عَمادة الدِّراسات العليا
جامعة القدس

مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة

كاترين عيسى محمد أبوعلان

رسالة ماجستير

القدس – فلسطين

1443هـ / 2022م

مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة

إعداد:

كاترين عيسى محمد أبوعلان

بكالوريوس علم اجتماع من جامعة فلسطين الأهليّة/فلسطين

المشرف: د. وفاء الخطيب

قُدِّمتْ هذه الدراسةُ استكمالًا لمتطلّبات الحصول على درجة الماجستير في العدالة الجنائيّة وعلم الجريمة – عَمادة الدراسات العليا– جامعة القدس

1443هـ / 2022م

جامعة القدس

عَمادَة الدّراسات العليا

ماجستير العدالة الجنائيّة وعلم الجريمة

إجازة الرّسالة

مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة

اسم الطالبة: كاترين عيسى محمد أبوعلان

الرقم الجامعي: 21811505

المشرف: د. وفاء الخطيب

نوقِشتْ هذه الرسالةُ وأُجيزتْ بتاريخ: 21 / 5/ 2022 من لجنة المناقشة المدرجة أسماؤهم وتواقيعهم أدناه:

1. رئيس لجنة المناقشة: د. وفاء الخطيب التوقيع:.....
2. ممتحناً داخلياً: أ.د.عايد الوريكات التوقيع:
3. ممتحناً خارجياً: أ.د. عباطه الظاهر التوقيع:

القدس – فلسطين

1443هـ / 2022 م

الإهداء

إلى القلوب الكبيرة والنُّفوس الطَّيِّبة (أبي وأمي).

إلى القلوب الطّاهرة والرّقيقة أخوتي (إسلام – عبير – عبيدة).

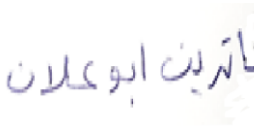
إلى رفيق الَّدرب وشريك الحياة (ماجد).

إلى كُلِّ مَنْ ساعدني في إتمام هذه الدِّراسة.

كاترين عيسى محمد أبوعلان

إقْرار

أُقِرُّ أنا مُعِدَّةَ الرِّسالةِ بأنَّ هذهِ الدِّراسةِ قُدِّمت لجامعة القدس؛ لنيل درجة الماجستير، وأنّها نتيجة أبحاثي الخاصّة، باستثناء ما أُشيرَ إليه حيثُما ورَدَ، وأنَّها –أو أيّ جزء منها– لم يُقدَّمْ لنيل درجة عُليا لأيِّ جامعةٍ أو معهدٍ آخَرَ.

التوقيع: 

الاسم: كاترين عيسى محمد أبوعلان

التاريخ: 21/ 5 /2022

الشُّكر والتَّقدير

الحمدُ لله الَّذي علَّم بالقلم، علَّم الإنسان ما لم يعلَمْ، والصّلاة والسلام على النّبي الأكرم نبيِّنا محمد صلوات الله عليه، الحمد لله الذي وفَّقنا وهدانا لهذا، وما كنا لنهتدي لولا أنْ هدانا الله أما بَعْدُ
فإنّه لا يَسعُني في هذا المقام إلّا أن أتقدم بالشكر والتقدير إلى أُستاذتي ومشرفتي الدّكتورة وفاء الخطيب، التي قدَّمَتْ لي كلَّ جَهْد واهتمام، وزوَّدتني بالمعلومات والملحوظات؛ لإتمام هذا العمل، فلها مني جلُّ الاحترام والتقدير، كما أتقدَّمُ بأجمل آيات الشُّكر إلى عائلتي التي كانت خير سَنَدٍ لي طيلة فترة الدِّراسة.

كما أتقدّم بأسمى عبارات الشُّكر والتقدير إلى أعضاء لجنة المناقشة الموقَّرين؛ لِتَكرُّمِهم بمناقشة الرسالة ولمَلْحوظاتِهِم القيّمة فلهم مني جزيل الشكر والتقدير، ولا أنسى مديري العقيد/ جمال طقاطقة؛ لما قدَّمَه لي من نصيحةٍ وتسهيلٍ في الدراسة، والشُّكرُ موصولٌ –أيضًا– إلى العاملين في وزارة الاتِّصالات وتكنولوجيا المعلومات؛ لما قَدَّموه من دعْمٍ وتعاون في الإجابة عن أسئلة المقابلة، وإلى كُلِّ من أسْهمَ في إنجاز هذه الرسالة أسمى آيات الشكر والتقدير.

كاترين عيسى محمد أبوعلان

الملخص:

هدفت الدراسة التعرف الى مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة، استنادًا إلى طبيعة الدراسة وأهدافها، استخدامت الدراسة المنهج الوصفي بشقه الكيفي (النوعي) من خلال استخدام دليل المقابلة؛ حيث تكوَّن مُجتمع الدراسة وعينته من جميع العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في مدينة رام الله والبيرة من فئة العاملين في تكنولوجيا المعلومات والاتصالات البالغ عددهم (50) حسب إحصائيات (وزارة الاتّصالات وتكنولوجيا المعلومات،2021)

تمّ تحليل أسئلة المُقابلة وتمّ التوصل لمجموعة من النتائج لعل من أهمها أن للذَّكاء الاصطناعيّ دورًا قويًّا وفعالًا جدًّا في الكشف عن الجريمة الإلكترونيّة، وأن هناك ضرورة لسن قوانين وتشريعات تتعلق ببرامج الذَّكاء الاصطناعيّ بالإضافة الى تشديد القوانين على مرتكبي الجرائم الالكترونيّة، كما وأظهرت النتائج أن الإحتلال الإسرائيلي والبنيّة التحتيّة والموازنات الماليّة والكادر البشري هي من أبرز المُعوِّقات التي تعيق عمليّة تطبيق الذَّكاء الاصطناعيّ في الحد من ممارسة الجريمة الإلكترونيّة، كما وتوصلت إلى أن المجتمع الفلسطيني لا يزال بعيد كل البعد عن التطور التكنولوجي ولا يزال يحتاج الى مزيد من الجهد في سبيل التوصل الى تطور تكنولوجي.

وعليه قدمت الدراسة بعض التوصيات لعل من أهمها تفعيل دور الذَّكاء الاصطناعيّ وتطبيقه في الكشف عن الجرائم المرتكبة في الفضاء الإلكتروني، وغرس ثقافة الذَّكاء الاصطناعيّ بين أبناء المجتمع الفلسطيني واللحاق بسلسلة التطورات التكنولوجية الحديثة، وضرورة فتح قسم خاص بـ(الذَّكاء الاصطناعيّ وتتبع الجرائم الإلكترونيّة)، وكذلك ضرورة العمل على تكثيف الدورات وورشات العمل للموظفين ذات الفائدة ونقل الخبرة والمهارة للأخرين لتوسيع نطاق الإستفادة في هذا المجال.

الكلمات المفتاحيّة: مُعوِّقات، الذَّكاء الاصطناعيّ، الجريمة الإلكترونيّة، وزارة الاتّصالات وتكنولوجيا المعلومات، محافظة رام الله والبيرة.

Obstacles to the application of artificial intelligence in reducing the practice of cybercrime from the point of view of workers in the Ministry of Communications and Information Technology in Ramallah and Al-Bireh Governorate

Prepared by: Katreen Issa Mohammad Abu Allan.

Supervisor: Dr. Wafa'a Al-khateeb.

Abstract:

The study aimed to identify the obstacles to the application of artificial intelligence in reducing the practice of cybercrime from the point of view of workers in the Ministry of Communications and Information Technology in Ramallah and Al-Bireh Governorate. The study need the qualitative method theory the use of interview tool. In addition, it relied on the content analysis method to analyze the data of books, newspapers, magazines and articles obtained through a comprehensive survey of Arab and foreign libraries and previous studies and to analyze the cybercrime data available at the official Palestinian sources.

The comprehensive social survey method was also used. consisted of (50) workers in the Information and Communications Technology Department of the Ministry of Communications and Information Technology.

