الحماية القانونية لضحايا الجرائم الإلكترونية في ظل التحديات الرقمية المعاصرة

الاستاذ المشرف

محمد علي حاجي ده ابادي

دكتوراه في القانون الجنائي وعلم الإجرام استاذ مشارك في كلية القانون /جامعة قم - إيران

طالب الدكتوراه احمد محمد ناصر السلمان

جامعة قم / كلية القانون / قسم القانون الجنائي إيران

البريد الإلكتروني Email : dr_hajidehabadi@yahoo.com

الكلمات المفتاحية: الحماية القانونية، ضحايا، الجرائم الإلكترونية، التحديات الرقمية المعاصرة، القانون العراقي.

كيفية اقتباس البحث

ابادي ، محمد علي حاجي ده، احمد محمد ناصر السلمان، الحماية القانونية لضحايا الجرائم الإلكترونية في ظل التحديات الرقمية المعاصرة،مجلة مركز بابل للدراسات الانسانية، شباط ٢٠٢٦، المجلد:١٦ ،العدد:٢ .

مفهرسة في Indexed
IASJ

مسجلة في Registered
ROAD

Legal protection for victims of cybercrime in light of contemporary digital challenges

Mohammad Ali Haji De Abadi
PhD in Criminal Law and Crime Science. Associate Professor at the Faculty of Law / University of Qom – Iran

PhD Candidate Ahmed Mohammed Nasser Al-Salman
University of Qom / Faculty of Law / Department of Criminal Law, Iran

Keywords : Legal protection, victims, cybercrimes, contemporary digital challenges, Iraqi law.

How To Cite This Article
Abadi, Mohammad Ali Haji De, Ahmed Mohammed Nasser Al-Salman, Legal protection for victims of cybercrime in light of contemporary digital challenges, Journal Of Babylon Center For Humanities Studies, February 2026,Volume:16,Issue 2.

Abstract

The digital space in the modern era is a source of both opportunities and challenges. Cybercrime has become an increasing threat to individuals and societies, especially in countries like Iraq, which is experiencing rapid internet and digital technology adoption. These crimes include online extortion, financial fraud, defamation, and cyber espionage, often targeting vulnerable groups such as women and children, resulting in severe psychological and material harm. The importance of this research stems from the noticeable rise in cybercrime rates in Iraq. Official reports indicate a 33% increase in online fraud and a 27% increase in online child exploitation in recent years. In the context of digital challenges such as the spread of artificial intelligence and social networks, Iraqi law struggles to keep pace with these developments. It

relies on general laws, such as the Telecommunications Law No. (65) of 2004, to address cybercrime, leading to gaps in protection. This research adopts a descriptive-analytical approach, describing the current legal framework in Iraq by analyzing laws such as the Penal Code and the Telecommunications Law, and comparing them with international standards to assess their effectiveness in protecting victims of cybercrime. The methodology also includes case studies and official statistics to understand digital challenges, utilizing secondary sources such as international reports to propose legislative recommendations. The research concluded that the Iraqi legal framework suffers from a lack of specialized legislation for cybercrimes, which limits the effectiveness of protecting victims against evolving crimes. While the Cybercrime Directorate and the Cyber Security Center contribute to improving monitoring and investigation, the absence of a comprehensive law weakens these efforts. The research recommends enacting a specialized cybercrime law that covers all emerging types, guarantees the protection of freedom of expression in accordance with international standards, and establishes a compensation fund for victims of cybercrimes to cover material and moral damages, with clear compensation mechanisms.

الملخص

يُعد الفضاء الرقمي في العصر الحديث مصدراً للفرص والتحديات على حد سواء، حيث أصبحت الجرائم الإلكترونية تهديداً متزايداً للأفراد والمجتمعات، خاصة في دول مثل العراق التي تشهد انتشاراً سريعاً للإنترنت والتقنيات الرقمية. تشمل هذه الجرائم الابتزاز الإلكتروني، الاحتيال المالي، التشهير، والتجسس الإلكتروني، والتي غالباً ما تستهدف فئات ضعيفة مثل النساء والأطفال، مما يؤدي إلى أضرار نفسية ومادية جسيمة يأتي أهمية هذا البحث في ظل الارتفاع الملحوظ في معدلات الجرائم الإلكترونية في العراق، حيث أفادت تقارير رسمية بزيادة بنسبة ٣٣% في الاحتيال الإلكتروني و٢٧% في استغلال الأطفال عبر الإنترنت خلال السنوات الأخيرة في سياق التحديات الرقمية مثل انتشار الذكاء الاصطناعي والشبكات الاجتماعية، يواجه القانون العراقي صعوبة في مواكبة التطورات، حيث يعتمد على تطبيق قوانين عامة مثل قانون الاتصالات رقم (٦٥) لسنة ٢٠٠٤ لمعالجة الجرائم الإلكترونية، مما يؤدي إلى فجوات في الحماية ويعتمد يعتمد هذا البحث على المنهج الوصفي التحليلي، حيث يتم وصف الإطار القانوني الحالي في العراق من خلال تحليل قوانين مثل قانون العقوبات وقانون الاتصالات، مع مقارنتها بالمعايير الدولية لتقييم فعاليتها في حماية ضحايا الجرائم الإلكترونية. كما يشمل المنهج دراسة حالات عملية وإحصاءات رسمية لفهم التحديات الرقمية، مع الاستعانة بمصادر ثانوية

مثل التقارير الدولية لاقتراح توصيات تشريعية وتوصل البحث الى يعاني الإطار القانوني العراقي من نقص تشريعات متخصصة للجرائم الإلكترونية، مما يحد من فعالية حماية الضحايا أمام الجرائم المتطورة كما تُسهم مديرية مكافحة الجرائم الإلكترونية ومركز الأمن السيبراني في تحسين الرصد والتحقيق، لكن غياب قانون شامل يُضعف هذه الجهود وأوصى البحث سن قانون متخصص للجرائم الإلكترونية يغطي جميع الأنواع الناشئة، مع ضمان حماية حرية التعبير وفق المعايير الدولية وإنشاء صندوق تعويض لضحايا الجرائم الإلكترونية لتغطية الأضرار المادية والمعنوية، مع تحديد آليات واضحة للتعويض.

المقدمة

يُعد الفضاء الرقمي في العصر الحديث مصدراً للفرص والتحديات على حد سواء، حيث أصبحت الجرائم الإلكترونية تهديداً متزايداً للأفراد والمجتمعات، خاصة في دول مثل العراق التي تشهد انتشاراً سريعاً للإنترنت والتقنيات الرقمية. تشمل هذه الجرائم الابتزاز الإلكتروني، الاحتيال المالي، التشهير، والتجسس الإلكتروني، والتي غالباً ما تستهدف فئات ضعيفة مثل النساء والأطفال، مما يؤدي إلى أضرار نفسية ومادية جسيمة. في ظل هذه التحديات الرقمية المعاصرة، يبرز دور القانون في توفير الحماية للضحايا، حيث يعتمد العراق حالياً على قانون العقوبات رقم (١١١) لسنة ١٩٦٩ لمعالجة بعض هذه الجرائم، مثل المواد (٣٦٩) و(٣٩٦) المتعلقة بالابتزاز الجنسي والعنف، إلا أن غياب قانون متخصص يعيق الاستجابة الفعالة.

مع تزايد انتشار الإنترنت في العراق، حيث بلغ عدد مستخدمي الإنترنت أكثر من ٣٠ مليون شخص بحلول عام ٢٠٢٥، أصبحت الجرائم الإلكترونية تشكل تهديداً للأمن الوطني والاجتماعي، مما دفع الحكومة إلى إنشاء مديرية مكافحة الجرائم الإلكترونية في وزارة الداخلية في فبراير ٢٠٢٥ لتعزيز الرصد والتحقيق. ومع ذلك، يظل الإطار القانوني غير كافٍ، إذ فشلت محاولات سن قوانين متخصصة مثل مشروع قانون جرائم المعلوماتية المقترح في ٢٠١١ و٢٠١٩ بسبب انتقادات حقوقية تتعلق بتقييد حرية التعبير. هذا الواقع يبرز الحاجة إلى توازن بين مكافحة الجرائم وحماية الحقوق الأساسية، مع التركيز على آليات التعويض والدعم النفسي للضحايا.

في سياق التحديات الرقمية مثل انتشار الذكاء الاصطناعي والشبكات الاجتماعية، يواجه القانون العراقي صعوبة في مواكبة التطورات، حيث يعتمد على تطبيق قوانين عامة مثل قانون الاتصالات رقم (٦٥) لسنة ٢٠٠٤ لمعالجة الجرائم الإلكترونية، مما يؤدي إلى فجوات في الحماية. يؤكد ذلك على أهمية دراسة الحماية القانونية للضحايا، مع النظر في الاتفاقيات الدولية

مثل اتفاقية بودابست لمكافحة الجرائم الإلكترونية، التي يمكن أن تساعد في تعزيز التعاون الدولي لمواجهة الجرائم عابرة الحدود

إشكالية البحث:

تتمثل إشكالية البحث في ضعف الحماية القانونية المقدمة لضحايا الجرائم الإلكترونية في ظل التحديات الرقمية المعاصرة، حيث تتسم هذه الجرائم – كالاحتيال الإلكتروني، التشهير الرقمي، سرقة الهوية، والابتزاز الإلكتروني – بسرعة الانتشار عبر الحدود، صعوبة تتبع الجناة، وغموض الاختصاص القضائي، مما يعيق تعويض الضحايا واستعادة حقوقهم، رغم وجود تشريعات جزئية كقانون مكافحة جرائم المعلوماتية رقم ١١١ لسنة ٢٠١٩ في العراق وقانون جرائم الحاسوب لسنة ٢٠٠٧ في إيران، إذ تفتقر هذه النصوص إلى آليات تنفيذية فعالة، تعاون دولي منسق، وتوعية قانونية كافية، مما يفرض ضرورة دراسة مقارنة لتقييم مدى كفاية الإطار القانوني في مواجهة التهديدات الرقمية المتطورة وتحقيق العدالة التعويضية للمتضررين.

