HNSJ Humanities & Natural Sciences Journal
ISSN: (e) 2709-0833
www.hnjournal.net

مجلة العلوم الإنسانية والطبيعية
مجلة علمية محكمة (التصنيف: NSP)
معامل التأثير العربي للعام 2024 = 0.44

عنوان البحث

آثار استخدام الذكاء الاصطناعي في الجرائم الدولية

عمار حسين ترف المسعودي[1]

[1] الجامعة الإسلامية في لبنان.

اشراف الاستاذ الدكتور: محمد عبده

HNSJ, 2026, 7(4); https://doi.org/10.53796/hnsj74/47

المعرف العلمي العربي للأبحاث: https://arsri.org/10000/74/47

تاريخ الاستقبال: 2026/03/12م تاريخ القبول: 2026/03/20م تاريخ النشر: 2026/04/01م

المستخلص

تتناول هذه الدراسة آثار استخدام الذكاء الاصطناعي في الجرائم الدولية، في ظل ما أفرزه التطور التقني من أنماط إجرامية مستحدثة تتجاوز الحدود التقليدية للجريمة من حيث الوسائل والنطاق وصعوبة الملاحقة. وتهدف الدراسة إلى بيان صور توظيف الذكاء الاصطناعي في ارتكاب الجرائم ذات البعد الدولي، سواء من قبل الدول من خلال الهجمات السيبرانية وجرائم التجسس والاحتيال والسرقة الإلكترونية، أو من قبل الأفراد عبر جرائم التهديد والابتزاز وانتهاك البيانات الشخصية. اعتمدت الدراسة على المنهج الوصفي التحليلي، من خلال تحليل طبيعة هذه الجرائم وآثارها القانونية والأمنية، مع الإشارة إلى أوجه القصور في الأطر التشريعية التقليدية في مواجهة الجرائم الذكية العابرة للحدود. وقد خلصت الدراسة إلى أن الذكاء الاصطناعي أصبح أداة فعالة في تطوير الأساليب الإجرامية وزيادة خطورتها، إذ يمنح الجناة قدرة أكبر على التخفي، وتحليل البيانات، واختراق الأنظمة، وتنفيذ الهجمات بطرق معقدة يصعب كشفها بالوسائل التقليدية. كما بينت الدراسة أن الطابع العابر للحدود لهذه الجرائم يثير تحديات جوهرية تتعلق بالاختصاص القضائي، وجمع الأدلة الرقمية، وتحديد المسؤولية الجنائية. وتوصي الدراسة بضرورة تحديث التشريعات الوطنية، ووضع أطر قانونية واضحة لاستخدام الذكاء الاصطناعي، وتعزيز التعاون الدولي في مكافحة الجرائم السيبرانية، وتطوير آليات رقابية وتقنية قادرة على الكشف المبكر عن إساءة استخدام هذه التقنيات، بما يحقق التوازن بين الاستفادة من الذكاء الاصطناعي وحماية أمن الدول وحقوق الأفراد.

الكلمات المفتاحية: الذكاء الاصطناعي؛ الجرائم الدولية؛ الجرائم السيبرانية؛ التجسس الإلكتروني؛ الابتزاز الإلكتروني؛ حماية البيانات الشخصية.

RESEARCH TITLE

The Effects of Using Artificial Intelligence in International Crimes

Abstract

This study examines the effects of using artificial intelligence in international crimes in light of the technological developments that have produced new criminal patterns exceeding the traditional limits of crime in terms of methods, scope, and difficulty of prosecution. The study aims to identify the forms in which artificial intelligence is employed in committing crimes of an international dimension, whether by states through cyberattacks, espionage, fraud, and electronic theft, or by individuals through threats, extortion, and violations of personal data. The study adopts the descriptive analytical method by analyzing the nature of these crimes and their legal and security implications, while highlighting the shortcomings of traditional legislative frameworks in confronting smart transnational crimes. The study concludes that artificial intelligence has become an effective tool in developing criminal methods and increasing their seriousness, as it gives perpetrators greater ability to conceal their identities, analyze data, penetrate systems, and carry out attacks through complex methods that are difficult to detect using traditional means. The study also shows that the transnational nature of these crimes raises fundamental challenges related to jurisdiction, the collection of digital evidence, and the determination of criminal liability. It recommends updating national legislation, establishing clear legal frameworks for the use of artificial intelligence, strengthening international cooperation in combating cybercrime, and developing regulatory and technical mechanisms capable of early detection of the misuse of these technologies, in a way that balances the benefits of artificial intelligence with the protection of state security and individual rights.

Key Words: Artificial Intelligence; International Crimes; Cybercrime; Cyber Espionage; Electronic Extortion; Personal Data Protection.

المقدمة

إن سهولة استخدام الذكاء الاصطناعي وتوفره بشكل كبير وتمتعه بمميزات عالية الدقة، جعلته مركز اهتمام لجماعات الإجرام الرقمي والتكنولوجي، والاحتيال وغيرها من الجرائم التي تقوم بها هذه المجموعات ضد الدول والأفراد[1].

لذا إن استخدام الذكاء الاصطناعي في الجرائم الدولية يشكل تحديًا كبيرًا ويرتب من جراء ذلك آثار سلبية على المجتمعات والدول من خلال تعزيز التكنولوجيا للمجرمين ويمكنهم من تطوير أدوات وتقنيات متقدمة لتنفيذ الجرائم، حيث يستخدم القراصنة والمهاجمون الذكاء الاصطناعي في اختراق الأنظمة الأمنية والوصول غير المشروع إلى المعلومات الحساسة وتنفيذ هجمات سيبرانية متقدمة.

ويتميز الذكاء الاصطناعي بالسرعة والدقة والفعالية في تنفيذ الجرائم ويمكن استخدام تقنيات التعرف على الوجود والمراقبة الآلية لتحديد الأهداف وتتبع حركاتهم بشكل سريع ودقيق.

ويشكل استخدام الذكاء الاصطناعي تهديدًا للأمان السيبراني العالمي، حيث يمكن استغلاله في شن هجمات سيبرانية على البنية التحتية الحيوية للدول والمؤسسات ويمكن لهذه الهجمات تسبب أضرارًا كبيرة وتعطيل الخدمات الحيوية.

أهمية البحث

تنبع أهمية هذا البحث من خطورة الجرائم المرتكبة باستخدام الذكاء الاصطناعي، وما تخلّفه من آثار قانونية وأمنية واقتصادية على المستويين الوطني والدولي. كما تتجلى أهمية البحث في مساهمته في تسليط الضوء على التحديات التي تواجه الأنظمة القانونية في مواجهة الجرائم الذكية العابرة للحدود، وبيان الحاجة الملحّة إلى تطوير التشريعات وتعزيز آليات التعاون الدولي، بما يضمن حماية حقوق الأفراد وصون أمن الدول في ظل التحول الرقمي المتسارع.

أهداف البحث

يهدف هذا البحث إلى:

1. بيان مفهوم استخدام الذكاء الاصطناعي في الجرائم الدولية وأبرز صوره.
2. تحليل الآثار القانونية والأمنية المترتبة على الجرائم المرتكبة باستخدام الذكاء الاصطناعي.
3. التمييز بين الجرائم المرتكبة من قبل الدول وتلك التي يرتكبها الأفراد باستخدام الذكاء الاصطناعي.
4. إبراز أوجه القصور في التشريعات القائمة في مواجهة الجرائم المرتبطة بالذكاء الاصطناعي.
5. اقتراح آليات قانونية وتشريعية تسهم في الحد من مخاطر هذه الجرائم.

إشكالية البحث

تتمحور إشكالية هذا البحث حول التساؤل الرئيسي الآتي:

إلى أي مدى يسهم استخدام الذكاء الاصطناعي في تطور الجرائم الدولية، وما مدى كفاية الأطر القانونية القائمة في مواجهتها؟

ويتفرع عن هذا التساؤل عدد من التساؤلات الفرعية، من أبرزها:

-ما هي أبرز صور الجرائم الدولية المرتكبة باستخدام الذكاء الاصطناعي؟

-ما الآثار القانونية والأمنية المترتبة على هذه الجرائم؟

-هل التشريعات الحالية قادرة على مواكبة الجرائم الذكية العابرة للحدود؟

[1] محمود ثائر، مقدمة في الذكاء الاصطناعي، مكتبة المجتمع العربي والتوزيع، عمان، الأردن، 2009، ص 23.

منهج البحث

اعتمد هذا البحث على المنهج الوصفي التحليلي، من خلال وصف الظاهرة المتمثلة في استخدام الذكاء الاصطناعي في الجرائم الدولية، وتحليل آثارها القانونية والأمنية. كما تم الاستعانة بالمنهج المقارن عند الاقتضاء، لبيان أوجه الاختلاف والتشابه بين بعض التشريعات في تنظيمها للجرائم المرتبطة بالذكاء الاصطناعي، إضافة إلى الاستفادة من الدراسات الفقهية والآراء القانونية ذات الصلة.

خطة الدراسة:

للإجابة على الإشكالية المطروحة سنتناول خطة البحث التالية وتقسيمه إلى مطلبين:

المطلب الأول: آثار استعمال الذكاء الاصطناعي من قبل الدول.

المطلب الثاني: آثار استعمال الذكاء الاصطناعي من قبل الأفراد.

المطلب الأول

آثار استعمال الذكاء الاصطناعي من قبل الدول

إن استخدام الذكاء الاصطناعي من قبل الدول يتنوع بشكل كبير ويشمل مجموعة واسعة من التطبيقات والأغراض، يعتبر الذكاء الاصطناعي تكنولوجيا حيوية قوية تساعد الدول في تعزيز القدرات وتحسين الخدمات المقدمة للمواطنين، بالإضافة إلى دوره في القطاعات الاقتصادية والأمنية[1].

على الرغم من الفوائد المحتملة للاستخدامات، فإن الذكاء الاصطناعي من قبل الدول يثير أيضًا قضايا أخلاقية وقانونية، مثل الخصوصية والتحكم والتمييز والتأثير في سوق العمل، لذا يجب أن تتبع الدول سياسات قانونية صارمة لضمان استخدام الذكاء الاصطناعي بطريقة مسؤولة.

إذ يجب توصية استخدام الذكاء الاصطناعي بواسطة الدول بما يحترم حقوق الأفراد ويضمن الشفافية والمساءلة وأن يتم تطوير السياسات والتشريعات التي تحدد المعايير والقواعد لاستخدام الذكاء الاصطناعي في مختلف المجالات، وضمان وجود آليات للرقابة والمراقبة لمنع سوء الاستخدام والتجاوز.

