

إطار تشريعي مقترح للحد من الجرائم الإلكترونية وتعزيز الأخلاقيات الرقمية في العراق

A Proposed Legislative Framework to Reduce Cybercrimes and Promote Digital Ethics in Iraq

- الاستاذ الدكتور: طلال ناظم الزهيري¹

- قسم المعلومات وتقنيات المعرفة/ الجامعة المستنصرية- العراق

تاريخ الاستقبال: 2025/01/08 تاريخ القبول: 2025/04/15 تاريخ النشر: 2025/06/12

ملخص:

مع التطور التكنولوجي المتنامي والاعتماد المتزايد على الإنترنت، أصبحت الجرائم الإلكترونية والأخلاقيات الرقمية من أبرز التحديات التي تواجه المجتمعات الرقمية وتهدد أمنها. تهدف هذه الدراسة إلى تقديم إطار تشريعي مقترح يساهم في الحد من الجرائم الإلكترونية في العراق وتعزيز قيم الأخلاقيات الرقمية. تنطلق الدراسة من استعراض تجارب الدول الأخرى في وضع قوانين لمكافحة الجرائم الإلكترونية، ثم تنتقل لتحليل التشريعات العربية القائمة بهدف فهم نقاط القوة والضعف فيها. كما تسلط الضوء على التحديات المرتبطة بحماية الحقوق الرقمية ومكافحة الأنشطة غير القانونية في الفضاء الرقمي. تقدم الدراسة مجموعة من التوصيات العملية لصياغة تشريعات حديثة وشاملة تواكب التطورات التكنولوجية، مع تعزيز الأمن السيبراني وضمان احترام خصوصية وحقوق المواطنين العراقيين.

الكلمات المفتاحية: الجرائم الإلكترونية، الأخلاقيات الرقمية، التشريعات العراقية، الأمن السيبراني، الحقوق الرقمية

Abstract:

With rapid technological advancements and growing reliance on the internet, cybercrimes and digital ethics have become some of the most pressing challenges facing digital communities and threatening their security. This study aims to propose a legislative framework to curb cybercrimes in Iraq while fostering digital ethics. It begins by reviewing the experiences of other countries in drafting cybercrime laws, followed by an analysis of existing Arab legislations to identify their strengths and weaknesses. The study also highlights challenges related to protecting digital rights and combating illegal activities in the digital realm. Practical recommendations are provided for crafting modern,

¹ - الإيميل: drazzuhairi@gmail.com

إطار تشريعي مقترح للحد من الجرائم الإلكترونية وتعزيز الأخلاقيات الرقمية في العراق

comprehensive legislation that aligns with technological advancements, enhances cybersecurity, and ensures the privacy and rights of Iraqi citizens are safeguarded.

Keywords: Cybercrimes, Digital Ethics, Iraqi Legislation, Cybersecurity, Digital Rights

1. المقدمة

مع التطور المتنامي في التطبيقات التكنولوجية والاعتماد المتزايد على الإنترنت، أصبحت الجرائم الإلكترونية وانتهاكات الأخلاقيات الرقمية تعد من التحديات الرئيسية التي تواجه المجتمعات الحديثة. ومع ذلك، وفي سياق الحالة العراقية، تعاني التشريعات الحالية من قصور في معالجة هذه القضايا، مما يثير تساؤلات حول فعاليتها في حماية الحقوق الرقمية للأفراد والمؤسسات وقدرتها على مواجهة المخاطر المتزايدة في الفضاء الرقمي.

تستند هذه الدراسة إلى الحاجة الملحة لتطوير إطار تشريعي شامل ومتكامل في العراق يحقق التوازن بين حماية الحقوق الرقمية للمواطنين ومكافحة الجرائم الإلكترونية. تهدف الدراسة إلى تحليل القوانين العراقية الحالية ومدى كفايتها للحد من الجرائم الإلكترونية والأخلاقيات الرقمية للكشف عن نقاط القوة والضعف والفجوات التي تحتاج إلى معالجة. كما تسلط الضوء على طبيعة الجرائم الإلكترونية وآليات ارتكابها، مما يساعد في فهم أعمق للتحديات القائمة.

بالإضافة إلى ذلك، تستفيد الدراسة من استعراض التجارب الناجحة للدول العربية التي طورت تشريعات رقمية متقدمة، واستخلاص الدروس المستفادة منها وتكييفها لتناسب مع السياق العراقي. تسعى الدراسة في النهاية إلى تصميم إطار تشريعي متكامل يعتمد على التحليل والمقارنة، ويشمل مبادئ واضحة وقواعد تفصيلية يمكن تطبيقها لتحديث التشريعات العراقية.

تكمن أهمية هذه الدراسة في ارتباطها بأحد أبرز التحديات التي تواجه العراق اليوم، وهو تحقيق الأمن المجتمعي الرقمي في ظل التحول الرقمي الواسع. فالجرائم الإلكترونية لا تهدد الأفراد فقط، بل تؤثر أيضًا على المؤسسات والبنية التحتية الرقمية، مما يجعل تطوير تشريعات متقدمة ضرورة مطلقة لحماية المجتمع وضمان استدامة التطور الرقمي.

2. الأخلاقيات الرقمية

يشير (عبد الله، 2022) إلى أن مفهوم الأخلاقيات الرقمية هي عبارة عن مجموعة من المبادئ والقواعد التي تُنظم السلوك الرقمي للأفراد والمؤسسات عند استخدام الوسائل الإلكترونية مثل الحواسيب والهواتف الذكية،

الأستاذ الدكتور: طلال ناظم الزهيري

والإنترنت. حيث تهدف هذه القواعد إلى منع الإضرار بالآخر و تعزيز السلوك المسؤول و ضمان احترام الحقوق والقيم الإنسانية. ويضيف الى إن بعض المصادر قد تتوسع في مفهوم الأخلاقيات الرقمية لتشمل إجراءات وممارسات تقنية تهدف إلى حماية المعلومات و ضمان استخدامها بطريقة أخلاقية، مع الالتزام التام بعدم انتهاك الخصوصية أو التعدي على القيم العامة.

ويتفق مع هذا التعريف كل من (الأحمد، عمر، و هديب، 2017) بالقول إن مفهوم الأخلاقيات الرقمية، يعكس المبادئ التي تحكم التفاعل بين البشر والتكنولوجيا الحديثة. مع تركيز على أهمية فهم هذه العلاقة لتحسين الوعي بأبعادها وتأثيراتها. من خلال وضع إطار شامل للأخلاقيات الرقمية عن طريق دراسة النصوص والعالم الافتراضي لتحديد القواعد التي تنظم السلوك في البيئة الرقمية لضمان استخدام المصادر الرقمية بشكل مسؤول، مع مراعاة الفرق بين الاستخدامات العامة والخاصة.

كما يؤكد الباحثين على أهمية تعزيز ثقافة الحوار واحترام التنوع في الآراء، مع التحذير من الانتهاكات الأخلاقية التي قد تنتج عن سوء استخدام التكنولوجيا، مثل الرسائل المسيئة أو الاستغلال غير الأخلاقي للبرامج الرقمية والتي يفسرها (منصوري، 2014) ان أخلاقيات الأفراد الواقعية في تواصلهم غالبا ما تكون مرآة لممارساتهم الاخلاقية في الواقع الافتراضي، إلا أن البعض قد يلجأ إلى التخفي وراء هويات وهمية، مما يتيح لهم التصرف في الفضاء الرقمي من دون التقيد بالضوابط الأخلاقية المعتادة. ينتج عن ذلك إزعاج الآخرين من خلال الرسائل الإلكترونية أو نشر الصور، وأحيانا يصل الأمر إلى التشهير، سواء بدافع الانتقام أو لإثارة الإزعاج، مما يؤدي إلى الإخلال بالقيم الاجتماعية. حيث تعتبر هذه السلوكيات تحدياً رئيسياً يواجه أفراد المجتمع الافتراضي وتاثر بشكل مباشر على طبيعة التواصل في العصر الرقمي.

ومن منظوري الشخصي اجد ان مفهوم الاخلاق الرقمية لا يمكن فصله عن مفهوم الاخلاق بشكل عام الا في حدود اختلاف البيئة التي تمارس فيها. حيث يتسع نطاق البيئة الرقمية لتتداخل فيه الممارسة الاخلاقية مع ثقافات وعادات و تقاليد مختلفة كليا او جزئيا. بالتالي المحافظة على المسؤولية الاخلاقية للفرد تكون اكثر تعقيدا في الفضاء الرقمي مقارنة مع المسؤولية الاخلاقية للفرد في حدود مجتمعه الضيق. وهذا الامر يدعو الى اهمية وجود موثيق تضبط مسار الممارسات الاخلاقية في البيئة الرقمية.

