International Journal of Law Research and Studies (IJLRS)
المجلة الدولية للبحوث والدراسات القانونية
Vol. (5), No. (1)
January 2026
الإصدار (5)، العدد (1)

الجرائم الإلكترونية وتأثيرها على المؤسسات والأفراد والمجتمع

راســم مسيــر جاســم
أستاذ مشارك دكتور، تخصص القانون الجنائي، قسم القانون، كلية المنصور الجامعة، العراق

معن زكي كاظم الكرعاوي
محامي، دكتور، المدير المفوض لشركة القسطاس الذهبي للخدمات والاستشارات القانونية، بغداد، العراق
maan_advocate99@yahoo.com

الملخص

إن الثورة التكنولوجية وبخاصة ثورة الاتصالات أهم التطورات التي يعيشها العالم اليوم، وتعتبر ثورة الاتصالات هي المحرك الأساسي في التطورات الحادثة في الوقت الحالي، إلا أنها ليست المحرك الوحيد في هذه التطورات حيث أن التطور الكبير في تكنولوجيا الحاسبات قد أسهم بصورة كبيرة في تسارع معدلات التقدم في مجال الاتصالات والمعلومات.

وقد كان من نتاج التطور في الجانبين ظهور أدوات واختراعات وخدمات جديدة في مختلف المجالات ولقد نتج عن الثورة التكنولوجية تلك ظهور نوع جديد من المعاملات يسمى المعاملات الإلكترونية تختلف عن المعاملات التقليدية التي نعرفها من حيث البيئة التي تتم فيها هذه المعاملات.

ويقصد بالمعاملات الإلكترونية كل المعاملات التي تتم عبر تجهيزات إلكترونية مثل الهاتف، والفاكس، وأجهزة الحواسب، وشبكة الإنترنت، ومؤخراً الذكاء الاصطناعي واستغلاله في الإساءة على الأشخاص والمؤسسات والشخصيات العامة وعن طريق الهاتف المحمول. وتتكون تلك المعاملات من عدد من المكونات الأساسية، يهمنا في هذه الورقة طرح مكون أساسي فيها وهو الجزء الخاص بجرائم تلك المعاملات، أو بمعني أدق القواعد القانونية الجنائية التي تحكم الأفعال التي تتم من خلال أجهزة الحواسب، أو عبر شبكة الإنترنت.

إن جرائم الكمبيوتر والإنترنت، أو ما يسمى Cyber Crimes هي ظواهر إجرامية تقرع أجراس الخطر لتنبه مجتمعنا عن حجم المخاطر والخسائر التي يمكن أن تنجم عنها، خاصة أنها جرائم ذكية تنشأ وتحدث في بيئة إلكترونية أو بمعنى أدق رقمية، يقترفها أشخاص مرتفعي الذكاء ويمتلكون أدوات المعرفة التقنية، مما يسبب خسائر للمجتمع ككل علي المستويات الاقتصادية والاجتماعية والثقافية والأمنية مع صعوبة كشفها والاستدلال على فاعلها ومرتكبها وتدخل فيها ربما أشخاص عاديون أو مؤسسات عامة أو دول أحياناً لتحقيق مأرب سياسية ومجتمعية مقيتة، وهو ما سوف نحاول أن نتعرض له بشيء من التفصيل في هذا البحث محاولين أن نضع ولو لبنة صغيرة في الإطار التنظيمي والتشريعي في تلك المسألة.

الكلمات المفتاحية: الجرائم الإلكترونية، التكنولوجيا، الأمن الشخصي، الأفراد، المجتمع، المؤسسات.

International Journal of Law Research and Studies (IJLRS)
Vol. (5), No. (1)
IJLRS
January 2026
المجلة الدولية للبحوث والدراسات القانونية
الإصدار (5)، العدد (1)

Cybercrimes and Their Impact on Institutions, Individuals, and Society

Rasem Mseer Jasim
Assistant Professor, Department of Law, Al-Mansour University College, Iraq

Maan Zaki Kadhim Al Karraawi
Attorney-at-Law, PhD, Managing Director of Al-Qistas Al-Dhahabi Legal Services and Consultations Company, Baghdad, Iraq
maan_advocate99@yahoo.com

Abstract

The technological revolution, and especially the communications revolution, is one of the most important developments the world is experiencing. The communications revolution is the primary driver of current developments, but it is not the only driver. The significant advancements in computer technology have greatly contributed to accelerating progress in the field of communications and information.

The development in both areas has resulted in the emergence of new tools, inventions, and services in various fields. This technological revolution has led to the emergence of a new type of transaction called electronic transactions, which differ from traditional transactions in terms of the environment in which they take place.

Electronic transactions refer to all transactions that take place through electronic equipment such as the telephone, Fax machines, computers, the internet, and more recently through artificial intelligence and its misuse to harm individuals, institutions, and public figures, including through mobile phones. These transactions consist of several basic components. In this paper, we are concerned with presenting a fundamental component: the crimes related to these transactions, or more precisely, the criminal legal rules that govern actions carried out through computers or the internet.

Computer and internet crimes, or what are called cybercrimes, are criminal phenomena that sound the alarm, alerting our society to the extent of the risks and losses that can result from them. This is especially true since they are sophisticated crimes that arise and occur in an electronic, or more precisely, digital environment. They are committed by highly intelligent individuals who possess the tools of technical knowledge, causing losses to society as a whole on economic, social, cultural, and security levels, These crimes are also characterized by the difficulty of detection and identifying their perpetrators, and they may involve ordinary

individuals, public institutions, or even states at times, in order to achieve reprehensible political and societal objectives. This is what we will try to address in some detail in this research, attempting to lay even a small brick in the regulatory and legislative framework for this issue.

Keywords: Cybercrime, Technology, Personal Security, Individuals, Society, Institutions.

المقدمة

أفرز التطور التكنولوجي المتسارع الذي شهده العالم في العقود الأخيرة واقعاً جديداً أعاد تشكيل أنماط الحياة الإنسانية على مختلف المستويات. فقد أصبحت الوسائل الرقمية جزءاً لا يتجزأ من الحياة اليومية للأفراد وللشركات، وعنصراً أساسياً في عمل المؤسسات الرسمية والخاصة، وأداة محورية في إدارة شؤون المجتمعات وحتى الدول. غير أن هذا التحول، رغم ما حمله من مزايا كبيرة، أوجد في المقابل أنماطاً حديثة من السلوك الإجرامي، تمثلت فيما يعرف بالجرائم الإلكترونية، التي باتت تشكل أحد أبرز التحديات القانونية والأمنية في العصر الرقمي.

حيث شكلت الجرائم الإلكترونية انعكاساً مباشراً لاعتماد الإنسان المتزايد على التكنولوجيا، إذ انتقل الفعل الجرمي من الفضاء المادي التقليدي إلى الفضاء الافتراضي وبواقعية حيث ترتكب الجريمة باستخدام وسائل إلكترونية متطورة جداً ومشاركة التطور، وتستهدف بيانات أو أنظمة أو أفراداً عبر الشبكات الرقمية. وتمتاز هذه الجرائم بطابعها غير الملموس، وبقدرتها على تجاوز الحدود الجغرافية للدول، الأمر الذي يجعل اكتشافها وملاحقة مرتكبيها أكثر تعقيداً وصعوبة مقارنة بالجرائم التقليدية الأخرى.

