Journal of Libyan Academy Bani Walid 2026
مجلة الأكاديمية الليبية بني وليد
e-ISSN: 3104-3860
Volume 2, Issue 2, 2026, Pages: 66-83
Website: https://journals.labjournal.ly/index.php/Jlabw/index

The Legal Structure of Cybercrime: A Comparative Study Between Libyan Law No. (5) of 2022 and Egyptian Law No. (175) of 2018

Tarek Ammar Karkub *
Department of Criminal Law, Faculty of Law, Al-Jafara University, Libya
*Email: karkoubtarek28@gmail.com

البنيان القانوني لجرائم تقنية المعلومات: دراسة مقارنة بين القانون الليبي رقم (5) لسنة 2022م والقانون المصري رقم (175) لسنة 2018م

طارق عمار محمد كركوب *
القسم الجنائي، كلية القانون، جامعة الجفارة، ليبيا

Received: 10-01-2026	**Accepted:** 28-02-2026	**Published**: 15-03-2026

Abstract

This research examines cybercrime through a comparative analytical study between Libyan Law No. (5) of 2022 on Combating Electronic Crimes and Egyptian Law No. (175) of 2018 on Combating Information Technology Crimes. The study analyzes the legal structure of cybercrime in light of the general theory of crime, focusing on its legal, material, and moral elements. It explores the scope of criminalization, the protected legal interests, penal policy, and procedural regulation of digital evidence strictly according to the provisions of both laws. The research adopts analytical and comparative methodologies to identify similarities and differences between the two legislations. It concludes that both laws adhere to the traditional criminal framework while differing in the degree of legislative detail, particularly regarding service providers' obligations and technical measures.

Keywords: Cybercrime, Information Technology Crimes, Legal Structure of Crime, Digital Evidence, Criminal Policy, Criminal Liability, Comparative Legislation.

الملخص

يتناول هذا البحث جريمة تقنية المعلومات في إطار دراسة تحليلية مقارنة بين القانون الليبي رقم (5) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية، والقانون المصري رقم (175) لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات. ويهدف إلى بيان مدى اتساق البنيان القانوني المعتمد في كلا التشريعين مع أحكام

النظرية العامة للجريمة، وتحليل نطاق التجريم، ومحل الحماية الجنائية، والسياسة العقابية، والتنظيم الإجرائي للأدلة الرقمية، كما يعالج البحث الخصائص القانونية للجريمة الإلكترونية، ويقف على أركانها الثلاثة: الشرعي والمادي والمعنوي، في ضوء نصوص القانونين دون تجاوز لما ورد فيهما. وقد اعتمدت الدراسة على المنهج التحليلي في تفسير النصوص، والمنهج المقارن في بيان أوجه الاتفاق والاختلاف، وصولًا إلى تقييم علمي للبنية التشريعية في كلا النظامين. وانتهت الدراسة إلى أن كلا التشريعين يلتزمان بالإطار التقليدي للنظرية العامة للجريمة، مع تفاوت في درجة التفصيل والتنظيم، خاصة في مجال مسؤولية مقدمي الخدمة والتدابير التقنية.

الكلمات المفتاحية: جرائم تقنية المعلومات، الجرائم الإلكترونية، البنيان القانوني للجريمة، الأدلة الرقمية، السياسة الجنائية، المسؤولية الجنائية، التشريع المقارن.

مقدمة

شهد العالم خلال العقود الأخيرة تحولًا عميقًا في طبيعة النشاط الإنساني نتيجة الثورة الرقمية المتسارعة، حيث أصبحت تقنيات المعلومات والاتصال تمثل البنية التحتية الأساسية لإدارة مؤسسات الدولة، وتنظيم المعاملات الاقتصادية، وتسيير العلاقات الاجتماعية. ولم يعد الفضاء الرقمي مجرد وسيلة مساعدة، بل تحول إلى بيئة قائمة بذاتها تمارس فيها الأنشطة المختلفة، وتنتقل عبرها البيانات بسرعة تفوق الحدود الجغرافية والسيادية.

غير أن هذا التطور لم يكن بمعزل عن مظاهر الانحراف الإجرامي، إذ ظهرت أنماط جديدة من الجرائم اتخذت من الأنظمة المعلوماتية والبيانات الرقمية محلًا مباشرًا للاعتداء. وأصبح بالإمكان ارتكاب أفعال خطيرة دون استعمال القوة المادية، بل من خلال الدخول غير المشروع إلى منظومة معلوماتية، أو اعتراض بيانات، أو نشر محتوى إلكتروني ضار.

وقد كشف هذا الواقع عن قصور النصوص العقابية التقليدية عن استيعاب هذه الأفعال المستحدثة، الأمر الذي استدعى تدخلًا تشريعيًا خاصًا. وفي هذا السياق صدر في مصر القانون رقم (175) لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، كما صدر في ليبيا القانون رقم (5) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية.

وتسعى هذه الدراسة إلى تحليل جريمة تقنية المعلومات في ضوء النظرية العامة للجريمة، ثم بيان البنيان القانوني الذي اعتمده كل من المشرعين الليبي والمصري، وقياس مدى اتساقه مع المبادئ الجنائية العامة، ومدى كفايته في تحقيق الحماية القانونية للبيئة الرقمية.

أهمية الدراسة

تنبع أهمية هذه الدراسة من عدة اعتبارات:

أولًا: الأهمية النظرية

إذ تسهم في تأصيل المفهوم القانوني للجريمة الإلكترونية، وإخضاعها لأحكام النظرية العامة للجريمة، بما يعزز وضوح البناء المفاهيمي.

ثانيًا: الأهمية التشريعية

نظرًا لحداثة القانون الليبي رقم (5) لسنة 2022، فإن تقييم بنيانه القانوني في ضوء التجربة المصرية يمثل إسهامًا في تطوير السياسة التشريعية.

ثالثًا: الأهمية العملية

لأن الجرائم الرقمية تثير صعوبات إثباتية وإجرائية تتطلب تنظيمًا دقيقًا، خاصة فيما يتعلق بالأدلة الرقمية.

رابعًا: الأهمية المقارنة

إذ تكشف المقارنة عن أوجه القوة والقصور في كل من التشريعين.

إشكالية الدراسة

تتمحور الإشكالية الرئيسة حول:

مدى نجاح القانون الليبي رقم (5) لسنة 2022م, والقانون المصري رقم (175) لسنة 2018م في بناء تنظيم قانوني متكامل لجريمة تقنية المعلومات، يراعي خصوصيتها التقنية، ويتسق مع أحكام النظرية العامة للجريمة.

ويتفرع عن ذلك التساؤلات الآتية:

- هل استوعب التشريعان الأركان التقليدية للجريمة في البيئة الرقمية؟
- ما مدى دقة تحديد السلوك الإجرامي؟
- هل السياسة العقابية ملائمة لطبيعة الاعتداء الرقمي؟
- كيف نظم كل قانون مسؤولية مقدمي الخدمة؟

أهداف الدراسة

تهدف هذه الدراسة إلى تحقيق جملة من الأهداف العلمية والمنهجية، يمكن إجمالها فيما يأتي:

1- بيان المفهوم القانوني لجريمة تقنية المعلومات في ضوء نصوص القانون الليبي رقم (5) لسنة 2022 والقانون المصري رقم (175) لسنة 2018، واستخلاص عناصرها الأساسية.

2- تحليل الجريمة الإلكترونية في إطار النظرية العامة للجريمة، من خلال دراسة الركن الشرعي والمادي والمعنوي، وبيان مدى انطباقها على الجرائم المعلوماتية.

3- تحديد نطاق التجريم ومحل الحماية الجنائية في كلا القانونين، وبيان المصالح التي قصد المشرع صونها في البيئة الرقمية.

4- دراسة السياسة العقابية والتنظيم الإجرائي المعتمدين، وتقييم مدى ملاءمتهما لطبيعة الجرائم المعلوماتية.