The resulting in-depth interview data indicated that artificial intelligence has a strong and effective role in detecting cybercrime, Furthermore, it was shown that Israeli occupation, infrastructure, financial budgets and human cadre are the most prominent difficulties which hold back the process of applying artificial intelligence in limiting the practice of cybercrime It was also shown that the Palestinian society is still far away from technological development and still need more effort in order to reach technological development. Accordingly, it is recommended to activate the role of artificial intelligence and to apply it in detecting cybercrimes, to implant the culture of artificial intelligence among the Palestinian society, and to monitor the series of modern technological developments. It is also recommended to bring the light of the necessity of opening a specialized section called (Artificial Intelligence and Tracking Electronic Crimes), as well as the need of intensifying courses and workshops for its employees, and to transfer their experience and skills to others to expand the scope of benefit in this field.

Keywords: obstacles, artificial intelligence, electronic crime, Ministry of Communications and Information Technology, Ramallah and Al-Bireh Governorate.

الفصل الأول

الإطار العام للدراسة

1.1 مقدمة:

يُعَدُّ انتشار التكنولوجيا وشبكات التواصل الاجتماعي أحدَ أبرزِ مظاهر مواكبةِ الدُّول للتَّقدُّم، وتحقيق الرفاهية الاجتماعية، وسهولة الاتصال والتواصل بين الأشخاص، وبالرغم من استخداماتها السليمة في تطور المتجمعات فإنّها جلبت أشكالًا جديدة من الجرائم، تمثلت بالجريمة الإلكترونيّة التي تفاقمَتْ في المجتمعات بأشكالها المختلفة؛ فأصبحت هذه الاختراقات والانتهاكات والتعدي على الخصوصية تشكل للأفراد هاجسًا، ومصدر قلق دائم، وانعدام الشعور بالأمان (مدين 2019).

والدليل على ذلك أنَّ المجرمين استطاعوا استغلال الإنترنت وتقنيات المعلومات لخدمة أغراضهم الخاصة؛ لِتُمَكِّنَهُم من القيام بأعمالهم الإجرامية، فقد أثَّرتِ الجريمةُ الإلكترونيّة في مختلف المجتمعات العربية، خاصَّةً أنه يمكن ارتكاب هذه الجرائم بعيدًا عن أعين الجهات الأمنيَّة، لذا سهلت على الْجُناة القيام بالأعمال الإجراميَّة. والمجتمعُ الفلسطيني –كغيره من المجتمعات الأخرى– واكب هذه التطورات وشهد انفتاحًا كبيرًا في استخدام الإنترنت، إضافة الى أن سيطرة الاحتلال الإسرائيلي على سماء فلسطين وفضائها أثَّر في نسيجه الاجتماعي بشكل خطير، والدليل على ذلك انتشار جرائم الابتزاز، والجرائم الأخلاقية، والتحرش، والسطو (معالي، 2018)، فقد بلغت نسبة الأسر التي تستخدم الإنترنت بناءً على ما أشارت إليه إحصائيات وزارة الاتِّصالات وتكنولوجيا المعلومات خلال عام (2017) (56%)، في حين بلغت عام (2018) (65%)، وبلغت عام (2019) (80%)، وبلغت نسبة استخدام الإنترنت فائق السرعة عام (2020) (200%).

إن الزيادة في إستخدام شبكة الإنترنت أدى إلى زيادة الجرائم الإلكترونيّة، فالمجتمع الفلسطيني يمُرُّ بزيادة ملحوظة في الجرائم الإلكترونيّة الْمُرْتَكَبَةِ لديه، فعلى أرض الواقع وحسب (الهندي، 2020) أكَّد أن نسبة الجريمة الإلكترونيّة ازدادت بشكل كبير خلال فترة انتشار جائحة كورونا، خاصَّةً فيما يتعلق

بجرائم الابتزاز، فقد بلغ عددها خلال فترة الجائحة في بضعة شهور (332) شكوى، بعْدَ أنْ كانت نسبتُها طوال عام (2019) (293) شكوى، فاستغلال المجرمين لانتشار الجائحة والثغرات الأمنية الإلكترونيّة زادت التهديدات التي تواجه المجتمع، لا سيّما أنَّ هذه الجرائم لا تقتصر أضرارها –فقط– في محيط الفضاء الإلكتروني، إنما تتخطى ذلك لتؤثر في تدمير النسيج المجتمعي من بث روح الكراهية والعنف والتأثير في الترابط والتماسك المجتمعي؛ ما قد ينتج عنها جرائمُ أخرى، كالقتل، والعنف، والانتحار وغيرها من الجرائم ذات العلاقة.

وإزاء التصدي لهذه الاختراقات والانتهاكات في الفضاء الإلكتروني، تَطلَّب الأمرُ التَّفكيرَ في أساليبَ وطرائِقَ أكثرَ جدوى لمواجهة الجريمة الإلكترونيّة، والحاجة إلى المزيد من التكنولوجيا التي يمكن لأنظمتها اكتشاف السلوكات الطبيعية عن السلوكات غير الطبيعية والمخاطر، بحيث تكون هذه الأنظمة قادرة على التكيف، واكتشاف التهديدات، واتخاذ قرارات ذكية قائمة على العلم والمعرفة، تمثلت في تصميم تطبيقات حديثة في مجال مواجهة الجرائم الإلكترونيّة (الصمد ومحمد، 2020).

لعلَّ من أهم تلك الأنظمة الذكاء الاصطناعي الَّذي يُعَدُّ أحد الأسس الرئيسة في العصر الحديث، فهو نتاج (2000) عام من الفلسفة، والتفكير، وتركيز الخيال العلمي على ابتكار مثل هذه النظم، كما أنه يُعَدُّ حقلًا من حقول علم الحاسوب، وتاريخًا عريقًا في الترابط بين علم النفس والتعامل مع المواقف، بطريقة مشابهة لتفكير الإنسان، وفي الوقت نفسه تستطيع تلك الأنظمة أن تخزن المعارف والخبرات المتراكمة واستخدام كل ما تمتلكه من معلومات في اتخاذ القرارات. (أبو غزالة، 2018).

فقد أثبتت الدراسات أن الذكاء الاصطناعي أداة فعّالة، وقادرة على مواجهة الجريمة الإلكترونيّة تأكيدًا على ذلك ما أشار إليه كل من شو وآخرون (Xu & Others, 2020) من الدور الْمُهمّ للذكاء الاصطناعي في الكشف عن الجريمة الإلكترونيّة، وتصنيف الهجمات الإلكترونيّة، وأكد بهاشكير (Bhasker, 2015) من خلال اقتراحه نظام للكشف عن التسلل الإلكتروني يعمل على أَخْذِ عينات عشوائيَّة، وتحليل المسلكيات على الشبكة حول ما إذا كانت منحرفة أو طبيعية، وفي السياق نفسه قدم جاغدال وضهار ورنا (Jagdale & Dhar & Rana, 2014) نظامًا يعمل على حساب درجة المخاطر والتنبؤ بوجود مسكليات منحرفة على الشبكة الإلكترونيّة من المُتَصيّدين.

يُلاحَظُ ممّا سبق أن التطوّرات الْمُحْرَزَة في نظم الذكاء الاصطناعي من شأنها أن تعمل على وقاية مستخدمي الإنترنت ومواقع التواصل الإجتماعي من الوقوع ضحايا للمجرمين الإلكترونيين، وعلى المؤسسات الفلسطينية الاستفادة منها؛ من أجل العمل على تقليل مخاطر الجرائم الإلكترونيّة التي أصبحت تنهش في المجتمع الفلسطيني، ولكي تتسنى الفرصة للاستفادة منها وتطبيقها لا بد من معرفة

المُعوقات التي تواجه تطبيقها، من هنا كان لا بد من القيام بدراسة تُسَلِّطُ الضوء على المُعَوِّقات التي تواجه تطبيق نظم الذكاء الاصطناعي في المجتمع الفلسطيني ووضع مجموعة من الآليات لمواجهتها.

2.1 مشكلة الدراسة:

إن مواكبة متطلبات العصر الحالي بالإعتماد على التكنولوجيا والإنترنت وشبكات التواصل نتيجة التغيرات الإجتماعية في أنماط المعيشة من شأنها أن تؤدي إلى تفاقم الجرائم الإلكترونيّة وإنعكاسها على الجوانب الإجتماعية والإقتصادية والنفسية والثقافية بأشكالها المختلفة من إبتزاز أو تشهير أو سرقة مصارف وبطاقات ائتمانية وغيرها من الجرائم التي تشكل خطراً يومياً على حياة الأفراد في الضفة الغربية.

