد أن نجحت الجمعية العامة في اعتماد أول اتفاقية دولية لمنع ومكافحة الجرائم الإلكترونية، وجاء ذلك بعد مجهودات تفاوضية استمرت خمس سنوات، وهذه الاتفاقية ستدخل حيز التنفيذ بعد مرور 90 يوم من تاريخ التصديق عليها من قبل الدولة الموقعة الأربعين[4].

2- على الصعيد الاقليمي:

في عام 1999 انعقد مؤتمر بجامعة ستانفورد بولاية كاليفورنيا في الفترة من 6: 7 ديسمبر بمباركة العديد من الهيئات والمؤسسات، وتم اقتراح الاتفاقية الأمريكية المتعلقة بجرائم الحاسب الآلي والإنترنت وتضمن الاتفاقية تحديد تعاريف للمصطلحات، ولضرورة اعتماد نهج موحد في التصدي للجرائم الإلكترونية وفرض العقوبات التي تتناسب وحجم المخاطر[5].

---

(1) A/RES/55/63, See at : https://www.itu.int/ITUD/cyb/cybersecurity/docs/UN_resolution_55_63.pdf

(2) A/RES/56/121, https://docs.un.org/ar/A/RES/56/121

(3) د. محمد أحمد سليمان عيسى، الجهود الدولية الإقليمية لمواجهة الجرائم الإلكترونية، مجلة العلوم القانونية، المجلد4، العدد8، كلية القانون ، جامعة عجمان، يوليو 2018، ص191: 194

(4) الجمعية العامة تعتمد اتفاقية تاريخية بشأن الجرائم الإلكترونية 2024/12/24، على موقع الأمم المتحدة على الانترنت، الزيارة 2025/4/1 الرابط التالي: https://news.un.org/ar/story/2024/12/1137776

(5) د. محمد احمد سليمان، الجهود الدولية، مرجع سابق، ص199

وفي عام 2001 نجحت الدول الأوروبية في ابرام اتفاقية بودابست لمقاومة الجرائم التقنية والاتصالات، ولقد تم التوقيع عليها من طرف ثلاثون دولة في العاصمة المجرية " بودابست" ومن بين الدول الموقعة: دول أعضاء من الاتحاد الأوروبي ، إضافة إلى كندا، اليابان، جنوب إفريقيا أمريكا، وجاءت هذه الاتفاقية لتعالج إشكالية دولية للجريمة الالكترونية و تجاوزها للحدود الدولية بما يساعد الدول على مكافحة هذه الجريمة و تعقب مرتكبيها والمساعدة على الاستدلال عليهم و ضبطهم كما تحدد أفضل الطرق الواجب إتباعها في التحقيق في جرائم الانترنت التي تعهد الدول الموقعة بالتعاون الوثيق من أجل محاربتها، كما فصلت الاتفاقية النصوص الجنائية الموضوعية للجريمة و أنواعها كما تشمل جوانب عديدة من جرائم الانترنت من بينها الإرهاب وعمليات تزوير بطاقات الائتمان و غيرها[1].

وعلى المستوى العربي، تم ابرام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[2]، ونصت في مادتها الأول على هدف الاتفاقية المتمثل في تعزيز التعاون بين الدول في مكافحة الاجرام التقني ثم أوردت المادة الثانية تعاريف للمصطلحات، وتضمنت الاتفاقية نصوصًا تتعلق بمجال التطبيق، وأنواع الجرائم الإلكترونية، مع بيان بعض القواعد الإجرائية المتعلقة بالملاحقة الجنائية والتحقيق[3].

ثانيًا– الجهود الوطنية:

تحرص كافة الدول على مواجهة الجرائم التقنية بمختلف السبل، بيد أن الاستراتيجية المتبعة في هذا الشأن قد تختلف من دولة إلى أخرى، بحسب امكانياتها الاقتصادية، وبنيتها التحتية التكنولوجية والإطار القانوني المتبع في التصدي لهذه النوعية الخطيرة من الجرائم.

---

(1) د. حاتم محمد احمد بطيخ تطور السياسة التشريعية، مرجع سابق، ص20؛ د. سامي جاد واصل، التعاون الدولى فى مكافحة الجرائم الإلكترونية، مجلة القانون والتكنولوجيا، المجلد3، العدد1، كلية القانون ، الجامعة البريطانية بالقاهرة، أبريل 2023، ص53

(2) وردة شرف الدين، التعاون القضائي والقانوني لمكافحة جريمة غسيل الأموال والمرتكبة بواسطة تقنية المعلومات - وفقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، مجلة الباحث للدراسات الأكاديمية، المجلد8، العدد2، 2021، ص642؛ وأنظر نصوص الاتفاقية على الرابط التالي على الانترنت، الزيارة 2025/3/2
https://haqqi.info/ar/haqqi/legislation/arab-convention-cyber-%E2%80%8B%E2%80%8Bcrimes

(3) وقد وافقت مصر على الاتفاقية بقرار رئيس الجمهورية رقم 276 لسنة 2014، الجريدة الرسمية، العدد46، بتاريخ 2014/11/13

وتأتي الولايات المتحدة الأمريكية في مقدمة الدول التي تتبنى استراتيجية مطورة في مواجهة الإجرام التقني، وتجمع في استراتيجيتها بين الأدوات التقنية الهائلة ، إلى جانب التدابير التشريعية المتطورة وكذلك التعاون بين الوكالات الفيدرالية وبين الجهات المعنية في كل ولاية، كما أن هناك ارشادات وزارة العدل التي تلعب دورًا محوريًا في مواجهة الجرائم التقنية[1]، ففي الهند وأمام مخاطر الجرائم المستحدثة اتجه المشرع إلى اجراء تعديلات جزرية، حيث ألغى القوانين الجنائية التي تعود للحقبة الاستعمارية وأصدر قانون جديد للعقوبات، وآخر للإجراءات الجنائية[2] كما أصدر كذلك قانون حماية البيانات[3] إلى جانب قانون تكنولوجيا المعلومات لعام 2000[4].

أما فيما يخص أستراليا، فهي تتمتع بإطار قوي للجرائم الجنائية وإنفاذ القانون لمعالجة مجموعة واسعة من الجرائم الإلكترونية، فإلى جانب قانون الكومنولث، هناك تشريعات خاصة بكل ولاية للتعامل مع الجرائم التقنية، وانضمت استراليا الى اتفاقية دول أوروبا لمكافحة الجرائم الإلكترونية، كذلك سنت تشريع خاص بالسلامة الإلكترونية عام 2021، إلى جانب أنها تبنت في عام 2013 استراتيجية وطنية لمكافحة الجرائم التقنية، وفي سنة 2022، قامت الحكومة الأسترالية بتطوير هذه الاستراتيجية[5].