3. الجرائم الالكترونية

في ظل التقدم التكنولوجي الكبير الذي يشهده العالم اليوم، ومع الانتشار الواسع لاستخدام الإنترنت، بدأت الفجوة الرقمية بين المجتمعات تتقلص بشكل ملحوظ. هذا التحول التكنولوجي الواسع أسهم في إتاحة فرص كبيرة للبشرية للوصول إلى المعلومات، لكنه في الوقت نفسه فتح المجال لظهور تحديات جديدة، أبرزها الجرائم

إطار تشريعي مقترح للحد من الجرائم الإلكترونية وتعزيز الاخلاقيات الرقمية في العراق

الإلكترونية. ورغم أن هذا المصطلح أصبح شائعاً كما أشار (Gordon, 2006)، إلا أن تحديده بدقة لا يزال يشكل عقبة، حيث يفتقر إلى تعريف شامل للأدوات والبرمجيات التي تسهم في ارتكاب هذه الجرائم. وتتمثل إحدى خصائص الجريمة الإلكترونية، شأنها شأن الجريمة التقليدية، في تنوعها واختلاف بيئاتها وسيناريوهاها. فبعض التعريفات الشائعة تركز على الهجمات على البيانات أو التعديات على حقوق الملكية الفكرية، في حين يدعو البعض إلى توسيع نطاق التعريف ليشمل أنشطة أخرى مثل الاحتيال والوصول غير المصرح به، وترويج المواد الإباحية. لكن على الرغم من تباين الآراء حول تعريف هذا المصطلح، إلا أن هناك إجماعاً على أن الجرائم الإلكترونية باتت تشكل تهديداً حقيقياً للمعلومات الشخصية والمؤسسية، التي أصبحت عرضة للاختراق والاستغلال.

وبالنظر إلى التطور المستمر في أدوات وأساليب تنفيذ الجرائم الإلكترونية، يتضح حجم التحديات التي تواجه المجتمعات في حماية بياناتها وأنظمتها. إذ لم تقتصر الجرائم الإلكترونية على اختراق الأجهزة أو سرقة البيانات فحسب، بل تطورت لتشمل أشكالاً معقدة مثل الابتزاز الإلكتروني، التجسس السيبراني، والتلاعب بالرأي العام عبر منصات التواصل الاجتماعي. والأكثر خطورة هو أن هذه الجرائم تتجاوز الحدود الجغرافية، مما يجعل مكافحتها مسؤولية مشتركة تتطلب تضامناً الجهود على الصعيدين الدولي والإقليمي. في هذا السياق نلخص المفهوم بالقول إلى أن الجرائم الإلكترونية تشمل مجموعة من الأنشطة غير القانونية التي تُرتكب باستخدام التكنولوجيا والإنترنت. وفيما يلي بعض الأنواع الرئيسية لهذه الجرائم مع تعريف مختصر لكل منها:

1.3: القرصنة الإلكترونية (Hacking):

القرصنة الإلكترونية هي عملية اختراق الأنظمة الحاسوبية أو الشبكات بهدف الوصول غير المصرح به إلى البيانات أو المعلومات المخزنة. تشمل هذه العملية تقنيات متعددة لاستغلال الثغرات الأمنية في البرمجيات أو الأجهزة بهدف الوصول إلى الأنظمة والبيانات دون إذن من أصحابها. يمكن للقرصنة الإلكترونية تنفيذ هذه الهجمات لأغراض متعددة مثل السرقة المالية، التلاعب بالبيانات، التجسس، أو حتى تخريب الأنظمة بشكل كامل. تنقسم القرصنة إلى أنواع متعددة حسب الغرض والأسلوب المستخدم. على سبيل المثال، يمكن أن تشمل الهجمات التي تستهدف المؤسسات المالية لسرقة الأموال أو بيانات العملاء، أو الهجمات التي تهدف إلى سرقة الملكية الفكرية للشركات الكبرى. بعض القرصنة قد يهدفون إلى نشر الفوضى أو التأثير في الأنظمة السياسية عن طريق الهجمات الإلكترونية التي تستهدف البنى التحتية الحيوية (Sukhai, 2004).

2.3: سرقة الهوية (Identity Theft):

سرقة الهوية هي عملية غير قانونية يتنكر فيها الجاني في شخصية شخص آخر من أجل استخدام معلوماته الشخصية لتحقيق مكاسب مالية أو لارتكاب جرائم أخرى. يتضمن هذا النوع من الجرائم الحصول على

الأستاذ الدكتور: طلال ناظم الزهيري

معلومات حساسة مثل الأسماء، أرقام الضمان الاجتماعي، أرقام بطاقات الائتمان، أو تفاصيل الحسابات المصرفية، وغالبًا ما يتم ذلك عن طريق وسائل إلكترونية مثل التصيد الاحتيالي (*Phishing*) أو اختراق الأنظمة. تُستخدم المعلومات المسروقة في العديد من الأغراض، مثل فتح حسابات مصرفية جديدة باسم الضحية، إجراء عمليات شراء غير مصرح بها، أو الحصول على قروض دون علم صاحب الهوية. في بعض الحالات، يمكن أن تشمل سرقة الهوية أيضًا التلاعب بالأنظمة الحكومية أو التأثير على سمعة الضحية. من الجدير بالذكر أن جرائم سرقة الهوية تمثل تهديدًا خطيرًا لكل من الأفراد والشركات. فعلى الرغم من الجهود المبذولة لزيادة الوعي حول حماية المعلومات الشخصية، إلا أن التقنيات المستخدمة في سرقة الهوية تزداد تطورًا، مما يزيد من صعوبة اكتشاف الجرائم في مراحلها المبكرة (Adil, 2020).

3.3: الاحتيال الإلكتروني (*Online Fraud*):

الاحتيال الإلكتروني هو نوع من الجرائم التي يتم فيها استخدام الإنترنت لارتكاب عمليات احتيال بهدف الحصول على أموال أو معلومات حساسة من الأفراد أو المؤسسات بطريقة غير قانونية. يتم هذا الاحتيال من خلال تقنيات وأساليب متنوعة مثل التصيد الاحتيالي (*Phishing*)، المواقع المزيفة، وعمليات البيع الوهمية. كما يمكن أن يشمل أيضًا الاحتيال عبر المزادات الإلكترونية أو عمليات الدفع عبر الإنترنت التي تهدف إلى سرقة المال أو البيانات. تشمل أمثلة الاحتيال الإلكتروني (Cross, 2019):

1. **التصيد الاحتيالي (*Phishing*):** حيث يتم إرسال رسائل بريد إلكتروني أو رسائل نصية تحتوي على روابط مزيفة تهدف إلى جمع معلومات حساسة من الضحية مثل كلمات المرور وأرقام الحسابات.
2. **الاحتيال عبر البطاقات الائتمانية:** حيث يقوم الجاني بسرقة تفاصيل البطاقة الائتمانية للمستخدم عبر الإنترنت واستخدامها بشكل غير قانوني.
3. **المزادات الوهمية:** تتضمن إنشاء مواقع مزادات إلكترونية مزيفة لبيع سلع غير موجودة أو للحصول على أموال من المشتريين بدون تسليم المنتج.

تزداد حالات الاحتيال الإلكتروني بشكل كبير نتيجة للانتشار الواسع للإنترنت والتجارة الإلكترونية، حيث يعتمد العديد من الأفراد والشركات على الإنترنت للتفاعل المالي. وهذا يفرض تحديات كبيرة على السلطات الأمنية لمكافحة هذه الأنشطة وتوعية المستخدمين حول كيفية حماية أنفسهم من هذه الأنواع من الجرائم.

4.3: الابتزاز الإلكتروني (*Cyber Extortion*):

الابتزاز الإلكتروني هو نوع من الجرائم الإلكترونية يتم من خلاله تهديد الأفراد أو المؤسسات بكشف معلومات سرية أو نشرها أو تعطيل أنظمتهم الإلكترونية ما لم يتم دفع فدية أو الامتثال لطلب معين. يتمثل هذا

إطار تشريعي مقترح للحد من الجرائم الإلكترونية وتعزيز الاخلاقيات الرقمية في العراق

النوع من الجرائم في تهديد الضحايا باستخدام وسائل إلكترونية مثل البريد الإلكتروني، الرسائل النصية، أو حتى المواقع الإلكترونية. يُعد الابتزاز الإلكتروني أحد أخطر الجرائم السيبرانية، حيث يترتب عليه تأثيرات جسيمة على الأفراد والشركات على حد سواء. تتعدد أساليب الابتزاز الإلكتروني وتشمل (Salvi, 2016) :

1. هجمات الفدية: (*Ransomware*) حيث يقوم الجاني بإصابة أنظمة الضحية ببرمجيات خبيثة تُقيد الوصول إلى البيانات أو الأنظمة، ويطلب بعدها دفع فدية مقابل استعادة الوصول.
2. التهديد بكشف معلومات حساسة: حيث يهدد الجاني بنشر بيانات أو صور خاصة أو محتوى حساس للضحية، مثل الصور الخاصة أو رسائل البريد الإلكتروني، إذا لم يتم دفع فدية.
3. الابتزاز عبر الإنترنت: (*Cyberstalking*) قد يشمل هذا النوع من الابتزاز تهديد الضحية بنشر أو إفشاء معلومات خاصة عبر وسائل التواصل الاجتماعي أو المنتديات إذا لم يتم تلبية الطلبات.