أهمية البحث

يأتي أهمية هذا البحث في ظل الارتفاع الملحوظ في معدلات الجرائم الإلكترونية في العراق، مما يستلزم دراسة الحماية القانونية للضحايا لسد الفجوات التشريعية. يساهم البحث في تعزيز الوعي بضرورة تطوير قوانين متخصصة توفر آليات سريعة للإبلاغ والتعويض، خاصة للفئات الضعيفة، وبالتالي يدعم بناء مجتمع رقمي آمن يتماشى مع أهداف التنمية المستدامة للأمم المتحدة. كما يبرز البحث أهمية التوازن بين مكافحة الجرائم وصون حرية التعبير، مما يساعد في منع إساءة استخدام القوانين ضد الناشطين.

فضلا عن ذلك، يساهم البحث في تقديم توصيات عملية للمشرع العراقي لتحديث الإطار القانوني، خاصة مع إنشاء مركز الأمن السيبراني في ٢٠٢٥، الذي يمثل خطوة نحو تعزيز الحماية الرقمية. يعالج البحث الآثار الاجتماعية والنفسية للجرائم الإلكترونية، مثل الابتزاز الذي يؤدي إلى حالات انتحار، مما يؤكد على الحاجة إلى برامج دعم للضحايا وتدريب القضاة والشرطة، وبالتالي يعزز من الاستقرار الاجتماعي في ظل التحول الرقمي السريع.

اهداف البحث

١.بيان الإطار القانوني لضحايا الجرائم الإلكترونية في القانون العراقي

٢.بيان التحديات الرقمية المعاصرة وآليات حماية الضحايا

منهج البحث

يعتمد هذا البحث على المنهج الوصفي التحليلي، حيث يتم وصف الإطار القانوني الحالي في العراق من خلال تحليل قوانين مثل قانون العقوبات وقانون الاتصالات، مع مقارنتها بالمعايير الدولية لتقييم فعاليتها في حماية ضحايا الجرائم الإلكترونية. كما يشمل المنهج دراسة حالات عملية وإحصاءات رسمية لفهم التحديات الرقمية، مع الاستعانة بمصادر ثانوية مثل التقارير الدولية لاقتراح توصيات تشريعية.

خطة البحث:

المبحث الأول الإطار القانوني لضحايا الجرائم الإلكترونية في القانون العراقي

المطلب الأول التشريعات الحالية لمواجهة الجرائم الإلكترونية

المطلب الثاني دور الجهات التنفيذية والتشريعية في تعزيز الحماية

المبحث الثاني: التحديات الرقمية المعاصرة وآليات حماية الضحايا

المطلب الأول التحديات الرقمية المعاصرة

المطلب الثاني آليات حماية الضحايا

المبحث الأول

الإطار القانوني لضحايا الجرائم الإلكترونية في القانون العراقي

يُمثل الفضاء الرقمي في العراق، مع تزايد مستخدمي الإنترنت إلى أكثر من ٣٢ مليوناً بحلول عام ٢٠٢٥، تحدياً كبيراً يتمثل في ارتفاع معدلات الجرائم الإلكترونية مثل الاحتيال المالي، الابتزاز الجنسي، والتشهير عبر المنصات الرقمية. يعتمد الإطار القانوني الحالي على قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩، خاصة المواد (٣٦٩) و(٤٣٠) المتعلقة بالابتزاز والتشهير، وقانون الاتصالات رقم (٦٥) لسنة ٢٠٠٤، لكن هذه القوانين غير مصممة خصيصاً لمواجهة الجرائم الإلكترونية المتطورة، مما يُحد من فعالية الحماية. هذا النقص التشريعي، إلى جانب فشل مشاريع قوانين جرائم المعلوماتية في ٢٠١١ و٢٠١٩ بسبب مخاوف من تقييد حرية التعبير، يُبرز الحاجة إلى تطوير إطار قانوني شامل يوازن بين حماية الضحايا وصون الحقوق الأساسية[١].

تُسهم الجهود الحكومية، مثل إنشاء مديرية مكافحة الجرائم الإلكترونية ومركز الأمن السيبراني في ٢٠٢٥، في تعزيز الرصد والتحقيق، لكنها تظل محدودة بسبب ضعف التدريب على التعامل مع الأدلة الرقمية وغياب آليات تعويض ودعم نفسي للضحايا. تتطلب التحديات الرقمية المعاصرة، مثل التلاعب بالذكاء الاصطناعي والجرائم عابرة الحدود، تعاوناً دولياً أقوى، خاصة

من خلال تفعيل اتفاقية بودابست للجرائم الإلكترونية التي انضم إليها العراق في ٢٠٢٣. وبالتالي، يُعد تطوير الإطار القانوني ضرورة ملحة لضمان حماية فعالة للضحايا ودعم الأمن الرقمي في العراق.[٢]

وعليه ينقسم المبحث على مطلبين نبحث في المطلب الأول التشريعات الحالية لمواجهة الجرائم الإلكترونيةوتخصص المطلب الثاني دور الجهات التنفيذية والتشريعية في تعزيز الحماية.

المطلب الأول التشريعات الحالية لمواجهة الجرائم الإلكترونية

يُشكل انتشار التقنيات الرقمية في العراق وتحدياً كبيراً يتمثل في تصاعد الجرائم الإلكترونية مثل الاحتيال المالي، الابتزاز الجنسي، التشهير، وسرقة الهوية الرقمية. هذه الجرائم، التي تستهدف غالباً الفئات الضعيفة مثل النساء والأطفال، تُسبب أضراراً نفسية ومادية جسيمة، مما يستلزم إطاراً قانونياً قوياً لتوفير الحماية اللازمة. يعتمد العراق حالياً على مجموعة من التشريعات العامة لمواجهة هذه الجرائم، وفي مقدمتها قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩، وقانون الاتصالات رقم (٦٥) لسنة ٢٠٠٤، إلى جانب بعض الأنظمة الإدارية. ومع ذلك، فإن هذه القوانين، التي صيغت في سياقات غير رقمية، تفتقر إلى التخصص اللازم لمواكبة التحديات الرقمية المعاصرة، مما يُبرز الحاجة إلى تطوير تشريعات شاملة تُعالج الجرائم الإلكترونية بفعالية مع الحفاظ على الحقوق الأساسية[٣].

يُعتبر قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ الركيزة الأساسية للتعامل مع الجرائم الإلكترونية في غياب قانون متخصص. تنص المادة (٣٦٩) على معاقبة الابتزاز بالحبس لمدة تصل إلى سبع سنوات، وهو ما يُطبق على حالات الابتزاز الإلكتروني، مثل تهديد نشر صور أو فيديوهات خاصة عبر منصات التواصل الاجتماعي. كما تتناول المادة (٤٣٠) جرائم التشهير، التي تُعاقب بالحبس أو الغرامة إذا أُثيرت عبر وسائل إلكترونية، مثل نشر تعليقات مهينة على الإنترنت. فضلا عن ذلك، تُستخدم المادة (٣٩٦) لمعالجة الاعتداءات الجنسية، بما في ذلك تلك التي تُرتكب عبر الإنترنت، مثل التحرش الرقمي. ومع ذلك، فإن هذه المواد لا تُغطي بشكل مباشر الجرائم الإلكترونية الحديثة مثل القرصنة أو سرقة البيانات، مما يجعل تطبيقها محدوداً في مواجهة الجرائم المتطورة تقنياً[٤].

من جهة أخرى، يُوفر قانون الاتصالات رقم (٦٥) لسنة ٢٠٠٤ إطاراً إضافياً للتعامل مع بعض الجرائم الإلكترونية المتعلقة باختراق الأنظمة أو اعتراض البيانات. تنص المادة (٢١) من هذا القانون على عقوبات تصل إلى الحبس لمدة ثلاث سنوات أو غرامة مالية لمن يتعمد إتلاف شبكات الاتصالات أو يتدخل فيها بشكل غير قانوني. يُمكن تطبيق هذه المادة على

حالات اختراق المواقع الإلكترونية أو سرقة البيانات، لكنها لا تُغطي الجرائم الناشئة مثل التلاعب بالصور باستخدام الذكاء الاصطناعي أو الاحتيال عبر التطبيقات المزيفة. وإن هذا القانون يركز بشكل أساسي على تنظيم البنية التحتية للاتصالات، مما يجعله غير كافٍ لمعالجة الآثار الاجتماعية والنفسية للجرائم الإلكترونية على الضحايا.

شهد العراق محاولات لسن قانون متخصص للجرائم الإلكترونية، لكن هذه المحاولات لم تُكلل بالنجاح. ففي عامي ٢٠١١ و٢٠١٩، قُدم مشروع قانون جرائم المعلوماتية، لكنه أُوقف بسبب انتقادات منظمات حقوق الإنسان التي رأت أن بعض بنوده قد تُستخدم لتقييد حرية التعبير والصحافة. على سبيل المثال، اشتمل المشروع على عقوبات صارمة لنشر محتوى "يُخل بالآداب العامة"، مما أثار مخاوف من إساءة استخدامه ضد الناشطين والصحفيين. هذا الفشل أدى إلى استمرار الاعتماد على القوانين العامة، مما يُعيق الاستجابة السريعة للجرائم الإلكترونية المتزايدة، حيث أفادت تقارير وزارة الداخلية لعام ٢٠٢٤ بارتفاع الاحتيال الإلكتروني بنسبة ٣٣% واستغلال الأطفال عبر الإنترنت بنسبة ٢٧%.[٥]

لتعزيز الإطار القانوني، أنشأت الحكومة العراقية مديرية مكافحة الجرائم الإلكترونية في وزارة الداخلية في فبراير ٢٠٢٥، بهدف رصد الجرائم وتسريع التحقيقات. تتولى هذه المديرية التعامل مع قضايا مثل الاحتيال عبر البريد الإلكتروني والابتزاز الجنسي، كما أُسس مركز الأمن السيبراني في العام نفسه لتنسيق الجهود بين الجهات الحكومية وتحسين الحماية الرقمية. ومع ذلك، تواجه هذه الجهود تحديات كبيرة، مثل نقص التدريب المتخصص للشرطة والقضاة في التعامل مع الأدلة الرقمية، مما يؤدي إلى تأخير المحاكمات. فعلى سبيل المثال، في قضية احتيال إلكتروني عام ٢٠٢٢، استغرق التحقيق أكثر من عام بسبب صعوبة توثيق الأدلة الرقمية[٦].

