تأثير الذكاء الاصطناعى على أنماط ارتكاب الجرائم الإلكترونية
"دراسة ميدانية على عينة من الضحايا"

إعـــداد
محمد سمير أبو الفتوح عبد الجواد
مدرس علم الاجتماع-كلية الآداب-جامعة بنها
mohamed.aboelfetoh@fart.bu.edu.eg

ملخص

يهدف البحث إلى التعرف على دور الذكاء الاصطناعى فى ارتكاب الجرائم الإلكترونية ، بالإضافة إلى دراسة الأسباب المؤدية إلى ارتكاب هذه الجرائم المدعومة بتقنيات الذكاء الاصطناعى من وجهة نظر الضحايا ، كما يسعى إلى رصد المخاطر والتحديات المختلفة التى يواجهها الضحايا نتيجة تعرضهم لهذه الجرائم ، وتحليل موقفهم وأساليب تعاملهم معها ، علاوة على ذلك يهدف البحث إلى استعراض المقترحات التى قد تساهم فى حماية الأفراد من الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، وذلك من منظور الضحايا أنفسهم .

واعتمد البحث على طريقة دراسة الحالة ، حيث تم تطبيقه على عينة عمدية تم اختيارها باستخدام طريقة كرة الثلج ، وشملت العينة (٢٠) حالة من ضحايا الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى فى محافظة القليوبية.

وتوصل البحث إلى أن جميع حالات الدراسة الميدانية تعرضت لمختلف أشكال الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، والتى شملت جرائم الابتزاز والتشهير، سرقة الحسابات البنكية ، الابتزاز الجنسى ، تشويه السمعة، والقرصنة الإلكترونية (الهاكرز) ، كما تبين أن آليات تنفيذ هذه الجرائم تنوعت وتعددت ، حيث استغل المجرمون بناء علاقات عاطفية مع الضحايا لكسب ثقتهم ، ثم استغلالهم مالياً أو للحصول على معلومات حساسة ،أما عن أسباب الجرائم الإلكترونية المدعومة بالذكاء الاصطناعى الأسباب الاجتماعية: شملت التفكك الأسرى، ضعف الرقابة العائلية ، غياب الرقابة المجتمعية ، الأسباب الاقتصادية: تمثلت فى الضغوط المالية ، الرغبة فى تحقيق الثراء السريع ، والبطالة ، الأسباب الثقافية: ارتبطت بالتطور التكنولوجى المتسارع، التأثيرات الثقافية السلبية ، وانتشار ثقافة الإفلات من العقاب ، الأسباب الذاتية: شملت رغبة الجانى فى إثبات ذاته ، تحقيق مكانة اجتماعية ،

السعى للانتقام أو التسلية ، وإلحاق الأذى بالضحايا ، وعن المخاطر والتحديات التى تواجه الضحايا فقد تعددت وشملت العديد من الآثار منها الآثار الاجتماعية : تتجلى فى العزلة الاجتماعية ، تدمير السمعة الشخصية والمهنية، وتهديد العلاقات الأسرية ، الآثار الاقتصادية: تشمل الخسائر المالية المباشرة ، فقدان الوظائف وفرص العمل ، وارتفاع التكاليف القانونية الناجمة عن محاولات استعادة الحقوق ، الآثار النفسية : تتمثل فى القلق والتوتر المستمر والتأثيرات النفسية العميقة التى قد تصل إلى الاضطرابات العاطفية ، وبالنسبة لموقف الضحايا عند التعرض للجرائم الإلكترونية ، فعند تعرض الضحايا لهذه الجرائم ، مرّوا بعدة مراحل ، بدأت بالصدمة والارتباك ، ثم البحث عن الدعم والمساعدة ، وأخيراً اتخاذ الإجراءات الأمنية والقانونية لمواجهة تداعيات الجريمة

الكلمات المفتاحية: الذكاء الاصطناعى ، الجرائم الإلكترونية ، الضحايا.

The Impact of Artificial Intelligence on Patterns of Cybercrime "A Field Study on a Sample of Victims"

Abstract:

The research aims to identify the role of artificial intelligence in committing cybercrimes, as well as to study the reasons leading to the commission of these AI-supported crimes from the victims' perspective. It also seeks to identify the various risks and challenges faced by victims as a result of their exposure to such crimes, analyze their stance and methods of dealing with them. Furthermore, the research aims to present proposals that may contribute to protecting individuals from AI-supported cybercrimes, from the perspective of the victims themselves.

The research adopted the case study method, applied to a purposive sample selected using the snowball sampling technique. The sample included (20) cases of victims of AI-supported cybercrimes in Qalyubia Governorate.

The research found that all cases in the field study were exposed to various forms of AI-supported cybercrimes, including blackmail, defamation, bank account theft, sexual extortion, reputation damage, and electronic hacking

(hackers). It was also revealed that the mechanisms of these crimes varied, as criminals exploited emotional relationships with victims to gain their trust, subsequently using them financially or extracting sensitive information.

Regarding the causes of AI-supported cybercrimes:

- **Social causes**: Included family disintegration, weak parental supervision, and lack of societal control.
- **Economic causes**: Consisted of financial pressures, the desire for quick wealth, and unemployment.
- **Cultural causes**: Were linked to rapid technological advancements, negative cultural influences, and the spread of an impunity culture.
- **Personal causes**: Included the offender's desire to prove themselves, gain social status, seek revenge or entertainment, and harm victims.

As for the risks and challenges victims face, they included multiple impacts:

- **Social impacts**: Social isolation, destruction of personal and professional reputation, and threats to family relationships.
- **Economic impacts**: Direct financial losses, loss of jobs and career opportunities, and high legal costs resulting from attempts to restore rights.
- **Psychological impacts**: Continuous anxiety and stress, along with deep psychological effects that may lead to emotional disorders.

Regarding the victims' responses to cybercrimes, they went through several stages: shock and confusion, seeking support and assistance, and finally, taking security and legal measures to confront the consequences of the crime.

Keywords: **Artificial Intelligence**, **Cybercrimes**, **Victims**.

المقدمة:

يُعَدّ الذكاء الاصطناعى من المجالات المهمة التى تستقطب اهتمام الباحثين ، ومع التقدم السريع فى تكنولوجيا الحاسبات فى الوقت الراهن ، وبفضل قدرة الحواسيب على تحصيل المعلومات وتخزينها واستخدامها ، تنشأ علاقة ارتباط وثيقة بين استخدامات الحاسب الآلى وارتكاب بعض الجرائم المستحدثة ، إذ يُوظَّف الحاسب الآلى كأداة لارتكاب أفعال غير مشروعة ، سواء كان هو محل الجريمة الإلكترونية أو وسيلتها ، ويُعدّ انتشار الوسائل المعلوماتية نتيجة لثورة المعلومات ، التى تتوسع بسرعة هائلة وتغزو مختلف مجالات الحياة ، أحد العوامل التى تسهم فى تفاقهم هذا النوع من الجرائم المستحدثة ، فعندما تُنتهك خصوصية الأفراد والمؤسسات والدول من خلال تدمير مواقعهم الإلكترونية أو اختراقها ، أو عبر قرصنة البيانات والمعلومات الخاصة بالمواقع الحكومية ، فإن ذلك يؤدى إلى ظهور تحديات قانونية جديدة تستلزم آليات تنظيمية حديثة ، وبذلك فإننا أمام مجموعة من الجرائم الإلكترونية المستحدثة التى تتميز بتقنيات متطورة مستندة إلى تطور الحاسب الآلى.(عبد الرازق،٢٠٢١،ص٤٣٠)

ومع التقدم التكنولوجى المتسارع ، تتغير الطريقة التى يتفاعل بها الأفراد مع العالم الرقمى ، ولم تكن الجريمة استثناءً من هذا التطور ، حيث يسعى المجرمون باستمرار إلى تطوير أساليبهم واستغلال الابتكارات التقنية لتعزيز أنشطتهم غير القانونية ، ويُعَد الذكاء الاصطناعى أحد أبرز الابتكارات الحديثة التى باتت تلعب دوراً محورياً فى هذا التحول ، إذ يمكنه تنفيذ مهام تتطلب عادة ذكاءً بشرياً ، مثل تحليل البيانات ، واكتشاف الأنماط ، واتخاذ قرارات مبنية على كميات هائلة من المعلومات ، ومع ذلك ، فإن هذه القدرات المتقدمة لم تقتصر على الاستخدامات المشروعة ، بل أصبحت أداة قوية فى يد المجرمين الإلكترونيين ، حيث يتم استغلال الذكاء الاصطناعى فى تنفيذ جرائم إلكترونية أكثر تعقيداً وخداعاً ، مثل إنشاء صور ومقاطع فيديو مزيفة باستخدام تقنية التزييف العميق لانتحال الشخصيات والابتزاز ، أو تحسين كفاءة الهجمات السيبرانية عبر تحليل نقاط الضعف فى الأنظمة المستهدفة ، وإن توظيف الذكاء الاصطناعى فى الجرائم الإلكترونية يعكس تحدياً متزايداً للجهات الأمنية والمتخصصين فى الأمن السيبرانى ، مما يتطلب تطوير أدوات دفاعية تعتمد على الذكاء الاصطناعى نفسه لرصد هذه التهديدات ومكافحتها بفعالية. (Parti,Dearden,2023,p.1)

كما ادى انتشار التكنولوجيا الحديثة الى فرض واقعاً جديداً أو فضاء رقمياً يسمى بالفضاء السيبرانى أو الافتراضى ، أثر هذا الفضاء على حياة الأشخاص والمؤسسات ، فترتبت عنه آثاراً إيجابية عدة ، لكن وبالمقابل أنتج العديد من الظواهر السلبية ، لعل أهمها انتشار الجرائم الالكترونية ،أو كما تسمى أيضاً جرائم الانترنت ،أو جرائم الكمبيوتر ،أو جرائم المعلوماتية والتى تطورت بالتزامن مع التطورات

التى تطرأ على التقنيات والتكنولوجيا والتى لا يقتصر استخدامها على الإنسان الخير بل كذلك الإنسان الشرير الذى قد يوصف كمجرم لسعيه وراء أطماعه واقتناصه الفرص لتحقيق أغراضه غير المشروعة ، ولا يتوانى عن استغلال التقنية لتطوير قدراته الإجرامية بإستخدام شبكة المعلوماتية كوسيلة سهلة لتنفيذ العمليات الإجرامية ، مما يلحق ضرراً بالآخرين.(طاله ،٢٠٢٠، ص ٦٤)

وأن التطور الهائل فى مجال استخدام الذكاء الاصطناعى وشبكة المعلومات الدولية على الرغم من إيجابياته المتعددة إلا أنه ينطوى فى داخله على مخاطر تفوق كافة التصورات فى تهديده للأمن فى المستقبل ويكفى أن نعرف أنه بلمسة واحدة يمكن لشخص أو مجموعة أشخاص أن يكبدوا بعض المؤسسات أو الشركات الكبرى خسائر مالية كبيرة ،أو يهددوا أمن واستقرار المجتمع ، كما أن عمليات التعارف على شبكة المعلومات الدولية أدت– كما طالعتنا وسائل الإعلام– إلى حدوث جرائم الانتحار الجماعى التى نفذها بعض المراهقين فى أمريكا ، هذا بالإضافة إلى جرائم خطف الأشخاص والطلاق والسرقة والاغتصاب والتهديد والقذف وتشويه السمعة وغيرها من الجرائم التى وقعت فى مختلف بلاد العالم ومن بينها مصر .(عوض،٢٠١٨،ص٢٢٧)

ويُعَد الذكاء الاصطناعى من منظور أمنى سلاحاً ذو حدين ، حيث تسعى الأجهزة الأمنية إلى توظيفه لتعزيز قدراتها فى مكافحة الجرائم الإلكترونية ورفع كفاءتها فى مجالات الأمن والسلامة ، بينما تستغل العصابات الإجرامية ذات التقنيات ذاتها لتطوير أساليب إجرامية أكثر تعقيداً ، مما يؤدى إلى نشوء نوع جديد من " الجريمة المعقدة تكنولوجياً" ، ويظهر هذا بوضوح فى الجرائم الإلكترونية المدعومة بالذكاء الاصطناعى ، مثل عمليات التهريب عبر تقنيات الذكاء الاصطناعى فى التشفير وإخفاء البيانات ، وتطوير برمجيات خبيثة متقدمة ، واستخدام التزييف العميق فى الاحتيال وانتحال الهوية ، فضلاً عن الجرائم التقليدية التى تم تعزيزها عبر هذه التقنيات مثل تزييف العملات والمستندات الرسمية ، والتجسس الصناعى والتجارى ، وحتى العمليات الإرهابية الإلكترونية التى تستغل تقنيات الذكاء الاصطناعى فى التخطيط والتنفيذ ، ونتيجة لذلك ، بات هناك سباق محموم بين الأجهزة الأمنية والمجرمين الإلكترونيين ، حيث يسعى كل طرف إلى استغلال التكنولوجيا الحديثة لتحقيق أهدافه ، مما يفرض تحديات متزايدة تتطلب تطوير استراتيجيات أمنية أكثر ذكاءً وقدرة على مواجهة هذه التهديدات المتطورة. (الحاج،٢٠٠٢،ص ١٨)

أولاً: مشكلة البحث:

أدى التطور السريع للذكاء الاصطناعى إلى تأثيرات إيجابية كبيرة ، حيث ساهم فى تحسين العديد من جوانب الحياة اليومية وجلب وسائل راحة متطورة ، إلا أنه فى المقابل ساهم أيضاً فى ظهور تحديات أمنية جديدة ، من أبرزها نشوء أنماط مستحدثة من الجرائم الإلكترونية ، فقد أصبحت الجرائم التقليدية مثل السرقة والاحتيال تتخذ أشكالاً رقمية جديدة ، مستفيدة من تقنيات الذكاء الاصطناعى ، مما أدى إلى تطور مفهوم "الجرائم الإلكترونية المدعومة بالذكاء الاصطناعى"، ومع استمرار تطور هذه التقنيات ، تتغير طبيعة الجرائم الإلكترونية لتصبح أكثر تعقيداً ،إذ توفر هذه التكنولوجيا وسائل متطورة للمجرمين تتيح لهم تنفيذ أنشطتهم الإجرامية بسهولة أكبر، مع زيادة صعوبة كشفهم أو ملاحقتهم ، علاوة على ذلك ، تسهم تكنولوجيا المعلومات والذكاء الاصطناعى فى عولمة الجريمة الإلكترونية ، حيث تلغى الحدود الجغرافية بين الدول ، مما يجعل من الصعب رصد هذه الجرائم أو منعها ، كما تعيق جهود الأجهزة الأمنية فى تعقب الجناة والقبض عليهم ، الأمر الذى يتطلب استراتيجيات أمنية متقدمة لمواجهة هذه التحديات المستجدة. (Dilek,Cakır,2015,P.22)

وتأتى جرائم الذكاء الاصطناعى على قمة جرائم المستقبل القريب ،إن لم يكن بدأ بعضها الآن– فقد أدى التطور التكنولوجى خلال السنوات الماضي ، والذى تسارعت وتيرته فى الفترة الحالية إلى ظهور العديد من الجرائم الإلكترونية ، حيث أعطت البرمجة المتطورة لبعض الآلات التى تعمل بالذكاء الاصطناعى قدرات تصل خطورتها إلى بناء خبرة ذاتية تمكنها من اتخاذ قرارات مفردة فى أى مواقف تواجهها مثل الإنسان البشرى.(Hubbard,2011,p.421)

كما أصبحت الجرائم الإلكترونية واحدة من أهم الجرائم التي يتم تداولها بين الشركات والمنظمات والأفراد ، والتي تعتبر واحدة من أخطر الجرائم ، فتسعى هذه الجرائم إلى سرقة البيانات وتغيير مسار أجهزة الكمبيوتر عن طريق التلاعب بالأنظمة وتغيير برامج الحماية، وتؤثر الجرائم الإلكترونية على أداء أجهزة الكمبيوتر وكذلك الحالة النفسية للمستخدمين ، حيث أن سرقة البيانات أو تغييرها أو حذفها هي واحدة من أخطر الإجراءات التي تواجهها الشركات والأفراد. (Mijwil,Aljanabi,2023,p.65)

وتُعَدّ الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى من أبرز التحديات الأمنية المستحدثة التى أفرزتها العولمة ، حيث أصبح تطور التكنولوجيا الرقمية عاملاً رئيسياً فى توسع نطاق هذه الجرائم وتعقيدها ، فقد أسهم التقدم التقنى الهائل خلال السنوات الأخيرة فى تحويل العالم إلى قرية صغيرة مترابطة ، مما مكَّن المجرمين الإلكترونيين من استغلال هذا التطور لتنفيذ أنشطتهم الإجرامية عبر الحدود دون عوائق تذكر ، وقد تجاوزت إمكانيات التقنيات الحديثة قدرة الأجهزة الرقابية التقليدية ،

مما أضعف من فاعلية تطبيق القوانين الوطنية لمكافحة هذه الجرائم ، الأمر الذى يشكل تهديداً مباشراً لأمن الدول وأمن مواطنيها ، وفى ظل هذا الواقع بات من الضرورى تطوير استراتيجيات أمنية رقمية متقدمة وتعزيز التعاون الدولى لمواجهة الجرائم الإلكترونية ، خصوصاً تلك المدعومة بتقنيات الذكاء الاصطناعى ، والتى باتت تشكل خطراً متزايداً على الأفراد والمجتمعات. (المشهدانى،٢٠١٥،ص٢٤)

فلقد أدى الذكاء الاصطناعى إلى ميل المجرمين إلى استخدام أدوات جديدة فى ارتكاب جرائمهم ، ولم يعد المجرمون يستخدمون الأسلحة البيضاء والمسدسات والقنابل أو حتى المدافع الرشاشة ، فلقد أصبحت مثل هذه الأدوات بدائية لا تتلاءم مع روح العصر التكنولوجى الحالى ، فلقد اختلفت الصورة الكلاسيكية لعصابات المافيا وهى تلك العصابات التى بدأت فى جزيرة صقلية ثم عبرت المحيط الأطلنطى إلى أمريكا ومنها انتشرت فى جميع أنحاء العالم ، حيث كان رجال المافيا عبارة عن لصوص وقتلة ومحترفين ، وكانت ملامح وجوههم كفيلة بالتعرف كتهريب الخمور والمخدرات والسطو المسلح وفرض الإتاوات وإدارة شبكات الدعارة والبغاء، ولقد حل محل الصورة الكلاسيكية السابقة صور إجرامية حديثة تكنولوجية تعتمد فيها العصابات الإجرامية على الحاسبات الآلية وشبكة المعلومات الدولية ، بل أصبح لمثل هذه العصابات القدرة على امتلاك شركات صناعة برامج الحاسبات الآلية، وكونت ثروات هائلة من خلال العديد من عملياتها الإجرامية مثل التجارة البشرية والتجارة فى المخدرات وفى عمليات غسيل الأموال التى جمعتها من مصادر غير شرعية ، وكانت أسلحة مثل هذه العصابات قاصرة على المسدسات والمدافع الرشاشة والقنابل والشاحنات الناسفة ،أما الآن ونحن فى بداية الألفية الثالثة فإن العصابات الإجرامية تستخدم أسلحة تعمل بأشعة الليزر ، وتستخدم قنابل يمكن تفجيرها بالريموت كنترول أو حتى بمجرد إشارة لاسلكية من هاتف جوال ، وتخلت العصابات الإجرامية عن ممارسة الابتزاز من خلال خطف الأشخاص أو المطالبة بفدية مقابل إطلاق سراحهم أو تهديد أصحاب الأعمال والشركات ، ومن أهم أدوات الجريمة العصرية استخدام الحاسب الآلى وشبكة المعلومات الدولية وأجهزة الليزر والفاكس.(عوض،٢٠١٨،ص ص ٢٣٧-٢٣٨)

علاوة على ذلك نجد أن المجتمع الافتراضى الذى يشمل التفاعلات والأنشطة الاجرامية عبر الإنترنت ومنصات التواصل الاجتماعى ، له تأثير كبير على الأمان المجتمعى ، وذلك من خلال زيادة الجرائم مثل القرصنة والاتجار بالبشر وتداول المواد المخدرة والعقاقير المصطنعة وغسل الأموال بالإضافة إلى استخدام المنصات الرقمية والدارك ويب "الإنترنت المظلم" فى التواصل والتخطيط لتلك الجرائم ، ويشير هذا المصطلح إلى التفاعلات والتواصلات فى العالم الرقمى ؛ حيث يتيح للأفراد التفاعل والمشاركة بسهولة دون معوقات المسافات والزمان ويمكن المجتمع الافتراضى للأفراد من تبادل الأفكار والمعلومات

بوسائل متنوعة ، سواء عبر شبكات التواصل الاجتماعى ، والمنتديات، ووسائل الدردشة ، والمدونات ، وغيرها من المنصات. (البابلى،٢٠٢٤،ص ص ١٤٤-١٤٥)

ولا شك أن الذكاء الاصطناعى ، رغم فوائده العديدة التى تعود بالنفع على البشرية ، يحمل فى طياته جوانب خطرة تهدد أمن وسلامة المجتمع ، حيث أصبح استغلال المجرمين لهذه التقنية واقعاً ملموساً ، بل إن بعض صور الجرائم الإلكترونية المدعومة بالذكاء الاصطناعى قد تم توثيقها على المستوى العالمى ، وتشمل هذه الجرائم أشكالاً متعددة ، مثل التزوير والاحتيال والسرقة والقتل الإلكترونى . بالإضافة إلى القرصنة الرقمية وانتهاك الخصوصية ، وغيرها من الجرائم التى تستغل قدرات الذكاء الاصطناعى المتقدمة ، كما أن التطور المستمر فى تطبيقات الذكاء الاصطناعى يمنحه قدرة هائلة على رصد وتحليل البيانات الشخصية والحكومية ، مما قد يؤدى إلى تعرض الأفراد والمؤسسات ، بما فى ذلك الجهات الحكومية ، لتهديدات خطيرة مثل الابتزاز الإلكترونى وتسريب المعلومات والاختراقات الأمنية ، الأمر الذى يتطلب استراتيجيات فعالة لمكافحة هذه الجرائم المتطورة.(الذباحى،٢٠٢٤،ص ٣)

وتبدو مشكلة الدراسة فى أن معظم جرائم الذكاء الاصطناعى تعد من الجرائم الخفية Dark Numbers of crimes حيث يقع العديد منها دون اكتشافه ، لطبيعة هذه الجرائم التى تنطوى على قدر كبير من الخداع والاحتيال الذى يبدو فى قدرة مرتكبيها على إقناع ضحاياهم بأن أهدافهم عادية ومشروعة ، كما تتسم هذه الجرائم بالتعقيد المتزايد الأمر الذى يعوق عملية الكشف عنها أو حتى ملاحقة مرتكبيها وعقابهم لقدرتهم الفائقة على إخفائها ، هذا بالإضافة إلى عدم وجود أجهزة متخصصة لكشفها والتحقق منها ، وللقصور التشريعى فى مواجهتها ، وموقف الضحايا السلبى إما لعدم علمهم بإرتكاب جرائم ضدهم ،أو لعدم وجود دليل مادى على مرتكبى الجرائم ضدهم ،أو للتسجيل المغلوط لجرائم التطور التكنولوجى.(عوض،٢٠١٨، ص ٢٢٨)

فى ضوء الطرح السابق ، تتبلور مشكلة الدراسة الحالية فى استكشاف تأثير الذكاء الاصطناعى على أنماط ارتكاب الجرائم الإلكترونية ، وذلك من خلال تحليل كيفية توظيف تقنيات الذكاء الاصطناعى فى تسهيل هذه الجرائم ، وتحديد المخاطر والتحديات التى تواجه الضحايا.

ثانياً: الإطار النظرى حول تأثير الذكاء الاصطناعى على أنماط ارتكاب الجرائم الإلكترونية:

يعد تأثير الذكاء الاصطناعى على أنماط الجرائم الإلكترونية من القضايا الحديثة التى تشغل اهتمام الباحثين والمختصين فى مجال الأمن السيبرانى ، وعلم الاجتماع الجنائى ، والتكنولوجيا الرقمية ، فقد أدى التطور السريع فى تقنيات الذكاء الاصطناعى إلى ظهور أساليب جديدة ومتطورة لإرتكاب الجرائم الإلكترونية ، مما أتاح للمجرمين فرصاً غير مسبوقة لتنفيذ هجماتهم بطرق أكثر تعقيداً وفعالية .

يستعرض هذا القسم الإطار النظرى للدراسة من خلال عرض للدراسات والبحوث السابقة التى تناولت تأثير الذكاء الاصطناعى على أنماط الجرائم الإلكترونية ، وأيضاً تحليل المفاهيم المرتبطة بالذكاء الاصطناعى والجرائم الإلكترونية ، بالإضافة إلى مناقشة النظريات المفسرة لهذا التأثير ، والاتجاهات البحثية التى تناولت العلاقة بين التطورات التكنولوجية والجريمة ، كما يهدف إلى رصد وتحليل أهم الأبعاد الاجتماعية والاقتصادية الناتجة عن استخدام الذكاء الاصطناعى فى الجرائم الإلكترونية ، مع التركيز على عرض لأهم الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى.

ولقد تعددت الدراسات والبحوث التى تناولت تأثير الذكاء الاصطناعى على أنماط ارتكاب الجرائم الإلكترونية ، حيث ركزت كل منها على جانب معين من هذه الظاهرة المتنامية ، ومنها: دراسة(الحوتى ،٢٠٢٠) هدفت هذه الدراسة فى التعرف على أنماط الجرائم الإلكترونية فى المجتمع المصرى ، والكشف عن الدوافع الذاتية لإرتكاب هذا النمط الإجرامى ، وتفسير الجرائم الإلكترونية فى ضوء بعض المتغيرات الموضوعية والاجتماعية والثقافية ، وقد اعتمدت الدراسة على المنهج الوصفى ، وتم الاعتماد على أداة دراسة الحالة لطائفة من نزلاء سجن شديد الحراسة بمدينة جمصة محافظة الدقهلية ، لـ٢٢ حالة من مرتكبى الجرائم الالكترونية بأنماطها المختلفة ، وقد توصلت الدراسة لعدد من النتائج نذكر منها : تنوعت أنماط الجرائم الإلكترونية ما بين السب والقذف والتشهير واختراق الحسابات البنكية ، وسرقة بطاقات الائتمان ، والتهديد والابتزاز عبر الانترنت ، كشفت الدراسة الميدانية أن أبرز الدوافع لهذه الجرائم الطمع وحب الثراء والرغبة فى تحقيق النجاح المادى ، وخاصة جرائم اختراق الحسابات البنكية ، قرصنة الشبكات ، سرقة كروت الائتمان ، والابتزاز الالكترونى ، تمثل الجرائم الالكترونية تهديداً للأمن القومى للمجتمعات ، ومن أبرز الدوافع هو الرغبة فى الانتقام ، وأكدت الدراسة أيضاً ان نمط الجريمة الإلكترونية يتم بطرق وأساليب احتيالية متباينة وهو سرقة بطاقات الائتمان ، سواء عن طرق عمليات القرصنة الإلكترونية على قواعد البيانات أو من خلال الاحتيال على الضحايا برسائل خادعة ، كما جاءت نتائج الدراسة بأستعراض بعض الحالات الخاصة بالتشهير والسب والقذف عبر الانترنت ، ومن ثم التهديد

بأسلحة من نوع خاص ، وهى البيانات الشخصية أو الصور الخاصة بضحاياهم ، لتؤكد أن عوامل الانتقام تتم بطرق وأساليب غير تقليدية، وإنما بطرق مستحدثة وعبر وسائط الكترونية .

دراسة(الشمرى،٢٠٢١): تهدف هذه الدراسة الى التعرف على مفهوم الجريمة الإلكترونية وانواعها ، والكشف عن مدى تأثيرها فى العراق ولا سيما وان العراق شهد تصاعد فى وتيرة الجرائم الالكترونية، كما يهدف البحث الى معرفة اهم الجرائم الالكترونية التى يعانى منها العراق، فضلاً عن معرفة ابرز وسائل مكافحة الجرائم الالكترونية فى العراق والوقاية منها ، ومن اهم نتائج الدراسة: ان الجرائم الالكترونية تعد اكثر الجرائم المعاصرة انتشاراً، وقد أصبحت من التحديات الرئيسية للأمن الوطنى لأية دولة ، لاسيما وان بعضها لا تستهدف الافراد فحسب وانما البنية الحيوية للدولة، كما ادى الانتشار الواسع لوسائل التواصل الاجتماعى فى العراق الى ارتفاع كبير فى نسبة الجرائم الالكترونية، واما ابرز هذه الجرائم فهى الابتزاز والاتجار بالبشر والارهاب والتسقيط السياسى ، وقد أثرت هذه الجرائم بشكل مباشر فى المجتمع العراقى ، وبالرغم من نجاح المؤسسات الامنية المختصة فى الحد من هذه الظاهرة بيد ان ذلك لا يقلل من تزايد خطورتها وتأثيراتها السلبية ، كما توصلت الدراسة الى ان وسائل مكافحة الجرائم الالكترونية لا تقع مسؤوليتها على عاتق الدولة فقط ، وانما تشمل الافراد ايضاً وهذا يتطلب الالمام بأبسط قواعد ضمان امن المعلومات والاجهزة التقنية المستخدمة ، ورفض الرسائل المشبوهة التى تصل الى المستخدمين ، وعدم تحميل برامج من مصادر غير موثوقة ، وعدم الافصاح عن جميع المعلومات الشخصية غير معروفة مسبقاً، وغيرها الكثير من اجراءات الوقاية والسلامة الالكترونية.

دراسة(عبدالرازق،٢٠٢١) تهدف الدراسة إلى التعرف على تأثير استخدام الذكاء الاصطناعى على ارتكاب الجرائم الالكترونية ، وذلك نظراً لاستحداث عدد من الجرائم الفنية المستمدة من التقنية المعلوماتية ،فبعض المجرمين اتجهوا لاستخدام الوسائل التقنية المستحدثة لتنفيذ جرائمهم ، وقد توصلت الدراسة الى عدد من النتائج لعل من أهمها: يلعب الذكاء الاصطناعى دوراً مهماً فى زيادة الجرائم الالكترونية وانتشارها وهو ما يثبت صحة فرضية الدراسة ،لم يتفق فقهاء القانون على تعريفاً جامعاً للجريمة الإلكترونية ،تعتبر الجرائم الالكترونية أقل عنفاً من الجرائم التقليدية، حيث أنها لا تحتاج إلى أدنى مجهود عضلى ؛ بل تعتمد على الدراسة الذهنية والتفكير العلمى القائم على معرفة بتقنيات الحاسوب ، وإن الباعث على ارتكاب الجرائم الالكترونية هو الحصول على النفع المادى السريع ،ولا يتم فى الغالب الإبلاغ عن جرائم الإنترنت إما لعدم اكتشاف الضحية لها وإما خشيته من التشهير ، كما توصلت الدراسة الى انه يسهل ارتكاب الجرائم الالكترونية على الرغم أنها تعتبر جرائم صعبة الإثبات ، حيث يصعب فى كثير من الأحيان العثور على أثر مادى للجريمة الالكترونية ، كما تؤدى عولمة الجرائم الإلكترونية إلى تشتيت

جهود التحرى والتنسيق الدولى لتعقب مثل هذه الجرائم ، فتعتبر هذه الجرائم هى صورة صادقة من صور العولمة.

دراسة (الهديف،٢٠٢٢) سعت هذه الدراسة الى التعرف على الجرائم الالكترونية ومعرفة آثارها الاجتماعية والاقتصادية،وقد توصلت الدراسة الى عده نتائج نذكر منها: ان الجريمة الالكترونية ذات بعد دولى عابرة الحدود فهى قد تتجاوز الحدود الجغرافية ، مرتكب الجريمة الالكترونية قد يكون منسجماً اجتماعياً وقادراً مادياً، أصحاب الجريمة الالكترونية رغبتهم فى الحصول على الأموال بطرق غير شرعية ، كما يتميزون بالذكاء ومهارات عالية بنظام الحاسوب ، عدم اهتمام مؤسسات الدولة بالجرائم الالكترونية وعدم وضع سياسات لها ، تنوع الجرائم الالكترونية من حين إلى آخر.

دراسة (حسين،٢٠٢٢): هدف هذا البحث فى التعرف على أنماط الجريمة الالكترونية من وجهة نظر طلاب بحوث التخرج بكليتي الآداب والعلوم بجامعة سبها، ولتحقيق هذا الهدف قامت الباحثة بإعداد أداة لجمع المعلومات المتعلقة بموضوع البحث كمقياس : الجريمة الالكترونية، وتكونت العينة من (٥٠) طالب وطالبة، وتم اختيارهم بالطريقة العشوائية البسيطة، وتم استخدام المنهج الوصفي التحليلي، وقد تم تحليل البيانات بواسطة الحزمة الاحصائية للعلوم الاجتماعية(spss) ، وقد أسفرت نتائج البحث على أنه : توجد فروق ذات دلالة احصائية فيما يتعلق بأنماط الجريمة الالكترونية من وجهة نظر طلاب بحوث التخرج بكليتي الآداب والعلوم بجامعة سبها، وهذه الفروق لصالح الدرجة الحيادية، وتوجد فروق ذات دلالة احصائية في أنماط الجريمة الالكترونية من وجهة نظر طلاب بحوث التخرج بكليتي الآداب و العلوم على محور (القرصنة الالكترونية)، والأداة ككل، وهذه الفروق لصالح الذكور على حساب الإناث، ولا توجد فروق في أنماط الجريمة الالكترونية على محور(التهديد والابتزاز ونشر الفيروسات) بإختلاف متغير الجنس، ولا توجد فروق ذات دلالة احصائية في أنماط الجريمة الالكترونية من وجهة نظر طلاب بحوث التخرج بكليتي الآداب و العلوم على محور(القرصنة الالكترونية والتهديد والابتزاز والأداة ككل)، وتوجد فروق في أنماط الجريمة الالكترونية على محور(نشر الفيروسات)، وهذه الفروق لصالح الطلاب ممن لديهم مهارة ضعيفة بإختلاف متغير مهارات الاستخدام، ولا توجد فروق ذات دلالة احصائية في أنماط الجريمة الالكترونية من وجهة نظر طلاب بحوث التخرج بكليتي الآداب و العلوم بإختلاف متغير الكلية، ولا توجد فروق ذات دلالة احصائية في أنماط الجريمة الالكترونية من وجهة نظر طلاب بحوث التخرج بكليتي الآداب و العلوم بإختلاف متغير مرحلة البحث.

دراسة(الدسوقى،٢٠٢٢)تهدف هذه الدراسة إلى تسليط الضوء على تأثير استخدام الذكاء الاصطناعى على ارتكاب الجرائم ، فقد حقق التطور التقنى المعلوماتى قفزات نوعية ،وأحدث تغييرات إيجابية على المستويين الدولى والإقليمى، وقد توصلت الدراسة الى عدد من النتائج الهامة نذكر منها: تعد الجرائم

الإلكترونية وجرائم التقنيات الحديثة أقل عنفاً من الجرائم التقليدية ، حيث إنها لا تحتاج إلى أدنى مجهود عضلى، بل تعتمد على الدراسة الذهنية والتفكير العلمى القائم على معرفة بتقنيات الحاسوب والآلة ، وإن الباعث على ارتكاب الجرائم الإلكترونية هو الحصول على النفع المادى السريع إضافة إلى الإضرار بالمصلحة العامة للبلاد ، ويسهل ارتكاب الجرائم الإلكترونية وجرائم التقنيات الحديثة ، على الرغم من أنها تعد جرائم صعبة الإثبات ، حيث يصعب فى كثير من الأحيان العثور على أثر مادى للجريمة .

دراسة(الأميرى، والعموش،٢٠٢٢) تسعى هذه الدراسة إلى تدارك العلاقة بين استعمال التكنولوجيا بوصفها نشاطاً روتينياً وازدياد معدلات الجريمة ، وتكمن اهمية الدراسة فى أنه على الرغم من الجهود التى تبذلها الحكومات وأدوار الإعلام فى التنبيه والتحذير من سلبيات ومخاطر التكنولوجيا إلا أن هناك ارتفاعاً فى معدلات الجريمة بسبب عدم وجود الخبرات اللازمة للتعامل مع هذا العالم الافتراضى ، لذا وجب تلافى الأضرار والمخاطر الاجتماعية والأمنية والاقتصادية ، الناجمة عن استعمال التكنولوجيا بوصفها نشاطاً روتينياً من دون وعى وعدم توافر للخبرات اللازمة للتعامل معها أو على الأقل الحد من آثارها ، وقد أظهرت نتائج الدراسة أن أكثر ضحايا استعمال التكنولوجيا كان لهم أثر فيما أصابهم فما أن وجد جانى وضحية فى مكان وزمان مع غياب الرقابة تحدث الجريمة طبقاً لنظرية الأنشطة الروتينية ، ومن جانب آخر نجد أن تطابق فرضيات نظرية أسلوب الحياة جاء مؤكداً لأثر المجنى عليه فى وقوع الجريمة، كما تبين انه بقدر ما أسهمت به التكنولوجيا من دعم وتوفير سبل الراحة وسهولة التواصل إلا أن لها جوانب سلبية وخيمة على الأفراد والمجتمعات والدول ، فكما تم ذكره أضحت الجريمة الإلكترونية عائقاً يواجه مختلف مظاهر الحياة الأمنية منها والاقتصادية والاجتماعية ، مما ينذر بخطر من شأنه أن يزعزع أمن المجتمع الدولى برمته واستقراره.

