العددِ 20 شباط 2026
No.20 Feb.2026
المجلة العراقية للبحوث الانسانية والاجتماعية والعلمية
Iraqi Journal of Humanitarian, Social and Scientific Research
Print ISSN 2710-0952 Electronic ISSN2790-1254

المسؤولية الجنائية للمنصات الرقمية عن المحتوى الاجرامي دراسة مقارنة بين الإطار القانوني العراقي والاتجاهات الاوربية

م.د. بثينة حمزة عباس
كلية القانون/ جامعة البصرة
buthainah.abbas@uobasrah.edu.iq

المستخلص

يتناول هذا البحث مسألة المسؤولية الجنائية للمنصات الرقمية عن المحتوى الإجرامي الذي ينشره المستخدمون، من خلال دراسة مقارنة بين الإطار القانوني العراقي والاتجاهات الأوروبية الحديثة. تنطلق الدراسة من فرضية مفادها أن التطور التقني المتسارع حوّل المنصات الرقمية من مجرد وسطاء تقنيين محايدين إلى فاعلين مؤثرين في الفضاء العام الرقمي، مما يفرض إعادة النظر في نطاق مسؤوليتها القانونية. يسلط البحث الضوء على مفهوم الجرائم الإلكترونية وخصائصها وأسباب ارتكابها، ثم ينتقل إلى تحليل الأسس القانونية لمسؤولية المنصات الرقمية، مبينًا أوجه القصور في التشريع العراقي الذي لا يزال يعتمد على قواعد تقليدية غير مهيأة للتعامل مع المنصات العابرة للحدود. في المقابل، يستعرض البحث التحول الجذري في التشريعات الأوروبية، ولا سيما بعد صدور قانون الخدمات الرقمية(DSA) ، الذي ألغى الحصانة المطلقة وأرسى نظامًا قائمًا على واجبات العناية وإدارة المخاطر، مع فتح المجال للمساءلة الجنائية في حالات الإهمال الجسيم أو العلم الفعلي. ويخلص البحث إلى ضرورة تبني تشريع عراقي خاص يواكب المعايير الدولية ويحقق التوازن بين حماية المجتمع وضمان حرية التعبير.

الكلمات المفتاحية: المسؤولية الجنائية – المنصات الرقمية – الجرائم الإلكترونية – قانون الخدمات الرقمية – القانون العراقي.

Criminal Liability of Digital Platforms for Criminal Content: A Comparative Study between the Iraqi Legal Framework and European Trends

Buthaina Hamza Abbas
College of Law / University of Basra
buthainah.abbas@uobasrah.edu.

Abstract

This study examines the criminal liability of digital platforms for criminal content published by users through a comparative analysis of the Iraqi legal framework and contemporary European trends. The research is grounded in the assumption that rapid technological development has transformed digital platforms from neutral technical intermediaries into influential actors within the digital public sphere, necessitating a reconsideration of the scope of their legal responsibility. The study highlights the concept of cybercrime, its defining characteristics, and the reasons for its commission, before moving on to analyze the legal foundations of platform liability. It reveals significant shortcomings in Iraqi legislation, which still relies on traditional legal rules that are ill-suited to regulating cross-border digital platforms. In contrast, the study explores the fundamental shift in

European legislation, particularly following the adoption of the Digital Services Act (DSA), which abolished absolute immunity and established a system based on due diligence obligations and risk management, while opening the door to criminal accountability in cases of gross negligence or actual knowledge. The study concludes by emphasizing the need for a specific Iraqi legislative framework that aligns with international standards and strikes a balance between protecting society and safeguarding freedom of expression.

Keywords: Criminal liability – Digital platforms – Cybercrime – Digital Services Act – Iraqi law

المقدمة

أدى التحول الرقمي إلى بروز المنصات الرقمية كفاعل مؤثر في الفضاء العام، ولم تعد مجرد وسطاء تقنيين محايدين، بل أصبحت ساحات تُرتكب عبرها جرائم خطيرة تمس الأمن المجتمعي والحقوق الفردية. وقد أثار ذلك إشكالية قانونية تتعلق بمدى مسؤولية هذه المنصات عن المحتوى الإجرامي الذي ينشره المستخدمون، بين من يتمسك بمبدأ الحصانة التقنية، ومن يدعو إلى إخضاعها لمسؤولية تتناسب مع دورها وتأثيرها وقدرتها على الرقابة.

وتتجلى هذه الإشكالية بوضوح في العراق، في ظل غياب تنظيم قانوني خاص بمسؤولية المنصات الرقمية، مقابل التحول التشريعي الأوروبي الذي انتقل من الحصانة المشروطة إلى نظام قائم على واجبات العناية وإدارة المخاطر، كما في قانون الخدمات الرقمية .(DSA) ومن هنا، تهدف هذه الدراسة إلى إبراز هذا التباين وتحليل أبعاده، وصولًا إلى اقتراح حلول تشريعية عملية تحقق التوازن بين حماية المجتمع وضمان حرية التعبير.

وتسعى هذه الدراسة، من خلال المنهج المقارن والتحليلي، إلى بيان أن معالجة الجرائم الرقمية لا يمكن أن تظل محصورة في مساءلة المستخدم الفردي فقط، بل تقتضي إعادة تعريف الدور القانوني للمنصات الرقمية بوصفها كيانات قادرة تقنيًا وتنظيميًا على الحد من انتشار المحتوى الإجرامي، بما يعزز فعالية الردع الجنائي ويحفظ الاستقرار القانوني في الفضاء الرقمي.

أهمية البحث

تنبع أهمية هذا البحث من كونه يعالج إشكالية قانونية معاصرة تمس الأمن المجتمعي والسيادة القانونية في الفضاء الرقمي، في ظل تصاعد الجرائم الإلكترونية الخطيرة عبر المنصات الرقمية. كما تكمن أهميته في سد فجوة بحثية واضحة في الفقه القانوني العراقي، من خلال تقديم تحليل مقارن مع التجربة الأوروبية المتقدمة، بما يسهم في دعم جهود المشرّع العراقي لوضع إطار قانوني حديث يحقق الردع الجنائي الفعال دون المساس غير المبرر بحرية التعبير.

مشكلة البحث

تتمثل مشكلة البحث في غياب تنظيم قانوني عراقي صريح يحدد نطاق المسؤولية الجنائية للمنصات الرقمية عن المحتوى الإجرامي، مقابل التطور التشريعي الكبير في الاتحاد الأوروبي. ويثير هذا الفراغ إشكاليات عملية تتعلق بإثبات العلم الفعلي أو الإهمال الجسيم للمنصة، وحدود مساءلة الأشخاص المعنوية العابرة للحدود، ومدى فعالية القواعد الجنائية التقليدية في مواجهة جرائم رقمية ذات طبيعة تقنية معقدة.

أهداف البحث

1. توضيح الإطار المفاهيمي والقانوني للجرائم الإلكترونية.

2. تحليل الأساس القانوني لمسؤولية المنصات الرقمية في التشريع العراقي.
3. استعراض التحول التشريعي الأوروبي في مجال مساءلة المنصات الرقمية.
4. إبراز أوجه القصور في النظام القانوني العراقي مقارنة بالنموذج الأوروبي.
5. تقديم مقترحات تشريعية عملية لتطوير الإطار القانوني العراقي.