إضافة إلى ذلك، انضم العراق إلى اتفاقية بودابست لمكافحة الجرائم الإلكترونية عام ٢٠٢٣، وهي خطوة تهدف إلى تعزيز التعاون الدولي في مواجهة الجرائم عابرة الحدود، مثل القرصنة أو غسيل الأموال الرقمي. تُلزم هذه الاتفاقية الدول الأعضاء بتطوير تشريعات تُجرّم أنشطة مثل اختراق الأنظمة والاحتيال عبر الإنترنت، مع تسهيل تبادل المعلومات بين الدول. ومع ذلك، فإن تطبيق هذه الاتفاقية في العراق لا يزال في مراحله الأولية بسبب ضعف البنية التحتية التقنية والقانونية، مما يُعيق ملاحقة الجناة الذين يعملون من خارج الحدود.

تتضمن الجرائم الإلكترونية في العراق أنواعاً متنوعة، أبرزها الاحتيال المالي عبر البريد الإلكتروني أو التطبيقات المزيفة، والذي يستهدف الأفراد والشركات على حد سواء. كما يُعتبر

الابتزاز الجنسي، خاصة عبر منصات مثل فيسبوك وواتساب، من أكثر الجرائم شيوعاً، حيث تُستهدف النساء بشكل رئيسي، مما يؤدي إلى أضرار نفسية واجتماعية جسيمة، بما في ذلك حالات انتحار. كذلك، تشهد البلاد ارتفاعاً في جرائم استغلال الأطفال عبر الإنترنت، مثل التحرش أو إجبارهم على إنتاج محتوى غير قانوني[٧].

تشمل التحديات القانونية صعوبة إثبات الجرائم الإلكترونية، حيث تتطلب الأدلة الرقمية خبرة تقنية عالية لتوثيقها وحفظها بشكل قانوني. في العديد من القضايا، تُرفض الدعاوى بسبب عدم كفاية الأدلة أو فقدانها نتيجة سوء التعامل. على سبيل المثال، في قضية قرصنة إلكترونية عام ٢٠٢٤، فشلت المحكمة في إدانة المتهم بسبب عدم وجود بروتوكولات موحدة لتخزين الأدلة الرقمية. وإن استخدام الجناة لتقنيات التشفير أو الشبكات الافتراضية الخاصة (VPN) يُعقد عملية التتبع، مما يتطلب تطوير قدرات تقنية متقدمة للشرطة[٨].

من الناحية الاجتماعية، يُعاني الضحايا من غياب آليات دعم نفسي واجتماعي فعالة. في حالات الابتزاز الجنسي، على سبيل المثال، يواجه الضحايا، وخاصة النساء، وصمة اجتماعية قد تمنعهم من الإبلاغ عن الجريمة خوفاً من العواقب. وإن القوانين الحالية لا توفر آليات واضحة للتعويض المادي أو المعنوي، مما يزيد من معاناة الضحايا. على سبيل المثال، لا يوجد صندوق تعويض مخصص لضحايا الجرائم الإلكترونية، على عكس بعض الدول التي تُوفر مثل هذه الآليات لدعم المتضررين[٩].

تُبرز هذه التحديات الحاجة إلى تطوير تشريعات متخصصة تُعالج الجرائم الإلكترونية بشكل شامل. ينبغي أن يشمل القانون الجديد تعريفات واضحة للجرائم مثل سرقة الهوية، التلاعب بالذكاء الاصطناعي، والقرصنة، مع تحديد عقوبات متناسبة. كما يجب أن يتضمن القانون آليات لتسهيل إثبات الأدلة الرقمية، مثل اعتماد بروتوكولات معيارية لحفظ البيانات وتدريب القضاة والمحققين على التعامل معها. إضافة إلى ذلك، يُعد إنشاء مراكز دعم نفسي واجتماعي للضحايا ضرورة ملحة لتخفيف الأضرار الناتجة عن الجرائم الإلكترونية[١٠].

من الجوانب الإيجابية، ساهمت الجهود الحكومية الأخيرة في تحسين الاستجابة للجرائم الإلكترونية. فعلى سبيل المثال، أطلقت مديرية مكافحة الجرائم الإلكترونية خطاً ساخناً للإبلاغ عن الحوادث، مما سهل على الضحايا تقديم الشكاوى. وإن مركز الأمن السيبراني بدأ في تطوير قواعد بيانات لتتبع الجرائم، مما ساعد في تسريع التحقيقات في بعض القضايا. ومع ذلك، فإن هذه الجهود تحتاج إلى دعم تشريعي أقوى لضمان استدامتها وفعاليتها.

في سياق التعاون الدولي، يُمكن لاتفاقية بودابست أن تلعب دوراً مهماً في تعزيز قدرة العراق على مواجهة الجرائم عابرة الحدود. فعلى سبيل المثال، ساهمت الاتفاقية في تمكين السلطات العراقية من التعاون مع دول أخرى في قضايا الاحتيال المالي عبر الإنترنت، حيث تم إلقاء القبض على شبكة دولية في ٢٠٢٤ بمساعدة الإنتربول. ومع ذلك، يتطلب تفعيل هذه الاتفاقية تحديث التشريعات المحلية لتتماشى مع المعايير الدولية، فضلا عن تحسين البنية التحتية التقنية[١١].

من الضروري أن يركز الإطار القانوني المستقبلي على حماية الفئات الضعيفة، مثل النساء والأطفال، الذين يُشكلون النسبة الأكبر من ضحايا الجرائم الإلكترونية. ينبغي أن تتضمن التشريعات آليات للإبلاغ السري للضحايا، مع توفير حماية قانونية لهم لمنع الوصمة الاجتماعية. كما يُعد إنشاء صندوق تعويض للضحايا خطوة حاسمة لتغطية الأضرار المادية والمعنوية، على غرار ما تُطبقه دول مثل المملكة المتحدة[١٢].

حيث يُظهر الإطار القانوني الحالي في العراق لمواجهة الجرائم الإلكترونية جهوداً ملحوظة ولكنها غير كافية لمواكبة التحديات الرقمية المتسارعة. يتطلب الأمر سن قانون متخصص يُعالج جميع أنواع الجرائم الإلكترونية، مع تعزيز التدريب التقني للشرطة والقضاة، وتطوير آليات دعم الضحايا. من خلال هذه الإصلاحات، يمكن للعراق بناء نظام رقمي آمن يدعم التنمية الاجتماعية والاقتصادية، مع تحقيق العدالة للضحايا والمساهمة في استقرار المجتمع[١٣].

المطلب الثاني دور الجهات التنفيذية والتشريعية في تعزيز الحماية

تشهد الجرائم الإلكترونية في العراق تصاعداً ملحوظاً مع انتشار استخدام الإنترنت، مما يجعلها تهديداً متزايداً للأمن الاجتماعي والاقتصادي. تتنوع هذه الجرائم بين الاحتيال المالي، الابتزاز الجنسي، سرقة الهوية الرقمية، والتشهير عبر منصات التواصل الاجتماعي، وغالباً ما تستهدف الفئات الضعيفة مثل النساء والأطفال، مما يُسبب أضراراً نفسية ومادية جسيمة. في هذا السياق، تبرز أهمية دور الجهات التنفيذية والتشريعية في تعزيز الحماية الجنائية من هذه الجرائم، حيث تعتمد العراق حالياً على قانون العقوبات رقم (١١١) لسنة ١٩٦٩ وقانون الاتصالات رقم (٦٥) لسنة ٢٠٠٤، إلى جانب مبادرات تنفيذية مثل إنشاء مديرية مكافحة الجرائم الإلكترونية ومركز الأمن السيبراني في ٢٠٢٥. ومع ذلك، فإن غياب قانون متخصص ونقص الخبرة التقنية يُعيقان تحقيق حماية فعالة، مما يستدعي جهوداً منسقة لتطوير التشريعات وتعزيز القدرات التنفيذية حيث تتولى الجهات التشريعية، ممثلة بمجلس النواب العراقي، مسؤولية سن القوانين

التي تُنظم الجرائم الإلكترونية وتوفر الحماية للضحايا. يعتمد العراق حالياً على قانون العقوبات، حيث تُطبق المادة (٣٦٩) عقوبة الحبس لمدة تصل إلى سبع سنوات على الابتزاز، بما في ذلك الابتزاز الإلكتروني مثل تهديد نشر صور خاصة، بينما تُعالج المادة (٤٣٠) التشهير الإلكتروني بعقوبات الحبس أو الغرامة. كما يُستخدم قانون الاتصالات، خاصة المادة (٢١)، لمعاقبة اختراق الأنظمة أو اعتراض البيانات بعقوبات تصل إلى الحبس ثلاث سنوات. ومع ذلك، فإن هذه القوانين، التي صيغت في سياقات غير رقمية، لا تُغطي الجرائم الحديثة مثل التلاعب بالذكاء الاصطناعي أو سرقة الهوية الرقمية، مما يُضعف فعاليتها.[١٤]

محاولات سن قانون متخصص للجرائم الإلكترونية، مثل مشروع قانون جرائم المعلوماتية في ٢٠١١ و٢٠١٩، واجهت عقبات بسبب مخاوف من تقييد حرية التعبير. فقد تضمن المشروع بنوداً تُعاقب على نشر محتوى "يُخل بالآداب العامة"، مما أثار انتقادات منظمات حقوق الإنسان التي رأت فيها تهديداً للصحفيين والناشطين. هذا الفشل أدى إلى استمرار الاعتماد على القوانين العامة، مما يُعيق الاستجابة السريعة للجرائم المتزايدة.[١٥]

من جانب الجهات التنفيذية، تلعب وزارة الداخلية دوراً محورياً من خلال مديرية مكافحة الجرائم الإلكترونية، التي أُنشئت في فبراير ٢٠٢٥ لتتبع ورصد الجرائم مثل الاحتيال المالي والابتزاز الجنسي. كما أُسس مركز الأمن السيبراني في العام نفسه لتنسيق الجهود بين الجهات الحكومية وتحسين القدرات التقنية. فعلى سبيل المثال، ساهم المركز في الكشف عن شبكة احتيال دولية في ٢٠٢٤ بالتعاون مع الإنتربول، مما أدى إلى إلقاء القبض على عدد من الجناة. ومع ذلك، تواجه هذه الجهات تحديات كبيرة، أبرزها نقص التدريب المتخصص في التعامل مع الأدلة الرقمية، مما يؤدي إلى تأخير التحقيقات. في قضية قرصنة إلكترونية عام ٢٠٢٤، استغرق التحقيق أكثر من عام بسبب عدم توفر بروتوكولات موحدة لحفظ الأدلة الرقمية[١٦].