وفقاً لما تقدم سنتناول هذا المطلب من خلال الفرعين التاليين:

الفرع الأول: الجرائم السيبرانية وجرائم التجسس

الفرع الثاني: جرائم الاحتيال وجرائم السرقة

الفرع الأول

الجرائم السيبرانية وجرائم التجسس

إن ظهور الاعتداءات، والجرائم الإلكترونية، المعروفة أيضًا بالقرصنة السيبرانية وجرائم التجسس قد أصبحت تهديدًا خطيرًا يواجه العديد من الدول حول العالم.

[1] أشرف الراعي، التحري والإستدلال عن الجرائم عبر أنظمة الذكاء الاصطناعي، مجلة جامعة الزيتونة الأردنية للدراسات القانونية، المجلد 4، الأردن، 2023، ص 163.

أولاً- الجرائم السيبرانية:

تشير العديد من الدراسات إلى أن القراصنة السبيرانيين يستهدفون بشكل خاص البنية التحتية الحكومية ووسائل النقل العالمية، وذلك من خلال محاولة السيطرة على الأجهزة والأنظمة المتصلة بالإنترنت[1].

تزداد أهمية هذه القضية مع انتشار أجهزة الاتصال المتصلة بالإنترنت وأنظمة الأجهزة المتطورة، فكلما زاد عدد الأجهزة المتصلة بالإنترنت، زادت فرص القراصنة للقيام بأعمال تخريبية والاعتداء على أمن الدولة والنظم الحكومية.

بالتالي فإن البنية التحتية للدول تكون مكشوفة لهجمات القرصنة السيبرانية، وهذا يشكل تهديدًا كبيرًا على إستقرار الدول وسلامتها.

لمواجهة هذا التهديد، تعمل الحكومات والمنظمات الدولية على تعزيز قدراتها في مجال الأمن السبيراني والحماية من الاعتداءات الإلكترونية[2].

تشكل هذه الجهود إنشاء إطار قانوني قوي لمكافحة الجرائم الإلكترونية، وتعزيز التعاون الدولي في مجال مشاركة المعلومات وتبادل الخبرات، وتطوير تقنيات الحماية السيبرانية المتقدمة.

علاوة على ذلك، ينبغي على الشركات والمؤسسات أن يتبنوا ممارسات أمنية قوية لحماية الأنظمة والبيانات من الهجمات الإلكترونية، يشمل ذلك استخدام برامج مضادة للفيروسات وتحديثها بإنتظام، واستخدام كلمات مرور قوية وتغييرها بشكل دوري، والابتعاد عن فتح رسائل البريد الإلكتروني المشبوهة أو تحميل الملفات غير المعروفة.

لذا يجب أن تكون القضايا المتعلقة بالأمن السبيراني من أولويات الدول والمنظمات، ويجب على الأفراد والمؤسسات أن يكونوا مستعدين لمواجهة هذا التهديد المتزايد من خلال تبني إجراءات أمنية قوية، والتعاون في سبيل مكافحة الجرائم والاعتداءات الإلكترونية والجرائم السيبرانية التي تشكل تهديدًا خطيرًا على الدول والبنية التحتية الحكومية.

وتشير الدراسات إلى أن هذه الاعتداءات تزداد انتشارًا مع زيادة استخدام الأجهزة المتصلة بالإنترنت والتكنولوجيا المتقدمة.

تتضمن الاعتداءات الإلكترونية القرصنة السيبرانية من خلال السيطرة على الأجهزة والأنظمة الحكومية للدول، ويستغل القراصنة ثغرات الأمان، والضعف في الأنظمة لاختراقها وسرقة المعلومات الحساسة أو التلاعب بها أو تعطيل الخدمات الحكومية[1].

لمكافحة هذا التهديد، تعمل الدول على تعزيز قدراتها في مجال الأمن السبيراني وتطوير استراتيجيات للوقاية والاستجابة للهجمات الإلكترونية.

يتضمن ذلك التوعية والتدريب للموظفين الحكوميين حول أمن المعلومات وممارسات السلامة السيبرانية.

كما تعمل الحكومات على تعزيز التعاون الدولي في مجال مشاركة المعلومات وتبادل الخبرات في مجال الأمن السبيراني بالإضافة إلى ذلك، ينبغي على الدولة وأجهزتها اتخاذ إجراءات لحماية أنفسهم وأنظمتهم من الاعتداءات الإلكترونية. ويشمل ذلك استخدام برامج مضادة للفيروسات وتحديثها بإنتظام، وتعزيز الأمان واستخدام تقنيات التحقق وتوفير نسخ احتياطية للملفات الحساسة[2].

---

[1] غادة المنجم، الذكاء الاصطناعي، جامعة الملك سعود، الرياض، 2009، ص 63.

[2] محمود ثائر، مقدمة في الذكاء الاصطناعي، المرجع السابق، ص26.

[1] أشرف الراعي، التحري والإستدلال عن الجرائم، المرجع السابق، ص 169.

[2] غادة المنجم، الذكاء الاصطناعي، المرجع السابق، ص 77.

من المتوقع أن تشمل الهجمات السيبرانية التسلل إلى الأجهزة القابلة للاختراق.

يقوم القراصنة بالبحث عن ثغرات في الأنظمة والأجهزة للاختراق والوصول إلى المعلومات الحساسة أو تعطيل الخدمات تلك الهجمات السيبرانية تشكل عبئًا كبيرًا على الدول وأمنها، ويمكن أن تتسبب في أضرار مادية جسيمة فعندما يتم اختراق أجهزة الحكومة، يمكن أن يحدث توقف في الخدمات ما يؤثر على الاقتصاد والحياة اليومية للمواطنين.

علاوة على ذلك يمكن أن تتسبب الهجمات السيبرانية في تسريب المعلومات الحساسة والسرقة الإلكترونية مما يرتب على ذلك تبعات جسيمة[3].

فقد يترتب على ذلك تعرض الشركات والمؤسسات لفقدان المال، سواء بسبب سرقة البيانات المالية والاحتيال الإلكتروني.

من جانب الدولة، يمكن أن تؤدي الهجمات السيبرانية إلى تعطيل الأنظمة الحكومية والمؤسسات الحيوية مثل الشبكات الكهربائية أو أنظمة المياه والشركات وغيرها من تلق الممتلكات الحكومية وتعطيل العمليات الحكومية، مما يتطلب جهودًا وموارد مالية لإصلاح الأضرار وإستعادة النظام الطبيعي.

ثانيًا- جرائم التجسس:

إن التطور الهائل في تكنولوجيا الأجهزة الذكية، بما في ذلك التقدم في مجال الذكاء الاصطناعي، قد أدى إلى ظهور تحديات جديدة في مجال جرائم التجسس.

قد يستخدم الذكاء الاصطناعي وتقنيات التعلم الآلي لتنفيذ هجمات تجسسية متقدمة، فمثلاً يمكن استخدام الذكاء الاصطناعي لتحليل البيانات الكبيرة وإستخلاص أنماط ومعلومات حساسة منها، أو لتنفيذ هجمات احتيالية متقدمة لإبتكار طرق جديدة للتلاعب بالضحايا.

تعد جرائم التجسس باستخدام الذكاء الاصطناعي أمرًا خطيرًا، حيث يمكن استخدام الأجهزة ذات الذكاء الاصطناعي للتجسس على المؤسسات والحكومات، وسرقة المعلومات الحساسة بطرق متطورة وصعبة التعرف عليها[1].

إذًا إن جرائم التجسس باستخدام الذكاء الاصطناعي تستهدف سرقة المعلومات من الدول والمؤسسات والمنظمات، وتتضمن تجسسًا على مختلف أنواع المعلومات بما في ذلك البيانات السياسية والاقتصادية والعسكرية وغيرها.

توفر التكنولوجيا الحديثة تقنيات الذكاء الاصطناعي حرية أكبر وسهولة في تنفيذ عمليات التجسس بعيدًا عن الرقابة التقليدية.

تشمل جرائم التجسس الإلكتروني اختراق المواقع والصفحات الإلكترونية بهدف الوصول إلى المعلومات والبيانات الحساسة، وكذلك إرسال رسائل بريد إلكتروني تحتوي على ملفات برمجية مضرة تستخدم لسرقة المعلومات والتجسس على الأجهزة الذكية[2].

نذكر أن جرائم التجسس يمكن أن تتم باستخدام أي وسيلة تكنولوجية متاحة.

---

[3] محمود ثائر، مقدمة في الذكاء الاصطناعي، المرجع السابق، ص 51.

[1] الأمير عبد القادر حفوظة، حسام غرادين، الجريمة الإلكترونية وآليات التصدي لها، مداخلة قدمت ضمن أعمال الملتقى الوطني، آليات مكافحة الجرائم الإلكترونية، مركز جبل البحث العلمي، جامعة الجزائر، 2017، ص 84.

[2] محمود أحمد عباينة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، 2009، ص 47.

تتطور تقنيات التجسس باستمرار وتستخدم أدوات وأساليب متنوعة للاستيلاء على المعلومات الحساسة. وذلك عن طريق اختراق الأجهزة الذكية من قبل المهاجمين والتسلل للوصول إلى المعلومات المخزنة والمطلوبة.

قد يتم استخدام تقنيات التعلم الآلي بتطوير برامج خبيثة قادرة على اختراق الأجهزة الذكية وسرقة المعلومات. ويمكن استخدام الذكاء الاصطناعي لإستخراج المعلومات الحساسة والبيانات من الشبكة والأجهزة بطرق متقدمة[1].

يمكن تحليل كميات ضخمة من البيانات لاكتشاف الأنماط مما يزيد من خطورة الجرائم التجسسية.

التصيد الاحتيالي بواسطة الذكاء الاصطناعي من خلال إنشاء رسائل احتيالية وإيماءات اجتذابية تستهدف المؤسسات الحكومية والأنظمة التابعة لها بهدف الحصول على المعلومات السرية أو تنفيذ هجمات أخرى، يمكن استخدام الذكاء الاصطناعي في تنفيذ هجمات متقدمة تتلاعب بالبيانات وتعطل الأنظمة الحاسوبية إذ يمكن للمهاجمين استخدام تقنيات التعلم الآلي لتحسين قدرات الهجوم وتجنب اكتشافهم[2].

قد يكون الهدف من خلال عملية التجسس لمعرفة المواقف السياسية لصنّاع القرار في الدولة والمعلومات التي تتعلق بالسياسة الداخلية والخارجية التي تنتهجها الدولة.