5- إجراء مقارنة تحليلية بين التشريعين الليبي والمصري، لاستخلاص أوجه الاتفاق والاختلاف والوصول إلى نتائج علمية مدعمة بالتوصيات

منهج الدراسة

اعتمدت هذه الدراسة على المنهج التحليلي في تفسير نصوص القانون الليبي رقم (5) لسنة 2022م, والقانون المصري رقم (175) لسنة 2018م ، وذلك من خلال تفكيك الأحكام القانونية وبيان عناصرها وأركانها والكشف عن مدلولها في إطار القواعد العامة للقانون الجنائي. كما استندت إلى المنهج المقارن لبيان أوجه الاتفاق والاختلاف بين التشريعين من حيث نطاق التجريم ومحل الحماية والسياسة العقابية والتنظيم الإجرائي، وإلى جانب ذلك، تم توظيف المنهج النقدي عند تقييم مدى كفاية النصوص وملاءمتها لطبيعة الجرائم المعلوماتية، وصولًا إلى نتائج علمية وتوصيات عملية في ضوء التحليل الموضوعي للنصوص محل الدراسة.

خطة البحث

ينقسم البحث إلى أربعة مباحث:

المبحث الأول: التأصيل النظري لجريمة تقنية المعلومات.

المبحث الثاني: نطاق التجريم ومحل الحماية في القانونين.

المبحث الثالث: السياسة العقابية والتنظيم الإجرائي.

المبحث الأول

التأصيل النظري لجريمة تقنية المعلومات

تمثل النظرية العامة للجريمة الإطار الذي تُبنى عليه المسؤولية الجنائية، وتقوم على ثلاثة أركان أساسية: الركن الشرعي، والركن المادي، والركن المعنوي. ولا يمكن فهم جريمة تقنية المعلومات بمعزل عن هذا الإطار، مهما بلغت خصوصيتها التقنية.

ومن ثم، يقتضي التحليل إخضاع الجرائم المنصوص عليها في القانونين الليبي والمصري لأحكام هذه النظرية، وبيان مدى انطباقها عليها.

المطلب الأول :- مفهوم جريمة تقنية المعلومات وخصائصها

قبل الولوج إلى تحليل الأركان القانونية لجريمة تقنية المعلومات، يقتضي المنهج العلمي الوقوف أولًا على تحديد مفهومها وضبط خصائصها المميزة. فالتحديد المفاهيمي ليس ترفًا نظريًا، بل يمثل الأساس الذي يُبنى عليه التكييف القانوني السليم، إذ لا يمكن إخضاع فعلٍ ما لأحكام النظرية العامة للجريمة دون بيان طبيعته القانونية ومحل الحماية الذي ينصرف إليه.

وقد أفرز التحول الرقمي واقعًا جديدًا لم يكن معهودًا عند نشأة القواعد التقليدية في قانون العقوبات، حيث أصبح الاعتداء يقع على نظم معلوماتية وبيانات رقمية غير ملموسة، وتتخذ الجريمة فيه وسيلة تقنية قد تُمكِّن الفاعل من التنفيذ عن بُعد، دون احتكاك مادي مباشر بالمجني عليه أو محل الجريمة. ومن هنا برز التساؤل حول ما إذا كانت هذه الجرائم تمثل مجرد تطبيق حديث لصور تقليدية من الاعتداء؟، أم أنها تُمثل نمطًا مستقلًا يستوجب توصيفًا خاصًا؟.

ولم يضع كل من القانون الليبي رقم (5) لسنة 2022 والقانون المصري رقم (175) لسنة 2018 تعريفًا جامعًا مانعًا لجريمة تقنية المعلومات، وإنما عالجاها من خلال تعداد صور السلوك المجرّم. وهو اتجاه تشريعي يقوم على ضبط الأفعال محل التجريم بدلًا من تقديم تعريف نظري قد يضيق أو يتسع عن المراد.

ومن ثم، فإن تحديد مفهوم جريمة تقنية المعلومات في هذه الدراسة سيتم استنباطه من مجموع النصوص الواردة في القانونين، مع تحليل خصائصها القانونية التي تميزها عن الجرائم التقليدية، تمهيدًا لإخضاعها لأحكام الركن الشرعي والمادي والمعنوي في المطالب التالية.

وستتناول الدراسة في هذا المطلب **أولًا** بيان المفهوم القانوني المستفاد من نصوص القانونين، ثم الوقوف على الخصائص الموضوعية التي تميز الجريمة الإلكترونية من حيث طبيعة السلوك، ومحل الاعتداء، والامتداد الزماني والمكاني، وأثر الوسيلة التقنية في تكوين الجريمة.

الفرع الأول: المفهوم في ضوء نصوص القانونين

لم يضع أي من القانونين تعريفًا جامعًا للجريمة الإلكترونية، وإنما حددا صور السلوك المجرم. ومن خلال استقراء النصوص، يتضح أن الجريمة تقوم متى وقع اعتداء غير مشروع على نظام معلوماتي أو بيانات أو حساب إلكتروني باستخدام وسائل تقنية المعلومات.

الفرع الثاني: خصائص جرائم تقنية المعلومات

1. خفاء الجريمة

يقصد بخفاء الجريمة صعوبة اكتشافها لعدم تركها آثارًا مادية مرئية كالموجودة في الجرائم التقليدية كالدماء أو أدوات الجريمة. فهي جريمة ناعمة لا تعتمد على العنف، وإنما على الإلمام بتقنية المعلومات، مما يقلل من عدد الجرائم المكتشفة. وترتكب غالبًا في بيئة المعالجة الآلية للبيانات، حيث يستطيع الجاني تنفيذ فعله في وقت وجيز بفضل خبرته التقنية. كما أن بعض الضحايا، لاسيما المؤسسات المالية، يفضلون عدم الإبلاغ خشية الخسائر أو المساس بالسمعة. وتشير بعض التقارير إلى أن نسبة ضئيلة فقط من هذه

الجرائم يُبلّغ عنها. ويُضاف إلى ذلك أن الإبلاغ يرتبط أحيانًا بحجم المنفعة المتوقعة منه. كما تلعب العوامل النفسية والشخصية دورًا في قرار الإبلاغ من عدمه.

2- غياب الدليل المرئي عليها

من سمات جرائم تقنية المعلومات أيضًا غياب الدليل المرئي عليها؛ نظرًا لأن الدليل في هذه الجرائم ليس ماديًا، فهو عبارة عن نبضات إلكترونية عبر النظام المعلوماتي.

3- صعوبة الوصول إلى الجاني

على سبيل المثال: في جريمة اختراق النظام والحصول على المعلومات أو إتلافها، فإذا كان يمكن معرفة الجهاز (أداة الاختراق) فإنه يصعب معرفة مستخدمه؛ فمن الوارد أن يكون الجاني مستخدمًا حسابًا غير حسابه الشخصي، أو أن يستخدم حاسبًا بأحد الأماكن العامة أو المقاهي (مقاهي الإنترنت).

4. جريمة دولية عابرة للحدود

يُقصد بالجرائم الدولية: هي تلك الجرائم التي تمثل عدوانًا على مصلحة يحميها القانون الدولي الجنائي، باعتبار أن كل المجتمع الدولي متفق على أن هذه الأفعال تشكل جرائم. أما الجرائم العابرة للحدود فهي جرائم داخلية معاقب عليها بموجب القانون الوطني، إلا أنها عابرة للحدود، وتعد جرائم تقنية المعلومات جرائم دولية لا تعرف الحدود بين الدول، ولا تتقيد بالزمان أو المكان، إذ يمكن ارتكاب السلوك الإجرامي في دولة وتتحقق نتيجته في أخرى، مما يثير إشكالية تحديد القانون الواجب التطبيق. ويُعد التعاون الدولي الوسيلة الأنجع لمكافحة هذه الجرائم.

5. تعدد الفاعلين في الجرائم التقنية

تتميز جرائم تقنية المعلومات غالبًا بتعدد الفاعلين فيها، على الأقل شخصان: الأول تكون مهمته الجانب الفني التقني الخاص بالجريمة، والثاني يحصل على العائد من جراء ارتكابها، حال إذا كان المنتفع من الجريمة شخصًا آخر غير مرتكبها.