تُعد الأدلة الرقمية تحدياً رئيسياً في التحقيقات الجنائية، حيث تتطلب خبرة تقنية عالية لتوثيقها وحفظها بشكل قانوني. غالباً ما تُرفض القضايا بسبب فقدان الأدلة أو سوء التعامل معها، مما يُقلل من فعالية الملاحقة القضائية. على سبيل المثال، في قضية تشهير إلكتروني عام ٢٠٢٣، فشلت الادعاء العام في تقديم أدلة رقمية موثوقة بسبب نقص الأدوات التقنية. ولمعالجة هذا التحدي، بدأت وزارة الداخلية بتطوير مختبرات رقمية متخصصة، لكن هذه المختبرات لا تزال في مراحلها الأولية وتتطلب استثمارات كبيرة في المعدات والتدريب[١٧].

انضمام العراق إلى اتفاقية بودابست لمكافحة الجرائم الإلكترونية في ٢٠٢٣ يُعد خطوة مهمة لتعزيز التعاون الدولي، خاصة في مواجهة الجرائم عابرة الحدود مثل غسيل الأموال الرقمي

والقرصنة. تُلزم هذه الاتفاقية الدول الأعضاء بتطوير تشريعات تُجرّم أنشطة مثل اختراق الأنظمة والاحتيال عبر الإنترنت، مع تسهيل تبادل المعلومات بين الدول. فعلى سبيل المثال، ساعدت الاتفاقية في إلقاء القبض على شبكة قرصنة دولية في ٢٠٢٤ كانت تستهدف البنوك العراقية. ومع ذلك، فإن تطبيق هذه الاتفاقية يتطلب تحديث التشريعات المحلية وتحسين البنية التحتية التقنية، حيث لا يزال العراق يعاني من تأخر في تطبيق المعايير الدولية حيث تُسهم الجهات التنفيذية أيضاً في توعية المجتمع من خلال حملات تهدف إلى تثقيف المواطنين حول مخاطر الجرائم الإلكترونية. فعلى سبيل المثال، أطلقت مديرية مكافحة الجرائم الإلكترونية حملة توعية في ٢٠٢٥ لتثقيف الشباب حول مخاطر مشاركة المعلومات الشخصية عبر الإنترنت. ومع ذلك، تظل هذه الحملات محدودة في المناطق الريفية، حيث يفتقر السكان إلى الوعي الرقمي، مما يزيد من تعرضهم للجرائم مثل الاحتيال عبر التطبيقات المزيفة.[١٨].

من الناحية التشريعية، ينبغي على مجلس النواب العمل على سن قانون شامل للجرائم الإلكترونية يُعرّف جميع أنواع الجرائم، مثل سرقة الهوية والتلاعب بالذكاء الاصطناعي، ويحدد عقوبات متناسبة. كما يجب أن يتضمن القانون آليات لتسهيل إثبات الأدلة الرقمية، مثل اعتماد بروتوكولات معيارية لحفظ البيانات. إضافة إلى ذلك، يُعد إنشاء صندوق تعويض للضحايا ضرورة ملحة لتغطية الأضرار المادية والمعنوية، خاصة في حالات الابتزاز الجنسي التي تُسبب أضراراً نفسية جسيمة[١٩]

تُعاني الجهات التنفيذية من نقص في الموارد البشرية والتقنية، مما يُعيق قدرتها على التعامل مع الجرائم الإلكترونية بفعالية. فعلى سبيل المثال، يوجد نقص في عدد المحققين المتخصصين في الأمن السيبراني، حيث لا يتجاوز عددهم ٢٠٠ محقق في جميع أنحاء العراق، وفقاً لتقرير وزارة الداخلية لعام ٢٠٢٤. وإن القضاة يفتقرون إلى التدريب الكافي على التعامل مع الأدلة الرقمية، مما يؤدي إلى تأخير المحاكمات أو رفض القضايا. في قضية تشهير إلكتروني عام ٢٠٢٣، استغرق الحكم أكثر من عام بسبب نقص الخبرة في تحليل الأدلة الرقمية.

تتطلب الحماية الجنائية الفعالة تعزيز التعاون بين الجهات التنفيذية والتشريعية. فمن الناحية التنفيذية، يجب استثمار المزيد في تطوير مختبرات رقمية متقدمة وتدريب المحققين على أحدث التقنيات. كما ينبغي إنشاء مراكز دعم نفسي واجتماعي للضحايا، خاصة في حالات الابتزاز الجنسي، حيث يُعاني الضحايا من وصمة اجتماعية تمنعهم من الإبلاغ. من الناحية التشريعية، يجب أن يتضمن القانون الجديد بنوداً تُعزز حماية الفئات الضعيفة، مثل النساء والأطفال، من خلال آليات إبلاغ سرية وعقوبات مشددة على الجناة.

تُظهر الإحصاءات أن الجرائم الإلكترونية لها تأثير اقتصادي كبير، حيث تسببت عمليات الاحتيال المالي في خسائر تقدر بملايين الدولارات في ٢٠٢٤، خاصة في القطاع المصرفي. وإن الجرائم مثل الابتزاز الجنسي تُؤدي إلى زيادة حالات الاضطرابات النفسية، مما يستدعي تدخلاً فورياً لدعم الضحايا. إضافة إلى ذلك، يُعاني العراق من نقص في برامج التثقيف الرقمي، مما يزيد من تعرض الأفراد للجرائم. من خلال سن تشريعات متخصصة، تحسين القدرات التقنية، وتطوير آليات دعم الضحايا، يمكن للعراق مواجهة التحديات الرقمية بفعالية، مما يدعم الاستقرار الاجتماعي والاقتصادي ويتماشى مع أهداف التنمية المستدامة.[٢٠]

المبحث الثاني

التحديات الرقمية المعاصرة وآليات حماية الضحايا

تواجه العراق تحديات رقمية معاصرة متزايدة مع انتشار الإنترنت. تُعقد هذه التحديات باستخدام الجناة لتقنيات التشفير والشبكات الافتراضية الخاصة، مما يصعب تتبعهم، إلى جانب نقص التثقيف الرقمي، خاصة في المناطق الريفية، وزيادة الجرائم الناشئة مثل التلاعب بالصور باستخدام الذكاء الاصطناعي. كما يُعيق نقص التدريب التقني للقضاة والمحققين التعامل مع الأدلة الرقمية، مما يؤدي إلى تأخير المحاكمات، كما حدث في قضية احتيال إلكتروني عام ٢٠٢٢ استغرقت أكثر من عام[٢١].

تتضمن آليات حماية الضحايا في العراق إجراءات محدودة مثل تقديم الشكاوى عبر مديرية مكافحة الجرائم الإلكترونية، لكنها تعاني من نقص الأدلة الموثقة وضعف الدعم النفسي للضحايا، خاصة في حالات الابتزاز الجنسي التي تُسبب وصمة اجتماعية. يُعزز انضمام العراق إلى اتفاقية بودابست عام ٢٠٢٣ التعاون الدولي لمواجهة الجرائم عابرة الحدود، لكن غياب مراكز دعم متخصصة وصندوق تعويض يُضعف الحماية. هناك حاجة إلى حملات توعية وطنية وتدريب الشرطة على الأدلة الرقمية لتعزيز استجابة النظام القانوني ودعم الضحايا.[٢٢]

وعليه انقسم المبحث الى مطلبين نبحث في المطلب الأول التحديات الرقمية المعاصرة وتحصص المطلب الثاني عن آليات حماية الضحايا

المطلب الأول التحديات الرقمية المعاصرة

يُعد انتشار التقنيات الرقمية في العراق، عاملاً رئيسياً في تصاعد الجرائم الإلكترونية، مما يُشكل تحديات معاصرة كبيرة للحماية الجنائية. تشمل هذه الجرائم الاحتيال المالي، الابتزاز الجنسي، سرقة الهوية الرقمية، التشهير عبر وسائل التواصل الاجتماعي، والقرصنة، والتي غالباً ما تُرتكب عبر منصات مثل فيسبوك وواتساب، مما يُسبب أضراراً نفسية ومادية جسيمة، خاصة

للفئات الضعيفة كالنساء والأطفال. يعتمد الإطار القانوني العراقي حالياً على قانون العقوبات رقم (١١١) لسنة ١٩٦٩، الذي يُطبق مواد مثل (٣٦٩) للابتزاز و(٤٣٠) للتشهير، وقانون الاتصالات رقم (٦٥) لسنة ٢٠٠٤، لكن هذه التشريعات غير مصممة خصيصاً للجرائم الرقمية، مما يُعيق الاستجابة الفعالة. مع إنشاء مديرية مكافحة الجرائم الإلكترونية في فبراير ٢٠٢٥ ومركز الأمن السيبراني، بدأت الحكومة في تعزيز الجهود، لكن التحديات الرقمية المعاصرة، مثل استخدام الذكاء الاصطناعي في التزييف العميق والتشفير، تُفاقم الفجوات في الحماية الجنائية، مما يتطلب إصلاحات جذرية لمواكبة التطورات التكنولوجية[٢٣].