وعلى مستوى الأفراد، تمثل الجرائم الإلكترونية تهديداً مباشراً للخصوصية وانتهاكاته والأمن الشخصي والمقربين منه. فالتعدي على البيانات الشخصية، واختراق الحسابات الإلكترونية، وانتحال الهوية الرقمية، كلها أفعال تؤدي إلى شعور الضحية بانعدام الأمان، وتزعزع ثقته في استخدام الوسائل التكنولوجية. وقد تتجاوز آثار هذه الجرائم الجانب المادي، لتترك بصمات نفسية عميقة، لا سيما في حالات الابتزاز الإلكتروني أو التشهير عبر الإنترنت، حيث قد يتعرض الفرد لضغوط نفسية واجتماعية تؤثر في حياته اليومية وعلاقاته بالمحيط الاجتماعي وخاصة في البرامج المتعلقة بالأنشطة الحديثة والسوشيال ميديا وتطور المشاريع في الذكاء الاصطناعي المذهل الذي يجعل من الأشخاص سخرية مجتمعية مقيتة.

ويزداد هذا التأثير حدة عندما تستهدف الجرائم الإلكترونية فئات أكثر هشاشة، مثل الأطفال والمراهقين وكبار السن، الذين قد يفتقرون إلى الوعي الكافي بالمخاطر الرقمية أو إلى القدرة على التمييز بين الاستخدام الآمن والخطِر للتكنولوجيا. ففي هذه الحالات، تتحول الجريمة الإلكترونية إلى أداة استغلال، تمس كرامة الفرد وحقوقه الأساسية، وتفرض تحديات إضافية على الأسرة والمجتمع في آن واحد.

أما على صعيد المؤسسات، فإن الجرائم الإلكترونية تشكل تهديداً حقيقياً لاستقرارها واستمرارية عملها.

فالهجمات التي تستهدف الأنظمة المعلوماتية قد تؤدي إلى تعطيل الخدمات، وتسريب معلومات سرية، وإلحاق خسائر مالية جسيمة، فضلاً عن الإضرار بسمعة المؤسسة وثقة المتعاملين معها. وفي ظل التحول المتزايد نحو الاقتصاد الرقمي، أصبحت البيانات والأصول الرقمية تمثل قيمة استراتيجية، ما يجعلها هدفاً رئيسياً للهجمات الإلكترونية.

إشكالية البحث

أفرز التطور المتسارع في تقنيات المعلومات والاتصالات أنماطاً جديدة من الجرائم لم تعد ترتبط بالمكان أو الزمان، بل باتت ترتكب في فضاء رقمي عابر للحدود، وهو ما يعرف بالجرائم الإلكترونية. وقد امتد تأثير هذه الجرائم ليطال الأفراد من خلال انتهاك الخصوصية وسرقة البيانات، كما أصاب المؤسسات بأضرار مالية جسيمة وهدّد أمنها المعلوماتي، فضلا عن انعكاساته السلبية على استقرار المجتمع وثقته بالفضاء الرقمي. ومع تزايد الاعتماد على الأنظمة الإلكترونية في مختلف مجالات الحياة، أصبحت هذه الجرائم تشكّل خطراً حقيقياً على الأمن الاقتصادي والاجتماعي. وتبرز الإشكالية في مدى قدرة التشريعات الحالية على مواكبة هذا التطور المتسارع، وعلى توفير حماية فعّالة للضحايا. فهل نجحت القوانين الجزائية والتقنية في الحد من الجرائم الإلكترونية وحماية الأفراد والمؤسسات؟ وإلى أي مدى يمكن تحقيق توازن فعّال بين مكافحة الجرائم الإلكترونية وضمان الحقوق والحريات الرقمية في المجتمع؟

أهمية البحث

من أخطر التحديات التي تواجه الأفراد والمؤسسات في العصر الرقمي هي الجرائم الإلكترونية واحدة، لما تحمله من تهديدات مباشرة للخصوصية والأمن المالي. فهي تعرض الشركات لخطر اختراق أنظمتها وسرقة بياناتها الحساسة، ما قد يؤدي إلى خسائر مالية كبيرة ويضع سمعتها على المحك. أما الأفراد، فيصبحون عرضة للابتزاز والاحتيال أو تسريب معلوماتهم الشخصية، الأمر الذي يخلق شعوراً بعدم الأمان وفقدان الثقة في البيئة الرقمية. وعلى مستوى المجتمع، تؤدي هذه الجرائم إلى تعطيل الخدمات وتعكير استقرار المؤسسات العامة والخاصة، مما يؤثر سلباً على الاقتصاد والنسيج الاجتماعي. لذلك، أصبحت دراسة الجرائم الإلكترونية ضرورة ملحة، بهدف تطوير استراتيجيات وقائية، وتشريعات رادعة، وتعزيز البنية التحتية للأمن السيبراني.

المبحث الأول: الجرائم الإلكترونية وأثرها على الأفراد

مع التقدم السريع للتكنولوجيا واعتماد الحياة اليومية على الشبكات الرقمية، برزت الجرائم الإلكترونية كأحد التحديات الأكثر تعقيداً في العصر الحديث. لم تعد الهجمات الإلكترونية مجرد اختراقات تقنية، بل تحولت إلى أفعال تحمل آثاراً مباشرة على حياة الأفراد وخصوصياتهم. فالأشخاص اليوم يضعون بياناتهم الشخصية، ومعلوماتهم المالية، وحتى تفاصيل حياتهم الخاصة على الإنترنت، مما يجعلهم عرضة للابتزاز،

والاحتيال المالي [1]، وتسريب المعلومات الحساسة. هذه الجرائم لا تقتصر على الخسائر المادية، بل تمتد لتؤثر على الصحة النفسية، حيث يشعر الضحايا بالقلق وفقدان الثقة في البيئة الرقمية المحيطة بهم، بل وحتى في محيطهم الاجتماعي.

تأثير الجرائم الإلكترونية على الأفراد يتجاوز الأضرار الفردية، إذ تهدد قدرتهم على ممارسة حياتهم بشكل طبيعي، وقد تعيفهم عن الاستفادة من الخدمات الرقمية الأساسية التي أصبحت جزءاً لا يتجزأ من الحياة اليومية. كما أن الوعي الرقمي المحدود يزيد من احتمالية الوقوع ضحية لهذه الهجمات، ما يضع مسؤولية كبيرة على الجهات التعليمية والتوعوية لتزويد المستخدمين بالمعرفة اللازمة للتعامل بأمان مع التكنولوجيا.

إضافة إلى ذلك، يمكن أن تؤدي الجرائم الإلكترونية إلى فقدان فرص عمل أو تشويه السمعة، خصوصاً في حالات نشر معلومات مضللة أو سرقة هويات رقمية. وفي أحيان أخرى، يكون الأثر الاجتماعي أكثر عمقاً، إذ قد تتعرض العلاقات الأسرية أو الاجتماعية للاضطراب بسبب الانتهاكات الرقمية، مما يخلق شعوراً دائماً بعدم الأمان وعند استعمال الذكاء الاصطناعي بأسلوب دنيء.