أو التي تنوي اتباعها أو السير بها، وقد يكون التجسس معنويًا ونفسيًا لشعوب الدول وقادتها ومعرفة مواطن القوة والضعف، وعوامل الوحدة والتفرقة والتيارات والنشازات القائمة داخل الدولة[3].

إضافة إلى التجسس الاقتصادي لمعرفة قدرات الدولة وحجم الإنتاج وميزانها التجاري والاحتياط المتوفر لديها، والمدة التي تستطيع الاعتماد على ذاتها وكذلك معرفة المرافق الاقتصادية الحيوية لديها.

كما يمكن أن يكون التجسس لمعرفة المعلومات الصناعية والعلمية والتطرق إلى أسرار هذه الصناعات والأبحاث العلمية المرتبطة بها، خاصة إذا كانت هذه الصناعات تتعلق بالدفاع الوطني، فهناك شركات تسهم في الإنتاج الحربي وتطوير الأسلحة، وقد يكون التجسس العلمي لمعرفة الدراسات العلمية المتطورة المرتبطة بالمجال الزراعي أو الهندسة أو الصحة[1].

لمكافحة هذه الجرائم، يجب على الدول والمؤسسات تعزيز الوعي الأمني واعتماد التدابير الوقائية مثل تحديث البرامج والأجهزة بإنتظام واستخدام حلول الأمان المتقدمة.

كما يجب على الشركات المصنعة بتكثيف الجهود لتعزيز الأمان في تصميم الأجهزة الذكية وتطبيقاتها وتقنيات الذكاء الاصطناعي[2].

بالإضافة إلى ذلك، يجب أن يكون هناك تركيز على حماية البيانات الخاصة التابعة للدولة أو المؤسسات القائمة وذلك من خلال اتخاذ إجراءات صارمة لحماية المعلومات الحساسة في جميع جوانب التصميم والتطوير في عصر الذكاء الاصطناعي.

---

[1] مصطفى سمارة، الجريمة الإلكترونية، مجلة المعلوماتية، العدد 29، الأردن، تموز 2008، ص 74.

[2] طارق عطية، الأمن المعلوماتي والنظام القانوني للحماية والمعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2003، ص 322.

[3] أيمن عبد الحفيظ، الإتجاهات النفسية والأمنية لمواجهة الجرائم المعلوماتية، 2005، ص 36.

[1] محمد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، 2005، ص 41.

[2] طارق عطية، الأمن المعلوماتي والنظام القانوني للحماية والمعلوماتية، المرجع السابق، ص325.

الفرع الثاني

جرائم الاحتيال وجرائم السرقة

يعتبر استخدام الذكاء الاصطناعي من جرائم الاحتيال وجرائم السرقة أمرًا ذا أهمية كبيرة. يمكن للمجرمين الاستفادة من تطور التكنولوجيا واستخدام القدرات المتقدمة للذكاء الاصطناعي لتنفيذ جرائم مالية تستهدف الدول ومؤسساتها[1].

تحظى جرائم الاحتيال وجرائم السرقة باستخدام الذكاء الاصطناعي الاهتمام العالمي، وتتطلب مكافحتها استراتيجيات شاملة وتعاون دولي قوي، إذ يجب على الدول تعزيز التشريعات والقوانين المتعلقة بمكافحة جرائم الاحتيال باستخدام الذكاء الاصطناعي وتعزيز التعاون لتبادل المعلومات والخبرات، كما ينبغي تعزيز القدرات التخفيفية والتقنية للتعامل مع هذه الجرائم وتعزيز التوعية بين الجمهور والمؤسسات المالية للتعرف على التهديدات واتخاذ التدابير الوقائية المناسبة.

أولاً–جرائم الاحتيال:

يعد الاحتيال الإلكتروني صورة من صور الاحتيال بشكل عام، ولكنه يتميز ببعض السمات التي تميزه عن الأشكال الآخرى، وذلك بسبب ارتباطه بتكنولوجيا المعلومات والذكاء الاصطناعي، حيث يمكن وصف الاحتيال بأنه طلب حيلة أو استخدام أو خداع للحصول على شيء من الآخرين بطرق غير مشروعة[2].

يتم استخدام الاحتيال الإلكتروني عندما يتم انتهاكات حقوق البيانات أو الحصول على معلومات بطرق غير مرخصة، ومنذ ظهور التكنولوجيا الذكية والذكاء الاصطناعي، دخلت عمليات الاحتيال والنصب في عالم الإلكترونيات والشبكات ومن ثم اتخذت أشكال جديدة من التكنولوجيا الذكية، تتميز جريمة الاحتيال الإلكتروني بأنها تختلف عن الجرائم التقليدية في العديد من النواحي، فعلى سبيل المثال فقلة الحالات التي يتم اكتشافها مقارنة بالجرائم التقليدية، وكذلك عدم وجود عنف في الاحتيال الإلكتروني كما هو موجود في الجرائم الآخرى[3].

إضافة إلى تختلف الأسباب أو العوامل التي تدفع إلى ارتكاب جريمة الاحتيال الإلكتروني عن الجريمة التقليدية[1]. لذلك يمكن القول إن الاحتيال الإلكتروني غير الذكاء الاصطناعي ووسائطه يهدف إلى تحقيق أرباح مالية غير مشروعة، ويتم ارتكاب جرائم الاحتيال باستخدام الأجهزة الإلكترونية المتطورة كوسيلة لتنفيذ الجريمة وبالتالي من الصعوبة الوصول إلى معرفة المجرمين.

كما أنه من الصعوبة جدًا على المجرم التوقف عند حد معين من جريمته عندما يكتشف أن هناك بابًا خفيًا يمكن الخروج منه أي الخروج من النظام[2].

إذًا يمكن استخدام الذكاء الاصطناعي لاختراق أنظمة الحكومة والتلاعب في البيانات أو تزوير الوثائق الرسمية بهدف الحصول على فوائد سياسية أو اقتصادية غير مشروعة[3].

ويمكن استخدام الذكاء الاصطناعي لمهاجمة المواقع الإلكترونية وأنظمة الحكومة مثل تعطيل البنية التحتية الحيوية

---

[1] خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2009، ص 86.

[2] هشام رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، 1994، ص 47.

[3] محمد محرم علي، جريمة النصب والاحتيال والتجارة الإلكترونية، دار النهضة، القاهرة، 1998، ص 9.

[1] نائلة قورة، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية تطبيقية، منشورات الحلبي، القاهرة، 2005، ص 223.

[2] طارق الشدي، آلية البناء الأمني لنظم المعلومات، دار الوطن للطباعة، الرياض، 2003، ص 19.

[3] منير الجنبهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، عام 2005، ص 135.

أو سرقة المعلومات الحساسة، وتنفيذ حملات تظليلية عبر وسائل التواصل الإجتماعي أو تلاعب في النظم واللوائح لأغراض معينة وتشويه العمل الديمقراطي. وأيضًا يمكن استخدام الذكاء الاصطناعي من خلال إنشاء وتنظيم أدوات أساليب احتيال للتلاعب بالأنظمة المالية العائدة للدولة لتحقيق مكاسب اقتصادية غير مشروعة أو للتسبب في اضطرابات، والتلاعب في الأسواق، حيث يمكن لخوارزميات الذكاء الاصطناعي تحليل كميات ضخمة من البيانات المالية لتحديد الأنماط وتنفيذ المعاملات الاحتيالية على نطاق واسع[4].

لذلك يترتب على أفعال جرائم الاحتيال الإلكتروني تنفيذها من قبل الجناة بهدف سرقة أموال أو المعلومات أو البيانات من داخل الأجهزة الإلكترونية العائدة لدولة أو مؤسسات أو شركات أخرى وذلك عن طريق استخدام شبكة المعلوماتية أو وسائل أخرى متعلقة ومرتبطة بالذكاء الاصطناعي، وعلى الرغم من تنوع الأشكال والأساليب التي يتم اتباعها في جرائم الاحتيال[5]، إلاّ أنها جميعًا تستهدف الوصول إلى هدف واحد، وهو التلاعب بالبيانات والمعلومات، وبالتالي تتميز جرائم الاحتيال بالإبتكار والتطوير المستمر لبرامجها وأساليبها المعتمدة وذلك مع مواكبة التطورات الحاصلة في حماية الذكاء الاصطناعي وهو ما يتم استخدامه من الوجهة السلبية[1].

وتستخدم الذكاء الاصطناعي في جرائم الاحتيال الإلكتروني لتحسين كفاءة وفعالية العمليات الاحتيالية، كاستخدام تقنيات التعلم الآلي وتحليل البيانات الضخمة لاختراق الأمان والوصول إلى المعلومات المالية الحساسة[2]، كما يمكن استخدام الذكاء الاصطناعي في إنشاء برامج وأدوات تساعد وتساهم في إجراء عمليات احتيال مستهدفة ومتقدمة.

مثل استعمال عمليات الاحتيال عبر البريد الإلكتروني المزيف، وكما يمكن استخدام الذكاء الاصطناعي في إنشاء برامج لكشف البيانات وبطاقات التعريف لسرقة المعلومات.

ثانيًا– جرائم السرقة:

إن جريمة السرقة باستخدام الذكاء الاصطناعي يشير إلى استخدام التقنيات والأدوات المبنية على الذكاء الاصطناعي في أنشطة السرقة الإلكترونية.

ثم استغلال القدرات التحليلية والتعلم الآلي للذكاء الاصطناعي لتنفيذ هذه الجريمة والاختراق بطرق متقدمة ومتطورة.

لذلك إن جريمة السرقة الإلكترونية تختلف عن السرقة التقليدية في عدة أنواع، وتتميز بطابع خاص[3].

فمن الخصوصيات البارزة للسرقة الإلكترونية أن المجرم يقوم عن عمد بالتدخل في نطاق النظم الإلكترونية والمعلوماتية المختلفة، بما في ذلك الذكاء الاصطناعي وما يتضمنه من تقنيات وأيضًا الدخول إلى البيانات الإلكترونية سواء في جمعها أو تجهيزها من أجل الوصول إلى المعلومات المطلوبة، كما يتدخل المرتكب أيضًا في مجال معالجة النصوص والكلمات بدقة باستخدام الوسائل المتاحة لديه فيغير نص الوثيقة أو يقوم بسرقتها[4].

لذا تعد جريمة السرقة الإلكترونية أو باستخدام الذكاء الاصطناعي من الجرائم الخطيرة التي تؤثر على المصالح المشروعة بين الدول سواء كانت مادية أو معنوية.

