An-Najah University Journal for Law and Economics

مجلة جامعة النجاح للقانون والاقتصاد

The Legal Regulation of Cybercrime Between Privacy Protection and Cybersecurity Requirements

Mohammed Abdullah El-Sheikh[1*]

(Type: Full Article). Received: 17th Apr. 2026, Accepted: 15th May. 2026
Accepted Manuscript, In Press

Abstract: Objective: To analyze the legal framework governing cybercrime amidst digital transformation, evaluate the adequacy of traditional legal rules in addressing these emerging crime patterns, and investigate the balance between cybersecurity imperatives and digital privacy protection while safeguarding fundamental rights and freedoms. **Methodology**: The study adopts a descriptive-analytical and comparative aproach to dissect legislative texts and judicial precedents, incorporating technological advancements such as "Agentic AI" and the most recent specialized legal updates. **Results**: Traditional liability and compensation rules are unable to accommodate the autonomy of smart systems, leading to a prominent "liability gap" caused by the complexity of digital evidence procedures and jurisdictional fragmentation in cross-border crimes. **Conclusions**: Classic legal theories are insufficient for the challenges posed by autonomous systems. This necessitates the creation of a flexible legislative framework that balances intellectual property and innovation with digital security needs, aligned with Sustainable Development Goals (SDGs) for promoting justice. **Recommendations**: Enacting specialized legislation that adopts "Digital Justice" concepts, strengthening international technical cooperation against cybercrime, and drafting ethical charters to protect fundamental rights and freedoms from the risks of expanded digital surveillance.

Keywords: Artificial Intelligence, Cybersecurity, Data Privacy, Civil Liability, Digital Justice.

التنظيم القانوني للجريمة الإلكترونية بين حماية الخصوصية ومتطلبات الأمن السيبراني

محمد عبدالله الشيخ[1*]

تاريخ التسليم: (2026/4/17)، تاريخ القبول: (2026/5/15)

الملخص: الهدف: تقييم مواءمة الأطر القانونية التقليدية لمواجهة الأنماط المستحدثة للجريمة الإلكترونية، وبحث إشكالية التوازن بين ضرورات الأمن السيبراني وحماية الخصوصية الرقمية في ظل التحول الرقمي الشامل . **المنهج** :اعتماد المنهج الوصفي التحليلي والمقارن لتفكيك النصوص التشريعية والاجتهادات القضائية، مع استصحاب المستجدات التقنية المتعلقة بالذكاء الاصطناعي "الوكيل (Agentic AI) "والتشريعات المتطورة . **أهم النتائج** : عجز قواعد المسؤولية والتعويض التقليدية عن استيعاب استقلالية الأنظمة الذكية، وبروز "فجوة مسؤولية" ناتجة عن تعقد إجراءات الإثبات الرقمي وتشتت الولاية القضائية في الجرائم العابرة للحدود . **الاستنتاجات** :عدم كفاية النظريات القانونية الكلاسيكية لمواكبة تحديات الأنظمة المستقلة، مما يستوجب ابتكار إطار تشريعي مرن يحقق التوازن بين حماية الملكية الفكرية والابتكار وبين مقتضيات الأمن الرقمي، اتساقاً مع أهداف التنمية المستدامة لتعزيز العدالة .**التوصيات** :سن قوانين متخصصة تتبنى مفاهيم "العدالة الرقمية"، تعزيز آليات التعاون الدولي التقني لمكافحة الجرائم السيبرانية، وصياغة مواثيق أخلاقية تضمن حماية الحقوق والحريات الأساسية من مخاطر المراقبة الرقمية الموسعة.

الكلمات المفتاحية: الذكاء الاصطناعي، الأمن السيبراني، حماية البيانات، المسؤولية المدنية، العدالة الرقمية.

المقدمة

أدى التطور التكنولوجي المتسارع، ولا سيما في مجالات الاتصالات وتقنيات المعلومات، إلى إحداث تحول جذري في بنية المجتمعات الحديثة، حيث أصبحت البيئة الرقمية فضاءً أساسيًا لممارسة الأنشطة الاقتصادية والاجتماعية والقانونية، غير أن هذا التحول، رغم ما يحمله من مزايا، أفرز في المقابل أنماطًا إجرامية مستحدثة تُعرف بالجريمة الإلكترونية، والتي تتسم بخصوصية تجعل مكافحتها أكثر تعقيدًا مقارنة بالجرائم التقليدية، وتكمن خطورة الجريمة الإلكترونية في كونها تمس بشكل مباشر أحد أهم الحقوق الأساسية، وهو الحق في الخصوصية، فضلًا عن تهديدها المستمر لأمن الفضاء السيبراني، ومن ثم أصبح لزامًا على المشرع التدخل لتنظيم هذا المجال بما يحقق التوازن بين متطلبات الأمن السيبراني من جهة، وضمان احترام الخصوصية والحريات الرقمية من جهة أخرى.

1 قسم القانون الرقمي، كلية العلوم الإنسانية، جامعة مسار، دبي، الإمارات العربية المتحدة.
* الباحث المراسل: elcounsellor@gmail.com

1 Department of Digital Law, College of Humanities, Masar University, Dubai, Country: United Arab Emirates.
Corresponding author: elcounsellor@gmail.com
ORCID: https://orcid.org/0009-0007-9222-0607

مشكلة الدراسة

تتمحور مشكلة البحث حول التساؤل الرئيسي الآتي: كيف يمكن تحقيق توازن قانوني فعال بين مكافحة الجريمة الإلكترونية وضمان حماية الخصوصية في ظل تصاعد متطلبات الأمن السيبراني؟

وتفترض الدراسة أن القواعد القانونية التقليدية غير كافية لتحقيق التوازن المطلوب، وأن الحل يكمن في تشريعات مرنة تجمع بين الردع والحماية الاستباقية للبيانات

أسئلة الدراسة

ويتفرع عن هذا التساؤل عدد من الأسئلة الفرعية، من أبرزها:

1. ما المقصود بالجريمة الإلكترونية وما خصائصها؟
2. ما الإطار القانوني لحماية الخصوصية الرقمية؟
3. إلى أي مدى تكفي التشريعات الوطنية والمقارنة، فضلًا عن الاتفاقيات الدولية، في تحقيق التوازن بين حماية الخصوصية ومتطلبات الأمن السيبراني؟
4. ما حدود مشروعية القيود المفروضة على الخصوصية باسم الأمن السيبراني؟

أهداف الدراسة

تهدف هذه الدراسة إلى ما يلي:

- تحديد المفهوم القانوني للجريمة الإلكترونية،
- بيان الأسس القانونية لحماية الخصوصية الرقمية،
- تحليل العلاقة بين متطلبات الأمن السيبراني وحقوق الأفراد،
- اقتراح حلول تشريعية تسهم في تحقيق التوازن بين الأمن وحماية الخصوصية.

أهمية الدراسة

تتمثل أهمية هذه الدراسة فيما يلي:

- تناوله لموضوع معاصر يمس صميم الأمن القانوني في العصر الرقمي
- من خلال إبراز الإشكالات القانونية المرتبطة بتنظيم الجريمة الإلكترونية
- وتحليل التداخل بين حماية الخصوصية ومتطلبات الأمن السيبراني
- المساهمة في تطوير الفكر القانوني المتعلق بالجرائم الرقمية.

منهج الدراسة

يعتمد هذا البحث على المنهج الوصفي التحليلي في دراسة الإطار القانوني للجريمة الإلكترونية، مع توظيف المنهج المقارن من خلال تحليل عدد من التشريعات الدولية والوطنية ذات الصلة، بما يتيح الوقوف على أوجه الاتفاق والاختلاف واستنباط أفضل الحلول التشريعية.

المبحث الأول: الإطار المفاهيمي والنظري للجريمة الإلكترونية والخصوصية الرقمية

المطلب الأول: مفهوم الجريمة الإلكترونية وخصائصها القانونية

تعريف الجريمة الإلكترونية

تُعد الجريمة الإلكترونية أحد أبرز أنماط الإجرام المستحدثة التي أفرزها التطور المتسارع في تقنيات المعلومات والاتصالات، حيث ارتبط ظهورها ارتباطًا وثيقًا بالاعتماد المتزايد على النظم الرقمية في مختلف مناحي الحياة، ويُقصد بها، وفقًا لتعريف بعض الفقهاء أنها هي كل سلوك غير مشروع يُرتكب باستخدام الوسائط الرقمية أو يستهدف نظم المعلومات والبيانات المخزنة أو المعالجة عبرها (Brenner, 2010, p. 62).

يتسم هذا التعريف بمرونة مفاهيمية تسمح باستيعاب التطور المستمر في صور الجريمة الإلكترونية، بما يشمل طيفًا واسعًا من الأفعال مثل الجرائم المالية والاختراق والاحتيال والتجسس والبرمجيات الخبيثة، إلا أنه يُؤخذ عليه افتقاره إلى الدقة القانونية، لعدم تمييزه بين الجريمة الموجهة ضد النظم المعلوماتية وتلك التي تُستخدم فيها التقنية كوسيلة فقط، مما يؤدي إلى توسع غير منضبط في نطاق التجريم.

كما أنه لا يضع معيارًا واضحًا للفصل بين الجريمة الإلكترونية والجريمة التقليدية ذات الوسيط الرقمي، ولا يبرز الركن التقني أو يحدد بدقة صور الاعتداء على البيانات والأنظمة، إضافةً إلى ذلك، يغفل تحديد الركن المعنوي وتمييز الأفعال العمدية عن غير العمدية، ولا يعكس الخصائص الحديثة للجريمة الإلكترونية مثل الطابع العابر للحدود وصعوبة الإثبات والتتبع، مما يستلزم تعريفًا أكثر دقة يوازن بين الشمول والانضباط القانوني.