وفي إسبانيا هناك استراتيجية متبعة للتعامل مع الجرائم التقنية، وقد اعتبر المشرع الجنائي الإسباني جرائم تقنية المعلومات من جرائم الخطر، كما تبنى نصوصًا تكفل الحماية الصارمة للخصوصية، وفي عام 2010 أدرج المشرع مجموعة من النصوص التي تستهدف مكافحة الجرائم

---

(1) Combatting Cyber Crime, https://www.cisa.gov/combatting-cyber-crime الزيارة 2025/4/2

(2) أنظر الرابط التالي على شبكة المعلومات الدولية ، الزيارة 2025/3/2 https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india

(3) Safeguarding India's Digital Landscape Key Government's Initiatives to Enhance Cybersecurity Awareness, Posted On: 25 JUL 2024 , https://pib.gov.in/PressReleasePage.aspx?PRID=2037115

(4) Diksha Jain, Comparative Analysis Of Cyber Laws - India, US And UAE, IJNRD | Volume 9, Issue 3 March 2024, pp.74: 75

(5) 2022 National Plan to Combat Cybercrime, https://www.ag.gov.au/crime/publications/2022-national-plan-combat-cybercrime

الالكترونية في قانون العقوبات الإسباني، وعلى الصعيد الاجرائي هناك اهتمام خاص بالتعاون الدولي، وتبنى نهج تزويد السلطات المختصة بالملاحقة بأحدث التقنيات الحديثة لتسهيل القيام بمهمتهم[1].

المبحث الثاني
التوجه نحو انشاء قضاء متخصص للنظر في الجرائم التقنية

كما سبق وأن ذكرنا فإن هناك بعض الدول تتبنى استراتيجية خاصة لمواجهة الجرائم التقنية، وتأتي الامارات العربية المتحدة في مقدمة الدول العربية[2]، حيث تبنت استراتيجية واضحة في مواجهة الجرائم الالكترونية وحماية النظام المالي للدولة تعتمد في المقام الأول على المشاركة والتعاون بين جميع الجهات المعنية كجهات إنفاذ القانون والمؤسسات المالية وغير المالية والتجارية والاقتصادية والجهات الحكومية، مثل الدور الكبير الذي تلعبه وسائل الإعلام المختلفة من خلال نشر الوعي لدى أفراد المجتمع بخطورة تلك الجرائم، كما تعمل باستمرار على تطور التشريعات الخاصة في هذا الشأن[3].

وفي المملكة الأرنية تم تبني الاستراتيجية الوطنية للأمن السيبراني 2018: 2023، بالإضافة إلى الرؤية والاستراتيجية الوطنية 2025، هناك العديد من الجهود التي تم اتخاذها في مكافحة الجرائم التقنية، فعلى الصعيد التشريعي، سن المشرع الأردني مجموعة من التشريعات، منها قانون الجرائم الإلكترونية لعام 2023، وكذلك قانون حماية البيانات الشخصية، وقانون الأمن السيبراني[4].

---

(1) Otero, P. (2022). Criminal Law and the Risks Posed by Internet. An Examination of Spanish Criminal Law. In: Cayón Peña, J. (eds) Security and Defence: Ethical and Legal Challenges in the Face of Current Conflicts. Advanced Sciences and Technologies for Security Applications. Springer, Cham, PP.81: 92 https://doi.org/10.1007/978-3-030-95939-5_6

(2) د. جمال محمد خلفان، و د. سلطان محمد سالم عوض، التعاون الوطني والدولي فى الجرائم الالكترونية، المشكلات والحلول، مجلة المعهد العالى للدراسات النوعية، المجلد3، العدد16، يوليو 2023، ص5457 وما بعدها.

(3) استراتيجية اماراتية لمواجهة الجرائم الإلكترونية، على الرابط التالى ، الزيارة 2025/4/3
https://www.albayan.ae/across-the-uae/accidents/2013-09-26-1.1967235

(4) أنظر موقع المركز الوطني للأمن السيبراني على الانترنت، الزيارة 2025/4/3 الرابط التالي
https://ncsc.jo/Ar/List/Policies_and_Strategies_AR

أما على الصعيد الاجرائي فإن نهج الدول يختلف في شأن ملاحقة الجرائم التقنية ومحاكمة مرتكبيها فعلى صعيد الملاحقة اتجهت بعض الدول _ ومن بينها مصر والأردن _ إلى منح الاختصاص بملاحقة الجرائم الإلكترونية إلى جهاز أمني متخصص، أما فيما يخص الأجهزة القضائية فقد اتجهت بعض الدول لإنشاء محاكم خاصة للاضطلاع بهذه المهمة، بينما فضلت دول أخرى منح الاختصاص لدوائر خاصة، واتجهت دول أخرى إلى الابقاء على عدم تمييز الجرائم الإلكترونية عن الجرائم التقليدية في شأن الجهة المختصة بالفصل فيها.

ومن خلال هذا المبحث سنحاول التعرف على ماهية القضاء الجنائي المتخصص، ثم التعرف بعد ذلك على مسلك الدول بشأن الجهات القضائية المختصة بنظر الجرائم التقنية والفصل فيها.

المطلب الأول

ماهية القضاء الجنائي المتخصص

تتبنى معظم النظم القضائية نهجًا قائماً على مبدأ التخصص القضائي من أجل تحقيق المصلحة الخاصة للمتقاضين عن طريق الإنجاز المتقن والسريع للقضايا التي تتسم بالأهمية، وهو ما تتطلبه المصلحة العامة ومقتضيات حسن سير العدالة، ولا شك أن الجرائم التقنية باتت تشكل واحدة من أكثر التهديدات لأمن المجتمع، الأمر الذى دفع بعض الدول لاتباع انشاء محاكم متخصصة بالنظر في الجرائم التقنية، ويقتضى التعرف على ماهية القضاء الجنائي المتخصص تحديد مدلولة ثم تمييز المحاكم الجنائية الخاصة عن الدوائر الخاصة، ثم التعرض لأهمية المحاكم الجنائية الخاصة بشأن الجرائم الالكترونية وذلك على النحو التالي:

أولًا- مفهوم المحاكم الجنائية الخاصة:

يفرق الفقه[1] بين المحكمة المختصة والمحاكم المتخصصة، فبينما ينصرف مفهوم المحكمة المختصة إلى الهيئة القضائية التي أسند إليها المشرع بمهمة الفصل في نوعية معينة من الدعاوي وفقًا لمعايير الاختصاص المكاني والنوعي والقيمي، ومن أمثلة ذلك القضاء الإداري، القضاء

(1) د. يوسف عيسى حامد، تخصص القاضي الجنائي في الفقه والقانون، مجلة حوليات كلية الشريعة، العدد7، جامعة القرآن الكريم والعلوم الإسلامية،2018، ص145 وما بعدها

المدني، وغير ذلك فإن المحاكم المتخصصة هي تلك المحاكم التي اختصها المشرع بنظر نوعية محددة من القضايا ومنها المحاكم العسكرية، محكمة الطفل، محكمة الأسرة، إلى غير ذلك.

وفي رأى البعض ينصرف مفهوم القضاء المتخصص إلى انفراد محكمة بعينها باختصاص نوعي محدد بأنواع معينة من القضايا تتشابه وتتجانس في مقوماتها، بحيث يكون من شأن نظرها من قبل هيئة قضائية أو محكمة متخصصة تسهيل إجراءات الحكم فيها بمهنية وكفاءة ثم سرعة تنفيذ ذلك الحكم بوسائل تتناسب وطبيعة المنازعة وأطرافها[1].

ويمكننا تعريف المحاكم الجنائية المتخصصة بأنها" كيان قضائي متكامل من قضاة ومحققين وجهاز إداري يضطلع بشكل مستقل بالنظر في نوعية محددة من الجرائم وفقًا لما يراه المشرع".

ثانيًا- تمييز المحاكم المتخصصة عن الدوائر الخاصة:

يستفاد من التعريف المتقدم للمحاكم الجنائية االمتخصصة أنها تختلف عن الدوائر الخاصة، فبينما تعتبر المحاكم المتخصصة هيكلًا قضائيًا متكاملًا ومستقلًا، نجد أن الدوائر الخاصة تقتصر على مجموعة من القضاة داخل إحدى المحاكم العامة يسند إليها مهمة الفصل في قضايا بعينها، ومن أمثلتها الدوائر الجنائية بمحكمة النقض، فالدوائر المتخصصة ما هي إلا أقسام مخصصة داخل المحاكم العامة، ومن أهم خصائصها: الهيكل المتكامل؛ حيث تعمل كجزء من الإطار القضائي الأوسع، مما يسمح بتقاسم الموارد مع الأقسام الأخرى.

ويمكننا القول بأن أهم ما يميز المحاكم الخاصة بالجرائم التقنية يتمثل في:

- التوظيف المتخصص: حيث تشكل من قضاة متخصصين على درجة عالية من الالمام بعلوم الحاسب والتكنولوجيا الرقمية، يتلقى فيها القضاة، وموظفو الدعم تدريبًا مستهدفًا في القانون الرقمي ومنهجيات الطب الشرعي.
- إجراءات مبسطة :حيث يتم تصميم الإجراءات خصيصًا للتعامل مع الأدلة الرقمية المتقلبة والقضايا العابرة للاختصاصات القضائية.
- الاختصاص القضائي المركز: وهو يعني تتمتع هذه المحاكم بسلطة حصرية للفصل في قضايا الجرائم الإلكترونية، وغالبًا ما تستفيد من أطر تشغيلية مستقلة.

---

(1) فرج أحمد معروف، المحاكم المتخصصة كوسيلة للارتقاء بالعدالة، ورقة مقدمة إلى المؤتمر الرابع لرؤساء المحاكم العليا في الدول العربية، المنعقد بالدوحة 24،25سبتمبر 2013م، ص2

وتجدر الاشارة إلى أن تخصص المحاكم الجنائية يختلف عن مبدأ تخصص القاضي الجنائي فالأخير يشير إلى ضرورة عدم تكليف القاضي الجنائي بالنظر في قضايا أخرى غير القضايا الجنائية[1]، ويؤكد البعض على أن تخصص القاضي الجنائي من شأنه إعداد القاضي الذي يتصدى للفصل في المسائل والقضايا الجنائية إعداداً خاصاً يؤدي إلى إلمامه بالعلوم الجنائية وفروعها المتعددة مع اقتصار عمله على ذلك النوع من القضايا، ولا يوكل إليه النظر في مسائل أخرى، بما يحقق له خبرة خاصة تتسق مع مجرى الفصل في القضايا الجنائية[2].

ثالثًا– أهمية انشاء محاكم خاصة بالجرائم الإلكترونية:

يؤكد رأى في الفقه على أن الجرائم التقنية وما تتمتع به من خصائص متفردة وما تنطوي عليه من صعوبات تتصل بالتعاون الدولي، وتحصيل الدليل وإجراءات الملاحقة[3] يستدعى انشاء محاكم متخصصة للنظر في هذه النوعية من الجرائم، وأن انشاء هذه المحاكم سيحقق العديد من الفوائد ومنها[4]:

- أن هذه المحكمة ستجمع قضاةً يتمتعون بمعرفة واسعة بالتقنيات الحديثة. ويمكنهم تحسين هذه المعرفة ليس فقط من خلال المشاركة في دورات تدريبية متخصصة، بل أيضًا من خلال مراجعة القضايا الجديدة التي تُشكل سابقة قضائية يوميًا.
- وجود محكمة متخصصة سوف يضمن أن تُحل قضايا التقنيات الحديثة على يد أشخاص ذوي فهم متعمق لها.

---

(1) د. يوسف عيسى حامد، تخصص القاضي الجنائي، مرجع سابق، ص235؛ محمد محمود الشركسي، تخصص القاضي الجنائي وأثره في تحقيق العدالة ، مجلة العلوم والدراسات الانسانية، العدد35، كلية الآداب بالمرج، جامعة بنى غازي، ليبيا2017، ص3 وما بعدها

(2) د. محمد السعيد القزعة نحو قضاء جزائي متخصص بنظر جرائم تقنية المعلومات، دراسة مقارنة، مجلة جيل للدراسات المقارنة، المجلد8، العدد18، مركز جيل للبحث العلمي، 2024 ص113

(3) Ajoy P.B (2022). Effectiveness of Criminal Law in Tackling Cybercrime: A Critical Analysis. Sch Int J Law Crime Justice, 5(2): 74-79; https://saudijournals.com/media/articles/SIJLCJ_52_74-79.pdf

(4) Aleksandra Lisicka, Łukasz Lasek, Do we need a special court for cybercrime cases?17/11/2017 athttps://newtech.law/en/articles/we-need-a-special-court-for-cybercrime-cases

- أن الفهم الجيد والشامل للموضوع من شأنه أن يؤدي إلى إجراءات وقرارات أسرع وأكثر كفاءة. ستعرف المحاكم أي الأدلة يجب رفضها لعدم جدواها، وستكون أكثر استعدادًا لإصدار أمر بتأمين الأدلة الرقمية.

- والميزة الأكيدة لمثل هذه المحكمة المتخصصة هي تعزيز دور القضاء في تنظيم التقنيات الجديدة. فالتطور السريع للتقنيات الجديدة يعني أن المشرّعين لا يستطيعون مواكبتها أو وضع قوانين مناسبة. في نهاية المطاف، يقع على عاتق القضاة والمحامين حلّ القضايا الخارجة عن نطاق التنظيم المعتاد، كما أنه في ظل وجود هذه المحاكم ستصبح السوابق القضائية أكثر رسوخًا واتساقًا.

ومن وجهة نظر البعض[1] فإن تطور الجرائم التقنية وما يتميز به مرتكبي هذه النوعية من الجرائم يتطلب ضرورة العمل على تبني استراتيجية خاصة بشأن التحقيق وكذلك بشأن تعامل القضاء الجنائي مع هذه النوعية من الجرائم ومرتكبيها. كذلك؛ ونظرًا لمخاطر الجرائم التقنية وتميزها عن غيرها من الجرائم التقليدية يدعو البعض[2] إلى ضرورة إنشاء دوائر أو محاكم خاصة يسند إليها مهمة النظر في تلك الجرائم، نظرًا للعديد من النتائج الايجابية التي سيحققها هذا النهج، ومن بينها منح النظام القضائي مرونة أكبر للتكيف مع المتطلبات المتغيرة للعدالة في العصر الحديث، و إيجاد مبادئ توجيهية أكثر اتساقًا ومنطقية لإصدار الأحكام في الجرائم الإلكترونية، كما أن وجود هذه الهياكل المتخصصة من شأنه العمل على زيادة الردع من خلال التعامل السريع مع مجرمي الانترنت[3]

المطلب الثاني
تجارب بعض الدول بشأن المحاكم الخاصة بالجرائم التقنية

---

(1) Lanny L. Newville, Federal Probation Volume: 65 Issue: 2 Dated: September 2001,pp11:17

(2) د. محمد فؤاد الحريري، الإطار القانوني لتجريم القرصنة الإلكترونية فى مملكة البحرين، المجلة القانونية، العدد13 هيئة التشريع والرأي ، المنامة، البحرين 2023، ص119: 120

(3) Tad Simons, Is It Time for a Court Dedicated to Cybercrime?,20Jun 2018,at **https://www.thomsonreuters.com/en-us/posts/legal/justice-ecosystem-cybercrime-court/**

بينما أبقت العديد من الدول على اختصاص المحاكم الجنائية العادية ومن بينها الأردن، الكويت السعودية، العراق، الإمارات، اتجهت دول أخرى إلى انشاء محاكم متخصصة ومنحها الاختصاص بنظر الجرائم التقنية، ومن بينها سوريا، أما المشرع المصري فقد منح الاختصاص بالنظر في هذه الجرائم للمحاكم الاقتصادية، وتفصيل ذلك على النحو التالي.

أولًا – نماذج المحاكم الخاصة في الدول العربية

1-الجمهورية العربية السورية:

تأتى سوريا في مقدمة الدول العربية التي سنت تشريعًا خاصًا تقرر بمقتضاه إنشاء نيابات ومحاكم متخصصة بنظر الجرائم التقنية، حيث نص القانون رقم 9 لسنة 2018 على أن: "تحقق في كل محافظة من محافظات الجمهورية العربية السورية نيابة عامة ودوائر تحقيق تختص كل منها بالنظر في جرائم المعلوماتية وجرائم الاتصالات تملأ وظائفها من الملاك العددي للوظائف القضائية. ب/تمارس النيابة العامة المحدثة وفقا لأحكام الفقرة/أ من هذه المادة سائر الصلاحيات المخولة للنيابة العامة بمقتضى النصوص القانونية النافذة"[1].

كما جاء بنص المادة 2 من ذات القانون: " تحدث محاكم جزائية بدائية واستئنافية للنظر في قضايا الجرائم المعلوماتية وجرائم الاتصالات تملأ وظائفها من الملاك العددي لكل محافظة وتوزع بقرار من مجلس القضاء الأعلى".

2-**مصر**: أسند المشرع المصري الاختصاص بالنظر في الجرائم الإلكترونية للمحاكم الاقتصادية فقد نصت المادة الرابعة من قانون رقم ١٢٠ لسنة ٢٠٠٨ الخاص بإنشاء المحاكم الاقتصادية – والمعدل بالقانون رقم ١٤٦ لسنة ٢٠١٩ م[2] – على أنه: " مع عدم الإخلال بالاختصاصات المقررة للمحاكم الاقتصادية المنصوص عليها في أي قانون آخر، تختص المحاكم الاقتصادية

---

(1) المادة 1من القانون 9 لسنة 2018 بشأن احداث محاكم متخصصة بقضايا جرائم المعلوماتية والاتصالات، الجريدة الرسمية السورية بتاريخ 2018/3/25 على موقع رئاسة مجلس الوزراء السورى، الزيارة 2025/4/2

https://pministry.gov.sy/contents/13491

(2) الجريدة الرسمية، العدد31 مكرر (و)2019/8/7

بدوائرها الابتدائية والاستئنافية، دون غيرها، نوعيًا ومكانيًا بنظر الدعاوى الجنائية الناشئة عن الجرائم المنصوص عليها في القوانين الآتية:....21-قانون مكافحة جرائم تقنية المعلومات".

وفي تعديل لاحق بموجب القانون 156 لسنة 2024 تم تعديل قانون المحاكم الاقتصادية وبمقتضاه تم تعديل المادة 6 بشأن الاختصاص القيمي للدعاوى التي تنظرها الدوائر الابتدائية بالمحكمة الاقتصادية، وأصبحت هذه الدوائر مختصة بالدعاوى التي تجاوز قيمتها 15 مليون جنيه.

ويرى رأى في الفقه على أن المشرع المصري قد تبني نهج منح الاختصاص بنظر الجرائم الإلكترونية للمحاكم المتخصصة متمثلة في المحاكم الاقتصادية، ولكنه في ذات الوقت يؤكد أنها تجربة ناقصة على اعتبار أن جميع القضاة في المحاكم الاقتصادية منتدبين[1].

ومن جانبنا نرى أن مسلك المشرع المصري في منح الاختصاص بنظر الجرائم الإلكترونية للمحاكم الاقتصادية يستعصي على الفهم، كما أن المحاكم الاقتصادية في مصر – من وجهة نظرنا– لا تعد قضاءً جنائيًا متخصصًا، فالقضاة ليسو متخصصين في المجال التقني.

ونرى أنه لكى يصح القول بوجود قضاء جنائي متخصص بالجرائم الإلكترونية فلا بد من توافر بعض الشروط وهي:

- وجود نص قانوني يقر انشاء كيان مستقل ويمنح له الاختصاص بنظر جرائم تقنية المعلومات.
- أن يشكل هذا الكيان من قضاة مدربون ولديهم الالمام الدقيق بعلوم الحاسب الآلي وتقنية المعلومات والأمن السيبراني.
- وجود جهاز إداري مساعد على أعلى درجات الكفاءة على أن يضم بين أعضاءه خبراء في الأمن السيبراني.

ثانيًا نماذج المحاكم الخاصة في الدول الأجنبية

1-ماليزيا:

(1) أنظر د. محمد السعيد القزعة، نحو قضاء جزائى متخصص، مرجع سابق، ص116، وص 126

في ضوء تزايد خطر الجرائم الإلكترونية والحاجة إلى معالجة فعّالة لقضاياها، أعلنت الحكومة عن إنشاء محكمة خاصة للجرائم الإلكترونية. وقد بدأت أول محكمة خاصة للجرائم الإلكترونية، ومقرها مجمع محاكم كوالالمبور، أعمالها في الأول من سبتمبر 2016، ومن بعد هذا التاريخ تم انشاء محاكم من ذات النوع في باقي الولايات، وتضم هذه المحاكم قضاةً متخصصين ومدربين للنظر في قضايا الجرائم السيبرانية وغيرها من القضايا المدنية المتعلقة بالحاسوب[1].

2-الهند:

بموجب قانون تكنولوجيا المعلومات لعام 2000 تم انشاء محكمة الاستئناف السيبرانية لتختص بتسوية المنازعات السيبرانية، وتهدف إلى توفير اجراءات عادلة ونزيهة للأفراد والشركات في المجال الرقمي وتلعب دورًا بالغ الأهمية في كل ما يتعلق بحوادث الأمن السيبراني، وتتشكل المحكمة من رئيس، وهو عادةً قاضٍ متقاعد من المحكمة العليا أو إحدى المحاكم العليا إلى جانب أعضاءً خبراء ذوي معرفة في مجالات مثل تكنولوجيا المعلومات والأمن السيبراني والقانون. وتتمتع محكمة الاستئناف بسلطة قضائية حصرية على المسائل المنصوص عليها في قانون تكنولوجيا المعلومات[2].

3-**تركيا:**

في عام 2021 أصدر مجلس القضاء في تركيا قرارًا بإنشاء محاكم متخصصة للنظر في الجرائم الإلكترونية والمالية، وقد نُشرت قرارات المجلس بشأن إنشاء محاكم متخصصة جديدة في الجريدة الرسمية التركية بتاريخ 30 نوفمبر/تشرين الثاني 2021. وبناءً على ذلك، ستُخضَع الجرائم الإلكترونية والجرائم المالية، إلى جانب بعض الجرائم الأخرى، لسلطة المحاكم المتخصصة. على أن تُطبَّق قرارات المجلس اعتبارًا من 15 ديسمبر 2021، وقد جاءت تلك القرارات بهدف ضمان توحيد الممارسات وزيادة الكفاءة[3].

---

(1) Edwin Lee, Special Cyber Court and E-Court, May 24, 2018, at: https://lpplaw.my/insights/e-articles/special-cyber-court-and-e-court/

(2)Cyber Appellate Tribunal, https://lawforeverything.com/cyber-appellate-tribunal/

(3) Can Sozer & others, Establishment of Courts that Specialize in Cybercrimes and Financial Crimes1/12/2021 at https://www.esin.av.tr/2021/12/01/establishment-of-courts-that-specialize-in-cybercrimes-and-financial-crimes/

ومـــن أهـــم الجـــرائم التـــي ســـتختص بهـــا تلـــك المحـــاكم المتخصصـــة:

- السرقة المؤهلة والاحتيال المرتكب من خلال استخدام أنظمة المعلومات
- الاحتيال المؤهل من خلال قيام الفرد المعني بتقديم نفسه كموظف عام أو موظف في بنك أو مؤسسة تأمين أو ائتمان أو التصريح بأنه مرتبط بهذه المؤسسات والمنظمات
- الوصول إلى نظام معالجة البيانات، أو إعاقة النظام أو تدميره، أو حذف البيانات أو تغييرها
- الاستخدام غير السليم للبطاقات المصرفية أو الائتمانية
- استخدام الأجهزة أو البرامج المحظورة
- فرض الاحتياطات الأمنية على الجهات الاعتبارية المستفيدة من الجرائم الإلكترونية

4-الفلبين:

تحدد الجرائم الإلكترونية في الفلبين وفقًا لقانون الجمهورية رقم 10175، إلى جانب قانون منع الجرائم الإلكترونية لعام 2012، وادراكًا للحاجة إلى الخبرة المتخصصة، خصصت المحكمة العليا بعض محاكم الإجراءات الجنائية باعتبارها "محاكم للجرائم الإلكترونية" للتعامل مع انتهاكات قانون الجمهورية رقم 10175. وتقع هذه المحاكم عادة في المدن الكبرى، أو المقاطعات التي ترتفع بها نسبة ارتكاب الجرائم الإلكترونية، تمتلك محاكم الجرائم الإلكترونية المعينة في الفلبين سلطة قضائية على الأشخاص الذين يرتكبون جرائم إلكترونية إذا وقع أي عنصر من عناصر الجريمة داخل الفلبين أو كان الضحية موجودًا في الفلبين[1].

وختامًا نود التأكيد على أن الإجرام التقني قد أصبح يشكل تهديدًا خطيرًا للأمن القومي، وهو ما يستدعى التصدي له من خلال خطة واستراتيجية متكاملة تقوم على محاور ثلاث، المحور الأول هو محور الوقاية من خلال نشر الوعي بمخاطر هذه النوعية من الجرائم وآثارها المدمرة،

---

(1) Special Commercial Courts and Cybercrime Courts | Jurisdiction of Courts | JURISDICTION, January 22, 2025, https://www.respicio.ph/bar/2025/remedial-law-legal-ethics-legal-forms/jurisdiction/jurisdiction-of-courts/special-commercial-courts-and-cybercrime-courts hg.dhvm 3/4/2025

المحور الثانى ويتمثل في الاطار التشريعي وذلك من خلال تطوير التشريعات الجنائية التي تكفل عقوبات رادعة لمرتكبي هذه الجرائم، المحور الثالث وهو المتعلق بإجراءات التحقيق والملاحقة، وفي هذا الصدد لا بد من إسناد مهمة الملاحقة لجهاز أمنى مدرب على أعلى مستوى، على أن توفر له الامكانيات التقنية التي تعينه في أداء مهمته، كذلك وجود نيابة متخصصة للتحقيق في هذه النوعية من الجرائم مع تزويد أعضاءها بالخبرة في المجال السيبراني، وأخيرًا إنشاء محاكم متخصصة بالنظر في الجرائم الإلكترونية، وفي هذا الشأن يمكن تبني خطوة طويلة الأمد تتبنى في المقام الأول تفعيل الدراسات البينية[1] من خلال دمج مناهج الذكاء الاصطناعي وتقنية المعلومات ضمن مقررات كليات القانون، في سبيل تخريج دفعات مؤهلة للعمل القضائي في المجال التقني.

الخاتمة

جاء هذا البحث بهدف التعرف على مدى فاعلية وجود قضاء جنائي متخصص بالنظر في الجرائم الإلكترونية في التصدي لهذه النوعية من الجرائم ومكافحتها، ورأينا أن الأمر يقتضي في البداية التعرف على ماهية الجرائم التقنية، مع بيان خصائصها، ومخاطرها على المستوى الاقتصادي والاجتماعي والأمني، مع التعرض لبعض الجهود المبذولة على الصعيد الدولي والمحلي والوطنى لمواجهة الجرائم التقنية. وفي سبيل ذلك خصصنا المبحث الأول من الدراسة.

ثم جاء المبحث الثاني بهدف إلقاء الضوء على ماهية القضاء الجنائي المتخصص، ومن خلاله تعرضنا لتعريف المحاكم الجنائية المتخصصة، وأهمية وجودها، وفرقنا بين المحاكم المتخصصة والدوائر الخاصة، ثم تعرضنا بعد ذلك للحديث عن الشروط التي لا بد من توافرها في القضاء الجنائي المتخصص، وأخيرًا تجارب بعض الدول العربية والأجنبية في منح الاختصاص بالنظر في الجرائم الإلكترونية إلى أجهزة قضائية متخصصة، وقد انتهينا من خلال البحث إلى مجموعة من النتائج والتوصيات التي يمكن اجمالها على النحو التالي:

النتائج

1- على الرغم من أن كل الجرائم التقليدية يقابلها نموذج تقني إلا أنه لا يوجد تشريع حتى الآن يغطى كافة الجرائم التقنية.

---

(1) د. طارق السيد محمود، دور الدراسات البينية، مرجع سابق، ص109

2- نجاح الأمم المتحدة مؤخرًا في ابرام اتفاقية دولية لمكافحة الجرائم التقنية يعد خطوة هامة ستسهم في الحد من مخاطر تلك الجرائم.

3- التصدي لمخاطر الإجرام التقني يستلزم توافر استراتيجية متكاملة تقوم على محاور ثلاث وهي الوقاية، العمل على تطوير التشريعات، وجود هيئات متخصصة للملاحقة والتحقيق والمحاكمة.

4- إن وجود قضاء جنائي متخصص لا يقتصر على مجرد تعيين عدد من القضاة ومنحهم اختصاص بنظر الجرائم التقنية.

5- اتجهت العديد من الدول ومنها مصر والأردن والامارات إلى منح الاختصاص بملاحقة مرتكبي الجرائم الالكترونية إلى جهاز متخصص.

التوصيات

1- ينبغي العمل على سن تشريع مستقل بفرعيه الموضوعي والإجرائي تحت مسمي القانون الجنائي التقني كفرع مستقل تندرج تحته كافة صور الجرائم التقنية.

2- نقترح الاسراع بتفعيل دور الدراسات البينية وادراج مناهج الأمن السيبراني ضمن مقررات الدراسة بكليات القانون على نحو يسهم في تخريج دفعات مؤهلة للتعامل مع العصر التقني.

3- يفضل استكمال الاستراتيجية التي تبنتها الأردن في التصدي للجرائم التقنية وسرعة العمل على انشاء جهاز قضائي مستقل ومتخصص للنظر في الجرائم التقنية.

4- ضرورة نشر الوعي بالجرائم التقنية ومخاطرها وخصوصًا ما يرتبط منها بتقنيات الذكاء الاصطناعي مع افساح المجال لإشراك القطاع الخاص في هذه المهمة.

5- على المشرع المصري اعادة النظر في قانون المحاكم الاقتصادية وإلغاء اختصاصها بنظر الجرائم الإلكترونية، والإسراع بإنشاء كيان قضائي ينعقد له الاختصاص حصرًا بنظر هذه الجرائم.

قائمة المراجع:

1) أبو بكر أحمد همام، الآثار الاقتصادية للجرائم المعلوماتية وسبل مكافحتها، مجلة جامعة جنوب الوادي الدولية للعلوم القانونية، المجلد 6، العدد6، 2021

2) أحمد محمد براك، شرح قانون الجرائم الإلكترونية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2024.

3) تهاني محمد بن سويد، حماية الأطفال من الجرائم الإلكترونية مسؤولية مجتمعية، مجلة مستقبل العلوم الاجتماعية، المجلد 18، العدد3، الجمعية العامة العربية للتنمية البشرية والبيئية، يوليو 2024،

4) جمال محمد خلفان، و د. سلطان محمد سالم عوض، التعاون الوطني والدولي في الجرائم الالكترونية، المشكلات والحلول، مجلة المعهد العالي للدراسات النوعية، المجلد3، العدد16، يوليو 2023،

5) حاتم أحمد محمد بطيخ، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات، دراسة مقارنة، مجلة الدراسات القانونية، المجلد7، العدد1، كلية الحقوق، جامعة مدينة السادات، ملحق يوليو – اغسطس 2021

6) حرز الله محمد لخضر، جرائم الأنترنت وتحديات الأمن السيبراني: دراسة في متغيرات الجريمة ومقارباتها العلاجية.، مجلة المفكر، المجلد18، العدد1، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر 2023

7) حسينة شرون، فعالية التشريعات العقابية في مكافحة الجرائم الإلكترونية، مجلة دراسات وأبحاث، المجلد1، العدد1، جامعة زيان عاشور، الجلفة، الجزائر 2009

8) خالد عبد العال اسماعيل حسن، المسؤولية الدولية عن جرائم الأسلحة المستقلة ذاتية التشغيل، مجلة القانون والتكنولوجيا، المجلد2، العدد1، كلية القانون، الجامعة البريطانية بالقاهرة، أبريل 2022.

9) ذياب موسى البداينة، الجرائم الإلكترونية، المفهوم والأسباب، ورقة مقدمة في الملتقى العلمي الجرائم المستحدثة في ظل التغيرات والتحولات الاقليمية والدولية، عمان، الأردن، 2-2014/9/4

10) سامي جاد واصل، التعاون الدولي في مكافحة الجرائم الإلكترونية، مجلة القانون والتكنولوجيا، المجلد3، العدد1، كلية القانون، الجامعة البريطانية بالقاهرة، أبريل 2023

11) سعد فهد سعد ادبيس المطيري، مفهوم الجرائم الالكترونية وسماتها، المجلة القانونية، المجلد16، العدد5، كلية الحقوق، جامعة القاهرة، فرع الخرطوم، مايو 2023،

12) طارق السيد محمود أبو عقيل، دور الدراسات البيئية في إرساء قواعد القانون الجنائي التقني، مجلة الباحث للعلوم القانونية، المجلد 5، العدد2، كلية القانون جامعة الفلوجة، 2024

13) طارق السيد محمود، تقنيات الذكاء الاصطناعي ودورها في تسهيل الارهاب ومكافحته، مجلة جامعة الزيتونة الأردنية للدراسات القانونية، إصدار خاص، 2024.

14) عبد الإله محمد النوايسة، جرائم تكنولوجيا المعلومات، ط1، دار وائل للنشر والتوزيع، عمان، االأردن، 2017.

15) عصام حسنى الأطرش، تأثير جرائم ذوي الياقات البيضاء على الأمن القومي الفلسطيني، من وجهة نظر ذوى الاختصاص، مجلة، جامعة الشارقة للعلوم القانونية، المجلد21، العدد3، الامارات، سبتمبر 2024م.

16) فرج أحمد معروف، المحاكم المتخصصة كوسيلة للارتقاء بالعدالة، ورقة مقدمة إلى المؤتمر الرابع لرؤساء المحاكم العليا في الدول العربية، المنعقد بالدوحة سبتمبر 2013

17) كهينة علواش، مخاطر الجريمة الالكترونية عبر مواقع التواصل الاجتماعي بين اختراق الخصوصية وآليات المواجهة، مجلة دراسات، المجلد 11، العدد2، الجزائر، نوفمبر

18) ليندا شرابشة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية. الاتجاهات الدولية في مكافحة الجريمة الالكترونية، مجلة دراسات وأبحاث، المجلد 1، العدد1، جامعة زيان عاشور، الجزائر 2009

19) محمد أحمد سليمان عيسى، الجهود الدولية الإقليمية لمواجهة الجرائم الإلكترونية، مجلة العلوم القانونية، المجلد4، العدد8، كلية القانون، جامعة عجمان، يوليو 2018

20) محمد البلى العتوم، جرائم تكنولوجيا المعلومات، النظرية العامة للجرائم الالكترونية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2023.

21) محمد السعيد القزعة، نحو قضاء جزائي متخصص بنظر جرائم تقنية المعلومات، دراسة مقارنة، مجلة جيل للدراسات المقارنة، المجلد8، العدد18، مركز جيل للبحث العلمي، 2024.

22) محمد فؤاد الحريري، الإطار القانوني لتجريم القرصنة الإلكترونية في مملكة البحرين، المجلة القانونية، العدد13 هيئة التشريع والرأي، المنامة، البحرين 2023

23) محمد محمود الشركسي، تخصص القاضي الجنائي وأثره في تحقيق العدالة، مجلة العلوم والدراسات الإنسانية، العدد35، كلية الآداب، جامعة بنى غازي، ليبيا2017

24) محمد محمود فيالة، القانون الدولي والتحديات المعاصرة الجريمة السيبرانية نموذجا، مجلة الحقوق للبحوث القانونية، المجلد 2، العدد1، كلية الحقوق، جامعة الإسكندرية، 2024

25) محمود محمد صفاء الدين علي، الجهود الدولية والتشريعية لمكافحة جرائم الانترنت، مجلة البحوث القانونية والاقتصادية، المجلد54، العدد 3، كلية الحقوق، جامعة المنوفية، أكتوبر 2021 .

26) منصور فهيد سعد الحارثي، معوقات إثبات الجرائم المتعلقة بتقنية المعلومات، المجلة القانونية، المجلد 15، العدد4، كلية الحقوق، جامعة القاهرة، فرع الخرطوم، فبراير 2023

27) نايف شافي المظافرة، جرائم تقنية المعلومات في التشريع الأمريكى مقارنة بالتشريعات العربية، مجلة البحوث القانونية والاقتصادية، المجلد13، العدد83، كلية الحقوق، جامعة المنصورة 2023

28) هنادي محمود توفيق صالح، غسل الأموال عبر المتجر الإلكتروني، دراسة في التشريع الأردني، المجلة الأردنية في القانون والعلوم السياسية، المجلد16، العدد1، 2024

29) وردة شرف الدين، التعاون القضائي والقانوني لمكافحة جريمة غسيل الأموال والمرتكبة بواسطة تقنية المعلومات – وفقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، مجلة الباحث للدراسات الأكاديمية، المجلد8، العدد2، 2021،

30) وفاء نعيم، المؤتمر الدولي الثانى للعلوم الانسانية والاجتماعية، البحث العلمي في مواجهة المخاطر العالمية، الواقع والتحديات ورؤى المستقبل، المجلة الجنائية القومية، المجلد67، العدد 2، المركز القومي للبحوث الحنائية، القاهرة، 2024

31) ويليس كريش، الجانب المظلم للتكنولوجيا، مجلة التمويل والتنمية، المجلد53، العدد3، صندوق النقد الدولي، سبتمبر 2016

32) ياسر سيد فهمي، المواجهة الجنائية للجريمة الإلكترونية، دراسة تحليلية تأصيلية مقارنة، رسالة دكتوراة، كلية الحقوق، جامعة القاهرة، 2021

33) يوسف عيسى حامد، تخصص القاضي الجنائي في الفقه والقانون، مجلة حوليات كلية الشريعة، العدد7، جامعة القرآن الكريم والعلوم الإسلامية،2018

34) يوسف نفيد، المكافحة التشريعية لبعض صور الجرائم المعلوماتية وأصناف المجرم المعلوماتي، المجلة العربية للدراسات الأمنية، المجلد38، العدد2، أكاديمية نايف العربيوة للعلوم الأمنية، ديسمبر 2022م.

ثانيًا- المراجع الأجنبيّة:

1) Abel Yeboah-Ofori, Jamal-Deen Abdulai, Ferdinand Katsriku, Cybercrime and Risks for Cyber Physical Systems, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 8(1):2019

2) Ajoy P.B (2022). Effectiveness of Criminal Law in Tackling Cybercrime: A Critical Analysis. Sch Int J Law Crime Justice, 5(2).

3) Aleksandra Lisicka, Łukasz Lasek, Do we need a special court for cybercrime cases?17/11/2017 athttps://newtech.law/en/articles/we-need-a-special-court-for-cybercrime-cases

4) AL-Mulla, M.S. (2025). Cybercrime from Controllability to Subjectivity: A Serious Call for Legislative Review. In: Chawki, M., Abraham, A. (eds) Cybercrime Unveiled: Technologies for Analysing Legal Complexity. Studies in Computational Intelligence, vol 1181. Springer, Cham

5) Can Sozer & others, Establishment of Courts that Specialize in Cybercrimes and Financial Crimes1/12/2021 at

6) Christie, E.H., Ertan, A., Adomaitis, L. *et al.* Regulating lethal autonomous weapon systems: exploring the challenges of explainability and traceability. *AI Ethics* **4**, 229–245 (2024).

7) Combatting Cyber Crime,

8) Cyber Appellate Tribunal,

9) Diksha Jain, Comparative Analysis Of Cyber Laws – India, US And UAE, IJNRD | Volume 9, Issue 3 March 2024

10) Edwin Lee, Special Cyber Court and E-Court, May 24, 2018

11) Hemdani, M.G.K. (2025). Cryptocurrencies and the Dark Web: A Gateway to Money Laundering. In: Chawki, M., Abraham, A. (eds) Cybercrime Unveiled: Technologies for Analysing Legal Complexity. Studies in Computational Intelligence, vol 1181. Springer

12) Jain, R., Sonowal, B. (2025). Analyzing the Procedure for Investigation in Cybercrime and Admissibility of Electronic Evidence. In: Chawki, M., Abraham, A. (eds) Cybercrime Unveiled: Technologies for Analysing Legal Complexity. Studies in Computational Intelligence, vol 1181. Springer, Cham

13) Krishna Kumar & Praveen Gupta, A Study About Cyber Crimes And Cyber Law In India, JETIR May 2019, Volume 6, Issue 5,

14) Lanny L. Newville, Federal Probation Volume: 65 Issue: 2 Dated: September 2001,

15) Malatji, M., Tolah, A. Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. *AI Ethics* (2024)

16) 1Otero, P. (2022). Criminal Law and the Risks Posed by Internet. An Examination of Spanish Criminal Law. In: Cayón Peña, J. (eds) Security and Defence: Ethical and Legal Challenges in the Face of Current Conflicts. Advanced Sciences and Technologies for Security Applications. Springer, Cham

17) Ramadan, S.A., Qasim, A., Abdullah, A.F. (2024). Legal Liability Arising from Information Crimes in UAE Law. In: Alareeni, B., Elgedawy,

I. (eds) Opportunities and Risks in AI for Business Development. Studies in Systems, Decision and Control, vol 545. Springer

18) Rosli, W.R.W. Waging warfare against states: the deployment of artificial intelligence in cyber espionage. *AI Ethics* **5**, 47–53 (2025). https://doi.org/10.1007/s43681-024

19) Safeguarding India's Digital Landscape Key Government's Initiatives to Enhance Cybersecurity Awareness, Posted On: 25 JUL 2024 ,

20) Steve Morgan, 2024 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics,Jun 24,2024,

21) Tad Simons, Is It Time for a Court Dedicated to Cybercrime?,20Jun 2018

ثالثًا- مراجع على شبكة المعلومات الدولية:

file:///C:/Users/dr%20Tark/Downloads/s43681-024-00427-4.pdf

https://cybersecurityventures.com/cybersecurity-almanac-2024/

https://docs.un.org/ar/A/RES/56/121

https://doi.org/10.1007/978-3-030-95939-5_6

https://doi.org/10.1007/978-3-031-80557-8_12

https://www.itu.int/ITUD/cyb/cybersecurity/docs/UN_resolution_55_63.pdf

https://doi.org/10.1007/978-3-031-80557-8_6

https://doi.org/10.1007/s43681-023-00261-0

https://draya-eg.org/2022/02/24

https://encc-eg.org/pressroom/press.aspx?id=264

https://encc-eg.org/pressroom/press.aspx?id=267

https://haqqi.info/ar/haqqi/legislation/arab-convention-cyber-%E2%80%8B%E2%80%8Bcrimes

https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india

https://lawforeverything.com/cyber-appellate-tribunal/
https://link.springer.com/chapter/10.1007/978-3-031-65203-5_67
https://lpplaw.my/insights/e-articles/special-cyber-court-and-e-court/
https://ncsc.jo/Ar/List/Policies_and_Strategies_AR
https://news.un.org/ar/story/2024/03/1128737
https://news.un.org/ar/story/2024/12/1137776
https://pib.gov.in/PressReleasePage.aspx?PRID=2037115
https://pministry.gov.sy/contents/13491
https://saudijournals.com/media/articles/SIJLCJ_52_74-79.pdf
https://www.ag.gov.au/crime/publications/2022-national-plan-combat-cybercrime
https://www.albayan.ae/across-the-uae/accidents/2013-09-26-1.1967235
https://www.cisa.gov/combatting-cyber-crime
https://www.esin.av.tr/2021/12/01/establishment-of-courts-that-specialize-in-cybercrimes-and-financial-crimes/
https://www.jetir.org/papers/JETIRBW06027.pdf
https://www.thomsonreuters.com/en-us/posts/legal/justice-ecosystem-cybercrime-court/
Special Commercial Courts and Cybercrime Courts | Jurisdiction of Courts | JURISDICTION, January 22, 2025, https://www.respicio.ph/bar/2025/remedial-law-legal-ethics-legal-forms/jurisdiction/jurisdiction-of-courts/special-commercial-courts-and-cybercrime-courts hg.dhvm