5.3: التجسس الإلكتروني (*Cyber Espionage*):

التجسس الإلكتروني هو نوع من الجرائم الإلكترونية التي تشمل استخدام وسائل الإنترنت والتكنولوجيا الحديثة للتسلل إلى أنظمة الحاسوب أو الشبكات من أجل الحصول على معلومات حساسة أو سرية، والتي قد تتعلق بالحكومات أو الشركات أو الأفراد. يهدف الجاني في هذه الحالة إلى جمع البيانات بشكل غير قانوني بغرض استخدامها في أغراض التجسس أو لبيعها إلى أطراف أخرى، سواء كانت دولاً أو شركات منافسة. غالباً ما يرتبط هذا النوع من الجرائم بالصراع الجيوسياسي أو التنافس التجاري، ويُعتبر من أكثر أنواع الجرائم الإلكترونية تعقيداً وأشدّها خطراً. تتراوح أهداف التجسس الإلكتروني من سرقة أسرار صناعية وتكنولوجية، إلى اختراق الشبكات الحكومية لجمع معلومات استخباراتية. يتم تنفيذ هذه الهجمات باستخدام تقنيات متقدمة، مثل البرمجيات الخبيثة (*Malware*) أو الهجمات المنهجية ضد نقاط ضعف الأنظمة، بهدف اختراق الشبكات الحساسة. أبرز أشكال التجسس الإلكتروني تشمل (Kara, 2021) :

1. التجسس على الحكومات: (*Government Cyber Espionage*) حيث تقوم الدول باستخدام هجمات سيبرانية للحصول على معلومات استراتيجية من حكومات أخرى، مثل الأسرار العسكرية أو السياسية.
2. التجسس الصناعي: (*Industrial Espionage*) وهو استهداف الشركات للحصول على تقنيات أو استراتيجيات تجارية سرية بهدف استخدامها لصالح منافس أو بيعها.
3. التجسس على الأفراد: (*Personal Espionage*) في بعض الأحيان، يقوم المهاجمون بالتسلل إلى أجهزة الأفراد للحصول على معلومات شخصية، مثل الملفات المصرفية أو البيانات الصحية.

6.3: التنمر الإلكتروني (Cyberbullying):

التنمر الإلكتروني هو نوع من أنواع الجرائم الإلكترونية التي تحدث عندما يستخدم فرد أو مجموعة من الأفراد التكنولوجيا، وخاصة الإنترنت ووسائل التواصل الاجتماعي، للتسلط على شخص آخر أو تهديده أو مضايقته بشكل مستمر. يتم هذا النوع من التنمر عبر إرسال رسائل مسيئة، نشر محتوى ضار، أو التهديد العلني عبر الشبكات الرقمية، مما يسبب ألماً نفسياً وعاطفياً للضحية. يعتبر التنمر الإلكتروني من أكثر أشكال الجرائم الإلكترونية شيوعاً بين الشباب والمراهقين، ولكنه يمكن أن يحدث في أي فئة عمرية. يأخذ التنمر الإلكتروني عدة أشكال، مثل (Li, 2025):

1. الإهانة والتهديد: نشر تعليقات سلبية أو تهديدات عبر الرسائل النصية أو وسائل التواصل الاجتماعي بهدف إثارة الخوف والقلق.
2. النشر المغرض: نشر صور أو معلومات خاصة بالضحية بهدف تحقيرها أو تشويه سمعتها.
3. الاستبعاد الرقمي: عزل الضحية من المجموعات الرقمية أو المنتديات أو منصات التواصل الاجتماعي، مما يعزز الشعور بالوحدة والانعزال.
4. التشهير الإلكتروني: نشر أكاذيب أو إشاعات عبر الإنترنت بهدف تشويه صورة الضحية.
5. الابتزاز الإلكتروني: تهديد الضحية بنشر معلومات حساسة أو صور خاصة إذا لم تمتثل لمطالب الجاني.

7.3: البرمجيات الخبيثة (Malware):

عبارة عن برامج مصممة خصيصاً لإلحاق الضرر أو تعطيل الأنظمة الحاسوبية أو سرقة البيانات أو الوصول غير المصرح به إلى الشبكات. تعتبر البرمجيات الخبيثة من أخطر التهديدات التي تواجه الأمن السيبراني، حيث يمكن أن تضر بالأفراد والشركات على حد سواء من خلال تدمير البيانات أو التجسس على الأنشطة أو إحداث أضرار فنية في الأجهزة. وتنوع البرمجيات الخبيثة في شكلها وطبيعتها، ومن أبرز أنواعها: (Abusitta, 2021)

1. الفيروسات (Viruses): هي برامج تنتقل من جهاز إلى آخر وتقوم بتكرار نفسها داخل الملفات أو الأنظمة، مما يتسبب في تدمير البيانات أو تعطل النظام.
2. الدودة (Worms): تشبه الفيروسات، لكنها لا تحتاج إلى ملف ضار لتنتشر. يمكن للدودة أن تنتقل عبر الشبكة من جهاز إلى آخر بشكل مستقل، وتسبب التهام عرض النطاق الترددي وموارد النظام.
3. حصان طروادة (Trojan Horses): هي برامج تبدو غير ضارة لكنها تحتوي على تعليمات خبيثة تسمح للمهاجم بالوصول إلى النظام دون علم المستخدم. يتم عادةً تحميلها من الإنترنت عبر روابط أو ملفات مشبوهة.

إطار تشريعي مقترح للحد من الجرائم الإلكترونية وتعزيز الاخلاقيات الرقمية في العراق

4. البرمجيات التجسسية (*Spyware*): تهدف إلى مراقبة نشاطات المستخدمين على الإنترنت مثل تسجيل الكلمات المفتاحية أو تجميع البيانات الشخصية مثل كلمات السر والمعلومات المالية.
5. البرمجيات الإعلانية (*Adware*): هي برامج تعرض إعلانات مزعجة أو غير مرغوب فيها للمستخدمين، وقد تحتوي على برامج تجسس أو مكونات خبيثة أخرى تؤثر على أداء النظام.
6. برامج الفدية (*Ransomware*): هو نوع من البرمجيات الخبيثة التي تقوم بتشفير ملفات المستخدم وتطالب بفدية لإعادة الوصول إليها. هذا النوع من البرمجيات يسبب أضرارًا مالية جسيمة للمستخدمين والشركات.

8.3: الاعتداء على الخصوصية (*Privacy Violations*):

مع التوسع الهائل في استخدام الإنترنت، أصبح جمع البيانات الشخصية ومشاركتها أمرًا شائعًا، مما يعرض الأفراد إلى مخاطر فقدان الخصوصية والاحتفاظ بالبيانات الحساسة بعيدًا عن أعين المتطفلين.

تتنوع أشكال الاعتداء على الخصوصية وتختلف وفقًا للوسائل والأساليب المتبعة. ومن أبرز هذه الأنواع (5 Common Privacy Violations, 2024):

1. المراقبة الرقمي (*Digital Surveillance*): يشمل مراقبة الأنشطة الشخصية عبر الإنترنت مثل تتبع الموقع الجغرافي، مراقبة سلوكيات التصفح، أو جمع بيانات حساسة عبر منصات التواصل الاجتماعي.
2. جمع البيانات بدون إذن (*Unauthorized Data Collection*): يقوم بعض المواقع أو التطبيقات بجمع معلومات عن المستخدمين دون علمهم أو إذنهم، مثل جمع التفاصيل الشخصية من خلال الكوكيز أو تتبع الأنشطة عبر الإنترنت، وغالبًا ما يتم ذلك بغرض الإعلان الموجه أو البيع.
3. الاختراقات (*Hacking*): للوصول إلى بيانات شخصية: يشمل الوصول غير القانوني إلى حسابات المستخدمين أو سرقة البيانات المخزنة عبر الشبكات أو الأجهزة بهدف استخدامها لأغراض احتيالية أو تجارية.
4. التسريب المتعمد للمعلومات (*Data Breaches*): يتمثل في نشر أو تسريب البيانات الشخصية إلى أطراف غير مصرح بها، سواء عن طريق الاختراقات أو خطأ من قبل الشركات أو الأفراد المسؤولين عن حفظ هذه البيانات.
5. التصوير والتنصت على المحادثات (*Eavesdropping and Surveillance*): يشمل التنصت على المحادثات الشخصية أو استخدام تقنيات مثل كاميرات المراقبة أو الميكروفونات لاستخراج معلومات حساسة دون إذن.