وفي السياق ذاته يؤكد البعض الاخر أن الجريمة الإلكترونية تتميز بطابعها العابر للحدود، إذ لا ترتبط بإقليم جغرافي محدد ولا بزمن معين، كما لا تقتصر على فئة اجتماعية أو عمرية بعينها، حيث يمكن ارتكابها عن بُعد وفي أي وقت عبر الشبكات الرقمية العالمية (Clough, 2015, p. 92) ، ويترتب على هذا الطابع الدولي تعقيد ملحوظ في المسائل القانونية المرتبطة بمكافحتها، ولا سيما ما يتعلق بتحديد الاختصاص القضائي، وتنازع القوانين، وآليات التعاون القضائي الدولي، وهو ما يكشف عن محدودية القواعد الجنائية التقليدية في مواجهة هذا النمط من الإجرام، ويبرز الحاجة إلى تطوير أطر قانونية أكثر مرونة وملاءمة لطبيعة الفضاء السيبراني.

تُعد الجريمة الإلكترونية في التشريع المصري مفهومًا غير مُعرّف تعريفًا صريحًا، إذ اكتفى المشرع بتحديد بعض المصطلحات المرتبطة بها ضمن قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 (مصر، 2018)، مثل النظام المعلوماتي.

والبيانات والمواقع الإلكترونية، ومن ثم يُستفاد تعريفها بصورة غير مباشرة باعتبارها كل فعل غير مشروع يُرتكب باستخدام تقنية المعلومات أو يستهدف الأنظمة أو البيانات بما يمس أمنها أو سلامتها أو سريتها. ويُعبر هذا النهج عن أسلوب تشريعي مرن قائم على تجريم الأفعال بدلًا من وضع تعريف جامع، رغم ما قد يثيره من إشكاليات في التكييف القانوني.

أما اتفاقية بودابست (2001) فقد انتهجت أسلوبًا مختلفًا، حيث لم تضع تعريفًا عامًا للجريمة الإلكترونية، بل ركزت على تحديد صورها مثل الدخول غير المشروع، واعتراض البيانات، وتعديلها أو إتلافها، وإساءة استخدام الأجهزة، بما يعكس منهجًا عمليًا يهدف إلى الدقة وتجنب الغموض بدلًا من التعريف النظري.

وفيما يتعلق بالتشريعات العربية، فقد تأثرت نسبيًا باتفاقية بودابست من خلال تبني صور تجريمية مشابهة، كما هو الحال في التشريع المصري، إلا أن هذا التأثر ظل محدودًا بسبب عدم الانضمام الرسمي للاتفاقية في أغلب الدول، إلى جانب التحفظات المتعلقة بالسيادة وآليات التعاون الدولي، فضلًا عن وجود تفاوت بين المنهج التفصيلي للاتفاقية والنهج الأكثر عمومية في بعض التشريعات العربية، خاصة على مستوى الإجراءات الجنائية الرقمية.

وتتميز الجريمة الإلكترونية قانونيًا بعدة خصائص، أبرزها طابعها غير المادي، إذ تعتمد على آثار رقمية دون اعتداء مادي مباشر، مما يُضعف من كفاية قواعد الإثبات التقليدية ويستدعي تطوير وسائل إثبات تقنية متخصصة تتلاءم مع طبيعة البيئة الرقمية.

كما تتميز الجريمة الإلكترونية باعتمادها المكثف على أدوات تقنية متقدمة، حيث يلجأ مرتكبوها إلى استخدام برمجيات متطورة، وخوارزميات معقدة وتقنيات تشفير عالية المستوى، بل وأحيانًا تطبيقات قائمة على الذكاء الاصطناعي، بما يعزز قدرتهم على إخفاء هويتهم الرقمية ويجعل عملية تتبع مصدر الجريمة أكثر تعقيدًا بالنسبة لسلطات التحقيق، وتتجلى خصوصية هذا النمط من الجرائم كذلك في طابعها العابر للحدود الوطنية، إذ يمكن ارتكاب الجريمة الإلكترونية في دولة، بينما تقع آثارها أو ضحاياها في دولة أخرى، وهو ما يثير إشكاليات قانونية دقيقة تتعلق بتحديد الاختصاص القضائي، وتنازع القوانين، وفعالية آليات التعاون القضائي الدولي، كما أكدته اتفاقية بودابست بشأن الجريمة الإلكترونية (Council of Europe, 2001)، إلى جانب ذلك تُعد صعوبة الاكتشاف والإثبات من أبرز التحديات العملية المرتبطة بالجريمة الإلكترونية، حيث يتطلب كشف هذه الجرائم خبرات فنية متخصصة لتحليل الأدلة الرقمية، وتحديد العلاقة السببية بين السلوك الإجرامي والضرر الناتج عنه، وهو ما يزيد من تعقيد الإجراءات الجنائية ويطرح تحديات إضافية أمام القضاة وأجهزة العدالة الجنائية (Soyer, B., & Tettenborn, A. 2023, p.9). هذه الخصائص القانونية تؤكد على أن القوانين التقليدية غالبًا غير كافية لمواجهة الجرائم الرقمية، ما يفرض على المشرع الوطني والدولي تطوير أطر تشريعية جديدة، تحدد طبيعة الجرائم، والأدوات القانونية للملاحقة، وآليات التعاون الدولي.

المطلب الثاني: الخصوصية الرقمية في البيئة السيبرانية

طبيعة الخصوصية الرقمية

لم يعد مفهوم الخصوصية يقتصر على حماية الحياة الخاصة بالمعنى التقليدي المرتبط بالمجال الشخصي أو الأسري، بل شهد توسعًا ملحوظًا ليشمل الخصوصية الرقمية، التي تتعلق بحماية البيانات الشخصية والمعلومات الإلكترونية المرتبطة بالأفراد في الفضاء السيبراني.

وفي هذا السياق، يؤكد بعض الفقهاء أن البيانات الشخصية أصبحت تمثل أحد أهم الموارد في العصر الرقمي، نظرًا لما تتضمنه من معلومات حساسة، مثل البيانات الصحية، والمالية، والسلوكية، والاجتماعية، التي يمكن استغلالها بطرق تمس كرامة الأفراد وحقوقهم الأساسية.

ويؤدي الاعتماد المتزايد للأنظمة الذكية والتطبيقات الرقمية على تقنيات تحليل البيانات الضخمة إلى تعاظم مخاطر انتهاك الخصوصية، سواء من خلال الجمع غير المشروع للبيانات، أو إساءة استخدامها، أو معالجتها خارج الأغراض المصرح بها، ويثير هذا الواقع إشكاليات قانونية متعددة تتعلق بحدود تدخل الدولة في المجال الرقمي، ومسؤولية الشركات المطورة ومزودي الخدمات الرقمية، فضلًا عن مدى تمتع المستخدمين بسلطة حقيقية على بياناتهم الشخصية في ظل التعقيد التقني للأنظمة الذكية.

الأطر القانونية لحماية الخصوصية الرقمية

سعت التشريعات الحديثة إلى تكريس حماية الخصوصية الرقمية بوصفها أحد الحقوق الأساسية للأفراد، من خلال إرساء أطر قانونية تهدف إلى تنظيم جمع البيانات الشخصية ومعالجتها وضمان أمنها، ويُعد التنظيم الأوروبي العام لحماية البيانات (General Data Protection Regulation – GDPR) من أبرز النماذج التشريعية في هذا المجال، إذ أرسى مجموعة من المبادئ الأساسية لمعالجة البيانات، من بينها مبدأ المشروعية، والشفافية، وتقليل البيانات، وضمان حق الأفراد في الوصول إلى بياناتهم وتصحيحها، فضلًا عن فرض التزامات صارمة على الشركات

والمؤسسات بشأن أمن البيانات والمسؤولية عن أي خرق لها (European Union, 2016).

وعلى الصعيد العربي، بدأت بعض التشريعات الوطنية في مواكبة هذا التوجه، كما هو الحال في قانون حماية البيانات الشخصية في دولة الإمارات العربية المتحدة الصادر بموجب المرسوم بقانون اتحادي رقم (45) لسنة 2021، الذي نظم آليات جمع ومعالجة البيانات الشخصية، وأقر حقوقًا للأفراد في التحكم بمعلوماتهم، وحدد التزامات قانونية على الجهات المتحكمة في البيانات لضمان حمايتها من الانتهاك أو التسريب، غير أن التطبيق العملي لهذه التشريعات يواجه تحديات متزايدة، لاسيما في ظل تصاعد الجرائم الإلكترونية، وما يرافقها من توسع السلطات العامة في اتخاذ تدابير رقابية رقمية بدعوى حماية الأمن السيبراني، الأمر الذي قد يؤدي في بعض الحالات إلى تضييق نطاق الخصوصية الرقمية، ويُحدث توترًا قانونيًا بين حماية الحقوق الفردية ومتطلبات الأمن العام.

التحديات القانونية والتوازن بين الخصوصية والأمن السيبراني

تُعد مسألة التوفيق بين حماية الخصوصية الرقمية ومتطلبات الأمن السيبراني من أكثر القضايا القانونية تعقيدًا في العصر الرقمي، ويبرز في هذا الإطار مبدأ التناسب كأحد الضوابط الجوهرية، إذ يقتضي أن يكون أي تدخل في البيانات الشخصية ضروريًا لتحقيق هدف مشروع، وألا يتجاوز الحد الأدنى اللازم لتحقيق هذا الهدف، بما يضمن عدم المساس غير المبرر بالحقوق والحريات الفردية (Solove, 2008, p. 80)

وإلى جانب ذلك، تبرز أهمية الرقابة القضائية كآلية جوهرية لضمان مشروعية التدخلات الرقمية التي تقوم بها السلطات العامة، خاصة في ظل التوسع المتزايد في استخدام أدوات المراقبة الإلكترونية، مثل تقنيات تتبع الاتصالات، وتحليل البيانات الضخمة، واستخدام الذكاء الاصطناعي في رصد الأنشطة الرقمية.