دراسة (ابراهيم،٢٠٢٣) هدفت هذه الدراسة الى التعرف على استخدامات ضحايا التنمر الإلكترونى لمواقع التواصل الاجتماعى ، وصور هذا التنمر ، وأسبابه ، وموقف الضحية عند التعرض له ، وآثاره ، وآليات الحد منه ، واعتمد البحث على طريقة دراسة الحالة ، وتم التطبيق على عينة عمدية تم الوصول إليها بطريقة كرة الثلج ، وشملت (١٠) حالات من طلاب وطالبات جامعة دمياط الذين تعرضوا للتنمر الإلكترونى ، وقد توصل البحث إلى أن جميع حالات البحث تعرضوا للتنمر الإلكترونى عبر مواقع التواصل الاجتماعى ، حيث إن معظمهم قد تعرضوا للإساءة اللفظية والسخرية ، ومنهم من تعرض للتحرش ، وآخرون تعرضوا للمطاردة عبر مواقع التواصل الاجتماعى ، والبعض الآخر منهم تعرض لمنع التعبير عن رأيه فى مجموعات الواتساب ، وتبين أن الأسباب الاجتماعية المؤدية للتنمر الإلكترونى ترجع إلى التنشئة الاجتماعية الخاطئة للأبناء ، وضعف الرقابة الأسرية عليهم ، كما ترجع أيضاً الى رفاق السوء ، أما عن الأسباب فيمكن تلخيصها فى التطور التكنولوجى ، وغياب دور المؤسسات التعليمية

، ووسائل الإعلام ، وقد اتضح أن معظم حالات البحث لا يعرفون السبب الحقيقى الذى دفع للتنمر عليهم ، والبعض الاخر أفادوا بأنهم تعرضوا للتنمر بسبب تميزهم فى العمل واهتمامهم بمظهرهم الخارجى ، وارتفاع المستوى الاقتصادى لأسرهم وتميزهم فى الدراسة ، أما عن ردود أفعال الضحايا عند تعرضهم للتنمر الإلكترونى فقد تمثل فى حظر الشخص المتنمر تجاهل الرد عليه ، يلى ذلك غلق الحساب الشخصى للضحية ، ثم تحرير بلاغ فى مباحث الإنترنت ضد المتنمر ، وبالنسبة للآثار الناجمة عن التنمر الإلكترونى على الضحية ، فمن الناحية الاجتماعية أدى إلى معاناة معظم الضحايا من عينة البحث من العزلة الاجتماعية ، والبعض الآخر منهم فكر فى الانتحار ، ومن بينهم من عانوا من عدم التركيز فى عملهم ، أما بالنسبة للآثار النفسية فتمثلت فى أن معظم الضحايا من عينة البحث أصبحوا يلجئون إلى السلوكيات العدوانية نتيجة تعرضهم للتنمر الإلكترونى ، والبعض الآخر منهم عانوا من فقدان الثقة بالنفس ، ومنهم من أصبح لديه نوع من الرهاب الإلكترونى ، وبالنسبة للآثار الأكاديمية فإن معظم عينة البحث تغيبوا عن الجامعة وأهملوا فى دراستهم ، ومن بينهم من انخفضت قدرتهم على التحصيل الدراسى والفهم والتفكير.

دراسة(مغايرة،٢٠٢٤)هدفت هذه الدراسة إلى تسليط الضوء على ظاهرة جديدة ومستحدثة من جرائم الذكاء الاصطناعى يطلق عليها التزييف العميق، وذلك بعرض الجوانب الهامة التى تحيط بتلك التقنية ، وبيان فوائدها وأضرارها وعرض الجرائم التى ارتكبت والجرائم التى يحتمل ارتكابها والآثار الناتجة عن سوء الاستخدام، وتحليل بعض الجوانب القانونية الرئيسية المتعلقة بها لمعرفة ما إذا كان استخدام هذه التقنية بحد ذاته يشكل جريمة وقد توصلت الدراسة لعدد من النتائج نذكر منها:ان الجرائم الالكترونية ومنها جريمة التزييف العميق سلاح ذو حدين إيجابى مفيد وسلبى ضار يمكن استخدامها لارتكاب العديد من الجرائم التقليدية بأسلوب حديث، تعتبر جريمة التزييف العميق من الظواهر الاجرامية التى قد تسبب الكثير من الأضرار للأفراد والمؤسسات والدول ، لم تأت جريمة التزييف العميق بجرائم جديدة لكنها أداة حديثة لارتكاب العديد من الجرائم التقليدية أو السيبرانية بسهولة وأقل كلفة مقابل صعوبة اكتشاف حقيقة المحتوى المزيف واكتشاف المجرم.

دراسة (الشهومية،والكندى،٢٠٢٤)هدفت الدراسة الحالية إلى التعرف على تأثير استخدام تطبيقات الذكاء الاصطناعي على الخصوصية الرقمية للأفراد والمؤسسات في سلطنة عمان من حيث التعرف على استخداماتها على الشبكات الاجتماعية، والبرمجيات مفتوحة المصدر، والتعرف على التحديات الناجمة عن استخدامها، حيث اعتمدت الدراسة على المنهج النوعي، واستخدمت مجموعات التركيز التي بلغ عددها ثلاث مجموعات، والمقابلات شبه المقننة التي بلغ عددها ثمان مقابلات كأدوات لجمع البيانات ، شمل مجتمع الدراسة المؤسسات التي لها ممارسات في استخدام تطبيقات الذكاء الاصطناعي وتلك

التي تتعامل مع الأنظمة التقنية والتشريعية ذات العلاقة ، وقد تم اختيار عينة الدراسة بشكل قصدي، وتألفت من ست مؤسسات؛ منها أربع مؤسسات حكومية، ومؤسستان خاصة ، وتوصلت الدراسة إلى مجموعة من النتائج أبرزها: تستخدم بعض الشركات الكبرى تطبيقات الذكاء الاصطناعي ضمن مواقع الشبكات الاجتماعية والبرمجيات مفتوحة المصدر في انتهاك الخصوصية، والتعدي على بيانات المستخدمين عن طريق تحليلها وبيعها لمؤسسات أخرى لتحقيق أهداف سياسية أو ربح مادي، كما أوضحت النتائج أن تطبيقات الذكاء الاصطناعي قد تستخدم في ارتكاب جرائم معلوماتية كالابتزاز الإلكتروني، وسرقة البيانات الحكومية، وتعطيل الأنظمة، أو يمكن تطويعها من قبل المهندسين الاجتماعيين لارتكاب الجرائم الإلكترونية بطرق أكثر تقدمًا.

دراسة(Sellrs,2011) هدفت هذه الدراسة الى دراسة آثار المشاركة فى مواقع الشبكات الاجتماعية على جنوح الشباب بما فى ذلك المتغيرات التابعة ، وتعاطى المخدرات والجريمة والبلطجة على الآخرين وكونهم ضحية البلطجة ، وقد اعتمدت هذه الدراسة على المنهج الوصفى وإستخدمت الاستبانة كأداة لجمع البيانات وطبقت على عينة مكونة من (١٤٤) مفردة من الذكور والاناث من المدارس المتوسطة والثانوية ، وتوصلت الدراسة الى أن الشباب الكبار هم الأكثر مشاركة فى السلوك المنحرف والمراهقين الذكور هم الأكثر عرضة لمشاكل تعاطى المخدرات ، كما ان الخدمات التى تقدمها شبكات التواصل الاجتماعى خاصة تطبيقاتها على الهواتف المحمولة قد يؤثر على مشاركة المراهقين فى المشاكل المدرسية ، والجريمة ،وتعاطى المخدرات ، والبلطجة ، أو كونها ضحية العنف الالكترونى.

دراسة (Gupta,2017) تهدف هذه الدراسة الى التعرف على أثر الجريمة الالكترونية عبر مواقع التواصل على إدراك المراهقين للقضايا المجتمعية ، وتم اختيار عينة عشوائية من الطلاب وصلت الى (٣٠٠) طالب تتراوح أعمارهم من ١٢ الى ١٩ سنة ، معتمدة على المسح الاجتماعى مستخدمة اداة إستمارة الاستقصاء لجمع المعلومات والبيانات ، وتوصلت الدراسة الى مجموعة من النتائج اهمها: تشير نتائج الدراسة الى اهم الجرائم التى تعرضت لها العينة البحثية هى سرقة الملفات ، وسرقة هويات الاعضاء مما يكون إستخدامها بعد ذلك فى التعاملات البنكية وسرقة الأموال ،وايضاً لمواقع التواصل الاجتماعى تأثير إيجابى فى دعم ونشر مختلف المعارف المرتبطة بالامن الاجتماعى ، وغيره من القضايا المجتمعية الهامة ، كما أشارت نتائج الدراسة الى ان العوامل الرئيسية لحماية الشباب من تلك الجرائم الالكترونية يقع على عاتق الاسرة فهى تمنعهم من الوقوع ضحايا لمثل ذلك النوع من الجرائم الالكترونية التى تؤثر عليهم مادياً ومعنوياً.

دراسة(Shamiullam,2019) تهدف هذه الدراسة الى معرفة أدوات الذكاء الاصطناعى المختلفة وأهميتها وتأثيرها على الأمن السيبرانى ، كما تهدف الى قياس تأثير أدوات الذكاء الاصطناعى فى تحديد

الهجمات الإلكترونية المختلفة، وقد توصلت الدراسة الى ان الذكاء الاصطناعي موجود في كل مجال من مجالات حياة الإنسان ، على سبيل المثال: الألعاب ، معالجة اللغات ، التعرف على الكلام ، الأنظمة الخبيرة ، أنظمة الرؤية ، التعرف على الكتابة اليدوية ، الروبوتات الذكية ، المعاملات المالية، كل نشاط في حياة الإنسان أصبح جزءًا من الذكاء الاصطناعي على الرغم من الاستخدامات العديدة ، يمكن أيضًا استخدام الذكاء الاصطناعي لتدمير حياة الإنسان، هذا هو السبب في أن التدخل البشري مطلوب لمراقبة أنشطة الذكاء الاصطناعي، كما أصبحت الجرائم الإلكترونية شائعة جدًا وأصبحت خبرًا يوميًا، فهذه ليست مجرد مشكلة تواجه بلدًا واحدًا ؛ إنها في جميع أنحاء العالم، فلقد أصبح الذكاء الاصطناعى تهديدًا كبيرًا للحكومات والبنوك والشركات متعددة الجنسيات من خلال الهجمات عبر الإنترنت من قبل المتسللين، حيث يتم استغلال الكثير من البيانات الفردية والتنظيمية من قبل المتسللين ، ويصبح تهديدًا كبيرًا للعالم السيبراني.

دراسة (Carla,Irina,2023) تهدف الدراسة الى مناقشة ماهية الذكاء الاصطناعي وكيف يحدد حياتنا، ومعرفة الدور الذى يلعبه فى ارتكاب الجرائم الالكترونية وايضاً دوره فى منع ومكافحة الجرائم الإلكترونية ، وقد توصلت الدراسة الى عده نتائج نذكر منها:اتفاق المشاركون في استطلاع رأى (٨٥٠ مسؤولًا تنفيذيًا من الأمن السيبراني وتكنولوجيا المعلومات وأمن المعلومات وعمليات تكنولوجيا المعلومات من عشر دول) على أن الاستجابة التي تعمل بالذكاء الاصطناعي ضرورية بسبب استخدام مجرمي الإنترنت لتكنولوجيا الذكاء الاصطناعي لتنفيذ الهجمات ، ووفقًا لثلاثة من كل أربعة رؤساء تنفيذيين تم استطلاع آرائهم ، يمكّن الذكاء الاصطناعي شركتهم من الاستجابة للاختراقات بسرعة أكبر ، كما تعتقد ٦٩٪ من الشركات أن الذكاء الاصطناعي مطلوب للاستجابة للتهديدات ، ووفقًا لثلاثة من كل خمس شركات فإن استخدام الذكاء الاصطناعي يعزز دقة وكفاءة المحللين السيبرانيين ، ويقدم الذكاء الاصطناعي إجابات أفضل لمتطلبات الأمن السيبراني للمنظمة مع نمو الشبكات وزيادة تعقيد البيانات ، ببساطة البشر غير قادرين على التعامل مع التعقيدات المتزايدة بمفردهم ، وسيصبح استخدام الذكاء الاصطناعي أمرًا لا مفر منه عاجلاً أم آجلاً ، فقد أظهر الذكاء الاصطناعي حتى الآن أنه لا يعدو كونه إيجابيًا، فالذكاء الاصطناعي في طريقه إلى تغيير قواعد الحياة في الأخلاق والرعاية الاجتماعية والرعاية الصحية والقوى العاملة، نظرًا لأن هذه هي أهم مكونات الحياة.

دراسة**(Muyad, Mohammad,2023)** يعد التصيد الاحتيالي عبر الإنترنت تحديًا أمنيًا كبيرًا لمستخدمي الويب بسبب ثلاثة عوامل رئيسية: أولاً من السهل تنفيذه ولا يتطلب خبرة فنية عميقة في البرمجة أو الشبكات، ثانيًا: يمكن تنفيذه عبر منصات متنوعة بما في ذلك الويب والرسائل النصية ومنصات التواصل الاجتماعي، ثالثاً: يعتمد هذا النوع من الهجوم على الهندسة الاجتماعية مما يعني أن

استجابات المستخدمين تتأثر بالمحتوى المعروض عليهم، وتم استخدام مجموعة بيانات ضخمة تشمل ميزات الويب التي لا تحتوي على محتوى بإجمالي ١١١ سمة مميزة، وتم الاستفادة من الارتباطات بين هذه الميزات ونتائج التصنيف لتبسيط مجموعة الميزات، وتم استكشاف قيم ارتباط مختلفة كما توصلت الدراسة لعدد من النتائج من مراحل التدريب والتقييم على أهمية الارتباط بين الميزات التي تم اختيارها في تحديد دقة الخوارزمية،فيقدم البحث نهجًا مبتكرًا لمكافحة التصيد الاحتيالي عبر الويب، حيث يُظهر إمكانات تقنيات التعلم الآلي الهجينة والدور الحاسم لاختيار الميزات من خلال تحليل الارتباط لتعزيز دقة الكشف ،كما اظهر البحث أن أسباب هجمات التصيد على مواقع الويب نقص الوعي الأمني للمستخدمين ، ومتابعة المجرمين للحوافز المالية ، وعدم بذل العناية الواجبة من قبل المنظمات للتخفيف من هذه الهجمات.

دراسة(Zandi,Yaacob,2024) تقدم هذه الدراسة لمحة عامة شاملة عن تهديد الذكاء الاصطناعي للأمن السيبراني ، مع التركيز بشكل خاص على انتشار الذكاء الاصطناعي التوليدي وتأثيراته على إدارة المخاطر المالية، وقد توصلت الدراسة لعدد من النتائج نذكر منها: أن الذكاء الاصطناعي يُعيد تشكيل مشهد التهديدات الإلكترونية من خلال تزويد مجرمي الإنترنت بقدرات قوية وتغيير مفاهيم الأدلة والحقيقة، كما تؤكد الدراسة على أن التطور السريع للذكاء الاصطناعي يتجاوز القوانين واللوائح والمعايير المجتمعية الحالية ، مما يثير مخاوف بشأن احتمال حدوث "مستقبل ما بعد الثقة" ،وتؤكد أيضاً هذه الدراسة على أن الذكاء الاصطناعي يُساعد كلاً من المدافعين والمهاجمين ، حيث يتمتع مجرمو الإنترنت بإمكانية الوصول إلى نفس أدوات وتقنيات الذكاء الاصطناعي، وتشير الدراسة إلى أن قدرات الذكاء الاصطناعي التوليدي تُزيد من كفاءة ونطاق وقدرة عمليات الاحتيال والهجمات الإلكترونية الحالية ، مما يطرح تحديات كبيرة للمهنيين في مجال التمويل.

موقف الدراسة الحالية من الدراسات السابقة:

من خلال الاستقراء التحليلى للدراسات السابقة يتضح ما يلى:

تعدد وتنوع أنماط الأبحاث والدراسات التى تناولت تأثير الذكاء الاصطناعى على أنماط ارتكاب الجرائم الإلكترونية ، فقد ركزت بعض الدراسات على دور الذكاء الاصطناعى فى تسهيل ارتكاب الجرائم الإلكترونية ، فى حين سلطت دراسات أخرى الضوء على دوره فى مكافحة هذه الجرائم ، كما تناولت بعض الأبحاث أنماط الجرائم الإلكترونية فى المجتمع المصرى ، بينما اهتمت دراسات أخرى بدراسة الآثار الاجتماعية والاقتصادية لهذه الجرائم ، بالإضافة إلى ذلك ، سعى بعض الباحثين إلى استكشاف العلاقة بين الاستخدام الروتينى للتكنولوجيا وارتفاع معدلات الجريمة .

من حيث أهداف الدراسات السابقة: هدفت بعض الدراسات إلى تقديم لمحة عامة عن تهديد الذكاء الاصطناعى للأمن السيبرانى ، مع التركيز بشكل خاص على انتشار الذكاء الاصطناعى التوليدى وتأثيراته على إدارة المخاطر المالية ، بينما ركزت دراسات أخرى على مناقشة ماهية الذكاء الاصطناعى ، وكيفية تأثيره على حياتنا ودوره فى ارتكاب الجرائم الإلكترونية ، كما سلطت بعض الدراسات الضوء على أدوات الذكاء الاصطناعى المختلفة ، وأهميتها وتأثيرها على الأمن السيبرانى ، وفى سياق مختلف ، تناولت بعض الدراسات آثار المشاركة فى مواقع الشبكات الاجتماعية على جنوح الشباب ، بينما ركزت دراسات أخرى على تأثير استخدام تطبيقات الذكاء الاصطناعى على الخصوصية الرقمية للأفراد والمؤسسات فى سلطنة عمان ، كما سعت بعض الدراسات إلى تسليط الضوء على ظاهرة جديدة ومستحدثة من جرائم الذكاء الاصطناعى تعرف بالتزييف العميق ، فى حين ركزت دراسات أخرى على التعرف على كيفية استخدام ضحايا التنمر الإلكترونى لمواقع التواصل الاجتماعى ، وأشكال هذا التنمر وأسبابه ، وتتفق الدراسة الحالية مع الأهداف التى تناولتها الدراسات السابقة ،إلا أنها تتميز بتركيزها على تأثير الذكاء الاصطناعى على أنماط ارتكاب الجرائم الإلكترونية ، بالإضافة إلى تحليل الدور الذى يلعبه الذكاء الاصطناعى فى تسهيل ارتكاب هذه الجرائم ، كما تنفرد الدراسة برصد الأسباب المؤدية إلى ارتكاب الجرائم الإلكترونية من وجهة نظر الضحايا الذين تعرضوا لها ، فضلاً عن تحليل المخاطر والتحديات المختلفة التى تواجه الضحايا نتيجة هذه الجرائم ، كذلك تهدف الدراسة إلى استكشاف موقف الضحايا عند تعرضهم للجرائم الإلكترونية المدعومة بالذكاء الاصطناعى ، وأخيراص استخلاص المقترحات التى قد تسهم فى حماية الأفراد من هذه الجرائم ، وذلك من وجهة نظر الضحايا أنفسهم .

ومن حيث الرؤى النظرية: تنوعت الدراسات السابقة سواء العربية أو الأجنبية ، فى استخدامها للنظريات المفسرة لتأثير الذكاء الاصطناعى على أنماط ارتكاب الجرائم الإلكترونية ، فقد استندت بعض الدراسات إلى نظرية الثقافة الفرعية فى تفسير السلوك الإجرامى ، بينما اعتمدت دراسات أخرى على نظرية الدور ، نظرية النشاط الروتينى ، نظرية الرتب الاجتماعية ، ونظرية الانتقال الفضائى ، أما الدراسة الحالية فقد اعتمدت على ثلاث نظريات أساسية فى تفسير تأثير الذكاء الاصطناعى على أنماط ارتكاب الجرائم الإلكترونية ، وهى : نظرية النشاط الروتينى ، نظرية الاستخدامات والإشباعات ، ونظرية التفاعلية الرمزية.

ومن حيث الرؤى المنهجية: اختلفت الدراسات السابقة فى مناهجها البحثية وأدواتها ، حيث اعتمدت بعض الدراسات على المنهج الوصفى مستخدمة أداة دراسة الحالة ، وتم تطبيقها على إحدى السجون المصرية ، فى حين لجأت دراسات أخرى إلى استخدام المقياس كأداة لجمع البيانات ، وشملت

عيناتها (٥٠) طالباً وطالبة ، مع اعتماد المنهج الوصفى التحليلى ، أما بعض الدراسات الأخرى فقد اعتمدت على المنهج الوصفى ، وتم اختيار عينة عمدية بطريقة كرة الثلج ، شملت (١٠) حالات من طلاب وطالبات جامعة دمياط الذين تعرضوا للتنمر الإلكترونى ، فى المقابل اعتمدت بعض الدراسات على المنهج النوعى ، واستخدمت مجموعات التركيز ، حيث بلغ عددها ثلاث مجموعات ، بالإضافة إلى المقابلات شبه المقننة ، والتى بلغت ثمانى مقابلات كأدوات لجمع البيانات ، أما الدراسة الحالية فقد اعتمدت على المنهج الوصفى التحليلى ، نظراً لقدرته على وصف وتفسير وتحليل البيانات المرتبطة بتأثير الذكاء الاصطناعى على أنماط ارتكاب الجرائم الإلكترونية ، وقد تم اختيار عينة عمدية بطريقة كرة الثلج ، وذلك بمساعدة الإخباريين ، وشملت العينة (٢٠) حالة من ضحايا الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، كما تم استخدام أداة دراسة الحالة للتطبيق على هذه الحالات ، مما ساعد فى الحصول على بيانات تفصيلية ومعمقة حول الظاهرة محل الدراسة.

- **ومن خلال استعراض الدراسات السابقة ، يمكن تحديد الإسهامات التى تقدمها هذه الدراسة فى التراث النظرى لعلم الاجتماع على النحو التالى :**

- **تركز الدراسة الحالية بشكل مباشر:** على إشكالية الذكاء الاصطناعى وتأثيره على ارتكاب الجرائم الإلكترونية ، مع التطبيق على ضحايا الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى فى محافظة القليوبية.
- **تضيف هذه الدراسة بعداً جديداً:** من خلال استخدام مجموعة من النظريات والتوجهات النظرية التى تسهم فى فهم أعمق لتأثير الذكاء الاصطناعى فى تسهيل وارتكاب الجرائم الإلكترونية المختلفة.
- **يركز الجانب الميدانى لهذه الدراسة:** على تحليل أوضاع ضحايا الجرائم الإلكترونية المدعومة بالذكاء الاصطناعى ، مما يجعلها دراسة نوعية تهدف إلى فهم طبيعة هذه الجرائم وآثارها على الأفراد والمجتمع.

ثالثاً: أهمية البحث:

تنقسم أهمية البحث إلى :

الأهمية النظرية:

- تبرز أهمية الدراسة من خلال تسليط الضوء على أحد الموضوعات الحديثة والمهمة فى علم اجتماع الجريمة ، حيث تُعد الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى من الظواهر المستجدة التى لم تحظَ بالاهتمام الكافى من قِبل الباحثين ، رغم وجود بعض الدراسات العربية والأجنبية التى تناولت الجرائم الإلكترونية ، إلا أن معظمها لم يتوسع فى تحليل الجرائم المدعومة بالذكاء الاصطناعى أو استكشاف أنماطها المختلفة وتأثيراتها المتزايدة
- تسهم هذه الدراسة فى سد الفجوة البحثية عبر تقديم رؤية تحليلية متعمقة حول تأثير الذكاء الاصطناعى على أنماط ارتكاب الجرائم الإلكترونية ، مما يساعد على تطوير الأطر النظرية فى هذا المجال .
- كما تنبع أهمية البحث من حقيقة أن الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى أصبحت تشكل تهديداً مباشراً لأمن الأفراد ، حيث تؤدى الزيادة الهائلة فى حجم البيانات وتوسع استخدام الإنترنت فى تبادل المعلومات والأنشطة الرقمية إلى تزايد صور الاعتداءات الإلكترونية والتهديدات الأمنية ، ومع التطور المستمر لهذه التقنيات ، ظهرت أنماط جديده ومتطورة من الجرائم الإلكترونية ، مما يستدعى دراستها بشكل **معمّق لفهم طبيعتها ، وأساليب ارتكابها ، والآثار المترتبة عليها ، وذلك بهدف استخلاص استراتيجيات فعالة للوقاية والحد من مخاطرها**
- وتكمن أهمية البحث أيضاً فى الانتشار الواسع لتقنيات الذكاء الاصطناعى فى مختلف مجالات الحياة ، والذى يواكبه تزايد مستمر فى الجرائم الإلكترونية المدعومة بهذه التقنيات ، ومع هذا التطور أصبح من الضرورى دراسة دور الذكاء الاصطناعى فى ارتكاب الجرائم الإلكترونية ، وتحليل أساليبه وتأثيراته ، وذلك للحد من انتشاره ووضع آليات لمواجهته بفعالية.

الأهمية التطبيقية:

- رصد وتحليل الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، فى ظل تزايدها المستمر وتنوع أساليبها ، والتى تصل فى بعض الحالات إلى الابتزاز والاحتيال الرقمى وانتهاك الخصوصية.
- تقديم حلول وآليات فعالة للحد من ارتكاب الجرائم الإلكترونية المدعومة بالذكاء الاصطناعى داخل المجتمع المصرى ، بما يساعد صانعى السياسات ومتخذى القرار فى وضع استراتيجيات لمواجهة هذه الظاهرة ، من خلال سن القوانين والتشريعات المناسبة ، وتغليظ العقوبات على مرتكبى الجرائم الإلكترونية ، وتعزيز سبل الحماية الرقمية للأفراد.

رابعاً:أهداف البحث وتساؤلاته

يتحدد الهدف الرئيس لهذه الدراسة فى الكشف عن تأثير الذكاء الاصطناعى على أنماط ارتكاب الجرائم الإلكترونية ، وانطلاقاً من هذا الهدف العام ، تنبثق مجموعة من الأهداف الفرعية ، والتى تتمثل فيما يلى:

الهدف الأول: التعرف على دور الذكاء الاصطناعى فى ارتكاب الجرائم الإلكترونية

ولتحقيق هذا الهدف ، يسعى الباحث إلى الإجابة على التساؤل التالى:

- كيف يسهم الذكاء الاصطناعى فى تسهيل وتعزيز ارتكاب الجرائم الإلكترونية ضد الأفراد؟

الهدف الثانى: التعرف على الأسباب المؤدية إلى ارتكاب الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى من وجهة نظر الضحايا

ولتحقيق هذا الهدف ، يسعى الباحث إلى الإجابة على التساؤل التالى:

- ما العوامل والدوافع التى تسهم فى ارتكاب الجرائم الإلكترونية المدعومة بالذكاء الاصطناعى وفقاً لوجهة نظر الضحايا؟

الهدف الثالث: رصد المخاطر والتحديات المختلفة التى تواجه الضحايا نتيجة تعرضهم للجرائم الإلكترونية المعتمدة على تقنيات الذكاء الاصطناعى

ولتحقيق هذا الهدف ، يسعى الباحث إلى الإجابة على التساؤل التالى:

- ما ابرز المخاطر والتحديات التى يواجهها الضحايا بعد تعرضهم للجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى؟

الهدف الرابع: دراسة موقف الضحايا عند تعرضهم للجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى وكيفية تعاملهم مع هذه الجرائم

ولتحقيق هذا الهدف ، يسعى الباحث إلى الإجابة على التساؤل التالى:

- كيف يتعامل ضحايا الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى مع الجريمة عند وقوعها ؟ وما الإجراءات التى يتخذونها لمواجهتها ؟

الهدف الخامس : استعراض المقترحات التى قد تساهم فى حماية الأفراد من الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، وذلك من وجهة نظر الضحايا أنفسهم.

ولتحقيق هذا الهدف ، يسعى الباحث إلى الإجابة على التساؤل التالى:

- ما ابرز المقترحات والتوصيات التى يراها الضحايا ضرورية لحماية الأفراد من الجرائم الإلكترونية المدعومة بالذكاء الاصطناعى ؟

خامساً: مفهومات البحث:

١- مفهوم الذكاء الاصطناعى Arificial Intelligence

يُعد (جون مكارثى) أول من صاغ مصطلح الذكاء الاصطناعى ، وعقد أول مؤتمر للذكاء الاصطناعى سنة ١٩٥٦م ، ومنذ ذلك وإلى غاية ١٩٦٩م زاد حجم الاختراعات بشكل كبير ، فتم تطوير أول روبوت يدعى (Shakey) يقوم بأعمال متنوعة بناءاً على أوامر محددة فى قائمة المهام ، وفى عام ١٩٩٧م تم تصميم الكمبيوتر العملاق ديب بلو (Deep Blue) من شركة "Ibm" والذى تمكن من هزيمة بطل الشطرنج (غازى كاسباروف) ، ولم تتوقف الاختراعات إلى هذا الحد بل فى ٢٠٠٢م تم إنشاء أول مكنسة كهربائية روبوتية ناجحة تجارياً(Ekanem, 2019, p. 35)

وان الذكاء الاصطناعي هو مجال واسع من علوم الكمبيوتر يركز على إنشاء أنظمة قادرة على أداء المهام التي تتطلب عادةً ذكاءً بشريًا، وتتضمن هذه المهام فهم اللغة الطبيعية ، والتعرف على الأنماط ، وحل المشكلات ، واتخاذ القرارات ، ويمكن تصميم أنظمة الذكاء الاصطناعي للتعلم من البيانات وتحسين أدائها بمرور الوقت دون أن تتم برمجتها بشكل صريح لكل مهمة، كما تستخدم Machine learning ، وهي مجموعة فرعية من الذكاء الاصطناعي ، الخوارزميات والتقنيات الإحصائية لتمكين أجهزة الكمبيوتر من التعلم من البيانات وإجراء تنبؤات أو اتخاذ قرارات (Zandi,Yaacobm2024,p.164).

كما يمكن فهمه على أنه ذكاء غير طبيعى ،أو عقل بشرى مصطنع ، ويسمى أيضاً ذكاء الآلة أى قيام أجهزة الكمبيوتر بأعمال يقوم بها الأشخاص ولكن بشكل أفضل ؛ حيث تشمل أبحاث الذكاء الاصطناعى العديد من المجالات منها: التفكير والمعرفة والتخطيط والتعلم والإدراك والتنبؤ والقدرة على تحريك الأشياء ومعالجتها وتخزين المعرفة وتطبيقها لحل المشاكل واكتساب معرفة جديدة. (Rehnstrom, 2021, p.5).

ويمكن أيضاً تعريفه بأنه القدرة على التفكير والتصرف بطريقة ذكية ، وهنالك قياسات للذكاء الاصطناعى وذلك من خلال مجموعة مختلفة من المقاييس مثل قدرته على حل مشكلات التعلم من خلال التجربة والقدرة على برمجة وتكييف المواقف الجديدة.(التميمى،٢٠٢٤،ص١١٤)

ويمكن تعريفه ايضاً بأنه يشمل كل الآلات المخترعة بطريقة تحاكى ذكاء الإنسان فى إنجاز العديد من المهام لاسيما التى تعمل دون مساعدة يدوية أو جهاز تحكم بالسرعة والدقة المطلوبة والتى عادة ما تكون أضعاف قدرة البشر.(ertel,2018,p.1)

كما يمكن تعريف الذكاء الاصطناعى بأنه فرع من فروع الحاسوب يهتم بدراسة وصناعة أنظمة حاسوبية يمكنها إنجاز أعمال تتطلب ذكاءً بشرياً ، حيث تمتاز هذه الأنظمة بأنها تتعلم مفاهيم ومهام جديدة ، ويمكنها أن تفكر وتستنتج استنتاجات مفيدة حول العالم الذى نعيش فيه ، فيعد مصطلح الذكاء الاصطناعى شكلاً من أشكال "الحوسبة الذكية" من حيث إنها تعتمد على برامج الكبيوتر التى يمكن أن تستشعر وتفكر وتتعلم ، وتتصرف وتتكيف مثل الانسان. (الدسوقى،٢٠٢٢،ص١١٥٣)

ويعرف ايضاً بأنه تقليد لسلوكيات الناس بطريقة ذكية ،بإستخدام الروبوتات ،أو الآلات مع نظام مدمج من التفكير ، بالطريقة المعرفية نفسها ، التى يقوم بها البشر ، وأداء مهام مثل حل المشكلات واتخاذ القرارات والتعرف على الكلام والترجمة وغيرها.(Nasrallah,2021,p.24)

ويمكن تعريف الذكاء الاصطناعى أيضاً بأنه محاولة محاكاة القدرات البشرية فى التفكير ، واتخاذ القرار ، وحل المشكلات ، وتنفيذ المهام المختلفة من خلال برمجة الحواسيب والآلات الذكية ، ويتم ذلك عبر إجراء دراسات متعمقة على سلوك الإنسان ، واستخلاص نتائج تُسهم فى فهم آليات تفكيره ، ثم تحويل هذه النتائج إلى خوارزميات ونظم برمجية تطبق على الآلات ، بحيث تتمكن من التفاعل مع مختلف جوانب الحياة اليومية كما يفعل البشر (الشاهد ،٢٠٢٤،ص ١٠٠٦)

كما يعرف كذلك بكونه مسمى يطلق على نوعية الذكاء الذى يمكن أن تكتسبه الآلة من خلال تزوديها بالبرمجيات التى تجعلها تبدو وكأنها تمتلك عقلاً يحاكى العقل البشرى بقدراته المختلفة ، وبالتالى فهو يجعل تلك الآلة تتصرف وكأنها مثل الإنسان العاقل أو المميز بإستخدام أبحاث الذكاء الاصطناعى.(عبدالسلام،٢٠٢٣،ص٥٣٩)

ويمثل الذكاء الاصطناعى أهم مخرجات الثورة الصناعية الرابعة لتعدد استخداماته فى المجالات العسكرية والصناعية والاقتصادية والتقنية والتطبيقات الطبية والتعليمية والخدمية ، ويتوقع له أن يفتح الباب لابتكارات لا حدود لها وأن يؤدى إلى مزيد من الثورات الصناعية بما يحدث تغييراً جذرياً فى حياة الإنسان،وسيكون محرك للتقدم والازدهار فى السنوات القادمة ، فكانت بداية الثورة الصناعية الرابعة فى مطلع القرن الحادى والعشرين معتمدة على الثورة الرقمية والإنترنت المتحرك ، وتطور أجهزة الاستشعار عن بعد ، والذكاء الاصطناعى والتكنولوجيا الحيوية ،والروبوتات الذكية،والتحول الآلى ، والتقنيات الرقمية والأنظمة الذكية(عبدالرازق،٢٠٢١،ص٤٣١)

ومما تقدم يجد الباحث أن الذكاء الاصطناعى هو: محاكاة الانسان عبر أنظمة التقنية ، وتتم من خلال دراسة معرفة أنماط عمل الإنسان من خلال القيام بتجارب على أعمال البشر ودراسة أفعالهم وطريقة تفكيرهم وتصرفاتهم مع هذه المواقف ، من خلال جمع البيانات وتحليلها واتخاذ القرارات بناء على عملية تحليلية بصورة تحاكى طريقة تفكير البشر.(العميريين،٢٠٢٢،ص ٤٥٦)

التعريف الإجرائى للذكاء الاصطناعى: هو توظيف الأنظمة والبرمجيات الذكية ، القائمة على تقنيات التعلم الآلى وتحليل البيانات ، فى تخطيط وتنفيذ الجرائم الإلكترونية التى تستهدف الأفراد ، وذلك من خلال التلاعب بالمعلومات ، وانتحال الهوية ، والاحتيال المالى ، والاختراق غير المشروع للبيانات الشخصية ، بما يسهل عمليات الابتزاز ، والتشهير ، وسرقة الهوية ، دون الحاجة إلى تدخل بشرى مباشر ، مما يزيد من تعقيد كشف الجناة وملاحقتهم قانونياً.

٢- مفهوم الجريمة Crime

لقد اختلف الباحثين فى تعريف الجريمة ، فجاءت متنوعة فهناك من يتناول التعريف من الناحية التقنية ومنهم من يتناوله من الناحية القانونية ، وبينما تناوله اهل الفقه من جانب آخر، إلا أننا اخترنا أن ندرج تعريف لعلماء الاجتماع ، فعلماء الاجتماع يتفقون على أن الجريمة هى ظاهرة اجتماعية لا يخلو منها أى مجتمع إنسانى ، رغم أنها تتناقض مع الحاجات الأساسية والمصالح الرئيسية للمجتمع وتمثل خطراً عليه .(ذياب،بوترعه،٢٠٢٠،ص ٨)

ويعتبر علماء الاجتماع الجريمة ظاهرة اجتماعية ،وأن التجريم ليس حكراً على المشرع ، بقدر ماهو مستمد من الواقع الاجتماعى بما يحويه من قيم ومعايير اجتماعية ، أى أن الجريمة عبارة عن خروج عن معايير المجتمع أو عن قواعد الإجماع ، أى القواعد التى يحددها المجتمع وتحكم سلوك أفراده ، أو هى تلك الأفعال التى تمل خطراً على المجتمع وتجعل من المستحيل تحقيق التعايش والتعاون بين الأفراد الذين يؤلفون المجتمع ، أو هى كل مخالفة لمشاعر الولاء الاجتماعى ، وهذا ما ذهب إليه دور كايم وميرتون عندما اعتبرا الجريمة سلوكاً لا معيارياً أى منحرفاً عن المستوى المعيارى فى المجتمع. (طالة،٢٠٢٠، ص ص ٦٦-٦٧)

وتعرف ايضاً بأنها كل سلوك إنسانى معاقب عليه خرقاً لقيم المجتمع أو مصالح أفراده الأساسية متى كان هذا السلوك كاشفاً عن نفسية منحرفة أو عن تكوين إجرامى. (رقية،يسرى،٢٠٢١،ص٩)

كما تتضمن نشاطاً أجرامياً معقداً على نطاق واسع ، تنفذه مجموعات من الأشخاص على درجة من التنظيم وتهدف إلى تحقيق ثراء للمشتركين فيها على حساب المجتمع وأفراده ، وهى غالباً ما تتم عن طريق الإهمال التام للقانون ، وتتضمن جرائم تهدد الأشخاص وتكون مرتبطة فى بعض الأحيان بالفساد السياسى.(الفراوى،٢٠١٦،ص٨)

كما يمكن تعريف الجريمة من وجة النظر القانونية بأنها اعتداء أو عدوان على القانون ولذلك تستحق المحاسبة والمجازاة.(فاطيمة،٢٠٢٣،ص٥٦)

ووفقاً لمعناها القانونى أيضاً تعرف الجريمة بأنها كل فعل غير مشروع صادر عن إرادة جنائية ويقرر له عقوبة أو تدابير امن من التدابير الأمنية ، كما أنها كل فعل أو امتناع يمكن إسناده لمرتكبه ويقر له عقوبة جنائية.(مراد ،٢٠١٥،ص ٢٢٦)

المفهوم الإجرائى للجريمة:هى أى فعل أو امتناع عن فعل يعاقب عليه القانون ، ويؤدى إلى إلحاق ضرر بالفرد ، متجاوزاً بذلك الحدود القانونية والأخلاقية المعترف بها ، ويترتب عليه مسئولية قانونية تستوجب العقاب وفقاً للتشريعات العمول بها .