التلاعب في الرأي العام هو استخدام تقنيات وأدوات عبر الإنترنت، وخاصة منصات التواصل الاجتماعي، للتأثير على مواقف وآراء الأفراد أو الجماهير في قضايا معينة. هذا النوع من الجرائم الإلكترونية يعد من أخطر التهديدات التي تواجه المجتمعات الحديثة، حيث يتم استغلال القوة الكبيرة التي توفرها وسائل التواصل الاجتماعي للوصول إلى جمهور واسع من الأفراد في وقت قصير. تشمل أساليب التلاعب في الرأي العام مجموعة من الممارسات التي تهدف إلى تغيير أو تشكيل الرأي العام لصالح جهة أو طرف معين (عبس، 2024). ومن أبرز أشكال هذه الممارسات:

1. **الروبوتات (Bots) وحسابات وهمية:** تُستخدم الحسابات الوهمية أو الروبوتات للتفاعل مع المحتوى على منصات التواصل الاجتماعي، من خلال نشر تعليقات أو إعادة نشر منشورات بغرض زيادة الانتشار أو خلق انطباع زائف بأن هناك تأييد جماهيري لفكرة أو قضية معينة. الروبوتات قد تكون مبرمجة أيضًا لرفع ترتيب بعض الموضوعات في الخوارزميات الخاصة بالشبكات الاجتماعية، مما يساهم في توجيه الانتباه إليها.

2. **التضليل الإعلامي (Misinformation) و الأخبار الكاذبة (Fake News):** يتم نشر معلومات مغلوطة أو مُحَرَّفَة تهدف إلى نشر الفوضى أو تشويه الحقائق، سواء بهدف التأثير على الانتخابات السياسية، أو تغيير وجهات نظر الأفراد تجاه قضايا معينة مثل الأزمات الصحية أو الاجتماعية (كيلاني، 2015).

3. **التوجهات المزيفة (Fake Trends):** يمكن استخدام تقنيات مثل إضافة هاشتاغات كاذبة أو ترتيب محتوى بشكل مغلوطة بحيث يبدو أنه يحظى بتفاعل كبير، بينما في الواقع يتم التلاعب في بيانات التفاعل، وهو ما يخلق انطباعًا زائفًا بوجود دعم جماهيري لقضية ما.

4. **الاستهداف السياسي والتلاعب الانتخابي:** يتم استخدام منصات التواصل الاجتماعي للتأثير في الآراء السياسية للمواطنين في إطار انتخابات معينة، وذلك من خلال نشر محتوى مؤيد لأحزاب أو مرشحين سياسيين، أو نشر شائعات عن الخصوم السياسيين بهدف تشويه صورتهم. وتعد الحملات الانتخابية عبر الإنترنت نموذجًا حيويًا لهذا النوع من التلاعب.

5. **المحتوى المثير والمستفز (Clickbait):** يقوم بعض الأفراد أو المؤسسات بنشر عناوين أو محتوى مغرٍ بهدف جذب الانتباه وزيادة التفاعل، حتى لو كان هذا المحتوى غير دقيق أو يهدف إلى إثارة الجدل أو نشر الانقسامات.

6. **استغلال البيانات الشخصية:** في بعض الحالات، يتم جمع بيانات شخصية من خلال منصات التواصل الاجتماعي واستخدامها للتأثير في القرارات أو الآراء السياسية أو الاقتصادية للأفراد. قد تُستخدم هذه

إطار تشريعي مقترح للحد من الجرائم الإلكترونية وتعزيز الاخلاقيات الرقمية في العراق

البيانات في حملات دعائية موجهة، حيث يتم توجيه رسائل دعائية حسب اهتمامات المستخدمين أو موافقهم.

10.3: الجرائم المالية الإلكترونية (Cyber Financial Crimes):

الجرائم المالية الإلكترونية هي الأنشطة غير القانونية التي تُرتكب باستخدام الإنترنت أو التكنولوجيا الرقمية بهدف الحصول على أموال أو تحقيق مكاسب مالية غير مشروعة. هذه الجرائم تعد من أبرز التهديدات التي تواجه الأنظمة المالية والبنوك والأفراد على حد سواء، نظرًا لما تتضمنه من تقنيات متطورة وأساليب متعددة لاستغلال الثغرات في الأنظمة المالية الرقمية. تشمل الجرائم المالية الإلكترونية مجموعة واسعة من الأنشطة التي تهدف إلى الاحتيال أو السرقة أو التلاعب في المعاملات المالية عبر الإنترنت. ومن أبرز هذه الجرائم: (Michel, 2008)

1. الاحتيال المصرفي عبر الإنترنت: (*Online Banking Fraud*) يتضمن هذا النوع من الجرائم عمليات الاحتيال التي تستهدف حسابات الأفراد في البنوك عبر الإنترنت، مثل سرقة بيانات الدخول أو استخدام أساليب الخداع مثل "Phishing" للحصول على معلومات حساسة مثل أرقام الحسابات وكلمات المرور.
2. الاحتيال في بطاقات الائتمان: (*Credit Card Fraud*) يتم من خلاله سرقة أو استنساخ بيانات بطاقات الائتمان أو الخصم الخاصة بالأفراد، ثم استخدامها لإجراء عمليات شراء غير قانونية عبر الإنترنت أو سحب أموال.
3. التلاعب في سوق الأوراق المالية: (*Stock Market Manipulation*) يتمثل هذا النوع من الجرائم في التلاعب بأسعار الأسهم أو الأوراق المالية عبر الإنترنت من خلال نشر معلومات مغلوطة أو استخدام تقنيات "التداول عالي التردد" بهدف التلاعب بالأسواق المالية لتحقيق مكاسب غير مشروعة.
4. النقد الرقمي والتعاملات بالعملات المشفرة: (*Cryptocurrency Fraud*) هذه الجريمة تتضمن استغلال تقنيات العملات الرقمية مثل "البيتكوين" في عمليات احتيال. قد تشمل هذه الجرائم سرقة محافظ العملات الرقمية أو إنشاء أنظمة استثمار وهمية لجذب المستثمرين. (Kutera, 2022)
5. الابتزاز المالي الإلكتروني: (*Cyber Extortion for Money*) تتضمن هذه الجريمة تهديدات بالقيام بعمليات ضارة أو نشر معلومات حساسة عبر الإنترنت، مما يدفع الضحية لدفع مبالغ مالية لتجنب هذه التهديدات.
6. الهجمات على أنظمة الدفع: (*Payment Systems Attacks*) يشمل ذلك الهجمات الإلكترونية التي تستهدف أنظمة الدفع الرقمية مثل تلك الخاصة بالتجارة الإلكترونية، حيث يمكن للمهاجمين سرقة الأموال أو بيانات المعاملات الحساسة من أنظمة الدفع.

7. غسيل الأموال عبر الإنترنت (*Money Laundering via the Internet*) يتضمن هذا النوع من الجرائم استخدام الإنترنت والتكنولوجيا الرقمية لإخفاء مصدر الأموال غير المشروعة من خلال سلاسل من المعاملات المالية المعقدة باستخدام خدمات التحويل الإلكتروني أو العملات المشفرة (Popa, 2012).

8. الاحتيال على التأمين الإلكتروني (*Insurance Fraud*) تشمل هذه الجرائم تقديم مطالبات تأمين مزورة أو احتيالية عبر الإنترنت بهدف الحصول على تعويضات مالية غير مستحقة.

بعد هذا العرض التعريفي للجرائم الإلكترونية لابد من التأكيد على ان تلك الجرائم أصبحت واقعاً لا يمكن تجاهله، لما تشكله من تهديدات مباشرة للأفراد والمؤسسات والمجتمعات على حد سواء. إن تنوع هذه الجرائم، سواء كان ذلك في شكل قرصنة إلكترونية، سرقة الهوية، أو التلاعب بالرأي العام، يكشف عن مدى خطورتها وتأثيرها السلبي على الأمن الرقمي والاجتماعي والاقتصادي. تتطلب هذه التهديدات المتنامية استجابة شاملة تبدأ بإقرار قوانين وتشريعات صارمة تعمل على حماية الأفراد والمؤسسات من الجرائم الإلكترونية بكل أشكالها. إن وجود إطار قانوني واضح وقوي يعزز من قدرة المجتمعات على مكافحة هذه الجرائم من خلال تحديد المسؤوليات، وتقنين العقوبات وضمان ملاحقة المجرمين عبر الحدود الجغرافية. وفي ظل التطور المستمر في أساليب الجريمة الإلكترونية، يصبح التعاون الدولي والإقليمي ضرورة حتمية، حيث أن الطبيعة العابرة للحدود لهذه الجرائم تجعل من الصعب التعامل معها بشكل منفرد. فضلاً عن ذلك، فإن التوعية المجتمعية وتعزيز ثقافة الأمن السيبراني تمثلان جانبين أساسيين لمواجهة التحديات المتزايدة.