إذ تمثل هذه الرقابة صمام الأمان الذي يكفل خضوع تلك التدخلات لمبدأ سيادة القانون، ويحول دون تحولها إلى وسيلة لانتهاك الحقوق والحريات الأساسية تحت غطاء الحفاظ على الأمن السيبراني.

فالرقابة القضائية الفعالة لا تقتصر على مجرد الإذن المسبق بإجراء التدخلات، وإنما تمتد لتشمل رقابة لاحقة على مشروعية الإجراءات المتخذة، ومدى تناسبها مع الهدف المشروع، ومدى احترامها لمبدأ الضرورة والتناسب.

كما تسهم في تعزيز الشفافية والمساءلة، من خلال تمكين الأفراد من الطعن في الإجراءات التي تمس حقوقهم، وهو ما يعزز الثقة في النظام القانوني ويحد من مخاطر التعسف أو إساءة استخدام السلطة في البيئة الرقمية.

وفي هذا السياق، تبرز الخصوصية الرقمية باعتبارها ركيزة أساسية من ركائز حقوق الإنسان في العصر الرقمي، إذ لم تعد الخصوصية مقتصرة على الحياة المادية للفرد، بل امتدت لتشمل بياناته ومعلوماته وأنشطته في الفضاء السيبراني.

ويُعد انتهاك هذه الخصوصية، سواء من قبل جهات عامة أو خاصة، مساسًا مباشرًا بكرامة الإنسان واستقلاله الشخصي، الأمر الذي يستوجب توفير حماية قانونية فعالة ومتكاملة.

غير أن التحدي القانوني الحقيقي يتمثل في كيفية تحقيق التوازن بين حماية الخصوصية الرقمية ومتطلبات الأمن السيبراني، خاصة في ظل تصاعد التهديدات الإلكترونية، مثل الجرائم المعلوماتية والهجمات السيبرانية والإرهاب الرقمي.

فالمبالغة في حماية الخصوصية قد تعرقل جهود المكافحة، في حين أن التوسع غير المنضبط في إجراءات المراقبة قد يؤدي إلى تقويض الحقوق والحريات الأساسية. ومن ثم، فإن تحقيق هذا التوازن يتطلب وضع إطار قانوني دقيق يحدد بوضوح نطاق السلطات الممنوحة للجهات المختصة، ويضع ضمانات فعالة تحول دون إساءة استخدامها.

كما يتطلب ذلك تعزيز التعاون بين مختلف الفاعلين، وفي مقدمتهم المشرع، والسلطات القضائية، والجهات الرقابية، والخبراء التقنيون، من أجل صياغة تشريعات مرنة وقابلة للتطور، تستجيب لطبيعة البيئة الرقمية المتغيرة.

ويشمل هذا التعاون تبادل الخبرات، وتبني المعايير الدولية، وتطوير آليات رقابية وتقنية حديثة قادرة على مواكبة التطور التكنولوجي المتسارع.

ويتضح من ذلك أن العلاقة بين الجريمة الإلكترونية والخصوصية الرقمية هي علاقة تفاعلية ومعقدة، تتأثر بشكل مباشر بالتحولات التكنولوجية المتلاحقة، حيث يؤدي تطور وسائل ارتكاب الجريمة إلى تطور مماثل في وسائل مكافحتها، وهو ما ينعكس بدوره على نطاق الحماية المقررة للخصوصية.

وقد أكدت العديد من الدراسات الفقهية أن القوانين التقليدية، التي وُضعت في سياق مادي تقليدي، لم تعد كافية لمواجهة التحديات التي تفرضها البيئة الرقمية، سواء من حيث تعريف الأفعال المجرّمة، أو وسائل الإثبات، أو تحديد المسؤولية القانونية.

وعليه، يصبح من الضروري العمل على تطوير أطر تشريعية حديثة، سواء على المستوى الوطني أو الدولي، تستوعب خصوصية الجريمة الإلكترونية، وتكفل حماية فعالة للبيانات الشخصية، مع وضع قواعد واضحة لتحديد المسؤولية القانونية لمختلف الأطراف المتدخلة، سواء كانوا أفرادًا أو شركات أو مزودي خدمات رقمية.

كما يقتضي الأمر تطوير آليات التحقيق القضائي الرقمي، من خلال اعتماد وسائل تقنية متقدمة في جمع الأدلة وتحليلها، وضمان حجيتها أمام القضاء، بما يحقق الفعالية في ملاحقة الجرائم دون الإخلال بضمانات المحاكمة العادلة.

أن مواجهة التحديات القانونية التي تفرضها البيئة الرقمية لا يمكن أن تتم من خلال الأدوات التقليدية وحدها، بل تتطلب رؤية تشريعية متكاملة تستند إلى فهم عميق لطبيعة التحول الرقمي، وتوازن دقيق بين مقتضيات الأمن ومتطلبات حماية الحقوق والحريات، بما يضمن تحقيق ما يمكن تسميته بـ"العدالة الرقمية" في صورتها المعاصرة.

المبحث الثاني: المسؤولية القانونية عن الجرائم الإلكترونية

المطلب الأول: الإطار القانوني للمسؤولية عن الجرائم الإلكترونية

المسؤولية المدنية والجنائية في الفضاء الرقمي

يُعد تحديد المسؤولية القانونية الناشئة عن الجرائم الإلكترونية من أكثر الإشكاليات تعقيدًا في إطار الفضاء الرقمي، وذلك بالنظر إلى الطبيعة التقنية الخاصة لهذه الجرائم، وتعدد الفاعلين المتداخلين في ارتكابها أو المساهمة فيها، فضلًا عن الطابع اللامادي للأفعال محل التجريم.

وفي هذا السياق، يذهب جانب من الفقه إلى أن الجرائم الإلكترونية تُرتب نوعين متلازمين من المسؤولية القانونية، هما المسؤولية الجنائية التي تستهدف معاقبة الجاني وردع غيره، والمسؤولية المدنية التي تهدف إلى جبر الضرر وتعويض المتضررين عن الخسائر الناجمة عن الفعل غير المشروع (Brenner, 2010, p. 65).

وتقوم المسؤولية الجنائية في مجال الجرائم الإلكترونية على إخضاع مرتكبي الأفعال الإجرامية الرقمية، مثل الدخول غير المشروع إلى الأنظمة المعلوماتية، أو اختراق الشبكات، أو الاستيلاء على البيانات، أو الاحتيال الإلكتروني، للعقوبات المقررة قانونًا، وفقًا لمبدأ شرعية الجرائم والعقوبات.

غير أن تفعيل هذه المسؤولية يواجه تحديات خاصة، لعل أبرزها الطابع العابر للحدود لهذه الجرائم، حيث يمكن ارتكاب الفعل الإجرامي من دولة، وتوجيهه إلى ضحية في دولة أخرى، مع استخدام خوادم موجودة في دولة ثالثة، الأمر الذي يثير إشكالات معقدة تتعلق بتحديد الاختصاص القضائي، وتنازع القوانين، وصعوبة تحديد مكان ارتكاب الجريمة (Clough, 2015, p. 95).

كما تبرز إشكالية إثبات الجريمة الإلكترونية، نظرًا للطبيعة الرقمية للأدلة، التي قد تكون عرضة للتغيير أو الإتلاف بسهولة، فضلًا عن الحاجة إلى خبرات تقنية متخصصة لتحليلها واستخلاصها بشكل يضمن حجيتها أمام القضاء.

وهو ما دفع العديد من التشريعات إلى تطوير قواعد خاصة بالإثبات الرقمي، والاستعانة بوسائل تقنية حديثة في جمع الأدلة وتحليلها (Soyer, B., &Tettenborn, A.2023., p.9).

تتضاعف تحديات إثبات المسؤولية في الجرائم المعلوماتية نظراً للطبيعة الافتراضية للدليل الرقمي، مما يجعله عرضة للمحو أو التعديل دون ترك أثر مادي ملموس.

ولضمان حجية الدليل الإلكتروني أمام القضاء، يستوجب الأمر استيفاء ضوابط جوهرية، في مقدمتها صون سلامة 'سلسلة الحيازة الرقمية' (Chain of Custody) عبر توثيق دقيق لكافة مراحل التعامل مع الدليل منذ لحظة الضبط الفني وحتى تقديمه للمحكمة.

كما يغدو من المتعين ضمان عدم العبث بالأدلة الرقمية من خلال استخدام تقنيات التحقق الفني (مثل خوارزميات الـ Hash) التي تمنح الدليل بصمة رقمية فريدة تمنع التلاعب بمحتواه أو التشكيك في صدقيته، بما يكفل مطابقة المادة العلمية المقدمة للقضاء للأصل الرقمي المضبوط تمام المطابقة.

ويُضاف إلى ذلك تحدي التعاون القضائي الدولي، حيث تتطلب ملاحقة الجرائم الإلكترونية تنسيقًا فعالًا بين الدول، سواء في مجال تسليم المجرمين أو تبادل المعلومات أو تنفيذ الأحكام، وهو ما حاولت معالجته الاتفاقيات الدولية، وعلى رأسها اتفاقية بودابست بشأن الجرائم الإلكترونية (Council of Europe, 2001)، غير أن فعالية هذه الآليات لا تزال محل نقاش، خاصة في ظل اختلاف النظم القانونية وتباين مستويات التعاون الدولي.

أما المسؤولية المدنية، فتقوم على أساس تعويض الضحايا عن الأضرار المادية والمعنوية التي تلحق بهم نتيجة الاعتداءات الرقمية، ولا تقتصر بالضرورة على الفاعل المباشر للجريمة، بل قد تمتد لتشمل أطرافًا أخرى، مثل الشركات المطورة للبرمجيات، أو مزودي خدمات الإنترنت، أو مشغلي المنصات الرقمية، متى ثبت إخلالهم بواجبات الحيطة والحذر، أو تقصيرهم في اتخاذ التدابير التقنية والتنظيمية اللازمة لحماية البيانات وتأمين النظم المعلوماتية (Kuner, 2013, p. 112).