لذلك، أصبح فهم طبيعة الجرائم الإلكترونية وآلياتها ونتائجها على الأفراد ضرورة أساسية، ليس فقط لحماية البيانات الشخصية، بل للحفاظ على شعور الأمان والثقة في البيئة الرقمية. ومن هذا المنطلق، تتضح الحاجة الملحة إلى تعزيز الثقافة الرقمية للأفراد، وإلى تطوير حلول وقائية تشريعية وتقنية تقي المجتمع من مخاطر هذه الجرائم المتزايدة.

وبذلك قسمنا المبحث إلى مطلبين نتناول فيها أسباب الجرائم الإلكترونية على الأفراد وذلك في المطلب الأول، أما المطلب الثاني تأثير الجرائم الإلكترونية على الأفراد.

المطلب الأول: أسباب الجرائم الإلكترونية على الأفراد:

في العقدين الأخيرين، أصبح الفضاء الرقمي جزء لا يتجزأ من حياتنا اليومية. لم يعد الإنترنت مجرد وسيلة للتواصل أو الترفيه، بل تحول إلى مساحة واسعة للعمل والتعليم والتجارة، مما جعل الأفراد يقضون ساعات طويلة في التفاعل مع الشبكات الرقمية. ومع هذا الانتشار، ظهرت الجرائم الإلكترونية كظاهرة حديثة تمس الأفراد بشكل مباشر، وتؤثر في حياتهم المالية، النفسية، والاجتماعية. فقد أظهرت الدراسات أن الأضرار التي تلحق بالأفراد جراء هذه الجرائم لا تقتصر على فقدان المال أو البيانات، بل تمتد لتشمل فقدان الخصوصية والثقة بالبيئة الرقمية، وهو ما يبرز الحاجة إلى فهم الأسباب التي تدفع الأفراد للانخراط في هذه الأنشطة الإجرامية. [2]

تتداخل العوامل الاجتماعية في كثير من الأحيان مع السلوك الإجرامي للأفراد على الإنترنت. فالبيئة الأسرية

[1] خالد إبراهيم ممدوح، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2010، ص12.
[2] مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، دار النهضة العربية، القاهرة، 2008، ص23.

والمجتمع المحيط تلعب دوراً مركزياً في تشكيل وعي الفرد الرقمي، وقد أظهرت الدراسات أن ضعف الرقابة الأسرية وغياب التوجيه، بالإضافة إلى التأثير السلبي للأقران، يمكن أن يدفع الشباب إلى استكشاف أساليب غير قانونية لكسب المال أو لتحقيق النفوذ الرقمي. في دراسة ميدانية أجراها المركز القومي للبحوث الاجتماعية والجنائية [3]، تبين أن ارتفاع معدلات البطالة والفقر، بالإضافة إلى ضعف الرقابة الأسرية، يمثل عوامل مهمة تدفع الأفراد نحو الانخراط في الجرائم الإلكترونية، سواء كانت لغرض مالي أو لتحقيق شعور بالسيطرة.

علاوة على العوامل الاجتماعية، تلعب الدوافع النفسية والسلوكية دوراً كبيراً في تفسير أسباب الجرائم الإلكترونية. فالكثير من الشباب يجدون في الفضاء الرقمي فرصة للتعبير عن السلطة والسيطرة التي قد تكون غائبة في حياتهم الواقعية، سواء من خلال اختراق الحسابات، أو نشر معلومات شخصية للآخرين، أو حتى ممارسة الابتزاز الإلكتروني. كما أن الفضول والملل يمثلان محفزاً قوياً لدخول عالم الجرائم الرقمية، إذ يبدأ البعض بمحاولة اختبار حدود الفضاء الرقمي، قبل أن يتحول هذا الفضول إلى أفعال غير قانونية أكثر خطورة مع مرور الوقت. [4]

ولا يمكن تجاهل الرغبة في الانتقام أو التعبير عن الغضب كدافع نفسي مباشر. فقد أظهرت دراسة ميدانية في القاهرة أن كثيراً من حالات الابتزاز الرقمي واستخدام المعلومات الشخصية للانتقام كانت نتيجة نزاعات شخصية بين الأفراد، إذ تحولت الخلافات التقليدية إلى صراعات رقمية على الشبكة.

كما أن ضعف الوازع الأخلاقي لدى بعض الأفراد، وغياب الرقابة الذاتية، يجعلهم أقل مقاومة للانزلاق إلى أفعال مخالفة للقانون، خاصة في ظل شعورهم بأن الفضاء الرقمي بعيد عن أي سلطة قضائية مباشرة، فتلعب الظروف الاقتصادية دوراً محورياً في دفع الأفراد للانخراط في الجرائم الإلكترونية. فقد أظهرت الدراسات أن الفقر، وندرة فرص العمل، وتفاوت الدخل، يمكن أن تدفع البعض إلى البحث عن مكاسب سريعة من خلال الفضاء الرقمي، مثل الاحتيال على الحسابات المصرفية، أو التجارة غير القانونية عبر الإنترنت، أو بيع البيانات الشخصية للآخرين. وتوضح دراسة المركز القومي للبحوث الاجتماعية والجنائية أن الضغط الاقتصادي يعد من أهم المحفزات التي تدفع الشباب إلى الانخراط في الاحتيال الرقمي والتجارة غير المشروعة عبر الإنترنت، حيث يسهل الفضاء الرقمي الوصول إلى الأهداف دون قيود جغرافية أو رقابة صارمة. [5]

من جانب آخر، تسهم العوامل التقنية في تهيئة الظروف الملائمة للجرائم الإلكترونية. فسهولة الوصول إلى المعلومات، والثغرات في الأمن الرقمي لدى الأفراد، واستخدام كلمات مرور ضعيفة أو شبكات عامة غير آمنة، تجعل الأفراد أهدافاً سهلة للهجمات الإلكترونية. كما أن التطور التكنولوجي المستمر خلق

[3] جرائم الكمبيوتر والإنترنت في المجتمع المصري، IDSC، 2011، ص45.
[4] يوسف المصري، الجرائم المعلوماتية والرقمية للحاسوب والإنترنت، دار العدالة للنشر القاهرة، 2011، ص34–49.
[5] حاكم إبراهيم، جرائم الإنترنت في المجتمع المصري، دراسة ميدانية بالقاهرة، 2015، ص50–65.

أدوات وأساليب جديدة للجرائم، مثل هجمات الفدية الرقمية، والهندسة الاجتماعية للاحتيال، وسرقة البيانات الشخصية عبر تطبيقات الهواتف الذكية، مما يزيد من فرص وقوع الأفراد ضحايا لهذه الجرائم.