---

[4] خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، المرجع السابق، ص 89.

[5] أحمد تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، 2000، ص 73.

[1] هشام رستم، جرائم الحاسب المستحدثة، دار الكتب القانونية، القاهرة، 1999، ص 111.

[2] عبدالله عبدالله، جرائم المعلوماتية والإنترنت: الجرائم الإلكترونية، منشورات الحلبي، بيروت، 2011، ص 26.

[3] ناصر بن محمد النعيمي، جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية، دون دار نشر، السعودية، 2009، ص 82.

[4] محمد الشوابكة، جرائم الحاسوب والإنترنت، الجريمة المعلوماتية، دار النهضة العربية، عمان، 2011، ص 142.

فهي تنطوي على استخدام غير قانوني لتكنولوجيا المعلوماتية وتهدف إلى الاعتماد على هذه المصالح.

تتضمن جريمة السرقة الإلكترونية العديد من العناصر التي تختلف عن الجرائم التقليدية، مثل البيانات والنصوص والصور والأشكال والأحداث والرموز والقواعد البيانية وبرامج الحاسوب وغيرها من العناصر المشابهة التي تنشأ وتخزن أو تعالج أو تراسل بواسطة الوسائل الإلكترونية[1].

لقد عرفت جريمة السرقة الإلكترونية بأنها استخدام غير قانوني للتكنولوجيا والذكاء الاصطناعي، واء بالقيام بأعمال غير مشروعة أو بالإمتناع عن القيام بأعمال مشروعة وبهدف الاعتداء على مصالح الدول المشروعة سواء كانت مادية أو معنوية.

يتم استخدام الذكاء الاصطناعي لاختراق أنظمة الحماية والأمان والوصول بطريقة غير مشروعة إلى البيانات والمعلومات الحساسة للدولة أو للشركات والمؤسسات الحكومية وثم استخدام تقنيات التعلم الآلي لتطوير نماذج وأدوات تستخدم في عمليات السرقة والإختلاس المالي عبر الإنترنت مثل اختراق الحسابات المصرفية لدولة ما أو استخدام البطاقات الائتمانية بشكل غير قانوني[2].

ويجمع الذكاء الاصطناعي بين تقنيات الاختراق الإلكتروني والتعلم الآلي لتنفيذ هجمات متقدمة تستفيد من القدرات التحليلية والتكيفية للذكاء الاصطناعي في جرائم السرقة الإلكترونية.

إن أعمال السرقة باستخدام الذكاء الاصطناعي غالبًا ما يتم تنفيذها من قبل أطراف ومجموعات تمتلك مستوى عال من العلم والمعرفة والدهاء بالإضافة إلى توافر الوسائل والوسائط الإلكترونية من أجهزة تتعلق في مجال الذكاء الاصطناعي[3].

من الخصائص البارزة لجريمة السرقة الإلكترونية هي أنها عابرة للحدود ولها بعد دولي، فإن تنفيذ هذه الجرائم، يتم عبر شبكة المعلومات، مما يعني أنه يمكن للمرتكبين تخطي الحدود الجغرافية والتعامل مع الضحايا من مختلف الدول. وهذا الأمر يثير تحديات قانونية وإدارية وتقنية وسياسية فيما يتعلق بإجراءات الملاحقة الجنائية وتقديم المسؤولين عن هذه الجرائم إلى العدالة.

إن الجرائم الإلكترونية باستخدام الذكاء الاصطناعي يمكن أن يتم بطرق مختلفة، وذلك من خلال سرقة المعلومات المخزنة داخل الأجهزة عن طريق اختراق الأنظمة الأمنية[1].

والحصول على البيانات بطريقة غير مشروعة، ويتم نسخ المعطيات بطريقة غير قانونية دون احترام لحقوق الملكية الفكرية أو دون الحصول على موافقة صاحب البيانات.

لذا تعتبر جرائم السرقة الإلكترونية من المخالفات القانونية الخطيرة وتتطلب جهودًا قوية لمكافحتها وملاحقة المرتكبين ويجب اعتماد الإجراءات القانونية والتقنية لحماية البيانات وتعزيز الأمان الإلكتروني على مستوى المؤسسات والحكومات[2].

وبما أنها جريمة عابرة للحدود لا بد من التعاون الدولي في مجال مكافحة الجرائم المرتبطة بالذكاء الاصطناعي من خلال تبادل المعلومات والممارسات الجيدة والفعالة.

---

[1] أيمن فكري، جرائم نظم المعلوماتية، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2007، ص 96.

[2] كامل السعيد، جرائم الكمبيوتر والجرائم الآخرى في مجال تكنولوجيا المعلومات، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، المنعقد في القاهرة، 25/28/ 1993، دار النهضة العربية، القاهرة، 1993، ص 255.

[3] محمد الشوابكة، جرائم الحاسوب والإنترنت، المرجع السابق، ص 156.

[1] أحمد تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، المرجع السابق، 53.

[2] أيمن فكري، جرائم نظم المعلومات، المرجع السابق، ص 123.

المطلب الثاني

آثار استعمال الذكاء الاصطناعي من قبل الأفراد

إن الجرائم المرتكبة باستعمال الذكاء الاصطناعي من قبل الأفراد هي تشمل العديد من الأنشطة غير القانونية التي يستخدم فيها الذكاء الاصطناعي لتحقيق أهدافهم.

يقوم الأشخاص أصحاب الخبرة الإحترافية في مجال الذكاء الاصطناعي والتكنولوجيا باستخدام الأجهزة المتطورة مثل أجهزة الكمبيوتر والهواتف الذكية وغيرها من التقنيات الحديثة لارتكاب هذه الجرائم.

لقد أدى الاستخدام المتزايد للذكاء الاصطناعي والأجهزة المتطورة واستخدام الشبكات والأنظمة المعلوماتية[1]، إلى كثير من المخاطر، إذ أفرز هذا التطور الفائق أنواعًا جديدة من الجرائم المرتبطة بالذكاء الاصطناعي[2]، وظهرت جرائم ملازمة لهذا التطور في التكنولوجيا والمعلومات والوسائط الإلكترونية والتي ساعدت بدورها إلى إحداث الجرائم بسهولة وسرعة، حيث ألغت معها الحدود الجغرافية والسياسية للدول، وأصبحت سلاحًا ذو حدين يتمكن هذا التطور التكنولوجي أن يستخدم لصالح الخير والمنفعة العامة للأفراد والمجتمع والدولة. ويمكن استخدام هذا التطور في الذكاء الاصطناعي في تكنولوجيا المعلومات والأجهزة الإلكترونية الوجه السلبي وذلك من خلال تنفيذ الجرائم باستخدامها. كونها تطال في اعتداءاتها قيمًا جوهرية تختص الأفراد في كافة نواحي الحياة دون استثناء، كما أن هذه الجرائم تترك في النفوس تصورًا بعدم الأمان وغياب الثقة، الأمر الذي يؤدي إلى تهديد هذه التقنية لحياة الأفراد وأمنهم.

وفقًا لما تقدم سنتناول هذا المطلب من خلال الفرعين التاليين:

الفرع الأول: جرائم التهديد وجرائم الابتزاز.

الفرع الثاني: جرائم انتهاك البيانات الشخصية.

الفرع الأول

جرائم التهديد وجرائم الابتزاز

لقد أدى التطور الحاصل في مجال تكنولوجيا المعلومات والذكاء الاصطناعي فقد أتاح هذا التطور نقل النشاط بكافة أشكاله إلى عالم الإفتراضي، وعلى الرغم من الفوائد الكبيرة لهذا التطور إلاّ أنه ينطوي على خطر حقيقي يمثل في انتهاك الخصوصية وسرية المعلومات[1].

لذا قد أصبح من الممكن جمع وتخزين المعلومات والوصول إليها بطرق وأساليب غير مشروعة وغير قانونية، دون علم صاحبها، وهذا يشكل اعتداءً على حياة الأشخاص لذا تعد جرائم التهديد وجرائم الابتزاز الإلكتروني عن الجرائم الهامة في هذا السياق، حيث تختلف هذه الجريمة من حيث الصفة للضحية المستهدفة والأهداف المرتقبة.

فبعض الجرائم ذات النمط القائم على الذكاء الاصطناعي تستهدف الأفراد بشكل مباشر وأيضًا بشكل غير مباشر. ولكن الهدف الذي يسعى إليه المجرم هو تحقيق مصالحه الخاصة والشخصية على حساب الضحية[2].

---

[1] هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة،1992،ص 6.

[2] أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2006، ص 67.

[1] عبد الرحمن بن راشد، جرائم الحاسب الآلي، الخطر الآلي، الخطر الحقيقي في عصر المعلومات، المجلة العربية للدراسات الأمنية والتدريب، المجلد 15، الرياض، 2015، ص 181.

[2] عراب مريم، جريمة التهديد والابتزاز الإلكتروني، مجلة الدراسات القانونية المقارنة، كلية الحقوق، جامعة الجزائر، 2021، ص 1210.

لذلك يجب العمل على تعزيز الوعي والمعرفة بأهمية الأمن الإلكتروني وتوفير الحماية اللازمة للبيانات الشخصية والمعلومات الحسابية.

أولاً- جرائم التهديد:

لقد أدى توسع استخدام تقنيات الذكاء الاصطناعي والتي من ضمنها وسائل الاتصالات وشبكة الإنترنت والأجهزة المتطورة إلى انتشار جراء التهديد من خلال الذكاء الاصطناعي[3].

وقد أثر هذا الانتشار حول العالم بشكل كبير على مختلف جانب الحياة الخاصة، فيما يتعلق بزيادة مواد الجريمة وخطورتها إذ تتميز هذه الجرائم المستحدثة بخطورتها وقدرتها على أن تنفذ بسهولة من خلال الاستخدام السلبي لتكنولوجيا الذكاء الاصطناعي والتسهيلات التي تقدمها هذه الأجهزة ولا تقتصر آثارها على النطاق المحلي بل تتخطاه بسبب طبيعة الإنترنت وتطور الذكاء الاصطناعي.

بالإضافة إلى ذلك فإن مرتكبي هذه الجرائم تتوفر لديهم العلوم والمعرفة والذكاء في مجال معالجة البيانات والمعلومات وتحليلها إضافة إلى المهارات التقنية، مما يجعل صعوبة في اكتشافها[1].

في ظل هذا الاستخدام السلبي للتكنولوجيا المتطورة يجب إيجاد استراتيجيات فعالة لمكافحة والحد من جرائم التهديد الإلكتروني وذلك من خلال التعاون والتنسيق بين الأفراد والمؤسسات والشركات والأنظمة الحكومية.