6- صعوبة إثباتها

من أبرز خصائص جرائم تقنية المعلومات صعوبة إثباتها، لوقوعها في بيئة غير تقليدية تتمثل في النظم المعلوماتية وشبكاتها، وهي بيئة لا كيان مادي ملموس لها. فالأدلة فيها عبارة عن بيانات ونبضات إلكترونية غير مرئية، مما يُصعّب على جهات التحقيق جمعها وتتبعها. كما يسهل على الجاني محو آثار فعله أو إخفاؤها. وتعد وسائل المعاينة التقليدية غير كافية لإثباتها لغياب الآثار المادية المعتادة. وغالبًا ما تُرتكب عن بُعد دون تواجد مادي في مسرح الجريمة. ويُضاف إلى ذلك امتناع بعض المجني عليهم عن الإبلاغ عنها، مما يجعلها ضمن الجرائم ذات الرقم الأسود. كما أن نقص الخبرة الفنية والتقنية لدى رجال الأمن والقضاء يفاقم من صعوبة الإثبات.

7- سرعة التنفيذ

فارتكاب الجرائم التقنية لا يتطلب وقتًا كبيرًا في التنفيذ أو التخطيط؛ إذ تُرتكب هذه الجرائم بضغطة زر واحدة في مكان يتواجد به الوسيلة التقنية المستخدمة في ارتكاب الجريمة، فلا تُكلف مرتكبها أي صعوبات في ارتكابها.

8- جرائم ناعمة

تندرج الجرائم التقنية تحت فئة الجرائم الناعمة التي لا تحتاج إلى العنف في ارتكابها؛ إذ تعتمد على العقل والتفكير والخبرة التقنية خلافًا للجرائم التقليدية التي تتطلب عنفًا في التنفيذ، كاستخدام الأسلحة والضرب... إلخ، إذ تعتبر من الجرائم النظيفة الهادئة التي لا يترتب عليها إراقة الدماء أو أي أثر مادي محسوس وملموس.

9- جرائم منخفضة المخاطر

تُعد الجرائم التقنية (الإلكترونية) من قبيل الجرائم منخفضة المخاطر مقارنة بالجرائم التقليدية؛ إذ يرتكب المجرم التقني جريمته في بيئة افتراضية لا تكلفه الانتقال إلى مسرح فعلي مادي للجريمة، فيرتكب جريمته بوقت ضئيل وهو بمأمن من أي شيء قد يمثل إزعاجًا أو ضغطًا له أثناء ارتكاب جريمته.

وهذه الخصائص تؤثر في تفسير النصوص وتطبيقها.

المطلب الثاني :- الركن الشرعي

يقوم الركن الشرعي على مبدأ الشرعية الجنائية.

وقد نص **القانون المصري** صراحة على تجريم:

1- الدخول غير المشروع إلى موقع أو حساب أو نظام معلوماتي
2- إتلاف أو حذف أو تعديل البيانات
3- الاعتداء على حرمة الحياة الخاصة باستخدام وسائل تقنية المعلومات

كما نص **القانون الليبي** على تجريم:

1- الدخول غير المشروع إلى منظومة معلوماتية
2- اعتراض البيانات
3- الابتزاز الإلكتروني
4- نشر محتوى ضار

ويتضح أن كلا المشرعين التزم بتحديد الأفعال بنصوص صريحة، دون اللجوء إلى القياس.

المطلب الثالث :-الركن المادي

يُقصد بالركن المادي للجريمة بصفة عامة: "الكيان المادي لها"، ويعني آخر: "جسم الجريمة وهيكلها".

كما عرّفه البعض من الفقه بأنه: "المظهر الخارجي الملموس الذي تدركه الحواس، والذي يُحدث تغييراً في العالم الخارجي". إذ إنه: السلوك الإجرامي محل التجريم والعقاب.

فالمبدأ المستقر عليه: أنه لا جريمة بغير سلوك إجرامي يخرج الأفكار والنوايا والرغبات الدفينة إلى العالم المادي الملموس، فالقانون لا يعاقب على النوايا طالما لم يُعبَّر عنها بسلوك يخرجها من طيِّ الكتمان إلى أرض الواقع، وبذلك تتحقق الحماية القانونية لحقوق الأفراد وحرياتهم من التعسف الوارد وقوعه من السلطات العامة.

وقد قضت محكمة النقض المصرية "بأن الإنسان لا يوصف بكونه فاعلاً أو شريكاً إلا عمّا يكون لنشاطه دخل في وقوعه من الأعمال التي نصّ القانون على تجريمها، سواء أكان ذلك بالقيام بفعلٍ ما أم بالامتناع عنه مما يجرّمه القانون".

ويتكون الركن المادي من السلوك والنتيجة وعلاقة السببية.

اما السلوك يتمثل في أفعال إيجابية مثل الدخول أو التعديل أو النشر، وفي بعض الجرائم يكفي مجرد الدخول غير المشروع، مما يجعلها من جرائم الخطر، وفي جرائم أخرى يشترط تحقق نتيجة كتعطيل النظام، وتظل علاقة السببية خاضعة للقواعد العامة في قانون العقوبات، وسوف نتناول عناصر الركن المادي للجريمة بصفة عامة وهي :-

أ. السلوك الإجرامي

يُعدّ السلوك الإجرامي من أهم عناصر الركن المادي للجريمة بصفة عامة، ولجرائم تقنية المعلومات بصفة خاصة؛ إذ إنه يعبّر عن مخالفة الجاني لإرادة المشرّع بشكل مادي ملموس في العالم الخارجي.

ويمكن القول: إن السلوك الإجرامي بصفة عامة هو التجسيد المادي الملموس لما هو دفين بالنفس البشرية من رغبات غير شرعية يرتب القانون عليها العقاب، فهو "فعل أو امتناع عن فعل أمر به القانون وعاقب على مخالفته" ،وقد يتخذ السلوك الإجرامي إحدى صورتين

1- **السلوك الإيجابي**: يتمثل في حركة عضوية إرادية مُجرَّمة ينص القانون بأنها من شأنها إحداث نتيجة معيّنة.

2- **السلوك السلبي**: يُراد به الامتناع عن القيام بفعل معيّن كان يجب القيام به، أو اتخاذ موقف سلبي حيال أمرٍ ما يجب اتخاذ موقف إيجابي به.

والسلوك الإجرامي بجرائم تقنية المعلومات: هو سلوك/ فعل/ نشاط معيّن يأتيه الجاني في الجرائم المعلوماتية، يفترض ضرورة وجود بيئة رقمية واتصال بالإنترنت يطوّع الجاني (المجرم المعلوماتي) علمه وإتقانه لهذه التقنية ويستغله في ارتكاب جريمته المعلوماتية أيًّا كان شكلها؛ كأن يقوم باختراق جهاز معيّن أو بثّ فيروس لجهاز آخر... إلخ، أو إعداد برنامج فيروس تمهيدًا لنشره, ويستهدف السلوك الإجرامي بجرائم تقنية المعلومات المعلومة، سواء أكانت مخزَّنة بحسب الأصل على الحاسب أو التي يتم إدخالها، ويفترض لإتيان هذا السلوك ضرورة توافر قدر كبير من الخبرة التقنية لدى الجاني تؤهله لإتيانه.

2- النتيجة الإجرامية

هي العنصر الثاني للركن المادي للجريمة بصفة عامة، وللجرائم التقنية بصفة خاصة؛ ويُقصد بها الأثر الناجم عن السلوك الإجرامي المرتكب، الذي من شأنه يُمثِّل اعتداءً على مصلحة محمية قانونًا.

3- علاقة السببية

هي تلك العلاقة الرابطة بين العنصر الأول والثاني من عناصر الركن المادي للجريمة بصفة عامة، والجرائم التقنية بصفة خاصة، فنتيجةً لمبدأ شخصية المسؤولية الجنائية يجب وجود علاقة تربط بين السلوك الإجرامي المرتكب وبين النتيجة المترتبة عليه كأثرٍ ناتج عن السلوك المرتكب، تلك العلاقة هي ما تُعرف بعلاقة السببية.

وحال انتفاء علاقة السببية فلا يُسأل الجاني عن جريمة تامة، وإنما يُسأل عن جريمة ناقصة (الشروع في ارتكاب الجريمة) إذا كانت الجريمة عمدية. أما إذا كانت الجريمة غير عمدية فتنتفي المسؤولية بحالتها؛ لأنه لا شروع فيها.