ولا يخفى الدور الكبير الذي تلعبه القوانين والوعي القانوني في الحد من هذه الجرائم. فضعف إدراك الأفراد للعقوبات المترتبة على أفعالهم الإلكترونية يضاعف احتمالات ارتكابها. وفي هذا السياق، جاء قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 في مصر ليضع إطاراً تشريعياً واضحاً لمعاقبة الجرائم الإلكترونية وحماية الأفراد، إلا أن نجاحه يتوقف على فعالية تطبيقه ووعي المجتمع بالقوانين. [6]

تلعب وسائل التواصل الاجتماعي أيضاً دوراً محورياً في انتشار الجرائم الإلكترونية، فهي توفر بيئة خصبة للابتزاز والتحرش الرقمي ونشر المعلومات المضللة. وقد أظهرت الدراسات أن الشباب الذين يقضون أوقاتاً طويلة على هذه الشبكات هم الأكثر عرضة للانخراط في أنشطة غير قانونية، سواء بدافع الفضول أو التسلية أو التقليد الاجتماعي كما أن ضعف التربية الرقمية والتعليم القانوني المرتبط بالاستخدام الآمن للإنترنت يزيد من احتمالات ارتكاب الجرائم، إذ يفتقر الأفراد إلى المعرفة بكيفية حماية أنفسهم ومراعاة القوانين عند استخدامهم للتكنولوجيا.

ختاماً، يمكن القول إن أسباب الجرائم الإلكترونية لدى الأفراد متعددة الأبعاد، تتداخل فيها العوامل الاجتماعية والنفسية والاقتصادية والتقنية والتشريعية. فالشباب يمثلون الفئة الأكثر عرضة لهذه الجرائم نتيجة لمزيج من الفضول، والملل، وضغوط الحياة، وسهولة الوصول إلى التكنولوجيا، وضعف الوعي القانوني. وللحد من هذه الظاهرة، بات من الضروري تطوير برامج توعية رقمية، وتعزيز التعليم القانوني والرقمي، وتشديد العقوبات، وتحسين الأمن السيبراني، بما يسهم في خلق بيئة رقمية آمنة وحماية الأفراد والمجتمع من مخاطر الجرائم الإلكترونية.

المطلب الثاني: تأثير الجرائم الإلكترونية على الأفراد:

تأثير الجرائم الإلكترونية على الأفراد لا يقف عند مجرد الخسارة المالية. ففي كثير من الأحيان تتجاوز الأضرار المادية لتلامس الجانب النفسي والاجتماعي والأخلاقي، وتترك آثاراً عميقة في نفسية الضحية. فبعد حادثة سامح، بدأ يشعر بعدم الأمان في استخدام أي خدمة إلكترونية، وظهر عليه الخوف من تعرض بياناته للسرقة مرة أخرى، حتى في أبسط تصرفات حياته اليومية عبر الإنترنت. وقد وصف الباحث يوسف المصري هذه التأثيرات في كتابه الجرائم المعلوماتية والرقمية للحاسوب والإنترنت، مؤكداً أن الجرائم الإلكترونية تتسبب في ازدواج الخسارة: خسارة مالية يتبعها توتر نفسي وقلق دائم بانتظار هجوم آخر. [7]

وليس الخوف النفسي وحده ما يختبره الضحايا؛ فهناك وصمة اجتماعية مرتبطة أحياناً بالضحايا، خاصة في حالة اختراق المعلومات الشخصية أو تسريب الصور أو البيانات الخاصة. فعلى سبيل المثال، تعرّضت

[6] مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية دار النهضة، القاهرة، 2008، ص78–92.
[7] يوسف المصري، الجرائم المعلوماتية والرقمية للحاسوب والإنترنت، دار العدالة للنشر والتوزيع القاهرة، 2011، ص172.

شابة تدعى ندى لموقف محرج عندما تسربت محادثاتها الخاصة بعد تعرض حسابها للقرصنة، ما أثّر على علاقتها الأسرية والاجتماعية. وهنا يشير محمد نصر محمد في كتابه الجرائم الإلكترونية ومخاطرها إلى أن من أخطر ما تسبّبه هذه الجرائم هو الإيذاء المعنوي الذي يصيب الفرد حين تستغل بياناته الخاصة بطرق تشعِره بالإذلال والخزي. [8]

أما الطرف الثالث في هذه المعادلة، فهو العلاقات الاجتماعية التي تتأثر بدورها، إذ يعزل بعض الأفراد أنفسهم عن الشبكات الاجتماعية بعد أن صاروا عرضة للتجارب السيئة على الإنترنت. الشباب واليافعون الذين يمضون ساعات طويلة على الإنترنت يشيعون في ممارساتهم الطبيعية، لكن بعد تعرضهم لاختراق أو تشهير إلكتروني، يصبحون أكثر حذراً، أو حتى انسحاباً اجتماعياً، خشية تكرار التجربة. في هذا السياق، تؤكد الدراسات الميدانية أن الخجل والانسحاب الاجتماعي من أبرز الآثار النفسية التي تلاحق ضحايا الجرائم الإلكترونية، فتتحول شبكة الإنترنت من مساحة للحرية والتواصل إلى "منطقة خطر".

ولننظر الآن إلى البعد المهني: كثير من الأفراد يفقدون فرص عمل أو تتصدّر سيرتهم الذاتية علامة استفهام بعد أن تستغل بياناتهم على الإنترنت أو تشوه صورتهم في مواقع التواصل ومن المؤثرات التي لا ترى بالعين المجردة، تلك المتعلقة بالهوية الرقمية. فالمراجع الشخصية التي تسرَق أو تستغل تولّد شعوراً بفقدان الذات، إذ يشعر الفرد أن جزءاً من "حياته الرقمية" قد صار خارج إرادته. وقد ناقش هذا البعد الاجتماعي المعنوي في دراسات عربية عدة، مشيراً إلى أن الهوية الرقمية أصبحت امتداداً للهوية الحقيقية، وأن المساس بها يمس كيان الفرد نفسه.

ولا يمكن إغفال تأثير الجرائم الإلكترونية على الصحة النفسية. فالإحباط، واضطرابات القلق، وحتى الاكتئاب أصبحت من التجارب المشتركة بين العديد من ضحايا الهجمات الإلكترونية. وهذا لا يعني أن كل من يتعرّض لحادثة إلكترونية سي صاب بمرض نفسي، لكن كثيرين يطورون احتمالات عالية للاضطرابات النفسية نتيجة الضغط الذي يصاحب جرائم مثل الاحتيال المالي، أو الانتهاكات المتعلقة بالخصوصية. [9]

وقد أظهرت الدراسات أن العائدات المالية السريعة التي يتحصّل عليها المجرمون الإلكترونيون تفاقم من خطورة هذه الظاهرة، لأن الأفراد الذين يشعرون بالاستغلال أو الظلم الاجتماعي قد يلجؤون هم أنفسهم إلى أعمال غير قانونية، ما يجعل تأثير الجرائم الإلكترونية حلقة متشابكة تلتهم كل من الفاعل والضحية والمجتمع.

وعلى المستوى القانوني والعملي في مصر، فإن الجرائم الإلكترونية أثارت نقاشات جدّية بين واضعي القانون والممارسين القانونيين حول كيفية حماية الأفراد من هذه الأفعال، وكان من نتيجة هذه المناقشات صدور

[8] محمد نصر محمد، الجرائم الإلكترونية ومخاطرها، مصر، مركز الدراسات العربية، 2015، ص98–110.
[9] مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، دار النهضة العربية، 2008، ص141.

قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، الذي وضع ضمن أهدافه حماية البيانات الشخصية وتأمين البيئة الرقمية للأفراد، باعتبار أن التأثير على الفرد لا يتوقف عند لحظة الجريمة وحدها، بل يمتد إلى تأثير دائم على علاقة الفرد بالتكنولوجيا نفسها.

من هنا، لا يمكن النظر إلى تأثير الجرائم الإلكترونية على الأفراد كأمر ثانوي أو عابر، بل يجب التعامل معه كجزء لا يتجزأ من قضايا العدالة الاجتماعية والأمن النفسي والقانوني. فعندما يسرَق حساب بنكي أو ت نشر صور خاصة على الإنترنت، يتعرض الفرد لكسر في أساسيات الأمان، ليس فقط على مستوى المال، بل على مستوى السلامة النفسية والاجتماعية والمهنية.

إضافة إلى ما سبق، لا يمكن إغفال تأثير الجرائم الإلكترونية على الثقة الشخصية والاجتماعية لدى الأفراد. فبعد تعرض الشخص للاحتيال الرقمي أو اختراق حساباته، غالباً ما يشعر بعدم القدرة على التعامل بثقة مع منصات الإنترنت، وقد يمتنع عن استخدام الخدمات الإلكترونية حتى في الأمور البسيطة، مثل التسوق أو التواصل مع الأصدقاء. هذا الانكماش الرقمي لا يقتصر أثره على الفرد نفسه، بل يمتد ليؤثر على علاقاته الأسرية والاجتماعية، إذ يميل البعض إلى العزلة والانطواء خوفاً من تكرار التجربة أو التعرض للإحراج مرة أخرى.

إضافة لذلك، تشير الدراسات إلى أن التعرض المتكرر للجرائم الإلكترونية قد يؤدي إلى اضطرابات نفسية طويلة الأمد، تشمل القلق المزمن، والاكتئاب، وفقدان الثقة بالآخرين. [10] التكيف مع الحياة الرقمية الحديثة

المبحث الثاني: الجرائم الإلكترونية وأثرها على المؤسسات

في السنوات الأخيرة، أصبح الفضاء الرقمي جزءً أساسياً من حياة المؤسسات، سواء كانت شركات تجارية أو مؤسسات تعليمية أو هيئات حكومية. ومع هذا الاعتماد الكبير على الشبكات الرقمية والحواسيب، ظهرت الجرائم الإلكترونية كتهديد مباشر يواجه قدرة هذه المؤسسات على العمل بكفاءة وأمان. لم تعد الهجمات الرقمية مجرد اختراقات عابرة، بل تحولت إلى أحداث قادرة على تعطيل العمليات الأساسية، وتسريب البيانات الحساسة، أو ابتزاز المؤسسات مالياً ومعنوياً، لتصبح مسألة الأمن الرقمي ضرورة لا غنى عنها لكل كيان يعتمد على التكنولوجيا.

حيث تتأثر المؤسسات أيضاً على صعيد السمعة والثقة. فحين تتعرض بيانات العملاء أو الموظفين للتسريب، ينعكس ذلك على الصورة العامة للكيان، ويقلل من ثقة الشركاء والجمهور. وغالباً ما تحتاج المؤسسات إلى سنوات طويلة لإعادة بناء هذه الثقة، وهي عملية معقدة وصعبة، لا تقتصر على الإجراءات

[10] محمد نصر محمد، الجرائم الإلكترونية ومخاطرها، مركز الدراسات العربية للنشر والتوزيع، مصر، 2015، ص 115–120.

التقنية فقط، بل تشمل التفاعل مع الجمهور وإظهار الالتزام بحماية بياناتهم. [11]

تتجلى التحديات أيضاً على صعيد الإدارة الداخلية والعمليات التشغيلية. فالهجمات الرقمية تشتت انتباه الفرق التقنية وتستنزف مواردها، مما يؤدي إلى تأخير المشاريع وتعطيل سير العمل، خاصة في المؤسسات التي تعتمد على قواعد بيانات مركزية أو شبكات متصلة بالإنترنت. كما أن الضغوط النفسية التي يعاني منها الموظفون بعد التعرض لهجوم إلكتروني تزيد من صعوبة الإدارة، وتضعف الروح المعنوية، وقد تؤدي إلى انخفاض الإنتاجية أو ارتفاع معدل الانسحاب الوظيفي.

باختصار، تأثير الجرائم الإلكترونية على المؤسسات يمتد إلى ما هو أبعد من الخسائر المالية، فهو يشمل السمعة، والبنية التكنولوجية، والإجراءات القانونية، وحتى الجانب البشري داخل المؤسسة. لذا أصبح من الضروري اعتماد سياسات أمنية شاملة، وزيادة الوعي القانوني والتقني لدى جميع العاملين، لضمان قدرة المؤسسات على حماية بياناتها والحفاظ على استمرارية عملها في بيئة رقمية متزايدة التعقيد.

وندرس في هذا المبحث (الجرائم الإلكترونية وأثرها على المؤسسات) الفرع الأول، أما الفرع الثاني نتناول فيه (الجرائم الإلكترونية وأثرها على المجتمع).

المطلب الأول: الجرائم الإلكترونية وأثرها على المؤسسات:

في عالم اليوم، لم تعد التكنولوجيا مجرد وسيلة مساعدة في العمل، بل أصبحت العمود الفقري لكل مؤسسة، من الشركات التجارية إلى البنوك، ومن الهيئات الحكومية إلى المنظمات غير الربحية. كل شيء أصبح مرتبطا بالأنظمة الرقمية: المعاملات، التخزين، التواصل، وحتى اتخاذ القرارات الإدارية. ومع هذا التوسع، برزت الجرائم الإلكترونية كتهديد واقعي وحقيقي، ليس على مستوى البيانات فقط، بل على مستوى استقرار المؤسسات وسمعتها وثقة عملائها.

في أحد الأيام، اكتشفت مؤسسة مالية في القاهرة أن نظامها الإلكتروني تعرض لاختراق، وأن بيانات العملاء الشخصية تم الوصول إليها. كانت هذه اللحظة صادمة، إذ لم يكن التأثير المالي وحده ما يقلق الإدارة، بل الخوف من فقدان الثقة التي بنتها المؤسسة على مدار سنوات طويلة. هنا يتضح مفهوم الجرائم الإلكترونية كما يعرفه عبد الله عبد الكريم عبد الله في كتابه جرائم المعلوماتية والإنترنت (الجرائم الإلكترونية)، حيث يوضح أن أي فعل غير مشروع باستخدام الشبكات الرقمية يهدف إلى الإضرار بالمؤسسات أو الأفراد يعد جريمة إلكترونية. [12]

مع تتابع الأحداث، بدأ تأثير هذا الاختراق يظهر على المؤسسة بشكل متعدد الأبعاد. فقد تعطلت أنظمة

[11] عبد العال الدريبي، محمد صادق إسماعيل، الجرائم الإلكترونية: دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية، المركز القومي للإصدارات القانونية القاهرة، 2012، ص112.

[12] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت (الجرائم الإلكترونية): دراسة مقارنة في النظام القانونية، منشورات الحلبي الحقوقية، بيروت، 2007، ص23.