أحد أبرز التحديات الرقمية المعاصرة هو صعوبة إثبات الجرائم الإلكترونية بسبب طبيعتها غير المادية والاعتماد على أدلة رقمية تتطلب خبرة تقنية عالية. في العراق، يُعاني النظام القضائي من نقص في الخبراء القانونيين المتخصصين في الجرائم السيبرانية، مما يؤدي إلى رفض العديد من القضايا أو تأخيرها لسنوات، كما حدث في قضايا احتيال إلكتروني حيث فشل التحقيق بسبب عدم توثيق الأدلة بشكل صحيح. يُضاف إلى ذلك استخدام الجناة لتقنيات التشفير المتقدمة والشبكات الافتراضية الخاصة(VPN) ، التي تُخفي هويتهم وتُعيق عمل الشرطة، خاصة مع ضعف البنية التحتية الرقمية في البلاد. مما يُبرز كيف أن التحديات التقنية تتجاوز القدرات الحالية للملاحقة الجنائية. هذه الصعوبات تُفاقم بغياب قانون متخصص للجرائم الإلكترونية، حيث فشلت محاولات سن مشروع قانون جرائم المعلوماتية في ٢٠١١ و٢٠١٩ بسبب مخاوف من تقييد حرية التعبير، مما يجعل تطبيق القوانين التقليدية غير كافٍ لمواجهة الجرائم الناشئة مثل التزييف العميق باستخدام الذكاء الاصطناعي، الذي يُستخدم في الابتزاز والتشهير[٢٤].

تُشكل الجرائم الإلكترونية عابرة الحدود تحدياً إضافياً للحماية الجنائية في العراق، حيث يقوم الجناة غالباً من خارج البلاد باستخدام خوادم أجنبية أو منصات دولية، مما يُعيق التعاون الدولي. على الرغم من انضمام العراق إلى اتفاقية بودابست لمكافحة الجرائم الإلكترونية في ٢٠٢٣، إلا أن تطبيقها يظل محدوداً بسبب ضعف الاتفاقيات الثنائية والفجوات في تبادل المعلومات الاستخباراتية. على سبيل المثال، في حالات القرصنة على المواقع الحكومية أو سرقة البيانات المصرفية، يصعب تتبع الجناة الذين يعملون من دول مجاورة أو بعيدة، مما يُقلل من معدلات الإدانة. وإن التهديدات السيبرانية من الجماعات الإرهابية، مثل نشر الدعاية التطرفية عبر الإنترنت أو اختراق الحسابات الرسمية، تُهدد الأمن الوطني، حيث أشارت تقارير إلى اختراقات مستمرة لمواقع حكومية في ٢٠٢٥. هذه التحديات تتطلب تعزيز القدرات التنفيذية، لكن

نقص التمويل والتدريب في مديرية مكافحة الجرائم الإلكترونية، التي سجلت أكثر من ١٥٠٠ قضية في النصف الأول من ٢٠٢٥، يُعيق الاستجابة السريعة، مما يجعل الحماية الجنائية غير فعالة أمام التطورات الرقمية السريعة[٢٥].

من التحديات البارزة أيضاً تأثير الجرائم الإلكترونية على الفئات الاجتماعية الضعيفة، حيث يُستهدف النساء بشكل خاص في حالات الابتزاز الجنسي عبر نشر صور مزيفة أو تهديدات، مما يؤدي إلى وصمة اجتماعية وأضرار نفسية شديدة، بما في ذلك حالات انتحار. وإن استغلال الأطفال عبر الإنترنت، مثل التحرش أو إجبارهم على إنتاج محتوى غير قانوني، يزداد مع انتشار التطبيقات، لكن القوانين الحالية لا توفر حماية كافية للأطفال، مما يُعرضهم لمخاطر طويلة الأمد. هذه التحديات الرقمية تُبرز فجوة في الحماية الجنائية، حيث لا يوجد صندوق تعويض للضحايا أو بروتوكولات للإبلاغ السري، مما يمنع الكثيرين من اللجوء إلى القضاء خوفاً من العواقب الاجتماعية[٢٦].

يُضيف ضعف البنية التحتية الرقمية في العراق طبقة أخرى من التحديات، حيث تعاني الشبكات من عدم الاستقرار، مما يُسهل على الجناة الاختراقات والسرقات، كما حدث في هجمات على البنوك والمؤسسات الحكومية في ٢٠٢٥. أشارت تقارير مركز الأمن السيبراني إلى أن التهديدات السيبرانية تُهدد الاقتصاد، مع خسائر مالية تصل إلى ملايين الدولارات من الاحتيال، وهو ما يتطلب استثمارات في الأمن السيبراني لكن التمويل المحدود يُعيق ذلك. وإن انتشار الذكاء الاصطناعي في الجرائم، مثل إنشاء فيديوهات مزيفة للابتزاز أو الدعاية، يُعقد التمييز بين الحقيقي والمزيف، مما يُصعب على القضاء الإثبات. في سياق هذه التحديات، يبدو أن الحماية الجنائية تحتاج إلى تكامل مع التشريعات الدولية، لكن ضعف التنفيذ يجعل العراق هدفاً سهلاً في ساحة المعارك السيبرانية الإقليمية[٢٧].

فضلا عن ذلك، يُواجه النظام القانوني تحدياً في مواكبة التطورات التكنولوجية السريعة، حيث تُستخدم تقنيات مثل الـ "ديب فيك" (التزييف العميق) في الجرائم الاجتماعية، مما يُهدد الاستقرار الاجتماعي والأمني. في العراق، أدى ذلك إلى زيادة الجرائم مثل الترويج للمخدرات أو الاختطاف عبر الإنترنت، كما كشفت وزارة التخطيط عن نسبة كبيرة من الجرائم عبر وسائل التواصل. الحماية الجنائية تُعاني من نقص في التدريب للقضاة والمحققين، حيث لا يوجد برامج مستمرة للتعامل مع الأدلة الرقمية، مما يؤدي إلى أحكام غير عادلة أو إفراج عن الجناة. على سبيل المثال، في قضايا التنصت الإلكتروني، يصعب تحديد المسؤولية بسبب استخدام الوسائط

الرقمية المجهولة. هذه التحديات تتطلب إصلاحات تشريعية فورية، مثل سن قانون يُجرّم الجرائم الرقمية الناشئة ويُعزز التعاون مع الدول المجاورة[٢٨].

من الجوانب الاجتماعية، يُفاقم نقص التوعية الرقمية التحديات، حيث يفتقر الكثيرون، خاصة في المناطق الريفية، إلى معرفة بمخاطر مشاركة البيانات الشخصية، مما يزيد من تعرضهم للاحتيال أو الابتزاز مما يُبرز الحاجة إلى حملات توعية وطنية. وإن الجرائم الإلكترونية تُرتبط بالتطرف، حيث تستخدم الجماعات المتطرفة الإنترنت لنشر الدعاية، مما يُهدد الأمن الوطني ويُعقد الحماية الجنائية بسبب الحدود الرقمية. في هذا السياق، يبدو أن الحل يكمن في تكامل الجهود التنفيذية مع التشريعية لتطوير قدرات التحقيق وتوفير دعم للضحايا حيث تُمثل التحديات الرقمية المعاصرة في العراق عقبة كبيرة أمام الحماية الجنائية من الجرائم الإلكترونية، مع فجوات قانونية وتقنية تتطلب إصلاحات عاجلة. من خلال سن تشريعات متخصصة، تعزيز التدريب، وتعزيز التعاون الدولي، يمكن تحقيق حماية أفضل، مما يدعم التنمية الرقمية المستدامة.[٢٩]

المطلب الثاني آليات حماية الضحايا

يُعد الفضاء الرقمي في العراق بيئة خصبة للجرائم الإلكترونية مثل الاحتيال المالي، الابتزاز الجنسي، سرقة الهوية، والتشهير عبر منصات التواصل الاجتماعي، مما يُسبب أضراراً نفسية ومادية جسيمة، خاصة للفئات الضعيفة كالنساء والأطفال. ويعتمد الإطار القانوني العراقي حالياً على قانون العقوبات رقم (١١١) لسنة ١٩٦٩، وقانون الاتصالات رقم (٦٥) لسنة ٢٠٠٤، لكن هذه التشريعات لا تُغطي بشكل كامل الجرائم الإلكترونية الحديثة مثل التزييف العميق باستخدام الذكاء الاصطناعي. أدت الجهود الحكومية، مثل إنشاء مديرية مكافحة الجرائم الإلكترونية ومركز الأمن السيبراني في ٢٠٢٥، إلى تحسين الرصد والتحقيق، لكن غياب آليات دعم شاملة وصندوق تعويض يُضعف حماية الضحايا، مما يتطلب تطوير آليات قانونية واجتماعية لضمان العدالة[٣٠].

تتمثل إحدى الآليات الأساسية للحماية في تقديم الشكاوى عبر مديرية مكافحة الجرائم الإلكترونية، ومما سهل على الضحايا الإبلاغ عن الحوادث، لكن هذه الآلية تعاني من قيود مثل نقص الأدلة الرقمية الموثقة وتأخر التحقيقات بسبب ضعف التدريب التقني للمحققين. على سبيل المثال، في قضية احتيال إلكتروني عام ٢٠٢٢، استغرق التحقيق أكثر من عام بسبب صعوبة تحليل الأدلة الرقمية، مما أدى إلى إحباط الضحايا. وإن غياب بروتوكولات موحدة لحفظ الأدلة

يُعيق إدانة الجناة، حيث تُرفض العديد من القضايا بسبب فقدان الأدلة أو سوء التعامل معها، مما يُبرز الحاجة إلى تطوير مختبرات رقمية متقدمة وتدريب المحققين على أحدث التقنيات[٣١].