ختاماً، نستطيع القول ان الجرائم الإلكترونية ليست مجرد تهديد تقني، بل هي من وجهة نظرنا خطر يمس أمن المجتمعات واستقرارها. لذلك، نعتقد ان تعزيز الوعي بأهميتها، ووضع تشريعات رادعة، والاستثمار في تقنيات الحماية السيبرانية، هو السبيل الأمثل لحماية الأفراد والمؤسسات وضمان سلامة الفضاء الرقمي في المستقبل.

4. التشريعات العربية

لقد أصبحت التكنولوجيا والإنترنت جزءاً لا يتجزأ من حياتنا اليومية، حيث أسهمت في تسهيل التواصل، وتطوير الأعمال، وتعزيز الابتكار. ومع ذلك، وفي الوقت نفسه فتحت الباب أمام تحديات جديدة أبرزها الجرائم الإلكترونية، التي لا تقتصر على انتهاك الخصوصية وسرقة البيانات فحسب، بل تمتد لتشمل تهديدات أمنية، اقتصادية، واجتماعية تؤثر على الأفراد والمؤسسات والمجتمعات بأسرها. لمواجهة هذه التحديات المتنامية، ظهرت الحاجة إلى تطوير تشريعات وقوانين تعالج الطبيعة الفريدة والمتطورة لهذه الجرائم. في العالم العربي، بذلت جهود حثيثة لصياغة قوانين وتشريعات تهدف إلى مكافحة الجرائم الإلكترونية، مع التركيز على تعزيز الأمن الرقمي وضمان حماية حقوق الأفراد والمؤسسات في الفضاء السيبراني. في هذا السياق، سنستعرض بشكل مختصر أبرز

إطار تشريعي مقترح للحد من الجرائم الإلكترونية وتعزيز الاخلاقيات الرقمية في العراق

الجهود العربية المبذولة في مجال تشريع القوانين الخاصة بمكافحة الجرائم الإلكترونية، ومدى استجابته للتطورات التقنية، وفعاليتها في مواجهة التحديات الراهنة.

1.4: الإمارات العربية المتحدة: قانون مكافحة الجرائم الإلكترونية

المرسوم بقانون اتحادي رقم 34 لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية [1].

الموجبات :

- منع نشر الأخبار الكاذبة أو المضللة التي تضر بالمجتمع .
 - تنظيم المحتوى الإلكتروني بما يضمن احترام القيم الأخلاقية والثقافية للدولة .
 - حماية الخصوصية ومنع الوصول غير المشروع إلى البيانات الشخصية.
- التحفظات: القانون يهدف الى حماية المجتمع من المحتوى الضار ولكنه يثير تساؤلات حول الحرية الرقمية وحدودها.

2.4: المملكة العربية السعودية: نظام مكافحة الجرائم المعلوماتية

نظام مكافحة الجرائم المعلوماتية الصادر بموجب المرسوم الملكي رقم م/17 لعام 2007 [2].

الموجبات :

- حماية الحياة الخاصة من خلال معاقبة التجسس أو الاعتراض على البيانات الشخصية .
 - حظر الإساءة إلى الآخرين عبر الإنترنت أو التشهير بهم .
 - منع الوصول غير المصرح به إلى الشبكات والأنظمة .
- التحفظات: يوفر القانون حماية كبيرة للخصوصية لكنه يطرح مخاوف متعلقة بتوازن الأمن مع حرية التعبير.

3.4: مصر: قانون مكافحة جرائم تقنية المعلومات

القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات [3] .

الموجبات :

- منع الاستخدام غير الأخلاقي للتكنولوجيا مثل النصب والاحتيال الرقمي .
 - حماية البيانات الشخصية وتجرى استخدامها دون موافقة .
 - تنظيم النشر الرقمي بما يتفق مع القيم المجتمعية .
- التحفظات: القانون يُعتبر أحد الأطر التشريعية الشاملة ولكنه يثير مخاوف حول مراقبة المحتوى الرقمي.

4.4: الأردن: قانون الجرائم الإلكترونية

1. <https://uaelegislation.gov.ae/ar/legislations/1526>

2. https://www.cst.gov.sa/ar/mediacenter/publicationsandbrochures/Documents/PR_PRN_002A.pdf

3. <https://manshurat.org/node/31487>

-قانون الجرائم الإلكترونية رقم 27 لسنة 2015 (مع التعديلات في 2023) [1] .

الموجبات:

- حماية الخصوصية ومنع استخدام الصور والمعلومات الشخصية دون إذن .
- حظر التهديدات أو الإساءات عبر الإنترنت .
- تجريم نشر الأخبار الكاذبة والمحتوى المسيء للقيم المجتمعية .

التحفظات: يركز القانون على حماية المستخدمين ولكنه يثير تساؤلات حول القيود المفروضة على حرية التعبير.

5.4: تونس: قانون حماية البيانات الشخصية

القانون الأساسي رقم 63 لسنة 2004 المتعلق بحماية البيانات الشخصية [2].

الموجبات:

- ضمان حماية البيانات الشخصية ومعاينة انتهاكات الخصوصية .
- تنظيم معالجة البيانات بما يتفق مع مبادئ الشفافية والموافقة .
- إنشاء الهيئة الوطنية لحماية البيانات الشخصية لضمان الالتزام بالقانون .

التحفظات: يعد القانون خطوة رائدة ولكنه يواجه تحديات في التنفيذ الفعلي.

6.4: قطر: قانون مكافحة الجرائم الإلكترونية

القانون رقم 14 لسنة 2014 بشأن مكافحة الجرائم الإلكترونية [3] .

الموجبات:

- تجريم اختراق الأنظمة وسرقة البيانات .
- منع نشر المعلومات الكاذبة أو المسيئة عبر الإنترنت .
- حماية الخصوصية الرقمية للمستخدمين .

التحفظات: يوفر القانون حماية متقدمة لكنه يثير جدلاً حول حرية التعبير والقيود المفروضة على الصحافة الرقمية.

7.4: الكويت: قانون مكافحة جرائم تقنية المعلومات

القانون رقم 63 لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات [4] .

الموجبات :

- حماية البيانات الشخصية ومنع استخدامها دون تصريح .

¹<https://www.lob.gov.jo/?v=1&lang=ar#!/LegislationDetails?LegislationID=3398&LegislationType=2&isMod=false>

² . <https://igppp.tn/sites/default/files/Loi%202004-63%20AR.pdf>

³ . <https://mohamoon-qa.com/Default.aspx?action=ViewActivePages&Type=6&ItemID=11084>

⁴ . <https://www.moi.gov.kw/main/content/docs/cybercrime/ar/law-establishing-cyber-crime-dept.pdf>

إطار تشريعي مقترح للحد من الجرائم الإلكترونية وتعزيز الاخلاقيات الرقمية في العراق

- معاقبة الجرائم المتعلقة بالتشهير والسب الإلكتروني .
- تنظيم النشر بما يتوافق مع القيم الاجتماعية والدينية .

التحفظات: يهدف القانون لحماية القيم الاجتماعية لكنه قد يحد من الحريات الرقمية.

ختامًا، يُمكننا القول إن تحقيق التوازن بين مكافحة الجرائم الإلكترونية وحماية حرية التعبير وحرية الوصول إلى المعلومات يمثل تحديًا كبيرًا يواجهه الدول العربية. وعلى الرغم من التقدم الملحوظ في صياغة التشريعات ذات الصلة، إلا أن هذه القوانين لا تزال بحاجة إلى مزيد من التطوير لضمان فعاليتها وعدالتها. إن التركيز على الشفافية، وتعزيز التعاون الدولي، وزيادة الوعي المجتمعي، يمثل خطوات أساسية نحو بناء بيئة رقمية آمنة وعادلة تحفظ حقوق الأفراد، وتواجه التحديات التي تفرضها الجرائم الإلكترونية. جدير بالذكر أن القوانين العربية الهادفة إلى مكافحة الجرائم الإلكترونية تُعتبر خطوة مهمة في مواجهة التحديات المتزايدة التي فرضها التطور السريع في تكنولوجيا المعلومات. ومع ذلك، فإن مواجهة التحديات المرتبطة بموازنة حماية حقوق الإنسان الأساسية مع جهود مكافحة الجرائم الإلكترونية تظل إحدى الأولويات التي تتطلب معالجة دقيقة وشاملة.