ويُثير هذا الامتداد في نطاق المسؤولية المدنية تساؤلات جوهرية حول مدى كفاية القواعد التقليدية للمسؤولية التقصيرية في مواجهة المخاطر الرقمية، خاصة فيما يتعلق بإثبات الخطأ، وتحديد الضرر، وإقامة العلاقة السببية.

ففي كثير من الحالات، يكون الضرر ناتجًا عن تفاعل معقد بين عدة أنظمة تقنية، أو نتيجة خوارزميات يصعب تفسيرها، وهو ما يجعل من الصعب إسناد المسؤولية إلى طرف محدد (Pasquale, 2015, p. 192).

كما يطرح استخدام الذكاء الاصطناعي في الأنظمة الرقمية إشكاليات إضافية، تتعلق بإمكانية مساءلة الأنظمة الذكية ذاتها،

أو تحميل المسؤولية لمطوريها أو مستخدميها، خاصة في ظل ما تتمتع به هذه الأنظمة من قدر من الاستقلالية في اتخاذ القرار، وهو ما يستدعي إعادة النظر في المفاهيم التقليدية للمسؤولية القانونية (Sheward, 2018, p. 36).

ومن ناحية أخرى، اتجهت بعض التشريعات الحديثة إلى تبني نماذج جديدة للمسؤولية، تقوم على أساس المخاطر أو المسؤولية الموضوعية، بدلًا من المسؤولية القائمة على الخطأ، وذلك في محاولة لتجاوز صعوبات الإثبات وتحقيق حماية أكثر فعالية للمتضررين في البيئة الرقمية، كما يظهر في بعض التوجهات التشريعية الأوروبية ذات الصلة بالذكاء الاصطناعي والمسؤولية الرقمية (European Union, 2016).

يتضح أن المسؤولية القانونية في الفضاء الرقمي تشهد تحولًا عميقًا، نتيجة للتطورات التكنولوجية المتسارعة، وهو ما يفرض ضرورة تطوير الأطر القانونية التقليدية، واعتماد مقاربات تشريعية جديدة تراعي خصوصية البيئة الرقمية، وتحقق التوازن بين حماية الأفراد وتشجيع الابتكار، بما يضمن تحقيق العدالة في صورتها الرقمية المعاصرة.

التحديات العملية لإثبات المسؤولية القانونية عن الجرائم الإلكترونية

تواجه السلطات القضائية تحديات عملية جسيمة في مجال إثبات الجرائم الإلكترونية، ويُعد ذلك من أبرز العوائق التي تعترض سبيل تحقيق العدالة الجنائية والمدنية في الفضاء الرقمي، بالنظر إلى الطبيعة غير المادية لهذه الجرائم، واعتمادها على بيئة تقنية معقدة ومتغيرة باستمرار.

وتتمثل هذه التحديات بوجه خاص في صعوبة تحديد الجهة الفاعلة، إذ غالبًا ما تُرتكب الجرائم الإلكترونية باستخدام وسائل تقنية متقدمة تُخفي هوية الجاني الحقيقي، مثل الشبكات الخاصة الافتراضية (VPN) ، وتقنيات إخفاء الهوية، وخوادم الوسيط (Proxy Servers) ، فضلًا عن استخدام تقنيات الذكاء الاصطناعي والبرمجيات الخبيثة المؤتمتة، الأمر الذي يجعل من عملية تتبع الفاعل الحقيقي مسألة بالغة التعقيد (Brenner, 2010, p. 66).

كما تتفاقم هذه الصعوبة في ظل الطابع العابر للحدود للجرائم الإلكترونية، حيث يمكن تنفيذ الجريمة من إقليم دولة معينة، بينما تتحقق نتيجتها في إقليم دولة أخرى، مع مرور البيانات عبر عدة نظم قانونية مختلفة، وهو ما يطرح إشكالات دقيقة تتعلق بالاختصاص القضائي، وتنازع القوانين، وإمكانية الحصول على الأدلة الرقمية من خارج الحدود الوطنية (Clough, 2015, p. 96).

ومن ناحية أخرى، تبرز الإشكالية في خصوصية الأدلة الرقمية، التي تختلف من حيث طبيعتها وطرق جمعها وتحليلها عن الأدلة التقليدية، فهي أدلة غير ملموسة، وقابلة للتعديل أو الإتلاف بسهولة، وقد تكون موزعة عبر أنظمة متعددة أو مخزنة في بيئات سحابية، وهو ما يفرض ضرورة اتباع إجراءات دقيقة لضمان سلامة الدليل الرقمي وحجيته أمام القضاء.

وتشمل هذه الأدلة سجلات الخوادم (Logs)، وعناوين بروتوكول الإنترنت (IP Addresses)، والبيانات الوصفية (Metadata)، والرسائل الإلكترونية، والملفات المشفرة، وهي جميعها تتطلب خبرات فنية وتقنية عالية لفهمها وتفسيرها (Soyer, B., & Tettenborn, A.2023, p.10).

ويؤدي هذا التعقيد التقني إلى زيادة الاعتماد على الخبرة الفنية، حيث أصبحت تقارير الخبراء عنصرًا حاسمًا في تكوين قناعة القاضي، غير أن هذا الاعتماد يثير بدوره إشكاليات تتعلق بمدى فهم القاضي للجوانب التقنية، ومدى حياد الخبراء، فضلًا عن احتمال تضارب التقارير الفنية، وهو ما قد يؤثر سلبًا في مبدأ اليقين القضائي، ويؤدي إلى إطالة أمد النزاعات القضائية، بما يتعارض مع متطلبات العدالة الناجزة.

إلى جانب ذلك، يثير تعدد الأطراف المتداخلة في البيئة الرقمية إشكالات إضافية في تحديد نطاق المسؤولية القانونية، إذ قد تتوزع الأدوار بين المستخدم النهائي، ومزود خدمة الإنترنت، ومشغل النظام، ومطور البرمجيات، بل وحتى مزودي خدمات الاستضافة السحابية، الأمر الذي يعقد عملية إسناد الفعل الضار إلى طرف معين.

ويطرح ذلك تساؤلات دقيقة حول معيار المسؤولية وحدود التزام كل طرف، خاصة في ظل اختلاف أدوارهم التقنية والقانونية، وما إذا كان الأساس هو الخطأ أم المخاطر أم الالتزام بضمان السلامة (Kuner, 2013, p. 113).

كما تظهر صعوبات خاصة في إثبات العلاقة السببية، إذ قد يكون الضرر ناتجًا عن سلسلة من الأفعال المتداخلة أو عن خلل تقني متعدد المصادر، مما يجعل من الصعب تحديد السبب المباشر للضرر، وهو ما يكشف عن محدودية النظريات التقليدية في السببية عند تطبيقها على البيئة الرقمية (Pasquale, 2015, p. 192).

وتؤكد هذه الصعوبات مجتمعة الحاجة إلى تطوير قواعد إثبات مرنة ومتكيفة مع خصوصية الجرائم الإلكترونية، بحيث تراعي الطبيعة التقنية للأدلة الرقمية، وتسمح باستخدام وسائل حديثة في الإثبات، مثل التحليل الجنائي الرقمي (Digital Forensics)، وتقنيات تتبع البيانات، مع وضع ضمانات قانونية لحماية الحقوق والحريات الأساسية، خاصة الحق في الخصوصية وحماية البيانات الشخصية.

وفي هذا السياق، برزت اتجاهات تشريعية وفقهية تدعو إلى إعادة النظر في الإطار القانوني التقليدي، من خلال تبني نماذج أكثر ملاءمة للبيئة الرقمية، مثل المسؤولية الموضوعية القائمة على المخاطر، أو تخفيف عبء الإثبات عن المضرور،

أو إقرار قرائن قانونية تساعد في إثبات الخطأ أو العلاقة السببية، بما يسهم في تحقيق توازن بين حماية الضحايا وضمان فعالية الملاحقة القانونية.

كما يتطلب الأمر تعزيز التعاون الدولي في مجال تبادل الأدلة الرقمية، وتوحيد المعايير الإجرائية المتعلقة بجمعها وتحليلها، وهو ما سعت إليه بعض الاتفاقيات الدولية، مثل اتفاقية بودابست بشأن الجرائم الإلكترونية (Council of Europe, 2001)، التي أرست إطارًا للتعاون بين الدول في هذا المجال.

تُعد اتفاقية بودابست من أهم الأطر الدولية في مكافحة الجرائم الإلكترونية، لكنها تثير إشكاليات قانونية وسيادية، خاصة في السياق العربي، إذ يُؤخذ عليها تأثرها بالمنظور الغربي في تنظيم الفضاء الرقمي، بما قد لا ينسجم مع خصوصيات النظم القانونية العربية القائمة على اعتبارات السيادة والنظام العام.

كما تُثير الاتفاقية تحفظات تتعلق بتوسيع آليات التعاون الدولي وتبادل البيانات، وما قد يترتب عليه من مساس محتمل بالسيادة الوطنية والخصوصية، إلى جانب منح سلطات واسعة لجهات إنفاذ القانون في جمع الأدلة الرقمية دون ضمانات كافية في بعض الجوانب، ويُضاف إلى ذلك صعوبة تطبيق نموذجها الموحد في دول تختلف في بنيتها القانونية والتقنية، خاصة الدول النامية.

وبالتالي، فإن الاتفاقية تمثل إطارًا مهمًا لكنه نسبي وليس مثاليًا، مما يستدعي تطوير نماذج أكثر توافقًا مع الخصوصيات الوطنية، وتحديث القواعد القانونية والإجرائية بما يتلاءم مع طبيعة الجرائم الرقمية وتعقيداتها.