وبناءً على ما أشارت إليه إحصائيات (جهاز الشرطة الفلسطينية، 2020) بلغ عدد الجرائم الإلكترونيّة في الضفة الغربية لعام (2016) (1327) جريمةً، بينما بلغت في عام (2017) (2028) جريمة، في حين بلغت عام (2018) (2418) جريمة، وكانت في عام (2019) (2568) جريمة، وبلغت في عام (2020) (2720) وبلغت عام (2021) (2589)، هذه الزيادة توحي أن الجرائم الإلكترونيّة ظاهرة لا يستهان بها كونها تنتشر بسرعة كبيرة، فمن الممكن أن تزداد بشكل أكبر في السنوات المُقبلة أمام انتشار فيروس كورونا (كوفيد-19) الذي أجبر العالم إلى الانتقال من العالم الواقعي إلى العالم الإفتراضي، عَبْرَ استخدام شبكات الإنترنت من داخل البيت، لذا أصبح لزامًا على مؤسسات المجتمع الفلسطيني أن تستفيد من تقنيات الذكاء الاصطناعي الحديثة وُنظُمِه؛ لتوفير الأمان للمواطنين في أثناء استخدامهم للإنترنت وتقليل الفرص أمام الْجُناةِ من ممارسة جريمتهم، لكِنْ هناك كثيرٌ من المُعوقات التي تواجه هذا الاستخدام، لذا كان لا بد من عمل دراسة علميّة للتعرف إلى تلك المُعوقات، وعليه تكمُن مشكلة الدراسة في الإجابة عن السؤال الرئيس الآتي: ما مُعوِّقاتُ تطبيق الذكاء الاصطناعي في الحدِّ من ممارسة الجريمة الإلكترونيّة من وجهة نظر العاملين في وزارة الاتِّصالات والتكنولوجيا في محافظَتَي رام الله والبيرة؟

3.1 أهمية الدراسة:

تَكْمُنُ أهمية الدراسة في أهمية الموضوع الذي تتناوله، ويتمثَّل في معوقات تطبيق الذكاء الاصطناعي، في الحد من الجريمة الإلكترونيّة، من وجهة نظر العاملين في وزارات الاتّصالات، والتكنولوجيا، والمعلومات في محافظتي رام الله والبيرة، حيث إنها من الدراسات القليلة والنادرة التي تتناول عمليَّة الربط بين متغيّري الذكاء الاصطناعي والجريمة الإلكترونيّة، وهذا ما أكده (الهندي، 2020) خلال

الاجتماع معه يوم (الثلاثاء) بتاريخ (2020/10/20)؛ لمناقشة أهمية تطبيق الذكاء الاصطناعي في مواجهة الجرائم الإلكترونيّة، حيث أكَّد أنه يتم التركيز –في الاجتماعات التي تعقد مع القيادة– على تعزيز تطبيق الذكاء الاصطناعي، واستثماره في المجالات كافة؛ لما له من أهمية في مواجهة الجرائم الإلكترونيّة والحد منها، كما تتمثّل أهمية هذه الدراسة –من ناحية شخصيّة– في رغبة الدّارسة الجادّة في البحث والتنقيب في هذا الموضوع، إضافة إلى ذلك احتواء هذه الدراسة على أهمية نظريّة علميّة، وأخرى عمليّة تطبيقيّة.

أما الأهمية النظريّة العلميّة تتمثل في:

- أن الدراسة ستكون مرجعًا يستفيد منه الباحثون والمهتمون بهذه الظاهرة؛ كونها من الدراسات النادرة في فلسطين والعالم العربي، إذْ ستوفِّرُ إطارًا نظريًّا حول الذكاء الاصطناعي ودوره في الحد من ممارسة الجريمة الإلكترونيّة والمُعوقات التي تعوق تطبيقه.
- تزويد المكتبات الفلسطينية بهذا النوع من الدراسات وإغناء الأدب بها.
- إن الدراسة ستحدد أهم المعوقات التي تواجه تطبيق الذكاء الاصطناعي للحد من الجرائم الإلكترونيّة.

في حين تتمثل الأهميّة العمليّة التطبيقيّة في الجهات التي ستستفيد من نتائج الدراسة كما يعلى يأتي:

- الأجهزة الأمنية، خاصة وحدة الجرائم الإلكترونيّة: وتكمن استفادتها في زيادة القدرة على الكشف عن الجرائم التي يَصْعُبُ اكتشافها وتعقبها.
- وزارة الاتِّصالات وتكنولوجيا المعلومات: ستستفيد من نتائج الدراسة في توجيه جهودها؛ لإتخاذ خطوات تصحيحية، ووضع إستراتيجية مُهِمَّة؛ للحد من الجريمة الإلكترونيّة من خلال مواجهة العقبات التي تحول دون القدرة على تطبيق الذكاء الاصطناعي، بالإضافة إلى التوعية الجادة في مواجهتها، والحدِّ من انتشارها، عَبْرَ مجموعة من الندوات والمؤتمرات وورش العمل التي تهدفُ إلى زيادة وعي المواطن بالجريمة الإلكترونيّة ومخاطرها.
- الباحثون: ستكون الدراسة بدايةً لدراسات مشابهة يقوم بها الباحثون والمهتمون في المجال نفسه.

4.1 أهداف الدراسة:

تسعى هذه الدراسة إلى تحقيق هدف رئيس، تنبثق عنه أهداف أخرى فرعية، وأما الهدف الرئيس فإنّه يتمثل في التعرف إلى معوقات تطبيق الذكاء الاصطناعي في الحد من ممارسة الجريمة الإلكترونيّة، من وجهة نظر العاملين في وزارة الاتصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة، في حين تتمثل الأهداف الفرعية في التعرف إلى:

- دور الذكاء الاصطناعي في الكشف عن الجريمة الإلكترونيّة.
- آليّة عمل برامج الذكاء الاصطناعي لتتبع الجناة من مرتكبي الجرائم الإلكترونيّة.
- المُعوِّقات التي تواجه تطبيق الذكاء الاصطناعي في الحد من ممارسة الجرائم الإلكترونيّة.
- إتجاهات المبحوثين حول العلاقة بين الخصائص الديمغرافية (الجنس، مكان السكن، عدد أفراد الأسرة، التحصيل العلمي، العمر) وممارسة الجريمة الإلكترونيّة.

5.1 أسئلة الدراسة:

يُمكن بلورة أسئلة الدّراسة في مجموعة من المحاور الرئيسة والفرعية كما على النّحو الآتي:

- المحور الرئيسي الأول: ما دور الذكاء الاصطناعي في الكشف عن الجريمة الإلكترونيّة؟ يتفرع عنه:
    - هل هناك دور للذكاء الاصطناعي في الكشف عن الجريمة الإلكترونيّة؟
    - من وجهك نظرك، هل تشعر أن مدى الذكاء الاصطناعي مرتبط بمدى قبوله في المجتمع؟ كيف ولماذا؟
    - هل يُسْتخدمُ برامج الذكاء الاصطناعي في وزارة الاتصالات وتكنولوجيا المعلومات؟ ما أهم هذه البرامج؟ وما هي نطاقات استخدامها؟
    - هل تُسْهِم برامج الذكاء الاصطناعي في الحد من الجريمة؟
    - كيف يمكن أن تكون برامج الذكاء الاصطناعي رادعًا أمام الجناة لمنع ممارسة الجريمة الإلكترونيّة والحد منها؟

- المحور الرئيسي الثاني: ما آليّة عمل برامج الذكاء الاصطناعي لتتبع الجناة من مرتكبي الجرائم الإلكترونيّة؟ يتفرع عنه:

  - ما آليّة عمل برامج الذكاء الاصطناعي لتتبع الجناة من مرتكبي الجريمة الإلكترونيّة؟
  - كيف تُسْهِم الآليات المتبعة في استخدام برامج الذكاء الاصطناعي في التخفيف من الجريمة الإلكترونيّة المرتكبة؟
  - في حال ضعف او عدم توفر آليّات تتبع للجرائم الإلكترونيّة ماذا تقترح/ين لتوفير أو تحسين آليات العمل في تتبع الجرائم الإلكترونيّة؟
  - ما هي أكثر الجرائم الإلكترونيّة التي تقوم تطبيقات الذكاء الاصطناعي في الوزارة باكتشافها؟