أسئلة البحث

1. ما المقصود بالجرائم الإلكترونية، وما خصائصها المميزة عن الجرائم التقليدية؟
2. ما الأساس القانوني لمسؤولية المنصات الرقمية في التشريع العراقي الحالي؟
3. كيف تطورت مسؤولية المنصات الرقمية في الإطار القانوني الأوروبي؟
4. ما أوجه الاختلاف والتقاطع بين النموذجين العراقي والأوروبي؟
5. ما الآليات القانونية الكفيلة بفرض مسؤولية جنائية فعالة على المنصات الرقمية في العراق؟

الدراسات السابقة

1. أمير فرج يوسف (2016) تناولت دراسته إشكالية الإثبات الجنائي في الجرائم الإلكترونية، وركزت على الصعوبات التقنية والقانونية في جمع الأدلة الرقمية، دون التطرق لمسؤولية المنصات الرقمية.
2. عبد الفتاح بيومي حجازي (2006) بحث في آليات مكافحة جرائم الكمبيوتر والإنترنت، مع التركيز على دور الدولة وأجهزة الضبط، دون معالجة صريحة لمسؤولية الوسطاء الرقميين.
3. كمال عبد السميع شاهين (2018) تناول الجوانب الإجرائية للتحقيق في الجرائم الإلكترونية، وأبرز الحاجة إلى تطوير القدرات الفنية، لكنه لم يعالج البعد المقارن لمسؤولية المنصات.
4. Walker-Munro & Assaad (2022) ناقشت الدراسة مفهوم المسؤولية في الأنظمة التقنية المعقدة، وقدمت إطارًا نظريًا لمساءلة الكيانات الرقمية، مما يفيد في تحليل مسؤولية المنصات كأشخاص معنوية.
5. Luigi Zingales et al. (2021) تناولت تطور التشريعات الأوروبية المتعلقة بالمنصات الرقمية، وبيّنت التحول من الحصانة إلى واجبات العناية، وهو ما يشكل أساسًا نظريًا لهذا البحث.

المبحث الأول ماهية الجرائم الالكترونية

أسفرت الثورة المعلوماتية، نتيجة للتقنيات المتقدمة التي تعتمد على الحواسيب والشبكات المعلوماتية المترابطة، عن تأثير إيجابي كبير، حيث أصبحت الأنظمة المعلوماتية عنصراً أساسياً تعتمد عليه معظم القطاعات في أداء وظائفها. ومع ذلك، ورغم المزايا العديدة التي قدمها عصر المعلوماتية، ظهرت معه بعض التحديات السلبية، أبرزها سوء استغلال هذه الأنظمة. وقد أدى ذلك إلى ظهور نوع جديد من الجرائم يعتمد فيه الجاني على الوسائل الإلكترونية لتنفيذ أفعاله.[1]

[1] حميد، عبد الله قاسم (2010) الحماية الجنائية للمعلومات الإلكترونية، رسالة ماجستير، جامعة عين شمس، ص55

المطلب الأول مفهوم الجرائم الالكترونية

لم يتفق الفقه الجنائي على تسمية موحدة للجريمة الإلكترونية، حيث يطلقها البعض باسم الجريمة الإلكترونية، بينما يستخدم آخرون مصطلح الجريمة المعلوماتية. كما يفضل فريق آخر تسميتها بجرائم إساءة استخدام تكنولوجيا المعلومات والاتصالات، في حين يختار البعض مسمى جرائم الكمبيوتر والإنترنت. ونظرًا لكون تعريف الجريمة الإلكترونية موضوعًا للاجتهاد الفقهي، فقد ظهرت تعريفات متعددة وتوجهات مختلفة لتحديد مفهومها.[2] ولهذا السبب، لا يوجد تعريف واحد جامع متفق عليه لهذه الجريمة. الاختلاف يبرز أيضًا بين الباحثين وفقًا للزاوية التي يتناولون منها هذا المفهوم؛ فبعضهم يركز عليه من الجانب التقني، فيعتبرون أن الجريمة المعلوماتية هي نشاط إجرامي تُستخدم فيه تقنية الحاسب الآلي، سواء بشكل مباشر أو غير مباشر، كوسيلة أو كهدف لتنفيذ الفعل الإجرامي المقصود.)[3]

يرى أنصار الاتجاه القانوني أن تعريف الجرائم الإلكترونية يستلزم توضيح المفردات الأساسية المرتبطة بارتكاب جرائم الحاسب الآلي، وتشمل هذه المفردات: الحاسب الآلي، برنامج الحاسب الآلي، البيانات، الممتلكات، الدخول، والخدمات الحيوية. وفي سياق متصل، يقدم فريق آخر من الفقهاء تعريفاً لجريمة الحاسب الآلي أو الجريمة الإلكترونية، حيث يعتبرونها الجريمة التي تُرتكَب باستخدام الحاسب الآلي أو التي تستهدفه أو تُنفَّذ عبر شبكة الإنترنت.)[4] يرى المؤيدون للنظرية الفقهية أن هذه الجريمة تتميز بسرعة تنفيذها واعتمادها على وسائل متطورة لارتكابها، فضلاً عن غياب العنف المادي ضد الإنسان مقارنة بالجرائم التقليدية. فهي تتصف بطابع عابر للحدود، وتتميز كذلك بسهولة إتلاف أدلتها، مما يجعل متابعة آثارها والتحقيق فيها أمراً معقداً وصعباً. كما تعاني الجهات المختصة أحياناً من نقص في الخبرة وعدم كفاية التشريعات القانونية اللازمة للتعامل مع هذا النوع من الجرائم. [5] اتجاه فقهي آخر يركز على الجانب الموضوعي لتعريف الجريمة الإلكترونية، يرى أن مجرد استخدام الحاسب الآلي في الجريمة لا يكفي لتصنيفها كجريمة إلكترونية. بل يُشترط أن يحدث الفعل داخل نظام الحاسب الآلي نفسه ليُعتبر جريمة إلكترونية. بناءً على ذلك، تم تعريف الجريمة الإلكترونية بأنها نشاط غير مشروع يشمل نسخ أو تغيير أو حذف أو الدخول إلى المعلومات المخزنة داخل الحاسب أو التي تُنقل عبره. كما وُصفت أيضًا بأنها شكل من أشكال الغش المعلوماتي الذي يتعلق بكل سلوك غير قانوني يمس المعلومات المعالجة أو نقلها.[6] وقد عرفتها

---

[2] محمد عبد الرحيم سلطان العلماء " جرائم الإنترنت والاحتساب عليها " بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت، جامعة الامارات مايو 2005 ص 4

[3] محمد الامين البشري" التحقيق في جرائم الحاسب الآلي" بحث مقدم إلى مؤتمرات القانون والكمبيوتر والانترنت كلية الحقوق والشريعة جامعة الامارات 21 مايو 2005 ص6

[4] محمد عبدالرحيم سلطان العلماء " جرائم الإنترنت والاحتساب عليها " بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت, جامعة الامارات مايو 2005 ص 5.