الدفع الإلكتروني، وتوقف البريد الداخلي عن العمل، مما تسبب في تأخير المعاملات وخسائر مالية فورية. في الوقت ذاته، انتشرت أنباء الاختراق بين العملاء ووسائل الإعلام، فبدأت السمعة المؤسسية تتآكل، وأصبح الحفاظ على الثقة تحديا يوميا [13]، هنا يظهر بوضوح ما ذكره عبد الإله النوايسة في كتابه جرائم تكنولوجيا المعلومات، حول أن المؤسسات تواجه تبعات مالية وقانونية وأخلاقية عند تعرض بياناتها الرقمية للاختراق.

أما الجانب المادي، رغم أهميته، ليس وحده ما يعكس خطورة الجرائم الإلكترونية. فالاختراقات غالباً ما تكشف عن ثغرات تشغيلية وتقنية في النظام الرقمي للمؤسسة، ما يجعلها بحاجة إلى إعادة تقييم بنيتها الداخلية وإعادة تصميم أنظمتها لحماية البيانات. الموظفون الذين اكتشفوا أن بياناتهم الخاصة معرضة للانكشاف شعروا بعدم الأمان والخوف من المستقبل الرقمي، ما أثر بدوره على إنتاجيتهم وارتباطهم بالعمل. هذه الأبعاد النفسية والإدارية لا تقل أهمية عن الأبعاد التقنية أو القانونية.

لكن المؤسسات الذكية لا تنتظر وقوع الكارثة لتتعلم. فقد بدأت بعض المؤسسات بتبني ثقافة الأمن الرقمي، حيث يتم تدريب الموظفين على اكتشاف رسائل التصيد الاحتيالي، واستخدام كلمات مرور قوية، وفهم طبيعة التهديدات الرقمية الحديثة. كما تبنت بعض المؤسسات نظم حماية متقدمة ومراقبة مستمرة للأنظمة، بحيث يمكن اكتشاف أي اختراق في لحظته، قبل أن يتحول إلى كارثة. [14]

القصص الواقعية في المؤسسات العربية تعكس هذه الصورة. في إحدى شركات الاتصالات، أدى اختراق أحد الخوادم إلى تسريب بيانات العملاء ومعلومات عن الخدمات المتعاقد عليها، مما أجبر الإدارة على الإعلان عن الخرق، وتعويض العملاء، وإعادة تصميم نظم الحماية بالكامل. كانت هذه التجربة مكلفة مالياً وتشغيلياً، لكنها علمت المؤسسة درساً مهماً: أن الوقاية أفضل من العلاج، وأن الاستثمار في الأمن الرقمي ضرورة استراتيجية، لا خياراً تكميلياً.

وفي السياق ذاته، تشير الدراسات القانونية إلى أن التشريعات وحدها لا تكفي لحماية المؤسسات. فالقوانين الرقمية بحاجة إلى تنظيمات تشغيلية داخلية، مثل سياسات الاستجابة للطوارئ، وأنظمة مراقبة الأنظمة، وبرامج تدريب مستمرة للموظفين. هذه الاستراتيجية الشاملة هي ما يحد من المخاطر الرقمية ويجعل المؤسسة أكثر قدرة على الصمود أمام الهجمات [15] وتهيئة رقابة إلكترونية متطورة ونواكب التطورات المشاركة عالمياً بهذا الخصوص مع إشراك العاملين على ذلك وفق دورات تطويرية مستمرة.

---

[13] عبد الإله محمد النوايسة، جرائم تكنولوجيا المعلومات: شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، دار وائل للطباعة والنشر والتوزيع، عمان، 2017، ص112.

[14] عبد الإله النوايسة، حول التكامل بين الحماية التقنية والوعي القانوني والإداري لحماية المؤسسة من المخاطر الرقمية، دار وائل للطباعة والنشر، عمان، 2017، ص200.

[15] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت (الجرائم الإلكترونية)، مرجع سابق، ص27.

المطلب الثاني: الجرائم الإلكترونية وأثرها على المجتمع:

في العصر الرقمي الحديث، أصبح الإنترنت جزءًا أساسيًا من حياة الأفراد، فهو وسيلة للتواصل، والتعليم، والعمل، والترفيه. ومع انتشار هذا العالم الافتراضي، برزت الجرائم الإلكترونية كتهديد حقيقي للأفراد والمجتمع، إذ لم تعد هذه الجرائم مجرد أعمال فردية، بل أصبحت تؤثر في الأمن الاجتماعي والاقتصادي والثقافي. الفضاء الرقمي، رغم فوائده العديدة، يمثل بيئة خصبة لانتهاك الخصوصية، والاحتيال المالي، والابتزاز، ونشر الشائعات، وهو ما يجعل المجتمع في مواجهة تحديات مستمرة تتطلب اهتمامًا قانونياً واجتماعياً.

تظهر آثار الجرائم الإلكترونية على المجتمع في جوانب عدة، أولها البعد الاقتصادي. فالخسائر المالية التي تتعرض لها الأفراد والشركات والمؤسسات بسبب الاختراقات الرقمية أو الاحتيال الإلكتروني تؤثر على الثقة في التعاملات الإلكترونية وتضعف الاستثمار. ومع استمرار مثل هذه الجرائم، يشعر المجتمع بعدم الأمان، ويقلل من الاعتماد على التجارة الرقمية والخدمات الإلكترونية، وهو ما ينعكس على الاقتصاد ككل. كما أن هذه الجرائم تؤثر على تماسك المجتمع، إذ تثير شعورا بالقلق وعدم الاطمئنان بين الأفراد، ما يضعف الروابط الاجتماعية ويؤثر على التفاعلات اليومية. [16]

من الناحية القانونية، تحتاج المجتمعات إلى تطوير تشريعات فعالة لمواجهة الجرائم الإلكترونية، بما يضمن حماية الأفراد والمؤسسات، وتفعيل الرقابة الإلكترونية، وتدريب فرق التحقيق الجنائي الرقمي على أساليب التعامل مع الأدلة الرقمية. وفي غياب التشريعات المناسبة أو تطبيقها بشكل ضعيف، يصبح المجتمع أكثر عرضة للانفلات الرقمي، وانتشار محتوى ضار أو غير قانوني، مما يزيد من المشاكل الاجتماعية والنفسية بين الأفراد. [17]

كما أن للجرائم الإلكترونية آثارًا نفسية واضحة على الأفراد، فهي تؤدي إلى فقدان الخصوصية، والتعرض للابتزاز، وتقويض الثقة بالنفس وبالآخرين. الأطفال والمراهقون هم الأكثر عرضة لهذه الآثار بسبب اعتمادهم الكبير على الإنترنت ووسائل التواصل الاجتماعي [18]، وتُظهر الدراسات أن هؤلاء الضحايا قد يعانون من تأثيرات طويلة الأمد، تشمل القلق والاكتئاب، وانعكاس ذلك على الأداء الدراسي والمهني.

ولا يمكن إغفال البعد الثقافي والتربوي لهذه الجرائم، إذ يساهم انتشار المعلومات المضللة والشائعات في تشويه القيم المجتمعية، ويؤثر في تشكيل وعي الأفراد، خاصة بين الشباب. فالاعتماد المفرط على الإنترنت والانفتاح الكبير على المحتوى الرقمي يجعل المجتمع أكثر هشاشة أمام محاولات التأثير الرقمي [19]، سواء لأغراض سياسية أو اقتصادية أو اجتماعية، وهو ما يبرز أهمية التربية الرقمية.