يتضمن الإطار القانوني الحالي بعض الحماية من خلال قانون العقوبات، حيث تنص المادة (٣٦٩) على الحبس لمدة تصل إلى سبع سنوات للابتزاز، بما في ذلك الابتزاز الإلكتروني، والمادة (٤٣٠) على التشهير بعقوبات الحبس أو الغرامة. كما يُعاقب قانون الاتصالات، في المادة (٢١)، على اختراق الأنظمة بعقوبات تصل إلى الحبس ثلاث سنوات، لكن هذه القوانين لا توفر آليات تعويض واضحة للضحايا، مما يُضعف الحماية. على سبيل المثال، في قضايا الابتزاز الجنسي، غالباً ما يُعاني الضحايا من وصمة اجتماعية، خاصة النساء، مما يمنعهم من المطالبة بحقوقه لكن العديد من الضحايا امتنعوا عن الإبلاغ خوفاً من العواقب الاجتماعية، مما يُظهر الحاجة إلى آليات إبلاغ سرية ودعم نفسي. إضافة إلى ذلك، لا يوجد صندوق تعويض مخصص لتغطية الأضرار المادية والمعنوية، على عكس دول مثل المملكة المتحدة التي توفر مثل هذه الآليات[٣٢].

تُشكل التحديات الرقمية المعاصرة عقبة كبيرة أمام حماية الضحايا، حيث يستخدم الجناة تقنيات التشفير والشبكات الافتراضية الخاصة لإخفاء هويتهم، مما يُعيق التتبع. وإن الجرائم عابرة الحدود، مثل القرصنة أو الاحتيال عبر منصات دولية، تُصعب الملاحقة القضائية بسبب ضعف التعاون الدولي. على الرغم من انضمام العراق إلى اتفاقية بودابست لمكافحة الجرائم الإلكترونية في ٢٠٢٣، إلا أن تطبيقها يظل محدوداً بسبب نقص البنية التحتية التقنية والتشريعات الداعمة. فعلى سبيل المثال، في قضية قرصنة مصرفية عام ٢٠٢٤، تمكنت السلطات من التعاون مع الإنتربول لاعتقال شبكة دولية، لكن معظم القضايا عابرة الحدود تظل دون حل بسبب غياب آليات تبادل المعلومات الفعالة. هذه التحديات تُبرز أهمية تعزيز التعاون الدولي وتطوير تشريعات تتماشى مع المعايير العالمية[٣٣]

من التحديات الاجتماعية، يُعاني الضحايا، خاصة النساء والأطفال، من وصمة اجتماعية تمنعهم من الإبلاغ عن الجرائم، خاصة في حالات الابتزاز الجنسي، مما يُظهر الحاجة إلى مراكز دعم نفسي واجتماعي متخصصة. حالياً، لا توفر الحكومة العراقية مثل هذه المراكز، مما يترك الضحايا دون دعم كافٍ. وإن استغلال الأطفال عبر الإنترنت، مثل التحرش أو إجبارهم على إنتاج محتوى غير قانوني، يُفاقم المشكلة، حيث لا توجد برامج حماية مخصصة للأطفال، على الرغم من زيادة هذه الجرائم بنسبة ٢٧% في ٢٠٢٤. هذه الفجوات تتطلب تطوير آليات حماية اجتماعية تُركز على الفئات الضعيفة.

تُعد حملات التوعية إحدى الآليات المهمة للحماية، حيث أطلقت مديرية مكافحة الجرائم الإلكترونية في ٢٠٢٥ حملات لتثقيف الشباب حول مخاطر مشاركة المعلومات الشخصية عبر الإنترنت. ومع ذلك، تظل هذه الحملات محدودة في المناطق الريفية، حيث يفتقر السكان إلى الوعي الرقمي، مما يجعلهم أهدافاً سهلة للاحتيال. مما يُبرز الحاجة إلى توسيع نطاق التوعية. وإن نقص التثقيف الرقمي يُسهم في زيادة الجرائم مثل التزييف العميق، حيث يُستخدم الذكاء الاصطناعي لإنشاء صور أو فيديوهات مزيفة تُستخدم في الابتزاز أو التشهير. هذه التحديات تتطلب تكثيف حملات التوعية وإشراك المدارس والجامعات لتثقيف الأجيال الجديدة[٣٤].

تُشكل الجرائم الإلكترونية الناشئة، مثل التلاعب بالذكاء الاصطناعي، تحدياً كبيراً للحماية الجنائية، حيث لا تُغطي القوانين الحالية هذه الأنواع من الجرائم بشكل مباشر. على سبيل المثال، لا يوجد نص قانوني يُجرّم إنشاء فيديوهات مزيفة باستخدام الذكاء الاصطناعي، مما يُصعب إدانة الجناة. وإن ضعف البنية التحتية الرقمية في العراق يُسهل الاختراقات، حيث سجلت تقارير مركز الأمن السيبراني هجمات متكررة على مواقع حكومية في ٢٠٢٥، مما يُهدد الأمن الوطني. هذه التحديات تتطلب استثمارات في الأمن السيبراني وتطوير مختبرات رقمية لتحليل الأدلة، إلى جانب تشريعات جديدة تُعرّف الجرائم الناشئة وتحدد عقوباتها[٣٥].

من الناحية القانونية، يُعد تطوير تشريعات متخصصة ضرورة ملحة لتعزيز حماية الضحايا. ينبغي أن يشمل القانون الجديد تعريفات واضحة للجرائم مثل سرقة الهوية والتزييف العميق، مع عقوبات مشددة على الجناة في حالات استهداف الفئات الضعيفة. كما يجب أن يتضمن القانون آليات لتسهيل إثبات الأدلة الرقمية، مثل اعتماد بروتوكولات معيارية لحفظ البيانات. إضافة إلى ذلك، يُعد إنشاء صندوق تعويض للضحايا خطوة حاسمة لتغطية الأضرار، خاصة في ظل الخسائر المالية الكبيرة الناتجة عن لاحتيال، هذه الآلية ستُشجع الضحايا على الإبلاغ وتُخفف من أضرارهم النفسية والمادية[٣٦].

تُسهم الجهود التنفيذية، مثل إنشاء مركز الأمن السيبراني، في تحسين التنسيق بين الجهات الحكومية، لكن نقص الموارد البشرية يُعيق التقدم وإن القضاة يفتقرون إلى التدريب الكافي على التعامل مع الأدلة الرقمية، مما يؤدي إلى أحكام غير عادلة أو إفراج عن الجناة. تتطلب هذه التحديات برامج تدريب مستمرة للشرطة والقضاة، مع استثمار في المعدات التقنية لتحسين كفاءة التحقيقات[٣٧].

من الجوانب الإيجابية، ساهم انضمام العراق إلى اتفاقية بودابست في تعزيز التعاون الدولي، حيث ساعدت في إلقاء القبض على شبكات إجرامية دولية في ٢٠٢٤. ومع ذلك،

يتطلب تفعيل هذه الاتفاقية تحديث التشريعات المحلية لتتماشى مع المعايير الدولية، إلى جانب تحسين قنوات تبادل المعلومات. وإن إنشاء مراكز دعم نفسي واجتماعي يُعد ضرورة لدعم الضحايا، خاصة في ظل غياب هذه الخدمات حالياً. على سبيل المثال، يمكن أن تُساعد هذه المراكز في تقليل الوصمة الاجتماعية المرتبطة بالإبلاغ عن الجرائم، مما يُشجع الضحايا على المطالبة بحقوقهم.[٣٨]

الخاتمة

يُمثل الإطار القانوني للحماية من الجرائم الإلكترونية في العراق، المستند بشكل رئيسي إلى قانون العقوبات رقم (١١١) لسنة ١٩٦٩ وقانون الاتصالات رقم (٦٥) لسنة ٢٠٠٤، محاولة لمواجهة التحديات الرقمية المعاصرة، لكنه يظل غير كافٍ لتغطية الجرائم الإلكترونية المتطورة مثل سرقة الهوية أو التلاعب بالذكاء الاصطناعي. هذا النقص يُبرز الحاجة إلى تشريعات متخصصة توفر حماية شاملة للضحايا، خاصة مع تزايد مستخدمي الإنترنت وتُعد الحماية القانونية لضحايا الجرائم الإلكترونية ركيزة أساسية لتحقيق الأمن الرقمي والاستقرار الاجتماعي في العراق، حيث تُسبب هذه الجرائم أضراراً نفسية ومادية جسيمة، خاصة للفئات الضعيفة مثل النساء والأطفال. من خلال سن قوانين حديثة، تعزيز التعاون الدولي، وتوفير آليات تعويض ودعم نفسي، يمكن للعراق مواكبة التحديات الرقمية، مما يدعم بناء مجتمع رقمي آمن يتماشى مع أهداف التنمية المستدامة ويعزز الثقة في النظام القانوني.

النتائج:

١.يعاني الإطار القانوني العراقي من نقص تشريعات متخصصة للجرائم الإلكترونية، مما يحد من فعالية حماية الضحايا أمام الجرائم المتطورة.

٢.تُسهم مديرية مكافحة الجرائم الإلكترونية ومركز الأمن السيبراني في تحسين الرصد والتحقيق، لكن غياب قانون شامل يُضعف هذه الجهود.

٣.صعوبة إثبات الأدلة الرقمية ونقص التدريب للقضاة والشرطة تؤخر المحاكمات وتُقلل من تحقيق العدالة للضحايا.

٤.غياب آليات تعويض ودعم نفسي يُفاقم الأضرار الاجتماعية والنفسية للضحايا، خاصة في حالات الابتزاز الجنسي.

التوصيات:

١.سن قانون متخصص للجرائم الإلكترونية يغطي جميع الأنواع الناشئة، مع ضمان حماية حرية التعبير وفق المعايير الدولية.