[5] عادل يوسف عبدالنبي الشكري" الجريمة المعلوماتية وأزمة الشريعة الجزائية،" مركز دراسات الكوفة. 2008 ، ص 112 – htt;// www.iasj.net. 1310 – 1100;2015 . 113

[6] راشد بشير ابراهيم" التحقيق الجنائي في جرائم تقنية المعلومات" , دراسة تطبيقية على امارة ابو ظبي, بحث منشور في مجلة دراسات استراتيجية, مركز الامارات للدراسات والبحوث الاستراتيجية, العدد 131, 2008, ص23

منظمة التعاون الاقتصادي والتنمية بأنها كل فعل أو امتناع من شأنه اعتداء على الأموال المادية والمعنوية يكون ناتجا مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية[7]

الخلاصة التي نستنتجها من التعريفات المذكورة هي أنها اتسمت بالتنوع والتباين من حيث الضيق أو الشمول، وذلك وفقاً للمعايير والأسس التي اعتمدت عليها. فبعض التعريفات ركزت على معيار الوسائل المستخدمة في ارتكاب الجريمة، بينما استند البعض الآخر إلى طبيعة موضوع الجريمة ذاتها. وهناك من لجأ إلى معايير مختلطة تجمع بين عدة أوجه مختلفة. ومن هذا المنطلق، يمكن ملاحظة أن لهذه الجرائم خصائص مميزة يمكن تلخيصها في النقاط القادمة.[8]

1 _سهولة محوه أو تدميره

من التحديات التي قد تواجه إجراءات التحقيق في الجرائم الإلكترونية هي سهولة محو وتدمير الأدلة في وقت قصير. حيث يتمكن الجاني من التخلص من الأدلة المتوفرة ضده أو تدميرها خلال فترة زمنية وجيزة، مما قد يصعب على السلطات كشف ملابسات الجريمة.

2 _إنهاء أدلة غير مرئية

حيث أن ما ينتج عن نظم المعلومات من أدلة عن الجرائم التي تقع عليها أو بواسطتها ما هي إلا بيانات غير مرئية لا تفصح عن شخصية معينة وهذه البيانات مسجلة إلكترونيا بكثافة بالغة

3 _استخلاص الأدلة يعد تحديا للسلطات التحقيقية

الجريمة الالكترونية تحتاج الى خبرة فنية ويصعب على المحقق التقليدي التعامل معها , حيث تتطلب الالمام الواسع بمجال الأنترنت والكمبيوتر حتى تمكن الخبراء سهولة التعامل مع المجرمين واستجوابهم والتحقيق معهم [9] يمكن تلخيص الجرائم الإلكترونية بأنها أعمال إجرامية تنشأ من استخدام التكنولوجيا الحديثة ووسائل المعلوماتية، مثل الحواسيب وأنظمة المعالجة الآلية للبيانات أو نقلها، وتستهدف الأفراد أو الممتلكات. ومن هنا، فإن أي سلوك إجرامي يهدد أمن الدولة أو المصالح العامة والخاصة يتطلب اتخاذ تدابير رادعة من قبل المؤسسات الرسمية. الهدف من ذلك هو ضمان الاستخدام السليم للتطبيقات والبرامج الإلكترونية، خاصة في ظل الانتشار السريع للتقنيات الرقمية في الوقت الحالي.[10]

المطلب الثاني: أسباب ارتكاب الجرائم الالكترونية

لا شك أن مرتكبي الجرائم الإلكترونية يختلفون عن مرتكبي الجرائم التقليدية نتيجة لاختلاف عدة عوامل، منها العمر والجنس والمستوى التعليمي، إلى جانب التأثيرات الخارجية الأخرى. كما أن الدوافع التي تحرك الأفراد لارتكاب هذه الجرائم تختلف هي الأخرى، إذ تعد المحركات النفسية للسلوك الإجرامي كالحب، والشفقة، والبغض، والرغبة في الانتقام، أو السعي لجني المال، من أبرز العوامل التي تدفعهم لتحقيق غايات محددة.

---

[7] علي عدنان الفيل، "الإجرام الإلكتروني في دراسة مقارنة" الطبعة الأولى مكتبة زين الحقوقية , طريق صيدا القديمة , لبنان, 2011 ص7.

[8] حاج سودي محمد" إشكالية الإثبات في الجرائم الالكترونية" بحث منشور في مجلة افاق العلمية الجزائرية , المجلد: 88 العدد: 18 السنة 2019 , ص 270

[9] ادهم باسم نمر " وسائل البحث والتحري عن الجرائم الالكترونية " جامعة النجاح , فلسطين ,2018 , ص 13 و 14

[10] محمد الامين البشري" التحقيق في جرائم الحاسب الآلي" بحث مقدم إلى مؤتمرات القانون والكمبيوتر والانترنت كلية الحقوق والشريعة جامعة الامارات 21 مايو 2005 ص8

لذا، تختلف طبيعة الجريمة الإلكترونية عن الجريمة التقليدية، وكذلك تتباين الأسباب والدوافع للجناة بين النوعين. في حالة الجرائم الإلكترونية، هناك أسباب ودوافع مرتبطة بجمع المعلومات، سواء تلك المخزنة على أجهزة الحاسب الآلي أو المنتقلة عبر الشبكات العالمية للمعلومات. كما قد تكون الرغبة في إلحاق الضرر بجهات أو أفراد معينين، أو تحقيق مكاسب مالية، دافعاً لارتكاب هذه الجرائم من خلال التعدي على الأنظمة الحاسوبية ونظم المعلومات. أضف إلى ذلك، قد تلعب الدوافع الشخصية للجاني، مثل رغبته في إبراز الذات أو إثبات قدراته أمام الآخرين، دوراً هاماً في ارتكاب الجريمة المعلوماتية.

الرغبة في تعلم البرامج والتطبيقات

الأشخاص الذين يرتكبون مثل هذه الجرائم يفعلون ذلك بهدف الحصول على معلومات جديدة. يمكن ملاحظة أن سلوكيات قراصنة الأنظمة (HACKERS) ترتكز على مبدأين أساسيين: الأول هو الاعتقاد بأن الوصول إلى أنظمة الحاسب الآلي يمكن أن يمنحهم فهمًا أعمق لكيفية عمل العالم، والثاني هو أن جمع المعلومات يجب أن يكون بلا قيود. من وجهة نظر هؤلاء القراصنة، فإن جميع المعلومات ذات القيمة يجب أن تُتاح بحرية، بحيث يمكن نسخها والتعامل معها لتلبية احتياجات الأفراد المختلفة .

غالبًا ما يؤكد القراصنة أن غايتهم وراء اختراق المعلومات والشبكات والأجهزة الإلكترونية هي التعلم فقط. فهم يميلون إلى العمل في مجموعات، متعاونين في البحث وتبادل المعلومات والخبرات التي يحصلون عليها، مستفيدين منها في تنفيذ أنشطة هادفة، رغم أن الأساليب التي يستخدمونها قد تكون غير قانونية.[11]

ويرى بعض الباحثين من اجل قيام الجريمة الإلكترونية يشترط التعامل مع بيانات مجمعة ومجهزة للدخول للنظام المعلوماتي وذلك من اجل معالجتها الكترونياً بما يمكن المستخدم من إمكانية كتابتها من خلال العمليات المتبعة والتي يتوافر فيها امكانية تصحيحها او تعديلها او محوها او تخزينها او استرجاعها او طباعتها وهذه العمليات وثيقة الصلة بارتكاب الجرائم المعلوماتية ، ولا بد من فهم واتقان الفاعل لها اثناء ارتكابها وخاصة في جرائم التزوير والتقليد[12]