---

[16] أحمد الحسيني، الجرائم الإلكترونية وتأثيرها على المجتمع، دار النهضة العربية، القاهرة، 2018، ص45.
[17] علي الموسوي، الجريمة الإلكترونية في المجتمعات العربية، دار الكتب القانونية، مصر، 2017، ص140.
[18] محمد النجار، أمن المعلومات والجرائم الإلكترونية، دار الفكر العربي، مصر، 2019، ص105.
[19] خالد سليم، الجرائم الإلكترونية وأثرها على المجتمع، دار المعارف، القاهرة، 2016، ص88.

من هنا، أصبح من الضروري تبني استراتيجيات شاملة لمواجهة الجرائم الإلكترونية، تشمل رفع الوعي الرقمي، وتعزيز الثقافة القانونية، وتطبيق القوانين الرادعة، وتطوير أدوات الحماية الرقمية. فالمجتمع الذي يفتقر إلى هذه الإجراءات يصبح أكثر عرضة للخطر، ويصعب عليه حماية أفراده ومؤسساته من تبعات الجرائم الإلكترونية. وعليه، فإن مكافحة هذه الظاهرة تتطلب تكاتف الجهود القانونية والاجتماعية والتربوية لضمان بيئة رقمية آمنة ومستقرة، تحمي الحقوق الفردية والجماعية على حد سواء.

في نهاية المطاف، يمكن القول إن الجرائم الإلكترونية ليست مجرد تهديد تقني، بل هي تحد شامل للأبعاد المالية، القانونية، التشغيلية، والإنسانية للمؤسسات. فكل اختراق، كل تسريب بيانات، وكل تعطيل للنظام هو درس واقعي يفرض على المؤسسات إعادة التفكير في استراتيجياتها وحماية بنيتها التحتية الرقمية، وتعزيز وعي موظفيها، وتأمين علاقاتها مع المجتمع والشركاء القانونيين والتجاريين وتوسع المواقع والبرامج المختلفة وإشراك الأشخاص الطبيعية والمعنوية بهذهِ المواقع دون اكتراث بحسابات المنافع والمضار لديهِ كامل الأثر في عمليات الانتهاكات لذات الخصوصية العامة والخاصة.

الخاتمة

في رحلتنا عبر عالم الجرائم الإلكترونية، اتضح لنا أن هذه الظاهرة ليست مجرد تهديد تقني عابر، بل هي عبارة عن قوى خفية تمتد آثارها لتطال كل جانب من جوانب حياة الأفراد والمؤسسات. فقد بدأت القصة مع الأفراد، أولئك الذين أصبحوا يعيشون في بيئة رقمية متصلة بشكل دائم، حيث يعتمدون على الإنترنت في التواصل، والتعلم، والعمل، والتسوق، وحتى إدارة شؤونهم الشخصية. ومع هذا الاعتماد، أصبح الأفراد أكثر عرضة من غيرهم لمخاطر رقمية متنوعة، بدءً من سرقة الهوية، مروراً بالابتزاز، وانتهاء بخسارة الأموال أو البيانات الحساسة. كل عملية اختراق أو تهديد إلكتروني تترك أثراً نفسياً ملموساً شخصياً، يعكس شعوراً بعدم الأمان وفقدان السيطرة على حياتهم الرقمية واليومية، وهو ما يشير إليه الباحثون في مجال الجرائم المعلوماتية مثل يوسف المصري في كتابه الجرائم المعلوماتية والرقمية للحاسوب والإنترنت، حيث يؤكد أن الانتهاكات الرقمية للأفراد غالباً ما تترك أثراً طويل المدى على حياتهم الشخصية بالمجتمع الذي سرعان ما تتداول بهِ هذهِ التصرفات وخاصة الأخلاقية.

ولم تتوقف التداعيات عند الأفراد، بل امتدت لتطال المؤسسات، التي تمثل العمود الفقري للاقتصاد الرقمي. فقد كشفت التجارب الواقعية أن أي اختراق للنظم المؤسسية أو تسريب للبيانات يمكن أن يخلّ ببنية العمل، ويؤدي إلى خسائر مالية فادحة، وتراجع الإنتاجية، وحتى انهيار الثقة بين المؤسسة وعملائها وشركائها التجاريين. فالمؤسسات، سواء كانت صغيرة أو كبيرة، أصبحت تعيش في عالم لا يرحم الضعف الرقمي، حيث يمكن لهجمة إلكترونية واحدة أن توقف العمليات الحيوية، وتعرّض بيانات العملاء للخطر، وتلحق أضراراً لا يمكن إصلاحها بسهولة. كما يشير عبد الإله النوايسة في كتابه جرائم تكنولوجيا المعلومات إلى أن المؤسسات التي لا تستثمر في نظم حماية متقدمة وتثقيف موظفيها حول أساليب الوقاية الرقمية،

تجد نفسها أكثر عرضة للهجمات، ما يعرضها لمساءلة قانونية وغرامات من الجهات الرقابية ناهيكم عن جرائم الإزعاج بواسطة استخدام الأجهزة الأكثر تطوراً وتكنلوجيا حديثة.

ومع ذلك، فإن السردية الإنسانية لهذه الظاهرة لا تقتصر على الجانب السلبي. ففي قلب كل تهديد، يوجد درس وفرصة للنمو والتعلم. فقد أظهرت التجارب أن المؤسسات التي تتبنى ثقافة وعي أمني شامل، وتدمج بين التكنولوجيا الحديثة، والإجراءات القانونية، والتدريب المستمر للموظفين، تكون أكثر قدرة على الصمود أمام الهجمات الإلكترونية، بل ويمكنها تحويل أي أزمة إلى فرصة لتقوية بنيتها المؤسسية. وبالمثل، يستطيع الأفراد الذين يتلقون التوعية الرقمية والإرشاد حول أساليب الحماية أن يقللوا من تعرضهم للخطر ويستعيدوا شعورهم بالأمان الرقمي.

في النهاية، يمكن القول إن الجرائم الإلكترونية أصبحت جزءً لا يتجزأ من المشهد الرقمي العالمي، تؤثر بشكل مباشر على حياة الأفراد ومستقبل المؤسسات على حد سواء. فهي ليست مجرد أرقام أو بيانات، بل تجارب حقيقية يعيشها الناس والمؤسسات يومياً، تحمل في طياتها دروساً حول أهمية الحماية الرقمية، والوعي القانوني، والثقافة التقنية، والتعاون المجتمعي. إن مواجهة هذه التحديات تتطلب أكثر من الحلول التقنية، بل تحتاج إلى استراتيجيات شاملة تتكامل فيها الجوانب التقنية والقانونية والتربوية والإدارية، لضمان بيئة رقمية آمنة ومستدامة، تحمي مصالح الأفراد والمؤسسات على حد سواء، وتؤمن استمرار الأعمال، وتعزز الثقة في الاقتصاد الرقمي، وتخلق مجتمعاً واعياً قادراً على التكيف مع التحديات الرقمية المعقدة ناهيك بأنها برزت في وقت مبكر مع العولمة والأمن السيبراني والبرامج الإلكترونية والخوارزميات الحديثة رغم صدور بعض القوانين والعقوبات مع انتشارها ولكن لا نزال نحتاج إلى تنظيم قانوني واضح لكل حرب إلكترونية لاختلافها بالمضمون وعلى سبيل المثال أخذ القانون العراقي:

- المادة 403 التي تعاقب على كتب وصور مخلة بالحياء.
- المادة 433 جرائم القذف والسب والتهجم.
- المادة 434 تجرم السب بالتوثيق وصدور قانون جرائم المعلوماتية.