وبالنسبة لعلاقة السببية فتكون متوافرة بدنيًا **بجرائم تقنية المعلومات**، التي تتوافر بها النتيجة الإجرامية (جرائم الضرر).

المطلب الرابع :-الركن المعنوي

يُقصد بالركن المعنوي: الحالة النفسية والذهنية للجاني أثناء إقدامه على فعله المشين، ويتخذ الركن المعنوي شكل القصد الجنائي إذا كانت الجريمة عمدية، والخطأ غير العمدي إذا كانت الجريمة غير عمدية، والأصل العام أنه لا غنى عن توافر الركن المعنوي لقيام الجريمة

الأصل أن الجرائم المعلوماتية عمدية يتطلب القصد العام العلم بطبيعة الفعل وعدم مشروعيته

وفي بعض الجرائم يشترط قصد خاص، كنية الابتزاز أو الإضرار بالأمن، ولم يضع القانونان نظامًا خاصًا لإثبات القصد، بل يخضع للقواعد العامة.

رأي الباحث يتبين أن جريمة تقنية المعلومات لا تخرج عن الإطار التقليدي للنظرية العامة للجريمة، إذ تقوم على الأركان الثلاثة ذاتها، وإن كانت خصوصية البيئة الرقمية تؤثر في طبيعة السلوك والنتيجة والإثبات، وبذلك يظل البناء الجنائي التقليدي صالحًا كأساس لتحليل الجريمة الإلكترونية، مع ضرورة مراعاة الخصوصية التقنية عند التطبيق.

المبحث الثاني
نطاق التجريم ومحل الحماية في القانونين الليبي والمصري

إذا كان المبحث الأول قد تناول جريمة تقنية المعلومات من زاوية نظرية، بإخضاعها لأحكام النظرية العامة للجريمة، فإن هذا المبحث ينتقل إلى المستوى التشريعي التطبيقي، من خلال تحليل نطاق التجريم كما رسمه كل من المشرعين الليبي والمصري، وتحديد نطاق التجريم يعني بيان الأفعال التي عدّها المشرع جرائم، والمصالح التي قصد حمايتها من الاعتداء. فالسياسة الجنائية لا تتجلى فقط في مقدار العقوبة، وإنما في اختيار محل الحماية ذاته، وتحديد السلوك المجرم بدقة.

ومن خلال استقراء نصوص القانونين، يمكن تقسيم نطاق التجريم إلى ثلاثة محاور رئيسة:

1. الجرائم الواقعة على الأنظمة والمواقع والحسابات المعلوماتية.
2. الجرائم الواقعة على البيانات والخصوصية والمحتوى الرقمي.
3. الجرائم الماسة بالأمن والنظام العام عبر الوسائل التقنية.

وسيتم تناول كل محور في مطلب مستقل، مع تحليل مقارن بين النصين.

المطلب الأول:- الجرائم الواقعة على الأنظمة والمواقع والحسابات المعلوماتية

تُعد الأنظمة المعلوماتية والمواقع والحسابات الإلكترونية حجر الأساس في البيئة الرقمية، إذ تقوم عليها المعاملات والخدمات والاتصالات. ومن ثم، كان من الطبيعي أن يضع المشرعان نصوصًا تجرم الاعتداء عليها، سواء من حيث الدخول غير المشروع أو تعطيلها أو التلاعب بها , ويظهر من نصوص القانونين أن حماية الأنظمة تمثل الدائرة الأولى في نطاق التجريم.

الفرع الأول ـ جريمة الدخول غير المشروع

نص **القانون المصري** رقم (175) لسنة 2018 على تجريم الدخول بغير حق إلى موقع أو حساب خاص أو نظام معلوماتي، كما جرم البقاء فيه بغير وجه حق، واعتبر تجاوز حدود الحق المخول صورة من صور السلوك الإجرامي.

ويُفهم من النص أن الجريمة تتحقق بمجرد تحقق فعل الدخول غير المشروع، دون اشتراط وقوع ضرر فعلي، وهو ما يجعلها من جرائم الخطر، التي يكفي فيها تهديد المصلحة المحمية.

أما **القانون الليبي** رقم (5) لسنة 2022، فقد جرم الدخول غير المشروع إلى منظومة معلوماتية أو نظام معلوماتي، سواء تم ذلك عبر اختراق وسائل الحماية أو دون إذن من صاحب الحق.

ويتضح من المقارنة أن:

أ- كلا المشرعين اكتفى بمجرد الدخول غير المشروع لقيام الجريمة.

ب- لم يشترط أي منهما تحقق نتيجة مادية كإتلاف البيانات.

ج- شدد القانونان العقوبة إذا اقترن الدخول بقصد خاص أو ترتب عليه اعتداء لاحق على البيانات

,ومن حيث محل الحماية، يتبين أن المقصود هو حماية سرية النظام المعلوماتي وسلامته، باعتباره فضاءً خاصًا لا يجوز النفاذ إليه دون إذن.

ويرى الباحث أن تجريم مجرد الدخول غير المشروع يعكس تحولًا في الفكر الجنائي، إذ أصبح مجرد اختراق الحاجز الرقمي اعتداءً في ذاته، حتى ولو لم يتحقق ضرر ملموس.

الفرع الثاني ـ جريمة تعطيل أو إتلاف الأنظمة المعلوماتية

تناول **القانون المصري** تجريم الأفعال التي من شأنها إتلاف أو تعطيل أو إبطاء أو اختراق نظام معلوماتي، كما جرم حذف أو تعديل أو نسخ أو إعادة نشر البيانات المخزنة به دون وجه حق.

ويلاحظ أن النص المصري جاء بصياغة واسعة تشمل صورًا متعددة للمساس بالنظام، سواء كان ذلك عبر الإتلاف الكامل أو الجزئي، أو الإبطاء، أو تعطيل الكفاءة التشغيلية.
أما **القانون الليبي**، فقد نص على تجريم الأفعال التي تؤدي إلى إتلاف البيانات أو التلاعب بها أو تعطيل المنظومة المعلوماتية، بما في ذلك إدخال بيانات أو برامج بقصد الإضرار.
ويظهر من المقارنة أن:

أ- كلا القانونين يجرم الاعتداء المادي والبرمجي على النظام.
ب- النص المصري أكثر تفصيلًا في تعداد صور السلوك.
ج- النص الليبي يركز على فكرة الإضرار بالمنظومة أو البيانات.

ومن حيث الطبيعة القانونية، فإن هذه الجرائم تُعد جرائم ضرر إذا تحقق الإتلاف أو التعطيل فعليًا، بينما قد تُعد جرائم خطر إذا اقتصر الفعل على إدخال برنامج ضار دون تحقق النتيجة.
ويؤكد ذلك أن محل الحماية هنا هو سلامة البنية التقنية ذاتها.

الفرع الثالث ـ جريمة اعتراض البيانات أو التنصت عليها

نص **القانون المصري** على تجريم اعتراض أو التقاط أو تسجيل ما هو مرسل عبر شبكة معلوماتية بغير وجه حق.
كما نص **القانون الليبي** على تجريم اعتراض البيانات أو الاتصالات أو التقاطها دون إذن.
ويتضح أن المشرعين قصدا حماية سرية الاتصالات الرقمية، وهو امتداد لمبدأ سرية المراسلات في القانون التقليدي, ويُعد اعتراض البيانات اعتداءً مستقلًا، حتى ولو لم يتم استخدامها لاحقًا، لأن مجرد الاطلاع غير المشروع يُخل بسرية المعلومة.
ويرى الباحث أن تجريم اعتراض البيانات يعكس تطورًا في مفهوم الحماية الجنائية، إذ لم يعد الاعتداء مقتصرًا على الاستيلاء أو الإتلاف، بل يشمل مجرد النفاذ إلى المعلومة.

المطلب الثاني :- الجرائم الواقعة على البيانات والخصوصية والمحتوى الرقمي

لم يعد محل الحماية في البيئة الرقمية مقصورًا على النظام ذاته، بل امتد إلى البيانات المخزنة فيه، وإلى المحتوى المتداول عبر الشبكات. وقد أولى المشرعان عناية خاصة بحماية الخصوصية والبيانات الشخصية.