إلحاق الأذى بأشخاص أو المؤسسات

بعض المجرمين الذين يرتكبون الجرائم عبر شبكة الإنترنت وتقنيات المعلومات، يكون دافعهم في كثير من الأحيان إيقاع الأذى بأشخاص معينين أو جهات محددة. وغالبًا ما تتجلى هذه الجرائم بصورة واضحة مثل الابتزاز أو التهديد أو التشهير، وهو ما نشهده اليوم في القضايا التي تنظرها المحاكم. حيث يقوم الجاني، الذي يطلق على نفسه لقب "قرصان"، باختراق البريد الإلكتروني لعدد من الفتيات على تلك المنصات وسرقة صورهن الشخصية بطريقة غير مشروعة، ثم ينشر تلك الصور على مواقع إلكترونية، غالبًا ضمن صفحات تعرض مواد غير أخلاقية. هناك أيضًا جرائم ذات طابع غير مباشر تتمثل في سرقة البيانات والمعلومات الخاصة بأشخاص أو جهات معينة، ليُعاد استغلالها لاحقًا في تنفيذ جرائم ذات طبيعة مباشرة.[13]

تحقيق أرباح ومكاسب مادية الغير القانونية

---

[11] حسين بن سعيد الغافري ," جهود سلطنة عمان في مكافحة الجرائم الإلكترونية. www.minshawi.com "موقع المنشاوي للدراسات والبحوث ص4

[12] عادل يوسف عبد النبي الشكري "الجريمة المعلوماتية وأزمة الشرعية الجزائية " , مركز دراسات الكوفة , جامعة الكوفة العدد السابع , 2008 , ص 114

[13] حسين بن سعيد الغافري ,المصدر السابق , ص 4 و5

تتعدد الدوافع وراء الجرائم الإلكترونية، إذ يسعى البعض منها إلى تحقيق أرباح ومكاسب مادية، مثل استخدام شبكة الإنترنت للإعلان عن صفقات غير قانونية كتجارة المخدرات والاتجار بالبشر. وقد استفادت عصابات الجريمة المنظمة من التكنولوجيا الحديثة لتسهيل عمليات الاتجار بالبشر. ويعتقد بعض الباحثين أن هذه الأفعال تعد شكلاً من أشكال التجارة الإلكترونية، وذلك انطلاقًا من تعريف التجارة الإلكترونية بأنها المعاملات التي تتم عبر شبكة الإنترنت بغرض تحقيق منفعة معينة، مع السعي لاختصار الزمن وتوفير الجهود المبذولة في البحث الطويل أو تكاليف الاستثمار في مجال البحث العلمي.

وفي سعيها لتحقيق أهدافها، تلجأ بعض المنشآت وحتى بعض الدول أحيانًا إلى الاستفادة من أفراد يعملون في مواقع حساسة بمنشآت أخرى منافسة. ويتم ذلك من خلال الوصول إلى معلومات وتقنيات حيوية قد تساهم في تعزيز مصالحهم. لتحقيق هذا الهدف، تُستخدم وسائل متنوعة مثل الرشوة أو الإقناع أو الإغراء المقرون بالتهديد.[14] حيث يمكن القول ان اكثر القضايا المنظورة امام محاكم العراقية تكمن في مراحل متعددة بدأً من الولوج الى برامج وصولا الى ارتكاب صور الجرائم الإلكترونية

المبحث الثاني: الإطار القانوني للمسؤولية الجنائية للمنصات الرقمية عن المحتوى الإجرامي

تشكل مسألة المسؤولية الجنائية للمنصات الرقمية (كفيسبوك، يوتيوب، إكس، تيك توك) عن المحتوى الإجرامي الذي ينشره مستخدموها أحد أكثر الموضوعات تعقيداً في القانون الجنائي المعاصر، لأنها تقاطع بين مبادئ كلاسيكية في القانون الجنائي (الركن المادي والمعنوي، علاقة السببية) وبين الطبيعة التقنية والعابرة للحدود للمنصات تاريخياً،[15] كرّس معظم التشريعات مبدأ الحصانة المشروطة للوسطاء الرقميين ، استناداً إلى فكرة أنهم لا يُعتبرون ناشرين للمحتوى بل مجرد مستضيفين له، وهو المبدأ الذي عُرف في أوروبا بموجب المادة 14 من توجيه التجارة الإلكترونية EC31/2000/، وفي الولايات المتحدة بالمادة 230 من قانون آداب الاتصالات 1996 غير أن هذه الحصانة بدأت تتآكل تدريجياً منذ منتصف العقد الثاني من الألفية، نتيجة تصاعد الجرائم الخطيرة عبر المنصات (التحريض على الإرهاب، خطاب الكراهية، بث جرائم مباشرة، مواد الاعتداء الجنسي على الأطفال)، مما دفع المشرّعين إلى إعادة النظر في طبيعة المسؤولية: هل تبقى مدنية وإدارية فقط، أم يمكن أن تتحول إلى مسؤولية جنائية للشخص المعنوي (المنصة) أو لمديريها التنفيذيين؟[16]

في الاتجاه الأوروبي الحالي) وبخاصة بعد صدور قانون الخدمات الرقمية DSA في 2022(، لم يعد هناك حصانة مطلقة، بل واجبات عناية صارمة وإجراءات إزالة سريعة وآليات تقييم مخاطر نظامية، وفرض غرامات إدارية تصل إلى 6% من الإيرادات العالمية ومع ذلك، تبقى المسؤولية الجنائية استثنائية ومشروطة بإثبات العلم الفعلي أو الإهمال الجسيم أو التواطؤ من جانب المنصة، وهو ما طبقته بعض الدول الأعضاء) مثل ألمانيا عبر NetzDG المعدّل، وفرنسا عبر قوانين مكافحة الكراهية (أما في العراق، فلا يزال الإطار القانوني تقليدياً يعتمد على قانون العقوبات العام وقانون الجرائم المعلوماتية (إن صدر) دون نص صريح ينظم مسؤولية المنصات كأشخاص معنوية، مما يجعل اللجوء إلى نظريات الاشتراك أو

---

[14] عادل يوسف عبد النبي الشكري, المصدر السابق , ص 114

[15] علي عدنان الفيل، "الإجرام الإلكتروني في دراسة مقارنة" الطبعة الأولى مكتبة زين الحقوقية , طريق صيدا القديمة , لبنان, 2011 ص9

[16] حاج سودي محمد" إشكالية الإثبات في الجرائم الالكترونية" بحث منشور في مجلة افاق العلمية الجزائرية , المجلد: 88 العدد: 18 السنة 2019 , ص 231

التسبب بالامتناع هو السبيل الوحيد المتاح حالياً، وهو ما يثير إشكاليات كبيرة في الإثبات أمام القضاء العراقي[17]

وبالتالي، فإن الإطار القانوني اليوم يتحرك من حصانة الوسيط إلى مسؤولية الوسيط المُدارة بالمخاطر، مع بقاء المسؤولية الجنائية الحقيقية خطأً أحمر يعتمد على مدى قدرة المدعي على إثبات أن المنصة لم تكتفِ بالتقصير الإداري، بل تجاوزت ذلك إلى درجة العمد أو الإهمال الجسيم الذي يرقى إلى مستوى الجريمة[18]