٣-مفهوم الجريمة الالكترونية Cybercrime

تعرف الجرائم الالكترونية بأنها تلك الجرائم الناتجة عن استخدام المعلوماتية والتقنية الحديثة المتمثلة بالكمبيوتر والانترنت فى أعمال وأنشطة إجرامية بهدف أن تحقق عوائد مالية ضخمة عبر شبكة الانترنت أو تداول الأسهم وممارسة الأنشطة التجارية عبر هذه الشبكة التى تحمل ارقاماً سرية بالشراء.(الهديف،٢٠٢٢،ص ١٤٣)

وقد عرفها البعض بأنها نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلى والتى تحول طريقه ، ويندرج هذا النوع تحت جرائم المعالجة الآلية للبيانات ، بالنظر إلى موضوع الجريمة ونمطها فهى لا تقع على ماديات ، وإنما على برامج الكمبيوتر وما يحتويه من معلومات.(الدسوقى،٢٠٢٢،ص ١١٥٥)

فالجريمة الإلكترونية هى جريمة تقع على الأفراد أو المؤسسات الذين يستخدمون جهاز الحاسب الآلى أو الهواتف الذكية ،لذا تعتبر فعل لا أخلاقى وغير مصرح به ويرفضه المجتمع والقانون ويعاقب عليه ويدينه الشرع ، وبالنظر لتوسع أدوات الاتصال الحديثة بالإضافة إلى مجموعة البرامج والتقنيات المعدة سهلت عملية الجريمة الإلكترونية.(ذياب، وبوترعه،٢٠٢٠، ص١١)

أما أنصار الاتجاه القانونى فيذهبون إلى تعريف الجرائم الإلكترونية يتطلب تعريف المفردات الضرورية المتعلقة بإرتكاب جرائم الحاسب الآلى وهى برنامج الحاسب الآلى، البيانات، الممتلكات، الدخول والخدمات الحيوية.(بن عبدالله،بن حمو ،٢٠٢٢،ص٦٦٤)

كما يمكن تعريفها بأنها سلوك غير قانونى من خلال استخدام الأجهزة الالكترونية، ينتج منه حصول المجرم على فوائد مادية أو معنوية مع تحميل الضحية خسارة مقابلة ، وغالباً ما يكون هدف هذه الجرائم هو القرصنة من أجل سرقة أو إتلاف المعلومات الموجودة فى الأجهزة ومن ثم ابتزاز الضحايا بإستخدام تلك المعلومات المسروقة .(الداغر،٢٠٢٤،ص٥٠)

وتكمن الطبيعة الخاصة لهذه الجرائم فى قدرة شبكة المعلومات على نقل وتبادل معلومات ذات طابع شخصى وعام فى آن واحد ، مما يؤدى إلى ارتكاب الفعل ، والسبب فى ذلك توسع بنوك المعلومات

بأنواعها ، علاوة على رغبة الأفراد وسعيهم إلى ربط حواسيبهم بالشبكة ، على أساس أن هذه الجرائم ترتكب ضمن نطاق المعالجة الإلكترونية للبيانات ، سواء أكان فى تجميعها أو تجهيزها أم فى إدخالها إلى الحاسب المرتبط بشبكة المعلومات ، ولغرض الحصول على معلومات معينة ، كما قد ترتكب هذه الجرائم فى مجال معالجة النصوص ، وصعوبة التكييف القانونى لهذه الجرائم تكمن فى طبيعتها الخاصة ، بحيث أن القواعد التقليدية لم تكن مخصصة لهذه الظواهر الإجرامية المستحدثة ، وبالتالى تطبيقها على هذا النوع من الجرائم يثير مشاكل عديدة فى مقدمتها مسألة الإثبات ، ومتابعة مرتكبيها ، وعلى ضوء الاعتبارات السابقة يمكن القول بأن هذه الجرائم تتمتع بطبيعة قانونية خاصة. (عادل ، وبشرى ،٢٠١٨، ص١٤)

وتتشابه الجريمة الالكترونية مع الجريمة التقليدية فى أطراف الجريمة وتختلف عنها فى أداة ومكان الجريمة ، حيث أن الأداة فى الجريمة الالكترونية عالية التقنية ،والمجرم فيها لا يحتاج إلى التنقل الحركى لمكان وقوع الجريمة ، بل يقوم بالفعل الإجرامى عن بعد باستخدام خطوط وشبكات الاتصال ، وبالتالى فإن خطر هذه الجريمة أضحى يطال أمن الأفراد والأموال والبلاد، وقد تعددت تعريفات الجريمة الالكترونية وفق زاوية كل اختصاص نذكر منها. (رقية،يسرى،٢٠٢١،ص ص ١٠-١١)

- **تعريف يقوم على أساس موضوع الجريمة:**هنا تعرف الجريمة الالكترونية على أنها نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التى تحول عن طريقه .
- **تعريف يقوم على وسيلة ارتكاب الجريمة:**تتحقق الجريمة الالكترونية باستخدام الكمبيوتر كأداة رئيسية لارتكابها،وأشار "تايديمان" إلى أنها "كل أشكال السلوك غير المشروع الذى يرتكب باستخدام الحاسوب" ، وعرفتها منظمة التعاون الاقتصادى والتنمية بأنها "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية".
- **تعريف على أساس صفات شخصية لمرتكب الفعل:**وصفت وزارة العدل الأمريكية تعريفاً للجريمة الالكترونية بأنها"أى جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها"، وعرفها David Thomson بأنها أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسوب
- **تعريف على أساس محل الجريمة:**فى هذا المفهوم يعد جهاز الكمبيوتر الضحية والوسيلة حيث عرف Smedighoff الجريمة الالكترونية بأنها"أى ضرب من النشاط الموجه ضد أو المنطوى على استخدام نظام الحاسوب" ، ويعرفها كلا من Robert J.Lidquist و Bolonga Jack على أنها" الجريمة

التى يستخدم فيها الحاسوب كوسيلة لارتكابها أو يمثل إغراء بذلك أو جريمة يكون الكمبيوتر نفسه ضحية"

وبذلك اصبحت الجرائم الالكترونية مصطلحاً واسعاً يشمل جميع الجرائم التى تستهدف أجهزة الكمبيوتر وشبكات تكنولوجيا الكمبيوتر ، والتى افضت الى مشكلات كبيرة ساعدها فى ذلك ان الفضاء السيبرانى وفر عدد لا يحصى من فرص الأنشطة غير القانونية ، والفرص الإجرامية التى لا تقيدها قيود الزمان والمكان ، بل ان الجرائم التقليدية عملت على الاستفادة من الخصائص الفريدة للفضاء الالكترونى، ولذا ظهرت جرائم الكترونية جديدة مثل القرصنة وهجمات البرامج الضارة ، والتجسس الصناعى فعن طريق الفضاء السيبرانى يمكن من خلاله الحصول على الأسرار التجارية بشكل غير قانونى من الشركات لصالح شركات أخرى ، لا سيما تكنولوجيا الطاقة ، وتكنولوجيا المعلومات والاتصالات ، التكنولوجيا الحيوية ، وتكنولوجيا الدفاع، وغيرها الكثير وهذا يؤدى الى احداث فوضى على المستوى الوطنى لأية دولة. (الشمرى،٢٠٢١،ص ص ١٢١-١٢٢)

التعريف الإجرائى للجريمة الإلكترونية: هى أى سلوك إجرامى يرتكب ضد الأفراد باستخدام تقنيات الذكاء الاصطناعى ، بهدف الإضرار بهم نفسياً ومادياً واجتماعياً ، وذلك من خلال وسائل مثل الاحتيال ، الابتزاز ، التشهير ، انتهاك الخصوصية ، التزييف العميق Deepfake ،أو اختراق الحسابات والبيانات الشخصية ، مما يؤدى إلى تهديد أمنهم الرقمى واستغلالهم بطرق غير مشروعة.

خصائص الجريمة الإلكترونية:

تتميز الجريمة الإلكترونية بعدة خصائص لعل من أبرزها مايلى: (عبدالرازق،٢٠٢١،ص ص ٤٣١-٤٣٢)

- تعد الجرائم الإلكترونية أقل عنفاً من الجرائم التقليدية أى أنها لا تحتاج إلى أدنى مجهود عضلى، بل تعتمد على القدرة الذهنية والتفكير العلمى المدروس المستند إلى معرفة بتقنيات الحاسب الآلى .
- يختلف الباعث على ارتكاب الجرائم الإلكترونية عنه بالنسبة إلى الجرائم التقليدية ،ففى الجرائم الأخيرة يتمثل الباعث بالرغبة فى مخالفة النظام العام والخروج عن القوانين أكثر من استهداف الحصول على الربح ، فى حين نجد أن الباعث لدى مرتكبى الجرائم الإلكترونية هو الحصول على النفع المادى السريع ،فإن المبالغ التى يمكن تحقيقها من وراء ذلك تكون طائلة.
- يرتكب الكثير من الجرائم الإلكترونية ، ولكن نادراً ما تقع جريمة معلوماتية ويقوم المجنى عليه بالإبلاغ عنها ؛وذلك بسبب عدم اكتشافه للجريمة ،أو لأنه اكتشفها ولكنه يخاف من الإساءة لسمعته وفقدان الثقة فى التعامل معه، لذلك لا يتم فى الغالب الإبلاغ عن جرائم الإنترنت إما لعدم اكتشاف

الضحية لها وإما خشيه من التشهير ، لذا نجد ان معظم الجرائم تم اكتشافها بالمصادفة ، بل وبعد وقت طويل من ارتكابها.

- يصعب فى كثير من الأحيان العثور على أثر مادى للجريمة الإلكترونية، والسبب فى ذلك يعود إلى استخدام الجانى وسائل فنية وتقنية معقدة فى كثير من الأحيان ، كما يتمثل السلوك المكون للركن المادى فيها بعمل سريع قد لا يستغرق أكثر من بضع ثوان ، فمن السهل إخفاء معالم الجريمة وصعوبة تتبع مرتكبيها، وسهولة محو الدليل المادى التقليدى؛ لذا فهذه الجرائم لا تترك أثراً لها بعد ارتكابها.
- تعتمد الجرائم الإلكترونية على قمة الذكاء فى ارتكابها ؛ ويصعب على المحقق التقليدى التعامل مع هذه الجرائم ،إذ يصعب عليه متابعة جرائم الإنترنت والكشف عنها وإقامة الدليل عليها ، فهى جرائم تتسم بالغموض ؛وإثباتها والتحقيق فيها يختلف عن التحقيق فى الجرائم التقليدية، والوصول للحقيقة بشأنها يستوجب الاستعانة بخبرة فنية عالية المستوى.
- يؤدى عولمة الجرائم الإلكترونية إلى تشتيت جهود التحرى والتنسيق الدولى لتعقب مثل هذه الجرائم، فتعتبر هذه الجرائم هى صورة صادقة من صور العولمة ، فمن حيث المكان يمكن ارتكاب هذه الجرائم عن بعد ،وقد يتعدد هذا المكان بين أكثر من دولة .

أهداف الجريمة الإلكترونية:

تتعدد أهداف الجريمة الإلكترونية وتشمل الأتى: (عبد الحكيم،٢٠٢٢،ص١٠)

- الوصول الى المعلومات بشكل غير قانونى ، كسرقة المعلومات او الاطلاع عليها او حذفها او تعديلها بما يحقق هدف المجرم.
- الوصول الى الأجهزة الخادمة الموفرة للمعلومات وتعطيلها او تخريبها وعادة ماتتم هذه العملية على مواقع الانترنت.
- الحصول على معلومات تغيير عناوين مواقع الانترنت بهدف التخريب على المؤسسات العامة وابتزازها.
- الوصول الى الأشخاص او الجهات المستخدمة للتكنولوجيا ، بغرض التهديد او الابتزاز كالبنوك والدوائر الحكومية والأجهزة الرسمية والشركات بكافة اشكالها.
- الاستفادة من تقنية المعلومات من اجل كسب مادى او معنوى او سياسى غير مشروع كعمليات تزوير بطاقات الائتمان وعمليات اختراق المواقع الالكترونية على الشبكة العنكبوتية.

- استخدام التكنولوجيا فى دعم الإرهاب والأفكار المتطرفة او نشر الأفكار التى يمكن ان تؤسس الى فكر تكفيرى.

أركان الجريمة الإلكترونية:

بما أن الجريمة الالكترونية فعل إجرامى يعاقب عنه القانون فهى تقوم على نفس أركان الجريمة العادية والمتمثلة فى الركن الشرعى والمادى والمعنوى: (طالة،٢٠٢٠، ص ٦٩)

- **الركن الشرعى:** معناه اعتراف المشرع والنص على تجريم الفعل المرتكب "لا جريمة ولا عقوبة إلا بنص"
- **الركن المادى:** يتكون الركن المادى للجريمة الالكترونية من السلوك الإجرامى والنتيجة والعلاقة السببية ، علماً أنه يمكن تحقق الركن المادى دون تحقق النتيجة ، كالتبليغ عن الجريمة قبل تحقيق نتيجتها مثلاً: إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة إلا أنه لا مناص من معاقبة الفاعل ، ويتخذ الركن المادى فى هذه الجريمة عدة صور بحسب كل فعل إيجابى مرتكب مثلاً: جريمة الغش المعلوماتى" الركن المادى فيها هو تغيير الحقيقة فى التسجيلات الالكترونية أو المحررات الإلكترونية.
- **الركن المعنوى:** يتكون الركن المعنوى للجريمة الإلكترونية من عنصريها أى العلم ،أى إدراك الفاعل للأمور والإدارة ، بمعنى اتجاه السلوك الإجرامى لتحقيق النتيجة.

٤-مفهوم الضحية Victim

إن للضحية أهمية كبيرة بإعتبارها ركناً أساسياً من أركان الجريمة ، ولكنها لم تحظى بالاهتمام العلمى من قبل علماء الجريمة والاجتماع والقانون وعلم النفس إلا حديثاً ، حيث ركزة الاهتمامات العلمية سابقاً على المجرم والجريمة باعتبارها ظواهر اجتماعية تهدد الفرد والمجتمع ، وأهملة الضحية او المجنى عليه ، فى حين لم يكن هناك اهتمام كبير بالضحية من حيث الدراسات التى نالها المجرم فى دراسة الفعل الإجرامى او دراسة الجريمة ، فى حد ذاتها كنتيجة لهذا الفعل الإجرامى ،إلا انه لا يمكن أن يكون هناك جريمة دون ضحية فالجريمة فى اى زمان ومكان مهما اختلفت المجتمعات الإنسانية لها أركان ثلاثة المجرم والجريمة والضحية ، فطالما وجدت جريمة فلا بد من وجود ضحية ،إلا ان الاهتمام بها يعد وليداً ، فلم تبدأ الدراسات العلمية لعلم الضحايا إلا بعد الحرب العالمية الثانية ، ورغم ذلك لم يأخذ

علم الضحية مساره فى التطور والتقدم فى كل منطقة من مناطق العالم ،إذ بينما نراه متقدم فى بعض الدول ويكون متجاهلاً فى دول أخرى ، ولرغم وجود تشابه فى الوسائل المنهجية (الكيفية والكمية) المستخدمة فى دراسة ضحايا الجريمة ، ورغم مرور حوالى قرن من الزمان ، مازال هناك خلاف قائم حول مفهوم علم الضحايا ومدى نطاقه وذلك لصعوبة حصر أسباب التضرر الذى يتعرض له الإنسان فى هذا العصر ، سواء أكانت تلك الأسباب مرجعها الإنسان او الطبيعة ، ولكن الحقيقة التى لا خلاف حولها ، ان الإنسان يتعرض لمخاطر وأضرار عديدة تهدد أمنه وسلامته .(مراد،٢٠١٥،ص ٢٢٦)

ويمكن تعريف الضحية ايضاً بالشخص الذى قد أصيب بضرر فردى أو جماعى وقد يكون الضرر بدنى أو عقلى أو تعرض لمعاناة نفسية أو خسارة اقتصادية أو عدم التمتع بحق من حقوقه عن طريق فعل أو إهمال شكل انتهاك للقوانين الجنائية .(الأميرى ،٢٠٢٢، ص ٣٠٣)

ويعرف كوهين وفيلسون الضحية بأنها هى الهدف المناسب والذى قد يكون شخصاً أو شيئاً ما ، كما يمكن تعريف الضحايا بأنهم الأفراد الذين يعانون من الإصابات أو الخسائر أو المصاعب لأى سبب من الأسباب ، يمكن أن يصبح الناس ضحايا للحوادث والكوارث الطبيعية والأمراض أو المشاكل الاجتماعية ويتضرر ضحايا الجرمية بفعل غير قانونى.(ابراهيم ،٢٠٢٣،ص ١٥٢)

والضحية فى مواقع التواصل الاجتماعى تختلف عن الضحية فى الشارع ، فالضحية فى هذه المواقع تلعب دور أيضاً فى الجريمة ، فهى ليست مفعول بها عشوائى ، بل كانت شخص معيناً تفاعل مع المجرم قبل تنفيذ الجريمة ، وسهلت عليه تنفيذها أيضاً فى بعض الحالات ، كما أنها يمكن أن تكون مقيمة خارج الحدود الإقليمية للمجرم ، وهذا ما يصعب إيجاده فى اغلب الحالات ومتابعته ، فينجو من المتابعة الجزائية.(حطاب،٢٠١٧،ص ٤١٤)

التعريف الإجرائى للضحية: يقصد بهم الأشخاص الذين تعرضوا لاعتداءات إلكترونية تم تنفيذها باستخدام تقنيات الذكاء الاصطناعى ، مثل التزييف العميق ، الاحتيال الإلكترونى ، الاختراقات المتقدمة ، والتلاعب بالمعلومات والبيانات الشخصية، وتشمل هذه الفئة الأفراد الذين عانوا من خسائر مالية ، انتهاكات خصوصية ، ابتزاز ، تشهير ، وأضرار نفسية واجتماعية واقتصادية ، نتيجة لهذه الجرائم.

سادساً:التوجه النظرى للبحث:

يعتمد البحث على مجموعة من النظريات العلمية التى تسهم فى تفسير تأثير الذكاء الاصطناعى على أنماط ارتكاب الجرائم الإلكترونية ، وذلك بهدف تقديم رؤية شاملة ومتكاملة لهذه الظاهرة ، ومن أبرز هذه النظريات: **نظرية النشاط الروتينى:** تفسر كيفية استغلال المجرمين للذكاء الاصطناعى فى تحديد الفرص الإجرامية ، حيث يسهم فى تحليل البيانات ورصد الأهداف المحتملة ، مما يسهل تنفيذ الجرائم فى البيئات الرقمية ، خاصة فى ظل غياب حارس رادع ، **نظرية الاستخدامات والإشباعات:** توضح كيف يستخدم الأفراد التقنيات المدعومة بالذكاء الاصطناعى لتحقيق أهدافهم ، سواء كانت مشروعة أو غير مشروعة ، مما يسهم فى ظهور أنماط جديدة من الجرائم الإلكترونية ، **نظرية التفاعلية الرمزية:** تركز على دور الذكاء الاصطناعى فى تشكيل التفاعل داخل الفضاء الرقمى ، حيث تتيح تقنيات مثل التزييف العميق (Deepfake) وتقنيات المحادثة الذكية فرصاً لتعزيز السلوكيات الإجرامية وبناء هويات رقمية مزيفة تُستخدم فى تنفيذ الجرائم الإلكترونية ، وسيتم تناول هذه النظريات وشرح أبعادها وتحليل تأثير استخدام الذكاء الصناعى على ارتكاب الجرائم الإلكترونية وذلك على النحو التالى:

١-نظرية النشاط الروتينى:

تم تصور نظرية النشاط الروتينى بوصفها طريقة لإيضاح أسباب ارتفاع معدلات الجريمة بعد الحرب العالمية الثانية، كانت المتغيرات الاجتماعية مثل الدخل والبطالة التى تستعملها النظريات الأخرى لشرح معدلات الجريمة المرتفعة تتحسن بالفعل بينما ارتفع معدل الجريمة اقترحا كوهين وفيلسون أن ارتفاع الجريمة لم يكن نتيجة الاختلافات فى سلوك الجانى ، بل أتى فى سلوك الضحية ، وقد تمكن كوهين وفيلسون ولخصوا هذا الاقتراح لمفهوم بسيط "إن الجريمة لكى تحدث يجب أن تتوافر ثلاثة عوامل أساسية آلا وهى : مجرم وضحية وغياب الرقابة فى وقت وزمان محددين حين ذلك من المرجح وقوع الجريمة ومن هذا المنطلق ولدت نظرية الأنشطة الروتينية" ، ولقد قام كوهين وفيلسون(١٩٧٩) باختبار النظرية مستعملين المقاييس لتحديد ما إذا كانت التغيرات قد حدثت بالفعل فى سلوك الضحية ، ومعرفة هذه التغيرات. (الأميرى،العموش،٢٠٢٢،ص ٣٠٣)

فمنذ نشأة نظرية الأنشطة الروتينية ، استعملت لدراسة الجرائم التى تحدث عندما يلتقى المستهدفون والمجرمون فى مكان مادى ، ومع ذلك ، منذ ظهور الإنترنت وانتشارها السريع فى أواخر التسعينيات ،أصبحت الجريمة التى لا يتلامس فيها الضحايا والجناة جسدياً أكثر قابلية للتطبيق. (Janus,Davis,2005,p.12)

وتم استخدام نظرية الأنشطة الروتينية كأطار نظري لشرح خصائص مرتكبي الجرائم المحددة ونقاط الضعف المستهدفة للجرائم الإلكترونية، وتفسر النظرية أن مرتكبي الجرائم المتحمسين في العشرينات من العمر من المرجح أن يرتكبوا جرائم في العالم الافتراضي، تشمل دوافع الجرائم الإلكترونية الشخصية لتحقيق مكاسب مالية أو إشباع جنسي، وأن الجرائم الإلكترونية في العالم الافتراضي تستهدف فئة الشباب. (Parti, Dearden,2023,p.2)

ويمكن تفسير زيادة ضحايا الجريمة الإلكترونية من خلال التغييرات فى أنشطة الناس الروتينية فى الحياة اليومية ، فمع ظهور شبكة الإنترنت فقد تغيرت طريقة الناس التى يتواصلون فيها أو يتفاعلون مع الآخرين فى العلاقات الشخصية والترفيه والتجارة ، ذلك أن التغييرات فى أنشطة الناس الروتينية مثل استخدام الانترنت وشبكات التفاعل الاجتماعى مثل الفيسبوك والايميل والمواقع وغيرها قد خلقت فرصاً للجناة المتحفزين مع وجود أهداف قيمة وسهلة فى الحيز الفضائى مع غياب الحراسة.(طاله،٢٠٢٠، ص٧٧)

كما يكمن الاختبار الأساسى لمعرفة ما إذا كان للتغييرات فى الأنشطة الروتينية تأثير فى اتجاهات الجريمة بالطريقة التى توقعها كوهين وفيلسون(١٩٧٩) فى المعدلات التفاضلية للتغيير ضمن فئات الجريمة ، على سبيل المثال ، نظراً لأن الناس يخرجون من منازلهم الآمنة فى كثير من الأحيان ، ينبغى توقع زيادة معدل الإيذاء على أيدى الغرباء ، وليس الأشخاص المعروفين للضحية وبالمثل ، يجب أن تزيد معدلات السطو أثناء النهار بمعدل أعلى من معدل السطو الليلى نظراً للتغير فى عدد المنازل غير المأهولة أثناء النهار ، فى الواقع هذا هو بالضبط ما لحظه كوهين وفيلسون ، يبدو أن تغييرات نمط الحياة التى قللت من الوصاية القادرة وزيادة ملاءمة الهدف أدت إلى تغيير حقيقى للغاية فى اتجاهات الجريمة. (الأميرى،العموش،٢٠٢٢،ص٣٠٤)

كما أن التغير الاجتماعى الذى يحدث فى المجتمعات المعاصرة ومنها المجتمعات العربية ، انبثق عنه نمط حياة جديد يتميز بالروتينية التى يتبعها الفرد فى حياته اليومية بشكل روتينى دون أن يحسب لنتائج ذلك النمط الجديد ، على أبناءه وأسرته ككل وعلى النواحى الإجرامية ، حيث أدى ذلك النمط إلى تمركز حياة الفرد اليومية خارج المنزل وأدى إلى كثرة غياب الآباء عن الأسرة والاهتمام بالكسب المادى أو اللهث وراء الماديات وربما دفع ذلك ببعض هؤلاء الآباء إلى نمط جديد من أنماط المعاملة يتمثل فى عدم الاهتمام بالابن وعدم مراقبته أو متابعته ، وهذا يعد من أهم عوامل إضعاف أو خفض مستوى ضبط الذات الذى قد يؤدى إليه انشغال الآباء عن الاهتمام بالأشراف على الأبناء ومراقبة سلوكياتهم ما يجعلهم عرضة للإهمال النفسى والعاطفى والتربوى فيصبحون فى ظل ضعف دور المدرسة

وتقصير الدعاة والمصلحين الاجتماعيين غير محصنين ضد الأفكار الإجرامية ما يجعل منهم أهدافاً مناسبة لإرتكاب الجرائم الإلكترونية. (الدوسرى،٢٠١٨،ص ٤٦٤)

فالتقنيات الحديثة تتيح فرص مستجدًة للجريمة من خلال إيجاد روابط جديدة بين الضحايا والجناة ،ووفقاً للفرضية التى تقدمها نظرية النشاط الروتينى ،فأنً مخاطر احتمال حدوث جريمة يزداد فى حالة الجرائم الإلكترونية ، حيث يمكن للجناة أن يصلوا إلى أعداد كبيرة من الأهداف من خلال الاستعمال المتزايد للخدمات الإلكترونية المباشرة من قبيل الخدمات المصرفية ، والتسوق ، وشبكات التواصل الاجتماعى ، والتشارك فى الملفات ، مما يجعل المستعملين عرضة "لهجمات التصيد الإلكترونى الاحتيالى" ، وخاصة أن التدابير الرقابية التى توجد بالفعل مثل البرمجيات الحاسوبية الأمنية ووجود مخاطر ضئيلة نسبياً للوقوع عرضة لإجراءات إنفاذ القانون ، يمكن أن تكون غير كافية لردع الجناة المدفوعين بإغراء تحقيق أرباح كبيرة.(الزبن،٢٠٢١،ص٢٨)

كما وجد الباحثون مع الاستخدام المتزايد للذكاء الاصطناعى ، بعض الدعم لتطبيق مبادئ نظرية النشاط الروتينى على الجرائم الالكترونية ، حيث وجد المجرمون فرصاً جديدة لتحقيق أهدافهم على منصة جديدة تماماً ، كما توصلت الأبحاث إلى أن مقدار الوقت الذى يقضيه الافراد على الانترنت ، وزيادة استخدام الخدمات المصرفية والمشتريات ، والسلوك المحفوف بالمخاطر الممارس عبر الانترنت ، ونقص برامج الحماية من الفيروسات وأمن الشبكات ، تجعلهم أهدافاً سهلة للمجرمين ، على سبيل المثال العالم Choi عام ٢٠٠٨م بتطبيق نظرية LRAT على الإيذاء الفردى من خلال الجرائم الالكترونية ، وخاصة جريمة القرصنة ، ووجد أن أحد المبادئ الثلاثة المتمثل فى غياب الوصاية ، هو المساهم الأكبر فى زيادة الجرائم الالكترونية، وذلك لأن سهولة الوصول إلى الإنترنت ، تجعل إمكانية وجود مجرمين متحمسين وأهداف مناسبة لا حدود لها ، حيث تقاس الوصاية من خلال مستويات مختلفة من تفعيل اجراءات الأمان عبر الانترنت ، مثل إعدادات الخصوصية على مواقع الشبكات الشخصية ، وتثبيت برامج الفيروسات وجدار الحماية، كما تم إجراء دراسة أخرى بواسطة كل من Reyns وFisher وHenson عام٢٠١١م وجدت نتائج مماثلة فى دراستهم "نظرية الأنشطة الروتينية لنمط الحياة السيبرانى والإيذاء للجرائم الإلكترونية"، والتى أهتمت بجريمة المطاردة عبر الانترنت ، وجد المؤلفون أن أهم مؤشر على وقوع ضحايا للمطاردة عبر الإنترنت هو التحدث بشكل متكرر إلى شخص ما بطريقة عنيفة ،أو التهديد بإيذائه جسدياً عبر الإنترنت ، ومحاولة اختراق مواقع التواصل الاجتماعى لشخص ،وإرسال صور جنسية إلى شخص ما من خلال الرسائل النصية عبر الإنترنت ، الأهم من ذلك ، تظهر النتائج دعماً لهذه النظرية ليتم تطبيقها على بيئات الإنترنت وأبحاث الجرائم الإلكترونية. (السيد،٢٠٢٣،ص ص ١٦٧-١٦٨).

تشير نظرية الأنشطة الروتينية إلى أن انخفاض آليات السيطرة على الفرد يزيد من احتمالية تعرضه للجرائم الإلكترونية ، حيث يؤثر أسلوب الحياة والأنشطة اليومية على إمكانية أن يصبح الشخص ضحية ، فمثلاً كلما قضى الأفراد وقتاً أطول فى المناطق الخطرة على الإنترنت زادت فرص استهدافهم من قبل المجرمين الإلكترونيين ، من هذا المنطلق فإن التفاعل المستمر داخل بيئة الإنترنت مثل التعرف على أفراد جدد ، تبادل الصور ومقاطع الفيديو ، ممارسة الألعاب الإلكترونية يجعل الإنترنت أكثر من مجرد وسيلة اتصال ، بل هو مساحة اجتماعية تتيح فرصاً متعددة للجرائم الإلكترونية ، فالشباب على وجه الخصوص يقضون فترات طويلة فى أنشطة رقمية متنوعة ، مما يزيد من احتمالية استغلالهم أو استدراجهم لارتكاب أعمال غير قانونية ، كما تنص النظرية على أن الحد من الجرائم الإلكترونية يتطلب تعديلات سلوكية مثل زيادة الإشراف الأبوى ، تعزيز الوعى الأمنى ، وتبنى سياسات أكثر صرامة لحماية المستخدمين ، مما قد يقلل من فرص استهداف الأفراد ويسهم فى تعزيز الأمن الرقمى .(ابراهيم، ٢٠٢٣،ص ١٥٥)

٢-نظرية الاستخدامات والإشباعات:

يعد مدخل الاستخدامات والإشباعات بمثابة نقلة فكرية فى مجال دراسة تأثير وسائل الاتصال ، حيث يعد النموذج البديل لنموذج التأثيرات التقليدى الذى يركز على كيفية تأثير وسائل الإعلام والاتصال على تغيير المعرفة والاتجاه والسلوك بينما يرتكز مدخل الاستخدامات والإشباعات على كيفية استجابة وسائل الاتصال لدوافع واحتياجات الجمهور ويتميز الجمهور فى ظل مدخل الاستخدامات والإشباعات بالنشاط والإيجابية والقدرة على الاختيار الواعى والتفكير ، وبذلك يتغير المفهوم التقليدى للتأثير والذى يعنى بما تفعله وسائل الإعلام بالجمهور ، إلى دراسة ماذا يفعل الجمهور بالوسيلة.(باسه ، راقية،٢٠٢٣، ص٣٢)

وقد اهتمت نظرية الاستخدامات والإشباعات بدراسة الاتصال الجماهيرى دراسة وظيفية منظمة فخلال عقد الاربعينات من القرن العشرين، أدى إدراك عواقب الفروق الفردية ، والتباين الاجتماعى على إدراك السلوك المرتبط بوسائل الإعلام إلى بداية منظور جديد للعلاقة بين الجماهير ووسائل الإعلام ، فكان ذلك تحولاً من رؤية الجماهير على أنها عنصر سلبى غير فعال ، إلى رؤيتها على أنها فعالة فى انتقاء أفرادها لرسائل ومضمون مفضل من وسائل الإعلام ويشير "ويرنر" و"تانكرد" إلى أن البحث فى أنواع الاحتياجات التى يحققها استخدام وسائل الإعلام قد بدأ منذ وقت مبكر فى الثلاثينيات ، حيث أجريت دراسات عديدة من هذا المنظور : على قراءة الكتب ، ومسلسلات الراديو ، والصحف اليومية ،

والموسيقى الشعبية ، وأفلام السينما وذلك للتعرف على أسباب استخدام الأفراد لوسائل الإعلام والنتائج التى تترتب على ذلك .(جنيفر ،٢٠٢٠،ص ص ٣-٤)

ويعتمد مدخل الاستخدامات والاشباعات على فكرة أن الأفراد يختلفون فى استخدام نفس المحتوى للرسالة وفقاً لأغراضهم ، فضلاً عن اختلاف تأثير وسائل الاتصال وفقاً لاستخدامات الجماهير ورغباتهم وتوقعاتها عن وسائل الاعلام (محمد ، الموسوى ،٢٠٢٢،ص٢٦)

كما تفترض هذه النظرية أن استخدام وسائل الاتصال يعبر عن الحاجات التى يدركها أعضاء الجمهور ، ويتحكم فى ذلك عوامل الفروق الفردية، وعوامل التفاعل الاجتماعى ، وتتنوع الحاجات بإختلاف الأفراد ، وأن الجمهور هو الذى يختار الرسائل والمضمون الذى يشبع حاجاته ، وتهدف الى السعى إلى اكتشاف كيف يستخدم الأفراد وسائل الاتصال ، وكذا شرح دوافع التعرض لوسيلة معينة من وسائل الاتصال ، والتفاعل الذى يحدث نتيجة هذا التعرض .(العزعزى ،٢٠١٥،ص ٩٨)

هذا وتنقسم الإشباعات إلى نوعين هما :

أولاً: إشباعات المحتوى: وتنتج عن التعرض لمحتوى وسائل الاتصال وينتج عنها نوعين من الإشباعات.

أ. **إشباعات توجيهية:** وتتضمن الحصول على المعلومات ، وتأكيد الذات وهى ترتبط بكثافة التعرض ، والاهتمام والاعتماد على وسائل الاتصال.

ب. **إشباعات اجتماعية:** ويقصد بها الربط بين المعلومات التى يحصل عليها الفرد بشكبة علاقاته الاجتماعية.

ثانياً: الإشباعات العملية: وتنتج عن عملية الاتصال والارتباط بوسيلة محددة ولا ترتبط مباشرة بخصائص الرسائل ، وتنقسم إلى نوعين.

أ. **إشباعات شبه توجيهية:** وتتحقق من خلال تخفيف الإحساس بالتوتر ، والدفاع عن الذات ، وتنعكس فى برامج التسلية والترفيه والإثارة.

ب. **إشباعات شبه اجتماعية:** وتتحقق من خلال التوحد مع شخصيات وسائل الإعلام ، وتزيد هذه الإشباعات مع ضعف علاقات الفرد الاجتماعية وزيادة إحساسه بالعزلة.

وتعتبر نظرية الاستخدامات والإشباعات من أنسب المداخل لدراسة عملية الاتصال عبر شبكة الإنترنت ، حيث أنه يساعد فى التعرف على اهتمام الأفراد باستخدام شبكة الإنترنت والإشباعات المتحققة من هذا الاستخدام.(الطوخى ،٢٠٠٢،ص ص ١٦٧-١٦٨)

وقد استعان البحث أيضاً بنظرية الاستخدامات والإشباعات فى النقاط الآتية:

١. **تصنيف دوافع مشاهدة مقاطع الفيديو:** قسم كل من "روبن" ، و"نيدهل" ، دوافع مشاهدة التليفزيون إلى نوعين هما : دوافع نفعية ، ودوافع طقوسية ، والمشاهدة النفعية يقصد بها مشاهدة التلفزيون لأشباب معرفية ويكون التعرض لمضمون محدد ، ويرتبط ذلك بإدراك الواقع ، ومستويات منخفضة من الألفة مع الوسيلة ، ومستويات أعلى للمشاهدة ، ودرجة من النشاط لأفراد الجمهور ، أما المشاهدة الطقوسية فيقصد بها مشاهدة التليفزيون كعادة ، أو لاستهلاك الوقت أو التسلية أو الاسترخاء ، وترتبط المشاهدة الطقوسية بمستويات أعلى للمشاهدة ، وبدرجة مرتفعة من الألفة مع الوسيلة(التلفزيون) ، ومستويات أقل من إدراك واقعية الأحداث.

٢. **مجالات التأثير الناتجة عن الاستخدام :** تحقق وسائل الإعلام ثلاثة تأثيرات هى :التأثير المعرفى والتأثير الوجدانى ، والتأثير السلوكى ، وتشمل الآثار المعرفية خمسة جوانب هى إزالة الغموض الناتج عن قلة المعلومات ، وتكوين اتجاهات لا سيما فى الأمور الخاصة بالمسائل والقضايا الجدلية والدعاية للرموز ، وترتيب أولويات الجمهور ، وأيضاً تعمل على اتساع المعتقدات وتنظيمها وتقسيمها إلى فئات تنتمى إلى الأسرة أو الدين أو السياسة ، كما توضح أهمية القيم المتفق عليها اجتماعياً ، وقد تخلق قيماً تطبع عليها المجتمع ، أما التأثيرات الوجدانية فتتعلق بالمشاعر والأحاسيس ، مثل زيادة الخوف والتوتر والحساسية للعنف ، وأيضاً التأثيرات المعنوية مثل الاغتراب عن المجتمع ، فى حين أن التأثيرات السلوكية هى نتاج التأثيرات المعرفية والوجدانية ، وتظهر فى النشاط وتعنى اتخاذ مواقف مؤيدة لقضية ما ، مثل حقوق المرأة ، وقد تظهر التأثيرات على شكل الخمول ، ويعنى ذلك تجنب القيام بعمل ما ، مثل عدم المشاركة السياسية.(ابراهيم ،عبد الجواد ،٢٠٢٤،ص ص ٣٥٨-٣٥٩)

وتأسيساً على ما سبق ، يمكن القول إن انتشار الوسائل التكنولوجية الحديثة المدعومة بتقنيات الذكاء الاصطناعى أتاح لمستخدميها حرية اختيار الوسيلة والأسلوب المناسب لارتكاب الجرائم الإلكترونية ، وفقاً لاحتياجاتهم ودوافعهم ، فالمجرمون الإلكترونيون يوظفون هذه التقنيات بطرق مختلفة ، حيث يستغلها البعض فى جرائم الابتزاز الإلكترونى ، بينما يتخصص آخرون فى سرقة بيانات البطاقات الائتمانية ، فى حين يلجأ بعضهم إلى إرسال البريد الدعائى المزعج والمضلل لتحقيق مكاسب غير مشروعة ، وتعكس هذه الأنماط الإجرامية تنوع الدوافع الفردية لمرتكبى الجرائم الإلكترونية المدعومة بالذكاء الاصطناعى ، حيث تستخدم هذه التقنيات لإشباع احتياجات إجرامية مختلفة وفقاً للفروق الفردية بينهم ، ومن ثم فإن انتشار ثقافة الذكاء الاصطناعى داخل المجتمع يسهم فى تشكيل

ملامح السلوك الإجرامى الرقمى ، حيث أصبحت الأدوات الذكية وسيلة رئيسية فى تنفيذ الجرائم الإلكترونية ، مما يزيد من تعقيد مكافحتها والحد من انتشارها.