٢.إنشاء صندوق تعويض لضحايا الجرائم الإلكترونية لتغطية الأضرار المادية والمعنوية، مع تحديد آليات واضحة للتعويض.

٣.تطوير برامج تدريب مكثفة للقضاة والمحققين حول التعامل مع الأدلة الرقمية لتسريع التحقيقات والمحاكمات.

٤.إطلاق حملات توعية وطنية لتثقيف المواطنين، خاصة في المناطق الريفية، حول مخاطر الجرائم الإلكترونية وطرق الوقاية.

٥.تعزيز التعاون الدولي من خلال تفعيل اتفاقية بودابست لمكافحة الجرائم الإلكترونية لتسهيل ملاحقة الجرائم عابرة الحدود.

الهوامش

[١] آلاء بنت سعيد بن ناصر حماية البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي رسالة ماجستير، ٢٠١٥، ص١٢

[٢] جيهان فقيه، حماية البيانات الشخصية في الإعلام الرقمي، مجلة العلوم الإنسانية، ع٧، ٢٠١٧، ص٣٢

[٣] أمين أعزان حماية البيانات الشخصية للمستهلك الإلكتروني، مجلة الاقتصاد والمستهلك، ع ٥,٦، ٢٠١٣، ص٣١

[٤] تامر محمد محمد صالح الحماية الجنائية للحق في المعلومات الرسمية (دراسة مقارنة)، مجلة القانون والاقتصاد، ملحق خاص العدد الثاني والتسعون، ٢٠١٩، ص٢٩

[٥] رضوان اسخيطة، التحقيق الجنائي الرقمي في ضوء قوانين حماية البيانات الشخصية، محلة الندوة للدراسات القانونية، ٢٦٦، ٢٠١٩، ص١١

[٦] حسن صادق المرصفاوى الإجرام والعقاب في مصر، منشأة المعارف بالإسكندرية، بدون سنه نشر ، ص٤٥

[٧] دراسة نقدية لقانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ ، ورشة عمل أعدها مركز بحوث القانون والتكنولوجيا كلية القانون بالجامعة البريطانية في مصر، اكتوبر ٢٠٢٠، ص٢٠

[٨] رمسيس بهنام الإجرام والعقاب علم الجريمة وعلم الوقاية والتقويم، منشأة المعارف بالإسكندرية، ١٩٧٨، ص١٤

[9] Zamroni Zamroni, Basri Basri Fakultas Hukum, Universitas Muhammadiyah Magelang, Magelang, Indonesia Legal Protection for Victims of Cybercrime as a Form of Transnational Crime, 2024

[١٠] هيثم أحمد محمود سلامة الحماية الجنائية لسوق الأوراق المالية: دراسة مقارنة رسالة دكتوراة، جامعة القاهرة، ٢٠١١.، ص١٦

[١١] غنام محمد غنام د. شيماء عبد الغنى عطا الله، مبادئ علم الإجرام، كلية الحقوق جامعة الزقازيق، ٢٠١٧، ص٣٦

[١٢] يحيى إبراهيم دهشان الحماية الجنائية لبيانات الشركات المقيدة في سوق الأوراق المالية – دراسة مقارنة رسالة دكتوراة، كلية الحقوق جامعة الزقازيق ٢٠٢٠، ص٥١

[١٣]يحيى إبراهيم دهشان المسئولية الجنائية عن جرائم الذكاء الاصطناعي مجلة الشريعة والقانون – كلية القانون جامعة الامارات العدد ٨٢، ابريل ٢٠٢٠، ص٣٥

[١٤]أسامة عبد الله فايد – الحماية الجنائية للحياة الخاصة وبنوك المعلومات دراسة مقارنة، دار النهضة العربية، الطبعة الثانية، ١٩٩٢.، ص٣٢

[١٥]أحمد شوقي عمر أبو خطوة – شرح الأحكام العامة لقانون العقوبات الجزء الأول – النظرية العامة للجريمة، دار النهضة العربية، القاهرة، ص٢٢

[١٦]سعيد عبد اللطيف حسن – إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت – دار النهضة العربية، الطبعة الأولى، القاهرة، ١٩٩٩.، ص٣٣

[١٧]سليمان عبد المنعم النظرية العامة لقانون العقوبات دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠٠، ص٤٤

[١٨]ربيع محمود الصغير – القصد الجنائي – دراسة تطبيقية على الجرائم المتعلقة بالانترنت رسالة دكتوراه كلية الحقوق جامعة عين شمس .٢٠١٥، ص٧٦

[١٩]جميل عبد الباقي الصغير – الانترنت والقانون الجنائي – الأحكام الموضوعية للجرائم المتعلقة بالانترنت، دار النهضة العربية، ١٩٩٩، ص٥٦

[٢٠]مروي السيد السيد الحصاوي – مبدأ العالمية في القانون الجنائي – رسالة دكتوراه، كلية الحقوق – جامعة المنصورة، ٢٠١٩.، ص٤١

[٢١]سالي وديع صبحي الاختبارات الإلكترونية عبر الشبكات، عالم الكتاب، القاهرة، ٢٠٠٥، ص٢١

[٢٢]صالح سليمان عبد العظيم – الأبعاد والتأثيرات الاجتماعية المرتبطة باستخدام الانترنت على الأسرة العربية، دراسة ميدانية على عينة من طالبات جامعة الإمارات العربية، ورقة مقدمة إلى مؤتمر واقع الأسرة في المجتمع، تشخيص للمشكلات واستكشاف لسياسات المواجهة، المنعقد بدار الضيافة، جامعة عين شمس، في الفترة من ٢٦ – ٢٨ سبتمبر ٢٠٠٤ ، كلية الآداب، قسم علم الاجتماع، مركز الدراسات المعرفية، المعهد العالي للفكر الإسلامي

[٢٣]عمر محمد أبو بكر يونس الجرائم الناشئة عن استخدام الانترنت الأحكام الموضوعية والجوانب الإجرائية رسالة دكتوراه، جامعة عين شمس دار النهضة العربية، القاهرة، ٢٠٠٤، ص١٨

[٢٤]علي حسن الطوالبه – مشروعية الدليل الالكتروني المستمد من التفتيش الجنائي دراسة مقارنة – بحث منشور عبر الانترنت مركز الإعلام الأمني البحرين، ٢٠٠٩، ص٢٧

[٢٥]نبيل جاد عزمي تكنولوجيا التعليم الإلكتروني، دار الفكر العربي، القاهرة، مصر ٢٠٠٨، ص٢٦

[٢٦]ربيع محمود الصغير – القصد الجنائي – دراسة تطبيقية على الجرائم المتعلقة بالانترنت رسالة دكتوراه كلية الحقوق جامعة عين شمس .٢٠١٥

[٢٧]علي حسن الطوالبه – مشروعية الدليل الالكتروني المستمد من التفتيش الجنائي دراسة مقارنة – بحث منشور عبر الانترنت مركز الإعلام الأمني البحرين، ٢٠٠٩.

[٢٨]ناول عبد الهادي – تقييم فعاليات المواجهة التشريعية لجرائم الانترنت مجلة العدل، المغرب، العدد ٣١ ، رجب ١٤٢٧، ص٣٩

[٢٩]جميل عبد الباقي الصغير – الانترنت والقانون الجنائي – الأحكام الموضوعية للجرائم المتعلقة بالانترنت، دار النهضة العربية، ١٩٩٩، ص٤١

[٣٠]ناول عبد الهادي – تقييم فعاليات المواجهة التشريعية لجرائم الانترنت مجلة العدل، المغرب، العدد ٣١ ، رجب ١٤٢٧، ص٣٥

[٣١]جميل عبد الباقي الصغير – الانترنت والقانون الجنائي – الأحكام الموضوعية للجرائم المتعلقة بالانترنت، دار النهضة العربية، ١٩٩٩، ص٦٧

[٣٢]أسامة عبد الله فايد – الحماية الجنائية للحياة الخاصة وبنوك المعلومات دراسة مقارنة، دار النهضة العربية، الطبعة الثانية، ١٩٩٢، ص١٩

[٣٣]سعيد عبد اللطيف حسن – إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت – دار النهضة العربية، الطبعة الأولى، القاهرة، ١٩٩٩. ص٣٩

[٣٤]سليمان عبد المنعم النظرية العامة لقانون العقوبات دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠٠.

[٣٥]ربيع محمود الصغير – القصد الجنائي – دراسة تطبيقية على الجرائم المتعلقة بالانترنت رسالة دكتوراه كلية الحقوق جامعة عين شمس .٢٠١٥

[36] 1. Porcedda, Maria Grazia, and David S. Wall. "Modelling the Cybercrime Cascade Effect in Data Crime." In Proceedings - 2021 IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2021, 161-77, 2021. https://doi.org/10.1109/EuroSPW54576.2021.00025.

[37] Onomrerhinor, Flora Alohan. "Eliminating Safe Havens for Transnational Cybercrimes in the African Continental Free Trade Area." Journal of Intellectual Property and Information Technology Law (JIPIT) 2, no. 1 (2022): 49-81. https://doi.org/10.52907/jipit.v2i1.206.