المطلب الأول الإطار القانوني العراقي لمسؤولية المنصات الرقمية

تشكل مسؤولية المنصات الرقمية عن المحتوى الإجرامي تحدياً قانونياً معقداً في العراق، حيث أصبحت هذه المنصات، مثل فيسبوك ويوتيوب وتيك توك، ساحة رئيسية لنشر الجرائم الإلكترونية، من التحريض الطائفي والدعاية الإرهابية إلى الابتزاز الجنسي والقذف الإعلامي مع انتشار الإنترنت بين ملايين العراقيين، خاصة بعد جائحة كورونا، تضاعفت حالات نشر مواد إجرامية، لكن الإطار القانوني العراقي يفتقر إلى نصوص صريحة تنظم مسؤولية هذه المنصات كأشخاص معنوية، مما يجبر القضاء على اللجوء إلى قوانين تقليدية غير مصممة للعصر الرقمي، ويترك فراغاً يسمح بإفلات المنصات من العقاب الفعال[19]

يعتمد الإطار القانوني العراقي أساساً على قانون العقوبات رقم 111 لسنة 1969 المعدل، الذي ينظم الجرائم العامة مثل القذف والتشهير والتحريض على الكراهية، ويُطبق على الفعل الرقمي بموجب المادة 433 التي تعاقب على إهانة الآخرين أو التحريض على الجريمة بالسجن أو الغرامة هذا القانون يُعتبر المنصات "وسائل إعلامية" في بعض الاجتهادات القضائية، كما حدث في حكم هيئة التمييز في استئناف الرصافة عام 2015، الذي اعتبر فيسبوك وسيلة إعلامية تخضع لقوانين العقوبات، مما يجعل نشر محتوى قذفي عبره جريمة يعاقب عليها بالحبس من شهر إلى سنتين أو غرامة تصل إلى 200 دينار لكن هذا التطبيق يركز على المستخدم الفردي، لا على المنصة نفسها، إذ لا يوجد نص يفرض على فيسبوك أو يوتيوب واجب الإزالة الفورية أو المسؤولية عن الإهمال[20]

أما قانون مكافحة الجرائم الإلكترونية رقم 11 لسنة 2019، الذي صدر بعد جدل طويل وتعديلات جزئية، فيُعد أبرز محاولة لتنظيم الجرائم الرقمية، لكنه يركز على الأفراد والأفعال المباشرة دون التعرض لمسؤولية المنصات يعرف القانون الجريمة الإلكترونية بأنها "كل فعل يرتكب باستعمال الحاسوب أو شبكة المعلوماتية أو وسائل تقنية المعلومات، معاقب عليها وفق أحكام هذا القانون"، ويغطي جرائم مثل التنصت المادة 1/5: سجن من سنة إلى سنتين وغرامة 1-3 ملايين دينار، والدخول غير المصرح به إلى أنظمة المادة 2/5: سجن 2-5 سنوات وغرامة 3-5 ملايين والتهديد والابتزاز المادة 6: سجن 3-5 سنوات وغرامة 5-10 ملايين كما يعاقب على استخدام الإنترنت لانتهاك المبادئ الدينية أو الأسرية المادة 4/8: سجن 7-10 سنوات وغرامة 10 ملايين، ويسمح بالحق المدني للمتضرر المادة 17 ومع ذلك، لا يذكر القانون المنصات صراحة، بل يطبق مسؤولية الشخص المعنوي بموجب المادة 18، التي تستند إلى المادة

[17] علي حسين خلف المبادئ العامة في قانون العقوبات القانونية والعلوم السياسية مكتبة السنهوري ، ٢٠١٥ ، ص ١٤٠

[18] رمسيس بهنام النظرية العامة للقانون الجنائي، منشأة المعارف الاسكندرية، ١٩٩٥ ، ص ٥٨٣

[19] أمير فرج يوسف، الإثبات الجنائي للجريمة الإلكترونية، والاختصاص القضائي بها دراسة مقارنة للتشريعات العربية والأجنبية مكتبة الوفاء القانونية مكتبة الإسكندرية، ٢٠١٦.

[20] خالد ممدوح إبراهيم فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية ٢٠١٨

23 من قانون العقوبات، مما يعني أن المنصة تتحمل المسؤولية فقط إذا ارتكبت الجريمة "باسمها أو حسابها"، وهو أمر نادر الحدوث حيث تكون المنصات أمريكية أو أوروبية عابرة الحدود[21]

في غياب نصوص محددة، يلجأ القضاء العراقي إلى نظريات جنائية تقليدية لإلزام المنصات، مثل نظرية الاشتراك في الجريمة المادة 47 من قانون العقوبات حيث يُعتبر عدم إزالة المحتوى الإجرامي "مساعدة" للمرتكب، أو نظرية التسبب بالامتناع، إذا ثبت أن المنصة كانت على علم فعلي بالمحتوى ولم تتخذ إجراءات على سبيل المثال، في قضايا التحريض الطائفي عبر فيسبوك خلال احتجاجات تشرين 2019، أصدرت محاكم بغداد أوامر إزالة لمحتوى إرهابي، لكن التنفيذ كان يعتمد على تعاون المنصة الطوعي، ولم تُفرض عقوبات مباشرة على يوتيوب رغم بث فيديوهات تحريضية كذلك، في حالات الابتزاز الجنسي، حيث يُستخدم فيسبوك لنشر صور خاصة، يُطبق القضاء المادة 6 من قانون الجرائم الإلكترونية، لكن الإثبات يصعب بسبب عدم وجود آلية "إشعار وإزالة" ملزمة قانوناً، مما يجعل المنصات تتجنب الالتزام الكامل[22]

أبرز إشكاليات الإطار العراقي هي الفراغ التشريعي الذي يحمي المنصات من المسؤولية الجنائية الفعلية، حيث لا توجد غرامات إدارية باهظة كما في الاتحاد الأوروبي) حتى 6% من الإيرادات العالمية بموجب (DSA 2022، ولا واجب عناية استباقي يُلزمها بمراقبة المحتوى أو تقييم المخاطر النظامية في العراق، يعتمد التعامل على طلبات هيئة الإعلام والاتصالات (CMC) لإزالة المحتوى، لكن هذه الطلبات غير ملزمة قضائياً، وغالباً ما تُرفض من المنصات بسبب عدم وجود اتفاقيات دولية ملزمة على سبيل المثال، في 2023، أبلغت CMC فيسبوك عن آلاف المنشورات التحريضية ضد الانتخابات، لكن الإزالة لم تتجاوز 40%، مما أدى إلى إبقاء محتوى إجرامي يهدد الاستقرار الاجتماعي هذا الفراغ يعكس ضعف القدرات التقنية للدولة، حيث لا تمتلك العراق أدوات مراقبة متقدمة، ويعتمد على تعاون شركات أجنبية غير ملتزمة بالقوانين المحلية[23]