والقطاع الخاص والمجتمع المدني، كما يجب تعزيز الوعي العام بأهمية الأمان السيبراني وتوفير التدريب والتثقيف للأفراد بشأن مخاطر جريمة التهديد وكيفية الوقاية منها، حيث يجب أن تتمتع الجهات المختصة بالقدرة على مراقبة وتحليل الأنشطة الإلكترونية وتتبع المتورطين في جرائم التهديد الإلكتروني من خلال استخدام الذكاء الاصطناعي[2].

نظرًا لحداثة ظاهرة هذه الجريمة ونقص التشريعات القانونية التي تنظمها، فإن جرائم التهديد عبر الإنترنت والأجهزة الحديثة تجتاز بطبيعتها الخاصة التي تختلف عن جرائم التهديد التقليدية.

إذ يتم ارتكابها من خلال استخدام الذكاء الاصطناعي عبر أجهزة الاتصال والتكنولوجيا الحديثة التي يستخدمها الفاعل، وهذا ما يعزز من خطورة هذه الجرائم وما تسببه للمجني عليه.

فالفاعل غالبًا ما يستخدم تلك الأجهزة والبقاء بعيدًا ومجهولاً أمام الآخرين، وهذا بدوره يشكل تهديدًا واسعًا على الأفراد والمجتمع[3].

وبسبب غياب تعريف واضح لهذه الجرائم في التشريعات المقارنة، فإنه يتم ترك المسألة للتعامل معها من الناحية الفقهية والقضائية، إذ تعددت التعريفات المطروحة حول هذه الجريمة، واختلاف الفهم والتصنيف وفقًا للتشريعات والأنظمة القانونية المتبعة والقائمة[4].

لذا يمكن تعريف جرائم التهديد الإلكتروني بأنها جميع الجرائم التي تعرض لها الشخص عبر الإنترنت والأجهزة

---

[3] نائلة قورة، جرائم الحاسب الآلي الاقتصادية، المرجع السابق، ص 43.

[1] محمد غانم يونس، الابتزاز الإلكتروني، دراسة في وجهة نظر قانونية ضمن مؤلف الابتزاز الإلكتروني، جريمة العصر الحديث، إصدار وزارة الداخلية العراقية، دار الكتب والوثائق، العراق، 2019، ص 11.

[2] عمار عباس الحسيني، التحقيق الجنائي والوسائل الحديثة في كشف الجريمة، منشورات الحلبي، بيروت، 2015، ص 35.

[3] نائلة قورة، جرائم الحاسب الآلي، المرجع السابق، ص 53.

[4] علي عدنان الفيل، الإجرام الإلكتروني، أساسها وتطورها، دار النهضة العربية، بيروت، 1991، ص 38.

المتطورة بغية إرغامه أو الضغوط عليه أو تهديده للقيام بعمل ما وغالبًا ما يهدد بدفع المال[1].

وتتميز هذه الجرائم بأنها تستخدم التطور التكنولوجي والذكاء الاصطناعي وسيلة لتقنية التهديد من خلال التقنيات المعلوماتية في مختلف تلك القطاعات وهذا ما يميز هذه الجرائم عن غيرها كونها لها خصائص قانونية ويترتب عليها عواقب قانونية جديدة تختلف عن تلك التي تترتب على الجرائم التقليدية.

فجرائم التهديد الإلكتروني أو عبر الذكاء الاصطناعي الحديث تتطلب إطارًا قانونيًا خاصًا ومحدثًا للتعامل مع هذا التطور من الجرائم.

بشكل عام إن جرائم التهديد عبر الذكاء الاصطناعي تعكس التحولات التكنولوجية المتطورة والسريعة في مجال تقنية المعلومات[2].

وتتسم جرائم التهديد الإلكتروني بسهولة حصولها، وصعوبة اكتشاف الجاني بسبب غياب الرقابة الأمنية وإن الضرر الناجم عن هذه الجرائم ليس له حدود، كونها سلوك غير مألوف وغير أخلاقي لا يعرفه المجتمع من قبل وذلك بسبب استخدام تقنيات الذكاء الاصطناعي العالية ولا تحتاج إلى جهد كبير لتنفيذها كالجرائم التقليدية المعروفة من قبل، وهي من الجرائم غير المقيدة بزمان أو مكان أو بأشخاص محددة، إذ تتميز بالتباعد الجغرافي وعدم الإلتزام بالزمن.

كما أن هذا التطور في هذه التقنيات يساعد المجرم على سهولة إخفاء جريمته نظرًا لاستخدامه الرموز المشفرة والذي يصعب الوصول إليها بشكل سهل وهذا إن دل على شيء فإنه يتطلب من منفذ هذه الجرائم وأن يكون ذو كفاءة عالٍ من العلم والمعرفة باستخدام تقنيات الذكاء الاصطناعي وتكنولوجيا المعلومات[3].

ثانيًا- جرائم الابتزاز:

لقد دخل التطور التكنولوجي مختلف جوانب الحياة، وأصبح لا يمكن الاستغناء عنه، ولا يوجد بديلاً له، وإعتبر أساسًا من أساسيات الحياة اليومية القائمة ويستخدم في كافة المجلات، وأقبل على هذا التطور نسبة كبيرة من سكان العالم وبشكل متفاوت، فلا يختلف اثنان على أن التطور التكنولوجي وخاصة شبكة الإنترنت وأجهزة الكمبيوتر زادت اتساعًا وانتشارًا حول العالم في الآونة الأخيرة ناهيك عن التطور الحاصل على صعيد أجهزة الهواتف النقالة وما تتمتع به من ذكاء عال على كافة المستويات لما تحتويه من تطبيقات وتقنيات الذكاء الاصطناعي[1].

والابتزاز هو سلب المال من الناس أو نزعه منهم بخفاء وقهر وكسب المال أو الشيء بطريقة غير مشروعة[2].

أما تعريف الابتزاز عبر الوسائل المتطورة من الذكاء الاصطناعي فإن التشريعات لا تضع اهتمامًا بالنسبة للتعريفات بقدر ما تهتم بالنصوص والأحكام.

لذا يمكن وصف الابتزاز على أنه عملية تتضمن الحصول على معلومات سرية أو صور شخصية أو فيديوهات خاصة بالضحية أو المجني عليه، إذ تتم عملية الابتزاز بالتهديد حول نشر ما يتوفر لدى الجاني من معلومات وصور

---

[1] نائلة قورة، جرائم الحاسب الآلي، المرجع أعلاه، ص 56.

[2] هشام رستم، الجوانب الإجرائية لجرائم المعلوماتية، دار النهضة العربية، القاهرة، 1998.

[3] ذياب البداينة، الجرائم الإلكترونية، المفهوم والأسباب، بحث مقدم إلى الملتقى العلمي للجرائم المستحدثة في ظل التغيرات والتحولات الرقمية الإقليمية والدولية، عمان، 2014، ص 64.

[1] حسن ظاهر داوود، جرائم نظم المعلومات، أكاديمية نايف للعلوم الأمنية، الرياض، 2000، ص 65.

[2] أحمد مختار عمر، معجم اللغة العربية المعاصرة، دار العلم للكتب، الرياض، 2008، صص 200.

ومواضيع تتعلق بالمجني عليه إذ لم يدفع مبلغ مالي أو يطلب منه تنفيذ عمل غير مشروع وذلك بناءً على طلب الجاني[3].

وعلى الرغم من أن هناك تشريعات تنظم هذا الموضوع إلاّ أن هذه التعريفات تختلف بين الدول وفقًا للتشريع المعتمد، وبما أن ظاهرة الابتزاز الإلكتروني عبر الذكاء الاصطناعي حديثة نوعًا ما، لذا قد لا تكون تناولتها التشريعات بشكل مباشر وإنما ترك أمر ذلك إلى القضاء والمحاكم وذلك لعدم وجود تعريفات محددة لها[4].

تتميز جرائم الابتزاز عبر الإنترنت بصفة عامة بخصائص فريدة ومميزة تميزها عن الجرائم التقليدية[5]، كونها نمط جرمي جديد ظهر مع التطور التكنولوجي الهائل في الذكاء الاصطناعي، إذ ترتكب هذه الجرائم وتنفذ ضمن البيئة الرقمية مثل شبكات الإنترنت وأجهزة الكمبيوتر بتميز المجرم في هذه الجريمة بالهدوء وعدم العنف، حيث يعتمد على التلاعب النفسي واستغلال المجني عليه عاطفيا ونفسيًا لتحقيق أهدافه الشخصية، حيث يقوم بابتزاز الضحية من خلال الضغط عليها وإجبارهم على القيام بأفعال خارج إرادته وإمكانياته[1].

وبفضل التكنولوجيا والذكاء الاصطناعي ومن خلال التواصل الإجتماعي والشبكة العنكبوتية، أصبح المجرم المثير قادرًا على استهداف ضحاياه خارج مكان تواجده في الإقليم أو الدولة مما يجعل من الصعوبة بمكان تحديد هويته الحقيقية ومكان تواجده الفعلي.

كونه يقوم باستخدام أحدث التقنيات المتوافرة في الذكاء الاصطناعي ويتلاعب بأنظمة الأمان والبرمجيات الخبيثة من أجل الوصول إلى مبتغاه دون القدرة على معرفته[2].

وبما أن جريمة الابتزاز تتطلب استخدام وسائل وتقنيات حديثة، لذا يتعين على المجرم أن يمتلك أجهزة متطورة من كمبيوتر وهاتف محمول، بالإضافة إلى توافر شبكة الإنترنت واستخدام مواقع التواصل الإجتماعي للوصول إلى المجني عليه والحصول على المعلومات والصور أو المقاطع أو البيانات الشخصية التي يستخدمها المجرم في عملية الابتزاز ضد الضحية[3].

لذلك يحتاج الفاعل أو المتسبب في جريمة الابتزاز باستخدام الذكاء الاصطناعي أدوات وتقنيات إلكترونية متطورة للقيام بتنفيذ الجريمة بسهولة. بالإضافة إلى ذلك يجب على الجاني أن يكون يتمتع بالعلم والمعرفة بكيفية استخدام والتعامل مع هذه التقنيات الحديثة وفي مقدمتها شبكة الإنترنت والأجهزة الإلكترونية والتي من خلالها أو عبر طريقها يرتكب جرمه.