المطلب الثاني: حماية الخصوصية الرقمية في مواجهة متطلبات الأمن السيبراني

مبدأ حماية البيانات الشخصية في البيئة الرقمية

أولت التشريعات الحديثة اهتمامًا متزايدًا بحماية الخصوصية الرقمية باعتبارها امتدادًا للحق في الحياة الخاصة في البيئة السيبرانية، في ظل ما يفرضه الفضاء الرقمي من مخاطر متنامية تتعلق بجمع البيانات الشخصية ومعالجتها وتحليلها، بما قد يؤدي إلى انتهاك خصوصية الأفراد عبر بناء ملفات تعريف دقيقة لهم.

وفي هذا السياق، أرست اللائحة الأوروبية العامة لحماية البيانات (GDPR) إطارًا قانونيًا متكاملًا يقوم على مبادئ أساسية، أبرزها المشروعية والشفافية وتحديد الغرض، إلى جانب تقليل البيانات ودقتها وتحديد مدة الاحتفاظ بها، بما يضمن عدم إساءة استخدامها أو الاحتفاظ بها دون مبرر قانوني.

كما منحت اللائحة حقوقًا موسعة للأفراد، مثل حق الوصول إلى البيانات وتصحيحها وحذفها (الحق في النسيان)، وحق تقييد المعالجة ونقل البيانات، بما يعزز سيطرة الأفراد على بياناتهم الشخصية ويكرس حماية فعالة للخصوصية في البيئة الرقمية (European Union, 2016).

ولا يقتصر نطاق الحماية القانونية للخصوصية الرقمية على تنظيم سلوك الأفراد أو تحديد حقوقهم فحسب، بل يمتد ليشمل فرض التزامات قانونية مباشرة على المؤسسات والشركات مقدمة الخدمات الرقمية، باعتبارها الجهات الأكثر قدرة على جمع ومعالجة كميات ضخمة من البيانات الشخصية.

وفي هذا السياق، أصبحت هذه الجهات ملزمة قانونًا بتطبيق تدابير تقنية وتنظيمية صارمة لضمان أمن البيانات، مثل التشفير، وإدارة صلاحيات الوصول، وإجراء تقييمات دورية للمخاطر الأمنية، بما يقلل من احتمالية وقوع انتهاكات أو تسريبات للبيانات.

كما ألزمت التشريعات الحديثة هذه المؤسسات بواجب الإبلاغ الفوري عن خروقات البيانات (Data Breach Notification)، سواء للجهات الرقابية أو للأفراد المتضررين، وهو ما يمثل تحولًا مهمًا في فلسفة الحماية القانونية، من نموذج رد الفعل إلى نموذج الوقاية والإنذار المبكر، بما يسمح باتخاذ إجراءات سريعة للحد من آثار الانتهاك.

وفي هذا السياق، يشير بعض الفقه إلى أن التشريعات الحديثة قد انتقلت بالفعل من الاكتفاء بإقرار التزامات عامة وغامضة إلى فرض واجبات تقنية وتنظيمية دقيقة ومحددة على الشركات، تشمل تأمين الأنظمة المعلوماتية وفق معايير أمنية معتمدة، وتبني سياسات داخلية لحوكمة البيانات، وتدريب العاملين على حماية الخصوصية الرقمية، واتخاذ تدابير وقائية استباقية لمنع الاختراقات والهجمات السيبرانية قبل وقوعها.

كما امتدت التزامات حماية البيانات لتشمل مختلف الفاعلين في البيئة الرقمية، وليس فقط الشركات الكبرى، بل أيضًا مقدمي خدمات الحوسبة السحابية، ومنصات التواصل الاجتماعي، ومطوري التطبيقات، نظرًا لدورهم المحوري في معالجة البيانات الشخصية.

ومع تطور تقنيات الذكاء الاصطناعي وتحليل البيانات الضخمة، أصبحت حماية البيانات أكثر تعقيدًا، إذ لم تعد المعالجة تقتصر على الاستخدام المباشر، بل شملت الاستخدامات الاستنتاجية والتنبؤية التي قد تكشف معلومات حساسة بشكل غير مباشر، مما يفرض تحديات تنظيمية جديدة، خاصة فيما يتعلق بالاستخدام الثانوي للبيانات.

وبذلك، أصبحت حماية البيانات الشخصية نظامًا قانونيًا متكاملًا يوازن بين حماية الخصوصية وضمان الابتكار الرقمي واستمرارية تدفق البيانات، وهو ما يتطلب تحديثًا

مستمرًا للتشريعات لمواكبة التطور التكنولوجي وتحقيق حماية فعالة وشاملة.

متطلبات الأمن السيبراني ومبرراتها القانونية

في ظل التحول الرقمي المتسارع، أصبح الأمن السيبراني ضرورة أساسية لضمان حماية الأنظمة المعلوماتية واستمرارية عملها، ولم يعد مجرد خيار تقني، بل متطلبًا استراتيجيًا تفرضه طبيعة البيئة الرقمية المعتمدة على البيانات.

ويتحقق الأمن السيبراني من خلال مجموعة متكاملة من التدابير التقنية والقانونية والتنظيمية، تشمل تعزيز أنظمة الحماية والتشفير، وتطوير أدوات الكشف المبكر عن الهجمات، إلى جانب سنّ تشريعات تجرّم الاعتداء على النظم المعلوماتية وتحدد المسؤوليات والعقوبات.

وفي المقابل، تتعدد التهديدات السيبرانية، مثل الهجمات المنظمة، والبرمجيات الخبيثة، وتسريب البيانات، والتجسس الإلكتروني، وهي مخاطر تمس خصوصية الأفراد وأمن المؤسسات والبنى التحتية الحيوية.

وعلى المستوى الدولي، تمثل اتفاقية بودابست إطارًا مرجعيًا مهمًا لمكافحة الجريمة الإلكترونية، حيث وفرت آليات فعالة للملاحقة وجمع الأدلة الرقمية، مع التأكيد على ضرورة احترام حقوق الإنسان، وخاصة الحق في الخصوصية.

ويعكس ذلك توجهًا نحو تحقيق توازن بين متطلبات الأمن السيبراني وحماية الحقوق والحريات، بما يؤكد أن الأمن السيبراني مجال قانوني متكامل يجمع بين البعد الأمني والحقوقي، ويستدعي تشريعات مرنة قادرة على مواكبة التطور التكنولوجي دون الإخلال بضمانات الأفراد.

إشكالية التوازن بين حماية الخصوصية ومتطلبات الأمن السيبراني

تتمحور الإشكالية القانونية الأساسية في هذا السياق حول كيفية تحقيق توازن دقيق بين تمكين السلطات العامة من اتخاذ تدابير فعالة وناجعة لحماية الأمن السيبراني من جهة، وبين ضمان احترام الحق في الخصوصية الرقمية من جهة أخرى، وعدم المساس به إلا في أضيق الحدود التي تقتضيها الضرورة وبما يتوافق مع مبدأي المشروعية والتناسب. ويثور التساؤل الجوهري هنا حول مدى مشروعية المراقبة الرقمية الواسعة النطاق، وحدود جمع البيانات ومعالجتها وتخزينها لأغراض أمنية، وضمان عدم تحول هذه التدابير الاستثنائية إلى أدوات دائمة للمراقبة الشاملة أو وسيلة لانتهاك الحقوق الأساسية للمستخدمين تحت غطاء الأمن العام (Solove, 2008, p. 85).

وتتزايد حدة هذه الإشكالية في ظل التطور المتسارع لتقنيات تحليل البيانات الضخمة والذكاء الاصطناعي، التي تتيح للسلطات أو حتى للجهات الخاصة إمكانية تتبع السلوك الرقمي للأفراد بشكل دقيق، واستخلاص أنماط حياتهم وتوجهاتهم، وهو ما قد يؤدي إلى ما يُعرف بـ "اقتصاد المراقبة" الذي تتحول فيه البيانات الشخصية إلى مورد اقتصادي وأمني في آن واحد(Pasquale, 2015, p. 193). وهو ما يثير مخاطر جدية تتعلق بإعادة تعريف مفهوم الخصوصية ذاته، من مجرد حق سلبي في عدم التدخل، إلى حق إيجابي في التحكم بالبيانات الشخصية وتحديد مصيرها.

ولمواجهة هذه الإشكالية، يقترح الفقه القانوني والتشريعات المقارنة مجموعة من الحلول، يأتي في مقدمتها تعزيز آليات الرقابة القضائية والإدارية على إجراءات المراقبة وجمع البيانات، بما يضمن خضوعها لمبدأ المشروعية، وعدم اتخاذها إلا بناءً على مبررات جدية ومحددة سلفًا، ووفقًا لضوابط صارمة تضمن احترام مبدأ التناسب بين الإجراء الأمني والهدف المراد تحقيقه (Clough, 2015, p. 96). كما تمتد هذه الرقابة لتشمل الرقابة اللاحقة على كيفية استخدام البيانات المخزنة، ومنع إساءة استغلالها أو إعادة استخدامها خارج الغرض الذي جُمعت من أجله.

كما يُؤكد الاتجاه الفقهي الحديث على أهمية اعتماد معايير تقنية وقانونية متقدمة لحماية الخصوصية، مثل تقنيات التشفير القوي للبيانات (Encryption)، وتقنيات إخفاء الهوية أو تقليل قابلية التعرف (Anonymization & Pseudonymization)، وتطوير نظم مراقبة ذكية قائمة على مبدأ "الحد الأدنى من البيانات (Data Minimization)"، بحيث يتم جمع أقل قدر ممكن من المعلومات اللازمة لتحقيق الغرض الأمني دون توسع غير مبرر في جمع البيانات (European Union, 2016).

ومن ناحية أخرى، تبرز الحاجة إلى مواءمة التشريعات الوطنية مع المعايير الدولية والإقليمية في مجال حماية البيانات والأمن السيبراني، من خلال استلهام التجارب المقارنة، ولا سيما النموذج الأوروبي الذي يُعد من أكثر النماذج تطورًا في هذا المجال، حيث وضع إطارًا قانونيًا متكاملًا لتنظيم معالجة البيانات الشخصية، وتحديد حقوق الأفراد، وفرض التزامات صارمة على الجهات العامة والخاصة على حد سواء (GDPR).