الفرع الأول ـ الاعتداء على الحياة الخاصة والبيانات الشخصية

نص **القانون المصري** على تجريم الاعتداء على حرمة الحياة الخاصة باستخدام وسائل تقنية المعلومات، بما في ذلك نشر أو إتاحة بيانات شخصية دون رضا صاحبها.
كما جرم **القانون الليبي** نشر أو تداول محتوى ينطوي على مساس بسمعة الأشخاص أو خصوصيتهم باستخدام الوسائل الإلكترونية، ويتضح أن كلا المشرعين اعتبر البيانات الشخصية محلًا مستقلًا للحماية الجنائية، ومن حيث الركن المادي، يتحقق السلوك بنشر البيانات أو تداولها أو إتاحتها دون إذن، أما الركن المعنوي، فيتطلب العلم بعدم المشروعية واتجاه الإرادة إلى النشر.
ويرى الباحث أن الاعتراف بالبيانات الشخصية كمحل حماية يعكس تحولًا في مفهوم الحق في الخصوصية، من حماية مادية إلى حماية رقمية.

الفرع الثاني ـ جريمة الابتزاز الإلكتروني

نص **القانون الليبي** صراحة على تجريم الابتزاز باستخدام وسائل تقنية المعلومات، إذا اقترن بتهديد بقصد الحصول على منفعة أو حمل المجني عليه على فعل أو امتناع.

كما جرم **القانون المصري** الأفعال التي تنطوي على تهديد أو ابتزاز عبر الشبكات المعلوماتية ويتضح أن الوسيلة التقنية تمثل ظرفًا جوهريًا في هذه الجريمة، إذ تميزها عن الابتزاز التقليدي وتتحقق الجريمة متى اقترن التهديد باستخدام الوسيلة الإلكترونية، ولو لم تتحقق المنفعة فعليًا.

الفرع الثالث ـ الجرائم المرتبطة بالمحتوى غير المشروع

تناول **القانون المصري** بعض صور نشر المحتوى الذي يخل بالقيم الأسرية أو النظام العام عبر الوسائل التقنية، كما نص **القانون الليبي** على تجريم نشر محتوى يشكل اعتداءً أو تحريضًا أو مساسًا بالنظام العام، ويظهر من النصين أن المشرعين توسعا في تجريم المحتوى الرقمي الذي يمثل خطرًا اجتماعيًا، مع ربط ذلك باستخدام الوسائل التقنية.

ويرى الباحث أن هذا الاتجاه يفرض على القضاء تفسيرًا دقيقًا للنصوص، حتى لا يؤدي اتساع مفهوم المحتوى إلى المساس بحرية التعبير خارج نطاق ما نص عليه القانون.

المطلب الثالث :ـ الجرائم الماسة بالأمن الوطني والنظام العام

يشكل الأمن الوطني والنظام العام من أهم المصالح التي يسعى القانون الجنائي إلى حمايتها. ومع انتشار الوسائل الرقمية، أصبح بالإمكان المساس بهما عبر نشر معلومات أو اختراق أنظمة ذات طابع سيادي.

الفرع الأول ـ تشديد العقوبة في حال المساس بالأمن

نص **القانون المصري** على تشديد العقوبة إذا كان الفعل من شأنه الإضرار بالأمن القومي أو المصلحة العامة، كما نص **القانون الليبي** على تشديد العقوبة إذا ارتبطت الجريمة بأمن الدولة أو النظام العام، ويتضح أن التشديد مرتبط بطبيعة المصلحة المعتدى عليها، لا بمجرد الوسيلة التقنية.

الفرع الثاني ـ الطبيعة القانونية لهذه الجرائم

تتميز هذه الجرائم بكونها تمس مصلحة جماعية، وقد تُعد من جرائم الخطر إذا كان مجرد الفعل كافيًا لتهديد الأمن.

ويرى الباحث أن إدراج ظرف المساس بالأمن يعكس إدراك المشرعين للبعد السيادي للفضاء الرقمي.

من خلال التحليل المقارن، يتبين أن:

أ- **القانون المصري** يتميز بتقسيم أكثر تفصيلًا للجرائم وتحديد أدق لصور السلوك.

ب- **القانون الليبي** ركز على الصور الأساسية للاعتداء الرقمي، مع تشديد في حال المساس بالأمن أو النظام العام.

ج- كلا التشريعين وسّعا محل الحماية ليشمل الأنظمة والبيانات والخصوصية والأمن.

ويؤكد ذلك أن نطاق التجريم في القانونين يعكس إدراكًا لخطورة البيئة الرقمية، وإن اختلفت درجة التفصيل التشريع.

المبحث الثالث

السياسة العقابية والتنظيم الإجرائي في جرائم تقنية المعلومات

لا يكتمل البنيان القانوني لأي جريمة دون تحديد السياسة العقابية التي يعتمدها المشرع في مواجهتها، إلى جانب الإطار الإجرائي الذي يضمن فعالية تطبيق النصوص. فالجزاء هو الأداة التي تتحقق بها الحماية الجنائية، والإجراءات هي الوسيلة التي تكفل الوصول إلى الحقيقة في حدود المشروعية.

وتتميز الجرائم المعلوماتية بخصوصية تستدعي تكييف السياسة العقابية والتنظيم الإجرائي بما يتناسب مع طبيعتها التقنية، سواء من حيث تنوع العقوبات، أو من حيث ضبط الأدلة الرقمية، أو من حيث دور مقدمي الخدمة في تسهيل التحقيق.
ومن ثم، يتناول هذا المبحث السياسة العقابية المعتمدة في القانونين، ثم التنظيم الإجرائي المتعلق بضبط الأدلة الرقمية، وأخيرًا مسؤولية مقدمي الخدمة في إطار الإجراءات الجنائية.

المطلب الأول :- السياسة العقابية في القانونين الليبي والمصري

تعكس السياسة العقابية فلسفة المشرع في تقدير خطورة السلوك الإجرامي. وفي الجرائم المعلوماتية، يتعين أن تكون العقوبة متناسبة مع طبيعة الاعتداء، الذي قد يكون غير مادي، لكنه شديد الأثر، وقد اعتمد كل من المشرعين الليبي والمصري مزيجًا من العقوبات السالبة للحرية والغرامات، مع التدرج بحسب جسامة الفعل.

الفرع الأول - العقوبات الأصلية

نص **القانون المصري** رقم (175) لسنة 2018 على عقوبات الحبس أو السجن والغرامة، وتختلف العقوبة بحسب نوع الجريمة، فالدخول غير المشروع يختلف عن تعطيل النظام أو المساس بالأمن القومي، كما نص **القانون الليبي** رقم (5) لسنة 2022 على عقوبات الحبس أو السجن والغرامة، مع تشديد العقوبة في بعض الحالات، خاصة إذا اقترنت الجريمة بالمساس بأمن الدولة أو النظام العام.
ويتضح من المقارنة أن:

أ- كلا القانونين اعتمدا مبدأ التدرج في العقوبة.
ب- العقوبات تتشدد إذا ترتب على الفعل ضرر أكبر أو تعلق بمصلحة عليا.
ج- الغرامة تمثل عنصرًا أساسيًا في الجزاء، نظرًا للطبيعة الاقتصادية لكثير من الجرائم الرقمية.