5. مشروع قانون الجرائم المعلوماتية العراقي

في العراق، تُوجد بعض القوانين والتشريعات التي تلامس الجوانب الرقمية، لكنها غالبًا ما تكون غير مكتملة أو تفتقر إلى التحديث اللازم لمواكبة التطورات التكنولوجية المتسارعة. ورغم غياب قانون شامل يعالج الأخلاقيات الرقمية والجرائم الإلكترونية بشكل متكامل، إلا أن هناك محاولات لتنظيم هذا المجال، أبرزها مشروع قانون الجرائم المعلوماتية الذي قدمته الحكومة العراقية إلى البرلمان العراقي عام 2011. لكنه أثار جدلاً واسعاً في الأوساط الشعبية، لا سيما بين المثقفين والمدافعين عن حقوق الإنسان، بسبب المخاوف من أن يؤدي إلى تقييد حرية التعبير والحق في الوصول إلى المعلومات. نتيجة لهذه المخاوف، ظل القانون معلقاً ولم يُقر بشكل نهائي حتى الآن. يُمثل مشروع قانون مكافحة الجرائم المعلوماتية خطوة ضرورية نحو تعزيز الأمن الرقمي في العراق، لكنه يحتاج إلى مراجعة شاملة ودقيقة لضمان ألا يتحول إلى أداة تُستخدم لتقييد الحريات الأساسية. تحقيق التوازن بين مكافحة الجرائم الإلكترونية وحماية حقوق الإنسان يتطلب نصوصاً قانونية واضحة وصارمة، توفر ضمانات ضد إساءة استخدام السلطة، مع التركيز على تعزيز حرية التعبير وضمان الوصول الحر إلى المعلومات كجزء لا يتجزأ من البيئة الرقمية العادلة. وفيما يلي عرض للقوانين العراقية ذات الصلة غير المباشرة بالأخلاقيات الرقمية و الجرائم الإلكترونية.

1. قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل^[1]: يمكن استخدامه لمعالجة قضايا مثل التشهير

أو الإساءة لكنه لا يغطي الجرائم الرقمية الحديثة بشكل كافٍ.

¹ . <https://www.iraqilaws.com/2023/10/111-1969.html>

2. قانون حماية حق المؤلف رقم 3 لسنة 1971^[1]: يعالج حقوق الملكية الفكرية لكنه يفتقر لتغطية انتهاكات الملكية الفكرية الرقمية.
3. قانون حماية المستهلك رقم 1 لسنة 2010^[2]: يحتوي على بعض البنود التي يمكن تطبيقها على التجارة الإلكترونية لكنه لا يغطي قضايا مثل الاحتيال الرقمي.

6. مقترح قانون مكافحة الجرائم الإلكترونية في العراق

بعد الاطلاع على التشريعات العربية المتعلقة بمكافحة الجرائم الإلكترونية، وتحليل أبرز الممارسات والتجارب القانونية في هذا المجال، إلى جانب دراسة الاعتراضات التي واجهت مشروع قانون الجرائم المعلوماتية في العراق، برزت الحاجة إلى وضع قانون متكامل يوازن بين متطلبات تعزيز الأمن في البيئة الرقمية وضمان حرية التعبير وحق الوصول إلى المعلومات. ولتحقيق هذا التوازن، وضمان معالجة فعّالة للتحديات المتزايدة التي تفرضها الجرائم الإلكترونية، نقدم مقترح القانون التالي.

ديباجة:

استناداً إلى أحكام الدستور العراقي، وحرصاً على حماية المجتمع من مخاطر الجرائم الإلكترونية وضمان التوازن بين الحفاظ على الأمن السيبراني واحترام حقوق الإنسان، صدر القانون الآتي:

الباب الأول: التعريفات والأحكام العامة

المادة (1): تعريفات

لأغراض هذا القانون، تكون للكلمات والعبارات التالية المعاني الموضحة قرين كل منها ما لم يقتض السياق خلاف ذلك:

1. الجريمة الإلكترونية: أي فعل غير مشروع يتم باستخدام تقنيات المعلومات أو الاتصالات.
2. النظام المعلوماتي: مجموعة من الأجهزة والبرمجيات المصممة لمعالجة البيانات إلكترونياً.
3. البيانات الإلكترونية: المعلومات التي يتم تخزينها أو معالجتها أو نقلها إلكترونياً.
4. الدخول غير المشروع: النفاذ إلى نظام معلوماتي دون تفويض أو بما يتجاوز التفويض الممنوح.
5. حقوق الإنسان الرقمية: حقوق الأفراد في الخصوصية، حرية التعبير، والوصول إلى المعلومات في البيئة الرقمية.
6. وسائط تقنية المعلومات: أي جهاز أو تطبيق إلكتروني يُستخدم لمعالجة أو تخزين أو تبادل البيانات الإلكترونية.

¹ . <https://wiki.dorar-aliraq.net/iraqilaws/law/4857.html>

² . <https://archive3.parliament.iq/ar/2010/02/08/>

إطار تشريعي مقترح للحد من الجرائم الإلكترونية وتعزيز الاخلاقيات الرقمية في العراق

7. الموقع الإلكتروني: مكان إتاحة المعلومات الإلكترونية على شبكة المعلومات من خلال عنوان محدد.
8. البطاقات الإلكترونية: كل بطاقة مصرفية، ائتمانية، مسبقة الدفع، أو أي وسيلة دفع إلكترونية أخرى تُستخدم لتنفيذ معاملات مالية أو شراء سلع وخدمات عبر الإنترنت أو من خلال أجهزة الدفع الآلي.
- المادة (2): نطاق التطبيق

1. تسري أحكام هذا القانون على أي جريمة إلكترونية ترتكب داخل جمهورية العراق أو تمتد آثارها إليه.
2. لا يخل تطبيق هذا القانون بأي عقوبات أشد ينص عليها قانون العقوبات أو أي قانون آخر.

الباب الثاني: الجرائم الإلكترونية والعقوبات

المادة (3): التنصت غير المشروع

1. يعاقب بالحبس مدة لا تزيد عن () وبغرامة لا تقل عن () دينار عراقي كل من تنصت على بيانات يتم إرسالها عبر شبكة معلوماتية أو أحد أجهزة الحاسوب دون مسوغ قانوني، أو قام بتسجيل كلام شخص أو صورته دون علمه أو موافقته.

المادة (4): الدخول غير المشروع

2. يعاقب بالحبس مدة لا تزيد عن () وبغرامة لا تقل عن () دينار عراقي ولا تزيد عن () دينار، أو بإحدى هاتين العقوبتين، كل من دخل عمدًا ودون تفويض نظامًا معلوماتيًا أو شبكة معلوماتية.

3. إذا أدى الدخول إلى إلغاء أو حذف أو تعديل بيانات أو معلومات، تكون العقوبة الحبس لمدة لا تقل عن () .

المادة (5): التعدي على الخصوصية

1. يعاقب بالحبس مدة لا تزيد عن () وبغرامة لا تقل عن () دينار كل من قام بنشر أو إفشاء بيانات شخصية دون موافقة صاحبها.
2. إذا كانت البيانات ذات طابع حساس، تشدد العقوبة بالحبس لمدة لا تزيد عن () .

المادة (6): التزوير الإلكتروني

1. يعاقب بالحبس مدة لا تقل عن () وبغرامة لا تقل عن () دينار كل من زور مستندًا إلكترونيًا أو استخدمه مع علمه بتزويره.

المادة (7): الابتزاز الإلكتروني

الأستاذ الدكتور: طلال ناظم الزهيري

2. يعاقب بالحبس مدة لا تزيد عن () وبغرامة لا تقل عن () دينار عراقي كل من استخدم وسائل تقنية المعلومات لتهديد أو ابتزاز شخص آخر لحمله على القيام بفعل أو الامتناع عنه، ولو كان هذا الفعل مشروعًا.

3. إذا كان التهديد يتضمن نشر أو إفشاء بيانات حساسة، تشدد العقوبة بالسجن لمدة لا تقل عن () سنوات.

المادة (8): التنمر الإلكتروني

1. يعاقب بالحبس مدة لا تزيد عن () وبغرامة لا تقل عن () دينار عراقي كل من استخدم وسائل تقنية المعلومات للإساءة إلى شخص آخر بشكل متكرر بقصد إلحاق الضرر النفسي أو الاجتماعي به.