وفي نهاية هذا البحث سنعمل على ذكر أهم الاستنتاجات والمقترحات التي توصلنا لها وهي:

أولاً: الاستنتاجات

1. تأثير شامل ومتعدد المستويات: تظهر التجربة الرقمية أن الجرائم الإلكترونية تتجاوز مجرد الخسائر المالية، لتطال الجوانب القانونية والإدارية والنفسية والاجتماعية للأفراد والمؤسسات على حد سواء، مما يجعلها تحدياً مركباً يتطلب فهماً متكاملاً.
2. أهمية الوعي والتثقيف الرقمي: المؤسسات والأفراد الذين يفتقرون إلى المعرفة بأساليب الحماية الرقمية يكونون أكثر عرضة للمخاطر، بينما أولئك الذين يتلقون تدريباً مستمراً في الأمن السيبراني يمكنهم التخفيف من آثار أي اختراق محتمل.

3. السمعة والثقة كأصل حساس: أي اختراق أو تسريب للبيانات يترك أثراً يمتد على المدى الطويل، فقد يؤدي إلى فقدان ثقة العملاء أو الشركاء التجاريين، ويؤثر في سمعة المؤسسة أو الفرد، وهو ما يصعب تعويضه بمجرد استعادة الأنظمة التقنية.
4. ضرورة التكامل بين الحلول: الحد من المخاطر الرقمية لا يتحقق بالاعتماد على جانب واحد، بل يحتاج إلى مزج استراتيجيات تقنية، وإجراءات إدارية، وتدريب قانوني، لخلق حماية شاملة وفعالة ضد أي تهديد محتمل.
5. فرص التعلم من التجارب السابقة: كل حادثة اختراق تمثل درساً عملياً، يتيح للمؤسسات والأفراد تعزيز نظم الحماية، إعادة صياغة السياسات الداخلية، وزيادة القدرة على مواجهة التهديدات المستقبلية بفعالية أكبر.

ثانياً: المقترحات

1. تعزيز الثقافة الرقمية: تصميم برامج تدريبية دورية وورش توعية للموظفين والأفراد، تهدف إلى تعليمهم كيفية التعرف على التهديدات الرقمية والتعامل معها بطريقة عملية وفعالة.
2. وضع سياسات حماية متكاملة: تطوير بروتوكولات أمنية شاملة تشمل حماية البيانات، مراقبة الأنظمة، وخطط استجابة للطوارئ، لضمان استعداد المؤسسة لأي اختراق محتمل.
3. تحديث التشريعات والقوانين: مراجعة الأطر القانونية بشكل دوري لتواكب التطورات التكنولوجية، وتوضيح المسؤوليات، وتحديد العقوبات المناسبة للحد من الجرائم الإلكترونية.
4. تعزيز التعاون بين الجهات: تشجيع تبادل الخبرات والمعلومات بين المؤسسات الحكومية والخاصة، بالإضافة إلى المشاركة في مبادرات مشتركة لرصد التهديدات وتبادل أفضل الممارسات في الأمن السيبراني.
5. تتدخل الدولة بشكل كبير فيما يلي:
   - عمل برامج أساسية وإيضاحية وتطويرية للمجتمع.
   - تأسيس إدارة متخصصة لديها السلطان والإشراف والمتابعة على جميع البرامج المتخصصة بهكذا نشاطات وخصوصاً ما يكون منها يتسبب في هلاكات المجتمع وتدميره وانتهاك الخصوصيات الفردية والمجتمعية.
   - تدخل الدولة في عمل البرامج الخاصة بهذا الشأن مع شبكات الإعلام وتدخل الدولة في عمل مع المؤسسات الأمنية لتتدخل بسرعة لكشف الفاعلين الأصليين.
   - العمل على تنظيف المجتمع من كل رواسب المجتمع ما بعد إحداث 2003 بسبب الانقلاب الأمني الكبير ودخول الإنترنت والبرامج والهواتف والحواسيب دون ضوابط ومعرفة علمية وقانونية وثقافية وشرح المخاطر من جراء الاستعمال لذلك.
   - تسديد العقوبة على الإساءات الإلكترونية التي تتعلق بالجوانب الأخلاقية للأفراد وجرائم الإزعاج.

قائمة المصادر والمراجع

أولاً: الكتب:

1. أحمد الحسيني، الجرائم الإلكترونية وتأثيرها على المجتمع، دار النهضة العربية، القاهرة، 2018.
2. حاكم إبراهيم، جرائم الإنترنت في المجتمع المصري، دراسة ميدانية بالقاهرة، 2015.
3. خالد إبراهيم ممدوح، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2010.
4. خالد سليم، الجرائم الإلكترونية وأثرها على المجتمع، دار المعارف، القاهرة، 2016.
5. عبد الإله النوايسة، حول التكامل بين الحماية التقنية والوعي القانوني والإداري لحماية المؤسسة من المخاطر الرقمية، دار وائل للطباعة والنشر، عمان، 2017.
6. عبد الإله محمد النوايسة، جرائم تكنولوجيا المعلومات، شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، دار وائل للطباعة والنشر والتوزيع، عمان، 2017.
7. عبد العال الدريبي، محمد صادق إسماعيل، الجرائم الإلكترونية: دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية، المركز القومي للإصدارات القانونية القاهرة، 2012.
8. عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت (الجرائم الإلكترونية): دراسة مقارنة في النظام القانونية، منشورات الحلبي الحقوقية، بيروت، 2007.
9. علي الموسوي، الجريمة الإلكترونية في المجتمعات العربية، دار الكتب القانونية، مصر، 2017.
10. محمد النجار، أمن المعلومات والجرائم الإلكترونية، دار الفكر العربي، مصر، 2019.
11. محمد نصر محمد، الجرائم الإلكترونية ومخاطرها، مركز الدراسات العربية، مصر، 2015.
12. محمد نصر محمد، الجرائم الإلكترونية ومخاطرها، مركز الدراسات العربية للنشر والتوزيع، مصر، 2015.
13. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية دار النهضة، القاهرة، 2008.
14. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، دار النهضة العربية، القاهرة، 2008.
15. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، دار النهضة العربية، 2008.
16. يوسف المصري، الجرائم المعلوماتية والرقمية للحاسوب والإنترنت، دار العدالة للنشر القاهرة، 2011.
17. يوسف المصري، الجرائم المعلوماتية والرقمية للحاسوب والإنترنت، دار العدالة للنشر والتوزيع القاهرة، 2011.