ونتناول عقوبة السجن والحبس في القانون المصري فقد توسع **المشرع المصري** أكثر من **المشرع الليبي** كالاتي:-
تناول المشرع المصري عقوبة السجن في المواد من (14) إلى (15) من قانون العقوبات المصري (2)، وفي إطار الحديث عن عقوبة السجن في مجال جرائم تقنية المعلومات نجد أن
المشرع قد نص على عقوبة السجن بجريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة حال توافر الظرف المشدد المنصوص عليه بالفقرة الثالثة بنص م (20)، التي تنص على:
"يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن 50 ألف جنيه ولا تجاوز 200 ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمداً أو بخطأ غير عمدي وبقي بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول، أو اخترق موقعاً أو بريداً إلكترونياً أو حساباً خاصاً أو نظاماً معلوماتياً يدار بمعرفة أو لحساب الدولة أو أحد أشخاص الاعتبارية العامة، أو مملوك لها أو يخصها.
فإذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية، تكون العقوبة السجن والغرامة التي لا تقل عن 100 ألف جنيه ولا تجاوز 500 ألف جنيه.
وفي جميع الأحوال، إذا ترتب على أي من الأفعال السابقة إتلاف تلك البيانات أو المعلومات، أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي أو البريد الإلكتروني، أو تدميرها أو تشويهها أو تغييرها أو تصميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها أو إلغائها كلياً أو جزئياً بأي وسيلة كانت، تكون العقوبة السجن والغرامة التي لا تقل عن مليون جنيه ولا تجاوز 5 ملايين جنيه".
كما جعل من السجن المشدد عقوبة بجريمة الاعتداء على سلامة الشبكة العنكبوتية حال توافر الظرف المشدد للجريمة، المتمثل في وقوع الجريمة على الدولة أو أحد الأشخاص الاعتبارية؛ إذ تنص م (21) من قانون مكافحة جرائم تقنية المعلومات على أن:

"يعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من تسبب متعمداً في إيقاف شبكة معلوماتية عن العمل أو تعطيلها، أو الحد من كفاءة عملها، أو التشويش عليها، أو إعاقتها، أو اعتراض عملها، أو أجرى بدون وجه حق معالجة إلكترونية للبيانات الخاصة بها.

ويعاقب كل من تسبب بخطئه في ذلك بالحبس مدة لا تقل عن ثلاثة شهور، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه أو بإحدى العقوبتين.

فإذا وقعت الجريمة على شبكة معلوماتية تخص الدولة أو أحد الأشخاص الاعتبارية العامة، أو تدار بمعرفتها أو تمتلكها، تكون العقوبة السجن المشدد وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه.

ولا يمكن إغفال عقوبة السجن حال توافر الظرف المشدد بنص م (23) المتعلقة بجرائم اصطناع المواقع والحسابات الخاصة والبريد الإلكتروني، التي تنص على:

"يعاقب بالحبس مدة لا تقل عن 3 أشهر وغرامة لا تقل عن 10 آلاف جنيه ولا تجاوز 30 ألف جنيه، أو بإحدى العقوبتين، كل من اصطنع بريداً إلكترونياً أو موقعاً أو حساباً خاصاً ونسبه زوراً لشخص طبيعي أو اعتباري.

فإذا استخدم الجاني البريد أو الموقع أو الحساب الخاص المصطنع في أمر يسيء إلى من نسب إليه، تكون العقوبة الحبس الذي لا تقل مدته عن سنة وغرامة لا تقل عن 50 ألف جنيه ولا تجاوز 200 ألف جنيه أو بإحدى العقوبتين.

وإذا وقعت الجريمة على أحد الأشخاص الاعتبارية العامة، فتكون العقوبة السجن والغرامة التي لا تقل عن 100 ألف جنيه ولا تزيد على 300 ألف جنيه."

وتكون العقوبة السجن المشدد بجريمة امتناع مقدم الخدمة عن تنفيذ القرار الصادر من المحكمة الجنائية بحجب أحد المواقع أو الروابط إذا توافر الظرف المشدد الذي تم النص عليه بالمادة الخاصة بالجريمة، م (30) من القانون محل الحديث، التي تنص على:

"يعاقب بالحبس مدة لا تقل عن سنة، والغرامة التي لا تقل عن خمسمائة ألف جنبه ولا تجاوز مليونًا، أو إحدى هاتين العقوبتين، كل مقدم خدمة امتنع عن تنفيذ القرار الصادر من المحكمة الجنائية المختصة بحجب أحد المواقع أو الروابط أو المحتوى المشار إليه في الفقرة الأولى من المادة (7) من هذا القانون.

فإذا ترتب على الامتناع عن تنفيذ القرار الصادر من المحكمة وفاة شخص أو أكثر أو الإضرار بالأمن القومي، وتكون العقوبة السجن المشدد وغرامة لا تقل عن ثلاثة ملايين جنيه ولا تجاوز عشرين مليون جنيه، وتقضي المحكمة فضلًا عن ذلك بإلغاء ترخيص مزاولة المهنة.

إضافة لما سبق، فقد نص المشرع بالمادة (34) من قانون مكافحة جرائم تقنية المعلومات على مجموعة من الظروف المشددة العامة، التي إن توافرت تكون العقوبة السجن المشدد، والتي تنص على:

"إذا وقعت أي جريمة من الجرائم المنصوص عليها في هذا القانون بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر، أو الإضرار بالأمن القومي للبلاد أو بمركزها الاقتصادي، أو منع أو عرقلة ممارسة السلطات العامة لأعمالها، أو تعطيل أحكام الدستور أو القوانين أو اللوائح، أو الإضرار بالوحدة الوطنية والسلام الاجتماعي، تكون العقوبة السجن المشدد"

ويرى الباحث أن اعتماد العقوبات السالبة للحرية إلى جانب الغرامة يعكس إدراك المشرعين لخطورة الاعتداء الرقمي، حتى وإن لم يكن مادياً بالمعنى التقليدي.

الفرع الثاني ـ التدابير التكميلية والمصادرة

تميز **القانون المصري** بإدراج تدابير إضافية، مثل:

أ- حجب الموقع الإلكتروني.

ب- غلق الموقع أو الحساب.

ج- مصادرة الأجهزة أو الأدوات المستخدمة في ارتكاب الجريمة.

وتُعد هذه التدابير ذات طبيعة وقائية، تهدف إلى إزالة الأثر الإجرامي ومنع استمراره.

أما **القانون الليبي**، فقد نص على المصادرة في بعض الحالات، باعتبارها أثرًا تبعيًا للحكم بالإدانة، دون توسع في تدابير الحجب والغلق على النحو التفصيلي الذي ورد في القانون المصري ,ومن حيث التحليل المقارن، يظهر أن التشريع المصري أولى عناية خاصة بإزالة الأثر الرقمي للجريمة، بينما ركز التشريع الليبي بصورة أكبر على الجزاء التقليدي.

ويرى الباحث أن الجمع بين العقوبة الشخصية والتدبير التقني يُعد أكثر ملاءمة لطبيعة الجريمة الرقمية، لأن استمرار الموقع أو النظام قد يُبقي الخطر قائمًا رغم معاقبة الفاعل.

الفرع الثالث ـ ظروف التشديد

نص **القانون المصري** على تشديد العقوبة إذا كان الفعل من شأنه الإضرار بالأمن القومي أو المصلحة العامة، أو إذا وقع على جهة اعتبارية عامة.

كما نص **القانون الليبي** على تشديد العقوبة في حال ارتباط الجريمة بأمن الدولة أو النظام العام.

ويكشف ذلك عن توجه مشترك لدى المشرعين نحو حماية المصالح العليا للدولة في الفضاء الرقمي، باعتبار أن الاعتداء عليها عبر الوسائل التقنية قد تكون له آثار واسعة النطاق.

المطلب الثاني :- التنظيم الإجرائي وضبط الأدلة الرقمية

تثير الجرائم المعلوماتية تحديات إثباتية خاصة، لأن الدليل فيها يكون رقميًا، قابلًا للتغيير أو المحو أو النسخ. ومن ثم، كان لزامًا أن يتضمن القانونان أحكامًا تتعلق بضبط الوسائط الرقمية وتمكين جهات التحقيق من الوصول إلى البيانات.

الفرع الأول ـ ضبط الأجهزة والوسائط الإلكترونية

نص **القانون المصري** على جواز ضبط الأجهزة أو الوسائط أو الأدوات المستخدمة في ارتكاب الجريمة، وذلك وفقًا للقواعد العامة في قانون الإجراءات الجنائية، كما أجاز اتخاذ تدابير حجب المواقع بقرار من الجهة القضائية المختصة.

أما **القانون الليبي**، فقد أجاز ضبط الوسائط والأجهزة المستخدمة في ارتكاب الجرائم الإلكترونية، مع إخضاع ذلك للقواعد العامة في الإجراءات الجنائية، ويتضح أن كلا القانونين لم يضع نظامًا إجرائيًا منفصلًا بالكامل، وإنما أضافا ما يلائم طبيعة الوسائط الرقمية ضمن الإطار العام للإجراءات الجنائية.