2. إذا كان الضحية طفلًا أو من ذوي الاحتياجات الخاصة، تشدد العقوبة بالسجن لمدة لا تقل عن () سنوات.

المادة (9): التعدي على الأمن الوطني

1. يعاقب بالسجن () كل من أنشأ أو أدار موقعًا إلكترونيًا بقصد الترويج لأفكار إرهابية أو نشر مواد تهدد أمن الدولة.

2. تكون العقوبة السجن لمدة لا تقل عن () إذا ترتب على الجريمة وفاة شخص أو إلحاق ضرر كبير بالبنية التحتية.

المادة (10): جرائم الإضرار بالنظام العام

1. يعاقب بالسجن مدة لا تقل عن () سنوات وبغرامة لا تقل عن () دينار كل من أنشأ أو نشر محتوى إلكترونيًا يهدف إلى الإضرار بالقيم الدينية أو الآداب العامة أو النظام العام أو تهديد السلم الأهلي أو الترويج للعنف الطائفي.

2. إذا كان المحتوى موجّهًا إلى الأطفال، تشدد العقوبة بالسجن لمدة لا تقل عن () سنوات.

المادة (11): الإعفاء من العقوبة بعد الإبلاغ

1. يعفى من العقوبات المنصوص عليها في هذا القانون كل من يبادر بالإبلاغ عن جريمة ارتكبتها مع شخص آخر أو كان يخطط لارتكابها، بشرط أن يتم الإبلاغ فورًا وبعد علمه بالجريمة، وأن يشمل الإبلاغ المعلومات المتعلقة بالأدوات أو الوسائل المستخدمة في تنفيذ الجريمة، والأشخاص المتورطين فيها.

2. في حال كان الإبلاغ بعد وقوع الجريمة أو في مرحلة متأخرة، يتعين على المبلغ أن يثبت أنه أقدم على الإبلاغ بنية صافية ولم يكن الدافع وراء ذلك محاولة التهرب من المسؤولية القانونية.

إطار تشريعي مقترح للحد من الجرائم الإلكترونية وتعزيز الاخلاقيات الرقمية في العراق

3. تُمنح المحكمة المختصة صلاحية تقدير ما إذا كان الإبلاغ قد تم في الوقت المناسب بما يتماشى مع القوانين المعمول بها.

الباب الثالث: بطاقات الدفع الإلكتروني

المادة (1): جرائم الاحتيال والتزوير باستخدام البطاقات الإلكترونية

1. يعاقب بالحبس مدة لا تقل عن () وبغرامة لا تقل عن () دينار عراقي كل من استخدم بطاقة إلكترونية مزورة أو مسروقة أو حصل عليها بطرق غير قانونية بهدف إجراء عمليات مالية أو شراء سلع أو خدمات.

2. يعاقب أيضًا كل من ارتكب عملية احتيال باستخدام بطاقة إلكترونية عبر تقديم معلومات مغلوطة أو مزورة للحصول على أموال أو سلع أو خدمات بشكل غير مشروع.

3. يعاقب كل من قام بتقديم معلومات خاطئة أو مضللة أثناء التقدم للحصول على بطاقة إلكترونية بهدف الاحتيال أو الاستفادة غير القانونية من خدمة مالية.

المادة (2): جرائم التلاعب والاختراق في الأنظمة المالية الإلكترونية

1. يعاقب بالحبس مدة لا تقل عن () سنة وبغرامة لا تقل عن () دينار عراقي كل من قام بتعديل أو اختراق أنظمة الدفع الإلكترونية أو البنوك الإلكترونية بهدف تحويل أموال أو إجراء معاملات غير قانونية.

2. يعاقب بالحبس مدة لا تقل عن () سنة وبغرامة لا تقل عن () دينار عراقي كل من قام بتوزيع أو توزيع أدوات أو برمجيات تهدف إلى اختراق أو تلاعب ببطاقات الدفع الإلكترونية أو الأنظمة المالية المرتبطة بها.

3. يعاقب بالحبس مدة لا تقل عن () سنة وبغرامة لا تقل عن () دينار عراقي كل من ساعد أو سهّل لشخص آخر استخدام بطاقة إلكترونية غير قانونية أو مسروقة أو مزورة لأغراض مالية غير مشروعة.

المادة (3): جرائم غسيل الأموال واستغلال البيانات الشخصية المرتبطة بالبطاقات الإلكترونية

1. يعاقب بالحبس مدة لا تقل عن () سنة وبغرامة لا تقل عن () دينار عراقي كل من استخدم البطاقات الإلكترونية في غسيل الأموال أو في تحويل الأموال عبر معاملات مالية غير مشروعة بهدف إخفاء المصدر الحقيقي للأموال.

2. يعاقب بالحبس مدة لا تقل عن () سنة وبغرامة لا تقل عن () دينار عراقي كل من حصل على بيانات بطاقة إلكترونية أو معلومات مصرفية تتعلق بشخص آخر دون إذن منه أو بطريقة غير قانونية بهدف استخدامها في عمليات مالية غير مشروعة أو بيعها أو استغلالها.

المادة (4): إجراءات وقائية لمكافحة الجرائم المالية المرتبطة بالبطاقات الإلكترونية

1. يلتزم مقدمو خدمات الدفع الإلكتروني والمؤسسات المالية باتخاذ التدابير الأمنية اللازمة لمنع التلاعب أو الاحتيال باستخدام البطاقات الإلكترونية.

2. يجب على المستخدمين اتخاذ كافة التدابير الوقائية للحفاظ على سرية بياناتهم المالية والبطاقات الإلكترونية، ويجب عليهم الإبلاغ عن أي استخدام غير قانوني لهذه البيانات فوراً.

المادة (5): التعاون الدولي في مكافحة الجرائم المالية المرتبطة بالبطاقات الإلكترونية

1. يُسمح للسلطات القضائية والمالية بالتعاون مع السلطات الدولية في التحقيق في الجرائم المالية المتعلقة بالبطاقات الإلكترونية، وتبادل المعلومات مع الهيئات الدولية لمحاربة هذه الجرائم.

الباب الرابع: حماية حقوق الإنسان الرقمية

المادة (12): حرية التعبير

1. يكفل هذا القانون حرية التعبير الرقمي شريطة ألا تتعارض مع النظام العام أو الآداب العامة أو الأمن الوطني.

2. لا يجوز تقييد الوصول إلى المعلومات إلا بقرار قضائي مسبب.

المادة (13): حماية الخصوصية

1. تلتزم الجهات الحكومية بحماية بيانات الأفراد وضمان عدم استخدامها إلا في حدود القانون.

2. يمنع أي نوع من المراقبة الإلكترونية دون إذن قضائي.

3. يُحظر أي استغلال للبيانات الشخصية لأغراض تجارية أو سياسية دون موافقة صريحة من صاحب البيانات.

الباب الخامس: الأحكام الإجرائية

المادة (14): اختصاصات القضاء

تختص المحاكم العراقية بالنظر في الجرائم المنصوص عليها في هذا القانون، بما في ذلك الجرائم ذات الطابع الدولي التي تمس العراق.

المادة (15): التعاون الدولي

يجوز للجهات المختصة التعاون مع الدول الأخرى والمنظمات الدولية لمكافحة الجرائم الإلكترونية وفقاً للاتفاقيات الدولية التي يكون العراق طرفاً فيها.

المادة (16): الأدلة الرقمية

1. تُعد التقارير الصادرة عن الجهات المعنية بالأدلة الرقمية من وسائل الإثبات الرسمية أمام المحاكم.

إطار تشريعي مقترح للحد من الجرائم الإلكترونية وتعزيز الاخلاقيات الرقمية في العراق

2. يجوز للقاضي المختص إصدار أوامر بحفظ وتحليل الأدلة الرقمية بما يتفق مع حماية الحقوق الفردية.

الباب السادس: أحكام ختامية

المادة (17): التوعية والتدريب

1. تلتزم الجهات المعنية بتنظيم حملات توعية بمخاطر الجرائم الإلكترونية.

2. يُلزم القانون الجهات القضائية والأمنية بتدريب كوادرها لمواكبة التطورات التقنية.

المادة (18): أحكام انتقالية

1. تُلغى جميع النصوص القانونية التي تتعارض مع أحكام هذا القانون.

2. يُنشر هذا القانون في الجريدة الرسمية ويُعمل به بعد () يوماً من تاريخ نشره.

المادة (19): إصدار اللوائح التنفيذية

يصدر مجلس الوزراء اللوائح اللازمة لتنفيذ أحكام هذا القانون خلال مدة لا تتجاوز () من تاريخ نشره في

الجريدة الرسمية.