وهذا يشتمل على معرفة الوصول إلى المعلومات المتعلقة بالضحية وكيفية استغلالها والحصول على المعلومات بطرق غير قانونية وغير صحيحة لممارسة الابتزاز وإلحاق الضرر بالمجني عليه[4].

---

[3] عبد الرحمن عبدالله المسند، جريمة الابتزاز، مكتبة الملك فهد الوطنية، الرياض، 2018، ص 15.

[4] سامي المطيري، المسؤولية الجنائية عن الابتزاز الإلكتروني، رسالة ماجستير، جامعة نايف للعلوم، الرياض، 2015، ص 27.

[5] محمود عباينة، جرائم الحاسوب، وأبعادها الدولية، دار الثقافة، عمان، 2009، ص 4.

[1] مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، 2000، ص 11.

[2] محمد علي سالم، حسون عبيد، الجريمة المعلوماتية، جامعة بابل الإنسانية، مجلد 14، عدد 2، العراق، 2007، ص 92.

[3] بصرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة الجزائر، 2019، ص 37-38.

[4] مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، المرجع السابق، ص 30.

الفرع الثاني

جرائم انتهاك البيانات الشخصية

إنّ التطور الذي عرفته المجتمعات المدنية من توافر تقنيات الذكاء الاصطناعي والأجهزة الإلكترونية والمعلوماتية ووسائل التواصل الإجتماعي، ساهم بشكل أو بآخر في تبادل كميات هائلة من البيانات الشخصية عبر هذه التقنيات الذكية، ومع ذلك فإن انتشار هذه البيانات تثير قضية حماية الخصوصية والحفاظ على سرية المعلومات الشخصية[1].

تعتبر جرائم انتهاك البيانات الشخصية للأفراد من أكثر الجرائم شيوعًا في العصر الرقمي. تشمل هذه الجرائم سرقة واختراق البيانات الشخصية والتجسس على المعلومات الشخصية بتسريبها واستغلالها بشكل غير قانوني أو غير مشروع.

تتسبب جرائم انتهاك البيانات الشخصية في تعريض الأفراد لمخاطر جسيمة، فقد يتم استغلال البيانات المسروقة في الاحتيال المالي، وسرقة الهوية والتشهير والتلاعب بالمعلومات الشخصية لأغراض غير قانونية.

تزداد أهمية حماية البيانات الشخصية مع تزايد الاعتماد على التقنيات الرقمية في حياتنا اليومية، بما في ذلك التسوق عبر الإنترنت والخدمات المصرفية، لذا يجب أن يكون هناك توازن بين تبادل البيانات المصرفية، لذا يجب أن يكن هناك توازن بين تبادل البيانات الشخصية وحماية الخصوصية وضمان تبني إجراءات أمنية قوية للحفاظ على سرية وسلامة هذه البيانات[2].

أولاً- استخدام بيانات شخصية غير صحيحة:

إنّ انتهاك البيانات الشخصية للأفراد يعتبر جريمة خطرة تنطوي على تهديدات تكنولوجية متقدمة للحياة الخاصة، ويتم تنفيذ هذه الجرائم من خلال سوء استخدام تقنيات الذكاء الاصطناعي والمعلومات المتعلقة بالأفراد.

تصبح صور الاعتداء على الحياة الخاصة صعبة التحديد بسبب تطور التكنولوجيا المعلوماتية بشكل مستمر، ومع ذلك، يمكننا الإشارة إلى بعض أبرز أشكال انتهاك حقوق الأفراد في حياتهم الخاصة[1].

يقوم الجاني بهذه الجرائم في محاولة للتدخل في الحياة الخاصة للفرد، وذلك من خلال اختراق الأنظمة المعلوماتية والوصول إلى معلومات تتعلق به.

حيث يستخدم الجاني هذه المعلومات، سواء كانت صحيحة أو غير صحيحة، من خلال التلاعب بها أو استغلالها بطرق مختلفة.

قد يكون للجاني صلاحيات قانونية للوصول إلى هذه الأنظمة، أو قد يكون غير مصرح له بها. بالإضافة إلى ذلك، يمكن للجاني جمع البيانات الشخصية للضحية لاستخدامها لأغراض شخصية، أو الكشف عن هذه المعلومات وسوء استخدامها[2].

إنّ اختراق حسابات البريد الإلكتروني أو وسائل التواصل الإجتماعي الشخصية للأفراد. والتلاعب بالمعلومات الموجود فيها، وذلك لما يتوفر لدى الجاني من أدوات ووسائل متطورة في الذكاء الاصطناعي قادرة على اختراق هذه البيانات

---

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، عمان، 2008، ص 174.

[2] محمد محمود المكاوي، الجوانب الأخلاقية والإجتماعية لجرائم المعلوماتية، المكتبة العصرية، مصر، 2010، ص 342.

[1] محمود الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، 2009، ص 343.

[2] نهلا عبد القادر المومني، الجرائم المعلوماتية، المرجع السابق، صص 183.

والمعلومات بسهولة والتعرض لها، كما يمكن للجاني استخدام برامج خبيثة لسرقة المعلومات الشخصية، مثل بيانات البطاقات الائتمانية أو معلومات الحسابات المصرفية.

إذ تتشكل جرائم انتهاك البيانات الشخصية خطرًا كبيرًا على خصوصية الأفراد وسلامتهم الشخصية والمالية[3].

إن استخدام البيانات الشخصية غير صحيحة، يشكل انتهاكًا آخر للحياة الخاصة للأفراد ويمكن تصنيف هذه الانتهاكات إلى نوعين رئيسيين:

1- التلاعب في البيانات الشخصية أو محوها، يتم ذلك عادة عن طريق أشخاص غير مصرح لهم بالقيام بذلك، إذ يقوم الجناة بتعديل أو حذف البيانات الشخصية لأغراض مادية تخدم مصالحهم الشخصية، ويترتب على ذلك انتهاك للسرية والحرمة الخاصة للفرد.

2- استخدام بيانات شخصية غير حقيقية، يتم ذلك عادة من قبل الأشخاص المصرح لهم قانونًا ويسمح لهم بالدخول إلى البيانات والاطلاع عليها، ويكون الإهمال هو السبب الرئيسي وراء جمع أو معالجة أو نشر بيانات شخصية غير صحيحة.

يمكن أن يحدث ذلك عن طريق الخطأ أو عمدًا، مما يؤدي إلى إتلاف سمعة الشخص المتضرر وتعريضه لمخاطر قانونية وإجتماعية. إن هذه الأفعال الجرمية التي يقوم بها الجاني باستخدام تقنيات الذكاء الاصطناعي تعرض خصوصية الأفراد للخطر وتؤثر على حياتهم الشخصية والمهنية[1].

ثانيًا- جمع وتخزين البيانات:

إنّ جمع وتخزين البيانات الشخصية صحيحة على نحو غير مشروع يعد فعلاً جنائيًا ويشكل انتهاكًا آخر لحق الأفراد في الحياة الخاصة، ويتم ذلك عن طريق استخدام أساليب غير مشروعة للحصول على هذه البيانات أو من خلال طبيعة مضمون البيانات نفسها[2]، ومن بين الأساليب غير المشروعة لجمع وتخزين البيانات الشخصية يمكن ذكر ما يلي:

1- مراقبة وإعتراض والتقاط الرسائل المتبادلة عبر البريد الإلكتروني، حيث يتم تجاوز سرية وحدود المراسلات الشخصية والتلاعب بالبيانات المرسلة والمستلمة عبر البريد الإلكتروني.

2- توصيل أسلاك الأجهزة والتقنيات المتطورة بطريقة خفية إلى الحاسوب الذي يحتوي على البيانات والمعلومات المطلوبة والمراد حيازتها أو التعرض لها أو نسخها وما إلى ذلك لذا يتم استخدام طرق غير قانونية للوصول إلى الأجهزة الإلكترونية من حواسيب وغيرها من التقنيات والاستيلاء على البيانات والمعلومات المخزنة بداخل هذه الأجهزة.

3- الحصول غير المشروع على ملفات بيانات تخص الآخرين، وذلك بتوافر هذه المعلومات والمعطيات داخل الأجهزة التي يتم الدخول إليها بطريقة غير مشروعة، ويتم الوصول إلى ملفات البيانات الشخصية للأشخاص الآخرين بطرق غير مصرح لهم بها وغير قانونية[3].

---

[3] حسين عبد السميع إبراهيم، الجرائم المستحدثة عن طريق الإنترنت، دار النهضة العربية، القاهرة، 2011، ص 562.

[1] محمود الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، 356.

[2] نهلا عبد القادر المومني، جرائم المعلوماتية، المرجع السابق، ص 176.

[3] حسين عبد السميع إبراهيم، الجرائم المستحدثة عن طريق الإنترنت، المرجع السابق، ص 563.

4- عدم مشروعية مضمون البيانات والمعلومات المجتمعة والمخزنة، إذ يمكن أن يتم تخزين وجمع بيانات ومعلومات ذات طبيعة شخصية متعددة ومتنوعة بطرق غير قانونية، مما يعني أن المحتوى نفسه للبيانات والمعلومات غير مشروع، لذا يعتبر هذه الأفعال انتهاكًا للخصوصية والحقوق الشخصية للأفراد، لذا يجب تشديد القوانين وتنفيذ إجراءات صارمة وحازمة لمكافحة هذه الأنشطة غير المشروعة، بالإضافة إلى تعزيز الوعي ونشر الثقافة حول حقوق الأفراد في الحماية من جمع واستخدام غير قانوني لبياناتهم الشخصية[1].

ثالثًا- الإفشاء غير المشروع للبيانات وإساءة استعمالها:

إنّ الإفشاء غير المشروع للبيانات الشخصية، وسوء استخدامها يشكلان انتهاكًا لحقوق الأفراد والحياة الخاصة، في هذه الحالة يتم جمع وتخزين ومعالجة البيانات والمعلومات الشخصية الخاصة بطريقة قانونية ومشروعة، ولكن يتم إفشاؤها ونشرها أو إعلام الآخرين بطرق غير قانونية وغير صحيحة أو يتم إساءة استخدامها من قبل الأشخاص الذين يحتفظون بها مما يؤدي إلى إلحاق الضرر بصاحب العلاقة[2].

قد يتم الإفشاء غير المشروع للبيانات الشخصية عن طريق بيعها لأطراف ثالثة بدون موافقة الأفراد المعنيين وأصحاب العلاقة، أو من خلال تسريبها أو نشرها عن طريق الخطأ أو عمدًا.