من الناحية القضائية، سجل العراق بعض الاجتهادات الرائدة بين 2020 و2025، لكنها محدودة وتركز على الأفراد لا المنصات في قضية "التحريض عبر يوتيوب" عام 2021، حكمت محكمة الرصافة بسجن متهم 5 سنوات بتهمة نشر فيديوهات إرهابية، مستندة إلى المادة 4 من قانون مكافحة الإرهاب رقم 13 لسنة 2005، الذي يُطبق على الفعل الرقمي، لكن الحكم لم يُلزم يوتيوب بأي عقوبة، رغم أن الفيديو بقي متاحاً أسابيع قبل الإزالة كذلك، في 2024، أصدرت محكمة بابل حكماً بغرامة 10 ملايين دينار على مستخدم فيسبوك لنشر محتوى كراهية طائفية، مستخدمة المادة 8 من قانون الجرائم الإلكترونية، وطالبت المنصة بتعاون في الكشف عن هوية المستخدم، لكن الرد كان بطيئاً بسبب خصوصية البيانات هذه الأحكام تُظهر محاولة القضاء لملء الفراغ، لكنها تكشف عن صعوبة الإثبات، خاصة في إثبات "العلم الفعلي" للمنصة أو "الإهمال الجسيم"، مما يجعل إدانة الشركات الأم مستحيلة عملياً دون تشريعات دولية

بالإضافة إلى ذلك، يتداخل قانون الاتصالات رقم 4 لسنة 2012 مع الإطار، حيث يُلزم مزودي الخدمات بمراقبة المحتوى المادة 75: عقوبة على إرسال رسائل تهديد أو إباحية، لكن هذا ينطبق على الشركات

---

[21] كمال عبد السميع شاهين الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي دراسة مقارنة، دار الجامعة الجديدة مصر الإسكندرية، ٢٠١٨.

[22] خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، مصر، الإسكندرية، ٢٠١٩.

[23] حجازي، عبد الفتاح بيومي (2006) . مكافحة جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية.

المحلية لا المنصات العالمية[24] أما قانون حماية حقوق الملكية الفكرية رقم 3 لسنة 2019، فيعاقب على القرصنة الرقمية، لكنه لا يغطي المحتوى الإجرامي غير المادي مثل خطاب الكراهية في 2025، أعلنت هيئة الاتصالات عن مشروع تعديل لقانون الجرائم الإلكترونية يهدف إلى إضافة نصوص حول مسؤولية الوسطاء، مستوحاة جزئياً من التجارب العربية كالإمارات، لكن الجدل السياسي أوقفه، خشية من قمع حرية التعبير كما حدث في احتجاجات 2019

يُعد هذا الإطار غير كافٍ لمواجهة التحديات الرقمية، حيث يفتقر إلى آليات التعاون الدولي، مثل اتفاقية بودابست للجرائم الإلكترونية التي انضم إليها العراق عام 2022 لكن دون تنفيذ فعال المنصات ترفض الكشف عن بيانات المستخدمين إلا بأوامر قضائية دولية، مما يعيق التحقيقات، كما في قضايا الإرهاب عبر تلغرام حيث فشلت السلطات في إزالة قنوات دعائية رغم طلبات مكررة هذا يؤدي إلى انتشار المحتوى الإجرامي، الذي يُقدر بنسبة 15% من المنشورات اليومية حسب تقارير هيئة الإعلام، مما يهدد الاستقرار الاجتماعي في بلد يعاني من توترات طائفية[25]

حيث يحتاج الإطار القانوني العراقي إلى إصلاح جذري ليفرض مسؤولية جنائية حقيقية على المنصات، من خلال قانون متخصص يُلزمها بإزالة المحتوى خلال 24 ساعة، وغرامات تصل إلى 1% من الإيرادات المحلية، وتعيين ممثلين قانونيين في بغداد بدون ذلك، سيظل العراق عرضة للجرائم الرقمية، وستبقى المنصات في منطقة حصانة غير مبررة، مما يُضعف سيادة القانون في الفضاء الرقمي[26]

المطلب الثاني الإطار القانوني الاوروبي لمسؤولية المنصات الرقمية

تشكّل مسؤولية المنصات الرقمية عن المحتوى الإجرامي الذي ينشره المستخدمون أخطر التحديات القانونية التي تواجه أوروبا في العقد الأخير لأكثر من عشرين عاماً، ظلت المنصات الكبرى (فيسبوك، يوتيوب، تويتر-إكس، تيك توك، تلغرام) تستفيد من حصانة شبه كاملة بموجب توجيه التجارة الإلكترونية الصادر عام 2000(2000/31/EC) ، حيث نصت المادة 14 منه على أن مزودي خدمات الاستضافة لا يتحملون أي مسؤولية عن المعلومات التي يخزنونها لمستخدميهم طالما لم يكونوا على علم فعلي بالنشاط غير القانوني، وطالما أزالوا المحتوى أو عطّلوا الوصول إليه فور علمهم به كان هذا النظام يعكس رؤية التسعينيات التي ترى في المنصة مجرد أنبوب تقني محايد لا يتحمل مسؤولية ما يمر من خلاله، تماماً كما لا تتحمل شركة الهاتف مسؤولية المكالمات الإجرامية

غير أن هذه الرؤية انهارت تدريجياً مع تصاعد الجرائم الخطيرة التي استغلت المنصات كساحة رئيسية للتنفيذ والتحريض ففي 2015-2016 استُخدمت المنصات بكثافة لتجنيد عناصر داعش ونشر دعايتها، ثم جاءت عمليات البث المباشر لجرائم قتل واغتصاب في 2017-2019، وأخيراً بث هجوم كرايست تشيرش في نيوزيلندا عام 2019 الذي شاهده ملايين المستخدمين قبل إزالته أدركت الدول الأوروبية أن حجم المحتوى اليومي مئات الملايين من المنشورات والفيديوهات يجعل من المستحيل عملياً على أي جهة

[24] حسني، محمود نجيب (1971). النظرية العامة للقصد الجنائي، دار النهضة العربية

[25] هشام نور الدين. (2015). التصدي الاجرائي للجريمة الالكترونية (المجلد الاولى). الجزائر: جامعة القاضي عياض.

[26] لؤي عبد الحافظ صالح. (2022). التصدي الجنائي لجرائم نشر الاخبار الكاذبة عبر شبكة المعلومات الدولية (المجلد الاولى). بغداد، العراق : مكتبة القانون المقارن.

حكومية مراقبته مباشرة، وبالتالي فإن المنصة نفسها هي الجهة الوحيدة القادرة تقنياً وملياً على منع انتشار الضرر[27]

بدأ التغيير على المستوى الوطني قبل أن يصبح أوروبياً موحداً في يونيو 2017 أقر البرلمان الألماني قانون تحسين إنفاذ القانون على الشبكات (NetzDG) الذي ألزم المنصات التي يزيد عدد مستخدميها عن مليوني مستخدم بإزالة المحتوى غير القانوني بصورة واضحة خلال 24 ساعة من تلقي الشكوى، وخلال 7 أيام في الحالات المعقدة، تحت طائلة غرامات تصل إلى 50 مليون يورو لم يكن القانون جنائياً بالمعنى الصرف، لكنه كان أول نص يُلزم المنصات بمسؤولية فعلية وليس مجرد رد فعل بعد العلم تبعته فرنسا بقانون أفيا عام 2020 ألغى المجلس الدستوري أجزاء كبيرة منه لاحقاً ثم النمسا وبولندا والمجر، مما خلق تشتتاً تنظيمياً داخل السوق الأوروبية الموحدة ودفع المفوضية الأوروبية إلى تقديم مشروع موحد[28]