٣- النظرية التفاعلية الرمزية:

تعتبر النظرية التفاعلية الرمزية من النظريات الاجتماعية التى يعتمد عليها فى تحليلها وتفسيرها وفهم النسق الاجتماعى بالأفراد من خلال المعانى والرموز ، وترى النظرية أن الخبرة الإنسانية فى متسع المعرفة والحضارة والمستقبل ، لذلك ترتبط بين المفاهيم والرموز فى فهم التفاعل والاتصال من خلال النظرية ، التى تشير فى أنهم ينظرون للأشياء من خلالها وما تحمله من معانى ، والمعانى والرموز نفسها من صنع الانسان ، ويعمل الانسان فيها ويحدها وفقاً لملتقى التحول ، وبذلك يتم فهم عمليات التفاعل عن الرموز التى هى وسائل التفاعل وارؤاها فى كل من حال التفاعل التى كانت بالعلاقات فى الحياة الاجتماعية بين الافراد والجماعات لذلك نجد أن النظرية اعتمدت على الآتى:

- أن الظواهر الاجتماعية الخارجية لا تحمل معانى داخلية خاصة بها ولم يمكن وجودها فى المعانى التى يضفها الافراد عليها .
- تلعب الرموز دوراً فى إضافة معانى معينة على الموضوعات الخارجية. (الهديف، ٢٠٢٢،ص ١٤٥)

وفى إطار ما تقدمه التفاعلية الرمزية من فهم الجريمة الإلكترونية ، يمكن التأكيد على أن الصورة الذهنية لدى الجناة نحو المجنى عليهم تدفعهم لتبنى أدواراً مغايرة ، والتى تمثل نوعاً من الإلحاح كالاحتياجات المادية ، والتى تتمثل فى الجوائز المالية أو العينية ، تلك التأويلات أو التفسيرات التى تمكن الشخص المحتال من استخدام الصورة الذهنية للحاجة بالاعتماد على الحاسوب من أجل إحداث نوع من التفاعل السلبى الإجرامى ، الذى يمكن الجانى من دفع المجنى عليه إلى الاستجابة للصور الذهنية المخادعة ، والتى تؤدى حالة الاستجابة لها إلى وقوع الجريمة الإلكترونية ، ومن ثم فإنه وبالتمكن من تصحيح الصورة الذهنية عن الفعل الإجرامى أمام المجنى عليهم يمكنهم من تجنب التعرض للجريمة الإلكترونية.(رجب،٢٠٢٣،ص ٣٠٧)

وقد صاغ "ميد" الفرضيات الأساسية للتفاعلية الرمزية على النحو الآتى:

أ. يحدث التفاعل الاجتماعى بين الأفراد الذين يشغلون أدواراً اجتماعية معينة ويأخذ زمناً يتراوح بين أسبوع إلى سنة.

ب. بعد الانتهاء من التفاعل يكون الأفراد المتفاعلون صوراً رمزية ذهنية على الأشخاص الذين يتفاعلون معهم ، وهذه الصور لا تعكس جوهر الشخص وحقيقته الفعلية وإنما تعكس الحالة الانطباعية السطحية التى كونها الشخص تجاه الشخص الآخر المتفاعل معه.

ج. عند تكوين الصورة الانطباعية عن الفرد تلصق هذه الصورة بمجرد مشاهدته أو السماع عنه أو التحدث إليه من دون التأكد من صحة المعلومة أو الخبر لأن الشخص اعتبر الفرد الآخر رمزاً ، والرمز هو الذى يحدد طبيعة التفاعل مع أن الصورة الرمزية التى يكونها عن الاخر قد تكون ايجابية أو سلبية اعتماداً على الانطباع الذى تكون عنه.

نستنتج من ذلك أن الدوافع المؤدية إلى ارتكاب الجرائم الإلكترونية ترتبط بعوامل نفسية واجتماعية تهدف إلى إشباع رغبات الذات ، حيث قد يكتسب الفرد الخبرة الإجرامية الرقمية من خلال عمليات تفاعلية داخل المجتمع الذى ينتمى إليه ، وعلى الرغم من أن الفرد قد ينشأ على إدراك رفض المجتمع للجريمة من خلال عمليات التنشئة الاجتماعية ، إلا أن تجاوزه لهذه القيم يشير إلى وجود خلل داخل الأنساق الاجتماعية واضطراب فى البناء القيمى للأفراد ، مما يسهم فى زيادة احتمالية ارتكاب الجرائم الإلكترونية ، وفى هذا السياق ، يصبح الفرد أكثر عرضة للوقوع فى سلوك إجرامى رقمى عندما يجد نفسه فى موقف يتصارع فيه بين إدراكه لعواقب الجريمة وبين الضغوط أو المغريات التى تدفعه إلى ارتكابها ، وهذا التفاعل السلبى يعكس تراجع مستوى الضبط الاجتماعى وضعف الروابط الاجتماعية ، مما يؤدى إلى ازدياد فرص الانخراط فى الأنشطة الإجرامية الإلكترونية ، خاصة فى ظل التطور السريع للذكاء الاصطناعى الذى يتيح أدوات وتقنيات متقدمة تسهل تنفيذ هذه الجرائم وتزيد من صعوبة كشفها والتصدى لها.

سابعاً: القضايا النظرية للبحث

تنقسم القضايا النظرية للبحث إلى عدة محاور رئيسية، تتمثل فيما يلى:

المحور الأول:-دور الذكاء الاصطناعى فى تطور أنماط ارتكاب الجرائم الإلكترونية:

فى ظل التطور الهائل للذكاء الاصطناعى والذى رافقه التطور الكبير فى تكنولوجيا الحواسيب والأجهزة الذكية ،أدى ذلك إلى ظهور أدوات واختراعات وخدمات جديدة نتج عنها نوع جديد من المعاملات يسمى بالمعاملات الالكترونية والذى يقصد بها كل المعاملات التى تتم عبر أجهزة الكترونية مثل الحاسوب ، شبكة الانترنت ، الهاتف المحمول ، والهواتف الذكية ، ونتيجة التطور الكبير والسريع لهذه الأجهزة ضعفت القدرة على المراقبة والتحكم ، مما أدى إلى ظهور نوع جديد من الجرائم يسمى بالجريمة الالكترونية أو المعلوماتية أو التقنية ، والتى هى عبارة عن نشاط إجرامى تستخدم فيه تقنية الحاسب الآلى أو الهواتف الذكية الموصولة بشبكة الانترنت بطريقة مباشرة أو غير مباشرة لتنفيذ الفعل الإجرامى.(فاطيمة ،٢٠٢٣،ص٥٩)

ونجد ان الذكاء الاصطناعى يستخدم بشكل متزايد كهدف وكأداة لارتكاب الجرائم الالكترونية ، فالأجهزة الإلكترونية وغيرها من المنتجات ذات التقنية العالية تمكن المجرمين من ارتكاب جرائم رخيصة وسهلة وأجهزة الكمبيوتر والهواتف والإنترنت وجميع أنظمة المعلومات الأخرى التي تم تطويرها لمنفعة البشرية عرضة للنشاط الإجرامي، فالجرائم التي تستهدف أنظمة تكنولوجيا المعلومات تستهدف عادة حسابات البريد الإلكتروني والحسابات المصرفية وأجهزة الكمبيوتر والخوادم ومواقع الويب والبيانات الشخصية والسجلات الرقمية للمؤسسات الخاصة والعامة، وتُعرف هذه الجرائم أيضاً باسم "الجرائم الرقمية" أو "جرائم الكمبيوتر" أو "جرائم تقنيات المعلومات" أو "جرائم الشبكة" أو "جرائم الإنترنت" وتتكون الجرائم الإلكترونية من مخالفات مثل اختراقات الكمبيوتر، وإساءة استخدام حقوق الملكية الفكرية، والتجسس الاقتصادي، والابتزاز عبر الإنترنت، وغسل الأموال الدولي، وعدم تسليم البضائع أو الخدمات. (Dilek,Cakır,2015,P.22)

كما أن محل الجريمة الالكترونية هو الحاسب الآلى: فيقع الاعتداء على أجزائه ومكوناته المادية ،وإما أن يتم الاعتداء على ما يحتويه من معلومات مثبتة ومخزنة فى ذاكرة الحاسب: مثل أن يقوم شخص بالاعتداء على الحاسب فيسرق ما به من معلومات ،أو برامج مستخدمة فيه ،أو يفشى ما به من معلومات وبيانات ،أو يعطل عمله ،أو يتلف طريقة استخدامه ،أو يبعث بما مسجل عليه من معلومات فيزورها أو ينسخها ،وإما أن تقع الجريمة باستخدام الحاسب ، فيكون هو الأداة المستخدمة فى ارتكاب الجريمة ، فقد يستخدم الحاسب فى جرائم اعتداء على الأموال: كالتزوير وخيانة الأمانة والنصب والسرقة، وانتهاك حرمة الحياة الخاصة ،وأشد خطورة من ذلك أن يستخدم فى جرائم القتل ؛ كبرمجة جهاز يتم التحكم فيه آلياً عن بعد لتفجير أماكن بما فيها من أشخاص ، فكل هذه الجرائم وأمثالها تستخدم بواسطة الحاسب ،فهو حينئذ أداة لإرتكاب الجريمة ، ومحل الجريمة يختلف حسب ما يقع عليه فعل المجرم ، والذى يعد محل الحق أو المصلحة المحمية.(عبدالرازق،٢٠٢١،ص ٤٣٢)

كما أن التطور الهائل فى مجال الذكاء الاصطناعى وتحديداً فى وسائل الاتصال ونقل المعلومات هيأ للعصابات الإجرامية الفرصة لإجراء عملياتهم الإجرامية بأسلوب لا يخضع دائماً لمراقبة الشرطة مباشرة الأمر الذى يترتب عليها صعوبة إحكام قبضة الأمن على مثل هذه العصابات ، هذا بالإضافة إلى سرعة انتقال الأساليب الإجرامية الجديدة أو المبتكرة وطرق ارتكاب الجرائم بين التشكيلات العصابية بعضها البعض وزيادة تعاونها معاً واعتمادها على أفراد من تشكيلات عصابية أخرى للقيام نيابة عنها ببعض المهام التى توكل إليها ، كما أن الذكاء الاصطناعى أدى إلى تحول نسبة كبيرة من الجرائم التقليدية إلى جرائم ذوى الياقات البيضاء التى يقوم بها مجرم مثقف يستخدم بالإضافة إلى الأساليب التكنولوجية الحديثة ذكاءه وإمكانياته العلمية والعملية بدون إراقة دماء .(عوض،٢٠١٨،ص ٢٣٥)

وتعتبر البدايات لاستخدام مصطلح الإرهاب السيبرانى Cyberterrorisme خلال فترة الثمانينات من العقد المنصرم على يد بارى كولين Barry Collin ، واصبح الإرهاب السيبرانى شراً يحوم فى الأفق ولا يمكن للأساليب التقليدية محاربته ولا السيطرة عليه ، وهو التلافى بين الإرهاب والفضاء الرقمى ، وهو استخدام الفضاء السيبرانى للقيام بالعمليات الإرهابية ضد أشخاص أو شركات أو دول بأكملها وذلك من أجل ترهيب وترويع وإكراه الحكومات وشعوبها من أجل تحقيق الأهداف السياسية والاجتماعية، وجعلهم يعيشون فى حالة من الخوف ، وتتضمن عمليات الإرهاب الإلكترونى القيام بإختراق المواقع والشبكات وأجهزة التحكم الرقمية تلك التى تتحكم وتدير منشآت بأكملها أو تتحكم فى نظام الأسلحة لجهة ما من أجل القيام بالتدمير ، كما يتضمن استعمال وسائل الاتصال والمعلومات لإيصال رسالة المنظمات الإرهابية الى أكبر فئة مستمعة ممكنة ، واستقطاب الأفراد للأنخراط فى هذه التنظيمات الإرهابية .(محمد،امينة،٢٠٢٣،ص٥٣٥)

وفى ذات السياق ، فقد ساعدت الأساليب التكنولوجية المستخدمة عبر شبكة الإنترنت على تشجيع ذوى الميول الإجرامية ومعتادى الإجرام فى تنفيذ عملياتهم الإجرامية وغير المشروعة عبر الشبكة ، وقد أثبتت الدلائل الواقعية أن تقنيات شبكة الإنترنت قد ساعدت مرتكبى هذه النوعية من الجرائم فى تطوير أساليبهم والتمادى فى سلوكياتهم الإجرامية عبر الشبكة ، للحصول على حقوق غير مشروعة من الغير ، أو انتهاك حرمات الآخرين ، والتوسع فى عمليات الابتزاز والتهديد والسب والقذف والتشهير ، مستغلين ما توفره لهم شبكة الإنترنت من ضمانات وحماية ، فضلاً عن إمكانية تنفيذ جرائمهم من أماكن بعيدة الصلة عنهم ، كمقاهى الإنترنت والفنادق والمطاعم أو من خلال استغلال خاصية الإنترنت اللاسلكى غير المشفر ، أو غير المؤمن بأى موقع عام أو خاص . (الحوتى ،٢٠٢٠، ص ٧٢٣)

المحور الثانى :أشكال الجرائم الإلكترونية وعلاقتها بالذكاء الاصطناعى:

تنوعت جرائم الحاسوب إلى جرائم ترتكب على نظم الحاسوب ،وأخرى ترتكب بواسطته، فهى جرائم تنصَب على معطيات الحاسوب(بيانات ومعلومات وبرامج) وتطال الحق فى المعلومات ، ويستخدم لاقترانها وسائل تقنية تقتضى باستخدام الحاسوب ،وأن الجرائم التى تنصَب على الكيانات المادية تدخل فى نطاق الجرائم التقليدية ولا يندرج ضمن الظاهرة المستجدة لجرائم الحاسوب، لذلك سنقوم بسرد أفعال الاعتداء فى مجال الأنظمة المعلوماتية فى خلال المطالب الآتية: بدءًا من محاولة الاعتداء على المعدات المادية لأنظمة المعلوماتية ، ومروراً بالاعتداء على المعلومات المختزنة آلياً ، ثم الاعتداء على برامج الحاسب الآلى، وجرائم اعتداء على أشخاص وهناك جرائم تقع على المال ، وأخيراً ضد الحكومة والجرائم الالكترونية الأخرى.(عبدالرازق،٢٠٢١، ص ٤٣٢)

والمجرم الإلكترونى لديه صفات خاصة تجعله يمتاز عن غيره من المجرمين الآخرين ، لذا نجد أن فى أكثر الأحوال المجرم الإلكترونى يتمتع بقدر عال من الذكاء ،إذ يمتلك المهارات التى تؤهله للقيام بتعديل فى الأنظمة الأمنية الإلكترونية وتطويرها ، فلديه القدرة على تكوين تصور كامل لجريمته حتى لا يتمكن أحد من ملاحقته وتتبع أفعاله عن طريق الشبكات أو داخل أجهزة الكمبيوتر ، لذا فالمجرم الإلكترونى عادة يخطط لارتكاب جرائمه بالتعرف على كافة الظروف المحيطة به ، لتجنب ما من شأنه ضبط أفعاله وكشف هويته ، وأنه يتمتع بقدرة ومهارة تقنية يستغلها فى اختراق الشبكات وكسر كلمات المرور أو الشفرات بغاية الحصول على البيانات والمعلومات الموجودة فى أجهزة الكمبيوتر وعن طريق الشبكات.(الأميرى،العموش،٢٠٢٢،ص٣٠٧)

وفيما يلى عرض لأهم اشكال الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى:

أ. التصيد أو الاحتيال أو الخداع الالكترونى(Phishing)

هى محاولة خداع العملاء بالكشف عن معلوماتهم الأمنية الشخصية ، مثلا أرقام بطاقات الائتمان الخاصة بهم أو تفاصيل الحساب المصرفى أو أى معلومات حساسة أخرى عن طريق التنكر فى صورة أعمال جديرة بالثقة فى رسالة بريد إلكترونى ، وتطلب فى رسائلهم من المستلمين تحديث أو التحقق من صحة أو تأكيد معلومات حساباتهم ، وفى الحقيقة أن المحتالين عبر الإنترنت يستخدمون إغراءات متطورة بشكل متزايد لأنهم يصطادون معلومات المستخدم المالية وبيانات كلمات المرور ، ويعد هذا النوع من الجرائم الالكترونية من أكثر الجرائم استخداماً فى وسائل التواصل الاجتماعية حتى الآن نظراً للسهولة الكبيرة فى تنفيذه ، ولا يتطلب اتصال مباشر بين المتسلل والضحية. (الشمرى ،٢٠٢١، ص ص١٢٢-١٢٣)

ب. الجرائم الواقعة على البرامج:

تكون جريمة الاعتداء على المكونات المادية للنظام المعلوماتى ،محل الجريمة هو الاعتداء على البرامج ؛ حيث إن هذه البرامج تحتوى على معلومات وبيانات ، ولا يستطيع ارتكاب تلك الجريمة إلا من كانت له معرفة فائقة فى محل البرمجه، ولقد تعددت جريمة الاعتداء على البرامج لتتمثل فيما يلى: (عبدالرازق،٢٠٢١، ص ٤٣٣)

- **جريمة الاعتداء على البرامج:**تكون جريمة الاعتداء على المكونات المادية للنظام المعلوماتى ، محل الجريمة هو الاعتداء على البرامج ، حيث إن هذه البرامج تحتوى على معلومات وبيانات ، ولا يستطيع ارتكاب تلك الجريمة إلا من كانت له معرفة فائقة فى مجال البرمجة.
- **جريمة الاعتداء على البرامج التطبيقية:**يقوم الجانى بالاعتداء على البرامج من خلال تعديلها ، والهدف الرئيس من هذا التعديل هو الاختلاس ، وأكثر هذه الجرائم تقع فى مجال الحسابات

مثال على ذلك:أن يقوم مبرمج بأحد البنوك بزرع برنامج فرعى بإدارة الحسابات ،فنتج عن ذلك تجاهل كل عمليات السحب- بطاقات أو شيكات حسابية- التى تتم بمعرفة المبرمج ، وبهذا جعل الجانى البنك يتحمل هذه المسحوبات فى باب ميزانية الإدارة، ولم تتم اكتشاف الجريمة إلا عندما أصيب الحاسب بفيروس فسبب عطلاً بأحد النظم المعلوماتية، مما جعل العاملين بالبنك مضطرين للمعالجة اليدوية لكل الحسابات، وحينئذ تظهر الجريمة.

- **جريمة الاعتداء على برامج الحاسب الآلى:**يمكن الاعتداء على برامج الحاسب الآلى فى أية مرحلة من مراحل صنع برامج التشغيل أو برامج التطبيق أو فى لحظة صيانتها أو تحديثها ، فلابد أن من يرتكب هذه الجرائم يكون من قبل المتخصصين الذين لديهم معرفة تقنية فى برامج الحاسب الآلى وبصفة خاصة فى مجال البرمجة، وبالتالى قد يتمكن الجانى من إحداث تعديل فى برامج التشغيل أو فى برامج التطبيق ، فبرامج التشغيل هى البرامج التى لا يعمل النظام المعلوماتى بدونها، وهى التى تقوم بتنظيم التعليمات الخاصة بالنظام ، ويتحقق الاعتداء عليها عندما يتدخل شخص فيضيف للبرامج عدة تعليمات يستطيع من خلالها أن يحصل على معلومات أو جميع البيانات المثبتة على النظام المعلوماتى.

ج. جريمة الاعتداء على الحق فى الخصوصية:

تعد مواقع التواصل الاجتماعى من أشهر مايوجد فى العالم الافتراضى، حيث يستخدم موقع الفيس بوك الخوارزميات كأحد تطبيقات الذكاء الاصطناعى ، من خلال ملفات تعريف الارتباط ، لتحقيق أهداف معينة ، كالتأكد من شخصية المستخدم وتحديد تفضيلاته ، ومعرفه موقعه، وتحليلات البحث، وغيرها من الأشياء الأخرى التى يستطيع معرفتها من خلال تلك الملفات ، ويتم ذلك بموافقة المستخدم ، فيتمثل الاعتداء على خصوصيات المستخدم من قبل برامج الفيس بتطبيق خوارزميات الذكاء الاصطناعى، بتحديد اهتمامات المستخدم من خلال تفاعلاته على الصور أو المنشورات ومتابعته لمنتجات معينة ، وكل ذلك من أجل استخدامها فى عرض إعلانات له تتوافق مع اهتماماته ، وايضاً عرض محتوى يتوافق مع اهتماماته لجعله يوجد فى الموقع أطول فترة ممكنة فى يومه، وفى الواقع تعد هى المخرج القانونى من مثل تلك الاعتداءات على خصوصياته.(الدسوقى ،٢٠٢٢،ص ص ١١٦٣-١١٦٤)

د. جرائم السطو على أرقام البطاقات الائتمانية:

مع بداية استخدام البطاقات الائتمانية خلال شبكة الانترنت واكبت ظهور الكثير من المتسللين للسطو عليها بلا هوادة ، فالبطاقات الائتمانية تعد نقوداً الكترونية والاستيلاء عليها يعد استيلاء على مال الغير ، ومع وضع تفعيل مفهوم التجارة الالكترونية قامت العديد من شركات الأعمال إلى استخدام

الانترنت والاستفادة من مزايا التجارة الالكترونية ، وإن الاستيلاء على بطاقات الائتمان أمراً ليس بصعوبة ، فلصوص بطاقات الائتمان مثلاً يستطيعون الآن سرقة مئات الألوف من أرقام البطاقات فى يوم واحد من خلال شبكة الانترنت ومن ثم بيع هذه المعلومات للآخرين ، ويتعدى الأمر المخاطر الأمنية التى يمكن أن تتعرض لها البطاقات الائتمانية الحالية فنحن الآن فى بداية ثورة نقدية يطلق عليها اسم النقود الالكترونية والتى يتنبأ لها بأن تكون مكملة للنقود أو البلاستيكية ومن المتوقع أيضاً أن يزداد الاعتماد على هذا النوع الجديد والحديث من النقود أن تحوز الثقة التى تحوزها النقود التقليدية. (دولى،ناصرى،٢٠١٨،ص ٥٥)

ومن أشهر لصوص البطاقات الائتمانية على شبكة الانترنت هو (تيم كورادو) جنسيته بريطانى ، قام باقتحام عشرات المواقع فى شبكة الانترنت ، واستولى على أرقام وبيانات ما يزيد على (١٢٤) الف بطاقة ائتمانية تخص عملاء هذه المواقع ، وقام بنشر أرقامها وبياناتها على شبكة الانترنت ، وقام أيضاً بإرسال بعض بيانات هذه البطاقات إلى بعض المواقع الشخصية لأفراد آخرين لا يعرفهم ولا يعرفونه ، وقال (تيم كورادو) حين القاء القبض عليه للمرة الأولى لا يملكون دليلاً واحداً ضده ، وقال أيضاً ان هدف من قام بهذه العمليات التى يتهم بها هو ايقاظ الشركات التجارية التى يوجد لها مواقع على شبكة الانترنت من سباتها العميق ودفعها لإنجاز المزيد من اجراءات الحماية لمواقعها الالكترونية ، وبالتالى حماية أموال زبائنها ، وأفلت كورادو من العقاب بسبب واحد وهو أن الموقع الذى تقول الشرطة انه استعمله فى عملياته مسجل فى شركة Great solution التى يوجد مقرها فى مقاطعة ويلز البريطانية ، ولكن كل البيانات الموجودة فى هذا الموقع لا تدل أبداً على أى شئ يتعلق بشخصية تيم كورادو(جواد ،٢٠١٥،ص٣٣)

هـ. جرائم البريد الدعائى المزعج أو المضلل (Spam)

ويقصد بها إرسال رسائل إلكترونية غير مطلوبة ، وبأعداد كبيرة لأهداف تجارية ، وفرضها على الناس مع عدم رغبتهم فى استلامها ، وقد عرفت اللجنة الوطنية للمعلوماتية والحريات فى فرنسا CNIL بأنه "عملية إرسال الرسائل غير المرغوب فيها وهى فى معظم الأحيان ذات طبيعة تجارية وبأعداد كبيرة ، وبشكل متكرر للأفراد الذين ليس لهم اتصال سابق مع المرسل ، وتم الحصول على عنوان البريد الالكترونى من الفضاء العام لشبكة الإنترنت ، مثل المجموعات الإخبارية،أو القوائم البريدية ،أو قائمة مواقع الويب" ، ويعانى معظم مستخدمى البريد الالكترونى من الرسائل المتطفلة مما يسبب ازعاجاً كبيراً لهم ، ومساساً بحرمة الحياة الخاصة للمستخدم ، وتعد من أهم مشكلات الجرائم الالكترونية كونها متنامية بإستمرار ، وأكثر انواع الاعتداء على قواعد البيانات.(الشمرى ،٢٠٢١،ص ١٢٣)

و. نشر الإباحة:

المقصود بنشر الإباحة إرسال أو نشر عمل إباحى أو بإعداد أو حفظ أو معالجة أو عرض أو طباعة أو نشر أو ترويج أنشطة أو أعمال إباحية أو اتصل بالدعارة أو الأعمال الإباحية ويتم ذلك عن طريق المواقع الإلكترونية الموجودة على الشبكة ، التى تستعمل بغرض الإثارة الجنسية عن طريق قيام المجرم الإلكترونى بنشر صور جنسية فاضحة وأفلام جنسية، وكثيراً ما تستهدف الأطفال والشباب لأن هذه الفئة أقل تحصيناً.(الأميرى،والعموش،٢٠٢٢، ص٣٠٨)

ز. جرائم تشويه السمعة والانتقام:

يتعرض الكثير من الأفراد إلى تشويه السمعة أو الانتقام عبر مواقع التواصل الاجتماعى والتطبيقات الحديثة من أشخاص معروفين للضحية أو مجهولى الهوية ، كتوجيه عبارات الشتم والتحقير أو القذف أو عرض صور خاصة للضحية ، لكن مع وصول تقنية التزييف العميق فالمخاطر والأضرار أصبحت أشد وطئاً ، وربما من الصعوبة بمكان إصلاح الأضرار الناتجة عن استخدامها. (مغايرة،٢٠٢٤،ص١٣٨)

ح. جرائم انتحال شخصية الفرد:

وهو إستغلال أشخاص بيانات عبر الإنترنت تخص شخص آخر أسوأ إستغلال ، مثل تاريخ الميلاد ورقم الضمان الاجتماعى والعنوان وما شابه ذلك ، من اجل الحصول على بطاقات ائتمانية أو الوصول لشراء سلعة ما على الإنترنت ، وإرتكاب جرائم تحت إسم هذه الشخصية ، ومن الملاحظ أن هؤلاء يستخرجون بطاقات ائتمانية بعد إنتحال الشخصية من قبل جهات لا يتخذون إجراءات صارمة أو إجراءات أمنية صحيحة ، أو من خلال الموظفين الذين لا يملكون الخبرة الكافية، ومن الملاحظ أن هناك كثيراً من الطرق المستخدمة الآن للوصول إلى معلومات الشخص بسهولة ويسر كتقليد صفحات لإحدى البنوك مثلاً ،أو إرسال بريد إلكترونى لمستخدمى البطاقات بحجة أن البنك يقوم بعمليات تحديث للمعلومات التى يصل إليها المجرم عن طريق بعض الأسئلة التى يجيب عليها الضحية وإيقاعه ومعرفة بياناته ، حيث أن كثير من هذه الجرائم تستخدم من الموظفين أنفسهم داخل المؤسسات و، اضافه الى ذلك إنتحال شخصيات فى مواقع التواصل الإجتماعى من خلال الإستفادة من المعلومات المقدمة للجمهور على صفحة الضحية ، أو يتم ذلك عن طريق كثير من الإعلانات التى تخاطب غريزة الطمع فى الإنسان ، والتى تزحم بها شبكة الإنترنت بعد تمنيه بالفوز بمبلغ مالى كبير أو بجائزة غالية الثمن ، ومن خلال تلك الإعلانات التى بواسطتها يتم الوصول إلى المعلومات التى تساعد فى إنتحال الشخصية. (دبابنة،٢٠١٥،ص٢٠)

ط. جرائم التزييف العميق (Deepfakes)

التزييف العميق هو نوع شائع من إساءة استخدام الذكاء الاصطناعي، حيث يتم إنشاء أو تعديل المعلومات الصوتية والمرئية لجعلها تبدو حقيقية باستخدام خوارزميات الذكاء الاصطناعي، مثال على ذلك مقطع فيديو مزيف يدّعي إظهار مساعد سياسي ماليزي متورط في علاقات جنسية مع وزير في الحكومة، مما أثار مطالب بالتحقيق مع هذا الوزير لاحتمال ارتكابه مخالفات، مثال آخر هو شركة طاقة مقرها المملكة المتحدة تعرضت للاحتيال وأرسلت أكثر من ٢٠٠,٠٠٠ جنيه إسترليني (حوالي ٢٦٠,٠٠٠ دولار أمريكي) إلى حساب مصرفي في المجر، بعد أن قام شخص ضار بانتحال صوت الرئيس التنفيذي للشركة باستخدام تقنية التزييف العميق الصوتية بالتعاون مع الممثل والمخرج السينمائي جوردان بيل، كما يمكن أن يكون بمثابة أداة مفيدة لتثقيف الناس حول الانتهاكات المحتملة التي قد يتعرضون لها.(Lozonschi,Bakhaya,2023,pp.122-123)

المحور الثالث: أسباب ودوافع الجرائم الالكترونية المرتبطة بالذكاء الاصطناعى:

تختلف أسباب ودوافع ارتكاب الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى عن تلك الخاصة بالجرائم التقليدية ، نظراً لاعتمادها على تقنيات متطورة تتيح إمكانيات جديدة للمجرمين ، وفيما يلى أبرز هذه الأسباب والدوافع:

١. **الرغبة فى جمع المعلومات وتعلمها** : أن الذين يرتكبون هذه الجرائم يقدمون عليها بغية الحصول على الجديد من المعلومات وقد أشار ليفى فى أحد مؤلفاته الخاصة بقرصنة الأنظمة Hacker إلى أن اخلاقيات هؤلاء القراصنة ترتكز على مبدأين أساسيين **الأول** أن الدخول إلى أنظمة الحاسب الآلى يمكن أن يعلمك كيف يسير العالم **والثانى** أن جمع المعلومات يجب أن يكون غير خاضع للقيود ، فهم يتعاونون فى البحث على شكل جماعات ويتقاسمون المعلومات والخبرات ولو بطرق غير مشروعة.

٢. **الاستيلاء على المعلومات** : يتمثل ذلك فى الحصول على المعلومة المحفوظة فى الحاسب الآلى أو المنقولة أو تغيرها أو حذفها أو إلغائها من النظام ويختلف الدافع لهذا التصرف فقد يكون دافع نفسى أو سببه الابتزاز.

٣. **قهر النظام واثبات التفوق على تطور وسائل التقنية:** حيث يكون الدافع وراء ارتكاب هذه الجرائم هو قهر النظام واثبات قدرة الجانى وتفوقه على تعقيدات وتطور وسائل التقنية الحديثة حيث يمضى كل وقته أمام أجهزته لكسر الحواجز الأمنية للأنظمة الإلكترونية واختراقها ليثبت براعته فى القدرة على تحدى أى تطور جديد.

٤. **إلحاق الأذى بأشخاص أو جهات عامة:** بعض المجرمون الذين يقدمون على ارتكاب الجريمة عبر شبكة المعلومات العالمية وتقنية المعلومات بصورة عامة يرتكز الدافع من ورائها على إلحاق

الأذى بأشخاص محددين أو جهات معينة ، وغالباً ما تكون تلك الجرائم مباشرة تتمثل فى صورة ابتزاز أو تهديد أو تشهير.

٥. **تحقيق أرباح ومكاسب مادية** : هناك بعض الجرائم الإلكترونية التى ترتكب يكون الدافع منها تحقيق أرباح ومكاسب مادية كإستخدام شبكة الانترنت للإعلان عن صفقات تجارية غير مشروعة مثل المخدرات وتجارة البشر.

٦. **تهديد الأمن القومى والعسكرى للدول:** بعض الجرائم الإلكترونية الهدف منها أسباب ودوافع سياسية كتهديد الأمن القومى والعسكرى ومن ذلك ظهر ما يعرف بالتجسس الإلكترونى والإرهاب الإلكترونى والحرب المعلوماتية كما هو الحاصل بين الدول المتقدمة إلكترونياً. (الهديف،٢٠٢٢،ص ص ١٤٦-١٤٧)

٧. **دافع الانتقام:** يعد دافع الانتقام من أخطر الدوافع التى يمكن أن تدفع الشخص إلى إرتكاب الجريمة لأنه غالباً ما يصدر من شخص يملك معلومات كبيرة عن مؤسسة أو الشركة التى يعمل بها ، ويقوم بدافع الانتقام إما نتيجة فصله من العمل أو تخطيه فى الحوافز أو الترقية ، او زرع فيروسات فى أجهزة العمل أو سرقة صور شخصية بنية التحرش أو التهديد.

٨. **دوافع ذهنية ونمطية:** الصورة الذهنية لمرتكبى الجرائم الإلكترونية غالباً هى صورة البطل والذكى يستحق الإعجاب لا صورة المجرم الذى يستوجب محاكمته ، فغالباً ما يكون الدافع لدى مرتكبى الجرائم الإلكترونية هى الرغبة فى إثبات الذات وتحقيق انتصار على تقنية المعلومات ، وهم فئة غير خطيرة لأن دافعهم هو الفضول بالدرجة الأولى وليس الربح ولا يملكون أية نوايا سيئة.(ذياب، بوترعة، ٢٠٢٠،ص ص ١٤-١٥)

ولابد من التأكيد على ان التطور التكنولوجى المتسارع يتطلب من الأفراد والحكومات على حد سواء تأمين جميع الحسابات الافتراضية والمعلومات التى ينشرونها فى وسائل التواصل الاجتماعى ومواقع الشبكات ، من أجل تقليل فرصة التعرض للهجمات الالكترونية، ولحماية المعلومات لا سيما المعلومات الحكومية السرية ومعلومات المؤسسات المالية التى يتم حفظها فى أجهزة الكمبيوتر او فى الفضاء السيبرانى ، لا سيما وان العديد من المجرمين الالكترونيين أدركوا بأن جمع البيانات من أجهزة الكمبيوتر والاستفادة من البيانات المسروقة ستحقق لهم ارباح مادية ، يضاف الى ذلك سهولة الجريمة وصعوبة الكشف عنها مما جعلها جرائم مغرية جداً ، ومن جانب اخر ان استمرار تطور الجرائم الالكترونية دفع بالحكومات الى سن تشريعات قانونية لمحاكمة الاشخاص الذين يرتكبون الجرائم الالكترونية ، وتجريم اختراق أى شخص يحاول الوصول الى المعلومات والبيانات المحفوظة بدون موافقة ، بل ان خطورة الجرائم الالكترونية تتطلب سن قوانين أكثر صرامة حتى تكون رادعة لهذه الجرائم.(الشمرى ،٢٠٢١، ص ١٢٤)

ثامناً:الإجراءات المنهجية للبحث:

لتحقيق أهداف البحث ، اعتمد الباحث على مجموعة من الإجراءات المنهجية المستندة إلى المنهج العلمى ، والتى تمثلت فيما يلى :

١.أسلوب البحث:

يحدد الباحث هذه الدراسة بوصفها "دراسة وصفية" ، حيث تركز على وصف البيانات التى تم جمعها حول موضوع البحث الراهن ، والمتمثل فى تأثير الذكاء الاصطناعى على أنماط ارتكاب الجرائم الإلكترونية ، كما تهدف إلى دراسة دور الذكاء الاصطناعى فى تسهيل ارتكاب هذه الجرائم ، للكشف عن العوامل المؤدية إليها ، والآثار المترتبة عليها ، وانعكاساتها على الضحايا ، ويتم ذلك من خلال تحليل وتصنيف البيانات المستخلصة ، وتفسير دلالاتها ، بهدف تقديم مقترحات تسهم فى حماية الأفراد من الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، وذلك من وجهة نظر ضحايا هذه الجرائم.

٢. طريقه البحث:

اعتمد البحث على طريقة دراسة الحالة باعتبارها أحد الأساليب الكيفية ، حيث تم تطبيقه على مجموعة من الضحايا الذين تعرضوا لجرائم إلكترونية مدعومة بتقنيات الذكاء الاصطناعى ، وقد هدف البحث إلى التعرف على مستوى تعليمهم ، وأنواع الجرائم الإلكترونية التى تعرضوا لها ، بالإضافة إلى دراسة الظروف المحيطة بهذه الجرائم ، كما سعى إلى تحليل أبرز الأسباب التى تؤدى إلى ارتكاب الجرائم الإلكترونية المختلفة ، إلى جانب استكشاف المخاطر والتحديات التى يواجهها الضحايا نتيجة لهذه الجرائم ، وأخيراً تقديم استراتيجيات لحماية الأفراد من الهجمات الإلكترونية القائمة على الذكاء الاصطناعى.

٣.مجتمع البحث:

يتكون مجتمع البحث من الضحايا الذين تعرضوا للجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، ويبلغ عددهم ٢٠ حالة فى محافظة القليوبية ، حيث تهدف الدراسة إلى تحليل أنماط هذه الجرائم ، وأسبابها ، وتأثيراتها المختلفة على الضحايا.

٤.أدوات جمع البيانات:

أ. **أداة الملاحظة:** تعد أداة الملاحظة وسيلة فعالة لجمع البيانات ، إذ تسهم فى رصد الظاهرة محل الدراسة وفهم الدوافع والأسباب الكامنة وراءها ، من خلال الملاحظة يتمكن الباحث من متابعة الحالة العامة للضحية ، وتحليل ما تسرده ، إلى جانب رصد تعابير وجهها والدلالات الشكلية التى قد تعكس مشاعرها وتأثرها ، كما تشمل الملاحظة منح الضحايا الوقت الكافى للتعبير عن مشاعرهم

وسرد تفاصيل ما حدث ، مع تدوين جميع المعلومات المستخلصة بدقة ، يتيح ذلك للباحث جمع بيانات ذات قيمة ، تعزز من فهمه العميق لضحايا الجرائم الإلكترونية.