كما تؤكد اتفاقية بودابست بشأن الجرائم الإلكترونية على أهمية التعاون الدولي في مواجهة الجرائم السيبرانية وضمان عدم إفلات الجناة من العقاب (Council of Europe, 2001).

وفي هذا السياق، يصبح من الضروري تحديد نطاق المسؤولية القانونية لكل من السلطات العامة والجهات الخاصة، بما في ذلك مزودو خدمات الإنترنت، وشركات التكنولوجيا، ومطورو البرمجيات، بما يضمن عدم توسع السلطة التقديرية بشكل يضر بالحقوق الأساسية، وفي الوقت ذاته يحقق فعالية

في مواجهة التهديدات الرقمية المتزايدة (Austin *et al.*, 2012, p. 211).

كما أن تحقيق هذا التوازن لا يمكن أن يتم من خلال قواعد جامدة، بل يتطلب تبني مقاربة مرنة وديناميكية في التشريع، تسمح بتطوير القواعد القانونية بشكل مستمر وفقًا لتطور التكنولوجيا، مع إدخال آليات تقييم دوري لمدى فاعلية الإجراءات المتخذة في حماية الأمن السيبراني دون الإضرار بالخصوصية.

يتضح أن التوازن بين حماية الخصوصية ومتطلبات الأمن السيبراني يمثل أحد التحديات المركزية في القانون المعاصر، حيث لم تعد المسألة مجرد اختيار بين الأمن والحرية، بل أصبحت عملية مركبة تتطلب إعادة صياغة المفاهيم القانونية التقليدية في ضوء التحول الرقمي، بما يضمن إنشاء منظومة قانونية متكاملة قادرة على مواجهة الجرائم الإلكترونية بفعالية، وفي الوقت نفسه صون الحقوق والحريات الأساسية للأفراد في البيئة الرقمية المعاصرة.

يتطلب تحقيق التوازن بين الخصوصية والأمن السيبراني تجاوز الطرح النظري العام إلى تبني مقاربة قانونية تطبيقية تقوم على معايير واضحة وآليات محددة قابلة للتنفيذ.

ويُعد مبدأ التناسب حجر الزاوية في هذا الإطار، إذ يقتضي أن يكون تدخل سلطات إنفاذ القانون في البيانات الرقمية مقصورًا على القدر الضروري لتحقيق الهدف الأمني، دون إفراط أو مساس غير مبرر بالحقوق الأساسية، إلى جانب مبدأ المشروعية الذي يفرض أن تستند جميع إجراءات المراقبة وجمع الأدلة الرقمية إلى أساس قانوني صريح ومحدد.

كما يتحقق هذا التوازن عمليًا من خلال ربط الحقوق بضوابط إجرائية مقابلة، بحيث يُقيد المساس بالخصوصية الرقمية بضرورة الحصول على إذن قضائي مسبق محدد النطاق والمدة، مع الالتزام بعدم الاحتفاظ بالبيانات إلا بقدر ما تقتضيه ضرورات التحقيق.

ويعزز ذلك اعتماد منظومة رقابية فعالة تشمل الرقابة القضائية المسبقة واللاحقة، وإقرار مبدأ المساءلة عن إساءة استخدام البيانات، وتمكين الأفراد من الطعن في مشروعية الإجراءات التي تمس حقوقهم، بما يضمن عدم تغوّل الاعتبارات الأمنية على حساب الحريات الأساسية.

وعلى هذا الأساس، يتجسد التوازن في إطار مؤسسي متكامل يقوم على تقنين دقيق للسلطات، وضمانات إجرائية صارمة، ورقابة فعالة تكفل تحقيق الحماية الأمنية دون الإخلال بجوهر الحق في الخصوصية.

وتُعد قضية Big Brother Watch وآخرون ضد المملكة المتحدة (2021) من أبرز الأحكام الصادرة عن المحكمة الأوروبية لحقوق الإنسان في مجال التوازن بين متطلبات الأمن القومي وحماية الخصوصية الرقمية، حيث تناولت المحكمة مشروعية أنظمة المراقبة الجماعية للاتصالات التي تعتمدها الدولة في إطار مكافحة التهديدات الأمنية.

وقد انصب النزاع على مدى توافق هذه الأنظمة مع أحكام المادة (8) من الاتفاقية الأوروبية لحقوق الإنسان، التي تكفل الحق في احترام الحياة الخاصة وسرية المراسلات.

وقد أقرت المحكمة، من حيث المبدأ، بأن اللجوء إلى المراقبة الجماعية لا يُعد في ذاته مخالفًا للاتفاقية، نظرًا لاعتبارات تتعلق بحماية الأمن القومي ومواجهة الجرائم الخطيرة، إلا أنها شددت على أن مشروعية هذه الممارسات تظل رهينة بتوافر ضمانات قانونية صارمة تحول دون التعسف أو إساءة الاستخدام.

وفي هذا السياق، أرست المحكمة مجموعة من المعايير الجوهرية، في مقدمتها ضرورة وجود أساس قانوني واضح ودقيق ينظم إجراءات المراقبة، ووجوب خضوع هذه الإجراءات لرقابة مستقلة وفعالة، سواء كانت قضائية أو شبه قضائية.

كما أكدت المحكمة على أهمية احترام مبدأ التناسب، بحيث لا تتجاوز إجراءات المراقبة الحد اللازم لتحقيق الهدف المشروع، مع ضرورة تقييد نطاق جمع البيانات واستخدامها، وضمان عدم الاحتفاظ بها لفترات غير مبررة. وأشارت كذلك إلى أهمية توفير ضمانات إجرائية تتعلق بعملية اختيار البيانات وتحليلها، بما يمنع الاستهداف العشوائي أو غير المبرر للأفراد.

وانتهت المحكمة إلى وجود انتهاك في بعض جوانب النظام البريطاني، خاصة فيما يتعلق بضعف الضمانات المرتبطة بعملية اختيار البيانات واعتراض الاتصالات، وهو ما يعكس توجهًا قضائيًا واضحًا نحو تقنين المراقبة الرقمية بدلًا من حظرها، من خلال إخضاعها لمجموعة من القيود والضوابط التي تضمن تحقيق التوازن بين متطلبات الأمن السيبراني وحماية الحقوق الأساسية.

ويُبرز هذا الحكم بجلاء أن التوازن بين الخصوصية والأمن لا يتحقق عبر تغليب أحدهما على الآخر، وإنما من خلال بناء إطار قانوني دقيق يقوم على المشروعية، والتناسب، والرقابة الفعالة، وهو ما يشكل مرجعًا مهمًا لكل من القاضي والمشرّع في تنظيم الممارسات المرتبطة بالمراقبة الرقمية (European Court of Human Rights, 2021).

المطلب الثالث: الإجراءات القانونية والسياسات التشريعية الحديثة لمواجهة الجريمة الإلكترونية

الأطر القانونية الوطنية والدولية المنظمة للجريمة الإلكترونية

أدركت التشريعات الحديثة، على المستويين الدولي والوطني، خطورة الجريمة الإلكترونية وما تمثله من تهديد

متصاعد للأمن السيبراني والخصوصية الرقمية، فضلًا عن آثارها الممتدة على الاستقرار الاقتصادي والاجتماعي والثقة في البيئة الرقمية.

وقد دفع هذا الإدراك المجتمع الدولي إلى تطوير أطر قانونية مشتركة تهدف إلى توحيد المفاهيم الأساسية المتعلقة بالجريمة المعلوماتية، وتنسيق الجهود التشريعية، وتعزيز التعاون القضائي العابر للحدود، بما يتناسب مع الطبيعة اللامادية واللامحدودة جغرافيًا للفضاء السيبراني (Clough, 2015, p. 97).

وتُعد اتفاقية بودابست لمكافحة الجريمة الإلكترونية الصادرة عن مجلس أوروبا النموذج الأبرز في هذا السياق، إذ تمثل أول صك دولي ملزم يعالج الجريمة المعلوماتية بشكل شامل، حيث وضعت تعريفات قانونية دقيقة للجرائم الإلكترونية، وحددت صورها الأساسية، مثل الدخول غير المشروع إلى الأنظمة المعلوماتية، واعتراض البيانات، وإساءة استخدام الأجهزة الرقمية.

كما أقرت الاتفاقية آليات متقدمة للتعاون الدولي، تشمل المساعدة القانونية المتبادلة، وتبادل المعلومات، وتسليم المجرمين، وجمع الأدلة الإلكترونية وحفظها بشكل عاجل، بما ينسجم مع الطبيعة العابرة للحدود للفضاء السيبراني، ويعزز من فعالية الملاحقة الجنائية في البيئة الرقمية (Council of Europe, 2001).

كما ساهمت هذه الاتفاقية في ترسيخ مبدأ أساسي في القانون الجنائي الرقمي، مفاده أن مكافحة الجريمة الإلكترونية لا يمكن أن تكون فعالة في إطار وطني منفرد، بل تتطلب تنسيقًا دوليًا مستمرًا، نظرًا لتعدد الولايات القضائية وتداخل البنى التحتية الرقمية بين الدول، وهو ما يجعل من التعاون القضائي الدولي عنصرًا جوهريًا في مواجهة هذا النوع من الجرائم.

وعلى الصعيد الوطني، اتجهت العديد من الدول إلى سن تشريعات خاصة بمكافحة الجرائم الإلكترونية وحماية البيانات الشخصية، استجابة للتطور المتسارع في أساليب ارتكاب الجرائم الرقمية، وما ترتب عليها من مخاطر تمس أمن الأفراد والمؤسسات.

وقد تضمنت هذه التشريعات تنظيم الأفعال المجرمة، مثل الاختراق غير المشروع، والاحتيال الإلكتروني، وانتهاك الخصوصية، ونشر البرمجيات الخبيثة، إلى جانب تحديد العقوبات الجنائية المناسبة التي تتدرج وفقًا لجسامة الفعل ونتائجه (Brenner, 2010, p. 70).