الفرع الثاني ـ حفظ البيانات وتمكين جهات التحقيق

ألزم **القانون المصري** مقدمي الخدمة بحفظ بيانات معينة لفترة زمنية محددة، وتمكين جهات التحقيق من الحصول عليها عند الطلب.

أما **القانون الليبي**، فقد أشار إلى التزام مقدمي الخدمة بالتعاون مع الجهات المختصة وتسليم البيانات وفق ما يطلب منهم قانونًا، ويظهر أن تنظيم حفظ البيانات يمثل عنصرًا محوريًا في التحقيق في الجرائم الرقمية، نظرًا لاعتماد الإثبات فيها على السجلات الإلكترونية.

ويرى الباحث أن وضوح التزام حفظ البيانات يعزز فعالية الملاحقة الجنائية، شريطة أن يمارس في إطار الضمانات القانونية.

الفرع الثالث ـ حجية الدليل الرقمي

لم ينص أي من **القانونين** على قواعد خاصة لحجية الدليل الرقمي خارج إطار القواعد العامة. وبالتالي يخضع الدليل الرقمي لمبدأ المشروعية، ويُقدر وفقًا لمبدأ الاقتناع القضائي الحر، ويظل لعنصر الخبرة الفنية دور جوهري في تفسير البيانات الرقمية وبيان سلامتها.

ويرى الباحث أن التحدي لا يكمن في الاعتراف بحجية الدليل الرقمي، بل في ضمان سلامة إجراءات جمعه وحفظه.

المطلب الثالث :ـ مسؤولية مقدمي الخدمة في الإطار الإجرائي

يمثل مقدمو خدمات الاتصالات واستضافة المواقع عنصرًا أساسيًا في البيئة الرقمية، لأنهم يحتفظون بالبيانات الفنية التي تُستخدم في تتبع الجناة.

قد عرَّفت اتفاقية بودابست مقدِّم الخدمة في المادة الأولى، البند (ج)، بأنه:

1- أي كيان عام أو خاص يقدِّم لمستخدمي الخدمة القدرة على الاتصال عن طريق نظام الكمبيوتر.
2- أي كيان آخر يقوم بمعالجة بيانات الكمبيوتر أو تخزينها نيابةً عن مزوِّد خدمة الاتصالات أو مستخدمي هذه الخدمة.

الفرع الأول ـ الالتزامات القانونية

ألزم القانون المصري مقدمي الخدمة بحفظ البيانات وتمكين السلطات المختصة من الاطلاع عليها.

أما القانون الليبي، فقد نص على التزام مقدمي الخدمة بالتعاون مع الجهات المختصة في إطار أحكام القانون.

الفرع الثاني ـ الجزاءات عند الإخلال

رتب **القانون المصري** جزاءات في حال امتناع مقدم الخدمة عن تنفيذ الالتزامات المنصوص عليها، كما نص **القانون الليبي** على مساءلة من يخالف أحكامه، وفقًا لنصوصه.

ويظهر أن المشرعين أدركا أن مكافحة الجرائم الرقمية لا تقتصر على معاقبة الفاعل، بل تمتد إلى تنظيم البيئة التقنية ذاتها.

رأي الباحث يتبين أن السياسة العقابية في كلا القانونين تقوم على التدرج والتناسب، مع تشديد خاص في حال المساس بالمصالح العليا، ويتميز القانون المصري بإدراج تدابير تقنية صريحة كالحجب والغلق، بينما يركز القانون الليبي على الجزاء التقليدي مع المصادرة.

أما من الناحية الإجرائية، فقد اعتمد القانونان إلى حد كبير على القواعد العامة، مع إدخال أحكام تتعلق بضبط الوسائط وحفظ البيانات.

التوصيات

1-كشفت الدراسة من خلال التحليل المقارن أن بعض نصوص القانون الليبي رقم (5) لسنة 2022 جاءت بصياغة موجزة في تحديد صور السلوك المجرَّم، مقارنة بالتفصيل الذي تبناه المشرع المصري، وهو ما يقتضي إعادة النظر في بعض هذه النصوص بهدف تدقيق نطاق التجريم وضبط المفاهيم القانونية المرتبطة به، تحقيقًا لمستوى أعلى من اليقين القانوني، وتفاديًا لأي توسع غير منضبط في التفسير القضائي.

2-أظهر البحث أن التنظيم الإجرائي المتعلق بالأدلة الرقمية في التشريع الليبي لا يزال يعتمد إلى حد كبير على القواعد العامة للإجراءات الجنائية، دون بيان تفصيلي لآليات جمع الدليل الرقمي وحفظه وضمان سلامته الفنية. ومن ثم، فإن إدراج نصوص أكثر تحديدًا في هذا الشأن يُعد خطوة ضرورية لتعزيز حجية الدليل أمام القضاء وتقليل احتمالات الطعن في مشروعيته أو سلامة إجراءاته.

3-بينت المقارنة أن التشرع المصري قد أولى عناية خاصة بالتدابير التقنية المصاحبة للعقوبة، كالحجب والغلق والمصادرة، باعتبارها أدوات لإزالة الأثر الإجرامي في البيئة الرقمية. وفي ضوء ذلك، يبدو من الملائم توسيع نطاق التدابير التقنية في القانون الليبي، بما يسمح بمعالجة النتائج الرقمية للجريمة بصورة فورية وفعالة، وبما يتلاءم مع طبيعة الاعتداءات الإلكترونية التي قد يستمر أثرها رغم صدور الحكم الجنائي.

4-اتضح من التحليل أن التزامات مقدمي الخدمة في القانون الليبي تحتاج إلى مزيد من التنظيم التفصيلي، لا سيما فيما يتعلق بمدة حفظ البيانات، ونطاقها، وضوابط تمكين الجهات المختصة منها، وإعادة تنظيم هذه الالتزامات بنصوص واضحة ومحددة من شأنه أن يحقق توازنًا دقيقًا بين متطلبات التحقيق الجنائي وضمانات حماية الخصوصية، وهو توازن جوهري في بيئة تتسم بكثافة المعالجة الرقمية للبيانات.

5-نظرًا للطبيعة التقنية المعقدة لجرائم تقنية المعلومات، وما تثيره من إشكالات فنية في تفسير الأدلة الرقمية وتقديرها، فإن دعم التخصص القضائي في هذا المجال يمثل ضرورة عملية، سواء عبر إنشاء دوائر متخصصة أو من خلال برامج تدريب فني وقانوني متقدمة، بما يضمن حسن تطبيق النصوص وتحقيق العدالة في إطارها الصحيح.

6-في ظل التطور التقني المتسارع، الذي يولّد باستمرار أنماطًا جديدة من السلوك الإجرامي، يصبح من الملائم اعتماد آلية مراجعة دورية للنصوص التشريعية ذات الصلة، حتى لا تتسع الفجوة بين الواقع الرقمي المتغير والإطار القانوني المنظم له، بما قد يؤدي إلى قصور في الحماية الجنائية أو عدم كفاية في المواجهة التشريعية.

7-وأخيرًا، يخلص الباحث إلى ضرورة تكريس التوازن بين الحماية الجنائية للفضاء الرقمي وصون الحقوق والحريات الأساسية، من خلال تطبيق نصوص التجريم في حدود ما قصده المشرع دون توسع غير مبرر في التفسير.

الخاتمة

خلصت هذه الدراسة إلى أن جريمة تقنية المعلومات، رغم حداثة محلها، تخضع في بنيانها العام لأحكام النظرية العامة للجريمة، من حيث الركن الشرعي والمادي والمعنوي. وقد التزم كل من القانون الليبي رقم (5) لسنة 2022 والقانون المصري رقم (175) لسنة 2018 بتحديد صور السلوك الإجرامي بنصوص صريحة، مع تفاوت في درجة التفصيل, ويظهر من التحليل المقارن أن التشريع المصري يتميز بتنظيم أكثر تفصيلًا للجرائم والتدابير التقنية ومسؤولية مقدمي الخدمة، في حين يمثل القانون الليبي إطارًا تشريعيًا حديثًا وضع الأساس للحماية الجنائية في البيئة الرقمية, كما تبين أن التنظيم الإجرائي في القانونين يعتمد إلى حد كبير على القواعد العامة للإجراءات الجنائية، مع إضافة بعض الأحكام الملائمة لطبيعة الدليل الرقمي.