هذا الإجراء أو الفعل يعرض الأفراد لخطر فقدان السرية لمعلوماتهم وبياناتهم الشخصية مما يؤدي إلى تعرضهم للاستغلال أو التهديد والابتزاز من قبل آخرين.

بالإضافة إلى ذلك، قد يتم سوء استخدام البيانات الشخصية من قبل الأشخاص الذين يتولون حفظها أو القيمين عليها وذلك باستخدامها قي مجالات أو أغراض غير قانونية أو غير مشروعة أو غير صحيحة، أو استغلالها بهدف الحصول على مكاسب شخصية أو مادية على حساب الأفراد المتضررين[3].

هذا النوع من الانتهاكات يعد خطيرًا، ويشكل تهديدًا للخصوصية والأمان الشخصي، لذا يب وضع تشريعات صارمة لحماية البيانات الشخصية وفرض عقوبات رادعة على أولئك الذين ينتهكون حقوق الأفراد في الاقتناء غير المشرو للبيانات وسوء استخدامها، كما يجب تعزيز الوعي والإدراك والتثقيف حول حقوق الأفراد وكيفية حماية بياناتهم الشخصية من هذه الانتهاكات[1].

في العديد من الأنظمة القانونية يتطلب جمع وتخزين ومعالجة البيانات الشخصية الإمتثال للقواعد والتشريعات الخاصة. ويطلب في بعض الحالات الحصول على ترخيص مسبق من الجهة المختصة قبل مزاولة أي نشاط جمع ومعالجة البيانات الشخصية. تتفاوت متطلبات الترخيص والإلتزام الشكلي من دولة إلى أخرى وقد تختلف تبعًا للمجال الصناعي والأغراض المحددة لجمع البيانات الشخصية[2].

تهدف هذه القواعد الشكلية إلى ضمان حماية البيانات الشخصية وخصوصيتها وضمان استخدامها بطرق قانونية ومشروعة. لذا عندما يتعذر الإلتزام بالقواعد الشكلية، قد يكون ذلك مخالفة للقانون ويمكن أن يتعرض المسؤولون عن جمع ومعالجة البيانات الشخصية للعقوبات القانونية المنصوص عليها.

---

[1] محمد العبادي، الجرائم المستحدثة، في ظل العولمة، دار جليس الزمان، عمان، 2015، ص 336.

[2] محمد أبو بكر سلامة، جرائم الكمبيوتر والإنترنت، منشأة المعارف، القاهرة، 2006، ص 193.

[3] سامر الجبوري، جريمة الاحتيال الإلكتروني، رسالة ماجستير، كلية القانون، جامعة النهرين، بغداد، 2014، ص 53.

[1] محمد محمود مكاوي، الجوانب الأخلاقية والإجتماعية لجرائم المعلوماتية، المرجع السابق، ص 365.

[2] سامر الجبوري، جريمة الاحتيال الإلكتروني، المرجع أعلاه، ص 67.

لذا يجب على الجهات الراغبة في جمع وتخزين ومعالجة البيانات الشخصية التأكد من الإمتثال للقواعد الشكلية المطبقة في الدول التي يتعاملون بها والحصول على التراخيص اللازمة قبل بدء النشاط[3].

بالإضافة إلى ذلك، ينبغي تعزيز الوعي بين الأفراد بشأن حقوقهم فيما يتعلق بالبيانات الشخصية وكيفية حمايتها.

وفي هذا السياق، يتطلب مكافحة جرائم انتهاك البيانات الشخصية تشريعات صارمة وحازمة وآليات فعالة للكشف عن هذه الجرائم ومعاقبة الفاعلين، إلى جانب ذلك، تلعب التوعية والمعرفة دورًا هامًا في تمكين الأفراد داخل المجتمع لاتخاذ التدابير اللازمة لحماية بياناتهم الشخصية، وتجنب الانتهاكات.

الخاتمة

أظهر هذا البحث أن الذكاء الاصطناعي، رغم كونه أداة فعالة في تطوير المجتمعات وتعزيز كفاءة المؤسسات، يمكن أن يتحول إلى وسيلة خطيرة لارتكاب الجرائم الدولية إذا ما أسيء استخدامه. فقد أسهمت هذه التقنيات في تطوير أساليب إجرامية معقدة يصعب كشفها أو مكافحتها بالوسائل القانونية التقليدية، الأمر الذي انعكس سلبًا على أمن الدول واستقرارها، وعلى حقوق الأفراد وحرياتهم.

كما بيّن البحث أن الجرائم المرتكبة باستخدام الذكاء الاصطناعي تتسم بالطابع العابر للحدود، مما يزيد من تعقيد مسألة الملاحقة الجنائية ويستدعي تعزيز التعاون الدولي وتوحيد الجهود التشريعية لمواجهتها. ومن هنا، فإن التصدي لهذه الجرائم يتطلب رؤية قانونية شاملة توازن بين الاستفادة من التطور التكنولوجي وحماية القيم القانونية والإنسانية الأساسية.

أولاً–النتائج

1. يشكّل الذكاء الاصطناعي أداة فعالة في تطوير أساليب الجرائم الدولية وزيادة خطورتها.
2. ساهم استخدام الذكاء الاصطناعي في تعقيد الجرائم السيبرانية وجرائم التجسس والاحتيال والسرقة.
3. تعاني التشريعات التقليدية من قصور واضح في مواجهة الجرائم المرتبطة بالذكاء الاصطناعي.
4. تمثل الجرائم المرتكبة باستخدام الذكاء الاصطناعي تهديدًا مباشرًا لأمن الدول وخصوصية الأفراد.
5. إن الطابع العابر للحدود لهذه الجرائم يعيق الملاحقة القضائية ويضعف فعالية الردع.

ثانياً– التوصيات

1. ضرورة تحديث التشريعات الوطنية بما يتلاءم مع الجرائم المستحدثة المرتبطة بالذكاء الاصطناعي.
2. تعزيز التعاون الدولي في مجال مكافحة الجرائم السيبرانية وتبادل المعلومات والخبرات.
3. إنشاء أطر قانونية واضحة تنظم استخدام الذكاء الاصطناعي وتحدّ من إساءة استعماله.
4. دعم برامج التوعية والتدريب في مجال الأمن السيبراني وحماية البيانات الشخصية.
5. اعتماد آليات رقابية وتقنية متقدمة للكشف المبكر عن الجرائم المرتكبة باستخدام الذكاء الاصطناعي.

[3] محمد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، المرجع السابق، ص 346.

لائحة المراجع

أولاً: الكتب

1. أحمد تمام، **الجرائم الناشئة عن استخدام الحاسب الآلي**، دار النهضة العربية، القاهرة، 2000.

Ahmed Tammam, *Crimes Arising from the Use of Computers*, Dar Al-Nahda Al-Arabiya, Cairo, 2000.

2. أحمد خليفة الملط، **الجرائم المعلوماتية**، دار الفكر الجامعي، الإسكندرية، 2006.

Ahmed Khalifa Al-Malt, *Information Crimes*, Dar Al-Fikr Al-Jami'i, Alexandria, 2006.

3. أحمد مختار عمر، **معجم اللغة العربية المعاصرة**، دار العلم للكتب، الرياض، 2008.

Ahmed Mukhtar Omar, *Dictionary of Contemporary Arabic Language*, Dar Al-Ilm lil-Kutub, Riyadh, 2008.

4. أيمن عبد الحفيظ، **الاتجاهات النفسية والأمنية لمواجهة الجرائم المعلوماتية**، دار النهضة، القاهرة، 2005.

Ayman Abdel Hafiz, *Psychological and Security Approaches to Confronting Information Crimes*, Dar Al-Nahda, Cairo, 2005.

5. أيمن فكري، **جرائم نظم المعلوماتية: دراسة مقارنة**، دار الجامعة الجديدة، الإسكندرية، 2007.

yman Fikri, *Information Systems Crimes: A Comparative Study*, Dar Al-Jami'a Al-Jadida, Alexandria, 2007.

6. حسن ظاهر داوود، **جرائم نظم المعلومات**، أكاديمية نايف للعلوم الأمنية، الرياض، 2000.

Hassan Daher Dawood, *Information Systems Crimes*, Naif Academy for Security Sciences, Riyadh, 2000.

7. حسين عبد السميع إبراهيم، **الجرائم المستحدثة عن طريق الإنترنت**، دار النهضة العربية، القاهرة، 2011.

Hussein Abdel Samee Ibrahim, *Emerging Crimes via the Internet*, Dar Al-Nahda Al-Arabiya, Cairo, 2011.

8. خالد ممدوح إبراهيم، **الجرائم المعلوماتية**، دار الفكر الجامعي، الإسكندرية، 2009.

Khaled Mamdouh Ibrahim, *Information Crimes*, Dar Al-Fikr Al-Jami'i, Alexandria, 2009.

9. طارق الشدي، **آلية البناء الأمني لنظم المعلومات**، دار الوطن للطباعة، الرياض، 2003.

Tariq Al-Shaddi, *The Mechanism of Security Structuring for Information Systems*, Dar Al-Watan for Printing, Riyadh, 2003.

10. طارق عطية، **الأمن المعلوماتي والنظام القانوني للحماية والمعلوماتية**، دار الجامعة الجديدة، الإسكندرية، 2003.

Tariq Atiya, *Information Security and the Legal System for Protection and Informatics*, Dar Al-Jami'a Al-Jadida, Alexandria, 2003.

11.عبد الرحمن عبد الله المسند، **جريمة الابتزاز**، مكتبة الملك فهد الوطنية، الرياض، 2018.

Abdulrahman Abdullah Al-Musnad, *The Crime of Blackmail*, King Fahd National Library, Riyadh, 2018.

12.عبد الله عبد الله، **جرائم المعلوماتية والإنترنت: الجرائم الإلكترونية**، منشورات الحلبي، بيروت، 2011.

Abdullah Abdullah, *Information and Internet Crimes: Cybercrimes*, Al-Halabi Publications, Beirut, 2011.

13.علي عدنان الفيل، **الإجرام الإلكتروني: أساسه وتطوره**، دار النهضة العربية، بيروت، 1991.

Ali Adnan Al-Feel, *Cybercrime: Its Basis and Development*, Dar Al-Nahda Al-Arabiya, Beirut, 1991.

14.عمار عباس الحسيني، **التحقيق الجنائي والوسائل الحديثة في كشف الجريمة**، منشورات الحلبي، بيروت، 2015.

Ammar Abbas Al-Husseini, *Criminal Investigation and Modern Methods of Crime Detection*, Al-Halabi Publications, Beirut, 2015.

15.غادة المنجم، **الذكاء الاصطناعي**، جامعة الملك سعود، الرياض، 2009.