ب. **دليل دراسة الحالة:** اعتمدت الدراسة الحالية على دليل دراسة الحالة لعينة مكونة من ٢٠ ضحية من ضحايا الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، وذلك بهدف تحليل طبيعة هذه الجرائم ، وفهم العوامل المؤدية إليها ، والتعرف على تأثيرها على الضحايا ، مع استخلاص النتائج التى تساهم فى وضع استراتيجيات للحد والوقاية من هذه الظاهرة

ج. **الإخباريون:** اعتمد الباحث فى دراسته على الإخباريين وهم مجموعة من أصحاب الشركات العاملة فى مجال الأمن السيبرانى والأنظمة الأمنية ، حيث تقدم هذه الشركات حلولاً متكاملة لحماية الأفراد من التهديدات الرقمية ، ويتميز الإخباريون بكونهم من سكان منطقة الدراسة ، مما أتاح لهم فهماً أعمق لطبيعة الجرائم الإلكترونية التى تستهدف الضحايا فى هذه البيئة ، وتعتمد الشركات التى يعمل بها الإخباريون على أحدث التقنيات العالمية فى مجال الأمن السيبرانى ، وتسعى إلى بناء بيئة رقمية آمنة وموثوقة لمستخدمى الإنترنت ، كما تتضمن مهامهم التدخل السريع لمساعدة ضحايا الابتزاز الإلكترونى وسرقة البيانات ، بالإضافة إلى تحليل وتتبع مصادر التهديد باستخدام تقنيات متقدمة ، واستعادة الحسابات والملفات المسروقة وتأمينها ضد الهجمات المستقبلية ، علاوة على ذلك ، تقدم هذه الشركات استشارات قانونية لمساندة الضحايا فى اتخاذ الإجراءات القانونية المناسبة ، فضلاً عن تعزيز الوعى الأمنى من خلال تنظيم ورش عمل ودورات تدريبية تهدف إلى حماية الأفراد من الوقوع ضحايا للاختراق والاحتيال الإلكترونى ، ومن بين الخدمات التى تقدمها الشركات استعادة الحسابات المسروقة مثل البريد الإلكترونى ، حسابات مواقع التواصل الاجتماعى ، والحسابات البنكية ، وإعادة تعيين كلمات المرور وضبط إعدادات الأمان لمنع أى اختراق مستقبلى ، وحذف وإزالة المحتوى المسرب من الإنترنت بالتعاون مع منصات التواصل الاجتماعى والجهات المختصة ، كما تقدم هذه الشركات دعماً قانونياً وإجراءات أمنية لمساعدة الضحايا ومنها: مساعدة الضحية فى تقديم بلاغ رسمى للجهات المختصة مثل النيابة العامة ومباحث الإنترنت ، وإعداد ملف قانونى قوى يتضمن الأدلة الرقمية الداعمة للقضية ، بما فى ذلك تتبع مصادر التهديد والمحادثات ، وسجلات الاختراق ، وقد لعب الإخباريون دوراً حاسماً فى مكافحة الجرائم الإلكترونية المدعومة بالذكاء الاصطناعى ، حيث تعانوا مع الضحايا عبر تقديم التوعية والدعم ، سواء من خلال المساعدة الإلكترونية أو تقديم النصائح حول كيفية التعامل مع الجرائم الواقعة عليهم ، كما قاموا بدور إرشادى فى توجيه الضحايا إلى الجهات الأمنية والقضائية المختصة بالتحقيق فى الجرائم الإلكترونية وملاحقة مرتكبيها وتطبيق القانون بحقهم ، وفى إطار هذه الدراسة ، اعتمد

الباحث على مساعدة الإخباريين فى كسب ثقة الضحايا وأسرهم ، والاستماع إلى رواياتهم ، مما ساهم فى جمع الحقائق والمعلومات المطلوبة بشكل أكثر دقة وموضوعية.

د. **دليل دراسة الحالة وأقسامه:** تم تقسيم دليل دراسة الحالة إلى عدة محاور ، بحيث يغطى كل محور أحد الأهداف الرئيسية للبحث

حيث اشتمل دليل دراسة الحالة على قسمين رئيسيين:

١. **البيانات الأولية:** تضمنت ثمانية متغيرات ديموغرافية أساسية تهدف إلى تحديد الخصائص العامة للمبحوثين

٢. **المحاور البحثية:** احتوت على خمسة محاور رئيسية ، كل منها يضم مجموعة من الأسئلة التى ترتبط بأهداف البحث ، على النحو التالى .

- **المحور الأول:** يتناول الأسئلة المرتبطة بالهدف الأول من الدراسة ، وهو التعرف على دور الذكاء الاصطناعى فى ارتكاب الجرائم الإلكترونية ، وكيفية استغلال تقنياته فى تسهيل هذه الجرائم.
- **المحور الثانى:** يركز على الأسئلة المتعلقة بالهدف الثانى ، وهو التعرف على الأسباب المؤدية إلى ارتكاب الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، من وجهة نظر الضحايا.
- **المحور الثالث:** يتناول الأسئلة المرتبطة بالهدف الثالث ، والمتمثل فى رصد المخاطر والتحديات التى يواجهها الضحايا نتيجة تعرضهم للجرائم الإلكترونية المعتمدة على الذكاء الاصطناعى.
- **المحور الرابع:** يركز على الأسئلة المتعلقة بالهدف الرابع ، وهو دراسة موقف الضحايا عند تعرضهم للجرائم الإلكترونية المدعومة بالذكاء الاصطناعى ، وكيفية تعاملهم مع هذه الجرائم.
- **المحور الخامس:** يتضمن الأسئلة المرتبطة بالهدف الخامس ، والذى يتمثل فى استعراض المقترحات التى قد تساهم فى حماية الأفراد من الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، وذلك من وجهة نظر الضحايا أنفسهم

هـ. **مراحل صياغة الدليل:** تمت صياغة دليل دراسة الحالة استناداً إلى أهداف الدراسة وتساؤلاتها الأساسية ، لضمان تحقيق أقصى درجة من الدقة والموضوعية فى جمع البيانات ، وفى البداية تم إعداد الدليل بحيث يغطى جميع الجوانب المتعلقة بالبحث ، مع التركيز على محاور الدراسة الأساسية ، بعد ذلك خضع الدليل لعملية مراجعة وتحكيم علمى من قبل ٦ أساتذة متخصصين فى علم الاجتماع ، حيث قاموا بتقييم محتواه ومدى ملاءمته لأهداف الدراسة ، وبناءً على ملاحظات المحكمين تم إجراء التعديلات اللازمة لتعزيز دقة وصياغة الأسئلة وضمان اتساقها مع

أهداف البحث ، وأخيراً تم تطبيق الدليل فعلياً على حالات الدراسة الميدانية ، مما أتاح جمع بيانات مباشرة وموثوقة تسهم فى تحقيق أهداف البحث بفعالية.

٥.مجالات الدراسة:

أ. **المجال المكانى:** أقيمت الدراسة فى محافظة القليوبية وهى إحدى محافظات مصر وتقع بمنطقة شرق الدلتا ، يحدها من الجنوب محافظتا القاهرة والجيزة ، ومن الشمال محافظتا الدقهلية والغربية ، ومن الشرق محافظة الشرقية ، ومن الغرب محافظة المنوفية .

ب. **المجال البشرى:** تم اختيار حالات الدراسة باستخدام طريقة كرة الثلج ، حيث قامت كل حالة بالإشارة إلى حالات أخرى ، مما ساهم فى الوصول إلى العدد المطلوب من حالات الدراسة ، والذى بلغ عشرين حالة من الضحايا الذين تعرضوا لجرائم إلكترونية مدعومة بتقنيات الذكاء الاصطناعى.

ج. **المجال الزمنى** : انقسم المجال الزمنى للدراسة الميدانية إلى ثلاث مراحل :

- المرحلة الاستطلاعية.
- مرحلة إعداد وتصميم دليل دراسة الحالة.
- مرحلة جمع البيانات وتحليلها

وقد امتدت هذه المراحل خلال الفترة من مايو ٢٠٢٤م إلى أغسطس ٢٠٢٤م

٦.عينة البحث:

أ.نوع العينة وطريقه اختيارها:

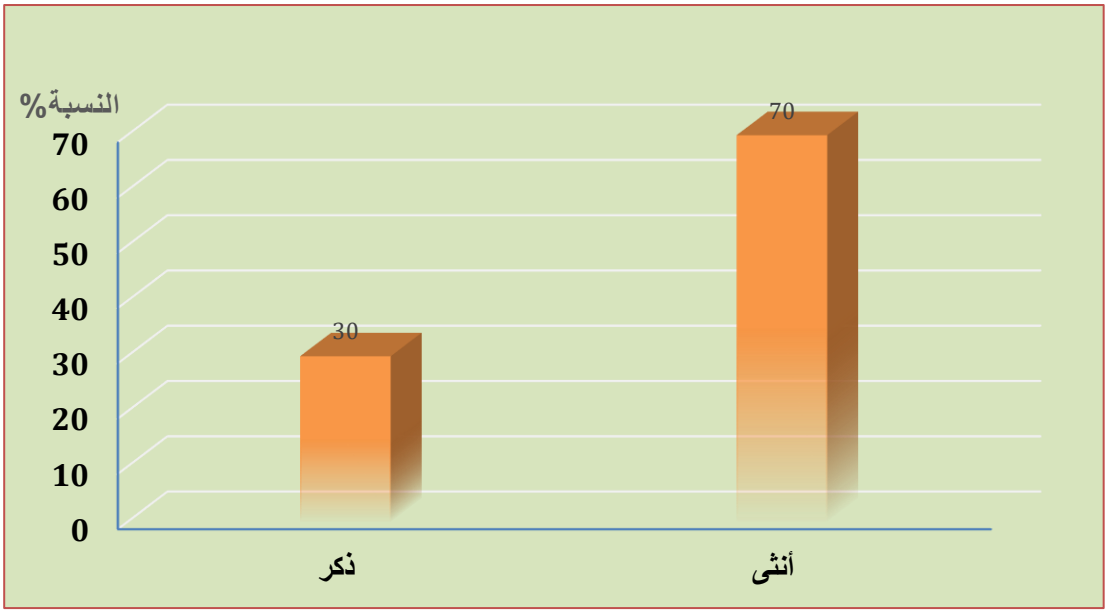
تمثلت عينة البحث فى عينة عمدية باستخدام طريقة " كرة الثلج" ، حيث تم فى البداية اختيار مجموعة صغيرة من ضحايا الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، ثم توسعت العينة تدريجياً من خلال ترشيحات المبحوثين والمخبرين الذين شملتهم الدراسة فى مرحلتها الأولى ، مما ساهم فى الوصول إلى بقية الضحايا المستهدفين .

ب: خصائص عينة البحث:

جدول(١)توزيع أفراد العينة حسب النوع

النوع	العدد	النسبة%
ذكر	٦	٣٠
أنثى	١٤	٧٠
الإجمالى	٢٠	١٠٠

المصدر:من حساب الباحث اعتمادا على دراسة الحالات



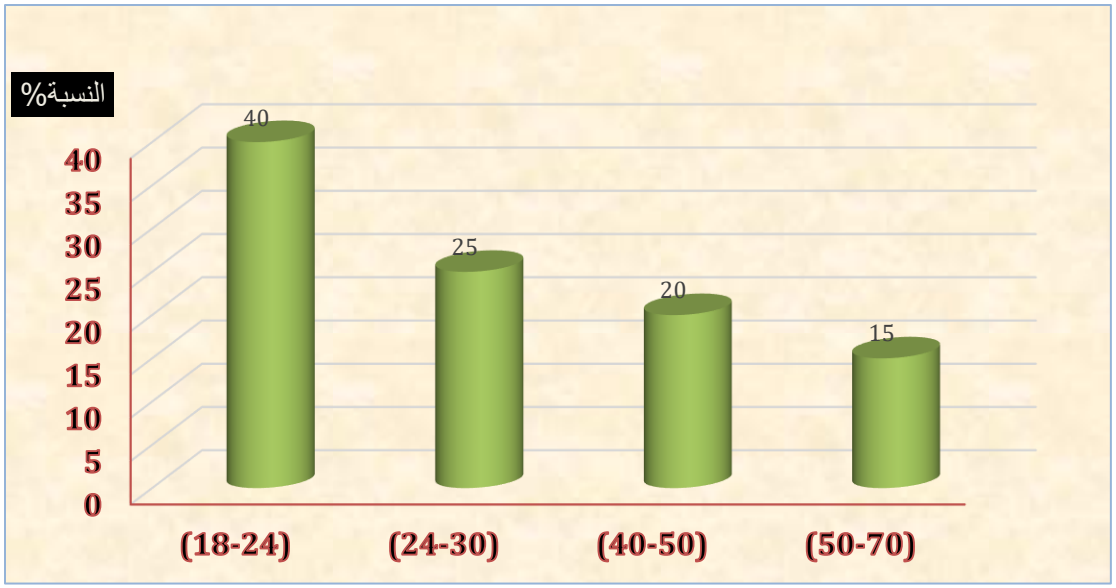
شكل(١) نسبة توزيع أفراد العينة حسب النوع

يتضح من الجدول(١)والشكل(١) أن عدد ضحايا الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى من الإناث (**١٤ فرداً بنسبة٧٠٪**) يفوق عدد الضحايا من الذكور(**٦ أفراد بنسبة ٣٠٪**) ، ويشير ذلك إلى أن النساء أكثر عرضة للجرائم الإلكترونية مقارنة بالرجال ضمن عينة البحث ، ويعود ذلك إلى أن النساء غالباً ما يكن هدفاً رئيسياً لجرائم الابتزاز الإلكترونى والتشهير نظراً للطبيعة الاجتماعية لهذه الجرائم ، حيث يتم استغلال صورهن أو بياناتهن الشخصية فى عمليات الاحتيال والابتزاز ، كما أن المجرمين يستغلون تقنيات الذكاء الاصطناعى لإنشاء صور ومقاطع فيديو مزيفة ، مما يزيد من احتمالية تعرض النساء للابتزاز والتشهير عبر وسائل التواصل الاجتماعى ، بالإضافة إلى ذلك تساهم الأدوات الحديثة مثل برامج Deepfake فى تسهيل استهداف النساء باستخدام صورهن دون علمهن ، مما يشكل تهديداً كبيراً لخصوصيتهن وأمنهن الرقمى

جدول(٢)توزيع أفراد العينة حسب الفئة العمرية

الفئة العمرية	العدد	النسبة%
(١٨-٢٤)	٨	٤٠
(٢٤-٣٠)	٥	٢٥
(٤٠-٥٠)	٤	٢٠
(٥٠-٧٠)	٣	١٥
الاجمالى	٢٠	١٠٠

المصدر:من حساب الباحث اعتمادا على دراسة الحالات



شكل(٢) نسبة توزيع أفراد العينة حسب الفئة العمرية

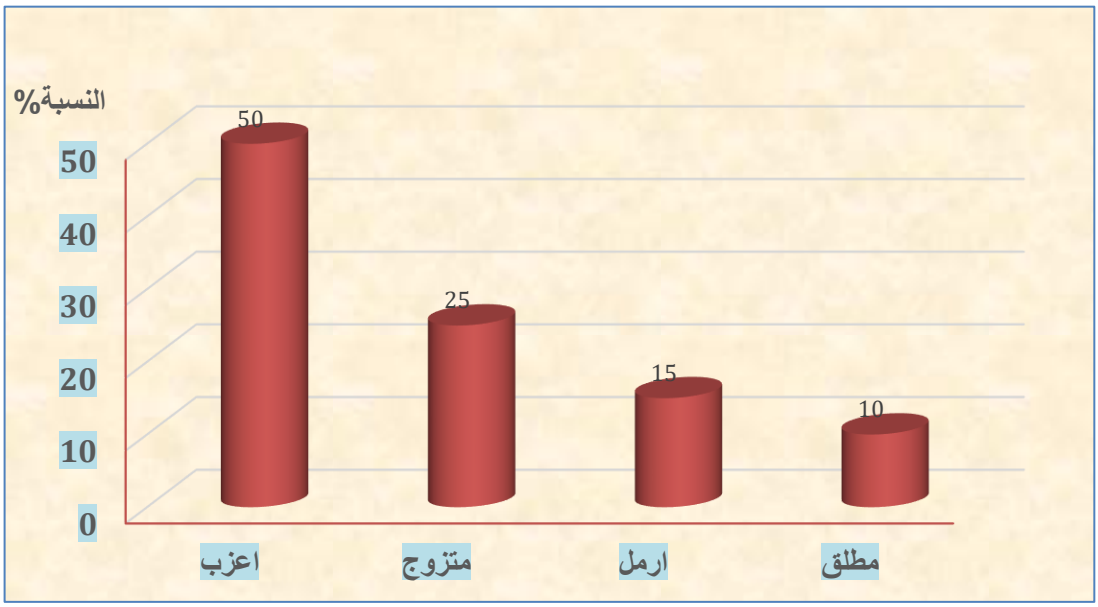
يتضح من الجدول(٢)والشكل(٢) أن الفئة العمرية (١٨-٢٤ سنة) تمثل النسبة الأكبر بين الضحايا ، حيث جاءت فى المرتبة الأولى بنسبة ٤٠٪ من عينة البحث ، ويعود ذلك إلى أن هذه الفئة تعد الأكثر نشاطاً على الإنترنت ووسائل التواصل الاجتماعى ، مما يجعلها أكثر عرضة للجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى مثل الابتزاز والتشهير وسرقة الحسابات ، كما أن قلة الخبرة الرقمية وضعف الوعى بمخاطر الأمن السيبرانى يزيدان من احتمالية تعرضهم لهذه الجرائم ، وفى المرتبة الثانية جاءت الفئة العمرية (٢٤-٣٠سنة) بنسبة٢٥٪ من عينة البحث ففى هذه المرحلة العمرية يتمتع الأفراد بمزيد من الاستقلالية ويعتمدون على الإنترنت فى مجالات متعددة ، مثل العمل والتواصل الاجتماعى مما يجعلهم أكثر عرضة للاحتيال الإلكترونى أو الاختراقات المالية ، أما الفئة العمرية

(٤٠-٥٠سنة) فقد احتلت المرتبة الثالثة بنسبة ٢٠٪ ورغم أن نشاط هذه الفئة على الإنترنت أقل مقارنة بالشباب ، إلا أنهم يقعون ضحايا للاحتيال المالى والاختراقات الإلكترونية بسبب استخدامهم المتزايد للخدمات الرقمية دون دراية كافية بأساليب تأمين بياناتهم ، ويعد التصيد الاحتيالى والاحتيال عبر البريد الإلكترونى من أبرز الجرائم التى تستهدفهم ، وأخيراً جاءت الفئة العمرية (٥٠-٧٠سنة) فى المرتبة الرابعة والأخيرة بنسبة ١٥٪ ، ورغم انخفاض مستوى تفاعلهم مع الإنترنت ،إلا أنهم يظلون عرضة للاحتيال المالى خاصة بسبب قلة وعيهم بتطور تقنيات الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى.

جدول(٣)توزيع أفراد العينة حسب الحالة الإجتماعية

الحالة الاجتماعية	العدد	النسبة%
اعزب	١٠	٥٠
متزوج	٥	٢٥
ارمل	٣	١٥
مطلق	٢	١٠
الاجمالى	٢٠	١٠٠

المصدر:من حساب الباحث اعتمادا على دراسة الحالات



شكل(٣)توزيع أفراد العينة حسب الحالة الإجتماعية

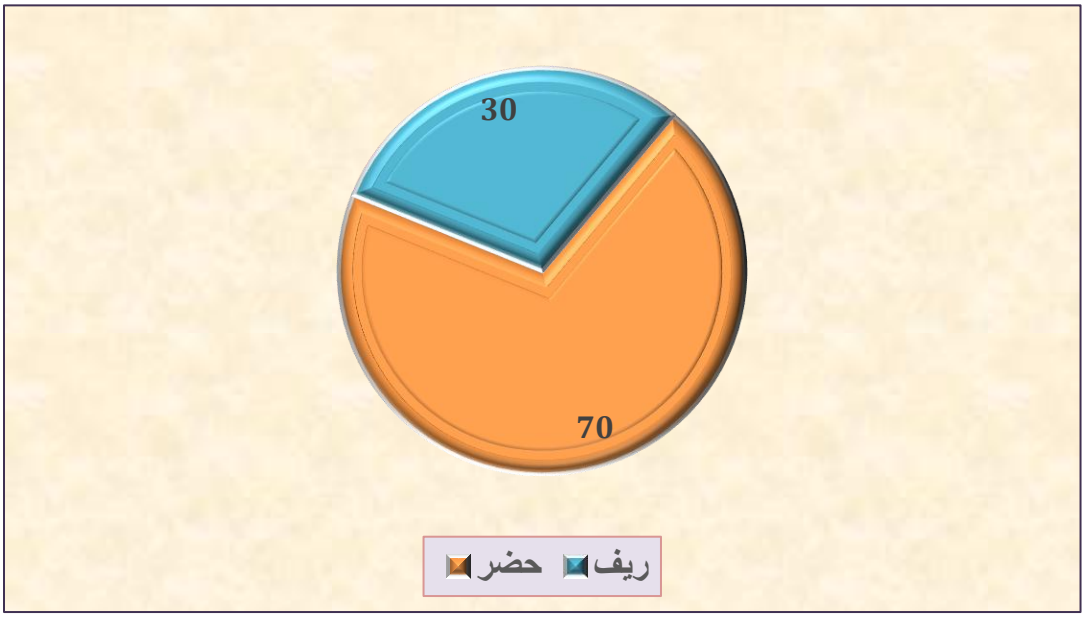
يتضح من الجدول(٣) والشكل (٣) أن الفئة الأكثر تأثراً بالجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى هى فئة العزاب ، حيث جاءت فى المرتبة الأولى بنسبة ٥٠٪ من عينة البحث ، ويرجع ذلك إلى أن الأعزب يكون أكثر نشاطاً على الإنترنت ووسائل التواصل الاجتماعى ، مما يجعله

أكثر عرضة للابتزاز الإلكترونى ، والاحتيال ، وسرقة البيانات الشخصية ، كما أن قلة المسؤوليات العائلية قد تدفع البعض إلى التفاعل الرقمى بشكل أكثر اندفاعاً ، مما يزيد من مخاطر استهدافهم من قبل مجرمى الجرائم الإلكترونية ، وتأتى فئة المتزوجين فى المرتبة الثانية بنسبة ٢٥٪ من عينة البحث ، ورغم انشغالهم بالحياة الأسرية ، فإنهم قد يكونون عرضة للاحتيال المالى والاختراقات الإلكترونية وسرقة البيانات الشخصية خاصة عند استخدام الإنترنت فى التعاملات المصرفية أو التسوق الإلكترونى ، أما فئة الأرامل فقد شكلت نسبة١٥٪ من عينة البحث ، مما يشير إلى أنهم قد يكونون أهدافاً لعمليات الاحتيال العاطفى أو المالى ، حيث قد يستغل المحتالون قلة خبرتهم فى التعامل مع التقنيات الحديثة أو حاجتهم للتواصل الاجتماعى ، وأخيراً تمثل فئة المطلقين نسبة ١٠٪ ، حيث يكونون عرضة للجرائم الإلكترونية نتيجة البحث عن التواصل الاجتماعى بعد الطلاق ، أو التعرض لمحاولات تشهير وابتزاز من أطراف أخرى.

جدول(٤)توزيع أفراد العينة حسب محل الإقامة

محل الاقامة	العدد	النسبة%
حضر	١٤	٧٠
ريف	٦	٣٠
الاجمالى	٢٠	١٠٠

المصدر:من حساب الباحث اعتمادا على دراسة الحالات



شكل(٤)توزيع أفراد العينة حسب محل الإقامة

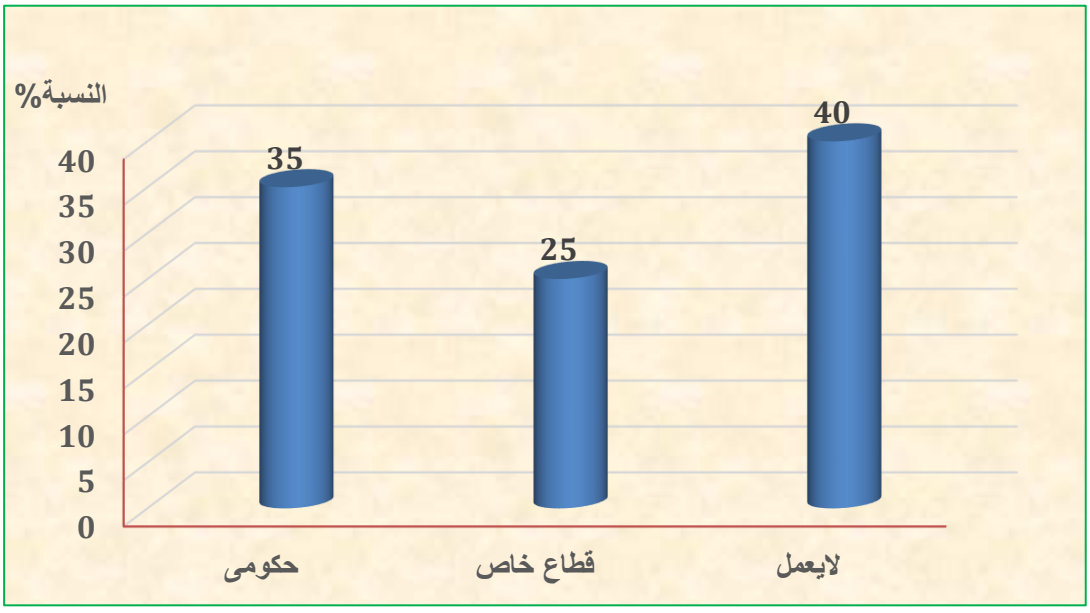
يتضح من الجدول (٤) والشكل(٤) أن النسبة الأكبر من ضحايا الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى هم سكان الحضر ، حيث بلغت نسبتهم ٧٠٪ من عينة البحث ، بينما جاءت

نسبة الضحايا من سكان الريف فى المرتبة الثانية بنسبة ٣٠٪ من عينة البحث ، ويمكن تفسير ذلك بعدة عوامل منها أن سكان الحضر أكثر استخداماً للتكنولوجيا والإنترنت فى حياتهم اليومية ، سواء فى العمل أو الترفيه أو التواصل الاجتماعى ، مما يزيد من فرص تعرضهم للجرائم الإلكترونية ، بالإضافة إلى ذلك فإن كثافة النشاط الرقمى فى المدن تسهل استهداف الأفراد بجرائم مثل الاحتيال الإلكترونى والابتزاز والاختراقات المختلفة ، أما سكان الريف فرغم تزايد استخدامهم للإنترنت ، إلا أن طبيعة الحياة الريفية قد تجعلهم أقل عرضة لمثل هذه الجرائم مقارنة بسكان المدن ، حيث يكون التفاعل الرقمى أقل نسبياً ، مما يقلل من فرص وقوعهم ضحايا للجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى.

جدول(٥)توزيع أفراد العينة حسب المهنة

المهنة	العدد	النسبة%
حكومى	٧	٣٥
قطاع خاص	٥	٢٥
لايعمل	٨	٤٠
الاجمالى	٢٠	١٠٠

المصدر:من حساب الباحث اعتمادا على دراسة الحالات



شكل(٥)توزيع أفراد العينة حسب المهنة

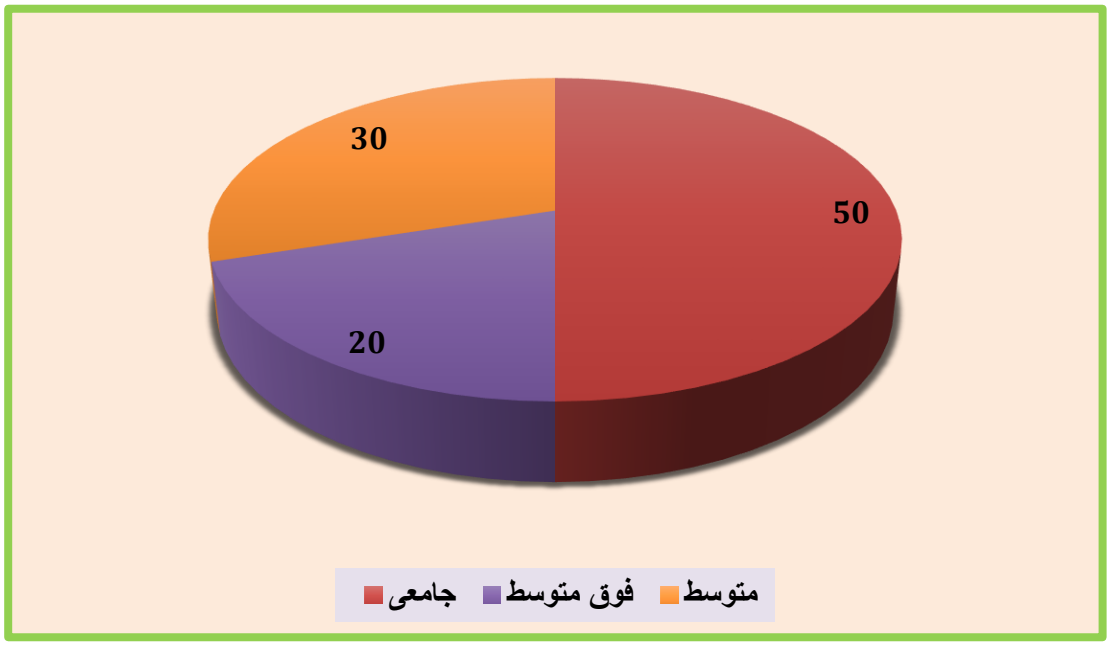
يتضح من الجدول(٥) والشكل (٥) أن الفئة الأكثر تأثراً بالجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى هم الأفراد غير العاملين ، حيث بلغت نسبتهم ٤٠٪ من عينة البحث ، وهو ما يتماشى مع الفئة العمرية الأكثر تضرراً (١٨-٢٤ سنة) التى جاءت فى المرتبة الأولى بنسبة ٤٠٪ ، يمكن تفسير ذلك بأن الأفراد غير العاملين يقضون وقتاً أطول على الإنترنت ووسائل التواصل الاجتماعى

، مما يزيد من فرص تعرضهم للجرائم الإلكترونية مثل الاحتيال والابتزاز وسرقة البيانات ، وتأتى الفئة العاملة فى القطاع الحكومى فى المرتبة الثانية بنسبة ٣٥٪ ، ويرجع ذلك إلى استخدامهم المتكرر للإنترنت فى بيئة العمل ، مما يعرضهم لمحاولات التصيد الاحتيالى والاختراقات الأمنية ، خاصة فى حال عدم اتباع إجراءات الحماية الرقمية بشكل كاف ، أما الفئة العاملة فى القطاع الخاص فقد جاءت فى المرتبة الثالثة بنسبة ٢٥٪ ويعود ذلك على الأرجح إلى التزامهم الأكبر بإجراءات الأمن السيبرانى التى تفرضها بيئات العمل الأكثر صرامة ، أو إلى قلة انخراطهم فى الاستخدام غير الآمن للإنترنت مقارنة بالفئتين الأخريين.

جدول(٦)توزيع أفراد العينة المستوى التعليمي

المستوى التعليمى	العدد	النسبة%
جامعى	١٠	٥٠
فوق متوسط	٤	٢٠
متوسط	٦	٣٠
الاجمالى	٢٠	١٠٠

المصدر:من حساب الباحث اعتمادا على دراسة الحالات



شكل(٦)توزيع أفراد العينة المستوى التعليمي

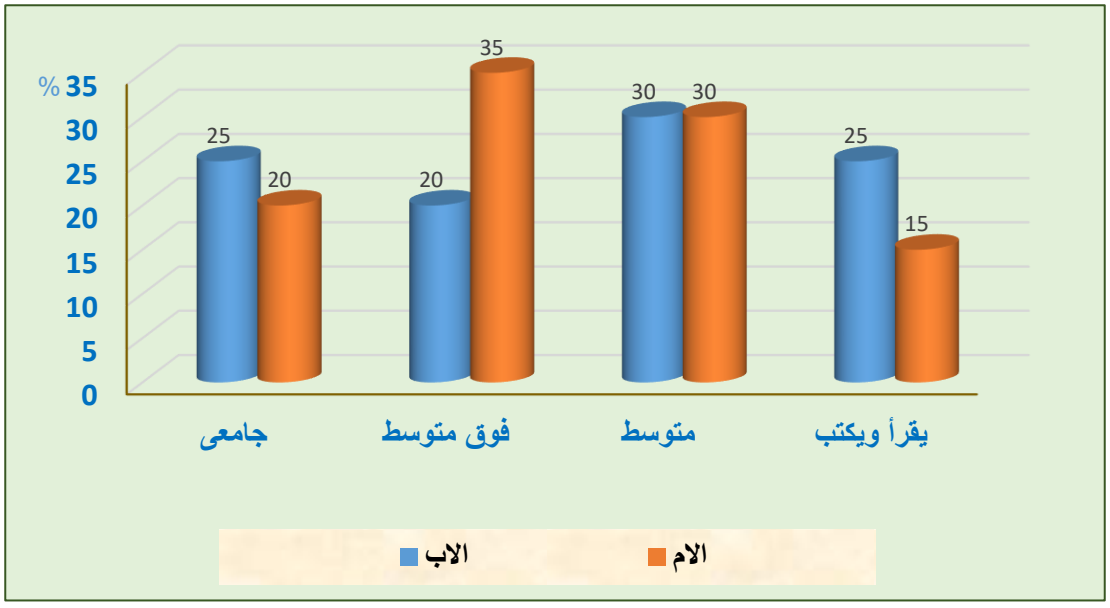
يتضح من الجدول(٦) والشكل (٦) أن الفئة الأكثر تأثراً بالجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى هى فئة الحاصلين على التعليم الجامعى حيث جاءت فى المرتبة الأولى بنسبة بلغت ٥٠٪ من عينة البحث ، ويمكن تفسير ذلك بأن هذه الفئة تعتمد بشكل كبير على الإنترنت ووسائل

التواصل الاجتماعى فى الدراسة والعمل والتواصل ، مما يزيد من احتمالية تعرضهم للاختراقات الإلكترونية والاحتيال والابتزاز عبر الإنترنت ، تأتى فى المرتبة الثانية فئة الحاصلين على التعليم المتوسط بنسبة ٣٠٪، وقد يكون ذلك بسبب قلة وعيهم بمخاطر الأمن السيبرانى ، مما يجعلهم أكثر عرضة للهجمات الإلكترونية مثل التصيد الاحتيالى وسرقة البيانات الشخصية ، أما فئة الحاصلين على التعليم فوق المتوسط فقد جاءت فى المرتبة الثالثة بنسبة ٢٠٪ فقد يشير ذلك إلى أن هذه الفئة تمتلك قدراً من المعرفة والوعى التقنى الذى يساعدهم فى تجنب بعض المخاطر الإلكترونية ، لكنهم لا يزالون عرضة للهجمات الإلكترونية بسبب الاستخدام اليومى للإنترنت فى حياتهم الشخصية والمهنية.

جدول(٧)توزيع أفراد العينة المستوى التعليمي للأب والأم

المستوى التعليمى	الأب	النسبة%	الأم	النسبة%
جامعى	٥	٢٥	٤	٢٠
فوق متوسط	٤	٢٠	٧	٣٥
متوسط	٦	٣٠	٦	٣٠
يقرأ ويكتب	٥	٢٥	٣	١٥
الاجمالى	٢٠	١٠٠	٢٠	١٠٠

المصدر:من حساب الباحث اعتمادا على دراسة الحالات



شكل(٧)توزيع أفراد العينة المستوى التعليمي للأب والأم

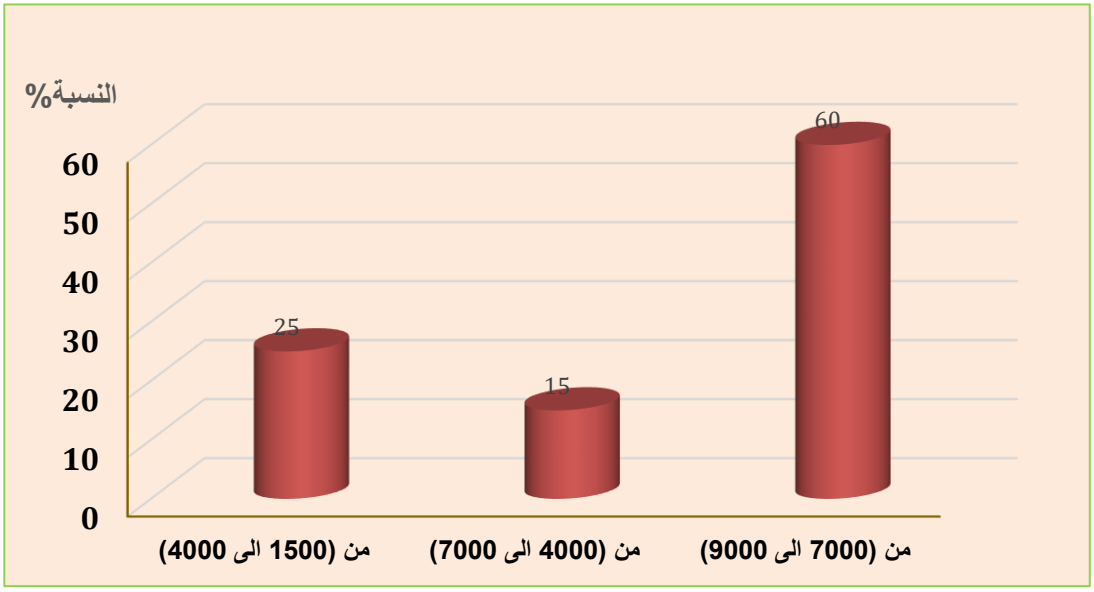
يتضح من الشكل(٧) والجدول(٧) أن مستوى التعليم لدى والدى الضحايا يتفاوت ، مما قد يؤثر على الوعى الرقمى للأبناء وقدرتهم على تجنب الوقوع فى الجرائم الإلكترونية ، وبالنسبة لمستوى تعليم الأب أتضح ان الفئة الأكثر شيوعاً هى الحاصلون على تعليم متوسط بنسبة ٣٠٪ ، يليها الحاصلون

على تعليم جامعى تساوت معها فى المرتبة ذاتها والنسبة نفسها الذين يقرؤون ويكتبون بنسبة ٢٥٪ لكل منهما ، وأخيراً الحاصلون على تعليم فوق المتوسط بنسبة ٢٠٪ ، وهذا يشير إلى أن معظم الآباء لديهم مستوى تعليمى متوسط أو أقل ، مما قد يؤدى إلى محدودية معرفتهم بالمخاطر الإلكترونية وكيفية توجيه أبنائهم بشأن الأمان الرقمى ، وبالنسبة لمستوى تعليم الآم فالفئة الأكثر انتشاراً هى الحاصلات على تعليم فوق المتوسط بنسبة ٣٥٪ ، تليها الحاصلات على تعليم متوسط بنسبة ٣٠٪ ، ثم الحاصلات على تعليم جامعى بنسبة ٢٠٪ ، وأخيراً الأمهات اللاتى يقرأن ويكتبن فقط بنسبة ١٥٪ ، ويشير ذلك إلى أن مستوى التعليم لدى الأمهات أقل نسبياً مقارنة بالآباء ، مما قد ينعكس على قدرة الأسرة على توجيه الأبناء فى التعامل مع الإنترنت بشكل آمن .