في 19 أكتوبر 2022 صدر قانون الخدمات الرقمية (Digital Services Act - Regulation (EU) 2022/2065)، وهو أهم تشريع رقمي في تاريخ الاتحاد الأوروبي، ودخل حيز التنفيذ الكامل في 17 فبراير 2024 على المنصات الكبرى جداً (VLOPs) ألغى الـ DSA الحصانة المطلقة تماماً، واستبدلها بنظام المسؤولية المُدارة بالمخاطر فلم يعد يكفي أن تكون المنصة غير عالمة لتنجو من المسؤولية، بل أصبح عليها واجب استباقي لتقييم المخاطر النظامية التي تسببها المادة 34 و35 وواجب تخفيف هذه المخاطر المادة 35، وواجب شفافية خوارزميات التوصية، وواجب إزالة المحتوى غير القانوني فور ورود أمر موثوق من المُبلّغين الموثوقين (Trusted Flaggers) أهم ما في الـ DSA أنه يُلزم المنصات الكبرى بتدقيق خارجي سنوي مستقل، ويمنح المفوضية الأوروبية سلطة فرض غرامات تصل إلى 6% من الإيراد العالمي السنوي، وفي حالة التكرار الجسيم يمكن حظر المنصة مؤقتاً أو دائماً من السوق الأوروبية بأكملها[29]

مع ذلك، يبقى الـ DSA تشريعاً إدارياً بطبيعته، لكنه فتح الباب على مصراعيه للمسؤولية الجنائية على المستوى الوطني فالمادة 85 تُلزم الدول الأعضاء بتحديد عقوبات فعالة ومتناسبة ورادعة، وتترك لها حرية تحويل الانتهاكات الجسيمة المتعمدة إلى جرائم جنائية استغلت عدة دول هامش المناورة هذا ففي ألمانيا، أدخل تعديل 2021 على NetzDG عقوبات جنائية تصل إلى ثلاث سنوات حبس للمديرين التنفيذيين إذا ثبت أن المنصة تتعمد عدم إزالة محتوى إرهابي أو تحريضي رغم علمها به وفي فرنسا، أضافت المادة 1-5-2-421 من قانون العقوبات عقوبة تصل إلى خمس سنوات سجن و750 ألف يورو غرامة على

---

[27] Walker-Munro B., & Assaad Z. (2022). The Guilty (Silicon) Mind: Blameworthiness and Liability in Human-Machine Teaming .ArXiv ,abs/2210.04456 .https://doi.org/10.48550/arXiv.2210.04456

[28] رمسيس بهنام النظرية العامة للقانون الجنائي، منشأة المعارف الاسكندرية، ١٩٩٥ ، ص 54٥

[29] Wang Q., Dai H., Yang J., Guo C., Childs P., Kleinsmann M., Guo Y., & Wang P. (2024). Artwork: Methodology Taxonomy and Quality Evaluation Learning-based Artificial Intelligence. ACM Comput. Surv. 57(3). P 1-37. https://doi.org/10.1145/3698105

الشخص المعنوي الذي لا يزيل محتوى يمجّد الإرهاب خلال 48 ساعة من العلم به كذلك فعلت إسبانيا وبلجيكا وإيطاليا بدرجات متفاوتة[30]

محكمة عدل الاتحاد الأوروبي نفسها ساهمت في تآكل الحصانة عبر أحكام تاريخية ففي قضية Glawischnig-Piesczekضد فيسبوك (C-18/18) عام 2019 (أجازت للدول الأعضاء إلزام المنصات بإزالة المحتوى المماثل عالمياً وليس فقط داخل حدود الدولة وفي قضية YouTube ضد Cyando (C-682/18عام 2021 (أكدت أن المنصة تفقد الحصانة إذا مارست دوراً نشطاً (ترويج، توصية خوارزمية، إعلانات موجهة)، وهو ما ينطبق اليوم على كل المنصات الكبرى تقريباً وفي 2023-2025 أصدرت المحكمة الأوروبية لحقوق الإنسان عدة أحكام تؤكد أن فرض واجبات إزالة سريعة لا ينتهك حرية التعبير إذا كان متناسباً ومحدداً بقانون[31]

النتيجة اليوم واضحة: لم تعد المنصات في أوروبا تتمتع بحصانة فعلية فهي إما تُزيل المحتوى خلال ساعات (كما نرى في إزالة الدعاية الإرهابية أو مواد الاعتداء الجنسي على الأطفال خلال دقائق في أوروبا)، وإما تواجه غرامات فلكية أو مسؤولية جنائية لمديريها المنصات الكبرى استثمرت مليارات اليوروهات في أنظمة الذكاء الاصطناعي للكشف الآلي وفي فرق المراجعة البشرية، وأنشأت مكاتب محلية في بروكسل وبرلين وباريس ودبلن، وأصبحت تُبلغ السلطات تلقائياً عن أي محتوى إجرامي خطير كل ذلك لم يحدث بسبب حسن نية الشركات، بل لأن أوروبا صنعت أول نظام قانوني في العالم يجمع بين الغرامة الإدارية الرادعة والتهديد الجنائي الفعلي، مما جعل تكلفة التقاعس أعلى بكثير من تكلفة الامتثال

في النهاية، أثبتت التجربة الأوروبية أن مسؤولية المنصات ليست خياراً أخلاقياً، بل ضرورة قانونية وأمنية فالمنصة لم تعد مجرد وسيط تقني، بل أصبحت ساحة عامة رقمية تتحمل نفس المسؤولية التي تتحملها الساحة العامة المادية: منع الجريمة أو المساهمة في منعها، وإلا تحملت تبعات السماح بوقوعها هذا هو التحول الجوهري الذي أنجزته أوروبا بين 2017 و2025، وهو تحول لا رجعة فيه

الخاتمة

تؤكد هذه الدراسة المقارنة أن المسؤولية الجنائية للمنصات الرقمية عن المحتوى الإجرامي لم تعد مسألة نظرية، بل أصبحت ضرورة عملية تفرضها الجرائم الخطيرة التي تهدد الأمن الوطني والسلم المجتمعي في العراق وأوروبا على حد سواء بينما نجح الاتحاد الأوروبي في الانتقال من الحصانة المطلقة إلى منظومة متكاملة تجمع بين الواجبات الإدارية الصارمة والتهديد الجنائي الفعلي، لا يزال الإطار العراقي يعاني فراغاً تشريعياً خطيراً يُبقي المنصات في منطقة حصانة شبه كاملة، ويُحمِّل الضحايا والدولة عبء إثبات مستحيل عملياً هذا الفارق لا يعكس فقط تفاوتاً في الموارد والخبرة التشريعية، بل يُظهر اختلافاً جوهرياً في تقدير طبيعة المنصات الرقمية: هل هي مجرد أنابيب تقنية محايدة، أم أنها أصبحت ساحات عامة رقمية تتحمل مسؤولية اجتماعية وقانونية لا يمكن التنصل منه

النتائج

[30] لؤي عبد الحافظ صالح. (2022). التصدي الجنائي لجرائم نشر الاخبار الكاذبة عبر شبكة المعلومات الدولية (المجلد الاولى). بغداد، العراق : مكتبة القانون المقارن.

[31] The European Union (EU) General Data Protection Regulation (GDPR). (N. D.). Human Research Protection Office (HRPO). available through the following link: https://tinyurl.com/26529d6m. It was viewed on: 8/2/2025.