وفي الوقت ذاته، لم تقتصر هذه التشريعات على الجانب الجنائي، بل امتدت لتشمل الجانب المدني، من خلال إقرار قواعد للمسؤولية المدنية تتيح تعويض المتضررين عن الأضرار المادية والمعنوية الناشئة عن الاعتداءات الرقمية، سواء كانت ناتجة عن فعل مباشر أو عن إهمال في تأمين الأنظمة المعلوماتية أو معالجة البيانات.

وقد أسهم هذا التطور في توسيع نطاق المسؤولية ليشمل أيضًا الأشخاص الاعتباريين، مثل الشركات ومقدمي خدمات الإنترنت ومطوري البرمجيات، متى ثبت إخلالهم بواجبات الحيطة والحذر.

كما عكست هذه التشريعات تحولًا جوهريًا في النظرة القانونية إلى الجرائم الإلكترونية، حيث لم تعد تُعامل باعتبارها مجرد أفعال تقنية معزولة أو مخالفات عابرة في الفضاء الرقمي، بل أصبحت تُصنف كاعتداءات قانونية خطيرة تمس حقوقًا أساسية، وعلى رأسها الحق في الخصوصية، وحماية البيانات الشخصية، وأمن المعلومات. وقد أدى هذا التحول إلى إعادة صياغة العديد من المفاهيم القانونية التقليدية، مثل الخطأ والضرر والعلاقة السببية، بما يتلاءم مع خصوصية البيئة الرقمية وتعقيداتها التقنية (Solove, 2008, p. 89).

يعكس التطور التشريعي في هذا المجال توجهًا عالميًا نحو مقاربات أكثر شمولًا ومرونة، تجمع بين الحماية الجنائية من جهة والضمانات المدنية والإدارية من جهة أخرى، بما يحقق التوازن بين مواجهة الجريمة الإلكترونية وحماية الحقوق والحريات.

كما تبرز أهمية مواءمة التشريعات الوطنية مع المعايير الدولية، في ظل التفاوت بين الأنظمة القانونية، بما يستلزم تعزيز التعاون وتبادل الخبرات القانونية والتقنية.

وبذلك، لم يعد تنظيم الجريمة الإلكترونية مجرد استجابة مؤقتة للتطور التكنولوجي، بل تحول إلى مسار قانوني متكامل يعكس تطورًا في فلسفة القانون نحو حماية شاملة للفضاء الرقمي وضمان توازن فعال بين الأمن والحقوق.

السياسات التشريعية والإجراءات العملية لتعزيز الحماية الرقمية

إلى جانب الأطر القانونية التقليدية القائمة على التجريم والعقاب، برزت سياسات تشريعية حديثة أكثر تطورًا تهدف إلى تدعيم الحماية القانونية في مواجهة المخاطر السيبرانية المتزايدة، وذلك من خلال تبني مقاربات وقائية وتعويضية وإدارية تتجاوز منطق الردع الجنائي وحده، نحو بناء منظومة متكاملة لإدارة المخاطر الرقمية والحد من آثارها قبل وقوعها وبعده.

ويعكس هذا التحول تطورًا في فلسفة القانون المعاصر، من قانون "لاحق على الضرر" إلى قانون "استباقي وقائي" يسعى إلى تقليل احتمالات وقوع الاعتداءات الرقمية منذ البداية.

ومن أبرز هذه السياسات فرض التأمين الرقمي الإلزامي على المؤسسات والشركات التي تعتمد على معالجة البيانات أو

تشغيل الأنظمة الرقمية، خاصة تلك التي تتعامل مع كميات ضخمة من البيانات الشخصية أو تقدم خدمات حساسة عبر الإنترنت.

ويهدف هذا النوع من التأمين إلى ضمان وجود غطاء مالي مسبق لتعويض الضحايا عن الخسائر الناجمة عن الهجمات السيبرانية أو اختراق البيانات أو الإهمال في تأمين الأنظمة، بما يخفف العبء عن الضحايا ويقلل من الحاجة إلى الدخول في نزاعات قضائية طويلة ومعقدة لإثبات المسؤولية وتحديد نطاق التعويض (European Union, 2016).

كما يُسهم هذا النظام في دفع المؤسسات إلى رفع مستوى الأمن السيبراني لديها، نظرًا لارتباط قيمة التأمين بدرجة التزامها بمعايير الحماية التقنية.

وفي السياق ذاته، اتجه الفقه الحديث إلى اقتراح إنشاء صناديق ضمان رقمي (Cyber Compensation Funds) تُمول من مساهمات الشركات التكنولوجية الكبرى ومقدمي الخدمات الرقمية، وتُخصص لتعويض المتضررين في الحالات التي يتعذر فيها تحديد الطرف المسؤول عن الضرر، أو عندما يكون الفاعل مجهول الهوية أو خارج نطاق الولاية القضائية الوطنية.

وتُعد هذه الآلية ذات أهمية خاصة في ظل الطبيعة المعقدة للهجمات السيبرانية، التي غالبًا ما تتداخل فيها عدة أطراف وتقنيات، مما يجعل إسناد الضرر إلى شخص محدد أمرًا بالغ الصعوبة (Pasquale, 2015, p. 193).

كما أن هذه الصناديق تُجسد تحولًا نحو مفهوم "التضامن الرقمي"، حيث تتحمل المنظومة التكنولوجية بأكملها جزءًا من عبء المخاطر الناتجة عن استخدامها، بدلًا من ترك الضحايا دون تعويض في الحالات التي يتعذر فيها تطبيق القواعد التقليدية للمسؤولية المدنية.

وهو ما يعزز الثقة في البيئة الرقمية، ويشجع على الاستخدام الآمن للتقنيات الحديثة دون خوف من فقدان الحماية القانونية.

ولا يقل عن ذلك أهمية تعزيز التعاون الدولي في مجال مكافحة الجريمة الإلكترونية، من خلال تبادل المعلومات والخبرات التقنية، وتنسيق الجهود الأمنية والقضائية بين الدول، بما يسمح بتتبع المجرمين الرقميين وملاحقتهم قضائيًا، ويحد من ظاهرة الإفلات من العقاب التي تستفيد منها الجرائم العابرة للحدود.

وقد أصبحت آليات التعاون الدولي اليوم تشمل إنشاء فرق استجابة سريعة للحوادث السيبرانية (CERTs)، وتفعيل اتفاقيات المساعدة القانونية المتبادلة، وتطوير منصات مشتركة لتبادل الأدلة الرقمية بشكل آمن وسريع (Council of Europe, 2001).

فرض تطور الجرائم الإلكترونية ضرورة تحديث التشريعات الوطنية عبر سن قوانين متخصصة في الأمن السيبراني وحماية البيانات، وإنشاء جهات قضائية وأمنية متخصصة، إلى جانب تأهيل الكوادر القانونية للتعامل مع الأدلة الرقمية بكفاءة.

كما اتجهت التشريعات الحديثة من المنهج العقابي التقليدي إلى نهج وقائي يركز على إدارة المخاطر وتعزيز الجاهزية الرقمية للمؤسسات، من خلال إلزامها بمعايير الأمن السيبراني، وإجراء اختبارات اختراق دورية، ووضع خطط للاستجابة للطوارئ.

ويعكس ذلك تحولًا نحو اعتبار حماية الفضاء الرقمي مسؤولية تشاركية بين الدولة والقطاع الخاص ومقدمي الخدمات والمجتمع الدولي، بما يستلزم تبني مقاربة قانونية مرنة توازن بين دعم الابتكار وحماية الحقوق والحريات.

تقييم السياسات التشريعية وأثرها على حماية الخصوصية والأمن السيبراني

يُظهر التحليل القانوني المقارن أن فعالية مواجهة الجريمة الإلكترونية لا تتحقق من خلال مجرد سن نصوص قانونية تقليدية أو الاكتفاء بتجريم الأفعال الرقمية، بل تتطلب تبني سياسات تشريعية متكاملة وشاملة تقوم على رؤية استراتيجية لإدارة المخاطر السيبرانية.

ويشمل هذا التكامل تحديدًا واضحًا ودقيقًا لنطاق المسؤولية القانونية لمختلف الفاعلين في البيئة الرقمية، سواء كانوا أفرادًا أو جهات اعتبارية أو مزودي خدمات تقنية، إلى جانب تعزيز الرقابة القضائية الفعالة على الإجراءات الرقمية التي تمس الحقوق والحريات، وضمان خضوعها الدائم لمبادئ المشروعية والضرورة والتناسب (Clough, 2015, p. 97).

كما تبرز أهمية توفير آليات تعويض فعالة وسريعة للضحايا، باعتبار أن طول وتعقيد الإجراءات القضائية التقليدية قد لا يتناسب مع طبيعة الأضرار الناجمة عن الجرائم الإلكترونية، والتي غالبًا ما تكون فورية، واسعة النطاق، وصعبة التتبع.

ومن ثم، فإن تطوير أدوات بديلة للتعويض، مثل صناديق الضمان الرقمي أو نظم التأمين السيبراني، يُعد عنصرًا أساسيًا في تحقيق العدالة الرقمية، حيث يضمن جبر الضرر حتى في الحالات التي يتعذر فيها تحديد الجاني أو الوصول إليه.

ويؤدي هذا التكامل بين التجريم والوقاية والتعويض إلى تحقيق توازن أكثر واقعية بين حماية الخصوصية الرقمية من جهة، ومتطلبات الأمن السيبراني من جهة أخرى، وهو توازن دقيق يتطلب إدارة قانونية مرنة قادرة على التكيف مع التطورات التقنية المتسارعة.