جدول(٨)توزيع أفراد العينة الدخل الشهرى

الدخل الشهرى	العدد	النسبة%
من (١٥٠٠ الى ٤٠٠٠)	٥	٢٥
من (٤٠٠٠ الى ٧٠٠٠)	٣	١٥
من (٧٠٠٠ الى ٩٠٠٠)	١٢	٦٠
الإجمالى	٢٠	١٠٠

المصدر:من حساب الباحث اعتمادا على دراسة الحالات



شكل(٨)توزيع أفراد العينة الدخل الشهرى

يتضح من الجدول(٨) والشكل (٨) أن الفئة الأكثر تأثراً بالجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى هى الفئة ذات الدخل الشهرى من ٧٠٠٠ إلى ٩٠٠٠ وجاءت فى المرتبة الأولى وبلغت نسبتهم ٦٠٪ من عينة البحث ، ويمكن تفسير ذلك بأن هذه الفئة تمتلك القدرة المالية التى تجعلها

هدفاً جذاباً للمجرمين الإلكترونيين ، حيث يكونون أكثر عرضة للاحتيال المالى ، واختراق الحسابات البنكية والابتزاز الإلكترونى نظراً لإمكاناتهم المادية ، تأتى فى المرتبة الثانية ذات الدخل الشهرى من ١٥٠٠ إلى ٤٠٠٠ بنسبة ٢٥٪ ، وقد يكون ذلك بسبب استخدامهم الإنترنت بشكل مكثف فى البحث عن فرص عمل أو الحصول على خدمات مجانية ، مما يزيد من احتمالية تعرضهم للتصيد الاحتيالى أو الاختراقات الرقمية ، أما الفئة ذات الدخل من ٤٠٠٠ إلى ٧٠٠٠ ، فقد جاءت فى المرتبة الثالثة بنسبة ١٥٪ ، وقد يشير ذلك إلى أن هذه الفئة تمتلك مستوى وعى أعلى بالمخاطر الإلكترونية أو أن نمط إنفاقهم الرقمى أقل مقارنة بالفئة الأعلى دخلاً ، مما يجعلهم أقل استهدافاً من قبل المجرمين الإلكترونيين.

تاسعاً:تحليل نتائج البحث الميدانى ومناقشتها فى ضوء الأهداف والبحوث والدراسات السابقة والتوجه النظرى للبحث:

١- النتائج المتعلقة بدور الذكاء الاصطناعى فى إرتكاب الجرائم الإلكترونية:

أ. تنوعت الجرائم الإلكترونية التى ارتكبها المجرمون بمساعدة تقنيات الذكاء الاصطناعى وتمثلت فى جرائم الابتزاز والتشهير ، جرائم سرقه حساب بنكى ، جرائم سرقة حسابات شخصية عبر مواقع التواصل الاجتماعى ، جرائم سرقة واختراق إلكترونى ، جرائم الابتزاز الجنسى ، جرائم الهاكرز ، جرائم النصب والاحتيال الإلكترونى ، جرائم تشويه السمعة والانتقام، وتتفق هذه النتيجة مع ماجاءت به دراسة**(الحوتى،٢٠٢٠)** فى تنوع أنماط الجرائم الإلكترونية ما بين التشهير واختراق الحسابات البنكية وسرقة بطاقات الائتمان والتهديد والابتزاز عبر الانترنت.

ب. أوضحت حالات الدراسة الميدانية أن الجرائم التى تعرض لها الضحايا وقعت منذ ما يقرب من عام إلى ثمانية أشهر، أو خلال فترة علاقة المجرم بالضحية ، كما تزامنت بعض هذه الجرائم مع وصول الحساب الشخصى للضحية إلى ٥٠ ألف متابع ، وقد شهدت تقنيات الذكاء الاصطناعى تطورات هائلة فى السنوات الأخيرة ، مما سهل على المجرمين استخدامها لتطوير أدوات وتقنيات إجرامية أكثر تطوراً ، كما أن توفر أدوات الذكاء الاصطناعى بشكل واسع جعل من السهل على المجرمين الوصول إليها واستغلالها فى تنفيذ جرائمهم ، وتتفق هذه النتيجة مع ماجاءت به دراسة **(الشهومية ،والكندى،٢٠٢٤)** فى ان تطبيقات الذكاء الاصطناعى قد تستخدم فى ارتكاب جرائم معلوماتية كالابتزاز الإلكترونى وسرقة الهويات

ج. وعن آلية تنفيذ الجرائم الإلكترونية بمساعدة الذكاء الاصطناعى، نجد انه أستغل المجرمون بناء علاقات عاطفية مع الضحايا ، وكسب ثقتهم ، ثم استغلالهم مالياً للحصول على معلومات

حساسة وتذكر أحدى حالات الدراسة "**ان المجرم قام بأخذ الباسورد الخاص بالإيكلود الخاص بالشركة اثناء تواجده بمفرده بمقر الشركة وهذا لأننا كنا واثقين فيه** "، كما يمكن للذكاء الاصطناعى تحليل بيانات الضحية من مصادر متعددة ، مثل وسائل التواصل الاجتماعى وسجلات الشراء لإنشاء رسائل تصيد مخصصة للغاية ، فيمكن لهذه الرسائل أن تستغل نقاط الضعف العاطفية للضحية أو اهتماماتها ، مما يزيد من فرص نجاحها وتذكر أحدى حالات الدراسة" **المجرم استخدم الذكاء الاصطناعى لإنشاء صور مزيفة بناءً على صور متاحة على وسائل التواصل الاجتماعى وقام بأبتزازى بها**" ، كما يتم استخدام تقنيات التزييف العميق لإنشاء مقاطع فيديو أو تسجيلات صوتية مزيفة تبدو وكأنها من مصادر موثوقة وتذكر أحدى حالات الدراسة "**قام المجرم بأنتحال شخصية أنثى مطالباً منى التحدث بريكوردات عن طريق تطبيق الواتس آب ، قام بأخذ الريكوردات وقام بإنشاء مقاطع صوتية تفيد بأننى شاذ جنسياً وطلب منى مبلغ كبير من المال لعدم نشر هذه المقاطع** " ، كما يتم استخدام الذكاء الاصطناعى لإنشاء هويات مزيفة ، وارتكاب عمليات احتيال مالى ، وانتحال الشخصية للحصول على مبالغ مالية وتذكر أحدى حالات الدراسة "**تم تهكير حسابى الشخصى وطلب المجرم من أقاربى ومعارفى مبالغ ماليه متنوعة عن طريق ارسال الرسائل عن طريق مواقع التواصل الاجتماعى وتم بالفعل حصوله على مبالغ ماليه**" ، وتتفق هذه النتيجة مع ماجاءت به دراسة **(Carla,Irina,2023)** فى ان مجرمى الإنترنت يستخدمون تكنولوجيا الذكاء الاصطناعى لتنفيذ الهجمات الإلكترونية.

نستنتج مما سبق تعدد وتنوع الجرائم الإلكترونية التى ترتكب باستخدام تقنيات الذكاء الاصطناعى ، والتى تشمل الابتزاز والتشهير ومراقبة الأنشطة وسرقة الحسابات الشخصية عبر مواقع التواصل الاجتماعى ، بالإضافة إلى جرائم الاختراق الإلكترونى والابتزاز الجنسى وعمليات الاحتيال الإلكترونى وهجمات القراصنة (الهاكرز) ، ويعود هذا التنوع إلى التطور التكنولوجى المستمر وزيادة التواصل الرقمى وصعوبة كشف هذه الجرائم ، كما أن استغلال العلاقة مع الضحية يسهل على المجرمين جمع المعلومات الشخصية والتلاعب بها ، بينما يجعل ارتفاع عدد المتابعين الضحية هدفاً جذاباً ، حيث يمكن استغلال شهرتها لتحقيق مكاسب غير مشروعة ، ويظهر استخدام تقنيات الذكاء الاصطناعى الحديثة تطور أساليب المجرمين ، ويعكس التسلسل الزمنى لهذه الجرائم استراتيجياتهم فى توظيف هذه التقنيات لتسهيل أعمالهم الإجرامية ، وتتفق هذه النتيجة مع ماجاءت به دراسة **(الهديف ،٢٠٢٢)** فى ان الجرائم الإلكترونية تتميز بتنوعها من حين إلى آخر وهذا بفعل التطور التكنولوجى ، وهذا ما أكدته

نظرية(**الاستخدامات والإشباعات**) ، حيث تشير إلى أن الجناة يستخدمون تقنيات الذكاء الاصطناعى لإشباع دوافعهم الإجرامية ، وذلك وفقاً للفروق الفردية بينهم ، فبينما يفضل بعض المجرمين ارتكاب جرائم الابتزاز الإلكترونى من خلال استغلال الضحايا للحصول على مكاسب مادية أو معنوية ، نجد أن آخرين يركزون على سرقة بيانات البطاقات الائتمانية لتحقيق أرباح مالية غير مشروعة.

أما فيما يتعلق بآلية تنفيذ الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى فقد تعددت وتنوعت نتيجة الفرص الكبيرة التى تتيحها هذه الجرائم لتحقيق أرباح مالية ضخمة ، مما يدفع المجرمين إلى استخدام أحدث التقنيات لتعظيم مكاسبهم ، كما يساعد الذكاء الاصطناعى فى إخفاء هوية المجرمين وتتبع آثارهم على الإنترنت ، مما يجعل من الصعب على الجهات الأمنية تعقبهم ، وبالتالى فإن تنوع أساليب تنفيذ هذه الجرائم يعود إلى القدرة المتزايدة للمجرمين على استغلال التقنيات المتقدمة لتحقيق أهدافهم الإجرامية ، ويمكن مناقشة هذا فى ضوء ما أشار إليه **(كوهين وفيلسون)** فى نظريتهم حول النشاط الروتينى ، حيث أوضحا أنه منذ ظهور الإنترنت وانتشاره السريع ،أصبحت الجرائم التى لا يتلامس فيها الضحايا والجناة جسدياً أكثر شيوعاً وقابلية للتطبيق فى سياق الجرائم الإلكترونية المدعومة بالذكاء الاصطناعى ، فإن زيادة النشاط الرقمى خاصة بين الفئات ذات الدخل المرتفع جعلتهم أهدافاً رئيسية للمجرمين الإلكترونيين ، مما يؤكد ان سهولة تنفيذ الجريمة الإلكترونية وعدم الحاجة إلى تلامس جسدى بين الضحية والجانى يجعلها أكثر أنتشاراً وتأثيراً فى العصر الرقمى.

٢-النتائج المتعلقة بالأسباب المؤدية للجريمة الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى من وجهة نظر الضحية:

أ. الأسباب الاجتماعية المؤدية إلى ارتكاب الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى من وجهة نظر الضحايا

هناك عدة أسباب اجتماعية تؤدى إلى ارتكاب الجرائم الإلكترونية المدعومة بالذكاء الاصطناعى ومن أبرزها مايلى:

- **التفكك الأسرى وضعف الرقابة العائلية:**

فغياب التوجيه والرقابة من الأهل يؤدى إلى انحراف بعض الأفراد نحو استخدام تكنولوجيا الذكاء الاصطناعى بطرق غير قانونية ، كما أن الأسر المفككة أو التى تعانى من ضعف الترابط ، قد يفتقد الأبناء التوجيه القيمى والأخلاقى ، مما يجعلهم أكثر عرضة لأستخدام التكنولوجيا بطرق غير مشروعة ، ففى بعض الأسر لا يوجد وعى كاف بضرورة مراقبة أنشطة الأبناء على الإنترنت ، مما يسهل تعرضهم لمحتوى مشجع على الجرائم الإلكترونية ، وتذكر احدى حالات الدراسة " **كان**

ابنى عمى عايز يتزوجنى ولما رفضت قام بتشويه سمعتى على الانترنت وقام بإنشاء صوت مماثل لصوتى معتمداً على برامج الذكاء الاصطناعى" وبسؤال الحاله عن السبب فى قيام الجانى بإرتكاب هذه الجريمه ردت قائله "**والده ووالدته منفصلين عن بعض والجانى عايش لوحده وأى فكره غير مشروعة تأتى له يقوم بتنفيذها**"، وتذكر ايضاً احدى الحالات الأخرى "**فى بينى وبين طليقى مشاكل واستغل صفحه الفيس بوك الخاصه بى وابتدى يكلم زمايلى ويرسل لهم صور خاصه بيا**" ، وتتفق هذه النتيجة مع ماجاءت به دراسة(**الأميرى،والعموش،٢٠٢٢**) فى ان أكثر ضحايا استعمال التكنولوجيا كان لهم أثر فيما أصابهم فما أن وجد جانى وضحية فى مكان وزمان مع غياب الرقابة الأسرية ، وتتفق ايضاً مع ماجاءت به دراسة **(ابراهيم،٢٠٢٣)** فى ان من أهم الاسباب الاجتماعية المؤدية للتنمر الإلكترونى ترجع إلى التنشئة الاجتماعية الخاطئة للأبناء ، وضعف الرقابة الأسرية عليهم.

ونستنتج مما سبق عدم وجود قيود على الأجهزة والتطبيقات يجعل من السهل الوصول إلى أدوات الذكاء الاصطناعى التى يمكن استغلالها فى الاحتيال والاختراقات ، ويؤدى ذلك الى وقوع الضحايا لعمليات الابتزاز الإلكترونى عبر الإنترنت نتيجة قلة الرقابة الأبوية والتفكك الأسرى ، حيث يستغل المجرمون الذكاء الاصطناعى لتزوير الصور وإنشاء محتوى مزيف لإجبار الضحايا على دفع المال وتفيذ طلبات غير مشروعة وغير قانونية

- **ضعف الرقابة المجتمعية:**

يؤدى غياب الرقابة المجتمعية على استخدام الإنترنت إلى زيادة احتمالية ارتكاب الجرائم الإلكترونية ، كما ان ضعف البرامج التوعوية وغياب الرقابة الفعالة يعززان خطورة هذه الجرائم ، لذلك يجد الجناة فى الفضاء الإلكترونى وسيلة لتعويض النقص العاطفى ، مما يدفعهم إلى استغلال تقنيات الذكاء الاصطناعى بطرق غير مشروعة ، مثل الابتزاز أو إنتاج محتوى إباحى مزيف أو إنشاء هويات مزيفة ، وذلك فى ظل غياب الرقابة المجتمعية على هذه الأفعال الإجرامية ، وتشير إحدى حالات الدراسة إلى "**قام احد الأشخاص بتهكير التليفون الخاص بى قام بإرسال لينك وقمت بالضغط عليه وسرق كل الصور والفيديوهات وابتزنى بيها** " وبسؤالها عن سبب الجريمة الإلكترونية ردت قائلة "**غياب الرقابة المجتمعية وعدم وجود رادع لهؤلاء الجناه هو الذى دفع بهم لإرتكاب مثل هذه الجرائم الإلكترونية**"

يتبين مما سبق عندما لايشعر الأفراد بأن هناك من يراقب تصرفاتهم عبر الإنترنت ، فيميلون إلى التورط فى سلوكيات غير قانونية وغير أخلاقية ، كما يوفر الإنترنت مستوى عالى من إخفاء الهوية ، مما يشجع المجرمين على ارتكاب الجرائم دون خوف من التعرف عليهم

- **تلبيه الحاجات الاجتماعية والجنسية:**

تلعب الحاجات الاجتماعية والجنسية لدى الجناه دوراً محورياً فى تشكيل سلوكهم حيث يسعى الجناه إلى إشباع هذه الحاجات من خلال التفاعل مع الآخرين وبناء العلاقات ، ومع تطور التكنولوجيا والاعتماد المتزايد على الإنترنت ووسائل التواصل الاجتماعى ، أصبحت هذه الحاجات تلبى بطرق جديدة وحديثة ، بعضها مشروع والبعض الآخر غير مشروع ويؤدى بصاحبه الى الأنحراف وارتكاب الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، وتشير احدى حالات الدراسة "**كان لى جار يحاول التقرب منى لانى ارمله ورفضته اكثر من مره فقام بسرقه صور لى عن طريق الفيس بوك وقام بتركيب فيديوهات وصور اباحيه وقام بإبتزازى بها لكى اوافقه**"

ويتضح مما سبق ان الجناه يبحثون عن مجتمعات افتراضية ليشعروا بالانتماء والتواصل ، وقد يستغل المجرمين هذه الحاجة لتكوين علاقات زائفة واستدراج الضحايا ، كما يبحث الجناه عن الإثارة والمتعة وإنتاج محتوى إباحى غير قانونى ويلجأون إلى التحرش أو الابتزاز الجنسى كوسيلة لتلبية رغباتهم الجنسية عبر الإنترنت .

كما يعيش الكثير من الجناة نوعاً من اللاتوازن بين متطلباتهم الاجتماعية والنفسية وحتى البيولوجية الجنسية منها وبين واقعهم الاجتماعى والثقافى بحيث يفرض هذا الاخير مجموعة من الضوابط الاجتماعية والمعايير الثقافية حول كيفية وطريقة تلبية هذه المتطلبات والحاجات ، بحيث يرى المجرم فى هذه الضوابط والمعايير نوعاً من الاجحاف فى حقه وتقييداً لطموحاته ورغباته ، وهذا ما يجعله يبحث عن بيئة أخرى غير بيئته الاجتماعية يتمتع فيها بالاستقلالية والحرية ويلبى فيها مجمل رغباته واحتياجاته بكل حرية ودون قيود ورقابة ، وبالتالى أصبح الكثير من الجناه يتجهون إلى البيئة الالكترونية ، لما تقدمه من خدمات متعددة فى هذا المجال ، بحيث اصبحنا نلاحظ على مواقع التواصل الاجتماعى الكثير من الجناه الى انتحال صفة شخصيات اجتماعية معروفة (باحثين ، رياضيين ، مسؤولين كبار.. الخ) من أجل جذب الانتباه وزيادة حجم التفاعل مع أفراد المجتمع ، والحصول على مبالغ مالية غير مشروعة ، فى حين يتجه جناه آخرين الى استغلال هذه المواقع الالكترونية كمنابر للسب والشتم والقذف وتركيب الصور والفيديوهات بمساعدة تقنيات الذكاء الاصطناعى وذلك لتفريغ مختلف الضغوط الاجتماعية والنفسية التى تفرضها عليهم بعض الجوانب التى يتفاعلون معها فى حياتهم اليومية والتى قد تكون هيئات حكومية ، أو جمعيات وفرق رياضية او افراد ومسؤولين ، هذا وقد اصبح الكثير من الجناه يستغلون هذه البيئة الالكترونية لتحقيق رغباتهم الجنسية واشباع نزواتهم سواء كان ذلك بمشاهدة المواد الإباحية او نشرها والتشجيع على فعل الدعارة وتجاوز الضوابط الاجتماعية والثقافية التى تقف حاجزاً امام هذه الأفعال الاجرامية ، وعليه فهذه البيئة الالكترونية اصبحت تشكل مرتعاً يساهم فى اغراء ودفع هؤلاء

الجناه على الادمان على مثل تلك السلوكيات الاجرامية.(عيسات ،وبوعزة،٢٠٢٢، ص ص ١٣٧-١٣٨) ، وهذا ما أكده **(كوهين وفيلسون)** فى تفسيرهما ، حيث أشارا إلى أن عدم اهتمام الآباء بأبنائهم ، وعدم متابعتهم ومراقبتهم ، يعد من العوامل الأساسية التى تؤدى إلى ضعف مستوى ضبط الذات لدى الأبناء ، فمع انشغال الآباء وإهمالهم للإشراف على سلوكيات أبنائهم ، يصبح هؤلاء الأبناء عرضة للإهمال النفسى والعاطفى والتربوى ، مما يجعلهم أكثر تأثراً بالمؤثرات الخارجية السلبية ، وفى ظل هذا الضعف فى دور الأسرة ، يكون الأبناء غير محصنين ضد الأفكار الإجرامية ، مما يجعلهم أهدافاً سهلة للتورط فى الجرائم الإلكترونية المختلفة ، خاصة تلك المدعومة بتقنيات الذكاء الاصطناعى ، فغياب الرقابة الأسرية قد يدفع الأبناء إلى الانخراط فى أنشطة غير مشروعة ، مثل القرصنة الإلكترونية والانخداع بأساليب الاحتيال الإلكترونى أو حتى الوقوع كضحايا للابتزاز والاستغلال عبر الإنترنت.

ب- الأسباب الاقتصادية المؤدية إلى ارتكاب الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى من وجهة نظر الضحايا:

تلعب الأسباب الاقتصادية دوراً محورياً فى انتشار الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ومن ابرزها ما يلى:

- **الضغوط الاقتصادية والرغبة فى الثراء :**

يعد الدافع المالى أحد أهم الأسباب لإرتكاب الجرائم الإلكترونية خاصة مع استخدام تقنيات الذكاء الاصطناعى الذى يزيد من كفاءة الهجمات الإلكترونية ، حيث يسعى بعض المجرمون إلى تحقيق مكاسب سريعة وغير مشروعة من خلال الاحتيال وسرقة البيانات أو عن طريق الابتزاز الإلكترونى ، وتذكر أحدى حالات الدراسة الميدانية " **المجرم استخدم الذكاء الاصطناعى لإنشاء صور مزيفه بناءً على صور متاحة على وسائل التوصل الاجتماعى وطلب منى مبلغ ٥٠ الف جنيه لكى لا ينشر هذه الصور**" وتذكر أيضاً أحدى الحالات "**قام أحد الأشخاص بأرسال رابط على الفيس بوك فقمت بالضغط علي الرابط فقام بسرقة حسابى واخذ المعلومات الشخصية وصور خاصه على الشات وطلب منى مبلغ ١٠ ألاف جنيه حتى لا يقوم بنشر الصور والمعلومات الشخصية**" ، ويتبين لنا تنوع أشكال الجرائم الإلكترونية التى يرتكبها الأفراد بمساعدة تقنيات الذكاء الاصطناعى تحت تأثير الضغوط الأقتصادية ، فمنها إنشاء صور مزيفه لأبتزاز الضحايا ، ومنها سرقه البيانات والصور الشخصية من أجل الحصول على المال ، ففى ظل الأزمات الأقتصادية وتزايد الفقر ، يجد المجرمون فى الفضاء الإلكترونى فرصه لتحقيق مكاسب مالية غير مشروعة، وتزداد خطورة الجرائم الإلكترونية مع استخدام تقنيات الذكاء الاصطناعى التى تمكن المجرمين من

تطوير أساليب أكثر تعقيداً وخطورة فى إرتكاب جرائمهم، وتتفق هذه النتيجة مع ماجاءت دراسة **(عبدالرازق،٢٠٢١)**، فى ان الباعث على ارتكاب الجرائم الالكترونية هو الحصول على النفع المادى السريع ، كما تتفق ايضاً هذه النتيجة مع دراسة **(الهديف،٢٠٢٢)** فى ان اصحاب الجريمة الالكترونية رغبتهم فى الحصول على الأموال بطرق غير شرعية.

- **البطالة:**

تؤدى البطالة إلى ضغوط مالية كبيرة وتوفر وقت فراغ كبير، مما يمكن المجرمون والعاطلين عن العمل من استغلال هذا الوقت وتعلم تقنيات جديدة وبرامج ضارة تضر الآخرين من تركيب صور وتغيير الأصوات بأستخدام الذكاء الاصطناعى واستخدامها فى إرتكاب الجرائم الإلكترونية المختلفة ، كما تدفع المجرمون أيضاً إلى البحث عن طرق غير مشروعة بمساعدة تقنيات الذكاء الاصطناعى لكسب المال ، كما ان الجرائم الإلكترونية توفر فرصاً كبيره لتحقيق أرباح سريعة.

وكشفت التحليلات السوسيولوجية للدراسة الميدانية التى أدلت بها حالات البحث عن ارتباط البطالة بإرتكاب الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، فقد ذكرت احدى حالات الدراسة " **أعمل فى شركة توريدات قام زميل لى مفصول من العمل لسوء سلوكه بتصويرى عن طريق كاميرا صغيره مرتبطه بالتليفون الخاص به ، عند استخدامى لحمام الشركة وتواصل معى من خلال رقم مجهول وقام بطلب مبلغ مالى منى لعدم نشر الصور**" ويتضح مما سبق استخدام المجرم لكاميرا تصوير مدعومة بالذكاء الاصطناعى ومرتبطة بالتليفون الخاص به يشاهد من خلالها ما يحلو له ، فأستخدام هذه التقنية يزيد من خطورة الجريمة ، حيث يمكن لهذه الكاميرا تسجيل وتخزين ومشاركة المحتوى بكل سهولة ، كما تجمع هذه الجريمه ما بين انتهاك الخصوصيه والابتزاز ، فالبطالة أدت إلى شعور المجرم باليأس والإحباط ، مما دفعه إلى إرتكاب جريمته كوسيله للتعبير عن غضبه ويأسه ، وكوسيله أيضاً للحصول على المال ، وأكدت حالة أخرى قائلة "**أحد الأشخاص كان يدعى امتلاكه شركه تسويق إلكترونى فقمت بتزويده بالمعلومات والصور والأموال لتوفير فرصه عمل خاصه بى وبعد فترة فوجئت بأنها حاله نصب إلكترونى**"

وبشكل عام يمكن القول أن العوامل الاقتصادية المتمثلة فى الضغوط الاقتصادية والبطالة ، توفر بيئة خصبة لأنتشار الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، حيث توفر الدافع والوسائل لإرتكاب هذه الجرائم ، كما ان الرغبة فى الثراء السريع قد يدفع المجرمين إلى اللجوء إلى هذه الجرائم ، خاصة فى ظل الظروف الاقتصادية الصعبة ، وهذا ما أكده **(كوهين وفيلسون)** فى تفسيرهم ، حيث أوضحا أن مرتكبى الجرائم الإلكترونية يرتكبون جرائمهم فى العالم الافتراضى ، مدفوعين بدوافع

مختلفة تشمل تحقيق مكاسب مالية أو إشباع رغبات شخصية مثل الدوافع الجنسية ، فالجرائم الإلكترونية خاصة تلك المدعومة بتقنيات الذكاء الاصطناعى ، توفر بيئة مثالية للمجرمين ، حيث يمكنهم استغلال الضحايا دون الحاجة إلى المواجهة المباشرة ، كما أن التطور التكنولوجى أتاح للمجرمين وسائل أكثر تعقيداً مثل التصيد الاحتيالى والابتزاز الإلكترونى والتلاعب بالصور والفيديوهات عبر تقنيات التزييف العميق (Deepfake) لتحقيق أهدافهم بطرق يصعب كشفها.

ج.الأسباب الثقافية المؤدية إلى ارتكاب الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى من وجهة نظر الضحايا:

تلعب العوامل الثقاية دوراً هاماً فى زيادة احتمالية الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى من وجهة نظر الضحايا:

- **التطور التكنولوجى:**

يشمل التطور التكنولوجى مجموعة واسعة من الاختراعات والابتكارات التى غيرت الطريقة التى نعيش بها ، فأحدث الإنترنت ثورة فى الاتصالات والمعلومات ، حيث يوفر وصولاً إلى كميات هائلة من البيانات والمعلومات ، فيتيح الذكاء الاصطناعى للمجرمين تطوير أدوات هجومية متطورة مثل برامج ضارة قادرة على التكيف مع أنظمة الحماية ، وهجمات التصيد الأحتيالى ، كما يمكن للذكاء الاصطناعى أتمتة عمليات معقدة ، مما يسمح للمجرمين بتنفيذ هجمات واسعة النطاق بسرعة وكفاءة ، ويمكن أيضاً استخدام تقنيات التزييف العميق لإنشاء مقاطع فيديو وصوت مزيفة تبدو حقيقية ، مما يسهل عمليات الاحتيال والتضليل ، ولا يقف الأمر على هذا فيمكن للذكاء الاصطناعى أيضاً تحليل البيانات الشخصية للضحايا من مصادر متعددة ، وإنشاء رسائل تصيد احتيالى مخصصة ، فتذكر أحد الضحايا "**قام المجرم بإرسال رسائل بريد إلكترونى تبدو وكأنها من مصادر موثوقة لسرقة معلومات شخصية وقام بتهكير الفيزا الخاصه بى وذلك لأنى أعطيته رمز cvv الموجود على البطاقة**" ، وقد أكدت هذه الحالة على استخدام المجرم لتقنيات الذكاء الاصطناعى وانها ساعدت المجرم فى إرتكاب جريمته الإلكترونية وكان تعليقها "**التطور التكنولوجى الرهيب ساعد المجرم على ارتكاب جريمته وجهلى بالتكنولوجيا جعلنى اسمع كلامه** " وقد ذكرت أحد حالات الدراسة أيضاً" **قام شخص مجهول بالنسبة لى بإرسال صور لى إباحيه تبدو وكأنها زى الحقيقة قام بتركيبها وهذه الصور تم أنشائها بواسطة الذكاء الاصطناعى**" ، وتتفق هذه النتيجة مع ماجاءت به دراسة**(ابراهيم ،٢٠٢٣)** فى تأكيدها على ان التطور التكنولوجى يلعب دوراً هاماً فى إرتكاب الجرائم الإلكترونية

نستنتج مما سبق ان التطور التكنولوجى يتيح للمجرمين الوصول إلى أدوات وتقنيات متطورة منها الذكاء الاصطناعى مما يسهل على المجرمين ارتكاب جرائم متطورة ، ويتيح أيضاً ابتكار أساليب جديدة لإرتكاب الجرائم الإلكترونية مثل التزييف العميق **Deepfake** للأحتيال على الأفراد واستخدام الذكاء الاصطناعى لتطوير برامج ضارة متطورة.

- **التأثيرات الثقافية السلبية:**

يتعرض بعض الأفراد للمحتوى العنيف أو الإباحى عبر الأنترنت ، مما قد يؤدى إلى تشويه القيم والأخلاق ، وقد تؤثر بعض الثقافات عبر الانترنت على الأفراد وتدفعهم إلى تقليد سلوكيات ثقافية منافية لثقافة المجتمع وتذكر احد الحالات "**كنا مخطوبين وكان عايز يرجعلى وكنت رافضه تماماً وهددنى بنشر صور جنسيه على النت**"

واستناداً لما سبق يتضح لنا أن تعرض الجناه لكافه المحتوى الثقافى عبر الانترنت قد يجعلهم عرضه لتقليد هذه النماذج السلبية بمجرد أنهم شاهدوها وحاولوا تقليدها، وبهذا يوفر الإنترنت بيئة خصبة لنشر الأفكار الثقافية السلبية ، حيث يمكن للمجرمين مشاركة خبراتهم والترويج لأساليب الأختراق والهجمات الإلكترونية المدعومة بالذكاء الاصطناعى ، هذا بالأضافة الى ضعف وعى الجناة بالقوانين المتعلقة بالجرائم الإلكترونية ، مما يجعل البعض منهم يعتقد أن أستخدام الذكاء الاصطناعى فى الاحتيال والأبتزاز لا يشكل خطراً قانونياً عليهم

- **انتشار ثقافة الإفلات من العقاب:**

فعندما يلاحظ الأفراد أن مرتكبى الجرائم الإلكترونية لا يحاسبون أو يعاقبون ، فإن ذلك يشجع الجناه على اتباع السلوك نفسه ، خاصة فى ظل توافر تقنيات الذكاء الاصطناعى التى تجعل تعقب المجرمين أكثر صعوبة وتذكر احدى حالات الدراسة "**صاحب شركة تداول اموال قام بإرسال رسائل جذابة تجلب ارباح كبيرة وفرص استثمارية وهمية طلب منى ارسال معلومات شخصية وتحويل أموال لحسابات وهمية**".

يتضح مما سبق ان المجرمين يستخدمون تقنيات متقدمة لإخفاء هويتهم ومواقعهم ، مما يجعل من الصعب على السلطات القانونية تعقبهم ، كما تكون العمليات المالية معقدة وتتضمن تحويلات عبر حسابات متعددة فى دول مختلفة ، مما يزيد من صعوبة تتبع الأموال .

ونستنتج أن العوامل الثقافية المؤدية إلى ارتكاب الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى تهيئ بيئة خصبة لانتشار هذه الجرائم ، فمع توسع استخدام الإنترنت ووسائل التواصل الاجتماعى تتغير القيم الثقافية والأخلاقية لدى الجناة ، مما يدفع بعضهم إلى التساهل فى ارتكاب

سلوكيات غير قانونية وغير أخلاقية عبر الإنترنت ، كما يسهم إخفاء الهوية فى العالم الرقمى فى زيادة هذا التساهل ، إذ يشعر المجرمون بأنهم أقل عرضة للمساءلة ، مما يعزز لديهم ثقافة الإفلات من العقاب ، وفى إطار ما تقدمه **(التفاعلية الرمزية)** من فهم للجريمة الإلكترونية ، يمكن التأكيد على أن الصورة الذهنية التى يكونها الجناة عن الضحايا تلعب دوراً أساسياً فى تبنيهم لأدوار إجرامية مغايرة ، حيث يدفعهم هذا التصور إلى الاندفاع نحو السلوك الإجرامى بدافع تحقيق احتياجات معينة ، مثل الوصول إلى جوائز وهمية تستخدم كوسيلة للإيقاع بالضحايا ، وتعكس هذه التأويلات والتفسيرات التى يبنيها الجناة طريقة استغلالهم للصورة الذهنية للحاجة ، حيث يعتمدون على استخدام الحاسوب والتقنيات الرقمية لإحداث نوع من التفاعل السلبى الإجرامى ، ويؤدى هذا التفاعل إلى خلق بيئة إلكترونية مليئة بالخداع والتلاعب ، مما يسهل عمليات الاحتيال والجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى.

د. الأسباب الذاتية المؤدية إلى ارتكاب الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى من وجهة نظر الضحايا.

مع تطور التكنولوجيا وظهور الذكاء الاصطناعى أصبحت الجرائم الإلكترونية أكثر تطوراً وتعقيداً ، حيث يستغل المجرمون هذه التقنيات لتنفيذ هجمات أكثر دقة وخداعاً وعلى الرغم من تعدد العوامل المؤدية الى إرتكاب الجرائم الإلكترونية إلا أن هناك أسباباً ذاتية تدفع بعض الأفراد إلى ارتكاب هذه الجرائم سواء بدافع الرغبة فى إثبات الذات وتحقيق المكانة الإجتماعية ، وإلحاق الأذى بالضحايا .

- **الرغبة فى إثبات الذات وتحقيق المكانة الإجتماعية:**

تعد الرغبة فى إثبات الذات وتحقيق المكانة الاجتماعية أحد أهم الدوافع الذاتية التى تدفع الأفراد إلى إرتكاب الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، فبعض المجرمين يرتكبون هذه الجرائم بدافع المتعة فى إثبات ذاتهم وقدراتهم فى العالم الافتراضى ، خاصة مع التطور التقنى الذى يتيح لهم التأثير على الآخرين ، سواء من خلال إلحاق الضرر بهم ، أو بدافع الانتقام ، أو بدافع حب الاستطلاع والتحدى والرغبة فى اختراق الأنظمة المعلوماتية ، كما تستخدم تقنيات الذكاء الاصطناعى كوسيلة للسيطرة على الضحايا من خلال الابتزاز الإلكترونى أو تسريب بياناتهم الخاصة ، بالإضافة إلى ذلك يستغل بعض المجرمين قدراتهم التقنية فى القرصنة والتجسس الإلكترونى للحصول على معلومات تمنحهم ميزة تنافسية أو سلطة على الضحايا ، وتذكر احدى الضحايا "**صاحب احد المتاجر قام بأنشاء حساب وهمى عبر وسائل التواصل الاجتماعى ونشر معلومات عن شغلى كذابة للتأثير على الزباين لتحقيق مكانه وسط الزبائن له ولكسب مزيد من الأموال** "

وفى هذا السياق يسعى بعض الجناة إلى تحقيق مكانة اجتماعية او إثبات الذات من خلال ارتكاب جرائم إلكترونية مدعومة بتقنيات الذكاء الاصطناعى ، ويتخذ هذا الدافع الذى ينبع من الرغبة الإنسانية فى التقدير والاعتراف وإثبات الذات أبعاداً خطيرة عندما يوظف فى سياق إجرامى ، فقد يشعر بعض الجناة بالنقص فى حياتهم الواقعية ، فيسعون إلى تعويض ذلك من خلال تحقيق إنجازات وهمية فى العالم الرقمى.