Ghada Al-Munajjim, *Artificial Intelligence*, King Saud University, Riyadh, 2009.

16.محمد أبو بكر سلامة، **جرائم الكمبيوتر والإنترنت**، منشأة المعارف، القاهرة، 2006.

Mohamed Abu Bakr Salama, *Computer and Internet Crimes*, Mansha'at Al-Maaref, Cairo, 2006.

17.محمد الشوابكة، **جرائم الحاسوب والإنترنت: الجريمة المعلوماتية**، دار النهضة العربية، عمان، 2011.

Mohamed Al-Shawabkeh, *Computer and Internet Crimes: Information Crime*, Dar Al-Nahda Al-Arabiya, Amman, 2011.

18.محمد العبادي، **الجرائم المستحدثة في ظل العولمة**، دار جليس الزمان، عمان، 2015.

Mohamed Al-Abadi, *Emerging Crimes in the Era of Globalization*, Dar Jalees Al-Zaman, Amman, 2015.

19.محمد الكعبي، **الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت**، دار النهضة العربية، القاهرة، 2005.

Mohamed Al-Kaabi, *Crimes Arising from the Unlawful Use of the Internet*, Dar Al-Nahda Al-Arabiya, Cairo, 2005.

20.محمد غانم يونس، **الابتزاز الإلكتروني: دراسة من وجهة نظر قانونية ضمن مؤلف الابتزاز الإلكتروني، جريمة العصر الحديث**، إصدار وزارة الداخلية العراقية، دار الكتب والوثائق، العراق، 2019.

Mohamed Ghanem Younis, *Cyber Blackmail: A Legal Perspective Study within the Book Cyber Blackmail, the Crime of the Modern Age*, issued by the Iraqi Ministry of Interior, Dar Al-Kutub wal-Watha'iq, Iraq, 2019.

21.محمد محرم علي، **جريمة النصب والاحتيال والتجارة الإلكترونية**، دار النهضة، القاهرة، 1998.

Mohamed Muharram Ali, *The Crime of Fraud, Deception, and E-Commerce*, Dar Al-Nahda, Cairo, 1998.

22.محمد محمود المكاوي، **الجوانب الأخلاقية والاجتماعية لجرائم المعلوماتية**، المكتبة العصرية، مصر، 2010.

Mohamed Mahmoud Al-Makawi, *The Ethical and Social Aspects of Information Crimes*, Al-Maktaba Al-Asriya, Egypt, 2010.

23.محمود أحمد عباينة، **جرائم الحاسوب وأبعادها الدولية**، دار الثقافة، عمان، 2009.

Mahmoud Ahmed Abayneh, *Computer Crimes and Their International Dimensions*, Dar Al-Thaqafa, Amman, 2009.

24.محمود الكعبي، **الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت**، دار النهضة العربية، القاهرة، 2009.

Mahmoud Al-Kaabi, *Crimes Arising from the Unlawful Use of the Internet*, Dar Al-Nahda Al-Arabiya, Cairo, 2009.

25.محمود ثائر، **مقدمة في الذكاء الاصطناعي**، مكتبة المجتمع العربي للنشر والتوزيع، عمان، الأردن، 2009.

Mahmoud Thaer, *Introduction to Artificial Intelligence*, Arab Society Library for Publishing and Distribution, Amman, Jordan, 2009.

26.محمود عباينة، **جرائم الحاسوب وأبعادها الدولية**، دار الثقافة، عمان، 2009.

Mahmoud Abayneh, *Computer Crimes and Their International Dimensions*, Dar Al-Thaqafa, Amman, 2009.

27.مدحت رمضان، **جرائم الاعتداء على الأشخاص والإنترنت**، دار النهضة العربية، القاهرة، 2000.

Medhat Ramadan, *Crimes of Assault against Persons and the Internet*, Dar Al-Nahda Al-Arabiya, Cairo, 2000.

28.منير الجنبهي، **جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها**، دار الفكر الجامعي، الإسكندرية، 2005.

Mounir Al-Janbihi, *Internet and Computer Crimes and Methods of Combating Them*, Dar Al-Fikr Al-Jami'i, Alexandria, 2005.

29.ناصر بن محمد النعيمي، **جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية**، دون دار نشر، السعودية، 2009.

Nasser bin Mohammed Al-Nuaimi, *Information Crimes and Their Combat in the Kingdom of Saudi Arabia*, no publisher, Saudi Arabia, 2009.

30.نائلة قورة، **جرائم الحاسب الآلي الاقتصادية: دراسة نظرية تطبيقية**، منشورات الحلبي، القاهرة، 2005.

Naila Qura, *Economic Computer Crimes: A Theoretical and Applied Study*, Al-Halabi Publications, Cairo, 2005.

31.نهلا عبد القادر المومني، **الجرائم المعلوماتية**، دار الثقافة، عمان، 2008.

Nahla Abdel Qader Al-Momani, *Information Crimes*, Dar Al-Thaqafa, Amman, 2008.

32.هدى حامد قشقوش، **جرائم الحاسب الإلكتروني في التشريع المقارن**، دار النهضة العربية، القاهرة، 1992.

Huda Hamed Qashqoush, *Computer Crimes in Comparative Legislation*, Dar Al-Nahda Al-Arabiya, Cairo, 1992.

33.هشام رستم، **الجوانب الإجرائية لجرائم المعلوماتية**، دار النهضة العربية، القاهرة، 1998.

Hisham Rustum, *Procedural Aspects of Information Crimes*, Dar Al-Nahda Al-Arabiya, Cairo, 1998.

34.هشام رستم، **جرائم الحاسب المستحدثة**، دار الكتب القانونية، القاهرة، 1999.

Hisham Rustum, *Emerging Computer Crimes*, Dar Al-Kutub Al-Qanuniya, Cairo, 1999.

35.هشام رستم، **قانون العقوبات ومخاطر تقنية المعلومات**، مكتبة الآلات الحديثة، القاهرة، 1994.

Hisham Rustum, *Criminal Law and the Risks of Information Technology*, Modern Machines Library, Cairo, 1994.

ثانياً: الأبحاث والمجلات العلمية

1. أشرف الراعي، **التحري والاستدلال عن الجرائم عبر أنظمة الذكاء الاصطناعي**، مجلة جامعة الزيتونة الأردنية للدراسات القانونية، المجلد 4، الأردن، 2023.

Ashraf Al-Ra'i, "Investigation and Inference of Crimes through Artificial Intelligence Systems," *Al-Zaytoonah University of Jordan Journal for Legal Studies*, Vol. 4, Jordan, 2023.

2. الأمير عبد القادر حفوظة، حسام غرادين، **الجريمة الإلكترونية وآليات التصدي لها**، مداخلة قدمت ضمن أعمال الملتقى الوطني: آليات مكافحة الجرائم الإلكترونية، مركز جبل البحث العلمي، جامعة الجزائر، 2017.

Al-Amir Abdel Qader Hafouza and Hossam Ghradin, "Cybercrime and Mechanisms for Confronting It," paper presented at the National Forum: Mechanisms for Combating Cybercrimes, Jabal Scientific Research Center, University of Algiers, 2017.

3. مصطفى سمارة، **الجريمة الإلكترونية**، مجلة المعلوماتية، العدد 29، الأردن، تموز/يوليو 2008.

Mustafa Samara, "Cybercrime," *Informatics Journal*, Issue 29, Jordan, July 2008.

4. كامل السعيد، **جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات**، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، المنعقد في القاهرة، 25-1993/28، دار النهضة العربية، القاهرة، 1993.

Kamel Al-Saeed, "Computer Crimes and Other Crimes in the Field of Information Technology," paper presented to the Sixth Conference of the Egyptian Association of Criminal Law, held in Cairo, 25–28/1993, Dar Al-Nahda Al-Arabiya, Cairo, 1993.

5. عبد الرحمن بن راشد، **جرائم الحاسب الآلي: الخطر الحقيقي في عصر المعلومات**، المجلة العربية للدراسات الأمنية والتدريب، المجلد 15، الرياض، 2015.

Abdulrahman bin Rashid, "Computer Crimes: The Real Threat in the Information Age," ***Arab Journal for Security Studies and Training*****, Vol. 15, Riyadh, 2015.**

6. عراب مريم، **جريمة التهديد والابتزاز الإلكتروني**، مجلة الدراسات القانونية المقارنة، كلية الحقوق، جامعة الجزائر، 2021.

Arab Mariam, "The Crime of Threat and Cyber Blackmail," ***Journal of Comparative Legal Studies*****, Faculty of Law, University of Algiers, 2021.**

7. ذياب البداينة، **الجرائم الإلكترونية: المفهوم والأسباب**، بحث مقدم إلى الملتقى العلمي للجرائم المستحدثة في ظل التغيرات والتحولات الرقمية الإقليمية والدولية، عمان، 2014.

Dhiab Al-Badayneh, "Cybercrimes: Concept and Causes," paper presented at the Scientific Forum on Emerging Crimes in Light of Regional and International Digital Changes and Transformations, Amman, 2014.

8. محمد علي سالم، حسون عبيد، **الجريمة المعلوماتية**، مجلة جامعة بابل للعلوم الإنسانية، المجلد 14، العدد 2، العراق، 2007.

Mohamed Ali Salem and Hassoun Obaid, "Information Crime," ***University of Babylon Journal for Humanities*****, Vol. 14, Issue 2, Iraq, 2007.**

ثالثاً: رسائل الماجستير

1. سامر الجبوري، **جريمة الاحتيال الإلكتروني**، رسالة ماجستير، كلية القانون، جامعة النهرين، بغداد، 2014.

Samer Al-Jubouri, ***The Crime of Electronic Fraud*****, Master's Thesis, College of Law, Al-Nahrain University, Baghdad, 2014.**

2. سامي المطيري، **المسؤولية الجنائية عن الابتزاز الإلكتروني**، رسالة ماجستير، جامعة نايف للعلوم الأمنية، الرياض، 2015.

Sami Al-Mutairi, ***Criminal Liability for Cyber Blackmail*****, Master's Thesis, Naif Arab University for Security Sciences, Riyadh, 2015.**

3. بصرة سعيدة، **الجريمة الإلكترونية في التشريع الجزائري: دراسة مقارنة**، رسالة ماجستير، كلية الحقوق، جامعة الجزائر، 2019.

Basra Saida, ***Cybercrime in Algerian Legislation: A Comparative Study*****, Master's Thesis, Faculty of Law, University of Algiers, 2019.**