فالإفراط في حماية الخصوصية قد يؤدي إلى إضعاف قدرة الدولة على مواجهة التهديدات السيبرانية، بينما التوسع غير المنضبط في إجراءات المراقبة قد يفضي إلى انتهاك الحقوق الأساسية للأفراد وتقويض الثقة في الفضاء الرقمي (Solove, 2008, p. 91).

يرتبط نجاح السياسات التشريعية في هذا المجال بقدرة المشرّع على مواكبة التطور التقني المستمر وتحديث الأطر القانونية بشكل دوري لمواجهة صور الجريمة المستحدثة، خاصة تلك المعتمدة على الذكاء الاصطناعي وتحليل البيانات الضخمة وتقنيات إخفاء الهوية.

كما يستلزم الأمر إدماج الخبرة التقنية في عملية التشريع لضمان ملاءمة النصوص القانونية للواقع الرقمي، ويعكس ذلك أن تنظيم الجريمة الإلكترونية لم يعد تطبيقًا تقليديًا لقواعد المسؤولية، بل إعادة صياغة لفلسفة قانونية جديدة تتناسب مع طبيعة الفضاء الرقمي، بما يتميز به من طابع عابر للحدود وتعدد الأطراف وسرعة التطور وصعوبة الإثبات، وهو ما يحد من كفاية القواعد التقليدية في مواجهتها. (Brenner, 2010, p. 71).

توضح الدراسة أن القوانين التقليدية، القائمة على الإقليمية والثبات في تحديد الزمان والمكان والفاعل، لم تعد كافية لمواجهة تعقيدات الجرائم الرقمية العابرة للحدود، مما يستلزم تطوير أطر تشريعية أكثر مرونة وشمولًا.

ويشمل ذلك تبني سياسات وقائية قائمة على إدارة المخاطر، وتطوير أدوات تقنية للكشف المبكر عن الجرائم، إلى جانب تعزيز نظم الإثبات الرقمي لضمان حجية الأدلة أمام القضاء.

كما يتطلب تحقيق العدالة الرقمية تعزيز التعاون الدولي وتوحيد المعايير القانونية والإجرائية بين الدول، بما يمنع تحول الفضاء السيبراني إلى بيئة للإفلات من العقاب، ويبرز في هذا السياق دور اتفاقية بودابست في وضع أسس التعاون وتبادل المعلومات في مجال الجرائم الإلكترونية. (Council of Europe, 2001).

يمكن القول إن مستقبل الحماية القانونية في البيئة الرقمية يعتمد على قدرة الأنظمة التشريعية على تحقيق توازن دقيق بين ثلاثية أساسية، تتمثل في: حماية الخصوصية الرقمية، وضمان الأمن السيبراني، وتعزيز الابتكار التكنولوجي.

وهو توازن لا يمكن تحقيقه إلا من خلال مقاربة قانونية مرنة، متعددة المستويات، تجمع بين التشريع، والقضاء، والتقنية، والتعاون الدولي، بما يضمن بناء منظومة قانونية متكاملة قادرة على مواجهة تحديات العصر الرقمي وتحقيق العدالة في صورتها الحديثة.

النتائج

خلصت الدراسة إلى أن الجريمة الإلكترونية تمثل أحد أبرز التحديات القانونية في العصر الرقمي، نظرًا لطبيعتها المعقدة وعابرة الحدود، وما تثيره من إشكالات تتعلق بضعف كفاية القواعد التقليدية في التجريم والإثبات وتحديد المسؤولية، كما أبرزت الدراسة أن التحول الرقمي فرض إعادة صياغة العلاقة بين حماية الخصوصية ومتطلبات الأمن السيبراني في إطار قانوني متوازن.

توصل البحث إلى مجموعة من النتائج، أهمها:

1. قصور المنظومة الجنائية التقليدية: أظهرت الدراسة أن خصائص الجريمة الإلكترونية، مثل عدم المادية والعالمية والديناميكية، جعلت القواعد الجنائية التقليدية غير قادرة على مواكبتها، مما يستلزم تطوير فلسفة التجريم وآليات الملاحقة.
2. تحول مفهوم الخصوصية الرقمية: تطور مفهوم الخصوصية من مجرد حماية الحياة الخاصة إلى حق في التحكم بالبيانات الشخصية، بما يفرض تعزيز الضمانات القانونية والتقنية لحماية هذا الحق.
3. الفجوة التشريعية العربية: تعاني العديد من التشريعات العربية من عمومية النصوص وضعف تحديد أركان الجريمة الإلكترونية، مما يضعف فعالية الردع وصعوبة مواجهة الجرائم المستحدثة.
4. التوازن بين الأمن السيبراني والحقوق: رغم أهمية تدابير الأمن السيبراني، إلا أن غياب الضوابط قد يؤدي إلى انتهاك الخصوصية، مما يستوجب الالتزام بمبادئ المشروعية والضرورة والتناسب مع رقابة قضائية فعالة.
5. إشكالية الإثبات الرقمي: تواجه الأدلة الرقمية تحديات تتعلق بالحجية وسهولة التلاعب، مما يتطلب تطوير قواعد إثبات متخصصة تضمن سلامة الدليل دون الإخلال بضمانات المحاكمة العادلة.

ويوصي البحث بما يلي:

1. التشريع المتكامل والحوكمة الرقمية: تطوير تشريعات مرنة ومتخصصة لمواجهة الجرائم الإلكترونية، مع تفعيل قانون حماية البيانات رقم 151 لسنة 2020 (مصر، 2020) بما يتوافق مع المعايير الدولية مثل GDPR.
2. حماية الخصوصية وضبط المراقبة: تعزيز حقوق الأفراد في البيانات مع إخضاع إجراءات المراقبة والأمن السيبراني لرقابة قضائية صارمة وفق مبدأي الضرورة والتناسب.
3. تطوير المسؤولية القانونية: إعادة تنظيم قواعد المسؤولية لتشمل المنصات الرقمية ومزودي الخدمات، وتبني نماذج

مسؤولية تتناسب مع التعقيد التقني مع إلزامهم بالتعاون في مكافحة المحتوى الإجرامي.

4. تحديث الإثبات والتأهيل الفني: وضع قواعد خاصة لحجية الأدلة الرقمية وضمان سلامة تداولها، مع تدريب القضاة وأعضاء النيابة على التعامل مع الدليل الإلكتروني.
5. تعزيز التعاون الدولي: توسيع التعاون القضائي والأمني عبر الاتفاقيات الدولية وتبادل المعلومات والأدلة بما يحد من الإفلات من العقاب في الفضاء السيبراني.
6. دعم البحث العلمي: تشجيع الدراسات البينية بين القانون والتكنولوجيا لتطوير سياسات تشريعية استباقية تواكب التطور الرقمي.

بيان الافصاح

- **الموافقة الأخلاقية والموافقة على المشاركة:** لا ينطبق. لم يتم إجراء تجارب على أشخاص أو جمع بيانات شخصية تتطلب موافقة أخلاقية أو موافقة المشاركين.
- **توافر البيانات والمواد:** لا تحتوي هذه الدراسة على بيانات أولية أو مواد قابلة للمشاركة، إذ تعتمد على تحليل نصوص قانونية ومصادر نظرية منشورة ومتاحة للجمهور.
- **مساهمة المؤلفين:** أعد المؤلف هذه الدراسة بالكامل، من حيث تحديد الفكرة، وجمع المصادر، وتحليلها، وصياغة النص النهائي، دون مشاركة من مؤلفين آخرين.
- **تضارب المصالح:** يصرّح المؤلف بأنه لا يوجد أي تضارب مصالح يؤثر على موضوع هذه الدراسة.
- **التمويل:** لم يتلق المؤلف أي تمويل مالي أو دعم مادي لإعداد هذا البحث.
- **مصدر البحث:** هذا البحث مستقل غير مستل من أي رسالة علمية.
- **الشكر:** يشكر المؤلف هيئة تحرير المجلة على جهودها في دعم البحث العلمي ونشره. (www.najah.edu)

Open Access

المراجع

- مصر. (2018). قانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات [Law No. 175 of 2018 on Anti-Cyber and Information Technology Crimes]. https://www.wipo.int/wipolex/ar/legislation/details/19959
- مصر. (2020). قانون رقم 151 لسنة 2020 بشأن حماية البيانات الشخصية [Law No. 151 of 2020 on Personal Data Protection]. https://mcit.gov.eg/Upcont/Documents/Reports%20and%20Documents_1232021000_Law_No_151_2020_Personal_Data_Protection.pdf

References

- Austin, S., Douglas, L., & Umphrey, M. M. (2012). *Imagining new legalities: Privacy and its possibilities in the 21st century*. Stanford University Press. https://doi.org/10.11126/stanford/9780804777049.001.0001
- Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. Praeger. https://archive.org/details/cybercrimecrimin2010bren
- Clough, J. (2015). *Principles of cybercrime*. Cambridge University Press. https://www.cambridge.org/core/books/principles-of-cybercrime/F172001ECA8742B5C3E0678CDF977718
- Council of Europe. (2001). Convention on cybercrime (Budapest Convention), Council of Europe Publishing.

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

– European Court of Human Rights. 2021. ANNUAL REPORT. https://www.echr.coe.int/documents/d/echr/Annual_report_2021_ENG

– European Union. (2016). General Data Protection Regulation (GDPR). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj

– Kuner, C. (2013). *Transborder data flows and data privacy law*. Oxford University Press. https://academic.oup.com/book/5440

– Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press. https://www.jstor.org/stable/j.ctt13x0hch

– Sheward, M. (2018). Cybercrime: Remember the People (Not Just the Data). *ITNOW*, *60*(4), 36–37. https://doi.org/10.1093/itnow/bwy099

– Solove, D. J. (2008). *Understanding privacy*. Harvard University Press. https://www.danielsolove.com/understanding-privacy/

– Soyer, B., & Tettenborn, A. (2023). Artificial intelligence and civil liability—Do we need a new regime? *International Journal of Law and Information Technology*, *30*(4), 385–397. https://doi.org/10.1093/ijlit/eaad001