ويشكل الفضاء الإلكترونى مجالاً مناسباً وفرصة للجناه لأستغلال طاقاتهم وافكارهم وتجسيدها بكل حرية واستقلالية فيتجهون للممارسة شغفهم واظهار قدراتهم من خلال استغلال الاجهزة الالكترونية واكتشاف ثغرات الانظمة المعلوماتية والسيطرة عليها واستغلالها لخدمة مصالحهم واهدافهم الآنية والشخصية وفرض انفسهم داخل المجتمع كأشخاص لهم القدرة على التأثير وفرض منطقهم الخاص وتجاوز ضوابط المجتمع التى يعتبرونها تحد من قدراتهم وتقيد طموحاتهم واهدافهم خصوصاً فى ظل الضبط الذاتى المنخفض الذى يعيشونه فى هذه المرحلة ، حيث يؤكد فى هذا الشأن كل من Gottfredson ، و Hirschi ان احتمالية انخراط الأفراد فى فعل إجرامى تحدث بسبب وجود الفرصة (فضاء الكترونى غير مراقب) وتوفر سمة شخصية من سمات الضبط الذاتى المنخفض وهو السلوك الطائش والذى يعتبر فى جوهره عملاً سهلاً قائم على القوة والخداع لتحقيق الرغبات الذاتية بسرعة ، وعليه فالفضاء الالكترونى والأجهزة الالكترونية المتطورة تعد دافعاً هاماً لولوج الجناه عالم الجريمة الالكترونية خصوصاً اذا ارتبط بعامل انخفاض الضبط الذاتى لديهم فى مسألة اثبات الذات وتحقيق التقدير داخل المجتمع.(عيسات ،بوعزة،٢٠٢٢،ص ١٣٦)

- **إلحاق الأذى بالضحايا:**

إلحاق الأذى بالضحايا كدافع ذاتي لارتكاب الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعي يعني أن الدافع الأساسي وراء هذه الجرائم هو الرغبة الشخصية في إيذاء الآخرين، سواء بدافع الانتقام أو الكراهية أو الغيرة، أو حتى بدافع التسلية ، ويمكن أن يتجسد هذا الدافع في عدة أشكال من الجرائم الإلكترونية، مثل التشهير والإساءة الرقمية، كقيام الجاني بنشر معلومات خاصة أو محرجة عن شخص ما بقصد تشويه سمعته، أو استخدام تقنيات التزييف العميق لتشويه صورة شخص معين عبر فبركة مقاطع فيديو أو تسجيلات صوتية مزيفة غير حقيقة ، بالإضافة إلى إرسال رسائل أو تعليقات مهينة على مواقع التواصل الاجتماعي بهدف إلحاق الضرر بالضحية ، وتذكر أحد حالات الدراسة " **ابن عمى قام بتشويه سمعتى على الانترنت وقام بإنشاء صوت مماثل لصوتى معتمداً على برامج**

الذكاء الاصطناعى " نجد ان هذه الحاله تم عرضها ضمن الدوافع الاجتماعية المؤدية إلى ارتكاب الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، وفى تأكيد صاحبه الحالة أن انفصال والدى الجانى والتفكك الاسرى كانا السبب الرئيسى وراء ارتكاب هذه الجريمة ، كما أن هناك دافعاً آخر دفع الجانى إلى ارتكاب جريمته هو رغبته فى إلحاق الأذى بهذه الفتاة بدافع الانتقام منها ، وتذكر حالة أخرى "**صحابى فى الجامعة أبلغونى بأن شخص ما انتحل صفتى وقام بأنشاء صفحة تحتوى على معلومات لى وصورتى الشخصية وقامو بإرسال اللينك الخاص بالصفحة الغير حقيقية وبالضغط على اللينك قاموا بتهكير حسابى والاستيلاء عليه وقامو بهذا الفعل لإلحاق الأذى والضرر بى** " ، وتتفق هذه النتيجة مع ماجاءت به دراسة **(الحوتى ،٢٠٢٠)** فى ان أبرز الدوافع لإرتكاب الجرائم الإلكترونية هو الرغبة فى الانتقام ، كما أن عوامل الانتقام تتم بطرق وأساليب غير تقليدية ، وانما بطرق مستحدثة وعبر وسائط الكترونية.

يتضح مما سبق تعدد الدوافع الذاتية المؤدية إلى ارتكاب الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، إذ إنها متنوعة وتختلف من شخص لآخر ، فقد يدفع الشعور بالحاجة إلى إثبات الذات أو الرغبة فى الانتقام أو الكراهية بعض الجناة إلى ارتكاب هذه الجرائم لإلحاق الأذى بالآخرين ، ويستغلون فى ذلك تقنيات الذكاء الاصطناعى لنشر معلومات كاذبة عن الضحايا والتسبب لهم فى الضرر ، وهذا ما أكدته النظرية**(التفاعلية الرمزية)** فى طرحها بأن دوافع ارتكاب الجرائم الإلكترونية ترتبط بعوامل متعددة تهدف إلى إشباع رغبات ذاتية لدى المجرم ، كما تشير النظرية إلى أن الفرد المجرم يكتسب خبرة ارتكاب الجريمة الإلكترونية من خلال عمليات تفاعلية داخل المجتمع الذى يعيش فيه حيث يتأثر بسلوكيات الآخرين وتصوراتهم حول الجريمة ، ورغم أن الفرد قد ينشأ فى بيئة تعزز القيم الأخلاقية وتؤكد أن الجريمة سلوك غير مرغوب فيه ، إلا أن عمليات التنشئة الاجتماعية قد لا تكون كافية دائماً لمنعه من الانخراط فى الأنشطة الإجرامية خاصة فى ظل التأثير القوى للبيئات الرقمية والتفاعلات الافتراضية التى قد توفر له فرصاً جديدة لتعلم أساليب الاحتيال الإلكترونى أو تقنيات الاختراق ، مما يجعله أكثر انخراطاً فى السلوك الإجرامى المدعوم بتقنيات الذكاء الاصطناعى.

٣-النتائج المتعلقة بالمخاطر والتحديات المختلفة التى تواجه الضحايا نتيجة تعرضهم للجرائم الإلكترونية المعتمدة على تقنيات الذكاء الاصطناعى

تؤثر الجرائم الإلكترونية المدعومة بالذكاء الاصطناعى على الضحايا بطرق متعددة حيث تترك آثاراً اجتماعية واقتصادية ونفسية ومن ابرز هذه الآثار:

- **الآثار الاجتماعية:**

أ.العزلة الاجتماعية:

يعانى ضحايا الجرائم الإلكترونية من فقدان الثقة فى الآخرين ، خاصة عند تعرضهم للأحتيال والابتزاز الإلكترونى وممارسة كافة أنواع الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى عليهم ، فقد تؤدى هذه الجرائم إلى العزلة الاجتماعية والشك فى الآخرين بسبب الخوف من التواصل عبر مواقع التواصل الاجتماعى ، والخوف من مواجهة المجتمع بعد تعرضهم لهذه الجرائم ، كما تؤدى الجرائم الإلكترونية بضحياها الى الانسحاب من الحياة الاجتماعية والشعور بالخجل من مشاركة التجربة مع الآخرين ، وتذكر احد حالات الدراسة "**بعد ارتكاب الجريمة انعزلت عن جميع الأفراد وقمت بأغلاق جميع مواقع التواصل الاجتماعى خوفاً من تكرار الجريمة مرة أخرى وقررت مرجعش فى قرارى مرة تانية**" ، تتفق هذه النتيجة مع ماجاءت به دراسة **(ابراهيم ،٢٠٢٣)** فى معاناة معظم الضحايا من عينة البحث من العزلة الاجتماعية.

يتضح مما سبق أن بعض الضحايا يشعرون بالخجل والعار عند تعرضهم لجرائم إلكترونية مدعومة بتقنيات الذكاء الاصطناعى ، خاصة إذا كانت الجريمة تتعلق بانتهاك الخصوصية أو نشر معلومات شخصية ، فقد يخشون من احكام الآخرين عليهم او التعرض للنبذ ، مما يدفعهم إلى الانعزال ، كما يفقد الضحايا الثقة بالآخرين ، لا سيما إذا كان الجانى شخصاً يعرفونه ، فيصبحون أكثر حذراً فى تكوين علاقات جديدة أو مشاركة معلوماتهم الشخصية ، مما يؤدى فى النهاية إلى العزلة الاجتماعية

ب.تدمير السمعة الشخصية والمهنية:

يمكن أن يؤدى نشر معلومات أو صور مزيفة للضحايا بإستخدام تقنيات الذكاء الاصطناعى إلى فقدان الضحية لوظيفته أو مكانته الاجتماعيه داخل الوسط الاجتماعى الذى يعيشه به ، ويعانى أيضاً بعض الضحايا من صعوبة فى استعادة سمعتهم بعد تعرضهم للأحتيال والتشهير والابتزاز الإلكترونى ، وتذكر احدى الضحايا "**معلم نفس تخصصى استخدم تقنيات التزييف العميق وانشأ مقاطع فيديو مزيفة بها تصريحات مزيفة لى وكان ذلك بهدف تشويه سمعتى لجلب الطلاب إليه**"

يتضح مما سبق نشر الجانى لمعلومات كاذبة ومضللة عبر الإنترنت بهدف تشويه سمعة الضحية والإضرار بها ، فيمكن أن يؤدى تدمير السمعة إلى فقدان الوظيفة أو صعوبة الحصول على وظائف جديدة

ج.تهديد العلاقات الأسرية والاجتماعية:

تؤدى الجرائم الإلكترونية إلى خلافات عائلية ، خاصة إذا كانت الضحية أنثى تعرضت للأبتزاز والتشهير الإلكترونى أو جرائم تشويه السمعه ، ففى بعض الحالات يؤدى التشهير الإلكترونى بتدمير الضحية وأيضاً العلاقات الزواجية أو الأسرية خاصة إذا تم استغلال الذكاء الاصطناعى لإنشاء صور مزيفه ، كما ان الاحتيال العاطفى عبر الانترنت يؤدى الى الشك المستمر بين الزوجين وتذكر احد حالات الدراسة "**عندما تعرضت لجريمه ابتزاز إلكترونى ونشر صور مفبركة لى زوجى طلقنى وعلاقتى بأولادى اتدمرت**" ، وتذكر احد حالات الدراسة "**عندما قام احد زملائى فى العمل بتشويه سمعتى ونشر معلومات مضلله باستخدام الذكاء الاصطناعى وعلاقتى بعائلتى تأثرت وابتعدو عنى**"

يتضح مما سبق ان الجرائم الإلكترونية تشكل تهديداً خطيراً للعلاقات الاسرية والاجتماعية ، إذ قد تؤدى إلى تدمير الثقة بين الزوجين وخلق بيئة يسودها الخوف والقلق وانعدام الأمان ، كما أن سرقة هوية أحد أفراد الأسرة قد تثير الشكوك وسوء الظن بين أفرادها ، مما يزيد من التوتر داخل الأسرة

نستنتج مما سبق ان الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى تشكل تهديداً متزايداً للأفراد ، حيث تتجاوز آثارها الخسائر المالية لتشمل تداعيات وآثار اجتماعية خطيرة كالعزلة الاجتماعية وتدمير السمعة الشخصية والمهنية وتهديد العلاقات الأسرية والاجتماعية ، وذلك لأنها تؤدى الى تآكل الثقة بين الضحايا والأفراد ، فيصبح الضحايا أكثر حذراً فى تفاعلاتهم عبر الإنترنت ، مما يؤثر على علاقاتهم الاجتماعية والمهنية.

- **الآثار الاقتصادية**

أ.الخسائر المالية:

يتعرض العديد من ضحايا الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعي لخسائر مالية كبيرة بطرق متعددة ، من بينها دفع مبالغ مالية للمجرمين نتيجة الابتزاز بالصور ومقاطع الفيديو المفبركة، بالإضافة إلى سرقة الحسابات المصرفية وتحويل الأموال وسرقتها دون إذن أصحابها ، كما يضطر الضحايا إلى دفع مبالغ مالية للشركات الإلكترونية المتخصصة في استعادة الحسابات الإلكترونية، بهدف استرجاع بياناتهم الخاصة ، وتذكر احدى الحالات "**الجانى طلب منى فلوس لعدم نشره الصور**

والفيديوهات المفبركه " ، وتذكر ايضاً حالة أخرى " **المجرم قام بتهكير حسابى البنكى واستولى على كل الأموال الموجوده فى الحساب**"

ويتضح مما سبق تزايد الخسائر الاقتصادية الناتجة عن الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى بشكل ملحوظ ، فمنها الخسائر المالية المباشرة من سرقة الأموال من خلال الاحتيال المالى الإلكترونى ، والابتزاز الرقمى وطلب الفدية ، والخسائر الناتجة عن اختراق البيانات المالية وسرقة معلومات بطاقات الائتمان

ب.فقدان الوظائف وفرص العمل:

يتم ذلك من خلال سرقة الهويات الرقمية للضحايا ونشر معلومات مضللة، مما يؤثر سلبًا على سمعتهم ويعرضهم لخطر فقدان وظائفهم ، كما أن الابتزاز الإلكتروني قد يدفع الضحايا إلى تقديم استقالتهم أو فقدان فرص وظيفية بسبب التهديد بنشر معلومات شخصية مزيفة ، كل ذلك يؤدي إلى شعور الضحايا بالقلق والضغط، مما قد يدفعهم إلى الاستقالة ، وتذكر احدى حالات الدراسة" **قام الجانى بسرقة الهوية الشخصية لى على الفيس بوك وقام بانتحال شخصيتى ونشر معلومات خاطئه عن شغلى وفقدت شغلى على اثر هذا العمل لأنه قام بتشويه سمعتى الائتمانية** " ، كما تذكر ايضاً احدى حالات الدراسة "**قام المجرم بأستخدام الذكاء الاصطناعى وقام بانشاء رسائل بريد إلكترونى احتيالية والحساب كان ملك الشركة وقام بأخذ كل الفلوس فى الحساب وفقدت وظيفتى** "

يتضح مما سبق أن الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى تحدث تأثيرات سلبية واسعة النطاق على الضحايا ، حيث تستخدم هذه التقنيات فى سرقة الهوية الرقمية للوصول إلى المعلومات الشخصية والمالية ، مما يؤدى إلى خسائر مالية كبيرة ، كما يمكن استغلال الذكاء الاصطناعى فى إنشاء رسائل بريد إلكترونى احتيالية أو مواقع ويب مزيفة ، مما يجعل الأفراد عرضة لعمليات الاحتيال ، بالإضافة إلى ذلك يستطيع المجرمون استخدام الذكاء الاصطناعى لجمع معلومات حساسة عن الضحايا وابتزازهم مقابل عدم نشرها ، مما يزيد من خطورة هذه الجرائم وتأثيرها على الأفراد والمجتمع.

ج.التكاليف القانونية:

يلجأ العديد من الضحايا إلى توكيل المحامين لاستعادة حقوقهم القانونية أو مقاضاة الجناة المتورطين في الجرائم الإلكترونية المختلفة، إذ تتطلب قضايا الاحتيال المالي وسرقة الهويات وقتًا طويلاً وجهدًا قانونيًا كبيرًا، كما أن استرداد الأموال في بعض القضايا قد يكون أمرًا بالغ الصعوبة، مما يجعل تكاليف المحامين عبئًا إضافياً ، وتذكر احدى حالات الدراسة "**لما عرفت بالجريمة ذهبت الى محامى**

لعمل توكيل ودفعت له مبلغ كبير لأسترداد حقى " ، وتذكر ايضاً احدى حالات الدراسة " **ذهبت الى خبير تقنى فى مجال الاحتيال المعلوماتى لحل المشكلة واخذ منى فلوس مقابل الخدمة المقدمة"**

يتبين لنا هنا أن التكاليف القانونية وأتعاب المحامين تشكل جزءاً كبيراً من الخسائر التى يتكبدها ضحايا الجرائم الإلكترونية ، فقد يحتاج الأفراد إلى استشارة محام لتقييم حقوقهم القانونية والخيارات المتاحة لهم بعد التعرض لجريمة إلكترونية ، فى حين يتجه البعض الآخر إلى الخبراء فى التقنية الرقمية بدلاً من المحامين ، بهدف استرجاع حقوقهم المادية واستعادة هويتهم الرقمية ، وتستوجب جميع هذه الإجراءات تكاليف مالية يضطر الضحايا إلى تحملها لاستعادة حقوقهم سواء كانت مادية أو قانونية.

نستنتج مما سبق أن الجرائم الإلكترونية تؤثر على الضحايا بطرق متعددة ، وغالباً ما تتداخل هذه التأثيرات مما يزيد من خطورتها وتأثيرها على حياة الأفراد ، وتشمل هذه التأثيرات الخسائر المالية مثل سرقة المعلومات الشخصية والمالية واستخدامها فى فتح حسابات بنكية أو إجراء عمليات شراء غير مصرح بها ، كما تمتد لتشمل الاحتيال المالى عبر الإنترنت والتصيد الاحتيالى على بطاقات الائتمان ، مما يؤدى إلى خسائر مالية كبيرة ، بالإضافة إلى ذلك قد يلجأ المجرمون إلى تهديد الضحايا بنشر معلومات حساسة أو صور خاصة مقابل دفع فدية ، مما يزيد من معاناتهم الاقتصادية ، علاوة على ذلك يضطر الضحايا إلى تحمل تكاليف قانونية وتقنية ، سواء من خلال الاستعانة بمحامين أو خبراء تقنين لاستعادة حقوقهم المادية والقانونية.

- **الآثار النفسية**

أ. القلق والتوتر المستمر:

يشعر ضحايا الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى بالخوف من التعرض لهجمات جديدة أو من أستخدام بياناتهم الشخصية ضدهم ، فيعيشون حالة من التوتر والقلق الدائم ، كما أن القلق من فقدان الأمان فى الفضاء الرقمى يجعلهم مترددين فى استخدام التكنولوجيا مرة أخرى ، وتذكر احدى حالات الدراسة "**اول ما اتعرضت لعمليه احتيال إلكترونى قلقت جداً وشعرت بالخوف وقررت لا استخدم الفضاء الرقمى مرة أخرى** " ، وتتفق هذه النتيجة مع ماجاءت به دراسة **(ابراهيم ،٢٠٢٣)** فى ان الضحايا عند تعرضهم للجرائم الإلكترونية عانوا من القلق والتوتر المستمر ، ومن فقدان الثقة بالنفس

ويمكن القول أن القلق والتوتر المستمر الناتجين عن الجريمة الإلكترونية من الآثار النفسية الشائعة التى يعانى منها الضحايا ، حيث تؤثر هذه المشاعر بشكل كبير على حياتهم اليومية ، فكثير من الضحايا يشعرون بانتهاك خصوصيتهم وتعرضهم للاعتداء ، مما يولد لديهم مخاوف مستمرة بشأن

إمكانية استغلال معلوماتهم الشخصية فى جرائم أخرى أو تعرضهم لمزيد من الهجمات الإلكترونية مستقبلاً.

ب.التأثير النفسى والاضطرابات العاطفية:

وذلك من خلال تعرض ضحايا للجرائم الإلكترونية ومن ضمنها التزييف العميق والتشهير الإلكترونى قد يسبب لهم صدمة نفسية، كما يمكن أن تؤدى الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى إلى القلق والاكتئاب أو حتى التفكير فى الانتحار ، وتذكر احدى حالات الدراسة "**عندما تعرضت لجريمة إلكترونية دخلت فى حالة اكتئاب حاد وفكرت فى الانتحار اكثر من مره بس كنت بفكر فى اولادى من بعدى** " ، وتذكر ايضاً احدى حالات الدراسة "**جالى شعور بالقلق الكبير ونفسياً كنت تعبان جدا ووصلت لمرحلة صعبه من الخوف والقلق** " ، وتتفق هذه النتيجة مع ماجاءت به دراسة **(ابراهيم،٢٠٢٣)** فى تفكير ضحايا الجرائم الإلكترونية فى الانتحار

يتضح لنا هنا أن الضحايا قد يشعرون بالحزن واليأس نتجية ممارسة الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى عليهم ، إلى جانب فقدان الاهتمام بالأنشطة اليومية وفقدان الثقة فى الآخرين وفى التكنولوجيا بشكل عام ، كما قد تؤدى الجرائم الإلكترونية إلى اضطرابات نفسية وعاطفية خطيرة ، مثل القلق والاكتئاب ، وقد يصل الأمر ببعض الضحايا إلى التفكير فى الانتحار نتيجة الضغوط النفسية الشديدة التى يتعرضون لها.

ج.التأثير على الأداء المهنى والأكاديمى:

تؤثر الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعي سلبًا على الأداء المهني والأكاديمي، إذ تخلق ضغوطًا نفسية وتحديات تقنية وقانونية تؤدي إلى تراجع الإنتاجية ، ويعود ذلك إلى الانشغال المستمر بالتفكير في الواقعة المرتكبة، مما يؤدي إلى انخفاض الأداء في العمل والدراسة نتيجة التوتر والقلق الدائم ، كما أن اضطرابات النوم الناجمة عن القلق والصدمة تؤثر سلبًا على الأداء العقلي والجسدي إضافةً إلى ذلك، يقضي الضحايا وقتًا طويلًا في محاولة استعادة بياناتهم وأموالهم، وهو وقت كان يمكن استثماره في إنجاز المهام المهنية والدراسية، وتذكر احدى حالات الدراسة "**عندما تعرضت لأبتزاز إلكترونى اعتزلت عن العالم ولم اذهب الى عملى وقصرت فيه**" ، كما تذكر ايضاً احدى حالات الدراسة "**بعدما تعرضت للجريمة قررت الا اذهب الى الجامعة ورسبت سنه** " ، وتتفق هذه النتيجة مع ماجاءت به دراسة **(ابراهيم ،٢٠٢٣)** فى معاناة ضحايا الجرائم الإلكترونية من عدم التركيز فى عملهم ، كما ان معظم الضحايا تغيبوا عن الجامعة وأهملوا فى دراستهم ، ومن بينهم من انخفضت قدرتهم على التحصيل الدراسى والفهم والتفكير

يتضح هنا ان الجرائم الإلكترونية تمثل تحدياً متزايداً يؤثر بشكل كبير على الأداء المهنى والأكاديمى للضحايا ،إذ تؤدى إلى تشتت الانتباه وصعوبة التركيز ، سواء فى العمل أو الدراسة ، كما تؤثر على التحصيل الدراسى ، مما ينتج عنه انخفاض الأداء فى الامتحانات والواجبات ، إضافة إلى تراجع معدلات الحضور والمتابعة الدراسية.

نستنتج مما سبق أن الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى تخلف آثاراً نفسية تتجاوز الخسائر المادية ، لتشمل القلق والتوتر والاضطرابات العاطفية والنفسية ، بالإضافة إلى تأثيرها على الأداء المهنى والأكاديمى ، إذ يعانى الضحايا من شعور دائم بعدم الأمان والقلق المستمر ، وقد يصل بهم الأمر إلى الاكتئاب ، وفقدان الرغبة فى الحياة ، وانعدام الثقة فى الآخرين وفى التكنولوجيا فضلاً عن الشعور بالعار والذنب ولوم النفس والخجل ، وتعد هذه الآثار النفسية للجرائم الإلكترونية واقعاً ملموساً يترك أثراً عميقاً فى نفوس الضحايا .

٤- النتائج المتعلقة بمعرفة موقف الضحايا عند تعرضهم للجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى وكيفيه تعاملهم مع هذه الجرائم.

عند تعرض الضحايا للجرائم الإلكترونية المختلفة المدعومة بتقنيات الذكاء الاصطناعى يكون موقفهم شديد التعقيد نظراً للطبيعة المتقدمة والمتطورة لهذه الجرائم ، مما يجعل الكشف عنها والتعامل معها أكثر صعوبة ، فيتعدد موقف الضحايا كما يلى:

أ.الصدمة والارتباك:

عند اكتشاف الجريمة ينتاب الضحية شعور بالدهشة والارتباك الشديد، لاسيما إذا كانت الجريمة قد ارتكبت باستخدام تقنيات الذكاء الاصطناعى ، مثل الابتزاز الإلكترونى والتزييف العميق والاحتيال وسرقة البيانات الشخصية على مواقع التواصل الاجتماعى ، وقد يجد الضحية نفسه فى حالة من الصدمة والحيرة ، متسائلاً عن كيفية وقوع الاختراق أو الابتزاز الإلكترونى،وتذكر احدى حالات الدراسة "**عندما تعرضت للجريمة الإلكترونية كنت فى حالة من الصدمة الشديدة ومش عارف اعمل ايه فكرت فى مستقبلى واسرتى**" ، وتذكر احدى حالات الدراسة "**لماعرفت بالجريمة الواقعة عليا ارتبكت جدا ولما كلمنى المجرم وطلب مبلغ من المال مترددش وقمت بارسال الفلوس فى الحال وده لأنى كنت مرتبك جدا ومش دارى بتصرفاتى**"

يتضح مما سبق غالباً ما يشعر ضحايا الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى بالصدمة والارتباك خاصة فى الجرائم التى تنطوى على انتهاك للخصوصية أو التزييف العميق ، كما يتعرض الضحايا من اضطراب ما بعد الصدمة خاصة إذا تعرضوا لتهديدات أو ابتزاز

ب.البحث عن الدعم والمساعدة:

يلجأ بعض الضحايا إلى طلب الدعم والمساعدة النفسية والعائلية بعد وقوع الجرائم الإلكترونية عليهم لمعرفة كيفية التعامل مع هذه الجرائم وخاصة إذا كان الضرر كبير ، فأن هذا الدعم يلعب دوراً أساسياً فى تخفيف الآثار النفسية السلبية ومساعدته على اتخاذ القرارات الصحيحة لمواجهة الأزمة ، وتذكر احدى حالات الدراسة "**عندما تعرضت لجريمة الكترونية تحدثت مع أخى لأنى بثق فيه وقدم لى الدعم النفسى والمعنوى**" ، كما تذكر أحدى حالات الدراسة " **كان ابى بمثابة الدعم النفسى والاجتماعى والمعنوى بالنسبه لى وقام بتهدأتى وقال لى انا واثق فيكى وهحل الموضوع ده** "

يتبين مما سبق أنه عندما يقع الأفراد ضحايا لجرائم إلكترونية ، يصبح البحث والمساعدة أمراً بالغ الأهمية ، فآثار هذه الجرائم لا تقتصر على الخسائر المادية فحسب ، بل تمتد لتشمل الأضرار النفسية والعاطفية ، التى قد تكون أكثر شدة وتأثيراً ، لذا يسعى الضحايا إلى الحصول على الدعم والمساندة من الأشخاص المقربين أو المختصين ، سواء للاستشارة أو طلب المساعدة ، كما أن الحصول على الدعم النفسى والاجتماعى والمعنوى يمكن أن يساعدهم فى التعامل مع هذه الآثار وتجاوزها بشكل أفضل .

ج.اتخاذ أجراءات أمنية وقانونية:

وذلك من خلال رفع دعاوى قضائية ضد المجرمين فى حال تم تحديد هويتهم أو الجهة المسؤولة عن الجريمة ، كما يتم توثيق جميع الأدلة مثل رسائل الابتزاز والمعاملات المالية غير المشروعة والصور المزيفة لتقديمها إلى الجهات المختصة للتحقيق ، ومع ذلك فإن بعض الضحايا يتجنبون تقديم بلاغات رسمية أو رفع دعاوى قضائية نظراً لطول الإجراءات القانونية أو خشية انتشار خبر الجريمة بين الأهل والأصدقاء والمعارف ، وبدلاً من ذلك يلجؤون إلى خبراء الأمن الإلكترونى لاستعادة بياناتهم وتأمين حساباتهم المخترقة ، وتذكر احدى الضحايا "**قمت بعمل محضر إثبات حالة فى قسم الشرطة وبعد ذلك قمت بعمل محضر ابتزاز إلكترونى فى مباحث الانترنت فى مديرية الأمن**" ، كما تذكر احدى حالات الدراسة "**قمت بإبلاغ مزود خدمة الإنترنت الخاص بى على موقع التواصل الاجتماعى** " كما تذكر حالة أخرى "**ذهبت الى مباحث الاتصالات فى القاهرة وقمت بتحرير محضر بالواقعه وكان معى المستندات والريكود المسجل**" وتذكر أيضاً حالة أخرى "**ذهبت الى شخص متخصص فى التقنية وقام بفحص الجهاز واستخدم برامج إلكترونية وتم استرجاع الحساب المسروق**"

يتبين لنا مما سبق ان الجرائم الإلكترونية تعد من أخطر التحديات التى تواجه الأفراد والمجتمعات فى عصر التكنولوجيا والذكاء الاصطناعى ، حيث تتسبب فى أضرار مادية ومعنوية كبيرة ، ولحماية

الضحايا من هذه الجرائم يلجأون إلى اتخاذ إجراءات أمنية وقانونية متنوعة تهدف إلى الحد من الأضرار واستعادة الحقوق.

نستنتج مما سبق تعدد الإجراءات الأمنية والقانونية التى يلجأ إليها ضحايا الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، ومنها تحرير محضر إثبات حالة فى قسم الشرطة ، بالإضافة إلى تقديم بلاغ فى مباحث الإنترنت ، كما يلجأ بعض الضحايا إلى تقديم بلاغ فى مباحث الاتصالات بالقاهرة ، فى حين يفضل آخرون إبلاغ مزود الخدمة على مواقع التواصل الاجتماعى ، ومن ناحية أخرى يتجنب بعض الضحايا الإجراءات القانونية المعتادة ويلجئون إلى متخصصين فى التقنية لاستعادة حساباتهم ، وتهدف هذه الإجراءات إلى حماية الضحايا من المزيد من الأضرار ، واستعادة حقوقهم المسلوبة ، وتحقيق العدالة.

٥- النتائج المتعلقة بالمقترحات التى يمكن ان تساهم فى حماية الأفراد من الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى من وجهة نظر ضحايا الجرائم الإلكترونية

- **دور الأسرة:**

فى ظل التطور التكنولوجى الذى نعيش فيه ، أصبح العالم الرقمى جزءاً أساسياً من حياتنا اليومية حيث يتم الأعتماد على الإنترنت والذكاء الاصطناعى فى مختلف المجالات سواء فى الترفيه والتواصل والتعليم والعمل ، ولكن مع هذه التطورات ظهرت تحديات ومخاطر جديدة للذكاء الاصطناعى وتأثيره على إرتكاب الجرائم الإلكترونية من الاحتيال والاختراق والابتزاز الإلكترونى والتزييف العميق ، وهنا يأتى دور الأسرة لحماية أفرادها من هذه المخاطر والتحديات من خلال التوعية وتعزيز السلوكيات الرقمية الآمنة ، والإشراف على المواقع الإلكترونية المختلفة

أ. الإشراف والمراقبة:

فمن خلال مراقبة أنشطة الأفراد على الإنترنت دون انتهاك خصوصيتهم ، وتشجيعهم على الإبلاغ عن أى تهديد أو محاولة ابتزاز واحتيال ، ومن الممكن أيضاً أستخدام أدوات الرقابة الأبوية وبرامج الحماية من الاختراقات الإلكترونية، وتذكر احدى حالات الدراسة "**لابد من مراقبة أنشطه الأفراد على الانترنت عن طريق الاسرة ومنع أى سلوك ضار فى بدايته**" ، كما تذكر احد حالات الدراسة " **لابد من الصغر تكون الاسرة مشرفة على برامج الانترنت حتى لا يقع الفرد فى ارتكاب جرائم إلكترونية**" كما تذكر احدى حالات الدراسة "**لابد من استخدام برامج مراقبة الأبوية لتتبع الأنشطة عبر الانترنت** "

من خلال ماورد من حالات الدراسة الميدانية (ضحايا الجرائم الإلكترونية) ، يتضح أن تبنى هذه الإجراءات يمكن أن يساعد الأسر فى خلق بيئة آمنة لأفرادها ، مما يسهم فى حمايتهم من مخاطر الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى.

ب. التوعية والتثقيف:

فمن خلال تثقيف أفراد الأسرة عن طريق البرامج التوعوية خاصة الشباب حول مخاطر الجرائم الإلكترونية مثل الابتزاز وجرائم الهاكرز وجرائم الاحتيال الإلكترونى وجرائم تشويه السمعه ، وتعليمهم كيفية التحقق من الأخبار والمعلومات الغير صحيحة التى يتم إنشاؤها بواسطة تقنيات الذكاء الاصطناعى ، وتذكر احدى حالات الدراسة "**يجب ان تعمل الاسرة على توعيه افرادها من خلال التحدث معهم بأستمرار عن مخاطر الجرائم الإلكترونية** " كما تذكر أحدى حالات الدراسة الأخرى "**مشاهده البرامج التوعويه والتثقفية معاً داخل الأسرة يعزز من التحقق من الأخبار والمعلومات الغير صحيحه ويوسع افق أفراد الأسرة نحو ارتكاب الجرائم الإلكترونية** " ، وتتفق هذه النتيجة مع ماجاءت به دراسة**(الشمرى ،٢٠٢١)** فى ان وسائل مكافحة الجرائم الالكترونية لا تقع مسؤوليتها على عاتق الدولة فقط ، وانما تشمل الأسرة ايضاً وهذا يتطلب الالمام بأبسط قواعد ضمان امن المعلومات والاجهزة التقنية المستخدمة.

يتبين لنا هنا أهمية التوعية والتثقيف داخل الأسرة فأصبح ضرورة ملحة لمواكبة التحديات والمخاطر التى تفرضها التقنيات الحديثة ، فالتوعية لا تقتصر على اكتساب الأفراد المعرفة فقط ، بل تمتد لتشمل فهم كيفية التعامل مع المعلومات والتقنيات بشكل آمن وفعال.

ج. تحفيز التواصل الأسرى:

فمن خلال تعزيز الحوار المفتوح بين أفراد الأسرة حتى يشعر الفرد بالأمان والطمأنينة عند التحدث عن أى مخاوف رقمية تعرض لها ، وأيضاً تبادل المعرفة حول التطورات التكنولوجية والذكاء الاصطناعى لتطوير أساليب الحماية والدفاع باستمرار ، فتذكر أحدى حالات الدراسة " **يجب على الأسرة التحدث بأستمرار مع أبنائها بدون خجل أو خوف لأن هذا سيكسر حاجز الرهبة بينهم ويشعرون بالأمان ضد اى مخاوف يتعرضون لها**" ، وتذكر حاله أخرى " **يجب على الأب والأم التعامل مع أبنائهم على أساس انهم كبار حتى يستطيعون احتضانهم و وتفريغ طاقتهم معهم**" ، وتتفق هذه النتيجة مع ماجاءت به دراسة **(Gupta,2017)** فى ان العوامل الرئيسية لحماية الشباب من تلك الجرائم الإلكترونية يقع على عاتق الاسرة فهى تمنعهم من الوقوع ضحية لمثل ذلك النوع من الجرائم الإلكترونية التى تؤثر عليهم مادياً ومعنوياً

نستنتج مما سبق ان الأسرة تلعب دوراً هاماً فى حماية افرادها من الوقوع ضحايا للجرائم الإلكترونية ، وذلك من خلال توفير الدعم والتوعية والإرشاد ، وتعزيز التواصل الأسرى بالإضافة إلى الإشراف والمراقبة ، فمن خلال هذه الإجراءات يمكن للأسرة أن تسهم بفاعلية فى حماية أفرادها من مخاطر الجرائم الإلكترونية وتوفير بيئة رقمية آمنة لهم

- **دور وسائل الاعلام**

أ.توفير نصائح وإرشادات تقنية

من خلال استضافة خبراء فى أمن وحماية المعلومات لشرح كيفية حماية البيانات الشخصية والحسابات التى تم الأستيلاء عليها من قبل المجرمون ، وأيضاً توجيه الأفراد نحو استخدام الأدوات والتطبيقات المختلفة التى تحميهم من الهاكرز والاختراقات والتزييف العميق والابتزاز الإلكترونى ، وتعزيز الشراكة مع الجهات الأمنية والتقنية المختلفة وذلك لنشر حملات التوعوية ذات مصداقيه عالية ونشر الجهود الحكومية فى مكافحة الجرائم الإلكترونية حتى يهاب المجرمون من الأفعال التى تقوم بها الحكومة فى ردع كل مجرم يرتكب جرائم الكترونية مدعومة بتقنيات الذكاء الاصطناعى ، وتذكر احد حالات الدراسة "**لازم الاعلام يعلن عن نصائح وارشادات للأفراد لحماية البيانات والمعلومات الشخصية وعدم اختراقها**" ، وتذكر حالة أخرى "**الاعلام له دور كبير فى توجيه الافراد وحمايتهم من الهجمات الإلكترونية المختلفة**"

نستنتج مما سبق الدور المهم التى تقوم به وسائل الاعلام فى نشر الوعى التقنى وتوفير النصائح والإرشادات التى تساعد الأفراد على حماية أنفسهم من المخاطر الإلكترونية ، فمن خلال إنتاج برامج تلفزيونية وإذاعية متخصصة فى الأمن والتقنية ، تتناول أحدث التهديدات الإلكترونية وتقدم نصائح عملية للمشاهدين والمستمعين.

ب.رصد وكشف أساليب الاحتيال:

وذلك من خلال نشر تقارير بصفة دورية تكشف وتوضح أحدث طرق الاحتيال والابتزاز الإلكترونى وتحذر من التطبيقات والمواقع المشبوهة التى قد تستغل الضحايا ، وايضاً توضح الطرق المختلفة لسرقة حسابات البنوك والحسابات المختلفة عبر مواقع التواصل الاجتماعى بأستخدام تقنيات الذكاء الاصطناعى فى ارتكاب مختلف الجرائم الإلكترونية ، وتذكر احدى حالات الدراسة "**على وسائل الاعلام نشر الطرق المختلفه لإرتكاب الجرائم الإلكترونية عبر شاشات التليفزيون وهذا للتوعيه بخطورتها وطريقه ارتكابها حتى يتوخى الضحايا الحذر من ممارسة الجرائم الإلكترونية عليهم** "

يتضح أن رصد وكشف أساليب الاحتيال يمثل تحدياً فى العصر الرقمى ، نظراً للتطور المستمر فى تقنياته ، ومع ذلك هناك العديد من الوسائل التى تساهم فى كشف هذه الأساليب والتصدى لها ، ومن أبرزها الدور الذى يؤديه الإعلام فى توعية الأفراد ، من خلال رصد مصادر الاحتيال وتوضيحها ، مما يساعدهم على تجنب الوقوع ضحايا لمثل هذه الجرائم

نستنتج مما سبق ان وسائل الإعلام تلعب دوراً هاماً فى التصدى للجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، وذلك من خلال رصد وكشف أساليب الاحتيال وعرضها عبر شاشات التلفاز لتوعية المواطنين باساليب ارتكاب هذه الجرائم ، كما تسهم فى تقديم النصائح والإرشادات التقنية ، وشرح كيفية استغلال المجرمين لهذه التقنيات الحديثة فى تنفيذ الجرائم الإلكترونية ، مما يساعد على تعزيز الوعى المجتمعى والحد من مخاطرها

- **دور المؤسسات التعليمية**

تلعب المؤسسات التعليمية دوراً مهماً فى حماية الأفراد من المخاطر المختلفة للجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى المختلفة وذلك من خلال التالى:

أ.تعزيز القيم والسلوك الرقمى الأخلاقى:

من خلال ترسيخ مبادئ احترام الخصوصية وعدم مشاركة البيانات الشخصية سواء معلومات شخصية او صور شخصيه عبر مواقع التواصل الاجتماعى المختلفة ، وتوعية الأفراد بأخطار الجرائم الإلكترونية المدعومة بالذكاء الاصطناعى وأساليب مواجهاتها ، وتعليم الأفراد المسؤولية الرقمية مثل عدم مشاركة ونشر المحتوى المزيف وغير الموثوق به ، وتذكر احدى حالات الدراسة "**يجب على المؤسسات التعليمية المختلفة تدريس مبادئ احترام الخصوصية بين الطلاب فى مراحل التعليم المختلفة**" ، وتذكر أحد حالات الدراسة الأخرى "**لابد من وجود كتب تثقيفية للأفراد عن السلوك الرقمى الإيجابى وعدم الانصياع وراء السلوك السلبى الرقمى الذى يؤدى الى إرتكاب الجرائم الإلكترونية**"

ونستنتج مما سبق أن تعزيز القيم والسلوك الرقمى الأخلاقى فى مختلف المواد الدراسية ، مثل علوم الحاسب والتربية الإسلامية ، يسهم فى ترسيخ مبادئ الاستخدام المسئول للتكنولوجيا ، فمن خلال تضمين قصص واقعية تتناول قضايا الأخلاق الرقمية ، مثل الحد من التنمر الإلكترونى ، وسرقة الهوية ، ونشر المعلومات المضللة ، والابتزاز الإلكترونى ، يمكن توعية الأفراد بأهمية السلوك الرقمى السليم ، كما تشجع هذه المواد الدراسية الطلاب على تحليل القضايا الأخلاقية المرتبطة بالتكنولوجيا ، مما يساعدهم على تطوير مهارات التفكير النقدى لديهم ، وتتفق هذه النتيجة مع ماجاءت به دراسة **(ابراهيم ،٢٠٢٣)** فى ان غياب دور المؤسسات التعليمية كان له اثر كبير على ارتكاب المجرمين للجرائم

الإلكترونية المختلفة ، ويجب تفعيل دور المؤسسات التعليمية لما تقوم به من دور فعال فى مكافحة الجرائم الإلكترونية.