- المحور الرئيسي الثالث: ما المُعوقات التي تواجه تطبيق الذكاء الاصطناعي في الحد من ممارسة الجرائم الإلكترونيّة، يتفرع عنه:

  - هل هناك مُعوقات تواجِهُ تَطبيق الوزارة للذكاء الاصطناعي في الحد من الجرائم الإلكترونيّة؟
  - ما ترتيب المُعوقات التي تواجِهُ تَطبيق الوزارة للذكاء الاصطناعي في الحد من الجرائم الإلكترونيّة حسب الأهميّة؟
  - ما طرق التغلب على المُعوقات التي تواجِهُ تَطبيق الوزارة للذكاء الاصطناعي في الحد من الجرائم الإلكترونيّة"؟
  - ما إتجاهات المبحوثين حول العلاقة بين الخصائص الديموغرافية (الجنس، مكان السكن، عدد أفراد الأسرة، التحصيل العلمي، العمر) وممارسة الجريمة الإلكترونيّة؟
  - هل لديك علم بمؤسسة أو وزارة أخرى تستخدم تطبيق الذكاء الاصطناعي في الحد من ممارسة الجريمة الإلكترونيّة؟
  - هل هناك تعاون وتنسيق بين الوزارة والمؤسسات المحليّة والدوليّة العاملة في مجال الجرائم الإلكترونيّة؟

6.1 حدود الدراسة:

تحددت الدراسة بمجموعة من الحدود من أهمها:

- الحدود الزمنية: تمّ إجراء هذه الدراسة في الفترة الواقعة ما بين الفصل الثاني من العام الدراسي (2020م– 2021م) والفصل الثاني من العام الدراسي (2021م – 2022م).
- الحدود المكانية: تمّ تطبيق هذه الدراسة على وزارة الاتِّصالات والتكنولوجيا والمعلومات في مدينة رام الله.
- الحدود البشرية: اقتصرت هذه الدراسة على العاملين في قسم (تكنولوجيا المعلومات والاتصالات) في وزارات الاتصالات والتكنولوجيا والمعلومات البالغ عددهم (50) موظفًا وموظفة حسب إحصائيات (وزارة الاتصالات وتكنولوجيا المعلومات، 2021م).

7.1 مفاهيم ومصطلحات الدراسة:

هناك العديد من المفاهيم والمصطلحات ذات العلاقة بموضوع الدراسة، لعل من أهمها ما يأتي:

- الذكاء الاصطناعي: عرفها (مرقس، 2021: 154) "أنها تطوير أجهزة الحاسوب؛ لتصبح قادرة على محاكاة العقل البشري، وأداء المهام التي تتطلب الذكاء البشري، مثل التعلم، والاستنتاج، والاستفادة من المعلومات السابقة، والإدراك البصري، والتعرف على الكلام وصنع القرارات".

  في حين يرى كل من (موسى و بلال، 2019: 16) أنه بالرغم من اختلاف أراء العلماء حول مفهومه فإنّه ينقسم الى كلمتين، يمكن تعريف الكلمة الأولى (الاصطناعي) "بأنها تشير إلى شيء مصنوع أو غير طبيعي"، والكلمة الثانية (ذكاء) وتعني "القدرة على الفهم والتفكير". ويُعدُّ الذكاء الاصطناعي –من وجهة نظر علماء النفس– "أحد فروع علم النفس الأساسية أي أنه عبارة عن برمجة الآلة بطريقة تمكنها من الإدراك والحدس واتخاذ القرارات أي العمل بطريقة عمل الإنسان نفسها، حيث تعمل هذه النظم على تطوير نفسها" حسب كرودير وكاربوني (Crowder, & Carbone, 2020).
- الذكاء الاصطناعي إجرائيًّا: آلة ذكية تختلف اختلافًا كليًّا عن الآلة التقليدية الَّتي يستخدمها البشر، ولديها القدرة على إتمام المهام التي تُطلب منها كافةً بمهاراتٍ عآليّة الدِّقَّة والسُّرعة والكفاءة من خلال ما قام البشر سابقًا بجمعه وتخزينه في قواعدها المعرفيّة.
- الجرائم الإلكترونيّة: "تعرف على أنها كل فعل ضارّ يأتيه الفرد أو الجماعة عبر استعماله للأجهزة الإلكترونيّة، يكون لهذا الفعل أثر ضار على غيره من الأفراد" (معالي، 2018: 3)،

وعرفها (لطفي، 2019: 27) على أنها "الجرائم المرتكبة عبر جهاز الكمبيوتر وغيرها من وسائل الاتِّصال الحديثة".

- الجريمة الإلكترونيّة إجرائيًّا: مجموعة من الأفعال والسلوكات المنحرفة التي من شأنها أن تُلحق الضرر بالمجني عليه، ومن حوله بأي جانب من جوانب حياته تتم في الفضاء الإلكتروني، يقوم بها الجاني من تزوير وابتزاز واحتيال، إما بدافع المنفعة، أو بدافع الانتقام، حيث تؤدي إلى أضرار كبيرة.
- وزارة الاتصالات والتكنولوجيا والمعلومات اصطلاحاً: "هي وزارة تقوم بتنظيم قطاع الاتصالات وإدارته ورقابته في فلسطين بموجب قانون الاتصالات رقم (3) لسنة (1996م)، بالإضافة إلى تنظيم عمل البريد في فلسطين والاتّصالات السلكية واللاسلكية، وفتح سوق الاتصالات أمام المشغلين الجدد، والترخيص لهم وتنظيم خدمات الإنترنت وغيرها من الأمور المتعلقة بالاتصالات وتكنولوجيا المعلومات في فلسطين" (وزارة الاتصالات والتكنولوجيا والمعلومات، 2013).
- تكنولوجيا المعلومات اصطلاحاً: "هي عبارة عن البحث عن أفضل الوسائل لتسهيل الحصول على المعلومات، وتبادلها وجعلها متاحة لطالبيها بسرعة وفاعلية" (الأمين، 2016: 124).
- تكنولوجيا المعلومات إجرائيًّا: تقنية تكنولوجية يستطيع من خلالها المختصون والعاملون فيها على مواكبة التطورات التي تطرأ على البرامج، فيتم تطوير هذه البرامج وترجمتها ووضع الحماية على البرامج من خلالها، كما تعمل على معالجة كثيرٍ من البيانات التي تحتوي على كثيرٍ من البرامج والتطبيقات المرتبطة مع بعضها بعضًا.

الفصل الثاني

الإطار النظري والدراسات السابقة وذات الصلة

1.2 مقدمة:

تُشَكِّلُ الاختراعات الحديثة أحد أهم أساسيات استمرار الحياة؛ فكلُّ زمن تمرُّ به المجتمعات تجدُ نفسَها مُلْزمةً على اختراع نُظُمٍ جديدة، تُمَكِّنُها من الحفاظ على استمراريتها ووجودها، ولِمواكبةِ متطلبات الحياة بدأت المجتمعات تتحول إلى عالم جديد من التكنولوجيا، وقد اسْتَدْعى ذلك من العلماء الاهتمام بتطويرِ تطبيقاتٍ ذكيَّةٍ، وبفضل جهود العلماء المبذولة في اختراع الذكاء الاصطناعي أصبح من أهم الإنجازات الَّتي قُدِّمَتْ للعصر الحالي، ويُمْكِنُ لأيِّ مؤسسة استثمارها للاستفادة منها، ففي السنوات السابقة بدأت المجتمعات بتطبيق الذكاء الاصطناعي على أرض الواقع، واستثماره بأفضل الطرق والوسائل، فهذه النظم تستطيع أن تتعلَّمِ اللُّغاتِ التي يستخدمها البشر، وإنجاز المهامِّ الْمُوْكَلَةِ إليها، واستخدام الصور والأشكال،وفي الوقت نفسه تستطيع أن تُخَزِّن المدركات والخبرات المكتسبة المتراكمة واستخدامها في عمليات اتخاذ القرارات (خليفة، 2019).