7. التوصيات

لتعزيز فعالية (قانون مكافحة الجرائم الإلكترونية) في العراق مقترح الدراسة في الملحق (1)، يمكن تبني مجموعة من التوصيات والمقترحات التي تساهم في الحد من هذه الجرائم وضمان تطبيق القانون بشكل فعال، بما في ذلك:

1. تعزيز التعاون بين الجهات الحكومية والقطاع الخاص

• ينبغي إقامة شراكة قوية بين الحكومة وشركات الاتصالات لتبادل المعلومات حول الأنشطة المشبوهة وتطبيق القوانين ضد الجريمة الإلكترونية.

• يجب تشجيع شركات التكنولوجيا المحلية والدولية على الاستثمار في تحديث وتحسين البنية التحتية الإلكترونية لتكون أكثر أماناً ضد الهجمات.

2. تعليم وتوعية الجمهور

• يجب أن تشمل الحملات التوعوية برامج تعليمية للمواطنين حول كيفية حماية معلوماتهم الشخصية على الإنترنت، وطرق تجنب الجرائم الإلكترونية مثل الاحتيال، والتصيد الاحتيالي.

• خصوصاً الشباب، وطلاب المدارس والجامعات، الذين يعدون الفئة الأكثر عرضة للانخراط في الأنشطة الإلكترونية غير المشروعة.

3. التدريب المستمر للمسؤولين الأمنيين والقضائيين

الأستاذ الدكتور: طلال ناظم الزهيري

- يجب توفير دورات تدريبية مستمرة للأجهزة الأمنية والمحاكم للتعامل مع الجرائم الإلكترونية بفعالية. يشمل ذلك التدريب على كيفية التعامل مع الأدلة الرقمية، وتفسير القوانين المتعلقة بالجرائم الإلكترونية.
- تدريب فرق متخصصة من الشرطة والقضاء للتعامل مع أنواع الجرائم الإلكترونية المتنوعة مثل الابتزاز الإلكتروني، الاحتيال، وتزوير المعلومات.
- 4. التركيز على القوانين المساندة للتنظيم والتدقيق
- فرض قواعد صارمة على المؤسسات المالية والرقابية لحماية البيانات الشخصية والمعاملات الإلكترونية، مع مراقبة تطبيق الإجراءات الأمنية المطلوبة.
- النظر في إضافة بعض العقوبات المشددة لمن يسيء استخدام التقنيات الجديدة مثل تطبيقات الذكاء الاصطناعي، أو محاكاة الهويات الإلكترونية لأغراض غير قانونية.
- 5. تحفيز البحث العلمي في مجال الأمن السيبراني
- دعم إنشاء مراكز أبحاث متخصصة في الأمن السيبراني لمواكبة التطورات السريعة في المجال، وتقديم حلول مبتكرة للوقاية من الجرائم الإلكترونية.
- تشجيع الجامعات على تقديم برامج تعليمية وبجته حول تقنيات الأمان الرقمي وأثر الجرائم الإلكترونية على المجتمع.
- 6. تعزيز التعاون الإقليمي والدولي
- تعزيز التعاون مع الدول المجاورة والمنظمات الدولية مثل منظمة الأمم المتحدة ومجموعة العشرين في تبادل الخبرات والمعلومات لمكافحة الجرائم الإلكترونية.
- للحد من الجرائم العابرة للحدود، يمكن توقيع اتفاقيات تعاون مع الدول الأخرى لتنسيق التحقيقات وتبادل الأدلة الرقمية في إطار محاربة الجريمة الإلكترونية.
- 7. تحسين الإجراءات القانونية والإدارية
- تسريع الإجراءات القضائية في قضايا الجرائم الإلكترونية لضمان سرعة المحاكمة والبت في القضايا التي تؤثر سلباً على الأفراد والمجتمع.
- حماية المبلغين من العقوبات ومنع تعرضهم للمضايقات أو الانتقام من المتورطين في الجرائم الإلكترونية.
- 8. مواكبة التطورات التكنولوجية
- بما أن الجريمة الإلكترونية تتطور بشكل مستمر، يجب أن يكون القانون مرناً بما يكفي للتكيف مع هذه التغيرات. على سبيل المثال، يمكن تعديل القانون بشكل دوري ليشمل التحديات الجديدة مثل الجرائم المتعلقة بالذكاء الاصطناعي.

إطار تشريعي مقترح للحد من الجرائم الإلكترونية وتعزيز الاخلاقيات الرقمية في العراق

- ضمان أن الشركات التي تستخدم هذه التقنيات تتبع ممارسات أمان صارمة لتجنب تسريب البيانات أو استخدامها لأغراض غير قانونية.
- 9. تشجيع ثقافة الأمان الرقمي في المؤسسات التعليمية
- يمكن إدخال موضوعات تتعلق بالأمن الرقمي في المناهج التعليمية لجميع المراحل الدراسية (الابتدائية، الإعدادية، والجامعية) لتدريب الأجيال الجديدة على التعامل الآمن مع التكنولوجيا.
- 10. تنفيذ مراقبة وتحليل دائمين للتهديدات الرقمية
- ينبغي إنشاء وحدات مراقبة دائمة لرصد التهديدات الأمنية الرقمية وتحليلها في الوقت الفعلي، ومواكبة آخر التطورات التكنولوجية في مجال الأمن السيبراني.
- 11. تعزيز حماية البنية التحتية الحيوية
- يجب أن تتخذ الحكومة إجراءات لحماية الأنظمة الحكومية والقطاعين الصحي والطاقة من الهجمات الإلكترونية التي قد تستهدف هذه القطاعات الحيوية.
- من خلال هذه التوصيات، يمكن تعزيز قدرة العراق على مكافحة الجرائم الإلكترونية وحماية المجتمع من المخاطر المحتملة التي قد تنشأ نتيجة للاستخدام غير القانوني للتكنولوجيا.

المراجع:

1. أحمد عبدالله الأحمد، ماجدة احمد عمر، و امجد احمد هديب. (2017). الاخلاقيات الرقمية والحدثة في التواصل الانساني. المجلة الاردنية للعلوم الاجتماعية، 251-263.
2. حنان كيلاي. (2015). التضليل الإعلامي وعلاقته بالآثار السلبية لشبكات التواصل الاجتماعي. المجلة المصرية لبحوث الرأي العام، 219-289.
3. منذر محمد عبيس. (2024). التضليل الإعلامي والحرب النفسية في الإعلام الرقمي وانعكاساته لخداع الرأي العام. مجلة دجلة، 543-556.
4. نديم منصوري. (2014). سوسيولوجيا الإنترنت. بيروت: مندى المعارف.
5. نوح عبد الله. (2022). الاخلاقيات الرقمية ومساهمتها في الوقاية من الجريمة الرقمية. مجلة العلوم القانونية و السياسية، 44-65.
6. Common Privacy Violations. (2024). Retrieved 15, 2025, from symptai: <https://www.symptai.com/resources/insights/data-and-privacy-protection/5-common-privacy-violations>

7. Abusitta, A. L. (2021). *Malware classification and composition analysis: A survey of recent developments*. . *Journal of Information Security and Applications*, 3-63.
8. Adil, M. K. (2020). *Preventive techniques of phishing attacks in networks*. In *2020 3rd International Conference on Advancements in Computational Sciences IEEE.*, (pp. 1-8).
9. Cross, C. (2019). *Online fraud*. Oxford: Oxford research encyclopedia of criminology.
10. Gordon, S. &. (2006). *On the definition and classification of cybercrime*. *Journal in computer virology*, 13-20.
11. Kara, I. (2021). *Cyber-Espionage Malware Attacks Detection and Analysis: A Case Study*. . *Journal of Computer Information Systems*, 1253–1270.
12. Kutera, M. (2022). *Cryptocurrencies as a subject of financial fraud*. *Journal of Entrepreneurship, Management and Innovation*, 45-77.
13. Li, T. Z. (2025). *A two-stage cyberbullying detection based on multi-view features and decision fusion strategy*. . *Applied Intelligence*, 1-21.
14. Mareline, A. (2022). *Understanding the Types of Cyber Crime and Its Prevention*. . *Mathematical Statistician and Engineering Applications*, 108-112.
15. Michel, P. (2008). *Financial crimes: The constant challenge of seeking effective prevention solutions*. . *Journal of Financial Crime*, 383-397.
16. Popa, C. (2012). *Money laundering using the internet and electronic payments*. *Metalurgia International*,, 219.
17. Salvi, M. H. (2016). *Ransomware: A Cyber Extortion*. *Asian Journal For Convergence In Technology*. Retrieved 15, 2025, from <http://www.asianssr.org/index.php/ajct/article/view/55/37>
18. Sukhai, N. B. (2004). *Hacking and cybercrime*. . In *Proceedings of the 1st annual conference on Information security curriculum development*