ب.توفير بيئة إلكترونية آمنة:

من خلال تأمين أنظمة البيانات والمعلومات داخل المؤسسات التعليمية المختلفة وذلك لحماية بيانات الأفراد والمعلمين ، وأيضاً مراقبة المحتوى الإلكترونى الذى يتم تداوله داخل المؤسسات التعليمية المختلفة وذلك للحماية من عمليات التهديدات والابتزاز والانتحال الإلكترونى، وتذكر احدى الضحايا "**لابد من المؤسسات التعليمية حماية أنظمتها المختلفة من الأختراق وحماية بيانات المعلمين وكذلك الطلاب حتى لا يتم استغلالها بطرق غير مشروعة لتحقيق جرائم إلكترونية**" ، وتذكر ايضا احد حالات الدراسة " **على المؤسسات التعليمية تحديث أنظمتها بأستمرار فهذا يؤدى الى تقليل عمليات الأختراق الإلكترونى**"

يتضح لنا هنا ان توفير بيئة إلكترونية آمنة يؤدى الى تقليل خطر الاختراق الإلكترونى ، كاستخدام كلمات مرور قوية والتحديثات المستمرة تقلل من فرص اختراق الحسابات والأجهزة .

ج.استخدام التكنولوجيا فى حماية وتوعية الأفراد:

وذلك من خلال توفير العديد من التطبيقات والمنصات التعليمية المختلفة لنشر الوعى الفنى والتقنى حول أساليب الاحتيال والأختراق الإلكترونى ، واستخدام تقنيات الذكاء الاصطناعى المختلفة لمراقبة التهديدات والابتزاز والاحتيال والسرقات الإلكترونية التى يتعرض لها الضحايا ، وتذكر احدى حالات الدراسة "**رى ما الجناه بيستخدمو التكنولوجيا والذكاء الاصطناعى لتنفيذ جرائمهم ،لابد من استخدام المؤسسات التعليمية المختلفة التكنولوجيا الحديثة فى حماية وتوعية الأفراد ضد مخاطر الجرائم الإلكترونية**" ، وتتفق هذه النتيجة مع ماجاءت به دراسة **(Gupta,2017)** ، فى تأكيدها على ان مواقع التواصل الاجتماعى لها تأثير إيجابى فى دعم ونشر مختلف المعارف المرتبطة بالامن الاجتماعى.

يتضح لنا هنا أن التكنولوجيا تلعب دوراً هاماً فى حماية وتوعية الأفراد من المخاطر الرقمية ، حيث تتيح أدوات وتقنيات متطورة لتعزيز ونشر الأمن الرقمى وذلك من خلال برامج الحماية المتطورة ، وحملات التوعية عبر وسائل التواصل الاجتماعى ، واستخدام الذكاء الاصطناعى فى تحليل البيانات واكتشاف الأنماط الاحتيالية فى المعاملات المالية والأنشطة عبر الإنترنت.

ونستنتج مما سبق تعدد الأدوار التى تقوم بها المؤسسات التعليمية المختلفة فى التوعية بمخاطر الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، من خلال اتخاذ مجموعة من الإجراءات

والتدابير التى تهدف إلى حماية الطلاب والمعلمين وكذلك الأفراد من المخاطر الإلكترونية المختلفة مثل وضع سياسات وإجراءات وضحة لاستخدام الإنترنت فى المؤسسات التعليمية المختلفة تحدد المواقع والتطبيقات المسموح بها والمحظورة ، ووضع سياسات واضحة لحماية خصوصية الطلاب وبياناتهم الشخصية ، وهذا بدوره يؤدى الى بناء مجتمع رقمى أكثر أماناً ، وإعداد أجيال قادرة على مواجهة تحديات العصر الرقمى وحماية أنفسهم من الجرائم الإلكترونية المتطورة ،

- **دور الدولة**

تلعب الدولة دوراً أساسياً فى حماية المجتمع من الجرائم الإلكترونية التى تستخدم تقنيات الذكاء الاصطناعى وذلك من خلال الآتى:

أ. سن القوانين والتشريعات:

من خلال وضع قوانين صارمة تجرم الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى وتعاقب مرتكبيها ، مع العمل على تحديث التشريعات باستمرار لمواكبة تطورات الذكاء الاصطناعى المستمرة وكذلك أساليب الابتزاز والاحتيال الرقمى ، مع فرض عقوبات رادعة على من يستخدم الذكاء الاصطناعى فى ارتكاب الجرائم الإلكترونية المختلفة ، وتذكر احد حالات الدراسة " **لابد من تغليظ العقوبات على الجناة مرتكبى الجرائم الإلكترونية المختلفة**" ، وتذكر ايضاً احدى حالات الدراسة "**التشريعات والقوانين لازم تكون متطورة لأن الجرائم الإلكترونية تستخدم الذكاء الاصطناعى فى ارتكابها**"

يتضح لنا هنا أن سن القوانين والتشريعات من أهم الأدوات التى تستخدمها الدول والمجتمعات لمواجهة الجرائم الإلكترونية ، خاصة تلك المدعومة بتقنيات الذكاء الاصطناعى ، فتساهم هذه القوانين فى تحديد الأفعال غير القانونية وتحديد العقوبات المناسبة لها مما يردع المجرمين ويحمى الضحايا.

ب.تأمين البنية التحتية الرقمية:

من خلال حماية الأنظمة الرقمية المختلفة من الهجمات الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى وايضاً من خلال تطوير أنظمة المراقبة متطورة ومحدثة للكشف عن التهديدات الإلكترونية والتصدى لها ، مع تعزيز الأمن الإلكترونى فى المنصات الرقمية المختلفة مثل مواقع التواصل الاجتماعية والحسابات الشخصية والحسابات البنكية ، وتذكر احدى حالات الدراسة"**لابد من توفير الأمان الإلكترونى وتطوير اجهزة الدولة للكشف والتحقق من الجرائم الإلكترونية بسهولة**"

يتضح لنا ان تأمين البنية التحتية الرقمية أمراً بالغ الأهمية ، حيث أصبحت حياتنا اليومية تعتمد بشكل كبير على التقنيات الرقمية وهناك بعض الجوانب الرئيسية لتأمين البنية التحتية منها حماية الشبكات ، حماية البيانات ، وحماية الأجهزة الإلكترونية والتوعية والتدريب المستمر بمخاطر الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، فمن خلال تنفيذ هذه الإجراءات يمكن للمؤسسات والأفراد حماية البنية التحتية الرقمية من التهديدات الأمنية المتزايدة.

ج.تسهيل الإبلاغ والمساعدة القانونية:

وذلك من خلال إنشاء منصات إلكترونية للإبلاغ عن الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى تسهيلاً على الضحايا مع توفير خطط حماية قانونية للضحايا ومساعدتهم فى استرداد حقوقهم ، وتذكر احد حالات الدراسة "**تمكنت الأجهزة الأمنية من تتبع عنوان ip للمجرم ، وتوصلت إلى هويته ، وتبين أنه شخص محترف فى النصب والابتزاز الإلكترونى وكان يستهدف الضحايا ، وتم القبض عليه وتمت مصادرة الأجهزة والبرامج التى استخدمها فى ارتكاب الجريمة**".

يتبين لنا هنا ان تسهيل الإبلاغ والمساعدة القانونية من العناصر الأساسية فى مكافحة الجرائم الإلكترونية ، حيث يشجع الضحايا على الإبلاغ عن الجرائم ويضمن حصولهم على الدعم القانونى اللازم ، وذلك من خلال إنشاء منصات إلكترونية للإبلاغ ، تبسيط الإجراءات القانونية ، نشر الوعى القانونى للجمهور حول حقوقهم القانونية فى حالة التعرض لجرائم إلكترونية ، وتتفق هذه النتيجة مع ما توصلت اليه دراسة**(ابراهيم،٢٠٢٣)** فى تحرير بلاغ فى مباحث الإنترنت ضد الجانى.

نستنتج مما سبق أن الدولة تساهم بمختلف الطرق فى بناء بيئة رقمية أكثر أماناً ، وتحد من تأثير الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى على الأفراد وذلك من خلال سن القوانين والتشريعات ، وتأمين البنية التحتية الرقمية ، وتسهيل الإبلاغ والمساعدة القانونية، فمن خلال هذه الإجراءات تسعى الدولة إلى خلق بيئة رقمية آمنة ، وحماية مواطنيها من مخاطر الجرائم الإلكترونية.

❖ النتائج العامه للبحث:

استطاعت الدراسة الإجابة على التساؤلات الآتية:

أولاً: تمكنت الدراسة من الإجابة على التساؤل الأول ، الذى يتناول كيفية إسهام الذكاء الاصطناعى فى تسهيل وتعزيز ارتكاب الجرائم الإلكترونية ضد الأفراد.

أ. تعرضت جميع حالات الدراسة الميدانية لمختلف أشكال الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى والتى تمثلت فى جرائم الابتزاز والتشهير : حيث يتم استغلال بيانات وصور الضحايا للضغط عليهم لتحقيق مكاسب معينة ، جرائم سرقة الحسابات البنكية: والتى تتضمن الوصول غير المصرح به إلى الحسابات المالية وسحب الأموال ، جرائم الابتزاز الجنسى: والتى تعتمد على تهديد الضحايا بنشر محتوى خاص بهم بهدف الحصول على المال أو تنفيذ طلبات محددة ، جرائم تشويه السمعة : من خلال نشر معلومات مضللة أو صور وفيديوهات مفبركة باستخدام تقنيات الذكاء الاصطناعى ، جرائم القرصنة الإلكترونية (الهاكرز): والتى تشمل اختراق الأنظمة والشبكات لتحقيق أهداف غير مشروعة ، جرائم سرقة الحسابات الشخصية عبر مواقع التواصل الاجتماعى: مما يؤدى إلى انتحال الهوية أو استخدامها لأغراض احتيالية.

ب. تبين أن الجرائم الإلكترونية التى تعرض لها الضحايا وقعت خلال فترة زمنية تتراوح بين ثمانية أشهر إلى عام ، أو خلال فترة ارتباط المجرم بالضحية ، كما أن بعض هذه الجرائم تزامنت مع وصول الحساب الشخصى للضحية إلى ٥٠ ألف متابع ، ويرجع ذلك لزيادة الظهور الرقمى فأرتفاع عدد المتابعين جعل الحسابات الشخصية أكثر جذباً للمجرمين الإلكترونيين ، حيث يمكنهم استغلال شهرة الضحية لتحقيق مكاسب غير مشروعة ، وتطور تقنيات الذكاء الاصطناعى فتمكن المجرمون من استخدام أدوات الذكاء الاصطناعى لتزييف المحتوى مثل Deepfake ، واستغلال العلاقات الاجتماعية ففى بعض الحالات استغل المجرم العلاقة المباشرة مع الضحية لجمع بيانات شخصية للوصول إلى حساباتها ، مما سهل تنفيذ الجريمة.

ج. تبين أن آلية تنفيذ الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى قد تنوعت وتعددت ، حيث استغل المجرمون بناء علاقات عاطفية مع الضحايا لكسب ثقتهم ثم استغلالهم مالياً أو للحصول على معلومات حساسة ، وقد اعتمد تنفيذهم لجرائمهم على بناء العلاقات وكسب الثقة ، وجمع المعلومات الشخصية والحساسة ، والاستغلال المالى والابتزاز ، وتنفيذ عمليات الاحتيال المختلفة.

ثانياً: تمكنت الدراسة من الإجابة على التساؤل الثانى ، الذى يتناول الدوافع والأسباب المؤدية إلى ارتكاب الجرائم الإلكترونية المدعومة بالذكاء الاصطناعى ، وذلك وفقاً لوجهة نظر الضحايا

أ. **فيما يتعلق بالأسباب الاجتماعية** المؤدية إلى الجرائم الإلكترونية ، فقد تعددت وتنوعت حيث شملت التفكك الأسرى ، وضعف الرقابة العائلية ، وغياب الرقابة المجتمعية ، بالإضافة إلى تلبية الحاجات الاجتماعية والجنسية بطرق غير مشروعة ،

ب. **أما الأسباب الاقتصادية** لارتكاب الجرائم الإلكترونية فقد تمثلت فى الضغوط المالية ، والرغبة فى تحقيق الثراء السريع ، فضلاً عن البطالة التى تدفع بعض الأفراد إلى البحث عن وسائل غير قانونية للحصول على المال ،

ج. **وفيما يخص الأسباب الثقافية** المؤدية إلى الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، فقد تمثلت فى التطور التكنولوجى المتسارع ، والتأثيرات الثقافية السلبية ، إلى جانب انتشار ثقافة الإفلات من العقاب ، أما الأسباب الذاتية ، فقد ارتبطت برغبة الجانى فى إثبات ذاته ، وتحقيق مكانة اجتماعية ،والسعى لإلحاق الأذى بالضحايا بدافع الانتقام والتسلية.

ثالثاً: تمكنت الدراسة من الإجابة على التساؤل الثالث ، الذى يتناول أبرز المخاطر والتحديات التى يواجهها الضحايا بعد تعرضهم للجرائم الإلكترونية المعتمدة على تقنيات الذكاء الاصطناعى

وفيما يتعلق بالمخاطر والتحديات التى تواجه الضحايا نتيجة الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، فقد تنوعت آثارها لتشمل الجوانب الاجتماعية والاقتصادية والنفسية.

أ. **وفيما يتعلق بالآثار الاجتماعية:** تتمثل فى العزلة الاجتماعية ، وتدمير السمعة الشخصية والمهنية ، بالإضافة إلى تهديد العلاقات الأسرية والاجتماعية ، مما يؤثر على استقرار الضحية فى محيطها الاجتماعى .

ب. **وفيما يتعلق بالآثار الاقتصادية:** تشمل على الخسائر المالية المباشرة ، وفقدان الوظائف ، وفرص العمل ،إلى جانب ارتفاع التكاليف القانونية الناجمة عن محاولات استعادة الحقوق أو مواجهة التبعات القانونية لهذه الجرائم .

ج. **وفيما يتعلق بالآثار النفسية:** تتمثل فى القلق والتوتر المستمر ، والتأثيرات النفسية العميقة التى قد تصل إلى اضطرابات عاطفية ، مما يؤثر على الأداء المهنى والأكاديمى للضحايا ، ويؤدى إلى تراجع مستوى إنتاجيتهم وثقتهم بأنفسهم.

رابعاً: تمكنت الدراسة من الإجابة على التساؤل الرابع ، الذى يبحث فى كيفية تعامل ضحايا الجرائم الإلكترونية المعتمدة على تقنيات الذكاء الاصطناعى مع الجريمة عند وقوعها بالإضافة إلى الإجراءات التى يتخذونها لمواجهتها.

أ. وعن موقف الضحايا عند التعرض للجرائم الإلكترونية المختلفة المدعومة بتقنيات الذكاء الاصطناعى فقد تعددت وتمثلت فى الصدمة والارتباك ، والبحث عن الدعم والمساعدة ، واتخاذ الاجراءات الأمنية والقانونية.

ب. أما بالنسبة لموقف الضحايا عند تعرضهم للجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، فقد اختلفت ردود أفعالهم وتعددت ، حيث تمثلت فى الصدمة والارتباك ، والبحث عن الدعم والمساعدة ، واتخاذ الإجراءات الأمنية والقانونية.

خامساً: تمكنت الدراسة من الإجابة على التساؤل الخامس ، الذى يتناول أهم المقترحات والتوصيات التى يراها الضحايا ضرورية لحماية الأفراد من الجرائم الإلكترونية المعتمدة على تقنيات الذكاء الاصطناعى.

وفيما يتعلق بالمقترحات التى يمكن أن تسهم فى حماية الأفراد من الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى فقد تنوعت على عدة محاور رئيسية ،

أ. يتمثل دور **الأسرة** فى الإشراف والمراقبة ، وتعزيز التوعية والتثقيف ، وتشجيع التواصل الأسرى الفعال .

ب. أما **وسائل الإعلام** فتتمثل مسؤوليتها فى تقديم الإرشادات والنصائح التقنية ، ورصد وكشف أساليب الاحتيال الإلكترونى .

ج. من جانبها تؤدى **المؤسسات التعليمية** دوراً مهماً فى تعزيز القيم والسلوك الرقمى الأخلاقى ، وتهيئة بيئة إلكترونية آمنة ،إلى جانب استخدام التكنولوجيا فى توعية الأفراد وحمايتهم .

د. وأخيراً تضطلع **الدولة** بمسئولية سن القوانين والتشريعات اللازمة ، وتعزيز أمن البنية التحتية الرقمية ، وتسهيل إجراءات الإبلاغ عن الجرائم الإلكترونية ، بالإضافة إلى تقديم الدعم والمساعدة القانونية للضحايا.

❖ توصيات البحث:

- تعزيز الوعى المعرفى حول مخاطر الجرائم الإلكترونية المدعومة بالذكاء الاصطناعى، من خلال نشر الوعى بين المواطنين ، وخاصة الشباب حول مخاطر التعامل مع المواقع والتطبيقات الإلكترونية التى قد تستغل تقنيات الذكاء الاصطناعى فى عمليات الاحتيال والاختراقات الإلكترونية.
- تفعيل دور المجتمع المدنى والمؤسسات الحكومية فى التوعية والوقاية ، فيجب أن تلعب المؤسسات الحكومية والمجتمع المدنى دوراً محورياً فى توعية الأفراد حول الأساليب الحديثة التى يستخدمها المجرمون لاستغلال الذكاء الاصطناعى فى الجرائم الإلكترونية ، وتوفير برامج تدريبية لمكافحة هذه التهديدات.
- ينبغى على الحكومات والجهات المانحة والمنظمات متعددة الأطراف دعم أنظمة البحث العلمى وتطوير حلول أمنية متقدمة قائمة على الذكاء الاصطناعى ، مما يسهم فى التصدى للهجمات السيبرانية وجرائم الاحتيال الإلكترونى .
- تعزيز التعاون بين الجهات المختصة والباحثين ، فيتطلب التصدى للجرائم الإلكترونية المدعومة بالذكاء الاصطناعى تعزيز التعاون بين المؤسسات الأمنية والجهات البحثية من خلال تبادل البيانات والإحصاءات حول أنماط الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعى ، مما يساعد فى تطوير استراتيجيات أكثر فعالية لمكافحتها.
- إجراء المزيد من الدراسات حول تأثير الذكاء الاصطناعى على الجريمة الإلكترونية ، نظراً للتطوير المستمر لتقنيات الذكاء الاصطناعى وأساليب استغلالها فى الجرائم الإلكترونية ، فمن الضرورى تشجيع الأبحاث العلمية لمواكبة هذه التطورات ، وتحليل أنماط الجرائم الناشئة ، واقتراح آليات للحد منها وحماية الأفراد والمؤسسات.

المصادر والمراجع:

أولاً المراجع العربية

١. **ابراهيم ، جيهان محمد على الشيخ**(٢٠٢٣): الابعاد الاجتماعية للتنمر الإلكترونى وتأثيراتها على الضحيه "دراسة لبعض الحالات فى جامعه دمياط"، مجله بحوث العلوم الاجتماعية والتنمية، المجلد الخامس، المنيا

٢. _____، **وعبدالجواد، محمد سمير ابو الفتوح**(٢٠٢٤): مواقع التواصل الاجتماعى وعلاقتها بجنوح الشباب "دراسة ميدانية على عينه من مستخدمى تطبيق التيك توك"، المجلة العلمية لكليه الآداب ، جامعه الآداب ، جامعه اسيوط، العدد٩٢، اسيوط.

٣. **الأميرى ، امينه ابراهيم ،والعموش ، احمد فلاح**(٢٠٢٢): اثر استخدام التكنولوجيا كنشاط روتينى فى زيادة معدلات الجريمه ، مجله الآداب ، جامعه بغداد ،المجلد١، العدد ١٤٣، العراق.

٤. **البابلى ، عمار ياسر محمد زهير**(٢٠٢٤): دور الذكاء الاصطناعى فى مواجهه الجريمة المنظمة عبر العالم الافتراضى "دراسة تحليليه"، مجله الدراسات القانونيه والأمنيه ، اكاديمية الشرطة ، مركز البحوث والدراسات الأمنية ، مجلد٤، العدد٢، القاهرة.

٥. **باسه ، ابراهيم، وراقيه ، بغدادى**(٢٠٢٣): تأثير صناع المحتوى فى التيك توك على سلوك الشباب الجامعى ، رساله ماجستير غير منشورة ، جامعه محمد خضير بسكرة ، كليه العلوم الانسانيه والاجتماعيه ، قسم العلوم الانسانيه ، الجزائر.

٦. **بن عبدالله ، نوال قادة ، وبن حمو ، محمد**(٢٠٢٢): الجريمه الإلكترونية : قراءة سوسيولوجيه لأهم النظريات المفسرة للسلوك الإجرامى ، مجله روافد للدراسات والابحاث العلمية فى العلوم الاجتماعية والانسانية ، المركز الجامعى بلحاج بوشعيب ،عين تموشنت ، المجلد٦، العدد٣، الجزائر.

٧. **التميمى ، عقيل نجم مهدى**(٢٠٢٤): المسؤوليه الإداريه عن الأفعال غير المشروعه للذكاء الاصطناعى ، مجله العلوم الإنسانيه والطبيعيه ، مجله علميه محكمه ، المجلد٥،العدد٥، العراق.

٨. **جنيفر ، هلاس**(٢٠٢٠): نظريه الاستخدامات والاشباعات، جامعه وهران احمد بن بله، كليه العلوم العلوم الانسانيه والعلوم الاسلاميه ، قسم علوم الاعلام والاتصال ، الجزائر.

٩. **جواد ، اشرف حسن محمد**(٢٠١٥): الجريمة المعلوماتيه او الإلكترونية انواعها وخصائصها وطرق الوقايه منها ، مجله الدراسات الماليه والمعرفيه ، الأكاديمية العربية للعلوم الماليه والمعرفيه ، مركز البحوث الماليه والمعرفيه ، المجلد٢٣، العدد١،الأردن .

١٠. **الحاج ، عمر محمد خير(٢٠٠٢)**: العولمه وآثارها فى تطور الجريمه ، مجله الأمن والقانون ، اكاديمية شرطه دبر ، المجلد١٠، العدد١، الامارات.

١١. **حسين ، منى على عبدالله (٢٠٢٢)**: أنماط الجريمة الإلكترونية من وجهة نظر طلاب بحوث التخرج بكليتى الآداب والعلوم بجامعه سبها، مجلد العلوم الانسانية العدد ٢١، المجلد ٣، ليبيا.

١٢. **حطاب ، حاجه خيرة (٢٠١٥)**: مواقع التواصل الاجتماعى : فضاء جديد للجريمه ، المجله العربيه فى العلوم الانسانيه والاجتماعية ، جامعه الجلفه، العدد٢٨، الجزائر.

١٣. **الحوتى ، فتحيه السيد(٢٠٢٠)**: الابعاد الاجتماعيه والثقافيه للجرائم الالكترونية فى مصر"دراسه تحليليه لطائفه من الحالات بسجن شديد الحراسه بجمصه محافظة الدقهلية" ، مجله كليه الآداب، جامعه الفيوم ، مجلد ١٢، العدد١، الفيوم.

١٤. **الداغر، مجدى(٢٠٢٤)**: رؤيه الخبراء لتطبيقات الذكاء الاصطناعى فى الكشف عن الأدلة الجنائية المصاحبة لجرائم شبكات التواصل الاجتماعى واتجاهاتهم نحو سيناريوهات تبنى توظيفها فى المؤسسات الأمنية العربية ، المجلة المصرية لبحوث الرآى العام ، المجلد ٢٣، العدد ٤، القاهرة.

١٥. **دبابنه، شيرين(٢٠١٥)**: الجرائم الإلكترونيه القرصنه الإلكترونية ، مجلة الدراسات الماليه والمصرفيه ، الاكاديمية العربية للعلوم الماليه والمصرفيه ، مركز البحوث الماليه والمصرفيه ، مجلد٢٣، العدد١، الاردن.

١٦. **الدسوقى ، منى محمد العتريس(٢٠٢٢)**: جرائم تقنيات الذكاء الاصطناعى والشخصيه القانونية الإلكترونية المستقله"دراسه مقارنه"، مجلة البحوث القانونية والاقتصادية ، جامعة المنصورة ، كلية الحقوق، العدد٨١، المنصورة.

١٧. **الدوسرى ، سمحان بن محمد ذيب(٢٠١٨)**: المؤسسات المجتمعية ودورها فى وقايه الشباب من التطرف فى ضوء نظريه النشاط الروتينى، المؤتمر الدولى السنوى لكليه الآداب : الشباب وصناعه المستقبل ، جامعه عين شمس ، كليه الآداب، القاهرة.

١٨. **دولى ، لخضر ، وناصرى ،نفيسه(٢٠١٨)**: دور الذكاء الاصطناعى فى مواجهة الجرائم الإلكترونية ، مجلة المؤشر للدراسات الاقتصادية ، جامعه طاهرى محمد ، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير ، مخبر الدراسات الاقتصادية والتنمية المحلية بالجنوب الغربى ، المجلد٢ ، العدد٢، الجزائر.

١٩. **الذباحى، على سيف**(٢٠٢٤): الذكاء الاصطناعى والجريمة ، الفكر الشرطى، القيادة العامة لشرطة الشارقه ، مركز بحوث الشرطة ، مجلد٣٣، العدد١٣٠، الامارات.

٢٠. **ذياب، سليمه ، وبوترعه ، بلال** (٢٠٢٠): الجريمة الإلكترونية " الأسس والمفاهيم ، مجله تطوير العلوم الاجتماعية ، العدد١، المجلد ١٣، جامعه الجلفة، الجزائر.

٢١. **رجب ، سها عيد**(٢٠٢٣): الجرائم الإلكترونية ووعى الشباب بانتهاكها لخصوصيه الفرد ، حوليات آداب عين شمس ، جامعه عين شمس ، كليه الآداب، مجلد٥١، القاهرة.

٢٢. **رقيه ، سلامه ، ويسرى ،نكاع (٢٠٢١)**:تداعيات شبكات التواصل الاجتماعى على المجتمع الجزائرى فى الحجر الصحى "الجريمة الإلكترونية أنموذجاً" وبائية الاضطرابات النفسية فى ظل الحجر الصحى الاسباب التداعيات ، طرق العلاج ، جامعة سطيف، يومى ٤/٥، ديسمبر، الجزائر.

٢٣. **الزبن ، ابراهيم بن محمد** (٢٠٢١): التفسيرات النفسية والاجتماعية للجرائم المعلوماتية والعوامل الدافعه لإرتكابها، مجله العلوم الانسانية ، جامعه حائل ، العدد١٢، السعودية.

٢٤. **السيد، خالد السيد شحاته** (٢٠٢٣): علم الجريمه الرقمى ومداخله السوسيولوجيه الحديثه المفسرة للجريمة فى مجتمع الرقمنه : نموذج نظرى ، مجله الدراسات الإنسانيه والأدبيه ، جامعه كفر الشيخ ، كليه الآداب ، العدد ٢٨، كفر الشيخ.

٢٥. **الشاهد ، محمود فكرى**(٢٠٢٤): الاطار القانونى لتأثير الأوراق التجارية الإلكترونية بتقنيات الذكاء الاصطناعى ، مجله المعهد العالى للدراسات النوعية ، مجلد ٤، العدد٤، القاهرة.

٢٦. **الشمرى، مصطفى ابراهيم سلمان**(٢٠٢١): الجرائم الإلكترونية وتأثيرها فى العراق ، المؤتمر العلمى الدولى التاسع بعنوان (العراق بعد عام ٢٠٠٣ الدولة المجتمع الاقتصاد ، العلاقات الخارجيه التحديات والفرص)، مركز الدراسات الاقليمية ، جامعه الموصل ، العراق.

٢٧. **الشهومية ، ابتسام سعيد ، والكندى ، سالم بن سعيد** (٢٠٢٤): تأثير استخدام تطبيقات الذكاء الاصطناعى على على الخصوصية الرقمية "دراسة حاله فى سلطنه عمان"، جامعه السلطان قابوس ، مجله الآداب والعلوم الاجتماعية ، المجلد ١٥، العدد٣، عمان.

٢٨. **طاله ، لاميه**(٢٠٢٠): الجريمة الالكترونيه : بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الاجتماعى ، مجله الرواق للدراسات الاجتماعيه والإنسانيه ، المركز الجامعى احمد زبانه ، مخبر الدراسات الاجتماعيه والنفسيه والانثروبولوجيه، المجلد ٦، العدد٢، الجزائر.

٢٩. **عادل ،لبيض ، وبشرى ، نزلى**(٢٠١٨): إثبات الجريمة الإلكترونية ، جامعه قاصدى مرباح ، ورقله ، كلية الحقوق والعلوم السياسيه ، قسم الحقوق ، رساله ماجستير غير منشورة ، الجزائر.

٣٠. **عبد الحكيم ، عماريه** (٢٠٢٢): اليقظة التكنولوجية وتحديات مواجهه الجريمه الالكترونية، ورقه عمل بمؤتمر بعنوان(المسائل الجديدة التى يطرحها تطور تكنولوجيا الاعلام والاتصال وتأثيرها على الجزائر" التهديدات السيبرانية الجديدة على الجزائر")، جامعه باتنه ، الجزائر.

٣١. **عبد الرازق، رانا مصباح عبدالمحسن** (٢٠٢١): تأثير الذكاء الاصطناعى على الجريمه الإلكترونية ، المجله العلمية لجامعه الملك فيصل ، العلوم الانسانية والإدارية، جامعه الملك فيصل ، المجلد٢٢،العدد١، السعودية.

٣٢. **عبد السلام ، امانى محمد شريف** (٢٠٢٣): التغير القيمى لدى طلاب جامعه اسيوط فى ضوء بعض التغيرات المعاصرة ، المجله العلمية لكلية التربية ، جامعه اسيوط ،عدد خاص بالمؤتمر العلمى (تطوير التعليم اتجاهات معاصرة ورؤى مستقبلية)، المجلد ٣٩، العدد ١٠، جزء ثانى ، اسيوط.

٣٣. **العزعزى ، وديع محمد سعيد**(٢٠١٥): استخدامات الشباب الجامعى لشبكه التواصل الاجتماعى (فيسبوك): دراسه مسحيه على طلبه كليات وأقسام الاعلام فى اربع جامعات عربيه ، المجله العربية للاعلام والاتصال ، الجمعيه السعوديه للأعلام والاتصال ، العدد١٤، السعوديه.

٣٤. **العميريين ، وجيه محمد سليمان**(٢٠٢٢): الذكاء الاصطناعى فى التحرى والتحقيق عن الجريمة :دراسة مقارنة، مجله الميزان للدراسات الإسلاميه والقانونية ، جامعه العلوم الإسلاميه العالمية ، عمادة البحث العلمى، المجلد٩، العدد٣، عمان.

٣٥. **عوض، السيد(٢٠١٨)**: التطور التكنولوجى والجريمة ، المجله الدوليه للآداب والعلوم الانسانيه والاجتماعية ، الأكاديمية العربيه للعلوم الانسانيه والتطبيقية ، العدد١٦،الجزء الاول، لبنان.

٣٦. **عيسات ،العمرى ، وبوعزة ، عبد الرؤوف(٢٠٢٢)**: الجريمة الالكترونية لدى المراهقين : دوافع الاقبال وآليات الضبط الاجتماعى ، مجله علوم الانسان والمجتمع ، جامعه محمد خضير بسكرة ، كليه العلوم الانسانية والاجتماعية ، المجلد ١١، العدد ١، الجزائر

٣٧. **فاطيمه ، الزهراء** (٢٠٢٣): مفهوم وتطور الجريمة الإلكترونية ، المجلة الاردنية الدولية اريام للعلوم الانسانية والاجتماعية ، مركز اريام للبحوث والدراسات ، المجلد ٥، العدد٣،الاردن.

٣٨. **الفراوى ، مبروكه عبد السلام غيث**(٢٠١٦): دور الانترنت ووسائل التقنيه الحديثه فى الجريمه المنظمة : الايجابيات والسلبيات ، المجله العربيه للعلوم الاجتماعية، المؤسسه العربية للاستشارات العلمية وتنمية الموارد البشرية ، العدد٩، المجلد٤، ليبيا.

٣٩. **محمد ، الصيدانى ،وامنيه ، الأخنش نورة** (٢٠٢٣):الذكاء الاصناعى كآليه لمجابهة الجريمة الإلكترونية ، مجلة القانون والعلوم البيئية ، المجلد ٢، العدد٢، الجزائر.

٤٠. **محمد ، عمار طاهر، والموسوى ، سعد معن**(٢٠٢٢): دوافع استخدام السجينات للقنوات الفضائية والاشباعات المتحققة منها "دراسه ميدانيه على الحكومات بالاعدام"، وقائع المؤتمر العلمى السنوى الخامس عشر لكليه الاعلام ، جامعه بغداد ، بغداد

٤١. **مراد، سالى**(٢٠١٥): ضحايا الجريمه منظور سوسيولوجى ، مجله الحوار الثقافى ، جامعه عبد الحميد بن باديس ، كليه العلوم الاجتماعية ، مخبر حوار الحضارات والتنوع الثقافى وفلسفة السلم ، المجلد٤، العدد٢، الجزائر.

٤٢. **المشهدانى ،اكرم عبد الرازق** (٢٠١٥): الجرائم الإلكترونية :التحديات والمعالجة ، مجلة الدراسات الماليه والمعرفيه ، الأكاديمية العربية للعلوم الماليه والمعرفيه ، مركز البحوث الماليه والمعرفيه ، المجلد٢٣، العدد١،القاهرة.

٤٣. **مغايرة ، علاء الدين منصور** (٢٠٢٤): جرائم الذكاء الاصطناعى وسبل مواجهتها جرائم التزييف العميق نموذجاً ، المجله الدولية للقانون ، جامعه قطر ، كليه القانون ، المجلد ١٣،العدد٢،قطر.

٤٤. **الهديف ، مفتاح ميلاد** (٢٠٢٢): الجرائم الإلكترونية ، مجلة التربوى ، مجله علمية محكمه تصدر عن كليه التربيه ، جامعه المرقب ، العدد٢٠، ليبيا.

٤٥. **الوخى ، عربى عبد العزيز احمد** (٢٠٠٢): دوافع استخدامات الأطفال لشبكه الانترنت والاشباعات المتحققه ، المجله المصريه لبحوث الرأى العام، جامعه القاهرة ، كليه الأعلام ، مركز بحوث الرأى العام، المجلد٣، العدد٤، القاهرة.

ثانياً: المراجع الاجنبية:

1. **Alkharabsheh**, **M**. **M**., **& Alshraideh**, **M**. (**2023**). Enhancing cybercrime deterrence with artificial intelligence. International Journal of Advanced Networking and Applications, 15(4).
2. **Day**, **J**. **C**., **Janus**, **A**., **& Davis**, **J**. (**2005**). Computer and internet use in the United States. U.S. Department of Commerce. Retrieved from https://www.census.gov/prod/2005pubs/.pdf
3. **Dilek**, **S**., **& Cakir**, **H**. (**2015**). Applications of artificial intelligence techniques to combating cyber crimes: A review. International Journal of Artificial Intelligence & Applications (IJAIA), 6(1).
4. **Ekanem**, **D**. (2020). Artificial intelligence as a mechanism for crime control in Nigeria: A critical appraisal. LAP LAMBERT Academic Publishing.
5. **Gupta**, **S**., **Singh**, **A**., **Kumari**, **S**., **& Kunwar**, **N**. (**2017**). Impact of cyber crime through social networking sites on adolescents' perceptions of social issues. International Journal of Law, 3(6).
6. **Hubbard**, **F**. **P**. (**2011**). "Do androids dream?": Personhood and intelligent artifacts. Temple Law Review, 83(1).
7. **Lozonschi**, **C**., **& Bakhaya**, **I**. (**2023**). Artificial intelligence and its impact on cybercrime. Proceedings of the International Conference on Cybersecurity and Cybercrime, Vol. X.
8. **Mijwil**, **M**. **M**., **& Aljanabi**, **M**. (**2023**). Towards artificial intelligence-based cybersecurity: The practices and ChatGPT-generated ways to combat cybercrime. Iraqi Journal for Computer Science and Mathematics, 16(4). Published by the University of Tehran, College of Management.
9. **Nasrallah**, **N**. **M**. (**2021**). Using artificial intelligence (AI) in banking services. Introductory Booklet Series, Issue No. 24. Arab Monetary Fund.

10. **Parti**, **K**., **& Dearden**, **T**. (**2023**). Understanding the use of artificial intelligence in cybercrime. International Journal of Cybersecurity Intelligence & Cybercrime, 6(2).

11. **Rehnström**, **F**. (**2021**). How capable is artificial intelligence (AI) in crime prediction and prevention? A literature review of reviews. Örebro University, School of Law, Psychology and Social Work.

12. **Sellers**, **S**. **C**. (**2011**, **December**). The influence of social networking websites on youth's behavior [Master's dissertation, Lamar University]. The Faculty of the College of Graduate Studies.

13. **Shamiulla**, **A**. **M**. (**2019**). Role of artificial intelligence in cybersecurity. International Journal of Innovative Technology and Exploring Engineering, 9(1).

14. **Zandi**, **G**., **Yaacob**, **N**. **A**., **Tajuddin**, **M**., **& Nik Abdul Rahman**, **N**. **K**. (**2024**). Artificial intelligence and the evolving cybercrime paradigm: Current threats to businesses. Journal of Information Technology Management, 16(4).