وتظل فعالية النصوص مرهونة بحسن التطبيق، وبمدى قدرة الجهات المختصة على مواكبة التطور التقني.

"والله ولي التوفيق"

المراجع

اولا ـ الكتب والمؤلفات:

1- د. أحمد شوقي عمر أبو خطوة. "جرائم التعريض للخطر العام"، دراسة مقارنة، دار النهضة العربية، القاهرة، 1999.

2- د. أحمد عبد الله المراغي "الجريمة الإلكترونية ودور القانون الجنائي في الحد منها"، دراسة تحليلية تفصيلية مقارنة، المركز القومي للإصدارات القانونية، الطبعة الأولى، 2017.

3-4- د. أحمد عوض بلال.

- "مبادي قانون العقوبات المصري" القسم العام .دار النهضة العربية.2005/2004
- "الإثم الجنائي"، دراسة مقارنة، دار النهضة العربية، 1988م

5-6- د. أحمد فتحي سرور.

- "الوسيط في قانون العقوبات، القسم العام"، الطبعة السادسة، 1999.
- "الحماية الدستورية للحقوق والحريات"، دار الشروق، الطبعة الأولى، 1999.

7- د. أحمد كمال." جرائم الكمبيوتر والإنترنت"، "آراء مجموعة الخبراء، التقرير الثاني"، المركز القومي للبحوث الاجتماعية والجنائية، شعبة بحوث الجريمة والسياسة الجنائية، قسم بحوث وجريمة، القاهرة، 2017.

8- د. أنصار فوزي النعيمي ."أمن الكمبيوتر والقانون"، دار الراتب الجامعية، لبنان، بيروت، 1996.

9- د. إيناس عبد الله فكري. "جرائم نظم المعلومات: دراسة مقارنة"، دار الجامعة الجديدة، 2017.

10- د. محمد سامي الجندي ، جرائم الإنترنت والحاسب الآلي، دار الجامعة الجديدة، الإسكندرية.

11- د. بهاء المري. "شرح جرائم تقنية المعلومات"، القانون رقم 175 لسنة 2018، منشأة المعارف، 2019.

12- د. جمال عبد الباقي العنزي. "الإنترنت والقانون الجنائي"، دار النهضة العربية، 1992.

13- د. حاتم عبد الرحمن منصور ."الإجرام المعلوماتي"، الطبعة الأولى، دار النهضة العربية، 2002.

14- د. حسام الدين كامل الأهواني ، الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، القاهرة.

15- د .حسن صادق المرصفاوي. "قانون العقوبات الخاص"، الإسكندرية، منشأة المعارف، 1991.

16- د. حسين علي قيس. "إجرام المعلومات"، كلية الآداب، قسم الأنثروبولوجيا التطبيقية، الجامعة المستنصرية.

17- د. خالد حربي السعدني. "جريمة إتلاف برامج ومعلومات الحاسب الآلي في التشريعين الكويتي والمقارن"، دار النهضة العربية، الطبعة الأولى، 2012.

18- د. خالد حسن أحمد لطفي ."المسؤولية الجنائية عن جريمتي القذف والسب عبر الوسائط الإلكترونية: دراسة مقارنة".

19- د. خالد ممدوح إبراهيم. "الجرائم المعلوماتية"، دار الفكر الجامعي، 2009.

20- د. رؤوف عبيد. "السببية الجنائية بين الفقه والقضاء"، دراسة تحليلية مقارنة، دار الفكر العربي، 1984.

21- د. شريف سيد كامل. "جرائم الاعتداء على الأشخاص"، دار النهضة العربية، 2005.

22- د. شريف نصر أحمد. "الأحكام الموضوعية لجرائم الدخول غير المشروع إلى الأنظمة المعلوماتية: دراسة مقارنة".

23- د.طارق سرور. "جرائم النشر والإعلام"، الطبعة الثالثة، منقحة ومزيدة، دار النهضة العربية، 2021.

24- د. رجب عمر سالم، عمر سالم ."مبادئ علم الإجرام والعقاب"، الجزء الثاني، 2017/2016.

25- رؤوف عبيد. "السببية الجنائية بين الفقه والقضاء"، دراسة تحليلية مقارنة، دار الفكر العربي، 1984.

26- د .سامح السيد جاد. "شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة والعقوبة والتدبير الاحترازي"، 2005، بدون دار نشر.
27- د. علي أحمد راشد. "مبادئ القانون الجنائي: المدخل وأصول النظرية العامة"، الطبعة الثانية، دار النهضة العربية، القاهرة، 1974.
28- د. علي أحمد عبد الرزقي. "الطبيعة القانونية للجريمة الإلكترونية - من كتاب الحق في الخصوصية"، موقع المرجع الإلكتروني للمعلوماتية:
https://almerja.com/reading.php?idm77365
29- د. علي عبد القادر القهوجي. "الحماية الجنائية لبرامج الحاسب"، دار الجامعة الجديدة للنشر، 1997.
30- د. عمر سالم. "شرح قانون العقوبات المصري"، دار النهضة العربية، سنة 2010.
31- د. عمر محمود الجبوري. "الوجيز في الحماية الجنائية من جرائم تقنية المعلومات وفق أحكام القانون 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات"، دار النهضة العربية، 2021.
32- د. فائزة يونس الباشا. "سياسية الجرائم الالكترونية"، دار النهضة العربية، القاهرة.
33- د. محمد الدسوقي الشهاوي. "الحماية الجنائية لحرمة الحياة الخاصة في مواجهة الصحافة"، دار النهضة العربية، الطبعة الأولى، 2001.
34- د. محمد أمين المهدي، .المسؤولية الجنائية عن جرائم الحاسب الآلي والإنترنت، دار الجامعة الجديدة، الإسكندرية.
35- د. محمد سامي الشوا. "ثورة المعلومات وانعكاساتها على قانون العقوبات - الجزء الأول - جرائم نظم المعلومات في قانون العقوبات"، دار النهضة العربية، 1994.
36- د. محمد علي سويلم." شرح قانون مكافحة جرائم تقنية المعلومات"، دار المطبوعات الجامعية، الطبعة الأولى، 2020.
37- د. محمد مأمون سلامة. "قانون العقوبات - القسم العام"، دار النهضة العربية، القاهرة، 2001.

38-39 د. محمود رجب فتح الله.
- "الوسيط في جرائم تقنية المعلومات"، دار الجامعة الجديدة، 2019.
- "شرح قانون مكافحة جرائم تقنية المعلومات في ضوء القانون رقم 175 لسنة 2018: دراسة تحليلية مقارنة"، دار الجامعة الجديدة، 2019.

40- د. محمود نجيب حسني. "شرح قانون العقوبات - القسم العام"، دار النهضة العربية، 1982.

ثانياً: الدوريات والبحوث العلمية

1-بحث منشور في مجلة القانون والاقتصاد، كلية الحقوق – جامعة القاهرة، حول الاختصاص القضائي في الجرائم الإلكترونية.
1- بحث منشور في مجلة الحقوق – جامعة الإسكندرية، بشأن حجية الدليل الرقمي في الإثبات الجنائي.
2- دراسة منشورة في المجلة الليبية للعلوم القانونية والاقتصادية حول الطبيعة القانونية لجرائم تقنية المعلومات.

ثالثا .الاتفاقيات وقوانين وقرارات، وتقارير رسمية:

* اتفاقية بودابست المتعلقة بالجريمة الالكترونية مترجمة باللغة العربية، متاحة على اللينك الآتي:
/https://rm.coe.int/budapest-convention-in-arabic
* اتفاقية بودابست باللغة الإنجليزية، متاحة على اللينك الآتي:
https://rm.coe.int/1680081561

*قانون رقم (5) لسنة 2022م بشأن مكافحة الجرائم الالكترونية الليبي.
* قانون العقوبات المصري رقم 58 لسنة 1937، المعدل بالقانون رقم 95 لسنة 2003م.
* قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018، الجريدة الرسمية، العدد (32) مكرراً (ج)، الصادر في 14 أغسطس سنة 2018.

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare that they have no conflict of interest.