[٣٨]أحمد شوقي عمر أبو خطوة – شرح الأحكام العامة لقانون العقوبات الجزء الأول – النظرية العامة للجريمة، دار النهضة العربية، القاهرة

المراجع

الكتب العلمية

١.أحمد شوقي عمر أبو خطوة – شرح الأحكام العامة لقانون العقوبات الجزء الأول – النظرية العامة للجريمة، دار النهضة العربية، القاهرة

٢.أسامة عبد الله فايد – الحماية الجنائية للحياة الخاصة وبنوك المعلومات دراسة مقارنة، دار النهضة العربية، الطبعة الثانية، ١٩٩٢

٣.جميل عبد الباقي الصغير – الانترنت والقانون الجنائي – الأحكام الموضوعية للجرائم المتعلقة بالانترنت، دار النهضة العربية، ١٩٩٩

٤.حسن صادق المرصفاوى الإجرام والعقاب في مصر، منشأة المعارف بالإسكندرية، بدون سنه نشر

٥.رمسيس بهنام الإجرام والعقاب علم الجريمة وعلم الوقاية والتقويم، منشأة المعارف بالإسكندرية، ١٩٧٨

٦.سالي وديع صبحي الاختبارات الإلكترونية عبر الشبكات، عالم الكتاب، القاهرة، ٢٠٠٥

٧.سعيد عبد اللطيف حسن – إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت – دار النهضة العربية، الطبعة الأولى، القاهرة، ١٩٩٩.
٨.سليمان عبد المنعم النظرية العامة لقانون العقوبات دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠٠
٩.صالح سليمان عبد العظيم – الأبعاد والتأثيرات الاجتماعية المرتبطة باستخدام الانترنت على الأسرة العربية، دراسة ميدانية على عينة من طالبات جامعة الإمارات العربية، ورقة مقدمة إلى مؤتمر واقع الأسرة في المجتمع، تشخيص للمشكلات واستكشاف لسياسات المواجهة، المنعقد بدار الضيافة، جامعة عين شمس، في الفترة من ٢٦ – ٢٨ سبتمبر ٢٠٠٤ ، كلية الآداب، قسم علم الاجتماع، مركز الدراسات المعرفية، المعهد العالي للفكر الإسلامي
٢٠٠٩.١٠
١١.نبيل جاد عزمي تكنولوجيا التعليم الإلكتروني، دار الفكر العربي، القاهرة، مصر ٢٠٠٨

الرسائل العلمية:

١٢.آلاء بنت سعيد بن ناصر حماية البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي رسالة ماجستير، ٢٠١٥
١٣.ربيع محمود الصغير – القصد الجنائي – دراسة تطبيقية على الجرائم المتعلقة بالانترنت رسالة دكتوراه كلية الحقوق جامعة عين شمس .٢٠١٥
١٤.عمر محمد أبو بكر يونس الجرائم الناشئة عن استخدام الانترنت الأحكام الموضوعية والجوانب الإجرائية رسالة دكتوراه، جامعة عين شمس دار النهضة العربية، القاهرة، ٢٠٠٤
١٥.غنام محمد غنام د. شيماء عبد الغنى عطا الله، مبادئ علم الإجرام، كلية الحقوق جامعة الزقازيق، ٢٠١٧
١٦.مروي السيد السيد الحصاوي – مبدأ العالمية في القانون الجنائي – رسالة دكتوراه، كلية الحقوق – جامعة المنصورة، ٢٠١٩.
١٧.هيثم أحمد محمود سلامة الحماية الجنائية لسوق الأوراق المالية: دراسة مقارنة رسالة دكتوراة، جامعة القاهرة، ٢٠١١
١٨.يحيى إبراهيم دهشان الحماية الجنائية لبيانات الشركات المقيدة في سوق الأوراق المالية – دراسة مقارنة رسالة دكتوراة، كلية الحقوق جامعة الزقازيق ٢٠٢٠

المجلات :

١٩.أمين أعزان حماية البيانات الشخصية للمستهلك الإلكتروني، مجلة الاقتصاد والمستهلك، ع ٥,٦، ٢٠١٣
٢٠.تامر محمد محمد صالح الحماية الجنائية للحق في المعلومات الرسمية (دراسة مقارنة)، مجلة القانون والاقتصاد، ملحق خاص العدد الثاني والتسعون، ٢٠١٩
٢١.جيهان فقيه، حماية البيانات الشخصية في الإعلام الرقمي، مجلة العلوم الإنسانية، ع٧، ٢٠١٧
٢٢.دراسة نقدية لقانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ ، ورشة عمل أعدها مركز بحوث القانون والتكنولوجيا كلية القانون بالجامعة البريطانية في مصر، اكتوبر ٢٠٢٠

٢٣.رضوان اسخيطة، التحقيق الجنائي الرقمي في ضوء قوانين حماية البيانات الشخصية، محلة الندوة للدراسات القانونية، ٢٦٦، ٢٠١٩

٢٤.علي حسن الطوالبه – مشروعية الدليل الالكتروني المستمد من التفتيش الجنائي دراسة مقارنة – بحث منشور عبر الانترنت مركز الإعلام الأمني البحرين،

٢٥.ناول عبد الهادي – تقييم فعاليات المواجهة التشريعية لجرائم الانترنت مجلة العدل، المغرب، العدد ٣١ ، رجب ١٤٢٧

المراجع الأجنبية:

1.Zamroni Zamroni, Basri Basri ,Fakultas Hukum, Universitas Muhammadiyah Magelang, Magelang, Indonesia Legal Protection for Victims of Cybercrime as a Form of Transnational Crime, 2024

2.Onomrerhinor, Flora Alohan. "Eliminating Safe Havens for Transnational Cybercrimes in the African Continental Free Trade Area." Journal of Intellectual Property and Information Technology Law (JIPIT) 2, no. 1 (2022): 49-81. https://doi.org/10.52907/jipit.v2i1.206.

3.Porcedda, Maria Grazia, and David S. Wall. "Modelling the Cybercrime Cascade Effect in Data Crime." In Proceedings - 2021 IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2021, 161-77, 2021. https://doi.org/10.1109/EuroSPW54576.2021.00025.

References

1.Ahmed Shawqi Omar Abu Khatwa - Explanation of the General Provisions of the Penal Code, Part One - The General Theory of Crime, Dar Al-Nahda Al-Arabiya, Cairo

2.Osama Abdullah Fayad - Criminal Protection of Privacy and Information Banks: A Comparative Study, Dar Al-Nahda Al-Arabiya, Second Edition, 1992

3.Alaa Bint Saeed Bin Nasser - Protecting the Personal Data of Social Media Users, Master's Thesis, 2015

4.Amin Azan - Protecting the Personal Data of the Electronic Consumer, Economics and Consumer Journal, Issues 5 & 6, 2013

5.Tamer Mohamed Mohamed Saleh - Criminal Protection of the Right to Official Information (A Comparative Study), Law and Economics Journal, Special Supplement, Issue 92, 2019

6.Jamil Abdel-Baqi Al-Saghir - The Internet and Criminal Law - Substantive Provisions for Internet-Related Crimes, Dar Al-Nahda Al-Arabiya, 1999

7.Jihan Faqih - Protecting Personal Data in Digital Media, Journal of Human Sciences, Issue 7, 2017

8.Hassan Sadiq Al-Marsafawi - Crime and Punishment in Egypt Knowledge Establishment, Alexandria, no publication date.

9.A Critical Study of Personal Data Protection Law No. 151 of 2020, Workshop prepared by the Center for Law and Technology Research, Faculty of Law, British University in Egypt, October 2020.
10.Rabie Mahmoud Al-Saghir - Criminal Intent - An Applied Study on Internet-Related Crimes, PhD Dissertation, Faculty of Law, Ain Shams University, 2015.
11.Rabie Mahmoud Al-Saghir - Criminal Intent - An Applied Study on Internet-Related Crimes, PhD Dissertation, Faculty of Law, Ain Shams University, 2015.
12.Rabie Mahmoud Al-Saghir - Criminal Intent - An Applied Study on Internet-Related Crimes, PhD Dissertation, Faculty of Law, Ain Shams University, 2015.
13.Radwan Askhita, Digital Criminal Investigation in Light of Personal Data Protection Laws, Al-Nadwa Journal for Legal Studies, No. 266, 2019.
14.Ramsis Bahnam, Crime and Punishment: Criminology and Prevention and Rehabilitation, Knowledge Establishment, Alexandria. 1978
15.Sally Wadih Sobhi, Electronic Testing via Networks, Alam Al-Kitab, Cairo, 2005
16.Saeed Abdel Latif Hassan, Proving Computer Crimes and Crimes Committed via the Internet, Dar Al-Nahda Al-Arabiya, First Edition, Cairo, 1999.
17.Suleiman Abdel Moneim, General Theory of Criminal Law, Dar Al-Jami'a Al-Jadeeda Publishing House, Alexandria, 2000
18.Saleh Suleiman Abdel Azim, Social Dimensions and Impacts Associated with Internet Use on the Arab Family: A Field Study on a Sample of Female Students at the United Arab Emirates University, Paper presented at the Conference on the Reality of the Family in Society: Diagnosing Problems and Exploring Confrontation Policies, held at the Guest House, Ain Shams University, September 26-28, 2004, Faculty of Arts, Department of Sociology, Center for Cognitive Studies, Higher Institute of Islamic Thought
19. Ali Hassan Al-Tawalbeh, The Legality of Electronic Evidence Derived from Criminal Investigations: A Comparative Study, Research published online, Bahrain Security Media Center, 2009
20.Omar Muhammad Abu Bakr Younis, Crimes Arising from Internet Use: Substantive Provisions and Procedural Aspects, PhD Dissertation, Ain Shams University, Dar Al-Nahda Al-Arabiya, Cairo, 2004
21.Ghanem Muhammad Ghanem, Dr. Shaimaa Abdelghani Attallah, Principles of Criminology, Faculty of Law, Zagazig University, 2017
22.Marwa Elsayed Elsayed Elhasawy, The Principle of Universality in Criminal Law, PhD Dissertation, Faculty of Law, Mansoura University, 2019
23.Nawal Abdelhady, Evaluating the Effectiveness of Legislative Countermeasures Against Cybercrime, Al-Adl Journal, Morocco, Issue 31, Rajab 1427
24.Nabil Gad Azmy, E-Learning Technology, Dar Al-Fikr Al-Arabi, Cairo, Egypt, 2008

25. .Haitham Ahmed Mahmoud Salama, Criminal Protection of the Stock Market: A Comparative Study, PhD Dissertation, Cairo University, 2011
26. Yahya Ibrahim Dahshan, Criminal Protection of Data of Companies Listed on the Stock Market: A Comparative Study, PhD Dissertation, Faculty of Law, Zagazig University, 2020