فوجودُ الذَّكاء الاصطناعي أصبح لزامًا في المجتمعات كافة؛ نظرًا لزيادة التطور في التكنولوجيا، وارتفاع نسبة استخدام الأفراد والمؤسسات لها، خاصة أن المجتمع الفلسطيني أَحَدُ المجتمعات التي تواكب التطور فقد أشار (جهاز الإحصاء المركزي، 2020م) إلى أن نسبة مستخدمي الإنترنت في الضفة الغربية وصلت إلى (83,5%) لعام (2019م)، ونسبة الأفراد الحاملين للهواتف الذكيّة كانت (90,8%) لعام (2019م)، وما نراه اليوم أن تأثير التكنولوجيا والبرامج الحديثة والمتقدمة في إمكاناتها وأساليبها المستخدمة أصبح عميقًا وواضحًا على الحياة، وجزءًا لا يتجزأ من المجتمع فهذه النظم هي التي تحرك المجتمعات، ولا يمكن إنجاز الأعمال إلا من خلالها. (الهادي، 2021).

2.2 الذكاء الإصطناعيّ:

1.2.2 مفهوم الذكاء الاصطناعيّ:

لا يُمْكِنُ حَصْرُ مفهوم الذكاء على ما يملكه الإنسان في دماغه فقط، إنما بدأ الإنسان يسعى إلى توظيفه في الماكينات الحديثة، والأجهزة الإلكترونيّة المتطورة لخدمه الإنسان.

- **الذَّكاء لُغةً:** "مُشتقَّةٌ من الفعل (ذكا) أي أسرع فهمه وتوقد" (المعجم الوسيط، 2014: 314).
- **أمّا اصطلاحًا:** فقد عرَّفَهُ همفري المُشار له في (العيد، 2018: 22) أنّه "القدرة على التَّفْكير والإدراك والتعلم من المهارات والخبرات، والقدرة على التكيّف والارتباط بالبيئة المحيطة".
- **الذكاء إجرائيًّا:** تنظيم القدرات الذهنية بطريقة تُمَكِّن مِن استخدامها في تحليل مجريات الأحداث التي يتعرض لها الفرد ويواجهها، بناءً على هذه القدرات المكتسبة فإنّها تُمَكِّنُه من التعامل مَعَ الموقف.
- **الاصطناعي لُغةً:** "يرجع أصل الكلمة إلى الجذر الثلاثي (صنع) أي العمل، وهو كل ما صنع مصنوع وصنعه" (المعجم الوسيط، 2014: 526).
- **الاصطناعي اصطلاحًا:** عرفه (ياسين، 2020: 100) "الذكاء الذي تكتسبه النُّظُم والبرامج بالاصطناع أو بالصناعة تميزًا عن الذكاء الإنساني، والمراد من استخدام كلمة الاصطناعيّ التأكيد على خاصية أن هذا الذكاء حتى لو اكتسب خصائص الذكاء الإنساني فهو ليس ذكاءً أصيلاً".

وعرفه كل من (الصمد وأحمد، 2020: 21) أنه "عبارة عن برامج حاسوبية، لديها القُدرة على التفكير بطريقة مماثلة لتفكير البشر، من خلال ما وصلت إليه من تطور في قواعد البيانات، كما وله القدرة على التعلم من الأخطاء السابقة التي مر بها؛ ما يمكنه من العمل بشكل أدقَّ وأفضلَ وأسرَعَ".

في حين عرفه جون مكارثي عام (1955م) المُشار له في (دهشان، 2019: 14) وهو الأب الروحي لمفهوم الذكاء الاصطناعي بأنه "وسيلة لصنع جهاز كمبيوتر أو روبوت، يتم التحكم به عن طريق الكمبيوتر، أو برنامج يفكر بذكاء، بالطريقة نفسها التي يفكر بها البشر الأذكياء".

ويُعرَّفُ –أيضًا– بأنه"أحد العلوم المُتفرِّعة عَنْ علم الحاسوب، وهو العلم المعني بجعل الحواسيب تقوم بمهامَّ مُشابِهةٍ لعمليات الذكاء البشري، منها التعلم والاستنباط واتخاذ القرارات" (الفاخري، 2018: 119).

ويرى (محمد، 2015: 112) أنَّ الذَّكاء الاصطناعيَّ "مجموعةٌ من الجهود الْمَبْنِيَّة عَلى تطوير الحاسب الآلي؛ لإعطائِهِ القدرة على القيام بوظائِفَ تحاكي ما يقوم به العقل الإنساني من حيث تعلم اللغات، والقدرة على التفكير والإدراك والفهم".

2.2.2 نشأة الذكاء الاصطناعي ومراحل تطوره:

نَشَأَ الذكاءُ الاصطناعيُّ بصورته البسيطة منذ العصور القديمة، عندما بدء العلماء بالاجتهاد والتفكير في صنع حاسبات آليّة مُستَحدثة، تحتوي على مُمَيِّزاتٍ وبرامِجَ وأنظمةٍ لديها القدرةُ على معالجة التحديات التي كانت في الماضي شبه مستحيلة، فضلًا عن قدرتها على التعلم من البيانات التي يُخزّنها الإنسانُ في قواعدها، فقد كُثِّفَتِ الأبحاث والدراسات بصورة جديدة وحديثة غير تلك التي اعتدنا عليها لتطوير هذه الآلة؛ كي تتمكن من التصرف مع مجريات الأحداث بطريقة مماثلة للدماغ البشري (أبو غزالة، 2019م).

واستطاع عالم الرياضيات (آلان تورينج) عام (1950م) من اختراع اختبارٍ ذكيٍّ، ومقارنته مع الإنسان، إذ كانت مهمة هذا الاختراع الإجابة عن الأسئلة التي تطرح على الإنسان وعلى جهاز الحاسوب، على أساس أن الحاسوب لا يمكن تمييزه عن الإنسان بإجابته عن الأسئلة التي تُطْرَحُ عليه، فيُجيبُ بالطريقة نفسِها التي يجيب عليها البشر، فقد كانت هذه الفكرة بمثابة مفتاح الدخول إلى عالم الذكاء الاصطناعي الذي أصبح أحدَ أهمِّ مخرجات الثورة الصناعيَّة الرابعة، وأصبح أمرًا واقعًا، لا مستحيلًا أعلن عنه العالم (جون مكارثي) بشكل رسمي في كليّة دارتموث، خلال مؤتمر عُقِدَ في الولايات المتحدة الأمريكية. (الهادي، 2021).

مر الذكاء الاصطناعي بعدة مراحل على فترات زمنية مختلفة على النحو الآتي حسب ما أشار إليه كل من (كاظم، 2012م) و (موسى وبلال، 2019م):

- **المرحلة الأولى:** كانت هذه المرحلة بمثابة أول ظهور حقيقي لآفاق الذكاء الاصطناعي امتدت ما بين (1950م–1940م).
- **المرحلة الثانية:** امتدت ما بين (1950م– 1963م) ركَّز فيها العلماء على تنفيذ الأفكار التي تتشكل في أذهانهم، وترجمتها بشكل ملموس على أرض الواقع، وقام في هذه المرحلة العالم (كلود شانون) عام (1950م) بالبحث والتقصي عن ماهية لعبة الشطرنج، وكيفية التعامل معها، كما أوْجَد العالِمان (فيجن وفيلدمان) حلولًا للألعاب، وفكًّا للألغاز بواسطة أجهزة الكمبيوتر، واستخدام بعض النماذج الحاسوبية التي تتمثل في اقتراح إجابات وحلول يمكن

الاستفادة منها في فك الألغاز التي تستوقف اللاعب، وهذا ما تم تطبيقه على لعبة الشطرنج فيما بعد.

- **المرحلة الثالثة:** سُمِّيَتْ هذه المرحلة بالمرحلة (الشاعرية)؛ كونها كانت البداية الحقيقة لظهور مفهوم الذكاء الاصطناعي بشكل معتمد ورسمي بعد أن أُعْلِنَ عنه في المؤتمر الَّذي عُقِدَ في كليّة (دارت موث، 1956م)، ففي هذه المرحلة أُنْشِئَ ما يُسمّى بالشبكات العصبيّة وهي إحْدى أهمِّ نُظُم الذكاء الاصطناعيّ، إضافةً لما سبق في هذه المرحلة قام العالم (ونجراد) بمحاولاته الأولى في وضع نظام لديه القدرة على الترجمة الآليّة والفورية للغات عَبْرَ إدراك الجمل المختلفة، وفهمها باللغة الإنجليزية، مثل الروايات والمحادثات والمخاطبات، وكلّ ما يُدْرَجُ تحت نطاق اللغات الَّتي يستخدمها البشر.
- **المرحلة الرابعة:** كانت هذه الفترة الزمنية بمثابة ثورة تكنولوجية كبيرة؛ لما أَحْدَثَهُ الذَّكاء الاصطناعي من تغيُّراتٍ في مختلف الجوانب الحياتيّة آنذاك، فقد شهدت هذه الفترة تطورًا في مختلف البرامج والنظم بأنواعها المختلفة، كذلك العمل على حل الألغاز الصعبة، حيث تمكن العالم الأمريكي (آرثر صاموئيل) إبّانَ هذه الفترة من وضع خوارزميات للعب منها لعبة الداما (وهي لعبة تعتمد في مبدئها على الذكاء)، بالإضافة إلى ما تميزت به من ظهورٍ لتقنيات الذكاء الاصطناعي وبرامجه، فهذه التِّقْنيّات أدَّتْ دورًا فعالًا في اكْتِسابِ جزء كبير من الذكاء الإنساني في برامجها، عَبْرَ تخزين المعلومات، وتُعَدُّ هذه الفترة بمثابة العصر الذهبي والنواة الأساسية لازدهار هذا العلم الحديث.
- **المرحلة الخامسة:** بعد ثورة التكنولوجيا التي مر بها الذكاء الاصطناعي عاش فترة من الركود، على الرغم من ذلك لم تتوقف جهود العلماء إلى هذا الحدِّ، إنّما قاموا بالتوسع في الدراسات والعمل، إذْ بدأ بالظهور بصورة متطورة أكثر من ذي قبل عام (1980م)، فقد ركَّزوا –في هذه المرحلة– على استخلاص خبرات الخبراء، خاصَّةً في التَّخصُّصات النادرة، بالإضافة إلى القدرة على حل المشكلات بطريقة أسرع من الخبير البشري، وفي عام (1990م) تم التركيز على نظم الشبكات العصبيّة بشكل كبير، وكذلك نظم التعلم الآلي عَبْرَ استخدام تِقْنيّات إحصائيَّة؛ لمنح الحاسوب القدرة على التعلم والتدريب واتخاذ القرارات في حل المشكلات بالإضافة إلى فهم اللغات الطبيعيّة والتَّرْجمة.

3.2.2 مكونات الذكاء الاصطناعي:

الذكاء الاصطناعي يتشكّلُ كما غيره من البرامج من ثلاثة مكونات وعناصر أساسية حسب ما أشار إليه شارما (Sharma, 2020):

- **المكون الأول:** يشمل القدرات المعرفيّة، وهي البيانات والمعلومات الْمُدْخَلَة عَبْرَ جهاز الحاسوب إلى النظام الذكي، إذْ يقوم المبرمجون –من أجل الاستفادة من هذه النظم– بتزويدها بكمٍّ هائل من البيانات الّتي تُعَدُّ بمثابة عملية تغذية لها، تعطيها القدرة على إدراك الأحداث وفهمها وتحليلها في النهاية بما يتناسب مع الموقف، كما تُخَزَّنُ المعرفة والخبرات المتراكمة في قاعدة النظام؛ لتكسبها مزيدًا من الخبرة والمهارة في التعامل مع الأحداث، حيث إنَّ هذا المكون مهمٌّ، وأساس نجاح الذكاء الاصطناعي في الاستمرار.
- **المكون الثاني:** يَعْتمدُ على أجهزة حسيّة تُسَمّى الْمُسْتَشْعِرات (الحسّاسات)، تساعد في التعرف على المعلومات فور إدخالها؛ كي تتمكن من استلامها، وتنظيم نشاطها، فهذه الْمُسْتَشْعِرات الحسّاسة ضرورية جدًّا في آليّة عمل الذكاء الاصطناعيّ؛ لِتُسهِّلَ عملية استقبال البيانات وتحليلها، والقدرة على فهم المشكلة التي تُدْخلُ بياناتها إلى جهاز الحاسب الآلي؛ كي يتمكن من التعامل معها.
- **المكون الثالث:** يَتمُّ عَبْرَ إدارة جميعِ التَّفاعلات التي تحدث داخل النظام بطريقة مشابهة لطريقة تفكير البشر، مثل استخدام أكثر من طريقة لتحليل الهدف المتوفِّر، وتعزيز القدرات الموجودة في قواعد البيانات الّتي أُدْخِلَتْ في النظام كالفهم والإدراك ووضع العديد من الحلول النموذجية من أجل الوصول إلى حَلٍّ نهائي عَبْرَ بناء استراتيجيات يُمْكِنُ أن تُحَقِّقَ كلَّ الأهداف الفرعية المرصودة.

4.2.2 الخصائص العامة للذكاء الاصطناعي:

الذكاء الاصطناعي –كغيره من المفاهيم والمتغيرات– يَتَمَيَّزُ بخصائِصَ عديدةٍ، لعلَّ من أهم تلك الخصائص من وجهة نظر (سليمان، 2020) ما يأتي:

- القدرة على فرز البيانات وتحليلها بما يتناسب مع ما هو مطلوب منها.
- القدرة على تميز مجموعة من الخصائص، مثل الأصوات وتحليل بصمة العين وتميز الصور.
- القدرة على تطوير نفسها من خلال التعلم المستمر والاستفادة من الخبرات المتراكمة.
- القدرة على التعامل مع المواقف والبيانات المدخلة بسرعة عآليّة وإعطاء نتائج دقيقة.
- في حين أشار (محمد، 2015: 113) إلى أنَّ الخصائص التي يتمتع بها الذكاء الاصطناعي تتمثل في القدرة على:

- إمكانية حل المشكلات التي تتعرض لها وإتخاذ القرارات من خلال المعطيات المتوافرة لديها.
- استيعاب البيانات بمختلف أشكالها وأحجامها والعمل على تطبيقها في المواقف.
- إمكانية التفكير والفهم بناءً على المهارات والمعلومات المكتسبة.
- التعامل مع المواقف المجهولة من خلال التجارب السابقة.
- التعامل مع الحالات المواقف الحرجة التي تتعرض لها الشبكات.
- الاستجابة السريعة للمواقف.

كما أشار جين ولويس (Jean & Louis, 1987) الى أن الخصائص التي يتميز بها الذكاء الاصطناعي هي على النّحو الآتي:

- الاستعانة بالخبرات المتوفِّرة لديه لحل المشاكل التي يتعرض لها وإدراكها بعد تحليلها.
- اكتساب المعرفة والمهارة والتدريب عليها من خلال التجارب السابقة التي تعرض لها.
- الاستجابة للمواقف التي يتعرض لها بسرعة، والتعامل مع أسوأ الظروف التي يمر بها.
- القدرة على حل المشكلات الصعبة والمعقدة التي يمر بها.
- القدرة على اتخاذ القرارات فيما يتعلق بالظروف التي يمر بها.
- القدرة على تقديم النصحية لاتخاذ القرار.

5.2.2 مجالات الذكاء الاصطناعي:

الذكاء الاصطناعي علم واسع كغيره من العلوم يشتمل على مجموعة واسعة من التطبيقات، ومن أهمها:

- **التعلم التلقائي (التعلم الآلي):** ظهرت هذه النظم عام (1959م) على يد العالم (أرثر صاموئيل)، فقد عرف كل من (بلال وموسى، 2019: 24) التعلم الالي على أنه "أحد فروع الذكاء الاصطناعي الذي يهتم بتطوير خوارزميات وتقنيات، تسمح لأجهزة الحاسب الآلي بامتلاك خاصية التعلم من تلقاء نفسها، وتطبيقات برمجية تصبحُ أَكْثَرَ دِقَّةً في تنبؤ النتائج دون القيام ببرمجتها بشكل مستمر".

  في حين عرفه (شهاب، 2018: 73) "بأنه من يجعل الآلات قادرة على التعلم وأداء مهامَّ واتخاذ قرارات بنفسها بناءً على قاعدة من البيانات، هذه البيانات تُكسبها المعرفة التي من خلالها تستطيع أن تعمل بطريقة عمل الْمُخِّ البشريّ نَفْسِها".

  فمن خلال الخبرات والمهارات التي يتم إدخالها في قواعدها المعرفية يمكن لهذه النظم بعد أن يصمّمها المبرمجون أن تقوم بتدريب نفسِها بنفسِها دون الحاجة إلى وجود مرجعية بشرية تستند

عليها في التدريب، ومِنْ ثَمَّ العمل على تطوير قدرتها على التنبؤ بالأمور واتخاذ القرارت في المواقف، هذا ما يميز برامج التعلم الآلي، فهي تتميز بقدرتها على تطوير نفسها بنفسها من خلال التدريب المستمر على البيانات الموجودة في قواعدها المعرفيّة والاستفادة من التجارب التي مر بها ناثان (Nathan, 2019)، حيث تتكون نظم التعلم الآلي حسب ما أشار لها جيشي (Jeshi, 2019) من الآتي:

- **النظام:** وهو الواجهة الأساسية للبرنامج وظيفته استقبال البيانات التي يُدْخِلُها الْمُسْتَخدمون إلى الحاسب الآليّ بالعودة إلى قواعد المعرفة، ومِنْ ثَمَّ تصنيفها.
- **المدخلات:** تتم بتكوين المفاهيم بعد أن تُصنَّفَ البيانات، ويُتَّخذ القرار حول السماح بإدخال هذه النوعية من البيانات إلى الشبكة أو عدم السماح بوصفها غير مهمة وتُشكِّل خطرًا.
- **مجموعات التدريب:** تقوم هذه المجموعات بالحصول على العناوين بعد الانتهاء من عملية التصنيف، ومِنْ ثَمَّ تعمل على مقارنتها بالبيانات الموجودة في قواعد المعرفة لديها وتعديل المعطيات التي تم الحصول عليها، بمعنى تقوم هذه المجموعات بتعليم نفسها بنفسها بناءً على التجارب السابقة التي تعرضت لها من خلال قواعد المعرفة.

- **النظم الخبيرة:** ظهرت النظم الخبيرة عام (1970م) على يد العالم (إدوارد فايجنباوم) فهو أول من طرح فكرة هذا النظام، وتُعَدُّ من أهم تِقْنيّات الذَّكاء الاصطناعي وأكثرها تطبيقًا في مختلف المجالات، هذه النظم كما عرَّفها (السيد ومحمد، 2020: 18) "أنها نُظُم كمبيوتر مُعَقَّدة تقوم على تجميع معلومات مخصصة، ووضعها في صورة تُمَكِّنُ البشر من تطبيق تلك المعلومات"، وتُعَرَّفُ –أيضًا– بأنها "برامج تستخدم تقنيات الذكاء الاصطناعي؛ من أجل محاكاة سلوك الإنسان، وتتمتع بالمعرفة الفنية والخبرة في مجالات معينة، وتعتمد على مُكَوِّنَيْنِ أساسيّيْن هما:

  - قاعدة المعرفة: هي مجموعة من الحقائق حول نطاق النظام.
  - محرك الاستدلال: يقوم بتحليل المعطيات المتوافرة في قواعدها وتفسيرها؛ لتتمكن –في النهاية– من الخروج بمجموعة من الإجوبة التي تمكنها من التشخيص والمراقبة" (موسى وبلال، 2019: 27).

إضافةً لما سبق تُعدُّ هذه النظم ذات فعآليّة في مجال (الرعاية، التحليل الكيميائي، الائتمان، الحركة الجوية، الهندسة الوراثية)؛ لأنَّ تلك البرامج –بطبيعة الحال– قائمة على الخبرات المتراكمة التي يقوم البشر بإدخالها إلى البرامج والأنظمة من خلال أجهزة الحاسوب؛ لتمكين هذه البرامج من إعطاء الإرشادات والتوجيهات الصحيحة، إذْ تقوم بفرز البيانات وتحليلها بناءً

على ما هو موجود في قواعدها المعرفية، بذلك يمكننا الحصول على برنامج ذكي يستخدم الخبرة التي يدخلها الإنسان في هذه الأنظمة التي من شأنها أن تعطي نتائج فعّالة على أرض الواقع (عفيفي، 2015)، وتتكون الأنظمة الخبيرة حسب ما أشار إليه (محمد ومحمد،2021م) من:

- **قاعدة البيانات:** تُعَدُّ وسيلة الاتصال والتواصل بين المستخدم والنظام الخبير، وتحتوي على مجموعة من البيانات التي تمكنه من ربط المعطيات مع بعضها بعضًا؛ من أجل حل المشاكل التي تواجه المستخدم .
- **مخزن المعلومات:** يتكون من المعلومات والمعارف كافَّةً التي يحتاجها النظام؛ لإتمام الأعمال، إذ يتم إدخال قَدْرٍ هائل من المعلومات إلى ذاكرة الكمبيوتر، تُمَكِّنُهُ من تحديد المعرفة المناسبة لإتخاذ القرار الصحيح لحل المشاكل، إنَّ هذه النظم وظيفتُها استقبال المدخلات من العالم الخارجي عَبْرَ واجهة المستخدم التي تُعَدُّ الوسيط ما بينها وبين المستخدم.
- **الآلات العاملة:** هو الجزء الأخير والمسؤول عن انتقال المعلومات الأوليَّة في سبيل الوصول إلى حلٍّ نهائيٍّ، فهي تعمل على فحص المعلومات الْمُدْخَلة واستخلاص النتائج من خلال تحليل المشكلة بناءً على قاعدة المعرفة، إضافة الى أنها تزود النظام بالمعرفة.

- **الشبكات العصبيّة الاصطناعيّة:** تُعرف على أنها "برامج تعتمد على خلايا مترابطة مع بعضها بعضًا تقوم كل خلية بتنفيذ عمليّة معالجة لحل المشاكل المعقدة وصعبة الفهم التي تتطلب حجمًا كبيرًا من البيانات" (ياسين، 2018: 232)، فقد ظهرت هذه النظم على يد العالمين (بيتس ووارن) عام (1958م)، حيث أُعْلِنَ عنها بشكل رسمي في أول مؤتمر للشبكات العصبيّة الاصطناعية عام (1987م)، كما برز مجموعة من العلماء فيما بعد تَبَنَّوْا الاهتمام بدراسة هذه النظم وتطويرها، وهم (ماك، هيب، مارفن، روزنبلات)، وهذه الشبكات مستوحاة من الجهاز العصبي البيولوجي للإنسان، ومهمتها جمع البيانات وتحليلها وتصنيفها، ومن ثم معالجتها بناءً على المعلومات المتوفِّرة لديها، ومن هنا أصبحت تستخدم في مختلف المجالات الحياتيّة حسب الشحات (Alshahat, 2018).

إضافة لما سبق تشكل هذه الشبكات العصبيّة أداة فعّالة ومهِمَّة في عصر التكنولوجيا؛ لأنها أداة أمنية تساعد على منع وصول الأشخاص غير المسموح لهم باستخدام المواقع، واكتشاف الهجمات الإلكترونيّة عَبْرَ الشبكات العصبيّة، ولأنَّ لها نتائج فعّالة ومفيدة كونها سريعة جدًّا في الكشف عن الخطر والاختراق والتسلل، فالشبكة العصبيّة لديها القدرة على تمييز الأنماط الطبيعية عن الأنماط غير الطبيعية التي تحصل داخل شبكة الإنترنت، عَبْرَ مجموعة من

الخلايا المترابطة مع بعضها وقواعد المعرفة، فتمكنها من تميز الأنماط على الشبكة حسب ديفاكريشس (Devikrishakes, 2013)، وتتكوّن الشبكات العصبيّة من وحدات تسمى خلايا تتكون هذه الخلايا حسب جالو (Gallo, 2015) من:

- **الخلايا الحسيّة (الْمُسْتَشْعِرات):** وظيفتها استلام الإشارات التي يُدْخِلُها مستخدم الشبكة.
- **خلايا الاستلام:** تعمَلُ هذه الْوَحْداتُ على جَمْعِ كُلِّ ما يُدْخَلُ إلى الشبكة واستقبالها في صندوق واحد؛ كي تتمكن من تصنيف هذه الْمُدْخَلات كافَّةً؛ لِتُخْرَج في صورتها النهائيّة.
- **وحدة العمليات:** تُشكّل هذه الخلايا وحدات الاستلام بوصفها طبقةً مخفيَّة وغير مرئيّة تقوم بإرسال الصندوق إلى هذه الوحدة؛ لتقوم بإرسال البيانات إلى الخلايا العصبيّة التي بدورها تنتظر التصنيف؛ لتكون هذه آخر خطوة في الشبكات والحصول عليها بصورتها النهائيّة.

- **النظام الذكي (الوكيل الذكي):** ظهر هذا النظام بشكل لافِتٍ للنظر في السنوات الأخيرة، حيث استطاعت المجتمعات استغلال تكنولوجيا الذكاء الاصطناعي وتطبيقاته الحديثة في تطوير أنظمتها المختلفة لكي يتمّ الاستفادة منها فيما بعد، وعَرَّفه كلٌّ من بينسيون وستيندينغ (Benson & Standing, 2020: 133) على أنه "كيانات برمجيَّة تتصرَّف بالوكالة عن أحد المستخدمين كوسيط بين المستخدم والنظام، ولديه القدرة على فهم البيئة المحيطة به"، وعَدَّها (ياسين، 2020: 118) أنه أحد فروع الذكاء الاصطناعي الْمُهِمَّة، وقد عَرَّفه على أنها "برامج تتصل وتتواصل مع بعضها من خلال استخدامها لغةً مشتركةً فيما بينها، فهي نظم ذكية واستباقية لديها القدرة على التنقل والتكيف في البيئة التي توضع فيها، تتكون نظم الوكيل الذكي حسب ما أشار إليها (جباري، 2017) من:
  - **المستشعرات:** تعمل على استقبال المدخلات الواردة إليها، واستشعار المتغيرات داخل البيئة المحيطة.
  - **المستجيبات:** تعمل على فرز هذه البيانات فور استيعابها لها.
  - **البيئة المحيطة:** هي مخرجات النظام من خلال رد الفعل على فعل معين يقوم به الوكيل الذكي، وهي نتاج لعمل المستشعرات وردود فعل المحركات الموجودة في هذا النظام.
- **الخوارزميات الجينيّة والمجموعات الضبابيّة:** تطورت الخوارزميات الجينيّة في بداية الثمانينيات لتصبح إحْدى الطرائق الْمُهِمَّة والفعّالة للتعامل مع المسائل المعقدة والبحث عن الأمثلة، وقد طرح العالم (جوهن) ومجموعة من طلابه فكرة هذا النظام، إذ تُعرف الخوارزميات الجينيّة على "أنها أسلوب يحاكي نفس طريقة عمل العمليات البيولوجية تقوم بالبحث عن الحلول المثلى بالتوازي، من خلال أسلوب البحث بطريقة عشوائيّة، فهي تعتمد في مبدئها على

مبدأ عمل الجينات الوراثية نَفْسِه" (المنجد، 2020: 46)، أما فيما يتعلق بالمجموعات الضبابيّة فأول من بدأت تتبادر إلى ذهنه هذه النظم العالم البولندي (جان لوكاسيفيتش) عام (1930م)، إضافة إلى العالم الإيراني (لطفي زادة) عام (1965م) فهي كما عرفها (خوالد، 2017: 58) "عبارة عن مهمات معينة، وهي نماذج حاسوبيّة تختص بمعالجة البيانات الْمُشَوَّشَة والغامِضة، أي أنها تعالج البيانات الوسيطة التي لا يمكن معالجتها عبر برامج الحاسوب التقليديَّة، تتكون المجموعات الضبابية حسب ما أشار إليها سايانتيني (Sayantini, 2019) من:

- **البيانات (نظم المنطق الضبابي):** تحتوي على المعلومات والبيانات التي يدخلها المبرمجون في قواعدها المعرفيّة، وتُحَدَّثُ باستمرار.
- **التحويل:** تتم هذه المرحلة بعد الحصول على البيانات واتمام عمليّة الإدخال، حيث تقوم هذه النظم بتحويل المدخلات إلى أرقام؛ كي تتمكن من التعامل معها بناءً على محركات النظام (الحساسات) الموجودة في تركيبتها.
- **المخرجات:** تقوم المحركات بتحويل البيانات إلى قِيَمٍ واضحة بالنسبة لها، ومِنْ ثَمَّ تعمل على اتخاذ القرار وتحويلها إلى مخرجات.

6.2.2 أهميّة الذكاء الاصطناعي:

أصبح الذكاءُ الاصطناعيُّ محورَ اهتمام العالم، فعمليّة التطور والتقدم في الوسائل التكنولوجيّة الحديثة تُعَدُّ من أهم العمليات التي تحافظ على استمرارية المجتمعات، لذا إن لعمليّة استحداث برامج الذكاء الاصطناعي أهمية كبيرة، تَكْمُنُ هذه الأهميَّة حسب وجهة نظر كل من (الصمد ومحمد، 2020) فيما يأتي:

- **في مجال الصحة:** ساعد الذكاء الاصطناعيُّ بشكل كبير في مجال الصحة، والكوادر الطبية، والتشخيص، وعلاج الأمراض، وغيرها من الأمور المتعلقة بالجانب الطبي، فقد اسْتُخْدِمتْ تطبيقاتُ الذكاء الاصطناعي (التعلم الآلي) في التنبؤ بإحتمآليّة إصابة الفرد بمرض معين أو لا، وتحديد نوع هذا المرض، إضافةً لاستخدام النظم الخبيرة بالاسْتِناد على قواعد البيانات في السجلات الإلكترونيّة للمرضى المراجعين، فهي تساعد في تشخيص المريض بصورة مبكرة؛ لتتمكن –فيما بعد– من توفير العلاج المناسب والدقيق وتأمينه له، فضلًا عن تفعيل تِقنيّات الذكاء الاصطناعي للتعرف إلى الكلام من خلال الاتِّصال والتواصل مع المرضى وتسجيل الملحوظات بطريقة تلقائيّة هذا حسب حسب وجهة نظر كل من دافينبورت وكالاكوتا (Davenport & Kalakota, 2019) كما وذكرت (صحيفة البيان، 2021) في موقعها

الرسمي بتاريخ (01\10\2021م) أن تطبيقات الذكاء الاصطناعي (التعلم الآلي) وبرامجه تمتلك القدرة على التنبؤ بأنواع عديدة من الفايروسات الْمُعْدِيَةِ الَّتي من شأنها أن تؤدي بالإنسان إلى الهلاك والموت، بتجميع زهاء (861) مِنْ مختلف أنواع الفايروسات التابعة لعدد كبير من العوائل، وإدخالها في مخازنها؛ لاستخدامها في عملية الفرز والتحليل، بناءً عليها يتمّ تحديد احتمآليّة إصابة الإنسان بالأمراض أو لا.

- **وفي مجال التعليم:** تم تطوير نظام خبير قائم على قواعد المعرفة؛ لمساعدة الطلاب في عملية التَّعلُّم، واستخدامه نظامًا مرجعيًّا؛ لتسهيل حصولهم على الشرح والفهم الكافي حول الأسئلة التي تراودهم، ولديه القدرة على تحليل أداء الطلاب الأكاديمي عَبْرَ تقييم نقاط الضعيف لديه، ثم إعطاؤه مجموعة من الأسئلة التي تركز على أماكن الضعف لديه؛ لتقويته، فضلًا عن أنَّ هذا النظام لديه القدرة على تحليل أداء الطلاب في المحاضرات وإجاباتهم في الامتحانات وتحديد الطلاب الأذكياء والمتفوقين في الصف عن غيرهم من الطلاب العاديين حسب سوبريغانتو وآخرون (Supriganto & Others, 2019).
- **أما في المجال العسكري:** عملت الولايات المتحدة الأمريكيّة على استخدام نظم الوكيل الذكي في العدالة الجنائيّة عند إطلاق السراح المشروط للنزلاء من خلال القيام بتنظيم درجة الخطورة، فهذه النظم يتمّ تطبيقها في جلسات إطْلاق السراح المشروط في مختلف البلاد لديها حسب ويلسيس (Welses, 2017).
- **وفي مجال أمن الدولة:** تعمل النُّظُم الذكيّة على التنقل عبر كميات هائلة من البيانات والفيديوهات الْمُلْتَقَطَة عَبْرَ نظام المراقبة، ومِنْ ثَمَّ إعطاء إشارات وتنبيهات بوجود نشاط غير طبيعي أو مشبوه، فهذه التطبيقات تساعد –بشكلٍ كبيرