جامعة الأزهر
كلية الشريعة والقانون
بالقاهرة

مجلة الشريعة والقانون

مجلة علمية نصف سنوية محكمة

تعنى بالدراسات الشرعية والقانونية والقضائية

تصدرها

كلية الشريعة والقانون بالقاهرة

جامعة الأزهر

العدد الخامس والأربعون

مايو ٢٠٢٥م

توجه جميع المراسلات باسم الأستاذ الدكتور: رئيس تحرير مجلة الشريعة والقانون

جمهورية مصر العربية – كلية الشريعة والقانون – القاهرة – الدراسة – شارع جوهر القائد

ت: 201221067852+

ت: 201028127441+

البريد الالكتروني

Journal.sha.law@azhar.edu.eg

جميع الآراء الواردة في هذه المجلة تعبر عن وجهة نظر أصحابها، ولا تعبر بالضرورة عن وجهة نظر المجلة وليست مسئولة عنها

رقم الإيـــداع

٢٠٢٥ / ١٨٠٥٣

الترقيم الدولي للنشر

ISSN: 2812–4774

الترقيم الدولي الإلكتروني

ISSN: 2812–5282

الموقع الإلكتروني

https://mawq.journals.ekb.eg/

فعالية السياسة الجنائية في مواجهة الجرائم المعلوماتية
(دراسة مقارنة في ضوء متطلبات الأمن السيبراني)

The Effectiveness of Criminal Policy in Combating Cybercrimes
A Comparative Legal Study in Light of Cybersecurity Requirements

إعداد

د. منى غازي حسان إبراهيم

أستاذ القانون الجنائي المساعد بقسم الأنظمة

كلية الشريعة والأنظمة جامعة الطائف

فعالية السياسة الجنائية في مواجهة الجرائم المعلوماتية (دراسة مقارنة في ضوء متطلبات الأمن السيبراني)

منى غازي حسان إبراهيم

قسم القانون الجنائي، كلية الشريعة والأنظمة، جامعة الطائف، الطائف، المملكة العربية السعودية.

البريد الإلكتروني: Mona_hassane@tu.edu.sa

ملخص البحث:

تواجه السياسة الجنائية المعاصرة تحديات متزايدة في ظل تطور الجرائم المعلوماتية وإرتباطها الوثيق بالأمن السيبراني، الأمر الذي إستدعى مراجعة جذرية للمنظومة الجنائية بمختلف أبعادها.

وتهدف هذه الدراسة إلى تقويم فعالية السياسة الجنائية في التصدي للجرائم المعلوماتية، من خلال تحليل الإطارين التشريعي والإجرائي في عدد من النظم القانونية المقارنة، وبخاصة في المملكة العربية السعودية، مصر، الإمارات، وفرنسا. وتعتمد الدراسة على منهج تحليلي مقارن، يرتكز على إستقراء النصوص القانونية ومضامين السياسات العامة ذات الصلة، مع رصد التحديات العملية والفقهية التي تعيق مواجهة هذه الجرائم.

وقد كشفت الدراسة عن فجوة قائمة بين تسارع التقنيات الرقمية ومرونة أدوات التجريم والعقاب والإثبات، مما يستلزم إعادة هندسة السياسة الجنائية بما يتلاءم مع خصوصية الجريمة المعلوماتية، ويحفظ في الوقت ذاته الضمانات القانونية والحقوق الرقمية.

كما توصي الدراسة بضرورة تعزيز التكامل بين التشريعات الجنائية وأدوات الأمن السيبراني وتطوير القدرات المؤسسية وتوسيع أطر التعاون الدولي، بما يفضي إلى سياسة جنائية أكثر فاعلية واستجابة لمخاطر الفضاء السيبراني المتنامية.

الكلمات المفتاحية: السياسة الجنائية، الجرائم المعلوماتية، الأمن السيبراني، التشريعات المقارنة، التعاون الدولي، الإثبات الرقمي، الردع الجنائي.

The Effectiveness of Criminal Policy in Combating Cybercrimes A Comparative Legal Study in Light of Cybersecurity Requirements

Mona Ghazi Hassane Ibrahim
Law Department, Faculty of Shari'a & Law, Taif University, Taif, Kingdom of Saudi Arabia.
E-mail: Mona_hassane@tu.edu.sa

Abstract:

Contemporary criminal policy faces escalating challenges in light of the rapid evolution of cybercrimes and their intrinsic link to cybersecurity. These developments necessitate a fundamental reassessment of the criminal justice system across its legislative and procedural dimensions. This study aims to evaluate the effectiveness of criminal policy in combating cybercrimes by analyzing legislative and procedural frameworks in selected comparative legal systems, particularly those of Saudi Arabia, Egypt, the United Arab Emirates, and France. Adopting a comparative analytical approach, the study examines legal texts and public policy orientations while identifying the practical and doctrinal challenges hindering the effective response to such crimes.

The findings reveal a persistent gap between the accelerating pace of digital technologies and the flexibility of mechanisms of criminalization, punishment, and evidence. This underscores the urgent need to redesign criminal policy to align with the specific nature of cybercrime while safeguarding legal guarantees and digital rights. The study recommends enhancing the integration between criminal legislation and cybersecurity tools, developing institutional capacities, and expanding international cooperation frameworks, thereby establishing a more responsive and effective criminal policy for the rising threats of cyberspace.

Keywords: Criminal Policy, Cybercrimes, Cybersecurity, Comparative Legislation, International Cooperation, Digital Evidence, Criminal Deterrence.

المقدمة

شهد العالم في العقود الأخيرة ثورة تكنولوجية هائلة، كان من أبرز تجلياتها انتشار الوسائط الرقمية واعتماد الأفراد والمؤسسات والدول على الشبكات المعلوماتية في مختلف جوانب الحياة. وقد رافق هذا التحول بروز نمط جديد من الجرائم عُرف بـ"الجرائم المعلوماتية"، وهي جرائم تتم باستخدام نظم المعلومات أو تستهدفها، وتمتاز بالتعقيد والانتشار العابر للحدود، مما يطرح تحديات كبيرة أمام أجهزة العدالة الجنائية.

كما أن السياسة الجنائية - بوصفها الإطار العام الذي يوجّه جهود الدولة في مجال التجريم والعقاب والوقاية - وجدت نفسها أمام واقع جديد يتطلب مراجعة شاملة في الأدوات والآليات يتناسب مع طبيعة الجريمة الرقمية وسرعة تطورها، وتنوع فاعليها، لا سيما في ظل التحديات المتزايدة للأمن السيبراني .

فالدول لم تعد تواجه مجرد اعتداءات تقليدية ؛ بل تهديدات معلوماتية قد تطال البنية التحتية الحيوية والأمن القومي مما فرض على السياسات الجنائية المعاصرة أن تتخلى عن نماذجها التقليدية، وتتجه نحو حلول تشريعية وإجرائية جديدة، تتكامل مع أدوات الأمن السيبراني، وتراعي الطبيعة التقنية المتغيرة لهذه الظاهرة.

مشكلة البحث

تكمن مشكلة البحث في التساؤل الرئيس التالي:

إلى أي مدى استطاعت السياسة الجنائية المعاصرة – على الصعيدين الوطني والدولي – مواكبة الجرائم المعلوماتية في ضوء متطلبات الأمن السيبراني ، وما أوجه القصور والإمكانات التطويرية في ذلك؟ وهل تكفي آليات التجريم والعقاب التقليدية لمواجهة طبيعة الجرائم المعلوماتية؟

وهل نجح التعاون الدولي- في ظل السياسة الجنائية- في مواجهة الجرائم العابرة للحدود؟

بل وكيف يمكن تطوير السياسة الجنائية لتعزيز متطلبات الأمن السيبراني دون الإضرار بالحقوق الرقمية؟

أهمية البحث

من هنا تنبع أهمية هذا البحث في كونه يسعى إلى دراسة مدى فعالية السياسة الجنائية في مواجهة الجرائم المعلوماتية، من خلال تحليل الأسس القانونية والتقنية التي تقوم عليها، مع إبراز التحديات التي تعيق فاعليتها في ظل البيئة الرقمية المعاصرة.

كما أن الطابع المعاصر للموضوع في ظل تسارع وتيرة الجرائم المعلوماتية وتطورها والبُعد الأمني المرتبط بالأمن السيبراني يجعله موضوعًا استراتيجيًّا لكافة الدول.

بالإضافة إلى ندرة الدراسات التي تناولت العلاقة التحليلية بين السياسة الجنائية ومتطلبات الأمن السيبراني في إطار مقارن تدفع للحاجة إلى مواءمة بين مقتضيات الحماية الجنائية ومتطلبات الحقوق والحريات الرقمية.

أهداف البحث

يسعى البحث إلى:

١. تحليل مدى ملائمة السياسة الجنائية الحالية لمواجهة الجرائم المعلوماتية.

٢. إبراز العلاقة بين السياسة الجنائية ومتطلبات الأمن السيبراني.

٣. مقارنة التجارب القانونية الوطنية والدولية في هذا المجال.

٤. تقويم مدى انسجام السياسة الجنائية مع متطلبات الأمن السيبراني في الحماية والوقاية.

٥. تقديم مقترحات لتطوير الإطار القانوني بما يعزز فعالية المواجهة الجنائية للجرائم السيبرانية.

المنهج المعتمد

أما عن المنهجية المتبعة، فقد اعتمد البحث على المنهج التحليلي لبيان المفاهيم والأسس النظرية للسياسة الجنائية والأمن السيبراني، والمنهج المقارن لرصد الفروقات والتقاربات بين التشريعات الوطنية المدروسة والبحث عن سبل تطوير السياسة الجنائية في المستقبل ، والمنهج الوصفي في تناول التحديات الواقعية والمستقبلية للجرائم المعلوماتية لوصف الظاهرة الإجرامية وأبعادها ، بالإضافة إلى توظيف المنهج الاستنباطي في استنتاج النتائج والتوصيات الملائمة.

وبهذا الإطار، يأتي هذا البحث ليشكل محاولة علمية تسهم في إثراء المكتبة القانونية العربية، وتفتح المجال أمام دراسات أكثر تخصصًا في مجال الجرائم المعلوماتية، لا سيما في ظل تسارع التحولات الرقمية وتنامي الأخطار السيبرانية.

وعليه سيتناول البحث الموضوع وفق الخطة التالية :-

خطة البحث

المبحث الأول: الأحكام العامة للإطار النظري للسياسة الجنائية والجرائم المعلوماتية

المطلب الأول : مفهوم السياسة الجنائية وتطورها

المطلب الثاني : ماهية الجرائم المعلوماتية وخصائصها القانونية

المطلب الثالث : التداخل بين السياسة الجنائية والأمن السيبراني ودوره في الوقاية من الجرائم المعلوماتية

المبحث الثاني : السياسة التشريعية في مكافحة الجرائم المعلوماتية

المطلب الأول : صور التجريم في التشريعات المقارنة

المطلب الثاني: العقوبات النظامية في ظل مبدأ التناسب العقابي

المطلب الثالث: دور المؤسسات الجنائية في مكافحة الجرائم المعلوماتية

المبحث الثالث: السياسة الإجرائية في الجرائم المعلوماتية ومتطلبات الأمن السيبراني

المطلب الأول : وسائل الإثبات الجنائي الرقمي وضوابط جمع الأدلة الرقمية

المطلب الثاني :التحديات الإجرائية للجرائم المعلوماتية

المطلب الثالث :التحديات المستقبلية وأطر التعاون الجنائي الدولي

تمهيد وتقسيم

شهد العالم في العقود الأخيرة تطورًا نوعيًّا في مجال التقنية الرقمية والاتصالات، الأمر الذي أسفر عن نشوء نمط جديد من الجرائم يُعرف بالجرائم المعلوماتية، وهي جرائم تتسم بالتعقيد، والسرعة، والعالمية، وتطرح تحديات قانونية غير مسبوقة تمس صميم وظائف السياسة الجنائية التقليدية. ولم تعد الوسائل التشريعية والإجرائية القائمة كافية لمواكبة هذا التطور، خصوصًا في ظل تصاعد المخاطر المرتبطة بالأمن السيبراني، وتزايد الاعتماد على الفضاء الرقمي في كافة مناحي الحياة.

وانطلاقًا من هذه الإشكالية، تسعى هذه الدراسة إلى مقاربة موضوع فعالية السياسة الجنائية في مواجهة الجرائم المعلوماتية من خلال معالجة ثلاثية الأبعاد، تمثل عناوين المباحث الرئيسة، وفق الآتي:

المبحث الأول ويُعنى بتأصيل الإطار النظري للسياسة الجنائية والجرائم المعلوماتية، من خلال استعراض مفاهيمها وتطورها، وتحليل خصائص الجريمة الرقمية، وإبراز التداخل القائم بين السياسة الجنائية ومتطلبات الأمن السيبراني بوصفه عنصرا حاكما في البناء التشريعي المعاصر.

أما **المبحث الثاني** فيتناول بالدراسة التحليلية المقارنة السياسة التشريعية والعقابية، من حيث صور التجريم وأساليب العقاب في عدد من التشريعات الوطنية والدولية، ومدى التزامها بمبادئ العدالة، ولا سيما مبدأ التناسب بين الجريمة والعقوبة، مع تسليط الضوء على الدور الذي تضطلع به المؤسسات الجنائية في مكافحة هذه الجرائم.

في حين يركز **المبحث الثالث** على الجانب الإجرائي، من خلال تناول السياسة الإجرائية في الجرائم المعلوماتية ومتطلبات التعاون الدولي، مع الوقوف على التحديات المتعلقة بالإثبات الرقمي، وصعوبات الملاحقة، وآفاق تطوير آليات التعاون العابر للحدود، تحقيقًا للفاعلية الجنائية دون الإخلال بالحقوق والحريات الأساسية.

بهذا البناء المنهجي، تأمل الدراسة أن تقدم إسهاما علميا جادا في تقييم مدى تكامل السياسة الجنائية المعاصرة مع مقتضيات الأمن السيبراني، بما يعزز القدرة على مواجهة هذا النمط المتجدد من الجريمة في إطار قانوني رشيد ومتوازن.

المبحث الأول
الأحكام العامة للإطار النظري للسياسة الجنائية والجرائم المعلوماتية
المطلب الأول
مفهوم السياسة الجنائية وتطورها

مفهوم السياسة الجنائية

تُعد السياسة الجنائية إحدى الركائز الأساسية في النظام القانوني لأي دولة، إذ تمثل الإطار العام الذي تُنظّم من خلاله كيفية مواجهة الظاهرة الإجرامية، والوسائل القانونية والاجتماعية المعتمدة لتحقيق الردع العام والخاص، والوقاية من الجريمة.

ويُشير مفهوم "السياسة" في اللغة إلى حسن تدبير الأمور وتنظيمها، فـ "ساسَ الناس سياسةً" أي تولّى شؤونهم ودبّر أمرهم بما يحقق المصلحة العامة[١] ، أما اصطلاحًا فالسياسة الجنائية تُفهم بوصفها مجموعة الوسائل والتدابير التي تعتمدها الدولة في مجال التجريم والعقاب والوقاية ، بغية التصدي للجريمة بمختلف أشكالها وتحقيق العدالة الجنائية بصورة توازن بين حماية المجتمع وحقوق الأفراد.

وقد عرّف بعض الفقه [٢] السياسة الجنائية بأنها "خطة الدولة في مواجهة الجريمة، وتشمل اختيار الجرائم التي يجب أن تجُرّم، وتحديد العقوبات المناسبة، وتطوير أجهزة العدالة الجنائية لتطبيق تلك السياسة بكفاءة ، بينما وصفها آخرون[٣] بأنها "الفن الذي تستخدمه الدولة في تنظيم رد فعلها ضد الظاهرة الإجرامية، سواء كان هذا الرد فعلًا تشريعيًّا أو قضائيًّا أو تنفيذيًّا.

وفي السياق المقارن، يرى بعض الفقه الفرنسي[٤] أن السياسة الجنائية تمثل "علم وفن وضع التدابير التي ينبغي أن تتخذها الدولة ضد الجريمة والمجرمين، بما يحقق الوقاية

---

(١) راجع ابن منظور، لسان العرب، مادة "ساس"، دار صادر، بيروت، ٧١١ هـ.

(٢) فهمي خليل الفريدي السياسة الجنائية المعاصرة: دراسة مقارنة، دار الثقافة للنشر، ٢٠١٤، ص١٣.

(٣) محمد عبداللطيف عبيد ، النظرية العامة للسياسة الجنائية، دار الجامعة الجديدة، ٢٠١٧، ص٩.

(4) Marc Ancel, Politique criminelle et science pénale, LGDJ, Paris, 1965, p.12.

والإصلاح معًا ؛لأنها تعبير عن الخيارات القيمية والاجتماعية للدولة في تعاملها مع الجريمة.[١]

إذن فالسياسة الجنائية هي مجموعة من المبادئ والقواعد التي تستخدمها الدولة لتحقيق الردع الجنائي ومكافحة الجرائم، من خلال تحديد طرق التجريم والعقاب، إضافة إلى وضع استراتيجيات الوقاية والتأهيل، وهي تمثل الاستراتيجية التي تعتمدها السلطات المختصة لمواجهة الظاهرة الإجرامية، من خلال مجموعة من التدابير التشريعية والتنظيمية والمؤسسية. ومن هذا المنطلق، تُعد السياسة الجنائية أداة ديناميكية تتغير وفق متطلبات المجتمع وتطور الجريمة، لاسيما مع بروز الجرائم الحديثة كالجرائم الإلكترونية، ما يفرض على المشرّع تكييف هذه السياسة بما يتوافق مع التحديات التقنية المعاصرة.

وتهدف السياسة الجنائية إلى الحفاظ على النظام العام وحماية حقوق الأفراد والمجتمع من خلال تدخل الدولة في الحالات التي تشكل تهديدًا للأمن الاجتماعي ، لأنها تعد انعكاسًا لإرادة الدولة في كيفية مواجهة السلوكيات الإجرامية، وتعتبر جزءًا من السياسة العامة للدولة التي تعتمد على مبدأ الردع سواء كان عامًّا أم خاصًّا .[٢]

وفي هذا السياق يمكن القول إن السياسة الجنائية لا تقتصر على معالجة الجرائم بعد حدوثها ؛ بل تشمل أيضًا الوقاية من حدوث الجرائم والتعامل مع المجرمين بعد ارتكابهم الجرائم (أي من خلال العقاب والتأهيل).

---

(١) كما عرفها الفقيه الألماني "فرانز فون ليست" بأنها "علم يحدد الأهداف التي يجب أن يتبعها المشرّع في التجريم والعقاب" ، راجع في ذلك ، محمود سليمان موسى، السياسة الجنائية والإسناد المعنوي ، دراسة مقارنة ، دار المطبوعات الجامعية ، ٢٠١٩، ص٢٤ وما بعدها .

(٢) أحمد مرغني ، السياسة الجنائية في مواجهة الجرائم المستحدثة، مجلة الدراسات القانونية ، العدد ٥ ، ٢٠٢٠ ، ص ١٢٥.

وأشار بعض الفقه بضرورة تمتع السياسة الجنائية بالمرونة للتكيف مع التغيرات الاجتماعية والتكنولوجية[١] في حين أشار البعض الآخر إلى ضرورة التركيز على احترام حقوق الإنسان داخل السياسة الجنائية بوصفها وسيلة لضمان العدالة الجنائية وليست مجرد وسيلة للقمع.[٢]

تطور السياسة الجنائية

مرت السياسة الجنائية بتطورات كبيرة على مر العصور، فقد تأثرت بالتحولات الاجتماعية والاقتصادية والسياسية، مما جعلها تتكيف مع احتياجات المجتمع في كل مرحلة زمنية، فبدأت بمفهوم الردع والقصاص في القوانين القديمة، لتنتقل إلى مفهوم العدالة والردع العام في العصور الوسطى، ثم تطورت في العصر الحديث لتُدمج مفاهيم إعادة التأهيل والوقاية خاصة مع بروز المدرسة الوضعية في علم الإجرام.[٣]

وفى عصر الفضاء السيبراني ، يقتضي هذا التحول قيام السياسة الجنائية بالتكيف مع التغيرات الجذرية المستجدة وظهور أشكال جديدة من الجريمة تتسم بالتعقيد والانتشار السريع، مما فرض تحديات غير مسبوقة على أدوات السياسة الجنائية التقليدية

ويمكن تقسيم تطور السياسة الجنائية إلى عدة مراحل أساسية:

١. **المرحلة التقليدية**: [٤] وارتبطت بأفكار فقهاء مثل سيزاري بيكاريا وبنتنام ، ركزت بشكل رئيس على العقوبات البدنية القاسية وأغفلت تماماً شخصية الجاني وظروف

---

(١) راجع في ذلك د محمود نجيب حسني ، شرح قانون العقوبات ، القسم العام ، دار النهضة العربية ، ٢٠٠٧ ، ص٤٥ وما بعدها .

(٢) انظر د أحمد فتحي سرور ، الوسيط في الإجراءات الجنائية ، دار الشروق ،٢٠١٥، ص١٢٣.

(٣) محمد فهد الجصعي، علم السياسة الجنائية ، مكتبة دار الزمان للنشر، ٢٠٢١، ص٨٠، وراجع أيضاً عبدالفتاح بيومي ، السياسة الجنائية المعاصرة ومواجهة الجرائم المعلوماتية ، دار الفكر العربي، الإسكندرية ،٢٠١٩ ، ص٦٧.

(٤) راجع في ذلك محمود سليمان موسى ، السياسة الجنائية والإسناد المعنوي، دراسة مقارنة ، دار المطبوعات الجامعية ٢٠١٩، ص٧٦.

الجريمة ، فلقد كانت السياسة الجنائية آنذاك تركز على مبدأ الشرعية والعدالة المطلقة مع العقوبات الثابتة التي تتميز بالقسوة.

٢. **المرحلة الإنسانية**:[١] التي ارتبطت بظهور المدرسة الوضعية وأفكار لومبروزو وجاروفالو وفيري حين أخذت طابعًا أكثر إنسانية وبدأت في إلغاء العقوبات القاسية ونادت بتفريد العقوبة واعتبرت الجريمة ظاهرة اجتماعية يمكن دراستها علمياً ، ويرى الفقه الحديث أنها مرحلة مهدت لتحديث السياسة الجنائية .

٣. **المرحلة الحديثة والمتكاملة**:[٢] مع تطور المجتمعات الصناعية والنمو السكاني، تطورت السياسة الجنائية لتشمل استراتيجيات أكثر شمولًا، مثل برامج الوقاية من الجريمة وبرامج التأهيل للمجرمين. كما أصبح الإهتمام يتركز على تحليل السلوك الإجرامي ومحاولة فهمه من خلال علم الجريمة. وبدأ الاهتمام يتزايد بالمؤسسات القانونية والاجتماعية التي تسهم في حماية المجتمع، مثل الشرطة و المحاكم، والسجون.

٤. **المرحلة المعاصرة**:[٣] بدأ التركيز على التطور التكنولوجي الذي أثر بدوره في تطور الجرائم ، أصبح من الضروري مواجهة الجرائم المستحدثة التي ترتكب في الفضاء السيبراني، مما دفع إلى تطوير السياسات الجنائية لتشمل تقنيات جديدة مثل التحقيقات الإلكترونية وحماية المعلومات. إضافة إلى ذلك شهدت السياسة الجنائية في هذه المرحلة تطورًا في التفكير حول العقوبات، حيث بدأت العديد من الدول في التفكير في عقوبات بديلة مثل الغرامات والبرامج الإصلاحية المجتمعية، التي تهدف إلى تحقيق إعادة تأهيل أفضل للجناة.

---

(١) أ كرم نشأت إبراهيم ،السياسة الجنائية دراسة مقارنة ، دار الثقافة للنشر ،٢٠٢١، ص٥١.

(٢) منى خليل المصري، السياسة الجنائية في مواجهة الجرائم السيبرانية، مجلة كلية الحقوق، جامعة الإسكندرية، العدد ٧١، ٢٠٢١،ص١٤.

(3) 13Julien Bacach, "Le droit pénal et les cybercriminals, l'évolution de la législation française, Presses Universitaires de France, 2021,p78

تأثير الجرائم المعلوماتية في السياسة الجنائية

أدى تزايد استخدام التكنولوجيا وانتشار الإنترنت إلى ضرورة تحديث السياسات الجنائية لمواكبة هذا التطور، فقد أسفرت الجرائم المعلوماتية عن ظهور تحديات جديدة تتطلب تعديل الفلسفات الجنائية القديمة. وهذا يتضمن:

التحديات القانونية: الحاجة إلى تحديث القوانين الجنائية لمواكبة الجرائم الرقمية الجديدة.

التحديات الإجرائية: تطوير أدوات التحقيق والبحث الجنائي في الجرائم الإلكترونية.[١]

التحديات الوقائية: إنشاء آليات للتوعية وحماية الأفراد والمجتمعات من المخاطر الرقمية.

تطور النصوص القانونية في بعض الأنظمة الوضعية

تم إصدار نظام مكافحة جرائم المعلوماتية [٢] السعودي الذي يعاقب على الجرائم المرتكبة باستخدام الوسائل الإلكترونية كالقرصنة الإلكترونية والتلاعب بالبيانات ، ويشمل النظام أيضًا الجرائم المتعلقة بالتحريض على العنف عبر الإنترنت أو التشهير بالأفراد. ويتماشى هذا النظام مع سياسة الدولة في حماية الأمن الرقمي[٣]، مما يعكس تطورًا في السياسة الجنائية لمواكبة الجرائم الجديدة التي تنشأ نتيجة التقدم التكنولوجي.

وفي الأنظمة القانونية المصرية يُعد قانون مكافحة جرائم تقنية المعلومات من أبرز التشريعات التي تنظم الجرائم المعلوماتية الذي يهدف إلى مكافحة جرائم القرصنة

---

(1) Saphy Lal Bullu, the global development of ICT, a quest for an assessment on the uncertainty impacts on countries development challenge to fight against corruption, National Journal of Cyber Security Law, Vol.8 No.2, 2025,p17.

(٢) نظام مكافحة الجرائم المعلوماتية الصادر بموجب المرسوم الملكي رقم م/ ١٧ لعام ٢٠٠٧. راجع نص النظام عبر الموقع الرسمي لمجلس الشورى السعودي.

(٣) مها حمد القريني ، واقع الجرائم المعلوماتية في المملكة العربية السعودية، تحليل قانوني، دار الكتب القانونية، ٢٠٢١، ص ١٧.

الإلكترونية والتشهير والاحتيال الإلكتروني، حماية البيانات الشخصية. ويُعتبر محاولة لتطوير السياسة الجنائية في مصر لمواكبة التحديات الرقمية.(١) كما أصدرت الإمارات العربية المتحدة مرسوما بقانون اتحادي رقم ٥ لسنة ٢٠١٢، لمكافحة جرائم تقنية المعلومات،٢٠١٢.

أما في النظام الفرنسي فتوجد العديد من التشريعات التي تتناول الجرائم المعلوماتية (٢)، تشمل الجرائم المتعلقة بالقرصنة، والتسلل إلى الأنظمة الحاسوبية ، وسرقة البيانات الشخصية.

---

(١) على سبيل المثال، المادة ٢٥ من القانون تفرض عقوبات على دخول أنظمة المعلومات بقصد التلاعب أو التغيير غير المشروع للبيانات ، راجع قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨، الموقع الرسمي للجريدة الرسمية المصرية.

(٢) قانون تعزيز الثقة في الاقتصاد الرقمي (LCEN) صدر في ٢١ يونيو ٢٠٠٤ ، ينظم التجارة الإلكترونية ومسئولية مزودي الخدمة والنشر الإلكتروني ، كما يعتبر من أهم الأسس التشريعية الأولى لتنظيم الفضاء الرقمي في فرنسا ...Légifrance-Loi LCEN

وهناك قانون الجمهورية الرقمية الصادر في أكتوبر ٢٠١٦ والذي يتناول تعزيز الحقوق الرقمية وحماية البيانات وإتاحة البيانات العامة .

، Légifrance-Loi République numérique أيضاً قانون حماية البيانات الشخصية (قانون المعلومات والحريات) الصادر في ١٩٧٨ الذي تم تعديله عدة مرات ليتوافق مع اللائحة العامة الأوروبية لحماية البيانات (GDPR) التي دخلت حيز التنفيذ في ٢٥ مايو ٢٠١٨ وتطبق مباشرة في فرنسا دون حاجة إلى قانون وطني ، وتنظم حماية البيانات الشخصية ومعالجتها للدول الأعضاء في الاتحاد الأوروبي. EUR-LEX-GDPR . هذا إلى جانب قانون العقوبات الفرنسي الخاص بالجرائم المعلوماتية رقم ٩٢-١٣٣٦ الصادر في ١٦ ديسمبر ١٩٩٢ وبدأ سريانه في ١ مارس ١٩٩٤ وهو يجرم الدخول غير المشروع إلى الأنظمة المعلوماتية .Cod pénal –Articles323-1 a 323-7

وتستند السياسة الجنائية الفرنسية في هذا المجال إلى التوجهات الأوروبية التي تهدف إلى تحقيق التعاون بين الدول لمكافحة الجرائم الإلكترونية. كما تتضمن القوانين الفرنسية عقوبات مشددة ضد المجرمين الذين يستغلون التقنيات الحديثة في ارتكاب الجرائم.

إذن يمكن القول إن السياسة الجنائية قد تطورت عبر العصور، بما يتناسب مع التحولات الاجتماعية والتكنولوجية. وفي الوقت الراهن، أصبحت ضرورة تطوير هذه السياسة أكثر إلحاحًا في مواجهة الجرائم المعلوماتية التي تتطلب استراتيجيات جديدة ومتطورة لمكافحتها. إن التحديات التي تطرحها هذه الجرائم تشير إلى الحاجة الملحة لتحديث التشريعات والإجراءات الجنائية بما يواكب التطور التكنولوجي والرقمي، وهو ما نراه في الجهود المبذولة من قبل الدول المختلفة مثل مصر والسعودية وفرنسا في تبني تشريعات قانونية حديثة ومتطورة.

المطلب الثاني
ماهية الجرائم المعلوماتية وخصائصها القانونية

في ظل الثورة الرقمية والتطور التكنولوجي السريع، ظهرت فئة جديدة من الجرائم المعروفة بالجرائم المعلوماتية، التي تستهدف الأنظمة المعلوماتية والبيانات الرقمية. لا تُعتبر الجرائم المعلوماتية مقتصرة على التقنيات الحديثة فحسب، بل تشمل أيضًا جميع الأفعال التي تضر بالبيانات والمعلومات باستخدام الوسائل الرقمية. هذه الجرائم تشكل تحديًا كبيرًا للأجهزة التشريعية والقضائية في مختلف البلدان، بما في ذلك السعودية، مصر، وفرنسا، حيث تتطلب تحديثًا مستمرًّا للقوانين لمواكبة هذا النوع من الجرائم. في هذا المطلب، سيتم تحديد ماهية الجرائم المعلوماتية، مع تحليل خصائصها القانونية من خلال القوانين المعمول بها في هذه الدول.

تعريف الجريمة المعلوماتية وتمييزها عن الجرائم التقليدية

شهد العالم تحولاً جذريًّا في طبيعة النشاط الإجرامي مع بزوغ عصر المعلومات ، فقد أصبحت التكنولوجيا الرقمية أداةً وهدفاً للجريمة في آنٍ واحد. وقد أسفر هذا التطور عن ظهور نوع جديد من الجرائم عُرفت باسم الجرائم المعلوماتية التي تختلف في بنيتها ووسائلها عن الجرائم التقليدية.

وتُعرّف الجريمة المعلوماتية بأنها: "كل فعل غير مشروع يتم باستخدام الأجهزة الحاسوبية أو الشبكات أو الأنظمة الرقمية، ويستهدف بيانات أو نظمًا أو خدمات إلكترونية بطريقة مباشرة أو غير مباشرة".

كما يمكن تعريفها بأنها الأفعال الإجرامية التي تُرتكب باستخدام وسائل تقنية المعلومات الحديثة، مثل الحواسيب، الإنترنت، أو أي نوع آخر من الشبكات الرقمية، حيث يُمكن لهذه الجرائم أن تؤدي إلى تعريض الأفراد والمؤسسات لمخاطر اقتصادية ، اجتماعية، وأمنية جسيمة ، مما يجعل معالجتها أمرًا حيويًّا في الإطار التشريعي والقانوني الحديث.

وقد تبنّت اتفاقية بودابست بشأن الجريمة السيبرانية [١] تعريفها بشكل عملي حين نصّت على تجريم الأفعال التي تستهدف سرقة البيانات، اختراق الأنظمة، ونشر البرمجيات الضارة، وغيرها من السلوكيات التي تُخلّ بالأمن الرقمي.

وقد عرّفها نظام مكافحة الجرائم المعلوماتية السعودي بأنها: "أي فعل يُرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام"[٢].

والملاحظ وجود جدل فقهي واضح حول تعريف الجريمة المعلوماتية ، وهو ناتج عن الطبيعة التقنية المتغيرة لهذا النوع من الجرائم وتداخلها مع مفاهيم قانونية تقليدية في ظل تعدد صورها وتطورها المستمر.[٣]

خصائص الجرائم المعلوماتية القانونية

تتميز الجرائم المعلوماتية بجملة من الخصائص، من أبرزها:

١. العالمية: تميل الجرائم المعلوماتية إلى أن تكون عابرة للحدود، مما يعني أنها قد تُرتكب من قبل أشخاص أو مجموعات في دول مختلفة. هذا يعقد عملية التحقيق والملاحقة القضائية، إذ تتداخل السلطات الوطنية مع القوانين الدولية، مما يستلزم التعاون بين الدول لمكافحة هذه الجرائم، من الممكن أن ترتكب الجريمة في دولة ويظهر آثارها في دولة أخرى.[٤]

---

(1) Budapest Convention on Cybercrime, Council of Europe, 2001, Article 2. https://www.coe.int/en/web/cybercrime/the-budapest-convention

(٢) راجع المادة الأولى من نظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/ ١٧ بتاريخ ٨/ ٣/ ١٤٢٨ موقع هيئة الخبراء https:llwww.boe.gov.sa

(٣) ويرى بعض الفقه أن التوسع المفرط في التعريف قد يؤدي إلى الغموض التشريعي، ويفضل اعتماد تعريف دقيق يرعي مبدأ الشرعية ...راجع د أحمد فتحي سرور ، مرجع سابق ، ص٨٩....وراجع أيضا....

Pieter Wolters, the EU digital services ACT,
what does it mean for online advertising and adtech ? , International Journal of Law and Information Technology, Oxford university press, Vol.33, Issue 1, 2025,p 76,

(4) Vàclav Janecek, rethinking law, regulation, and technology, International Journal of Law and Information Technology, Oxford university press, Vol.30, Issue 4, winter, 2022,p36.

٢. التطور المستمر: تتسم الجرائم المعلوماتية بتطور مستمر، حيث تظهر أساليب وتقنيات جديدة بصفة مستمرة. مما يجعل من الصعب على المشرعين مواكبة هذه التغييرات بشكل مستمر. هذا يخلق تحديًا قانونيًّا كبيرًا في وضع قواعد قانونية متطورة وفعالة في مواجهة الفضاء السيبراني.(١)

٣. السرعة وانتشار مع التخفي: تتميز الجرائم المعلوماتية بسرعة التنفيذ، حيث يمكن ارتكاب الجريمة في غضون دقائق قليلة من خلال الإنترنت. كما أن المجرم يمكن أن يُخفي هويته باستخدام تقنيات مثل الشبكات الافتراضية الخاصة (VPN) أو البرمجيات المشفرة(٢)، مما يعقد مسألة تحديد هوية الجاني، في كثير من الحالات لا يتم اكتشاف الجريمة إلا بعد فوات الأوان ، وأدواتها وأساليبها تتغير بوتيرة سريعة.

٤. الاستهداف المباشر للأنظمة المعلوماتية: ترتكز الجرائم المعلوماتية بشكل رئيس على الأنظمة الحاسوبية، إذ تستهدف البيانات الإلكترونية بشكل مباشر(٣). ولا تقتصر هذه الجرائم على الأفراد فحسب، بل تشمل أيضًا الشركات والمؤسسات الحكومية، وهو ما يعكس خطورة هذه الجرائم على مستوى الأمن الوطني والدولي.

٥. التأثيرات القانونية الكبيرة: تُعد الجرائم المعلوماتية من الجرائم التي يمكن أن تترتب عليها أضرار جسيمة للأفراد والمجتمعات على حد سواء. فقد يؤدي اختراق البيانات الشخصية(٤) أو سرقة المعلومات المالية إلى الإضرار بالثقة العامة في الأنظمة الإلكترونية والشبكات.

---

(١) ICTLC نظرة جديدة على اتفاقية بودابست بشأن الجرائم الإلكترونية
https://www.ictlc.com/a-new-look-at-the-budapest-convention-on-cybercrime/?lang=en

(٢) نظام مكافحة الجرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم م/ ١٧ بتاريخ ٨/ ٣/ ١٤٢٨ ، المادة السادسة.

(3) Loi n° 2015-993 du 17 août 2015 relative à la lutte contre le terrorisme et le crime organisé, Légifrance Loi lutte contre le terrorisme.

(4) Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique , Légifrance – Loi République numérique.

٦.الصعوبة الإثباتية: تتطلب خبرات تقنية وإجراءات متخصصة لجمع الأدلة نظراً لطابعها غير المادي، فهي تُرتكب عبر فضاء غير ملموس عبر الإنترنت [١].

لذا يمكن تميز الجريمة المعلوماتية عن الجريمة التقليدية من عدة جوانب منها:

طبيعة الوسيلة المستخدمة - فالجريمة المعلوماتية ترتكب غالبًا عن بُعد، باستخدام الوسائط الرقمية.

سرعة التنفيذ وصعوبة التتبع – حيث يتم تنفيذها في ثوانٍ معدودة ، وغالبًا ما تُستخدم وسائل لإخفاء هوية فاعلها.

عالمية التأثير-لأنها تؤثر على ضحايا من الممكن أن يكونوا في دول متعددة في وقت واحد، مما يخلق تعقيدًا قانونيًا في تحديد الاختصاص القضائي.

طبيعة الدليل - فدائماً يكون الدليل الرقميُّ غير مرئي، مما يُصعّب من جمعه وتوثيقه.

ومن أمثلة الجرائم المعلوماتية ، اختراق الأنظمة غير المشروع ، نشر البرمجيات الخبيثة، التصيّد، القرصنة الإلكترونية، الاحتيال الإلكتروني، التشهير الإلكتروني، وانتهاك الخصوصية الرقمية. [٢]

ولا شك أن لكل نوع من هذه الجرائم تأثيرات قانونية تفرض على التشريعات الوطنية ضرورة المراجعة المستمرة لضمان فعالية المواجهة القانونية.

التحديات التي تفرضها الجرائم المعلوماتية على السياسة الجنائية

أولاً: تحديات التجريم

من أبرز التحديات أمام السياسة الجنائية في مجال التجريم:

تحديد الأفعال التي تستوجب العقاب في ظل تطور أدوات الجريمة وتعدد صورها.

---

(١) الملف الوطني لمجلس أوروبا بشأن تشريعات الجرائم الإلكترونية في فرنسا
https://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/cyber_cp_France_2011.

(٢) نايف خالد الشريف ، الجرائم المعلوماتية في النظام السعودي ، دراسة مقارنة ، دار حافظ ، ٢٠١٩ ص٤٥.

مبدأ الشرعية الذي يفرض على المشرّع صياغة نصوص دقيقة ومحددة.

صعوبة مواكبة النصوص القانونية للتطور التقني المستمر.

ثانياً: تحديات الإثبات

تمثل مسألة الإثبات في الجرائم المعلوماتية إحدى أهم التحديات، نظرًا لغياب الأدلة المادية التقليدية، والاعتماد على أدلة إلكترونية معقدة، مثل سجلات الدخول، والعناوين الرقمية، والبصمات الرقمية، مما يتطلب خبرات فنية متقدمة.

ثالثاً: تحديات العقوبة والتنفيذ

تتطلب الجرائم المعلوماتية عقوبات مرنة تتناسب مع خطورتها الرقمية.

كما تطرح إشكاليات في تنفيذ العقوبات عبر الحدود، بسبب اختلاف الأنظمة القانونية بين الدول.[١]

رابعاً: تحديات التعاون الدولي

نظرًا للطابع العابر للحدود، تصبح آليات التعاون الدولي ضرورة حتمية [٢]، لكن هذا التعاون يصطدم بعدة عراقيل:

اختلاف التشريعات الوطنية، نقص الثقة المتبادلة بين الدول.[٣]، ضعف البنية التقنية في العديد من الدول النامية.

---

(١) مصطفي أحمد موسى ، الجرائم المعلوماتية في القانون المصري، دار النهضة العربية. ٢٠٢٢ ، ص٢٩.

(2) Edward Miller, Cybercrime and Digital Evidence, Oxford University Press 2022,P 55.

(٣) تقرير مشترك بين الوزارات الأوروبية حول مكافحة الجرائم الإلكترونية

http://www.ladocumentationfrancaise.fr/rapports-publics/144000372/

المطلب الثالث
التداخل بين السياسة الجنائية والأمن السيبراني ودوره في الوقاية من الجريمة المعلوماتية

أولاً: مفهوم الأمن السيبراني

يُقصد بالأمن السيبراني مجموعة الإجراءات والتقنيات والاستراتيجيات التي تهدف إلى حماية الأنظمة الرقمية والشبكات والبيانات من الهجمات أو الأضرار، ومنع الوصول غير المشروع للبيانات. وقد بات الأمن السيبراني عنصرًا أساسيًّا في حماية الأمن القومي، والاقتصادي، والاجتماعي للدول.(١)

وقد عرّف الاتحاد الدولي للاتصالات (ITU) الأمن السيبراني بأنه "حماية نظم المعلومات من التهديدات الإلكترونية لضمان توافرها وسريتها وسلامتها".(٢)

وإذا كانت الجرائم المعلوماتية تشير إلى الأفعال الإجرامية التي ترتكب بواسطة التكنولوجيا الرقمية ، فإن الأمن السيبراني يكون مجموعة من الإجراءات الوقائية التي تهدف إلى حماية الأنظمة والشبكات من المخاطر الرقمية .

ثانيًا: الأبعاد القانونية للأمن السيبراني

يتداخل الأمن السيبراني مع السياسة الجنائية من خلال عدة جوانب قانونية، أهمها:

التجريم الوقائي: بمعنى تجريم الأفعال التي تهدد البنية المعلوماتية حتى قبل وقوع الضرر.(٣)

---

(١) أحمد عبد الظاهر، الحماية الجنائية للأمن السيبراني، دار الجامعة الجديدة، الإسكندرية، ٢٠٢١. ص ٣٥.

(٢) ITN وكالة الأمم المتحدة المتخصصة في مجال التقنيات الرقمية ويقود الابتكار في مجال تكنولوجيا المعلومات والاتصالات مع ١٩٤ دولة عضوًا وأكثر من ١٠٠٠ شركة وجامعة ومنظمة دولية وإقليمية ، لمزيد من المعلومات راجع الموقع الإلكتروني

راجع https:llwww.itu.int

(3) Katie Logos, estaplishing a framework for the ethical and legal use of web scrabers by cybercrime and cybersecurity researchers, International Journal of Law and Information Technology, Oxford university press, Vol.31, Issue 3, 2023.

التنظيم القانوني للبنية التحتية الرقمية الحيوية، مثل الطاقة، والاتصالات، والبنوك.

إلزام المؤسسات باتخاذ تدابير الحماية السيبرانية.

حماية الخصوصية الرقمية بوصفها جزءاً من الأمن المعلوماتي الشامل.

السياسة الجنائية ومتطلبات الأمن السيبراني

أولاً: من التجريم إلى الوقاية

لم تعد السياسة الجنائية تعتمد فقط على العقاب [١]، بل اتجهت نحو تدابير وقائية تشمل:

رفع مستوى الوعي الرقمي لدى الأفراد.

إلزام مزودي الخدمات الرقمية بالتبليغ عن الاختراقات.

استخدام التكنولوجيا الاستباقية في الرصد والتحليل.

ثانيًا: دعم التحقيقات الرقمية

يتطلب الأمن السيبراني دعم الأجهزة الأمنية والقضائية بوسائل حديثة، مثل:

أدوات تحليل البيانات الضخمة (Big Data).

الذكاء الاصطناعي لتتبع السلوك الإجرامي عبر الإنترنت.

اتفاقيات تعاون فني دولية لتبادل الأدلة والمعلومات.[٢]

ثالثًا: تحدي التوازن بين الحماية والحقوق

على الرغم من الحاجة إلى حماية الأمن السيبراني، إلا أن هناك تحديًا كبيرًا في الحفاظ على الحقوق الرقمية للأفراد، لا سيما:

حرية التعبير.، حماية البيانات الشخصية.، عدم التعسف في المراقبة أو جمع الأدلة.[٣]

وهذا يتطلب رقابة قانونية صارمة على الإجراءات الأمنية، وضمان التناسب بين الإجراءات ودرجة التهديد.

---

(١) منى خليل المصري، السياسة الجنائية في مواجهة الجرائم السيبرانية، مجلة كلية الحقوق، جامعة الإسكندرية، العدد ٧١، ٢٠٢١.ص١٠٢

(2) Budapest Convention on Cybercrime, Council of Europe, 2001, Article 2.36

(٣) سامي عبد الباقي، الأمن السيبراني كمدخل للوقاية من الجريمة الإلكترونية، مجلة البحوث القانونية، جامعة عين شمس، ٢٠٢٠ ص ٥٦.

تقييم فعالية السياسة الجنائية المعاصرة في ظل الأمن السيبراني

أولاً: نجاحات السياسة الجنائية

يمكن رصد بعض النجاحات المهمة، منها:

تحديث التشريعات لتواكب التهديدات الرقمية.

إنشاء وحدات تحقيق متخصصة.

التوقيع على اتفاقيات دولية مثل اتفاقية بودابست.

ثانيًا: مواطن القصور

على الرغم من الجهود المبذولة، إلا أن هناك عدة نواقص، منها:

تأخر بعض الدول في تبني تشريعات سيبرانية حديثة.

قصور في التنسيق الدولي وتبادل المعلومات.

ضعف القدرات التقنية في بعض الأجهزة القضائية والشرطية.

ثالثًا: الحاجة إلى إصلاح شامل[1]

إن مواجهة الجرائم المعلوماتية لا تتطلب فقط قوانين جديدة، بل رؤية متكاملة للسياسة الجنائية تشمل:

بناء القدرات الفنية للمحققين والقضاة.

تعزيز ثقافة الحماية الرقمية لدى المجتمع.

تطوير التعاون الإقليمي والدولي في تبادل المعلومات والتحقيقات.

الأمن السيبراني ودوره في الوقاية من الجريمة المعلوماتية

يُعد الأمن السيبراني أحد أهم المرتكزات التي تقوم عليها حماية الفضاء الرقمي. ويُقصد به: "المجموعة من الوسائل التقنية والإدارية والتشريعية التي تهدف إلى حماية

---

(1) Council of Europe, "Convention on Cybercrime" , Treaty No 185. Available online: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

وراجع في ذلك أيضاً

-Federico Casolari, the EU data ACT in context, a legal assessment, International Journal of Law and Information Technology, Oxford university press, Vol.31, Issue 4, winter, 2023,p88.

الأنظمة المعلوماتية والبنى التحتية الرقمية من أي اختراق أو تخريب أو استخدام غير مشروع".[١]

كما يسهم الأمن السيبراني بشكل مباشر في الحد من الجرائم المعلوماتية من خلال :-

١-منع الاختراقات الأمنية قبل وقوعها عبر أنظمة المراقبة والحماية .

٢-رفع الجاهزية والاستجابة السريعة للهجمات السيبرانية .

٣-دعم التحقيقات عبر الأدلة الجنائية الرقمية .

٤-تعزيز الوعي السيبراني لدى الأفراد والجهات .

وبذلك فإن الأمن السيبراني ليس فقط إجراءً تقنياً ؛ بل هو جزء من المنظومة القانونية والجنائية الحديثة لمواجهة الجرائم الرقمية ، ويكمل الجانب التشريعي والعدلي .

لذلك أولت المملكة العربية السعودية اهتمامًا متزايدًا بالأمن السيبراني[٢] حين أُنشئت الهيئة الوطنية للأمن السيبراني لتكون الجهة المختصة بالأمن السيبراني في المملكة وتتولى وضع السياسات الوطنية وتأهيل الجهات الحكومية والخاصة على حد سواء لحماية أنظمتها الرقمية.[٣]

---

(١) خالد محمد الغامدي ، مقدمة في الأمن السيبراني والجرائم المعلوماتية ، جامعة نايف للعلوم الأمنية ، ٢٠٢٠ ص ٣٣.

وراجع في ذلك أيضاً-

Saphy Lal Bullu, the global development of ICT, a quest for an assessment on the uncertainty impacts on countries development challenge to fight against corruption, National Journal of Cyber Security Law, Vol.8 ,No.2, 2025,p9.

(٢) عبد الرحمن عبد الله الشايع، الجريمة السيبرانية في النظام الجنائي السعودي، دراسة تحليلية للقوانين السعودية في حماية الأمن السيبراني من منظور جنائي ، مجلة كلية الحقوق ، جامعة الملك سعود ، العدد ٣٢، ٢٠٢٠ ..ص ٧٨

(٣) الأمر الملكي رقم(أ/ ١٧) بتاريخ ٢٦/ ٢/ ١٤٣٩ الخاص بإنشاء الهيئة الوطنية السعودية للأمن السيبراني . https:llwww.boe.gov.sa

كما أصدرت دولة الإمارات القانون الاتحادي رقم (٥) لسنة ٢٠٢٠ في شأن حماية البنية التحتية للمعلومات الحيوية، الذي يعكس إدراكًا قانونيًّا بأهمية تأمين الفضاء السيبراني بوصفه جزءا من الأمن العام.[١]

مما سبق: نرى أن السياسة الجنائية أصبحت مطالَبة اليوم أكثر من أي وقت مضى بالتكامل مع متطلبات الأمن السيبراني، من خلال تحديث التشريعات، وبناء القدرات، وتطوير التعاون الدولي، بما يحقق حماية فعالة من التهديدات الرقمية المتزايدة دون الإخلال بالضمانات القانونية والحقوق الدستورية.[٢]

(1) UAE National Cyber security Strategy, Telecommunications and Digital Government Regulatory Authority (TDRA), 2020, p. 12

(2) united Nations Office on Drugs and Crime (UNODC), Comprehensive Study on Cybercrime, 2023, p.64.

المبحث الثاني
السياسة التشريعية في مكافحة الجرائم المعلوماتية

في هذا المبحث، سيتم تحليل الأسس التشريعية التي تقوم عليها سياسة التجريم وننتقل لبحث السياسة العقابية في الجرائم المعلوماتية ، من خلال دراسة مبدأ التناسب بين الجريمة والعقوبة، وبيان العقوبات المقررة في الأنظمة القانونية المقارنة، مع الوقوف على التحديات المستقبلية وسبل تطوير الإطار العقابي .

المطلب الأول
صور التجريم في التشريعات المقارنة

تُعدُّ الجرائم المعلوماتية من أبرز القضايا القانونية التي فرضتها الثورة التكنولوجية، حيث باتت تمثل تهديدًا للأمن الرقمي والمعلوماتي على مستوى الأفراد والمجتمعات. لذا، فإن التشريعات الجنائية الحديثة تتبنى سياسة تجريم الأفعال المعلوماتية بهدف حماية النظام المعلوماتي وضمان سلامته. وأصبحت التشريعات القانونية في العديد من البلدان – مثل المملكة العربية السعودية، جمهورية مصر العربية، الإمارات العربية المتحدة، وفرنسا – تعتمد على تجريم هذه الأفعال وتعزيز العقوبات التي تترتب عليها. ومن أهم أنواع الجرائم المعلوماتية :

١. القرصنة الإلكترونية[١] تُعرَف القرصنة الإلكترونية بأنها الدخول غير المشروع إلى أنظمة الكمبيوتر أو الشبكات بغرض سرقة أو تعديل البيانات أو تدمير الأنظمة. هذه الجريمة تضر بشكل مباشر بالأفراد والشركات، حيث قد تؤدي إلى سرقة معلومات حساسة أو تعريض سمعة المؤسسات للخطر.

٢. الاحتيال الإلكتروني[٢] يتمثل في استخدام الإنترنت أو التقنيات الرقمية لخداع الأفراد أو المؤسسات بهدف الحصول على أموال أو بيانات شخصية بطرق غير قانونية. يشمل

---

(١) راجع مثلاً المادة رقم ٧ من القانون الاتحادي الإماراتي لعام ٢٠٢١.

(٢) انظر نصوص القانون الفرنسي لتعزيز الثقة في الاقتصاد الرقمي (LCEN)
Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

الاحتيال الإلكتروني مثل عمليات الدفع المزورة عبر الإنترنت أو إنشاء مواقع وهمية لجمع بيانات المستخدمين.

٣. التشهير الإلكتروني[١] ويتمثل في نشر معلومات كاذبة أو مسيئة عن شخص أو مؤسسة عبر الإنترنت بهدف تشويه السمعة. ويمكن أن تؤدي هذه الجرائم إلى أضرار معنوية جسيمة وقد تثير نزاعات قانونية معقدة.

٤. التسلل إلى الأنظمة المعلوماتية[٢]

يشمل هذا النوع من الجرائم دخولًا غير قانوني إلى أنظمة الكمبيوتر بهدف الوصول إلى البيانات أو المعلومات الحساسة، أو لتعطيل النظام بأكمله. هذا النوع من الجرائم قد يتضمن كذلك استخدام الفيروسات أو البرمجيات الضارة.

٥. الجرائم المترتبة على الهجمات الإلكترونية: وهي الجرائم التي تشمل استخدام البرمجيات الخبيثة لتدمير أو تعطيل الأنظمة الإلكترونية أو سرقة البيانات الحساسة مثل المعلومات المصرفية أو بيانات المستخدمين.

أولاً: تجريم الأفعال المعلوماتية في النظام السعودي

تسعى المملكة العربية السعودية إلى التصدي للجرائم المعلوماتية من خلال نظام مكافحة الجرائم المعلوماتية الذي يعتبر واحدًا من أهم الأنظمة القانونية التي تناولت حماية المعلوماتية وأمن الشبكات الرقمية. يهدف النظام إلى مكافحة الأنشطة الإلكترونية غير المشروعة التي تهدد الأنظمة الإلكترونية والبيانات الشخصية.[٣] ومنها:

---

(١) راجع على سبيل المثال نص المادة ٢٥ من قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨.

(٢) انظر في ذلك على سبيل المثال المواد من ٤-٧ من القانون السعودي لمكافحة الجرائم المعلوماتية لعام ٢٠٠٧.

(٣) مرسوم ملكي رقم م/ ١٧ لعام ٢٠٠٧، نظام مكافحة الجرائم المعلوماتية، الجريدة الرسمية، المملكة العربية السعودية، ٢٠٠٧.

١. القرصنة الإلكترونية: تم تجريم الدخول غير المصرح به إلى الأنظمة المعلوماتية بهدف تعديل أو تدمير البيانات.

٢. الاحتيال الإلكتروني: يشمل استخدام التقنيات الرقمية لخداع الأفراد أو المؤسسات بهدف الحصول على المال أو البيانات بشكل غير قانوني.

٣. التشهير الإلكتروني: حيث يعاقب النظام على استخدام الوسائل الرقمية في نشر معلومات كاذبة أو مسيئة بهدف تشويه السمعة.

٤. التسلل إلى الأنظمة المعلوماتية: تجريم الدخول غير المشروع إلى الأجهزة أو الشبكات الرقمية التي تتعلق بالمؤسسات أو الهيئات العامة.

ثانيًا: تجريم الأفعال المعلوماتية في النظام المصري[١]

تمثل قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ في مصر محاولة كبيرة لمواكبة التطور التكنولوجي في البلاد، حيث يهدف القانون إلى مواجهة الجرائم الإلكترونية بمختلف أنواعها.[٢] ومن الأفعال المجرمة :

١. الاختراق الإلكتروني: يعاقب القانون المصري على الدخول غير المشروع إلى الأنظمة الحاسوبية أو الشبكات الخاصة.

٢. الاحتيال الإلكتروني: يشمل أي استخدام لوسائل التواصل الإلكتروني لإيهام الأشخاص أو المؤسسات بهدف تحقيق منفعة غير مشروعة.

٣. التشهير والتهديد الإلكتروني: يعاقب على أي فعل يتضمن التشهير أو التهديد عبر الإنترنت باستخدام أساليب مثل الرسائل النصية أو الوسائل الاجتماعية.[٣]

---

(١) قانون رقم ١٧٥ لسنة ٢٠١٨، مكافحة جرائم تقنية المعلومات، الجريدة الرسمية، جمهورية مصر العربية، ٢٠١٨.

(2) Ahmed El-Badry, Egypt's Cybercrime Law: Evolution, Challenges, and Impact. Journal of International Cyber Law,2020, 17(3), P315

(٣) إسلام جمعة مصطفى، الجرائم المرتكبة باستخدام تقنيات التكنولوجيا الحديثة في القانون المصري (الواقع الافتراضي والواقع المعزز والمختلط)، رسالة دكتوراة جامعة القاهرة ، يناير ٢٠٢٤ ، وراجع أيضاً

٤. سرقة البيانات الشخصية: تجريم الحصول على بيانات المستخدمين الشخصية أو المالية دون إذن مسبق.

ثالثًا: تجريم الأفعال المعلوماتية في النظام الإماراتي

في الإمارات العربية المتحدة، يُعد النظام الخاص بمكافحة جرائم تقنية المعلومات من التشريعات المهمة التي تتعامل مع الأفعال المجرمة في مجال التقنية الرقمية.(١) ومن أبرز الأفعال المجرمة في القانون الإماراتي:

١. القرصنة الإلكترونية: يعاقب القانون الإماراتي على اختراق الأنظمة الحاسوبية أو الشبكات الرقمية بهدف الوصول إلى المعلومات أو تعديلها.

٢. الاحتيال الإلكتروني: يُجرّم استخدام الإنترنت أو التطبيقات الإلكترونية في الحصول على الأموال أو البيانات بطريقة غير قانونية.

٣. التشهير الإلكتروني: يعاقب القانون على استخدام الإنترنت في نشر محتوى يَضر بالأشخاص أو المؤسسات بهدف التشويه.

٤. التسلل إلى الأنظمة: يشمل اختراق الأنظمة الرقمية أو الشبكات للسرقة أو التدمير أو التجسس.

ويُلاحظ أن المشرّع الإماراتي وسّع نطاق التجريم ليشمل محاولات الجريمة، والتحريض، والشروع، مما يعكس رؤية وقائية واستباقية.

رابعاً :تجريم الأفعال المعلوماتية في النظام الفرنسي

تسعى فرنسا إلى وضع إطار قانوني صارم لمكافحة الجرائم الإلكترونية من خلال القانون الخاص بمكافحة الجرائم الإلكترونية، الذي يعتبر واحدًا من أهم التشريعات الفرنسية في هذا المجال.(٢) واعتمد تعديلًا مهمًّا عبر "قانون الثقة في الاقتصاد الرقمي"،

أيمن عبدالله فكري ، الجرائم المعلوماتية ، دراسة مقارنة في التشريعات العربية والأجنبية ، مكتبة القانون والاقتصاد ٢٠٢٢،ص٧١.

(١) مرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢، مكافحة جرائم تقنية المعلومات، الجريدة الرسمية، دولة الإمارات العربية المتحدة، ٢٠١٢.

(٢) قانون العقوبات الفرنسي – الجرائم المعلوماتية Code pénal – Articles 323-1 à 323-7

وجرّم أفعالًا مثل: اعتراض أو عرقلة البيانات، التلاعب بالبرمجيات، الاعتداء على الخصوصية الرقمية، كما أقرّ عقوبات مغلّظة لجرائم استهداف البنية التحتية الرقمية، وسمح باستخدام الوسائل الإلكترونية في التحقيق والإثبات.(١)

ومن أبرز الأفعال المجرمة في القانون الفرنسي:

١. القرصنة الإلكترونية: يعاقب القانون الفرنسي على دخول الأنظمة الرقمية بشكل غير قانوني بهدف الوصول إلى المعلومات أو تدمير البيانات.

٢. الاحتيال الإلكتروني: يشمل استخدام الإنترنت أو وسائل التقنية الحديثة في عمليات الاحتيال مثل التزوير الإلكتروني وعمليات الدفع المزورة.

٣. التشهير الإلكتروني: تجريم نشر محتوى كاذب أو ضار عبر الإنترنت بهدف تشويه سمعة الأشخاص.

٤. الإضرار بالأنظمة الإلكترونية: يشمل الهجمات التي تؤدي إلى تعطيل الأنظمة أو تدمير المعلومات.

وبذلك يعد تجريم الأفعال المعلوماتية من السياسات التشريعية الأساسية التي تتبناها هذه الدول لمكافحة الجرائم الإلكترونية وحماية الأفراد والمؤسسات من الأضرار المحتملة، حيث تعتمد تشريعاتها صياغة قوانين رادعة تهدف إلى تقليص نطاق هذه الجرائم، وتوفير الحماية القانونية للأفراد من تهديدات العالم الرقمي.

---

(١) البوابة الفرنسية للأمن الحاسوبي

http://www.securite-informatique.gouv.fr/

وراجع أيضاً حكم المحكمة العليا ، الغرفة الجنائية ، ٨ فبراير ٢٠١٢، تدخل البيانات وتدخل النظام

http://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000025534746

المطلب الثاني
السياسة الجنائية العقابية للجرائم المعلوماتية

أمام تصاعد وتيرة الجرائم المعلوماتية وتنوع أشكالها وأساليب تنفيذها، وجدت الأنظمة الجنائية نفسها أمام تحدٍّ حقيقي يتمثل في ضرورة بلورة سياسة عقابية فعّالة تواكب هذا التحول الجذري في بنية الجريمة. فالجرائم الرقمية لا تُرتكب فقط عن بُعد، بل أيضًا بأساليب تقنية معقدة، وأحيانًا بأدوات غير تقليدية تصعب ملاحقتها أو ضبطها بالوسائل الجنائية التقليدية.

من هذا المنطلق، أصبح لزامًا على المشرع الجنائي ألا يكتفي بمجرد التجريم، بل أن يضع نظامًا عقابيًّا يعكس خطورة هذا النوع من الجرائم، ويحقق الردع العام والخاص، دون المساس بمبادئ العدالة الجنائية وضمانات حقوق الإنسان.

العقوبات النظامية ومدى كفايتها في الردع

تُشكل العقوبات النظامية المقررة للجرائم المعلوماتية الأداة القانونية الأساسية التي تعتمدها الدول لمواجهة هذا النوع من الجرائم، وتحقيق الردع العام والخاص. إلا أن فعالية هذه العقوبات لا تتوقف على مجرد وجودها في النصوص التشريعية، بل ترتبط بمدى وضوحها، وعدالتها، وتناسبها مع خطورة السلوك الإجرامي، فضلاً عن قابلية تنفيذها في بيئة تقنية معقدة ومتحولة.

مبدأ التناسب العقابي

يعد مبدأ التناسب بين الجريمة والعقوبة أحد المبادئ الأساسية في الأنظمة القانونية الحديثة [١]، الذي يضمن أن العقوبة المقررة على الجرائم تتناسب مع خطورة الجريمة

---

(١) الولايات المتحدة تبنّت مبكرًا تشريعات رقمية مثل قانون الاحتيال وإساءة استخدام الكمبيوتر (CFAA) لعام ١٩٨٦، ويغطي هذا القانون الوصول غير المشروع إلى أنظمة الكمبيوتر. ،سرقة المعلومات الحكومية أو البنكية. نشر الفيروسات والبرمجيات الخبيثة، ويُلاحظ أن القانون الأمريكي يركز على حماية المصالح الفيدرالية ، مع تشديد العقوبات في حالة المساس بالأمن القومي أو البنى التحتية الحرجة.....راجع في ذلك

المرتكبة، سواء من حيث طبيعتها أو نتائجها. في سياق الجرائم المعلوماتية ، يعتبر تطبيق مبدأ التناسب في تحديد العقوبات أمرًا بالغ الأهمية، نظرًا للطابع المتغير والمتعدد للجرائم الإلكترونية، التي قد تتراوح من سرقة البيانات إلى الهجمات الإلكترونية المدمرة.

كما يعد من الركائز الأساسية للعدالة الجنائية في جميع النظم القانونية المختلفة ، وهو يتطلب أن تكون العقوبة المقررة متناسبة مع جسامة الفعل الإجرامي وظروف ارتكابه، بحيث لا تكون العقوبة أشد مما تقتضيه المصلحة العامة ولا أخف مما يلزم لتحقيق الردع.

غير أن تطبيق هذا المبدأ في مجال الجرائم المعلوماتية يثير إشكاليات قانونية وعملية متعددة، نظرًا لحداثة هذه الجرائم، وغموض بعض صورها، وتفاوت آثارها من حيث الخطورة والضرر. فقد ترتكب الجريمة بواسطة ضغطة زر يسيرة لكنها تُحدث خللاً في أنظمة مؤسسية حيوية أو تضر بأمن الدولة أو الاقتصاد القومي، مما يستوجب عقوبات صارمة. وفي المقابل، قد تكون الجريمة يسيرة من حيث النتيجة، لكنها تُعاقب بعقوبات شديدة تفتقر إلى التدرج، وهو ما يخُل بمبدأ التناسب.[١]

ومن التحديات في هذا السياق أن العديد من الأنظمة القانونية لم تُعدّل منظومتها العقابية لتتناسب مع خصوصية الجرائم الرقمية، فطبّقت العقوبات التقليدية كما هي، دون اعتبار للخصوصية التقنية أو البُعد السيبراني. كما أن الجرائم المعلوماتية غالبًا ما تُرتكب من أشخاص صغار السن، أو أشخاص غير معتادين على الإجرام، ما يطرح تساؤلات حول ضرورة مراعاة شخصية الجاني عند تقدير العقوبة.

وفي المقابل، فإن الإفراط في التساهل قد يُفقد العقوبة وظيفتها الردعية، ويشجع على التمادي في ارتكاب هذه الجرائم. لذا تتجه بعض التشريعات الحديثة إلى اعتماد عقوبات

Ahmed El-Badry, Egypt's Cybercrime Law: Evolution, Challenges, and Impact. Journal of International Cyber Law,2020, 17(3), P32.

(١) علي أحمد حسن ، فلسفة العقوبة الجنائية وآثر التكنولوجيا الحديثة، رسالة ماجستير جامعة القاهرة ديسمبر ٢٠٢٤.

بديلة أو تكميلية (مثل المنع من استخدام الإنترنت أو مصادرة الأجهزة)، إلى جانب العقوبات السالبة للحرية، لتحقيق موازنة دقيقة بين الردع والتأهيل وإعادة الإدماج.

ويُلاحظ أن التطبيق القضائي يلعب دورًا حاسمًا في تحقيق التناسب، من خلال سلطة القاضي في تقدير العقوبة وفقًا للوقائع والملابسات. لكن هذا يفترض وجود تشريع مرن يتيح له هامشًا كافيًا للحركة ، دون أن يكون مقيدًا بنصوص جامدة لا تراعي اختلاف الحالات.

لذلك فإن احترام مبدأ التناسب في العقاب يتطلب تطوير البنية التشريعية للعقوبات في الجرائم المعلوماتية ، على نحو يُراعي خطورة الفعل وظروف الجاني، ويضمن في ذات الوقت حماية المصالح العامة والخاصة من التعدي الإلكتروني.[1] وعليه، سنستعرض دراسة بعض العقوبات المقررة للجرائم المعلوماتية في الأنظمة القانونية المختلفة، مع التركيز على مدى تطبيق مبدأ التناسب في تحديد تلك العقوبات.

أولاً: العقوبات المقررة في النظام السعودي

في النظام السعودي، يعتمد نظام مكافحة الجرائم المعلوماتية على فرض عقوبات تتناسب مع نوع الجريمة وظروفها. وتشمل العقوبات التي يُقرها النظام السجن والغرامة المالية ، كما نص على مجموعة من العقوبات تختلف حسب جسامة الفعل المرتكب وطبيعته ، فيعاقب النظام على هذه الجرائم بعقوبات تشمل السجن لمدة تصل إلى ٥ سنوات أو الغرامات المالية التي تصل إلى ٣ ملايين ريال أو كليهما، بالإضافة إلى عقوبات منع الجاني من العمل في مجال التقنية لفترات محددة ،أو عقوبة السجن لمدة تصل إلى عشر سنوات والغرامات المالية إلى خمسة ملايين أو كلاهما معاً في جرائم أخرى مثل التشهير الإلكتروني أو الاحتيال المالي، بالإضافة إلى مصادرة الأدوات والأجهزة المستخدمة في الجريمة، وكذلك إغلاق المواقع الإلكترونية أو الحسابات المستخدمة في ارتكاب الفعل الإجرامي . ومنها أيضاً

(1) Mohamed Said El-Ghamdi, Cybercrime Legislation in Saudi Arabia, A Critical Review of the Saudi Anti-Cybercrime Law. International Journal of Cyber Law and Ethics, 14(2),2020,P 129.

١. القرصنة الإلكترونية: التي تمثل أحد أبرز الجرائم التي يعاقب عليها القانون السعودي. فيعاقب على من يقوم بالدخول غير المصرح به إلى الأنظمة المعلوماتية بهدف الإضرار أو تدمير البيانات ، وتصل العقوبة إلى السجن لمدة ٥ سنوات أو غرامة مالية تصل إلى ٣ ملايين ريال .

٢. الاحتيال الإلكتروني: ويتضمن استخدام الوسائل الرقمية لخداع الآخرين للحصول على أموال أو بيانات غير مشروعة.

كما تتراوح العقوبة بين السجن والغرامات المالية التي تصل إلى السجن ٣ سنوات أو غرامة ٢ مليون ريال .

٣. التشهير الإلكتروني: يعاقب على التشهير بالأشخاص عبر الإنترنت بالسجن لمدة لا تزيد على سنتين أو غرامة مالية.

ويلاحظ أن المشرع السعودي راعى التناسب بين العقوبة وخطورة الجريمة على الأمن السيبراني والاقتصاد الوطني وخصوصية الأفراد ، لذلك يعكس هذا النظام في قوانينه مبدأ **التناسب** من خلال فرض عقوبات تتناسب مع خطورة الجريمة ومدى تأثيرها على الأفراد أو المؤسسات، مما يضمن تحقيق العدالة الجنائية.

ثانيًا: العقوبات المقررة في القانون المصري

يتضمن قانون مكافحة جرائم تقنية المعلومات المصري نصوصًا متعلقة بالعقوبات التي تفرض على الجرائم الإلكترونية، ويعتمد هذا القانون بشكل كبير على مبدأ التناسب في تحديد العقوبة ، حيث يفرض عقوبات تتراوح بين السجن والغرامات المالية التي قد تصل إلى ٢ مليون جنيه . وقد تتضمن العقوبات الحبس المشدد في الحالات التي تتضمن أضرارًا جسيمة للأنظمة أو الأفراد. فعلى سبيل المثال

١. القرصنة الإلكترونية: يعاقب على دخول الأنظمة الحاسوبية دون إذن، وتغيير أو تدمير البيانات بعقوبة السجن إلى ٣ سنوات أو غرامة مالية تصل إلى مليون جنيه .

٢. الاحتيال الإلكتروني: ويشمل جميع الأفعال التي يتم فيها خداع الأشخاص باستخدام التقنيات الرقمية.

ويعاقب مرتكب هذه الجرائم بالحبس مدة لا تزيد عن ٣ سنوات وغرامة مالية تتراوح بين ٥٠ ألفًا إلى مليون جنيه .

٣. التشهير الإلكتروني: يعاقب القانون المصري على نشر أو بث معلومات مضللة أو مسيئة عبر الإنترنت بالسجن لمدة سنتين أو غرامة مالية، وبذلك يتضح أن القانون المصري تبنى مبدأ التناسب من خلال فرض عقوبات تتناسب مع فداحة الجريمة الإلكترونية المرتكبة، مما يضمن أن العقوبة لا تتجاوز الضرر الواقع.[١]

ثالثًا: العقوبات المقررة في القانون الفرنسي

تتبنى فرنسا سياسة صارمة في مواجهة الجرائم المعلوماتية من خلال أنظمتها التي تشمل عقوبات جنائية تتناسب مع خطورة الجرائم الإلكترونية المرتكبة ، تشمل العقوبات في فرنسا السجن لمدة قد تصل إلى ٥ سنوات وغرامات مالية قد تتجاوز ٧٥,٠٠٠ يورو في حالات الجرائم الإلكترونية الكبيرة.

١. القرصنة الإلكترونية: وتشمل الدخول غير المصرح به إلى الأنظمة الإلكترونية أو تعديل البيانات، إذ يعاقب عليها

بالسجن لمدة قد تصل إلى ٥ سنوات وغرامة مالية تصل إلى ٧٥,٠٠٠ يورو.

٢. الاحتيال الإلكتروني: يشمل جميع أنواع الاحتيال التي تتم باستخدام الإنترنت أو البرمجيات الرقمية بعقوبة السجن إلى ٥ سنوات وغرامة مالية.

٣. التشهير الإلكتروني: يعاقب على نشر بيانات كاذبة أو تشويه السمعة عبر الإنترنت بالسجن لمدة سنتين وغرامة قد تصل إلى ٣٠,٠٠٠ يورو، ويلاحظ كيف التزم القانون الفرنسي بتطبيق مبدأ التناسب من خلال تصنيف الجرائم الإلكترونية على أساس مدى خطورتها على الأفراد أو المؤسسات، مما يسمح بفرض عقوبات عادلة ومتوافقة مع الجريمة.[٢]

---

(١) قانون رقم ١٧٥ لسنة ٢٠١٨، مكافحة جرائم تقنية المعلومات، الجريدة الرسمية، جمهورية مصر العربية، ٢٠١٨.

(2) Jonsy Lemoine, J, The Role of French Cybercrime Laws in the Fight Against Digital Threats. Journal of European Cyber security Law, 10(1) 2020, p66.

رابعًا: العقوبات المقررة في القانون الإماراتي

يعاقب القانون الإماراتي على الجرائم الإلكترونية بعقوبة السجن التي قد تصل إلى ١٠ سنوات، بالإضافة إلى الغرامات المالية التي قد تصل إلى مليون درهم ، كما تفرض العقوبات على الجرائم الإلكترونية بشكل يتماشى مع مبدأ التناسب. ولننظر إلى بعض الأمثلة[١]

١. القرصنة الإلكترونية: يعاقب القانون على اختراق الأنظمة الرقمية غير المصرح به بعقوبة السجن حتى ١٠ سنوات وغرامة تصل إلى مليون درهم .

٢. الاحتيال الإلكتروني: يشمل استخدام الإنترنت لتحقيق مكاسب غير مشروعة، وتتراوح العقوبة بين السجن والغرامة المالية التي قد تصل إلى مليون درهم.

٣. التشهير الإلكتروني: يعاقب على التشهير أو نشر محتوى مسيء عبر الإنترنت بالسجن لمدة سنتين أو غرامة مالية.

ويعكس القانون الإماراتي مبدأ التناسب في تحديد العقوبات التي تتناسب مع الضرر الناتج عن الجريمة، خاصة فيما يتعلق بالعقوبات المشددة ضد الجرائم الكبيرة مثل القرصنة والاحتيال الإلكتروني.[٢]

ويلاحظ مما سبق أن العقوبات المقررة في القوانين المختلفة لمكافحة الجرائم المعلوماتية تتسم بتطبيق مبدأ التناسب، حيث يتم تحديد العقوبة بناءً على خطورة الجريمة وتأثيرها على الأفراد والمؤسسات. وتضمن هذه العقوبات تحقيق العدالة الجنائية وضمان

---

(١) مرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢، مكافحة جرائم تقنية المعلومات، الجريدة الرسمية، دولة الإمارات العربية المتحدة، ٢٠١٢.

(٢) إمام حسنين خليل عطا الله ، جرائم الاعتداء على الشبكة المعلوماتية في التشريعات العربية ، دراسة تحليلية مقارنة بالتشريع الإماراتي ، المجلة الدولية للبحوث والدراسات القانونية ، العدد٤ ، ٢٠٢٤، ص١٨ منشور باللغة الإنجليزية . http:llijlrs.vsrp.co.uk

ردع الأفراد عن ارتكاب الجرائم الإلكترونية، كما يعتمد مبدأ التناسب على تصنيف الجرائم المعلوماتية مما يسمح بتطبيق عقوبات تتوافق مع طبيعة الجريمة وضررها الاجتماعي.

وقد تنوعت اتجاهات التشريعات المقارنة في هذا السياق ، فبينما وسّعت بعض الأنظمة من نطاق العقوبات وحدّتها، تبنّت أخرى مبدأ التدرج والتناسب مع التركيز على العقوبات التكميلية والاحترازية ، مثل مصادرة الأجهزة أو إغلاق المواقع. كما برز جدل واسع حول مدى كفاية العقوبات التقليدية في الردع فظهرت دعوات متزايدة لتبني مقاربة تشريعية تستند إلى التحليل الفني لطبيعة الجريمة المعلوماتية وخصوصية مرتكبيها.

المطلب الثالث
دور المؤسسات الجنائية في مواجهة الجرائم المعلوماتية

تمهيد

أدت الطفرة التكنولوجية إلى بروز الجرائم المعلوماتية بوصفها أحد أخطر أشكال الجريمة المعاصرة، لما تتمتع به من طابع عابر للحدود وسرعة في التنفيذ وصعوبة في التتبع. وقد تطلب هذا التحدي تدخل المؤسسات الجنائية بوصفها أحد أهم الفاعلين في السياسة الجنائية الحديثة، من أجل تطوير وسائلها القانونية والفنية لمكافحة هذه الظاهرة المتنامية.

وبالإضافة إلى الدور الجوهري الذي تقوم به السلطات التشريعية في العالم لتكييف الجريمة الرقمية من خلال سن القوانين الجنائية التي تواكب التغيرات الرقمية، وتعريف الجرائم المعلوماتية بشكل دقيق، وتحدد عناصرها وأركانها. وفي هذا السياق، عمدت العديد من الدول إلى سن تشريعات خاصة لمواجهة هذه الظاهرة،[١] يأتي دور المؤسسات الجنائية المختلفة الوطنية والدولية للحماية من أخطار هذه الجرائم وملاحقة مرتكبيها :

أولاً: دور أجهزة الشرطة الجنائية (الضبطية القضائية)

أصبحت الشرطة الجنائية مكلفة بمهمة معقدة تتمثل في تتبع الأدلة الرقمية [٢]، وجمعها دون الإخلال بحقوق الأفراد في الخصوصية. ومن أبرز الأدوار التي تضطلع بها:

---

(١) فرنسا: عبر المواد ٣٢٣-١ إلى ٣٢٣-٧ من قانون العقوبات، إضافة إلى قانون ٢٠٠٤-٥٧٥ بشأن الثقة في الاقتصاد الرقمي،

والمملكة العربية السعودية من خلال نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/ ١٧ وتاريخ ٨/ ٣/ ١٤٢٨هـ (٢٠٠٧م)، الذي يحدد الجرائم والعقوبات، ويعطي صلاحيات للنيابة العامة وهيئة الاتصالات لتتبع مرتكبيها.

بالإضافة إلى الإمارات من خلال القانون الاتحادي رقم ٥ لسنة ٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات والمعدل بالقانون رقم ٣٤ لسنة ٢٠٢١، ومصر بموجب القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، الذي وضع أحكامًا مفصلة للتجريم والعقوبة والتنظيم القضائي والإجرائي.

(٢) الوكالة الوطنية لأمن أنظمة المعلومات(http://www.ssi.gouv.frANSSI/)

- إنشاء وحدات متخصصة في الجرائم الإلكترونية (مثل قسم مكافحة الجرائم الإلكترونية في فرنسا، ووحدة مكافحة جرائم تقنية المعلومات في مصر، ووحدة الأمن السيبراني في السعودية). بل أيضاً من الضروري أن تتوفر لدى الشرطة وحدات متخصصة مثل "وحدة مكافحة الجرائم الإلكترونية" التابعة لوزارة الداخلية الإماراتية التي تقوم بالرصد والتتبع الرقمي للأنشطة المشتبه بها وتحليل الأدلة الإلكترونية والتنسيق مع الهيئات الدولية مثل الإنتربول ، كما يجب أن تتمتع هذه الوحدات بقدرات مميزة في كل من

- استخدام أدوات التحليل الرقمي الجنائي (Digital Forensics) لاسترجاع الأدلة من الأجهزة الرقمية.

- التعاون مع شركات التكنولوجيا ومزودي الخدمة للحصول على البيانات.

وتقابل هذا الدور تحديات كبيرة، أهمها: التشفير، وإخفاء الهوية، واستضافة البيانات في دول أخرى.

ثانياً: دور النيابة العامة والسلطة القضائية

تُعد النيابة العامة مسئولة عن تحريك الدعوى الجنائية في الجرائم المعلوماتية، وتتطلب هذه الجرائم كفاءة قانونية وفنية عالية لفهم طبيعة الفعل المجرم. وتشمل المهام:

- إصدار أوامر بالحجز والتفتيش الإلكتروني.

- التنسيق مع الشرطة القضائية للحصول على سجلات الاتصالات.

- الإشراف على عمليات التحليل الفني للأدلة.

وراجع أيضاً-

Darsheen Kaur, beyond the firewall, understanding the complexities of cybersecurity, National Journal of Cyber Security Law, Vol.8 ,No.2, 2025,p12.

كما تُمارس النيابة دورًا محوريًّا في الإذن بجمع الأدلة الرقمية وتفتيش الأجهزة الرقمية[١]، وتحتاج إلى تطوير مهارات أعضائها في فهم طبيعة الأدلة الإلكترونية، والتعامل مع التحقيقات العابرة للحدود.

ثالثًا: دور القضاء

أما القضاء، فله دور حاسم في تقدير مشروعية وسائل الإثبات الرقمية وتكييفها ضمن قواعد الإثبات التقليدي. وقد شهدت المحاكم في مصر والسعودية قضايا نوعية تتعلق بتهديد الأمن الإلكتروني، والنصب عبر الإنترنت، والتحريض على ارتكاب جرائم إلكترونية. حيث يواجه تحديات تتعلق بقبول الأدلة الرقمية، وتقييم موثوقيتها، وفهم الأسس التقنية المرتبطة بها. ولهذا، بدأت بعض الدول في إنشاء دوائر قضائية متخصصة في الجرائم السيبرانية، لتفادي الإشكاليات الفنية التي قد تؤثر على عدالة الأحكام.[٢]

رابعاً: الهيئات الوطنية للأمن السيبراني

وتعمل على وضع الأطر لإدارة المخاطر المتعلقة بالأمن السيبراني ومتابعة الالتزام بها وتحديثها ، وإشعار الجهات المعنية بالمخاطر والتهديدات ذات العلاقة بالأمن السيبراني ووضع أطر الاستجابة للحوادث المتعلقة به.

وتجدر الإشارة إلى أنه تأسست الهيئة السعودية للأمن السيبراني لتعزيزه في المملكة ومواجهة التهديدات الإلكترونية. حيث تقوم الهيئة بتطوير السياسات والإجراءات اللازمة لحماية الأنظمة والشبكات المعلوماتية.

وقد أظهرت الجهات الأمنية والعدلية في المملكة تطوراً ملحوظاً في ضبط الجرائم المعلوماتية وملاحقتها قضائياً بدعم من تقنيات الأمن السيبراني ، مما يجعل التجربة السعودية جديرة بالدراسة ، كما تسهم جميعها في تطبيق هذه النصوص ومواكبة التحديات الحديثة .[٣]

---

(١) مصطفي عبدالباقي ، التحقيق في الجريمة الإلكترونية وإثباتها ، دراسة مقارنة ، مجلة الشريعة والقانون، الجامعة الأردنية ،المجلد ٤٥ العدد ٤ ملحق ٢، ٢٠١٨، ص١٣.

(٢) محمد جبريل إبراهيم ، التحول الرقمي في نظام القانون الجنائي ، دراسة تحليلية تأصيلية، الدار العربية للعلوم ، يناير ٢٠٢٣ ،ص١٣٢.

(٣) إبراهيم الحيدري، الضوابط الإجرائية للجرائم المعلوماتية في النظام السعودي ، المجلة القضائية السعودية ، عدد خاص ٢٠٢٢،ص١٥ ، وراجع أيضاً إيمان محمد عزام ، العقوبة في نظام مكافحة الجرائم

خامساً: دور الأفراد والمؤسسات في مكافحة الجرائم المعلوماتية إلى جانب الجهود الحكومية، يلعب الأفراد والمؤسسات دورًا حيويًّا في مكافحة الجرائم الإلكترونية.

ويمكن تحقيق ذلك من خلال إتباع مجموعة من الممارسات الأمنية من خلال:

استخدام برامج الحماية

يجب على الأفراد والمؤسسات استخدام برامج الحماية المحدثة بانتظام للحماية من الفيروسات والبرمجيات الخبيثة.

ضرورة التوعية والتدريب

تعتبر التوعية بمخاطر الجرائم الإلكترونية والتدريب على كيفية الحماية منها جزءًا أساسيًّا من الجهود المبذولة لمكافحة هذه الجرائم. تقوم الجهات الحكومية والمؤسسات التعليمية بتنظيم حملات توعية وبرامج تدريبية للمواطنين والعاملين في القطاعين العام والخاص. فيجب على الجميع أن يكونوا على دراية بالأساليب الاحتيالية الشائعة وكيفية التعرف عليها وتجنبها.

إجراءات الأمان للبيانات

ينبغي للمؤسسات تنفيذ سياسات وإجراءات صارمة لحماية البيانات الحساسة، مثل تشفير البيانات واستخدام كلمات مرور قوية.

الإبلاغ عن الجرائم الإلكترونية

يجب على الأفراد والمؤسسات الإبلاغ عن أي جرائم إلكترونية يتعرضون لها للجهات المختصة، مثل الشرطة أو الهيئات الوطنية للأمن السيبراني.

سادساً: دور المؤسسات الدولية في دعم الجهود الوطنية

تسهم المنظمات الجنائية الدولية في تطوير قواعد التعاون العابر للحدود، ومن أبرزها:

- الإنتربول: من خلال مركز الجرائم الرقمية ومذكرات التوقيف الدولي للمجرمين الإلكترونيين.

- اليوروبول: عبر وحدة EC3 المختصة بالجرائم السيبرانية.

المعلوماتية في المملكة العربية السعودية دراسة تأصيلية مقارنة ، مجلة وزارة العدل ، العدد ٨٢ ، رجب ١٤٣٩ . https:ll www.adlm.moj.gov.sa

– اتفاقية(بودابست) وهي ليست مجرد وثيقة قانونية ؛ بل هي إطار عمل يسمح لمئات الممارسين من الأطراف بتبادل الخبرات وإنشاء علاقات تسهل التعاون في حالات محددة، بما في ذلك حالات الطوارئ، بما يتجاوز الأحكام المحددة المنصوص عليها في هذه الاتفاقية ، كما يجوز لأي دولة الاستفادة من هذه الاتفاقية بصفتها دليلا أو قائمة مرجعية أو قانونا نموذجيا ، كما تعد أول اتفاقية دولية تهدف إلى توحيد الجهود التشريعية لمكافحة الجرائم المعلوماتية، وقد انضمت إليها أكثر من ٦٠ دولة حتى الآن[1].

مما سبق يتضح أن نجاح المؤسسات الجنائية في التصدي للجرائم المعلوماتية مرهون بقدرتها على مواكبة التطور التقني، وتحديث ترسانتها القانونية، وتعزيز التعاون الدولي. كما يجب التركيز على التدريب والتخصص داخل الأجهزة القضائية والضبطية، لضمان كفاءة التحقيق والملاحقة، واحترام الضمانات القانونية.

(1) Budapest Convention on Cybercrime, Council of Europe, 2001 https://www.coe.int/en/web/cybercrime/the-budapest-convention

وانظر أيضاً

–Margarita Robles, digital identity, an approach to its nature, concept and functionalities, International Journal of Law and Information Technology, Oxford university press, Vol.32, Issue 1, 2024.

المبحث الثالث
السياسة الإجرائية في الجرائم المعلوماتية ومتطلبات الأمن السيبراني
المطلب الأول
وسائل الإثبات الجنائي الرقمي وضوابطه

تمهيد :

تُعدّ الجرائم المعلوماتية من أبرز التحديات التي تواجه الأنظمة الجنائية المعاصرة، نظراً لطبيعتها التقنية المعقدة، وسرعة تطورها، وتشعب وسائل ارتكابها. وقد فرضت هذه الخصوصية واقعاً جديداً أمام جهات التحقيق والقضاء، لاسيما فيما يتعلق بمسألة الإثبات، التي تُعدّ من أهم أركان المحاكمة العادلة في المجال الجنائي.

وفي هذا السياق ، يواجه المشرعون تحدياً مزدوجاً يتمثل من جهة في ضرورة ملاءمة قواعد الإثبات التقليدية مع الطابع غير المادي للأدلة الرقمية، ومن جهة أخرى في توفير الضمانات القانونية الكفيلة بصيانة الحقوق والحريات أثناء جمع وتحليل وتقديم هذه الأدلة. ويُلاحظ تفاوت واضح بين الأنظمة القانونية المقارنة في كيفية التعامل مع هذا النوع من الإثبات، سواء من حيث الاعتراف بحجيته ، أو من حيث الشروط والضوابط الإجرائية التي تحكم جمعه واستخدامه.

لذلك يتناول هذا المطلب الإطار التشريعي لإثبات الجرائم المعلوماتية، من خلال بيان طبيعة هذا الإثبات وصعوباته، ثم استعراض ضوابط جمع الأدلة الرقمية، وأخيراً تحليل مدى حجية هذه الأدلة في النظم القانونية المقارنة، لاسيما في النظامين السعودي والمصري، مع إضاءة على التجربة الفرنسية بوصفها مثالا رائدا في هذا المجال.

أولاً: مفهوم الإثبات الجنائي وأهميته

يُعد الإثبات الجنائي الركيزة الأساسية التي تقوم عليها العدالة الجنائية، إذ يمثل الوسيلة التي يعتمدها القاضي لتكوين قناعته تجاه ثبوت الجريمة ونسبتها إلى المتهم. وقد عرّف الفقه الإثبات الجنائي بأنه "الوسائل القانونية التي يتم من خلالها بيان الوقائع المادية المكونة للجريمة لإقناع المحكمة بارتكاب الفعل الإجرامي من قبل المتهم" [١]

---

(١) أنور سلطان، الإثبات في المواد الجنائية، دار النهضة العربية، ٢٠٠٣، ص١٥.

وتزداد أهمية الإثبات في المجال الجنائي بالنظر إلى خطورة الآثار المترتبة عليه، التي قد تصل إلى تقييد الحرية أو إهدار الحياة، لذلك يحرص المشرع على وضع قواعد دقيقة تكفل توازنًا بين مصلحة المجتمع في مكافحة الجريمة، وضمانات المتهم في محاكمة عادلة.(١)

ثانيًا: الطبيعة الخاصة للإثبات في الجرائم الرقمية

الجرائم الرقمية أو المعلوماتية تُعد من الظواهر المستحدثة في العصر الرقمي، وتتميز بخصائص تجعل من عملية إثباتها تحديًا كبيرًا، من أبرزها:

١. الطابع غير المادي: غالباً تكون غير ملموسة Non Tangible إذ تُرتكب الجرائم الرقمية في بيئة افتراضية، مما يعني غياب الأثر المادي التقليدي للجريمة.

٢. الطابع العابر للحدود: غالبًا ما تُرتكب هذه الجرائم من خلال شبكة الإنترنت التي لا تعترف بالحدود الجغرافية، ما يصعب من إجراءات التتبع والتحقيق.

٣. سهولة طمس الأدلة: في كثير من الحالات، يستطيع الجاني محو آثار الجريمة الرقمية خلال ثوانٍ، مما يتطلب سرعة عالية في جمع الأدلة الرقمية. وإزاء تلك الخصائص، بات من الضروري إعادة النظر في القواعد التقليدية للإثبات، بحيث تتماشى مع الطبيعة التقنية للجرائم الرقمية.(٢)

---

(١)د. عبد الرؤوف مهدي ، الإثبات الجنائي ، دار الأهرام للنشر ، ٢٠٢٣ ، ص ٨٣.

(٢) وتجدر الإشارة أنه في النظام الأنجلوسكسوني (الولايات المتحدة نموذجًا):

حيث اعتمد النظام الأمريكي على مبدأ "قابلية قبول الدليل" (Admissibility) وليس حجيته المطلقة، ويترك أمر تقدير وزنه إلى قناعة هيئة المحلفين أو القاضي، وأهم ما يُشترط لقبول الدليل الرقمي في النظام الأمريكي هو: أن يكون قد جُمع بطريقة قانونية (وفقًا للتعديل الرابع من الدستور الأمريكي المتعلق بالخصوصية)، وأن يكون موثوق المصدر (Authenticity)، ويُثبت ذلك بشهادة فنية أو تقرير خبير، وألا يكون الدليل قد تعرض للتلاعب أو الاختراق، كما أرست محكمة الاستئناف الفيدرالية في قضية(United States v. Tank 2000)مبدأً مهمًّا مفاده أن "الدليل الرقمي مقبول إذا أمكن تحديد مصدره بدقة وربطه بالمتهم دون لبس، راجع في ذلك ....

Daniel Solove J, Information Privacy Law, Aspen Publishers, 2020, p 210.

ثالثًا: التمييز بين الأدلة التقليدية والأدلة الرقمية

الأدلة التقليدية مثل الشهادة، والاعتراف، والمعاينة، لها طبيعة حسية مباشرة. أما الأدلة الرقمية، فهي بيانات تُخزن أو تُعالج أو تُرسل إلكترونيًّا، وتشمل مثلًا سجلات البريد الإلكتروني، وملفات الدخول (Logs)، والمحادثات عبر التطبيقات، والبيانات المخزنة في الأقراص الصلبة.

وقد اعترف القانون بعدد من هذه الأدلة في نصوصه، كما فعل قانون مكافحة جرائم تقنية المعلومات المصري الذي أشار في مادته الثانية إلى "البيانات والمعلومات الإلكترونية" بوصفها محلًا للحماية القانونية. كما نصت اتفاقية بودابست للجرائم السيبرانية على ضرورة قبول الأدلة الإلكترونية ما دامت قد تم جمعها وفقًا للقانون.

لذا يمثل هذا النوع من الأدلة تحدياً أمام القضاء نظراً لتغير معايير القوة الثبوتية بالأدلة التقليدية كالاعتراف أو شهادة الشهود.

رابعًا: التحديات القانونية في إثبات الجرائم الرقمية

يعد الإثبات في الجرائم المعلوماتية من أعقد الجوانب القانونية ؛ نظراً للطبيعة غير المادية للبيئة الرقمية ، واعتماد الجريمة المعلوماتية على وسائل تقنية متقدمة يصعب اكتشافها أو إثباتها بالطرق التقليدية ،بالإضافة إلى عدم وجود شهود عيان في الغالب [١]، واعتماد الإثبات على بيانات تقنية ، لذا تطرح الجرائم الرقمية تحديات خاصة تتعلق بالإثبات، من أبرزها:

١. صعوبة تحديد الجاني: قد يستعمل مرتكبو هذه الجرائم تقنيات الإخفاء كالشبكات الخاصة الافتراضية (VPN) أو الهوية المزيفة، مما يصعب ربط الفعل بشخص معين.[٢]

٢. ضعف التشريعات التقليدية: لا تزال بعض القوانين تعتمد مفاهيم إثباتية تقليدية لا تستوعب الطبيعة التقنية للدليل الرقمي، مما يؤدي إلى ثغرات في الإثبات.

---

(1) David Wall ,Cybercrime, The Transformation of Crime in the Information Age , 2nd Edition, Polity Press,2020.p90.

(٢) محمد عصفور الإثبات في الجرائم المعلوماتية دار الفكر الجامعي الإسكندرية ، ٢٠٢٣ ص٢١.

٣. إشكاليات حجية الدليل الرقمي: لا يكتسب الدليل الرقمي في بعض الأنظمة نفس الحجية القانونية للأدلة الأخرى، ما يثير جدلاً حول مدى اعتماد القضاء عليه.

٤. تأثر الدليل بالزمن والتقنية: قد يُفقد الدليل الرقمي أو يُتلف بسهولة، كما أن تغيّر الأدوات التقنية يجعل من بعض وسائل الإثبات سريعة التقادم.[١]

٥-ضرورة توافر الكفاءات الفنية المتخصصة في التحقيق الرقمي في الكثير من الأحيان.

وقد بين الفقه أن الإثبات في الجرائم المعلوماتية يعتمد على الأثر الرقمي الذي يتركه الجاني في النظام المعلوماتي ، مثل سجلات الدخول ، والبصمات الرقمية وسجلات السيرفرات .[٢]

يظهر مما سبق أن طبيعة الإثبات في الجرائم الرقمية تفرض على النظم القانونية تطوير أدواتها التشريعية والإجرائية لمواكبة هذه الظاهرة. ويجب أن يُراعى في ذلك الحفاظ على توازن دقيق بين متطلبات مكافحة الجريمة، وضمانات المتهم في محاكمة عادلة. ويُعد هذا التحدي أحد أبرز ما يواجه القضاء والنيابة في العصر الرقمي.

الضوابط العامة لجمع الأدلة في القانون الجنائي

في إطار القانون الجنائي التقليدي، يُشترط في عملية جمع الأدلة أن تتم وفقًا لضوابط صارمة أهمها:

١. المشروعية: فجمع الدليل لابد أن يستند إلى نص قانوني يسمح به، وتحت إشراف السلطة القضائية المختصة.

---

(١) وقد تناولت محكمة النقض المصرية في العديد من أحكامها مسألة مشروعية الدليل الرقمي، مؤكدة على ضرورة أن يُجمع وفقًا لضوابط القانون حتى يمكن الاعتماد عليه (طعن رقم ١٢٣٢ لسنة ٨٠ قضائية)، راجع .عبد العظيم وزير، الوجيز في الإجراءات الجنائية ، دار النهضة العربية . ٢٠٠٢، ص ١٢١ وما بعدها .

(٢) انظر في ذلك سامي قرقر ، الجرائم الإلكترونية دراسة مقارنة منشورات الحلبي الحقوقية ٢٠١٨ ص١٤٢ .

٢. الضرورة والتناسب: فالإجراء يجب أن يتناسب وضرورة الغرض الجنائي، دون انتهاك غير مبرر لحقوق الأفراد.

٣. عدم المساس بالحرية الشخصية: فلا يجوز تقييد الحرية إلا بموجب أمر قضائي مسبب.(١)

ضوابط جمع الأدلة الرقمية

إن الطبيعة التقنية للأدلة الرقمية تستدعي ضوابط خاصة في جمعها، أبرزها:

١. الحفاظ على سلامة البيانات الرقمية، ينبغي أن تُجمع الأدلة الرقمية دون تعديل أو حذف أو تلف، ويُفضل استخدام برامج متخصصة لضمان نسخ البيانات الأصيلة بطريقة لا تقبل الطعن.

٢. التوثيق الكامل لسلسلة الحيازة (Chain of Custody)، وهي عملية تتبع كل من تعامل مع الدليل منذ لحظة جمعه وحتى عرضه أمام المحكمة. ويعد هذا الإجراء ضروريًّا للحفاظ على سلامة الدليل من التلاعب.(٢)

٣. إذن قضائي مسبق: في حال اقتضى جمع الدليل الرقمي تفتيش أجهزة إلكترونية، أو اعتراض اتصالات، فلا بد من صدور إذن قضائي صريح بذلك.(٣)

٤. الاختصاص الفني للجهة القائمة على الجمع: يجب أن يتم جمع الدليل الرقمي بواسطة جهة متخصصة (مثل إدارة مكافحة جرائم الحاسوب)، لتفادي فقدان أو تزييف المعلومات، مع ضرورة وجود كوادر مؤهلة فنيًّا

---

(١) وفقًا لما نص عليه الدستور المصري في المادة الرابعة والخمسين، والمادة التاسعة من العهد الدولي للحقوق المدنية والسياسية، راجع د.عبد الرؤوف مهدي ، الإثبات الجنائي ، مرجع سابق ص ٨٩.

(٢) وفي هذا السياق أكد النظام المصري في مادته الخامسة من قانون مكافحة جرائم تقنية المعلومات على ضرورة الالتزام بإجراءات قانونية مشددة عند ضبط أو فحص الأجهزة الرقمية ، راجع القانون رقم ١٧٥ لسنة ٢٠١٨.

(٣) وهو ما أكده قانون الإجراءات الجنائية المصري في المادة (٤٥)، وأيضًا القانون التونسي عدد ٥ لسنة ٢٠٠٤ المتعلق بالسلامة المعلوماتية.

٥. ضمان خصوصية الأفراد: بما أن الأجهزة الرقمية قد تحتوي على بيانات خاصة، يجب أن يتم الجمع دون المساس غير المشروع بخصوصية المتهم أو أطراف آخرين[١]، تطبيقًا لمبدأ الخصوصية الرقمية المنصوص عليه في القانون الأوروبي لحماية البيانات (GDPR).

وعلى ذلك **أكد** المشرع السعودي على ضرورة أن يتم جمع البيانات الرقمية بمعرفة جهات الضبط الجنائي المختصة وبما لا يخل بالخصوصية المنصوص عليها نظاماً ، كما أشار نظام الإثبات السعودي إلى أهمية سلامة الوسائل الإلكترونية في جمع البيانات لضمان قبولها .وهذا ما أكدته المعايير الدولية .[٢]، كما تعتمد لائحة توثيق الإجراءات الرقمية الصادرة عن هيئة الحكومة الرقمية بوصفها مرجعا تقنيا وقانونيا في هذا السياق[٣] ، فرض عدداً من الضوابط القانونية والفنية لجمع الأدلة الرقمية من بينها :

-ضرورة حصول الجهة المختصة على إذن من النيابة العامة قبل البدء في إجراءات الضبط والتفتيش الرقمي .

-احترام خصوصية الأفراد وعدم تجاوز نطاق الجريمة قيد التحقيق .

-حفظ الأدلة الإلكترونية بطريقة تضمن سلامتها الرقمية وعدم العبث بها .

وقد حددت اللائحة التنفيذية لنظام الإجراءات الجزائية وقواعد التحقيق الجنائي الرقمي هذه الإجراءات لضمان التوازن بين مكافحة الجريمة و حماية الحقوق الدستورية للمواطنين .[٤]

---

(١) سامر عبد الرضا اللامي وسائل الإثبات في الجرائم المعلوماتية المتصلة بالحياة الخاصة، مركز الدراسات العربية للنشر والتوزيع، ٢٠٢٤، ص٧٧.

(٢) أرست اتفاقية بودابست إطاراً متكاملاً لجمع الأدلة الرقمية على المستوى الدولي حين نصت في المادة ١٩ على أن أي إجراء لضبط بيانات إلكترونية يجب أن يتم بموجب أوامر قانونية وباستخدام وسائل تقنية معتمدة مع الحفاظ على سجل واضح لكافة الإجراءات .....راجع في ذلك

Agreement on cybercrime (Budapest Convention),Council of Europe, 2001,Article19

(٣) راجع لائحة توثيق الإجراءات الرقمية ، هيئة الحكومة الرقمية ، المملكة العربية السعودية ٢٠٢٢.

(٤) راجع الدليل الإجرائي في التحقيقات الرقمية ، إصدارات وزارة الداخلية السعودية، الإصدار الثاني ٢٠٢٢.

رابعًا: التحديات القانونية والعملية في جمع الأدلة الرقمية

على الرغم من محاولة التشريعات مواكبة التطورات الرقمية، إلا أن هناك تحديات لا تزال قائمة، مثل:

-تعدد مصادر البيانات: يصعب في بعض الأحيان تحديد المكان الفعلي لتخزين الدليل (خوادم خارجية، سحابة إلكترونية... إلخ).

-الاعتماد على أطراف ثالثة: مثل شركات الإنترنت أو التطبيقات، مما يفرض ضرورة التعاون الدولي في الإجراءات.

-ضعف التنسيق بين الجهات القضائية والفنية: مما يؤدي إلى ضعف في إجراءات التوثيق أو فقدان الدليل.

-صعوبة تحديد توقيت الجريمة بدقة: فالبيانات الرقمية قد تُعدل دون ترك أثر زمني ظاهر، ما يثير الشك في سلامتها.

-صعوبة توفير كوادر فنية مؤهلة لجمع الأدلة الرقمية في بعض الدول العربية مما يؤثر على سلامة المحاضر والتحقيقات .

وقد أشار الفقه إلى أهمية تطوير تشريعات وطنية واضحة تُلزم الجهات المختصة باتباع معايير فنية صارمة في جمع الأدلة الرقمية.[١]

وعلى ذلك فإن جمع الأدلة الرقمية يتطلب مراعاة ضوابط قانونية دقيقة تضمن احترام الحقوق الدستورية للأفراد، وتحافظ في الوقت ذاته على سلامة الدليل وصلاحيته للإثبات أمام القضاء. ولتحقيق هذا التوازن، لا بد من تحديث التشريعات الوطنية بما يتلاءم مع المتغيرات الرقمية، ورفع كفاءة الجهات القضائية والفنية في التعامل مع هذا النوع من الأدلة.[٢]

الحجية القانونية للدليل الرقمي

الحجية القانونية للدليل تعني مدى قبول المحكمة لهذا الدليل بوصفه صالحًا لإثبات الوقائع الجنائية. وفي سياق الجرائم الرقمية، يُطرح التساؤل حول مدى إمكانية اعتماد

---

(١) انظر د.عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار الأهرام للإصدارات القانونية، ٢٠٢٠، ص١٠٤.

(2) Agreement on cybercrime (Budapest Convention),Council of Europe, 2001,Article14,

البيانات الإلكترونية بوصفها وسيلة إثبات قانونية ، بالنظر إلى طبيعتها التقنية وقابليتها للتعديل أو الإتلاف.

الدليل الرقمي يثير تحديات فريدة بسبب إمكانية التلاعب به ، لذا فحجيته أمام القضاء ليست فقط مسألة قانونية، بل فنية أيضًا، وتتوقف هذه الحجية على عدة عوامل منها: طريقة جمعه، وإثبات سلامته من التغيير، والجهة التي قامت بحفظه وتقديمه، ومدى توافقه مع الضمانات الدستورية.

ثانيًا: موقف بعض النظم القانونية من حجية الدليل الرقمي

١. حجية الأدلة الرقمية أمام القضاء السعودي

لم يكن النظام القضاء السعودي غافلاً عن التطور التقني وأثره على الإثبات لذا أقر بحجية الأدلة الرقمية ضمن عدد من التشريعات[١] بشرط أن تكون قد جُمعت بشكل مشروع، وتكون لها علاقة بالواقعة موضوع الاتهام ، كما أكد نظام الإثبات الجديد على جواز استخدام الوسائل الإلكترونية في الإثبات .

كما أخذ بحجية البيانات الإلكترونية، بما في ذلك الرسائل النصية والبريد الإلكتروني، والتسجيلات الصوتية والمرئية، طالما لم يتم الطعن فيها بالتزوير أو عدم السلامة ، ونص على أن للمحكمة سلطة تقديرية في قبول هذه الأدلة بحسب ظروف الدعوى.[٢]

وقد شدّد النظام على أهمية الاعتماد على جهات معتمدة تقنيًّا في التحقق من سلامة هذه الأدلة، وهو ما ورد في لائحة توثيق الإجراءات الرقمية الصادرة عن هيئة الحكومة الرقمية.

كذلك أشار مجلس القضاء الأعلى السعودي[٣] في عدد من التوجيهات إلى أن الدليل الرقمي، متى توافرت له شروط المشروعية، والسلامة الفنية، والصلة بالوقائع محل التحقيق، يكون مقبولًا في الإثبات، شأنه شأن الأدلة التقليدية.

---

(١) أبرزها نظام مكافحة الجرائم المعلوماتية في المادة ١١ حيث نص صراحة على جواز استخدام الوسائل الإلكترونية في الإثبات.

(٢) راجعً المادة الرابعة من نظام الإثبات السعودي الصادر بالمرسوم الملكي رقم م/ ٤٣ بتاريخ ٢٦/ ٥/ ١٤٤٣.

(٣) تقرير وزارة العدل السعودية عن نظام الإثبات الرياض ٢٠٢٢ ص١٣.

وقد أكد بعض الفقهاء السعوديين على ذلك [١]، حيث إن التعديلات القانونية بنظام الإجراءات الجنائية التي تسمح بالاستعانة بالتقنيات الحديثة في الإثبات عززت بشكل كبير هذه النصوص القانونية السابق الإشارة إليها

وتتوقف حجية الأدلة الرقمية على

١ -مدى موثوقية الأداة المستخدمة في جمعها .

٢ -ضمان عدم التلاعب أو التعديل فيها .

٣-توافر الضوابط الفنية والإجرائية أثناء جمعها وتحليلها .

كما تلعب هيئة الخبراء الرقمية التابعة للأدلة الجنائية دوراً جوهرياً في تقييم سلامة الأدلة المعروضة .

٢. النظام القانوني المصري

لم يكن القانون المصري يولي اهتمامًا كافيًا بالدليل الرقمي حتى صدور قانون مكافحة جرائم تقنية المعلومات، الذي اعترف صراحة في المادة الثانية بمشروعية الدليل المستمد من الوسائط الرقمية، بشرط أن يتم جمعه وفقًا للقانون على أن يتم جمعه بطريقة مشروعة [٢]، كما أقر قانون الإثبات حجية التوقيع الإلكتروني والرسائل الإلكترونية والسجلات الرقمية في المواد المدنية والتجارية، مما يمهد للاعتراف بها كذلك في المجال الجنائي إذا توافرت شروط الصحة والسلامة، وأيضاً تعززت هذه النصوص بتعديلات قانون الإجراءات الجنائية الذي سمح بالتقنيات الحديثة في الإثبات .

٣. النظام الفرنسي

يعترف النظام القضائي الفرنسي بالدليل الرقمي، ويخضعه لنفس معايير الحجية المعتمدة للأدلة التقليدية، بشرط أن يُجمع بواسطة جهة مختصة، وأن يُثبت أنه لم يتعرض

---

(١) إثبات الدليل الإلكتروني في القضاء السعودي يحظى بقبول متزايد، خاصة مع تطور البنية الرقمية للسلطة القضائية، واعتماد منصات رقمية موثوقة لتبادل الأدلة والإجراءات، راجع بندر العتيبي، الدليل الإلكتروني في نظام الإثبات السعودي، مجلة العدالة والقانون، العدد ١٤، ٢٠٢٢ ، ص ٧٧. وراجع أيضاً
Susan Brenner,Cybercrime Criminal Threats from Cyberspace, Praeger Security International, 2010,p143

(٢) راجع المادة السادسة من قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨.

للتعديل، كما يراعي فيه احترام الحقوق الدستورية، وتُعد مدونة الإجراءات الجنائية الفرنسية واضحة في هذا المجال، إذ تنص في المادة ٧٠٦-١٠٢ على إمكانية استخدام الأدوات التقنية في الإثبات الجنائي واعتماد التسجيلات الرقمية في المحاكم الجنائية مع الالتزام بضمانات الخصوصية والحقوق الأساسية للمتهم.[١]

٤. الجهود الدولية (اتفاقية بودابست نموذجًا)

أكّدت اتفاقية بودابست للجرائم السيبرانية في مادتها ١٤ على وجوب الاعتراف بالأدلة الإلكترونية من قبل الدول الأطراف، وألزمتها بتوفير ضمانات إجرائية لحماية سلامة تلك الأدلة ، ونصت على أن "الدليل الرقمي يجب أن يُعامل بالحماية نفسها والاعتبار الممنوح للأدلة التقليدية، بشرط جمعه وفق إجراءات قانونية مضمونة".

ثالثًا: المعايير المشتركة لحجية الدليل الرقمي

على الرغم من اختلاف الأنظمة القانونية، إلا أن هناك معايير مشتركة تعزز حجية الدليل الرقمي:

١. المشروعية: أن يتم جمع الدليل وفق إذن قضائي أو إجراء قانوني مشروع.

٢. السلامة الفنية: أن يَثْبت خلو الدليل من أي تعديل أو اختراق.

٣. الارتباط بالواقعة: أن يكون الدليل مرتبطًا موضوعيًّا بالواقعة محل الاتهام.

٤. إمكانية الفحص والمراجعة: أن يكون متاحًا للخبراء والطرف الآخر في الدعوى لمراجعته وتفنيده.

وقد أشار بعض الفقه إلى أن "حجية الدليل الرقمي لا ترتبط بطبيعته، وإنما بطريقة جمعه وتقديمه في ضوء المعايير القانونية والفنية المقررة".[٢]

---

(١) وقد أكدت المحاكم الفرنسية في عدة أحكام أن رسائل البريد الإلكتروني وسجلات المواقع الإلكترونية تعتبر أدلة مقبولة إذا تم التأكد من مصدرها وسلامتها -المحكمة العليا ، الغرفة الجنائية ، ٨ فبراير ٢٠١٢، تدخل البيانات وتدخل النظام .

http://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000025534746

(٢) عادل حامد بشير محمد ، الإثبات الجنائي للجريمة المعلوماتية، دار النهضة العربية للنشر والتوزيع، ٢٠٢١ ، ص٨٨.

رابعًا: إشكاليات تطبيقية في تقدير حجية الدليل الرقمي

صعوبة التحقق من المصدر الحقيقي: قد يُنسب الدليل الرقمي لشخص، بينما يكون الجاني قد انتحل هويته.

-عدم تجانس المعايير الدولية: تختلف شروط الحجية من دولة لأخرى، مما يُصعّب التعاون القضائي.

-نقص الخبرة القضائية والفنية: لا يزال كثير من القضاة يفتقرون للمعرفة التقنية اللازمة لتقييم هذه الأدلة بشكل موضوعي.[١]

-سهولة الطعن في سلامة الدليل: تُستخدم الطعون الفنية وسيلة دفاع ناجحة لنزع حجية الدليل الرقمي، ما لم يُوثق بشكل دقيق.

لذا يرتبط تقدير حجية الدليل الرقمي بعدة عوامل، أهمها سلامة الإجراءات الفنية كعدم التلاعب أو التعديل ،توافر الثقة في المصدر الذي أنتج البيانات ، بالإضافة إلى ضرورة الامتثال للإجراءات القانونية كالحصول على الإذن اللازم لجمع الدليل ، وتكمن التحديات الحقيقية في الجانب التطبيقي، إذ يتطلب الأمر تطوير مهارات الجهات القضائية والفنية، وتوحيد المعايير الدولية، وتعزيز التعاون عبر الحدود.

يتضح مما سبق أن الدليل الرقمي أصبح واقعًا لا غنى عنه في مجال الإثبات الجنائي، وقد اعترفت به معظم الأنظمة القانونية، ولكن بشروط وضوابط لضمان صحته ومشروعيته .

---

(١) رزق سعد علي ، استخدام تقنيات الذكاء الاصطناعي وتحليل البيانات في الكشف عن الجرائم، رسالة دكتوراة ، جامعة القاهرة ٢٠٢٤، ص٧٣.

وانظر أيضاً-

Abhijeet Shrivastava, revisiting due diligence in cyberspace, crafting international law's arsenal against transboundary botnets, International Journal of Law and Information Technology, Oxford university press, Vol.30, Issue 3, 2022,p11.

المطلب الثاني
التحديات الإجرائية للجرائم المعلوماتية

الاختصاص القضائي للجرائم المعلوماتية ذات الطابع الدولي

أفرزت الطبيعة العابرة للحدود للجرائم المعلوماتية تحديات جوهرية أمام قواعد الاختصاص القضائي التقليدية، والتي غالبًا ما تستند إلى المكان الذي ارتُكبت فيه الجريمة أو محل إقامة الجاني أو المجني عليه ، ففي عالم رقمي بلا حدود قد تُرتكب الجريمة في دولة ما ، ويقع ضررها في أخرى ، ويُستضاف المحتوى أو تُمرر البيانات عبر خوادم في دولة ثالثة ، مما يُعقّد فكرة تحديد الدولة المختصة بالتحقيق والمحاكمة.[١]

وقد ظهرت إشكاليات عديدة تتعلق بتحديد الاختصاص المكاني في هذا النوع من الجرائم ، خصوصًا في ظل تباين المعايير القانونية بين الدول، وغياب اتفاقيات دولية ملزمة وشاملة بهذا الخصوص، كما أن بعض الدول ترفض تسليم رعاياها ، أو تعتبر أن مجرد وجود الأثر الرقمي في إقليمها لا يكفي لتأسيس الاختصاص القضائي.[٢]

وبهذا أصبحت الحاجة ملحة إلى تطوير قواعد مرنة للاختصاص القضائي ، تأخذ في الاعتبار خصوصيات البيئة السيبرانية ، وتضمن في ذات الوقت احترام سيادة الدول وعدم التدخل التعسفي في شؤونها . وفي هذا الإطار، يتناول هذا المبحث إشكاليات تحديد الاختصاص المكاني في الجرائم الرقمية ، وموقف بعض الأنظمة القانونية المقارنة من هذه الإشكاليات ، مع التركيز على أوجه التعاون القضائي والأمني الدولي بوصفه مدخلا عمليا لتجاوز العقبات القانونية.

---

(١) وقد أوصت منظمة الأمم المتحدة المعنية بالحريمة والعدالة UNODC بضرورة اعتماد أدلة رقمية في المحاكم ضمن تقاريرها الصادرة عن برامج العدالة الجنائية الإلكترونية....راجع في ذلك....

United Nations Office On Drugs and Crime, (UNODC), "Use of Electronic Evidence in Criminal Justice 2020,p22

(٢) فيصل حعيلان العازمي ، إشكالية الملاحقة الجزائية في الجرائم الإلكترونية، مكتبة الملك سلمان للعلوم الأمنية، أبريل ٢٠٢٤،ص١٨.

الجرائم الرقمية العابرة للحدود وإشكاليات تحديد الاختصاص المكاني

تشكل الجرائم المعلوماتية ذات الطابع العابر للحدود أحد أبرز التحديات التي تواجه القانون الجنائي الدولي، إذ لا تنحصر آثارها ضمن إقليم دولة واحدة، بل تمتد إلى فضاءات متعددة، نظراً لاعتمادها على شبكات الاتصالات والمعلومات الدولية التي تتجاوز الحدود الجغرافية التقليدية.(١)

ويُقصد بالجرائم الرقمية العابرة للحدود تلك الجرائم التي تنطوي على عناصر ترتبط بأكثر من دولة، سواء من حيث مكان ارتكاب الفعل، أو محل إقامة الجاني أو الضحية، أو موقع الخادم الإلكتروني الذي تمر من خلاله البيانات. ومن الأمثلة الشائعة: جرائم الاحتيال الإلكتروني، الاختراقات العابرة، والهجمات على البنية التحتية السيبرانية لدول أخرى.

هذا التداخل يطرح إشكاليات قانونية بالغة التعقيد في تحديد الجهة القضائية المختصة، حيث قد تدعي أكثر من دولة اختصاصها بنظر الجريمة، أو قد تمتنع جميعها بحجة عدم وجود ارتباط كافٍ بترابها الوطني. كما أن تعدد المعايير المستخدمة لتحديد الاختصاص – كمعيار مكان التنفيذ، أو مكان حدوث الضرر، أو مكان وجود الخادم الإلكتروني مما يؤدي إلى تضارب أو تداخل الاختصاصات.

وقد واجهت بعض النظم القانونية هذه الإشكالية من خلال تبني قواعد مرنة تسمح بتوسيع نطاق الاختصاص الجنائي متى ثبت تحقق أحد عناصر الجريمة في الإقليم الوطني، في حين ما زالت أنظمة أخرى تعتمد تفسيرًا ضيقًا يجعل من ملاحقة هذا النوع من الجرائم أمرًا صعبًا من الناحية العملية.

وتُثار أيضًا إشكالية "الاختصاص القضائي السلبي"، حينما لا تبادر أي دولة باتخاذ الإجراءات اللازمة بدعوى أن الجريمة لم تقع ضمن اختصاصها المباشر، ما يخلق فراغًا قانونيًّا خطيرًا قد يُستغل من قبل المجرمين السيبرانيين للإفلات من العقاب.

ولذلك، فإن التطور التشريعي والتعاون الدولي القضائي أصبحا ضرورة مُلحّة لضمان فعالية الملاحقة في الجرائم الرقمية العابرة للحدود، وتعد معالجة هذه التحديات من

(1) Adam Noor, UAE Cybercrime Law: Legal Responses to Digital Threats. Middle Eastern Journal of Cyber security Law, 18(2),2021, p115.

أولويات السياسة الجنائية الرقمية والتي لم تعد تقتصر على التجريم والعقوبة ؛ بل تشمل بناء منظومة تقنية قضائية قادرة على مواكبة متطلبات الإثبات في الفضاء الرقمي العابر للحدود .

موقف الأنظمة القانونية من الاختصاص القضائي في الجرائم الدولية

أدركت العديد من الأنظمة القانونية المعاصرة أن الجرائم المعلوماتية، خصوصًا تلك العابرة للحدود، تتطلب أدوات قانونية جديدة تتجاوز المفاهيم التقليدية للاختصاص المكاني. لذا، سعت بعض التشريعات إلى تطوير قواعدها في هذا المجال لمواجهة هذا النوع من الجرائم بفعالية أكبر. وفي هذا السياق، يبرز التباين بين النظامين السعودي والمصري من جهة، والنظام الفرنسي من جهة أخرى، من حيث مدى اتساع أو ضيق دائرة الاختصاص القضائي في مواجهة هذه الجرائم.

أولاً: النظام السعودي تثير الجرائم المعلوماتية إشكاليات قانونية حول تحديد الجهة المختصة مكانياً ونوعياً نظراً للطبيعة العابرة للحدود لهذه الجرائم ، وقد اعتمد النظام السعودي مبادئ حديثة لتحديد الاختصاص القضائي منها :

-اختصاص محاكم المملكة عند ارتكاب الجريمة من داخل السعودية أو كان أثرها واقعاً فيها .

-اختصاص المحكمة الجزائية بالنظر في قضايا الجرائم المعلوماتية وفقاً للمادة ١٥ من نظام المرافعات الشرعية والمادة ١٢٩ من نظام الإجراءات الجزائية .

اختصاص النيابة العامة بإجراءات التحقيق والادعاء بالتعاون مع الجهات الفنية مثل الأمن السيبراني والأدلة الرقمية

وفي إطار نظام مكافحة جرائم المعلوماتية فقد تبنى المشرع السعودي توجهًا يسمح بتوسيع الاختصاص القضائي في بعض الجرائم المعلوماتية. حيث يمكن للجهات القضائية السعودية ملاحقة الجرائم التي تمت جزئيًا داخل المملكة، أو تلك التي أثّرت في مصالحها، حتى وإن أُرتُكبت من الخارج.

غير أن النصوص النظامية لم تتوسع صراحة في تنظيم الجرائم الدولية الرقمية، ما يستدعي تطويرًا تشريعيًّا أكثر تحديدًا لمواجهة التحديات العابرة للحدود.

ثانياً: النظام المصري أحدث قانون مكافحة جرائم تقنية المعلومات نقلة نوعية في القانون الجنائي المصري، إذ نص صراحة في المادة (٢) على أن "تسري أحكام هذا القانون على كل من ارتكب خارج جمهورية مصر العربية فعلًا يُشكل جريمة من الجرائم المنصوص عليها فيه، إذا كان هذا الفعل معاقبًا عليه في الدولة التي وقع فيها، وكان المجني عليه مصريًا، أو كانت الجريمة قد ارتُكبت على وسائط مملوكة للدولة المصرية، أو إذا امتدت آثارها إلى داخل الدولة".[١]

ويُعد هذا التوجه تشريعًا إيجابيًا، إذ يمنح الولاية القضائية لمصر في حالات متعددة تتعلق بالجرائم المعلوماتية الدولية، مما يسهم في التصدي للجرائم العابرة للحدود بشكل أكثر فاعلية.

ثالثاً: النظام الإماراتي تتبنى دولة الإمارات العربية المتحدة موقفاً حاسماً ومرناً في آنٍ واحد بشأن مسألة الاختصاص القضائي في الجرائم المعلوماتية ذات الطابع الدولي، حيث تسعى إلى مواءمة تشريعاتها الوطنية مع التطورات العالمية في هذا المجال. وتُظهر التشريعات الإماراتية[٢] توجهاً واضحاً نحو توسيع نطاق الاختصاص القضائي ليشمل الجرائم التي ترتكب كلياً أو جزئياً داخل الدولة، أو إذا كان أثرها يمتد إليها، حتى وإن وقعت من خارجها، وهو ما يتوافق مع مبدأ "الإقليمية الممتدة" المعترف به دولياً. كما تؤكد الإمارات من خلال مشاركاتها في الاتفاقيات الدولية، كاتفاقية بودابست بشأن الجرائم الإلكترونية، على التزامها بتعزيز التعاون الدولي القضائي وتبادل المعلومات، إدراكاً منها لخصوصية الجرائم المعلوماتية التي تتجاوز الحدود الجغرافية وتتطلب تنسيقاً عابراً للدول.

---

(١) أحمد السيد النجار، الوساطة الجنائية، دراسة مقارنة، رسالة دكتوراة جامعة القاهرة ٢٠٢٣، ص١١٥.

(٢) القانون الاتحادي رقم ٣٤ لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الإلكترونية، المادة (٢) الخاصة بنطاق السريان الإقليمي.

رابعاً: النظام الفرنسي يُعد النظام الفرنسي من بين الأنظمة الأكثر تطورًا في مجال مكافحة الجرائم السيبرانية. إذ يعتمد على مبدأ "الامتداد الإقليمي للجريمة" (Principe de l'ubiquité)، الذي يجيز للسلطات القضائية الفرنسية ملاحقة الجرائم التي وقعت جزئيًا على الإقليم الفرنسي، حتى وإن كان جزء كبير منها قد وقع خارجه. وتُطبّق المحاكم الفرنسية هذا المبدأ على الجرائم المعلوماتية، خاصةً إذا امتدت آثارها إلى فرنسا، أو استُخدمت خوادم فرنسية، أو استُهدف بها مواطنون فرنسيون. وقد أسهم هذا المبدأ في تعزيز قدرة القضاء الفرنسي على التصدي للجرائم الرقمية الدولية، لكنه في الوقت ذاته يثير تحديات تتعلق بالتنسيق الدولي واحترام سيادة الدول الأخرى.

يتضح من المقارنة السابقة، أن الأنظمة القانونية محل الدراسة قد تبنّت مقاربات مختلفة في تحديد الاختصاص القضائي في الجرائم الرقمية الدولية. ففي حين اعتمد النظام الفرنسي نهجًا مرنًا يستند إلى امتداد آثار الجريمة، تبنّى النظام المصري رؤية واضحة تدعم الولاية القضائية الخارجية في عدة حالات، أما النظام السعودي فظهر أكثر تحفظًا، مما يُبرز الحاجة إلى مزيد من التحديث التشريعي في هذا المجال لمواكبة التطورات الدولي.

المطلب الثالث
التحديات المستقبلية وأطر التعاون الجنائي الدولي

تتطور الجريمة المعلوماتية بوتيرة متسارعة بفعل الابتكار التقني وتعدد الوسائط ، مما يعرض على المشرعين تحديات مستقبلية تتطلب استعداداً دائماً للتحديث والمراجعة .

قصور بعض النصوص النظامية الحالية

على الرغم من التقدم الملحوظ في التشريع السعودي ، إلا أن بعض القصور لا يزال قائماً ، ومن أبرز أوجهه:

-عدم شمول النظام الحالي لكل صور الجريمة المستحدثة (مثل الجرائم المرتبطة ب NFT أو البيانات البيومترية).

-غياب الإطار التنظيمي للتعاون الدولي في المسائل الرقمية .

-الحاجة لمزيد من الضمانات في مجال الخصوصية الرقمية والتوازن مع الحريات .

وقد أشار بعض الفقه إلى أن مواجهة هذه التحديات تقتضي الانتقال من منهج التجريم التقليدي إلى سياسة جنائية مرنة تعتمد على أدوات استباقية وقانون ديناميكي .[١]

التحديات المستقبلية والتوصيات التشريعية

في ظل التسارع التكنولوجي الهائل وتحوّل الجريمة من نمطها التقليدي إلى بيئات إلكترونية معقدة، بات من الواضح أن الإطار التشريعي القائم في مجال الجرائم المعلوماتية يواجه تحديات حقيقية تتطلب استجابة قانونية متجددة وشاملة. إذ إن تطوّر أدوات ارتكاب الجريمة، وظهور تقنيات جديدة كـ"الذكاء الاصطناعي التوليدي" و"إنترنت الأشياء" و"العملات الرقمية"، يعيد تشكيل المشهد الجنائي ويختبر جاهزية الأنظمة القانونية لمواجهته.

أولاً: التحديات المستقبلية

ومن أبرز التحديات التي تواجه السياسة الجنائية في ظل الأمن السيبراني:

---

(١) راجع ماجد عبدالعزيز ، السياسة الجنائية في مواجهة الجرائم المعلوماتية قراءة تحليلية للنظام السعودي ، مجلة جامعة الإمام محمد بن سعود ، العدد ٣٦ ، ٢٠٢١ ص٧٨.

١-الذكاء الاصطناعي والجريمة : استخدام تقنيات الذكاء الاصطناعي في تنفيذ أو دعم أنماط جديدة من الجرائم كالهويات المزيفة العميقة المعروفة باسم Deepfakes والتزييف الصوتي وصعوبة ملاحقة مرتكبي الجرائم.

٢-إنترنت الأشياء IOT : ازدياد عدد الأجهزة المرتبطة بالإنترنت يخلق فرصاً جديدة للاختراق والاستغلال .مع الجريمة عبر العملات المشفرة : باستخدام العملات الرقمية بوصفها وسيلة لغسل الأموال أو تمويل الأنشطة غير المشروعة

٣-نقص الكوادر المتخصصة : لاتزال الحاجة ماسة إلى خبرات وطنية تقنية وقانونية قادرة على مواكبة الجريمة الرقمية المعقدة .

٤-الهجمات السيبرانية الممولة من بعض الجهات الإرهابية مما يخلق إشكالية في تحديد المسؤولية القانونية.

٥- والتحدي الأكبر هو ضعف البنية التشريعية والتقنية في العديد من الدول وبالأخص الدول النامية.

٦. ضعف مواكبة التشريعات للتقنيات الحديثة: فكثير من النصوص العقابية لا تزال ترتكز على مفاهيم تقليدية لا تنسجم مع أنماط الجريمة الحديثة ، ما يفتح المجال لاجتهادات قضائية قد تكون غير موحدة أو غير دقيقة.

٧. النطاق العابر للحدود للجرائم المعلوماتية: حيث تستغل الجماعات الإجرامية تفاوت الأنظمة القانونية بين الدول، وضعف التنسيق القضائي، لارتكاب الجرائم من أماكن بعيدة يصعب ملاحقتهم فيها.

٨. تحديات الإثبات الفني: صعوبة ضبط الأدلة الرقمية وحمايتها من التلاعب، مع غياب الكفاءات الفنية الكافية في بعض الأجهزة القضائية، تضعف من فاعلية الملاحقة الجنائية.

٩. محدودية العقوبات التقليدية: فالعقوبات السالبة للحرية قد لا تكون مناسبة دومًا، خصوصًا مع الجرائم ذات الطابع غير العنيف، ما يدعو إلى اعتماد عقوبات بديلة أكثر فاعلية.

ثانيًا: التوصيات التشريعية والعملية

بناءً على ما سبق يمكن اقتراح عدد من التوصيات التي تسهم في تعزيز مكافحة الجرائم المعلوماتية

١. تحديث النصوص العقابية بشكل دوري:

بما يضمن شمولها للصور المستحدثة من الجرائم الرقمية، وبناء بنية قانونية مرنة تتسع للتطور التقني، مع ضرورة إصدار نظام خاص بالأمن السيبراني يعزز الإطار القانوني للوقاية الرقمية .

٢. توسيع صلاحيات القضاء والنيابة في التعاون الدولي:

من خلال الانضمام إلى الاتفاقيات الدولية المتخصصة كاتفاقية بودابست الخاصة بالجرائم السيبرانية، وتبني آليات مباشرة للتعاون القضائي العابر للحدود.

٣. تعزيز الخبرات الفنية لأجهزة التحقيق والقضاء:

وذلك بإنشاء وحدات متخصصة داخل النيابات والمحاكم لمتابعة الجرائم المعلوماتية، وتوفير تدريب تقني مستمر للقضاة وأعضاء النيابة العامة، وكذلك دعم القدرات الفنية والوطنية في مجالات التحقيق والتحليل الجنائي الرقمي .

٤. إدماج العقوبات التكميلية والبديلة:

كمنع استخدام الإنترنت، أو خضوع المحكوم عليه لرقابة رقمية، أو فرض برامج تأهيلية تقنية، بدلًا من الاعتماد الحصري على السجن أو الغرامة.

٥. إنشاء جهة وطنية مستقلة متخصصة في الجريمة المعلوماتية:

تتولى التنسيق بين الجهات الأمنية والقضائية والفنية، وترصد تطور الجريمة الرقمية وتُصدر تقارير سنوية تدعم صانع القرار التشريعي، مع ضرورة إنشاء قاعدة بيانات وطنية

لرصد وتحليل أنماط الجريمة المعلوماتية بشكل منهجي ، وكذلك السعي نحو تعزيز برامج التوعية القانونية والتقنية للمستخدمين لحمايتهم من الوقوع ضحايا أو شركاء غير مقصودين في هذه الجرائم

ثانيًا: أطر التعاون الدولي

لمواجهة هذه التحديات، برزت الحاجة إلى:

اتفاقيات دولية موحدة مثل اتفاقية بودابست.

مراكز معلومات إقليمية لتبادل التحذيرات السيبرانية.

إنشاء فرق استجابة وطنية (CERT) متخصصة في مواجهة الحوادث الرقمية.[١]

– وحديثاً هناك اتفاقية الأمم المتحدة الجديدة لمكافحة الجرائم المعلوماتية والتي تم اعتمادها في ٨ أغسطس ٢٠٢٤،غير أنها لم تدخل حيز التنفيذ حتى كتابة هذا البحث، وركّزت على ثلاثة أهداف رئيسة هي: تحسين طُرق منع الجرائم الإلكترونية ومواجهتها، تعزيز التعاون الدولي لمكافحة الجرائم الإلكترونية بالإضافة إلى توفير المساعدة الفنية وبناء القدرات لا سيّما للبلدان النامية.[٢]

التعاون الدولي القضائي في مكافحة الجرائم المعلوماتية

نظراً لطبيعة الجرائم المعلوماتية العابرة للحدود ، أصبح التعاون الدولي أمراً حتمياً ويشمل ذلك

---

(١) وقد أطلقت دولة الإمارات "الهيئة الوطنية للأمن الإلكتروني" وفعّلت التعاون مع منظمات مثل الإنتربول و"المنتدى العالمي للأمن السيبراني". راجع في ذلك

UAE National Cyber security Strategy, Telecommunications and Digital Government Regulatory Authority (TDRA), 2020.

(٢) وصرح رئيس الجمعية العامة للأمم المتحدة، فيليمون يانغ "باعتماد هذه الاتفاقية، أصبحت في متناول يد الدول الأعضاء الأدوات والوسائل لتعزيز التعاون الدولي في منع ومكافحة الجرائم المعلوماتية و حماية الأشخاص وحقوقهم عبر الإنترنت".

https://news.un.org/ar/story/2024/12/1137776

-التعاون عبر الإنتربول والمنظمات الدولية مثل UNODC و ITU

-الانضمام إلى الاتفاقيات الثنائية والإقليمية التي تهدف إلى تبادل الأدلة والمعلومات .

-سن آليات مساعدة قضائية مشتركة تشمل التبليغ والاسترداد وتنفيذ الأحكام .

وقد عملت المملكة العربية السعودية على تعزيز دورها في المنظومة الدولية من خلال مشاركتها في المؤتمرات واللجان المتخصصة ، ووضع استراتيجيات وطنية للأمن السيبراني تتوافق مع المعايير الدولية .

الحدود السيبرانية والتعاون القضائي والأمني في مكافحة الجرائم المعلوماتية

إن الطابع الدولي للجرائم المعلوماتية يفرض على الدول تجاوز العمل الفردي، واللجوء إلى آليات التعاون القضائي والأمني الدولي لمواجهة هذا النوع من الجرائم بكفاءة وفعالية. إذ غالبًا ما تكون البنية الفنية للجريمة موزعة على أكثر من دولة، سواء من حيث الجاني أو المجني عليه أو محل الخادم الإلكتروني الذي يحتوي على الدليل الرقمي.[١]

ويأخذ التعاون الدولي أشكالًا متعددة، منها تبادل المعلومات، وإنابات التحقيق، وتسليم المجرمين، وتوحيد إجراءات ضبط الأدلة الرقمية، بالإضافة إلى التنسيق بين أجهزة إنفاذ القانون والنيابات العامة. وقد لعبت الاتفاقيات الدولية والإقليمية دورًا محوريًّا في هذا السياق، وعلى رأسها اتفاقية بودابست لعام ٢٠٠١ بشأن الجريمة السيبرانية، التي تُعد أول صك دولي مُلزم يُنظم سبل التعاون في هذا المجال.

أولاً: التعاون في النظام السعودي أشار نظام مكافحة جرائم المعلوماتية السعودي إلى أهمية التعاون الدولي، دون الدخول في تفاصيل إجرائية واضحة، حيث ترك تنظيم ذلك للوائح التنفيذية أو عبر الاتفاقيات الثنائية والمتعددة الأطراف التي تُبرمها المملكة. كما يُلاحظ أن السعودية ليست طرفًا في اتفاقية بودابست، على الرغم من كونها من أبرز الدول المتأثرة بالجرائم السيبرانية في المنطقة، ما قد يُحد من سرعة وكفاءة التعاون القضائي في بعض الحالات.[٢]

---

(١) محمد أحمد الناغي، الأحكام القانونية لأركان الجريمة المعلوماتية: دراسة في التشريع الجزائري والإماراتي، المجلة الجزائرية لبحوث الحقوق والعلوم السياسية، ديسمبر ٢٠٢٤ ،ص١٧.

(٢)هدية أحمد زعتر، الإشكاليات القانونية للجرائم الإلكترونية العابرة للحدود وسبل مواجهتها ، مجلة البحوث القانونية والاقتصادية ، كلية الحقوق جامعة المنصورة، المجلد ١٣ ، العدد ٨٤ ، ٢٠٢٣، ص٣٤

ثانياً: في النظام المصري انخرطت مصر في عدد من الاتفاقيات الثنائية والإقليمية في مجال مكافحة الجريمة السيبرانية، وأظهر قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ اهتمامًا واضحًا بالتعاون الدولي، فقد نص في المادة (٣٧) على أن "لجهات التحقيق المختصة أن تطلب من الجهات الأجنبية المختصة المساعدة القانونية والقضائية في سبيل كشف الأدلة الرقمية، وجمع المعلومات، وضبط الجناة". كما أتاح القانون للنيابة العامة التعاون المباشر مع الجهات الأجنبية في المسائل المستعجلة، وهو ما يعكس توجهًا عمليًّا لمواكبة الطبيعة السريعة للجرائم الإلكترونية.[١]

ثالثاً: وفي النظام الفرنسي يُعد النظام الفرنسي من أكثر الأنظمة تعاونًا على المستوى الدولي في مجال مكافحة الجرائم المعلوماتية، ليس فقط من خلال عضويته في اتفاقية بودابست، بل أيضًا من خلال تبنيه شبكة واسعة من الشراكات التقنية والاستخباراتية مع دول الاتحاد الأوروبي وخارجه. وتُتيح القوانين الفرنسية للنيابة العامة وأجهزة الشرطة القضائية العمل المشترك مع الهيئات الأجنبية، وتبادل البيانات والنتائج الفنية بصورة منظمة ، بما يتفق مع المعايير الدولية لحماية الحقوق.

إذن يُشكّل التعاون الدولي حجر الزاوية في مكافحة الجرائم المعلوماتية ذات الطابع العابر للحدود. ومع أن بعض الأنظمة – كالنظام الفرنسي – بلغت درجة متقدمة من الانخراط في التعاون القضائي[٢]، فإن أنظمة أخرى – كالسعودي – ما تزال بحاجة إلى تطوير آلياتها

،....وراجع أيضاً- محمد حسين الدوسري ، إشكالية التوصيف لقضايا الجرائم المعلوماتية، جريدة الوطن السعودية، مارس ٢٠٢١ http:llwww.alwatan.com.sa

(١) انظر في ذلك محمد محمود قبالة ، القانون الدولي والتحديات المعاصرة بالتطبيق على الجريمة السيبرانية، مجلة الحقوق للبحوث القانونية والاقتصادية ، جامعة الإسكندرية ، يوليو ٢٠٢٤، ص٣٥.

(٢) راجع مجموعة القوانين الفرنسية في هذا المجال ومنها على سبيل المثال

-Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique , Légifrance – Loi République numérique.

التشريعية والانضمام إلى الاتفاقيات الدولية ذات الصلة لتعزيز فاعليتها. وتُظهر التجربة المصرية تقدمًا ملموسًا في هذا المجال، خصوصًا بعد صدور القانون المنظِّم لعام ٢٠١٨.

الخاتمة

لقد كشفت هذه الدراسة عن الأهمية المتزايدة للسياسة الجنائية في مواجهة الجرائم المعلوماتية، في ظل تصاعد التهديدات الرقمية واتساع نطاق الفضاء السيبراني، مما فرض على النظم القانونية أن تعيد النظر في أدواتها التشريعية والإجرائية لمواكبة هذا التحول الجذري في طبيعة الجريمة.

ومن خلال الدراسة التحليلية المقارنة أمكن التوصل إلى عدد من النتائج والتوصيات المهمة

أولًا: النتائج

١. الجرائم المعلوماتية تمُثل تحديًا حقيقيًّا للسياسة الجنائية التقليدية، من حيث طبيعتها غير المادية وسرعة تطورها وانتشارها عبر الحدود، وإن كانت التشريعات العربية الحديثة شاملة في هذا المجال ؛ إلا أنها لا تزال تفتقر إلى قواعد إجرائية متخصصة بالأدلة الرقمية .

٢. السياسات الجنائية في الدول محل الدراسة (السعودية، مصر، الإمارات، فرنسا) شهدت تطورًا ملحوظًا في تجريم الأفعال المعلوماتية ، إلا أن هناك تفاوتًا في مستوى التحديث خاصة فيما يتعلق بالتعاون الدولي والأدلة الرقمية، في حين يقدم النموذج الفرنسي نموذجاً متوازناً بين الأمن الرقمي وضمان الحريات يستحق الدراسة والاقتباس في التجارب العربية .

٣. غياب تعريف موحّد للجرائم المعلوماتية أسهم في تعدد المقاربات الفقهية والتشريعية ، مما يفرض الحاجة إلى توحيد المفاهيم عبر اتفاقيات دولية.

٤. الأمن السيبراني أصبح جزءًا لا يتجزأ من السياسة الجنائية الحديثة ، ولم يعد مقتصرًا على التدابير التقنية ، بل أصبح يشمل الإطار التشريعي والتنفيذي لضمان الوقاية من الجريمة الرقمية.

٥. التناسب في العقوبات لا يزال يواجه إشكاليات في بعض التشريعات، مما يتطلب تكييف العقوبات بما ينسجم مع خطورة الفعل الإجرامي الرقمي وخصوصية مرتكبيه.

٦. الأدلة الرقمية تُشكل حجر الزاوية في إثبات الجرائم المعلوماتية ، وهو ما يستلزم تطوير الأطر القانونية والضوابط الفنية لضمان حجيتها ومشروعيتها، كما توجد فجوة حقيقية بين التوسع في التجريم وعدم كفاية الكوادر الفنية للتحقيق الجنائي الرقمي.

ثانيًا: التوصيات

١.دعوة المشرعين العرب إلى استكمال التشريعات الرقمية وخاصة السيبرانية بإجراءات إثبات متخصصة تراعي طبيعة الدليل الإلكتروني والتحديث بصورة دورية لمواكبة التطورات التقنية المستجدة ، كجرائم الذكاء الاصطناعي والعملات المشفرة والبيانات البيومترية، مع ضرورة اعتماد آليات تشريعية سريعة الاستجابة للتكنولوجيا الرقمية (قوانين طارئة أو مراسيم تنفيذية).

٢. إدماج وسائل الإثبات الرقمية في الأنظمة الإجرائية بشكل صريح ، وتوفير ضمانات قانونية تكفل عدم المساس بالحقوق الأساسية للأفراد أثناء جمع الأدلة وتحليلها، مع تعزيز قدرات الجهات الأمنية والقضائية من خلال إنشاء وحدات خاصة بالتحقيق في الجرائم السيبرانية.

٣. بناء القدرات التقنية والمؤسسية عن طريق إنشاء برامج تدريب متخصصة للقضاة وأعضاء النيابة وأفراد الشرطة في تقنيات التتبع والتحقيق الرقمي ، وتنمية مهارات التحليل الرقمي وأدلة الـ"Forensics"، ودعم وحدات الاستجابة للطوارئ السيبرانية (CERT/CIRT) بالمعدّات والخبرات التقنية الوطنية ، مع التأكيد على ضرورة إنشاء وحدات قضائية وأمنية متخصصة في الجرائم المعلوماتية ، مزوّدة بالخبرات الفنية والقانونية اللازمة للتعامل مع التحقيقات الرقمية والفضاء السيبراني.

٤. إقرار إطار قانوني متكامل للأمن السيبراني يتضمن دمج تعريفات شاملة للجرائم السيبرانية تواكب الأدوات والوسائل الناشئة، مع مراعاة مبدأ الشرعية وتحديد طبيعة الالتزامات القانونية على المؤسسات الخاصة والعامة في حماية البيانات والشبكات ، ضرورة إنشاء مراكز إقليمية مشتركة لتنسيق الاستجابة للحوادث السيبرانية وتبادل الخبرات.

٥. تفعيل النهج الوقائي والتوعوي من خلال تعزيز الوعي المجتمعي بالجرائم المعلوماتية ودعم برامج وطنية للتثقيف الرقمي، وإطلاق حملات توعية وطنية حول الأمن السيبراني تستهدف الهيئات الحكومية والمؤسسات الخاصة والمواطنين ، وكذلك إلزام مزوّدي الخدمات الرقمية بالمشاركة في منظومة الإنذار المبكر للهجمات السيبرانية والتبليغ الفوري عن الحوادث الأمنية ومشاركة بيانات التهديدات.

٦. تعزيز التعاون الدولي في مجال مكافحة الجرائم المعلوماتية من خلال الانضمام إلى الاتفاقيات الدولية ذات الصلة، مثل اتفاقية بودابست ، وتفعيل بروتوكولات التبادل السريع للمعلومات واستخلاص الأدلة عبر الحدود وتفعيل آليات تسليم المجرمين.

٧. البحث والتطوير المستمر من خلال دعم الدراسات والأبحاث المشتركة بين الجامعات ومراكز البحوث في مجال الجريمة السيبرانية ، تمويل المشاريع الابتكارية التي تستخدم الذكاء الاصطناعي لتحسين تقنيات الكشف والاستجابة.

بهذه التوصيات، نأمل أن تسهم السياسة الجنائية المعاصرة في بناء منظومة متكاملة تتصدى بفاعلية للتهديدات الرقمية، وتحقق التوازن المطلوب بين حماية الأمن السيبراني وصون الحقوق والحريات الأساسية.

وختاماً، فإن السياسة الجنائية المعاصرة لم تعد خيارًا تقليديًّا لمواجهة الجريمة، بل أصبحت ضرورة أمنية وقانونية تتطلب تجديدًا مستمرًّا وتنسيقًا دوليًّا لمواجهة التهديدات السيبرانية الآخذة في التوسع ، على نحو يضمن الحماية للمجتمع والعدالة في آنٍ واحد.

وذلك لأن مستقبل المكافحة القانونية للجرائم المعلوماتية مرهون بقدرة المشرعين على تفهم المخاطر الرقمية ، وسرعة استجابتهم لها بتشريعات مرنة عادلة ومواكبة. ويظل إصلاح السياسة العقابية عنصرًا محوريًّا في ضمان بيئة إلكترونية آمنة ، تحترم الحقوق وتحقق الردع دون إخلال بمبادئ العدالة الجنائية

قائمة المراجع

أولاً باللغة العربية

١ـ الكتب والمؤلفات العلمية:

ـ أحمد السيد النجار، الوساطة الجنائية، دراسة مقارنة، رسالة دكتوراة جامعة القاهرة ٢٠٢٣ .

– أحمد عبد الظاهر، الحماية الجنائية للأمن السيبراني، دار الجامعة الجديدة، الإسكندرية، ٢٠٢١.

–أحمد مرغني ، السياسة الجنائية في مواجهة الجرائم المستحدثة، مجلة الدراسات القانونية ، العدد ٥ ، ٢٠٢٠ .

– إسلام جمعة مصطفى، الجرائم المرتكبة باستخدام تقنيات التكنولوجيا الحديثة في القانون المصري (الواقع الافتراضي والواقع المعزز والمختلط)، رسالة دكتوراة جامعة القاهرة ، يناير ٢٠٢٤.

–أشرف أحمد هلال ، الجرائم المعلوماتية في الاعتداء على الحق في الحياة الخاصة، دار آل غالب للنشر ٢٠٢٤.

–أكرم نشأت إبراهيم ، السياسة الجنائية دراسة مقارنة ، دار الثقافة للنشر ،٢٠٢١.

– أنور سلطان ، الإثبات في المواد الجنائية ، دار النهضة العربية ، ٢٠٠٣.

–أيمن عبدالله فكري ، الجرائم المعلوماتية ، دراسة مقارنة في التشريعات العربية والأجنبية ، مكتبة القانون والاقتصاد ٢٠٢٢.

–خالد محمد الغامدي ، مقدمة في الأمن السيبراني والجرائم المعلوماتية ، جامعة نايف للعلوم الأمنية ، ٢٠٢٠.

– رزق سعد علي ، استخدام تقنيات الذكاء الاصطناعي وتحليل البيانات في الكشف عن الجرائم، رسالة دكتوراة ، جامعة القاهرة ٢٠٢٤.

- سامر عبد الرضا اللامي وسائل الإثبات في الجرائم المعلوماتية المتصلة بالحياة الخاصة، مركز الدراسات العربية للنشر والتوزيع، ٢٠٢٤.

- سامي قرقر ، الجرائم الإلكترونية دراسة مقارنة منشورات الحلبي الحقوقية ٢٠١٨ .

-سعد عاطف عبد المطلب حسنين، أحكام المسئولية الجنائية عن الجرائم المعلوماتية، دراسة مقارنة، رسالة دكتوراة جامعة القاهرة ٢٠٢٣.

- عبدالرؤوف مهدي ، الإثبات الجنائي ، دار الأهرام للنشر ، ٢٠٢٣ ،شرح القواعد العامة للإجراءات الجنائية، دار الأهرام للإصدارات القانونية ، ٢٠٢٠.

- عادل حامد بشير محمد ، الإثبات الجنائي للجريمة المعلوماتية، دار النهضة العربية للنشر والتوزيع، ٢٠٢١.

-عبدالعزيز جار الله ، جرائم الإنترنت وعقوباتها ، وآثار العولمة على مستخدميها ، دار الكتاب الجامعي ، ٢٠٢٤.

- عبد العظيم مرسى الوزير، الوجيز في الإجراءات الجنائية ، دار النهضة العربية . ٢٠٠٢.

-عبدالله أحمد الأسمري ، الجرائم السيبرانية ، ديوان العرب للنشر ، ٢٠٢٣.

- عبد الله القدرة ، الجرائم الإلكترونية دراسة مقارنة بين التشريعات الدولية والعربية، دار العلوم للنشر، ٢٠٢١.

-علي أحمد حسن ، فلسفة العقوبة الجنائية وآثر التكنولوجيا الحديثة، رسالة ماجستير جامعة القاهرة ديسمبر ٢٠٢٤.

-لينا محمد الأسدي ، مدى فاعلية أحكام القانون الجنائي في مكافحة الجرائم المعلوماتية ، دار الحامد للنشر ٢٠٢٥.

- محمد جبريل إبراهيم ، التحول الرقمي في نظام القانون الجنائي ، دراسة تحليلية تأصيلية، الدار العربية للعلوم ، يناير ٢٠٢٣ .

– محمد عصفور الإثبات في الجرائم المعلوماتية دار الفكر الجامعي الإسكندرية،٢٠٢٣ .

–محمد على سويلم ، مكافحة الجرائم المعلوماتية ، دراسة مقارنة ، دار المطبوعات الجامعية ، ٢٠٢٠.

–محمد فهد الجصغي ، علم السياسة الجنائية ، دار الزمان للنشر ،٢٠٢١.

–محمد نصير السرحان ، مهارات التحقيق الجنائي في جرائم الحاسوب والإنترنت ، رسالة ماجستير في العلوم الشرطية ، جامعة نايف للعلوم الأمنية ، الرياض ، ٢٠٢٤.

–محمود سليمان موسى ، السياسة الجنائية والإسناد المعنوي، دراسة مقارنة ، دار المطبوعات الجامعية ٢٠١٩.

–محمود عمر محمود ، الجرائم المعلوماتية ، دراسة مقارنة بين الشريعة والقانون الوضعي، دار خوارزم العلمية ، ٢٠٢٥.

–مصطفي أحمد موسى ، الجرائم المعلوماتية في القانون المصري، دار النهضة العربية، ٢٠٢٢ .

–مصطفي عبدالباقي ، التحقيق في الجريمة الإلكترونية وإثباتها ، دراسة مقارنة ، مجلة الشريعة والقانون ، الجامعة الأردنية ،المجلد ٤٥ العدد ٤ ملحق ٢، ٢٠١٨.

–مروان منصور الروقي ، القصد الجنائي في الجرائم المعلوماتية ، دراسة تأصيلية مقارنة ، مكتبة القانون والاقتصاد ، الرياض ٢٠٢٣.

– منى خليل المصري، السياسة الجنائية في مواجهة الجرائم السيبرانية، مجلة كلية الحقوق، جامعة الإسكندرية، العدد ٧١، ٢٠٢١.

–مها حمد القريني ، واقع الجرائم المعلوماتية في المملكة العربية السعودية ، بدون دار نشر ٢٠٢١.

-نايف خالد الشريف ، الجرائم المعلوماتية في النظام السعودي ، دراسة مقارنة ، دار حافظ ، ٢٠١٩ ص٤٥.

-هناء مصطفى الخبيري، الجرائم المعلوماتية وتقنين العملات الرقمية ، دراسة قانونية في التشريعات والاتفاقيات الدولية، النهضة العلمية للنشر والتوزيع ، ديسمبر ٢٠٢٣.

٢-الأبحاث والمقالات

-إبراهيم الحيدري ، الضوابط الإجرائية للجرائم المعلوماتية في النظام السعودي ، المجلة القضائية السعودية ، عدد خاص ٢٠٢٢.

-إيمان محمد عزام ، العقوبة في نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية دراسة تأصيلية مقارنة ، مجلة وزارة العدل ، العدد ٨٢ ، رجب ١٤٣٩ .

https:ll www.adlm.moj.gov.sa

- أيمن سيد محمد العسقلاني المسؤولية الجنائية عن الجرائم المعلوماتية الماسة بأمن الدولة: دراسة مقارنة في الفقه الإسلامي والنظام السعودي مجلة دراسات قانونية، البحرين ، مايو ٢٠٢٣.

-إمام حسنين خليل عطا الله ، جرائم الاعتداء على الشبكة المعلوماتية في التشريعات العربية: دراسة تحليلية مقارنة بالتشريع الإماراتي ، المجلة الدولية للبحوث والدراسات القانونية ، العدد٤ ، ٢٠٢٤ منشور باللغة الإنجليزية .

http:llijlrs.vsrp.co.uk

-بخدة صفيان ، الطبيعة القانونية للجرائم المستحدثة ووسائل ارتكابها ، جريمة الإنترنت كمثال، مجلة البحوث القانونية والسياسية ،جامعة طاهر بسعيدة، الجزائر ، مجلد ٣ العدد١٦ ، إبريل ٢٠٢١.

-بدور خالد الكربي ، تأثير التقنية على وسائل الإثبات الرقمية في النظام السعودي ، دراسة تحليلية ، مجلة البحوث الفقهية والقانونية ، كلية الشريعة والقانون بدمنهور ، العدد ٣٦ يوليو ٢٠٢٤.

- بندر العتيبي، الدليل الإلكتروني في نظام الإثبات السعودي، مجلة العدالة والقانون، العدد ١٤، ٢٠٢٢.

- حازم أحمد الهنيدي رضوان ، الجريمة المعلوماتية في شأن حق المؤلف على الإنترنت طبقًا للتشريع المصري، مجلة القانون، جامعة عين شمس، مايو ٢٠٢٣ .

jlaw.journals.ekb.eg

- سامي عبد الباقي، الأمن السيبراني كمدخل للوقاية من الجريمة الإلكترونية، مجلة البحوث القانونية، جامعة عين شمس، ٢٠٢٠.

-سعد عاطف عبدالمطلب ، أحكام المسئولية الجنائية عن الجرائم المعلوماتية ، دراسة مقارنة ، مجلة الدراسات القانونية والاقتصادية، العدد ٩، الإصدار الثالث ٢٠٢٣.

http:ll www.jdi.journals.exb.eg

- سليمان شاكر، القواعد الإجرائية والموضوعية للجريمة المعلوماتية في التشريع الجزائري، المجلة الجزائرية لبحوث الحقوق والعلوم السياسية، يونيو ٢٠٢٤.

-طارق العقلا ، حجية الدليل الإلكتروني في مجال الإثبات الجنائي للجرائم المعلوماتية في النظام السعودي ، مجلة كلية الشريعة والقانون ، جامعة أسيوط ، العدد ٣٥ إبريل ٢٠٢٣.

-عبد الرحمن عبد الله الشايع ، "الجريمة السيبرانية في النظام الجنائي السعودي"، مجلة كلية الحقوق ،جامعة الملك سعود ، العدد ٣٢، ٢٠٢٠.

-فيصل حعيلان العازمي ، إشكالية الملاحقة الجزائية في الجرائم الإلكترونية، مكتبة الملك سلمان للعلوم الأمنية، أبريل ٢٠٢٤.

-كمال عبد الله المهلاوي ، صعوبات التحقيق والإثبات في الجرائم المعلوماتية وأثرها على العدالة الجنائية ، مجلة جامعة المهرة للعلوم الإنسانية ، يونيو ٢٠٢٢.

-ماجد عبدالعزيز ، السياسة الجنائية في مواجهة الجرائم المعلوماتية قراءة تحليلية للنظام السعودي ،مجلة جامعة الإمام محمد بن سعود ، العدد ٣٦ ، ٢٠٢١.

- محمد أحمد الناغي، الأحكام القانونية لأركان الجريمة المعلوماتية: دراسة في التشريع الجزائري والإماراتي، المجلة الجزائرية لبحوث الحقوق والعلوم السياسية، ديسمبر ٢٠٢٤ .

-محمد حسين الدوسري ، إشكالية التوصيف لقضايا الجرائم المعلوماتية، جريدة الوطن السعودية، مارس ٢٠٢١.

-محمد محمود قبالة ، القانون الدولي والتحديات المعاصرة بالتطبيق على الجريمة السيبرانية، مجلة الحقوق للبحوث القانونية والاقتصادية ، جامعة الإسكندرية ، يوليو ٢٠٢٤.

-محي الدين عبدالله ، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية ،دراسة تحليلية مقارنة ، مجلة البحوث القانونية والاقتصادية ، جامعة المنصورة ، ٢٠٢١.

- منى خليل المصري، السياسة الجنائية في مواجهة الجرائم السيبرانية، مجلة كلية الحقوق، جامعة الإسكندرية، العدد ٧١، ٢٠٢١.

-نبيل محمود فريد عبد الرب ، مفهوم الجرائم المعلوماتية وتحدياتها التشريعية في فلسطين ، جامعة النجاح الوطنية، نابلس ، يناير ٢٠١٨.

-هدية أحمد زعتر ، الإشكاليات القانونية للجرائم الإلكترونية العابرة للحدود وسبل مواجهتها ، مجلة البحوث القانونية والاقتصادية ، كلية الحقوق جامعة المنصورة، المجلد ١٣ ، العدد ٨٤ ، ٢٠٢٣.

ثانيًا: المراجع باللغة الأجنبية

-**Abhijeet Shrivastava**, revisiting due diligence in cyberspace, crafting international law's arsenal against transboundary botnets, International Journal of Law and Information Technology, Oxford university press, Vol.30, Issue 3, 2022.

- **Adam Noor**, UAE Cybercrime Law: Legal Responses to Digital Threats. Middle Eastern Journal of Cyber security Law, 18(2),2021.

- **Ahmed El-Badry**, Egypt's Cybercrime Law: Evolution, Challenges, and Impact. Journal of International Cyber Law,2020, 17.**(٣)**

-Anebal Moneir , Le droit pénal à l'ère numérique : les nouvelles frontières de la cybercriminalité, Mon Code Juridique, 2020**.**

-Bhupinder Singh, prospects of information technology in reference to cyber terrorism,

National Journal of Cyber Security Law, Vol.8 ,No.2, 2025**.**

2022- **.Brad ofeinky** ,comparative Analysis of Cybercrime in the Criminal Law System

-Daniel Solove, J, Information Privacy Law, Aspen Publishers, 2020**.**

-Darsheen Kaur, beyond the firewall, understanding the complexities of cybersecurity, National Journal of Cyber Security Law, Vol.8 ,No.2, 2025**.**

- **David Wall** ,Cybercrime, The Transformation of Crime in the Information Age , 2nd Edition, Polity Press,2020**.**

-Edmond Miller , Cybercrime and Digital Evidence, Oxford University Press 2022**.**

-Édouard Champlin , La cybercriminalité , enjeux, législation et défis pour la justice du 21e siècle,28-3-2023**.**

-Federico Casolari, the EU data ACT in context, a legal assessment, International Journal of Law and Information Technology, Oxford university press, Vol.31, Issue 4, winter, 2023**.**

- **Felep Oniell** , Le droit pénal à l'ère numérique : les nouvelles infractions technologiques qui bouleversent la justice , Juridique Pro,2024**.**

-Garé Thierry, droit pénal, procédure pénale,paris ,editions Dalloz, 2023**.**

-Giovanni De Gregorio, digital constitutionalism in the new area of internet governance, International Journal of Law and Information Technology, Oxford university press, Vol.30, Issue 1, spring, 2022**.**

-Goug clough, Principles of Cybercrime (2nd ed.). Cambridge University Press,2021**.**

-Indrayudh Chowdhury, a discussion on cybercrimes with reference to the information technology Act 2000, National Journal of Cyber Security Law, Vol.6 ,No.1, 2022**.**

-Jeff Kosseff , Cybersecurity Law 6, Wiley , 2022**.**

- Jonsy Lemoine, J, The Role of French Cybercrime Laws in the Fight Against Digital Threats. Journal of European Cyber security Law, 10(1) 2020**.**

-Jorge Contreras, the equality machine, harnessing digital technology for brighter, more inclusive future, International Journal of Law and Information Technology, Oxford university press, Vol.31, Issue 3, 2023**.**

- **Julien Bacach**, "Le droit pénal et les cybercriminals, l'évolution de la législation française, Presses Universitaires de France, 2021**.**

-Katie Logos, estaplishing a framework for the ethical and legal use of web scrabers by cybercrime and cybersecurity researchers, International Journal of Law and Information Technology, Oxford university press, Vol.31, Issue 3, 2023**.**

-Katneni Sharan, cyber insurance, legal challenges and regulatory responses, National Journal of Cyber Security Law, Vol.8 ,No.2, 2025**.**

-Keerihana Krishna, the legal landscape of online games, an analysis of Cyber Law and its regulatitory challenges, National Journal of Cyber Security Law, Vol.8 ,No.1, 2025**.**

-Konrad Borowic, the data quality problem (in the European financial data space), International Journal of Law and Information Technology, Oxford university press, Vol.32, Issue 1, 2024**.**

-Margarita Robles, digital identity, an approach to its nature, concept and functionalities, International Journal of Law and Information Technology, Oxford university press, Vol.32, Issue 1, 2024**.**

-Mark Ryan, will the real data sovereign please stand up ? an EU policy response to sovereignty in data spaces, International Journal of Law and Information Technology, Oxford university press, Vol.32, Issue 1, 2024**.**

-**Mohamed Said El-Ghamdi**, Cybercrime Legislation in Saudi Arabia, A Critical Review of the Saudi Anti-Cybercrime Law. International Journal of Cyber Law and Ethics, 14(2),2020**.**

-**Nelam,** securing justice to victims of crime, victimization in the digital environment, National Journal of Cyber Security Law, Vol.6 ,No.1, 2022**.**

-**Niamh Kinchin**, voiceless, the procedural gap in algorithmic justice, International Journal of Law and Information Technology, Oxford university press, Vol.32, Issue 1, 2024**.**

-**Nilson Biedron** , Understanding Cybercrime in the COVID-19 Pandemic, Legal Implications and Enforcement Challenges , Master Degree ,University of Maryland ,2023. UMBC . https:llumd.edu

-**Orin kerr** ,computer crim law ,5th edition , west Academic , 2022**.**

-**Pieter Wolters**, the EU digital services ACT, what does it mean for online advertising and adtech ? , International Journal of Law and Information Technology, Oxford university press, Vol.33, Issue 1, 2025**.**

-**Rasikaviya Karesh**, harmonizing privacy and security cybercrime legislation in the digital age, National Journal of Cyber Security Law, Vol.8 ,No.1, 2025**.**

-**Richard Mackenzie**, supererogatory consumer choices grounded in the human right to privacy, International Journal of Law and Information Technology, Oxford university press, Vol.33, Issue 1, 2025**.**

-**Sameera Khan**, protection and empowerment of women in the Era of cyberspace, National Journal of Cyber Security Law, Vol.6 ,No.2, 2022**.**

-**Sam Schjlberg**, The History of Cybercrime, 1970 to 2020, Cyberspace Law & Policy Centre, 2020**.**

-**Samriddha Behere**, the facebook data breach and its consequences for privacy and cybersecurity, National Journal of Cyber Security Law, Vol.7 ,No.1, 2024**.**

- **Saphy Lal Bullu,** the global development of ICT, a quest for an assessment on the uncertainty impacts on countries

development challenge to fight against corruption, National Journal of Cyber Security Law, Vol.8 ,No.2, 2025.

-**Scarlet Rosalie Biedron** , Cybercrime in the Digital Age: Legal Challenges and Law Enforcement Strategies, Oxford PHD,2023.

-**Spellar Seigfried**, , Updating the Law of Computer Crime." Harvard Law Review, 134(3), 837–890,2020.

-**Steven Cerr** , Computer Crime Law, West Academic Publishing, 2018.

Oxford University Press , 2021.

-**Susan Brenner**, Cyber Crime, Law and Practice 3,

-**Susan Zacharia,** digital constitutionalism, an emerging dimension of Cyber Law, National Journal of Cyber Security Law, Vol.8 ,No.1, 2025.

-**Swetha Shree,** analysis of cyber phishing Laws, National Journal of Cyber Security Law, Vol.7 ,No.2, 2024.

-**Touodor Holt**, J, Cybercrime and Digital Forensics, An Introduction, (2nd ed) Routledge,2022.

-**Vàclav Janecek**, rethinking law, regulation, and technology, International Journal of Law and Information Technology, Oxford university press, Vol.30, Issue 4, winter, 2022.

-**Venkat Abhinav**, Cyber Law in the world, National Journal of Cyber Security Law, Vol.6 ,No.1, 2022.

-**Vinit Dhage,** cybercrime and cyberbulling, Targeting minors, National Journal of Cyber Security Law, Vol.6 ,No.2, 2023.

-**Vivek Sehrawat**, autonomous weapon systems and meaningful human control, International Journal of Law and Information Technology, Oxford university press, Vol.33, Issue 1, 2025.

-**Walte Brenner**,Cybercrime and the Law, Challenges, Issues, and Outcomes, Carolina Academic Press ,2021.

الأنظمة واللوائح

-نظام مكافحة الجرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم م/ ١٧ بتاريخ ٨/ ٣/ ١٤٢٨.

- الأمر الملكي رقم(أ/ ١٧) بتاريخ ٢٦/ ٢/ ١٤٣٩ الخاص بإنشاء الهيئة الوطنية السعودية للأمن السيبراني .

- الدليل الإجرائي في التحقيقات الرقمية ، إصدارات وزارة الداخلية السعودية ، الإصدار الثاني ٢٠٢٢.

- تقرير وزارة العدل السعودية عن نظام الإثبات، الرياض ٢٠٢٢.

- لائحة توثيق الإجراءات الرقمية ، هيئة الحكومة الرقمية ، المملكة العربية السعودية ٢٠٢٢.

- قانون مكافحة جرائم تقنية المعلومات، القانون المصري رقم ١٧٥ لسنة ٢٠١٨، الجريدة الرسمية، العدد ٣٢ مكرر (أ)، ١٤ أغسطس ٢٠١٨.

-قانون حماية البنية التحتية للمعلومات الحيوية، القانون الاتحادي رقم ٥ لسنة ٢٠٢٠، دولة الإمارات العربية المتحدة.

- مرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢، مكافحة جرائم تقنية المعلومات، الجريدة الرسمية، دولة الإمارات العربية المتحدة، ٢٠١٢.

-Code penal français ,

https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/

-Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

. Légifrance

-Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique Légifrance Loi LCEN.

-Code de procédure pénale , Chambre criminelle, Légifrance 2001.

-Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique , Légifrance – Loi République numérique.

-Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, Légifrance – Loi renseignement.

-Loi n° 2015-993 du 17 août 2015 relative à la lutte contre le terrorisme et le crime organisé, Légifrance – Loi lutte contre le terrorisme.

ـإصدارات رسمية باللغة الأجنبية

–Budapest Convention on Cybercrime, Council of Europe, 2001.

https://www.coe.int/en/web/cybercrime/the-budapest-convention

-CRS Legal Research Cybercrime and the Law, Primer on the Computer Fraud and Abuse Act and Related Statutes Congressional Research Service, 2023.

-Council of Europe, "Convention on Cybercrime" , Treaty No 185.

Avalable online: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

-Council of Europe, Budapest Convention on Cybercrime: 20 Years of Global Impact,2023.

https://www.coe.in

- European Union Agency for Cybersecurity (ENISA). (2023). Threat Landscape Report

https://www.enisa.europa.eu

-Les infractions liées au numérique enregistrées par les services de sécurité en 2024

الجهة الناشرة: وزارة الداخلية الفرنسية التاريخ: ٦ فبراير ٢٠٢٥

-UAE National Cyber security Strategy, Telecommunications and Digital Government Regulatory Authority (TDRA), 2020.

-United Nations Office on Drugs and Crime (UNODC), Comprehensive Study on Cybercrime, 2023.

-UNODC, Global Programme on Cybercrime, Annual Report,2022.

https://www.unodc.org

-National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity (Version 2.0)2022.

https://www.nist.gov

-Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 , GDPR – EUR-Le.

-Les infractions liées au numérique enregistrées par la police et la gendarmerie de 2016 à 2023 : Panorama d'une criminalité hétérogène

30-4-2024.(Service statistique ministériel de la sécurité intérieure)

السوابق القضائية الفرنسية

-محكمة استئناف باريس الغرفة ١٢ ، ٣٠ أكتوبر ٢٠٠٢، الوصول غير المشروع

http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=136

-محكمة الدرجة الأولى ، باريس، الدائرة ١٢ ، ١ يونيو ٢٠٠٧ ، الوصول غير القانوني

http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2179

-المحكمة العليا ، الغرفة الجنائية ، ٨ فبراير ٢٠١٢، تدخل البيانات وتدخل النظام

http://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000025534746

-المحكمة العليا ، الغرفة الجنائية ٢٩ أكتوبر ، تشرين الأول ٢٠٠٩ ، تأكيد تأهيل النشر الإلكتروني لثغرة أمنية كجريمة جنائية بموجب المادة١-٣- ٣٢٣ من القانون الجنائي الفرنسي (إساءة استخدام الجهاز والجرائم ذات الصلة)

http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000021299967&fastReqId=750589792

References:

alkutub walmualafat aleilmia:

• 'ahmad alsayid alnajar, alwisatat aljinayiyatu, dirasat muqaranati, risalat dukturat jamieat alqahirat 2023 .

• 'ahmad eabd alzaahir, alhimayat aljinayiyat lil'amn alsiybirani, dar aljamieat aljadidati, al'iiskandiriati, 2021.

• -'ahmad marghani , alsiyasat aljinayiyat fi muajahat aljarayim almustahdathatun, majalat aldirasat alqanuniat , aleadad 5 , 2020 .

• 'iislam jumeat mustafaa, aljarayim almurtakibat biaistikhdam tiqniaat altiknulujia alhadithat fi alqanun almisrii (alwaqie alaiftiradii walwaqie almueazaz walmukhtalita), risalat dukturat jamieat alqahirat , yanayir 2024.

• -'ashraf 'ahmad hilal , aljarayim almaelumatiat fi aliaetida' ealaa alhaqi fi alhayat alkhasati, dar al ghalib lilnashr 2024.

• -'akram nasha'at 'iibrahim , alsiyasat aljinayiyat dirasat muqaranat , dar althaqafat lilnashr ,2021.

• 'anwar sultan , al'iithbat fi almawadi aljinayiyat , dar alnahdat alearabiat , 2003.

• -'ayman eabdallah fikri , aljarayim almaelumatiat , dirasat muqaranat fi altashrieat alearabiat wal'ajnabiat , maktabat alqanun waliaqtisad 2022.

• -khalid muhamad alghamidi , muqadimat fi al'amn alsaybiranii waljarayim almaelumatiat , jamieat nayif lileulum al'amniat , 2020.

• razuq saed ealiun , aistikhdam tiqniaat aldhaka' aliaistinaeii watahlil albayanat fi alkashf ean aljarayimi, risalat dukturat , jamieat alqahirat 2024.

• samir eabd alrida allaami wasayil al'iithbat fi aljarayim almaelumatiat almutasilat bialhayat alkhasati, markaz aldirasat alearabiat lilnashr waltawziei, 2024.

• saami qarqar , aljarayim al'iiliktiruniat dirasat muqaranat manshurat alhalabii alhuquqiat 2018 .

• -saed eatif eabd almutalib hasnin, 'ahkam almasyuwliat aljinayiyat ean aljarayim almaelumatiati, dirasat muqaranati, risalat dukturat jamieat alqahirat 2023.

• eabdalrawuwf mahdi , al'iithbat aljinayiyu , dar al'ahram lilnashr , 2023 ,shrh alqawaeid aleamat lil'iijra'at aljinayiyati, dar al'ahram lil'iisdarat alqanuniat , 2020.
• eadil hamid bashir muhamad , al'iithbat aljinayiyu liljarimat almaelumatiati, dar alnahdat alearabiat lilnashr waltawzie, 2021.
• -eabdialeaziz jar allah , jarayim al'iintarnit waeuqubatuha , wathar aleawlamat ealaa mustakhdimiha , dar alkitab aljamieii , 2024.
• eabd aleazim marsaa alwaziri, alwajiz fi al'iijra'at aljinayiyat , dar alnahdat alearabia . 2002.
• -eabdallah 'ahmad al'asmari , aljarayim alsaybraniat , diwan alearab lilnashr , 2023.
• eabd allah alqudrat , aljarayim al'iilikturuniat dirasat muqaranat bayn altashrieat aldawliat walearabiati, dar aleulum lilnashri, 2021.
• -eali 'ahmad hasan , falsafat aleuqubat aljinayiyat wathar altiknulujya alhadithati, risalat majistir jamieat alqahirat disambir 2024.
• -lina muhamad al'asadiu , madaa faeiliat 'ahkam alqanun aljinayiyi fi mukafahat aljarayim almaelumatiat , dar alhamid lilnashr 2025.
• muhamad jibril 'iibrahim , altahawul alraqmiu fi nizam alqanun aljinayiyi , dirasat tahliliat tasiliatu, aldaar alearabiat lileulum , yanayir 2023 .
• muhamad eusfur al'iithbat fi aljarayim almaelumatiat dar alfikr aljamieii al'iiskandariat ,2023 .
• -muhamad ealaa suaylm , mukafahat aljarayim almaelumatiat , dirasat muqaranat , dar almatbueat aljamieiat , 2020.
• -muhamad fahd aljisghi , eilm alsiyasat aljinayiyat , dar alzaman lilnashr ,2021.
• -muhamad nusayr alsarhan , maharat altahqiq aljinayiyu fi jarayim alhasub wal'iintirnit , risalat majistir fi aleulum alshurtiat , jamieat nayif lileulum al'amniat , alriyad , 2024.
• -mahmud sulayman musaa , alsiyasat aljinayiyat wal'iisnad almaenawiu, dirasat muqaranat , dar almatbueat aljamieiat 2019.
• -mahmud eumar mahmud , aljarayim almaelumatiat , dirasat muqaranat bayn alsharieat walqanun alwadei, dar khawarzum aleilmiat , 2025.

• -mustafi 'ahmad musaa , aljarayim almaelumatiat fi alqanun almisrii, dar alnahdat alearabiati, 2022 .
• -mustifi eabdalbaqi , altahqiq fi aljarimat al'iiliktruniat wa'iithbatiha , dirasat muqaranat , majalat alsharieat walqanun , aljamieat al'urduniyat ,almujalad 45 aleadad 4 mulhaq 2, 2018.
• -marwan mansur alruwqi , alqasd aljinayiyu fi aljarayim almaelumatiat , dirasat tasiliat muqaranat , maktabat alqanun waliaqtisad , alriyad 2023.
• munaa khalil almisriu, alsiyasat aljinayiyat fi muajahat aljarayim alsiybraniati, majalat kuliyat alhuquqi, jamieat al'iiskandariati, aleadad 71, 2021.
• -maha hamad alqarinii , waqie aljarayim almaelumatiat fi almamlakat alearabiat alsueudiat , bidun dar nashr 2021.
• -nayif khalid alsharif , aljarayim almaelumatiat fi alnizam alsueudii , dirasat muqaranat , dar hafiz , 2019 si45.
• -hana' mustafaa alkhabiri, aljarayim almaelumatiat watiqnin aleumlat alraqamiat , dirasat qanuniat fi altashrieat waliatifaqiaat alduwliati, alnahdat aleilmiat lilnashr waltawzie , disambir 2023.

al'abhath walmaqalat

• -'iibrahim alhaydari , aldawabit al'iijrayiyat liljarayim almaelumatiat fi alnizam alsaeudii , almajalat alqadayiyat alsueudiat , eadad khasun 2022.
• -'iiman muhamad eazaam , aleuqubat fi nizam mukafahat aljarayim almaelumatiat fi almamlakat alearabiat alsaeudiat dirasatan tasiliat muqaranat , majalat wizarat aleadl , aleadad 82 , rajab 1439 .
https:ll www.adlm.moj.gov.sa
• 'ayman sayid muhamad aleasqalani almaswuwliat aljinayiyat ean aljarayim almaelumatiat almasat bi'amn aldawlati: dirasat muqaranat fi alfiqh al'iislamii walnizam alsaeudii majalat dirasat qanuniatin, albahrayn , mayu 2023.
• -'iimam hasanayn khalil eata allah , jarayim alaietida' ealaa alshabakat almaelumatiat fi altashrieat alearabiati: dirasat tahliliat muqaranatan bialtashrie al'iimaratii , almajalat aldawliat lilbuhuth waldirasat alqanuniat , aleadadu4 , 2024 manshur biallughat al'iinjilizia .
http:llijlrs.vsrp.co.uk

• -bakhdat sifyan , altabieat alqanuniat liljarayim almustahdathat wawasayil airtikabiha , jarimat al'iintirnit kamithali, majalat albuhuth alqanuniat walsiyasiat ,jamieat tahir bisaeidat, aljazayir , mujalad 3 aleudadu16 , 'iibril 2021.
• -bdur khalid alkarbi , tathir altaqniat ealaa wasayil al'iithbat alraqamiat fi alnizam alsaeudii , dirasat tahliliat , majalat albuhuth alfiqhiat walqanuniat , kuliyat alsharieat walqanun bidimanhur , aleadad 36 yuliu 2024.
• bandar aleutaybi, aldalil al'iiliktiruniu fi nizam al'iithbat alsueudii, majalat aleadalat walqanunu, aleadad 14, 2022.
• hazim 'ahmad alhunaydi ridwan , aljarimat almaelumatiat fi shan haqi almualif ealaa al'iintirnit tbqan liltashrie almisrii, majalat alqanuni, jamieat eayn shams, mayu 2023 .
jlaw.journals.ekb.eg
• sami eabd albaqi, al'amn alsaybiraniu kamadkhal lilwiqayat min aljarimat al'iiliktruniati, majalat albuhuth alqanuniati, jamieat eayn shams, 2020.
• -saed eatif eabdalmutalib , 'ahkam almasyuwliat aljinayiyat ean aljarayim almaelumatiat , dirasat muqaranat ,majalat aldirasat alqanuniat waliaiqtisadiati, aleadad 9, al'iisdar althaalith 2023.
http:ll www.jdi.journals.exb.eg
• sulayman shakiri, alqawaeid al'iijrayiyat walmawdueiat liljarimat almaelumatiat fi altashrie aljazayirii, almajalat aljazayiriat libuhuth alhuquq waleulum alsiyasiati, yunyu 2024.
• -tariq aleaqla , hijiat aldalil al'iiliktrunii fi majal al'iithbat aljinayiyi liljarayim almaelumatiat fi alnizam alsaeudii , majalat kuliyat alsharieat walqanun , jamieat 'asyut , aleadad 35 'iibril 2023.
• -eabd alrahman eabd allah alshaayie , "aljarimat alsaybiraniat fi alnizam aljinayiyi alsaeudii", majalat kuliyat alhuquq ,jamieat almalik sueud , aleadad 32, 2020.
• -faysal haeilan aleazimiu , 'iishkaliat almulahaqat aljazayiyat fi aljarayim al'iilikturuniati, maktabat almalik salman lileulum al'amniati, 'abril 2024.
• -kamal eabd allah almahlawi , sueubat altahqiq wal'iithbat fi aljarayim almaelumatiat wa'atharuha ealaa aleadalat aljinayiyat , majalat jamieat almuhrat lileulum al'iinsaniat , yunyu 2022.

• -majid eabdialeaziz , alsiyasat aljinayiyat fi muajahat aljarayim almaelumatiat qira'at tahliliatan lilnizam alsaeudii ,majalat jamieat al'iimam muhamad bn sueud , aleadad 36 , 2021.
• muhamad 'ahmad alnaaghi, al'ahkam alqanuniat li'arkan aljarimat almaelumatiati: dirasat fi altashrie aljazayirii wal'iimarati, almajalat aljazayiriat libuhuth alhuquq waleulum alsiyasiati, disambir 2024 .
• -muhamad husayn aldawsari , 'iishkaliat altawsif liqadaya aljarayim almaelumatiati, jaridat alwatan alsueudiati, maris 2021.
• -muhamad mahmud qubalat , alqanun alduwalii waltahadiyat almueasirat bialtatbiq ealaa aljarimat alsiybraniati, majalat alhuquq lilbuhuth alqanuniat walaiqtisadiat , jamieat al'iiskandariat , yuliu 2024.
• -mahi aldiyn eabdallah , hijiat aldalil alraqamii fi 'iithbat aljarimat almaelumatiat ,dirasat tahliliat muqaranat , majalat albuhuth alqanuniat walaiqtisadiat , jamieat almansurat , 2021.
• munaa khalil almisriu, alsiyasat aljinayiyat fi muajahat aljarayim alsiybraniati, majalat kuliyat alhuquqi, jamieat al'iiskandariati, aleadad 71, 2021.
• -nabil mahmud farid eabd alrabi , mafhum aljarayim almaelumatiat watahadiyatuha altashrieiat fi filastin , jamieat alnajah alwataniati, nabulus , yanayir 2018.
• -hadiat 'ahmad zaetar , al'iishkaliaat alqanuniat liljarayim al'iiliktruniat aleabirat lilhudud wasubul muajahatiha , majalat albuhuth alqanuniat waliaqtisadiat , kuliyat alhuquq jamieat almansurati, almujalad 13 , aleadad 84 , 2023.

al'anzima wallawayih

• -nizam mukafahat aljarayim almaelumatiat alsueudii alsaadir bialmarsum almalakii raqm mi/17 bitarikh 8/3/1428.
• al'amr almalakiu raqma('a/17) bitarikh 26/2/1439 alkhasi bi'iinsha' alhayyat alwataniat alsaeudiat lil'amn alsiybiranii .
• aldalil al'iijrayiyu fi altahqiqat alraqamiat , 'iisdarat wizarat aldaakhiliat alsaeudiat , al'iisdar althaani 2022.
• taqrir wizarat aleadl alsueudiat ean nizam al'iithbati, alriyad 2022.
• layihat tawthiq al'iijra'at alraqamiat , hayyat alhukumat alraqamiat , almamlakat alearabiat alsueudiat 2022.

• qanun mukafahat jarayim tiqniat almaelumati, alqanun almisriu raqm 175 lisanat 2018, aljaridat alrasmiat, aleadad 32 mukarir ('a), 14 'aghustus 2018.
• -qanun himayat albinyat altahtiat lilmaelumat alhayawiati, alqanun alaitihadiu raqm 5 lisanat 2020, dawlat al'iimarat alearabiat almutahidati.
• marsum biqanun atihadiin raqm 5 lisanat 2012, mukafahat jarayim taqniat almaelumati, aljaridat alrasmiati, dawlat al'iimarat alearabiat almutahidati, 2012.

alsawabiq alqadayiya alfaransia

• -mahkamat astinaf baris alghurfat 12 , 30 'uktubar 2002, alwusul ghayr almashrue
http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=136
• -mahkamat aldarajat al'uwlaa , baris, aldaayirat 12 , 1 yuniu 2007 , alwusul ghayr alqanunii
http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2179
• -almahkamat aleulya , alghurfat aljinayiyat , 8 fibrayir 2012, tadakhul albayanat watadkhul alnizam
http://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000025534746
• -almahkamat aleulya , alghurfat aljinayiyat 29 'uktubar , tishrin al'awal 2009 , takid tahil alnashr al'iiliktrunii lithaghrat 'amniat kajarimat jinayiyat bimujib almadati1-3- 323 min alqanun aljinayiyi alfaransii ('iisa'at aistikhdam aljihaz waljarayim dhat alsilati)
http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000021299967&fastReqId=750589792

فهـــرس الموضوعـــات

الموضـــــوع الصفحة

المقدمة ٢٦٢٤
مشكلة البحث ٢٦٢٤
أهمية البحث ٢٦٢٥
أهداف البحث ٢٦٢٥
المنهج المعتمد ٢٦٢٥
خطة البحث ٢٦٢٦
تمهيد وتقسيم ٢٦٢٧
المبحث الأول الأحكام العامة للإطار النظري للسياسة الجنائية والجرائم المعلوماتية ٢٦٢٩
المطلب الأول مفهوم السياسة الجنائية وتطورها ٢٦٢٩
المطلب الثاني ماهية الجرائم المعلوماتية وخصائصها القانونية ٢٦٣٦
المطلب الثالث التداخل بين السياسة الجنائية والأمن السيبراني ودوره في الوقاية من الجريمة المعلوماتية ٢٦٤١
المبحث الثاني السياسة التشريعية في مكافحة الجرائم المعلوماتية ٢٦٤٦
المطلب الأول صور التجريم في التشريعات المقارنة ٢٦٤٦
المطلب الثاني السياسة الجنائية العقابية للجرائم المعلوماتية ٢٦٥١
المطلب الثالث دور المؤسسات الجنائية في مواجهة الجرائم المعلوماتية ٢٦٥٨
المبحث الثالث السياسة الإجرائية في الجرائم المعلوماتية ومتطلبات الأمن السيبراني ٢٦٦٣
المطلب الأول وسائل الإثبات الجنائي الرقمي وضوابطه ٢٦٦٣
المطلب الثاني التحديات الإجرائية للجرائم المعلوماتية ٢٦٧٤
المطلب الثالث التحديات المستقبلية وأطر التعاون الجنائي الدولي ٢٦٧٩
الخاتمة ٢٦٨٦
أولًا: النتائج ٢٦٨٦
ثانيًا: التوصيات ٢٦٨٧
قائمة المراجع ٢٦٩٠
REFERENCES: ٢٧٠٣
فهـــرس الموضوعـــات ٢٧٠٩