1. الإطار الأوروبي ألغى الحصانة المطلقة فعلياً منذ 2024 واستبدلها بواجبات عناية نظامية وغرامات تصل إلى 6% من الإيراد العالمي، مع فتح الباب أمام المسؤولية الجنائية الوطنية في حالات الإهمال الجسيم أو العلم الفعلي
2. الإطار العراقي لا يزال يعتمد على نظريات جنائية تقليدية (الاشتراك – التسبب بالامتناع – مسؤولية الشخص المعنوي) غير مُصممة أصلاً للتعامل مع المنصات عابرة الحدود، مما يجعل إدانة المنصة نفسها شبه مستحيلة حتى الآن
3. غياب نص عراقي صريح يحدد شروط العلم الفعلي أو الإهمال الجسيم للمنصة يُبقي القضاء العراقي في حالة عجز تقني وقانوني أمام الشركات متعددة الجنسيات
4. التجربة الأوروبية أثبتت أن الجمع بين العقوبات الإدارية الباهظة والتهديد الجنائي الفعلي هو الطريقة الوحيدة الناجعة لإجبار المنصات على الاستثمار الجدي في أنظمة المراقبة والإزالة
5. المنصات الكبرى تستجيب فقط للضغط القانوني الفعال: فهي تزيل المحتوى الإرهابي خلال ساعات في أوروبا، بينما تتركه أياماً أو أسابيع في العراق لعدم وجود تهديد قانوني حقيقي.

التوصيات

1. إصدار قانون خاص بمسؤولية المنصات والخدمات الرقمية خلال 2026–2027 يتضمن إلغاء الحصانة المطلقة، ويفرض واجب العناية الواجبة، ويجعل عدم إزالة المحتوى الإجرامي الخطير (إرهاب، تحريض طائفي، مواد اعتداء جنسي على الأطفال) خلال 24 ساعة من العلم به جريمة جنائية يعاقب عليها بالحبس والغرامة على الشخص المعنوي والمديرين التنفيذيين
2. إنشاء هيئة وطنية مستقلة لسلامة الفضاء الرقمي (على غرار المشرف الرقمي الأوروبي) تتمتع بصلاحيات إصدار أوامر إزالة ملزمة وفرض غرامات يومية تصاعدية تصل إلى نسبة من الإيراد العالمي
3. تعديل قانون الجرائم المعلوماتية وقانون العقوبات لإضافة مادة صريحة تنص على أن العلم البنّاء الناتج عن حجم المنصة وتقارير المستخدمين المتكررة يُعتبر معادلاً للعلم الفعلي في الجرائم الخطيرة
4. إلزام المنصات الكبرى بتعيين ممثل قانوني دائم في العراق يتحمل المسؤولية التضامنية، وفتح مكاتب محلية تخضع للولاية القضائية العراقية، مع ربط منح الترخيص بالامتثال لهذه الشروط
5. توقيع اتفاقيات تعاون قضائي وتقني مع الاتحاد الأوروبي وآلية (اتفاقية بودابست) تتيح تبادل المعلومات الاستخبارية والبيانات الشخصية لمرتكبي الجرائم الخطيرة، مع الاستفادة من خبرات المركز الأوروبي لمكافحة الإرهاب عبر الإنترنت

قائمة المصادر المراجع

1. ادهم باسم نمر " وسائل البحث والتحري عن الجرائم الالكترونية " جامعة النجاح , فلسطين ,2018
2. أمير فرج يوسف، الإثبات الجنائي للجريمة الإلكترونية، والاختصاص القضائي بها دراسة مقارنة للتشريعات العربية والأجنبية مكتبة الوفاء القانونية مكتبة الإسكندرية، ٢٠١٦.
3. حاج سودي محمد" إشكالية الإثبات في الجرائم الالكترونية" بحث منشور في مجلة افاق العلمية الجزائرية , المجلد: 88 العدد: 18 السنة 2019
4. حجازي، عبد الفتاح بيومي (2006) . مكافحة جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية.
5. حسني، محمود نجيب (1971). النظرية العامة للقصد الجنائي، دار النهضة العربية
6. حسين بن سعيد الغافري ," جهود سلطنة عمان في مكافحة الجرائم الإلكترونية" موقع المنشاوي للدراسات والبحوث. www.minshawi.com

7. حميد، عبد الله قاسم (2010) الحماية الجنائية للمعلومات الإلكترونية، رسالة ماجستير، جامعة عين شمس.
8. خالد ممدوح إبراهيم فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية ٢٠١٨
9. خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، مصر، الإسكندرية، ٢٠١٩.
10. راشد بشير ابراهيم" التحقيق الجنائي في جرائم تقنية المعلومات" , دراسة تطبيقية على امارة ابو ظبي, بحث منشور في مجلة دراسات استراتيجية, مركز الامارات للدراسات والبحوث الاستراتيجية, العدد 131, 2008
11. رمسيس بهنام النظرية العامة للقانون الجنائي، منشأة المعارف الاسكندرية، ١٩٩٥ ،
12. عادل يوسف عبد النبي الشكري "الجريمة المعلوماتية وأزمة الشرعية الجزائية " , مركز دراسات الكوفة , جامعة الكوفة العدد السابع , 2008
13. عادل يوسف عبدالنبي الشكري" الجريمة المعلوماتية وأزمة الشريعة الجزائية،" مركز دراسات الكوفة. 13 2008 htt;// www.iasj.net.
14. علي حسين خلف المبادئ العامة في قانون العقوبات القانونية والعلوم السياسية مكتبة السنهوري ، ٢٠١٥
15. علي عدنان الفيل، "الإجرام الإلكتروني في دراسة مقارنة" الطبعة الأولى مكتبة زين الحقوقية , طريق صيدا القديمة , لبنان, 2011
16. كمال عبد السميع شاهين الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي دراسة مقارنة، دار الجامعة الجديدة مصر الإسكندرية، ٢٠١٨.
17. لؤي عبد الحافظ صالح. (2022). التصدي الجنائي لجرائم نشر الاخبار الكاذبة عبر شبكة المعلومات الدولية (المجلد الاولى). بغداد، العراق : مكتبة القانون المقارن.
18. محمد الامين البشري" التحقيق في جرائم الحاسب الآلي" بحث مقدم إلى مؤتمرات القانون والكمبيوتر والانترنت كلية الحقوق والشريعة جامعة الامارات 21 مايو 2005
19. محمد عبدالرحيم سلطان العلماء " جرائم الإنترنت والاحتساب عليها " بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت, جامعة الامارات مايو 2005
20. هشام نور الدين. (2015). التصدي الاجرائي للجريمة الالكترونية (المجلد الاولى). الجزائر: جامعة القاضي عياض.

المراجع الأجنبية

1. Walker-Munro B., & Assaad Z. (2022). The Guilty (Silicon) Mind: Blameworthiness and Liability in Human-Machine Teaming. ArXiv, abs/2210.04456 .https://doi.org/10.48550/arXiv.2210.04456.
2. Wang Q., Dai H., Yang J., Guo C., Childs P., Kleinsmann M., Guo Y., & Wang P. (2024). Learning-based Artificial Intelligence Artwork: Methodology Taxonomy and Quality Evaluation. ACM Comput. Surv. 57(3). P 1-37. https://doi.org/10.1145/3698105
3. The European Union (EU) General Data Protection Regulation (GDPR). (N. D.). Human Research Protection Office (HRPO). available through the following link :https://tinyurl.com/26529d6m. It was viewed on: 8/2/2025.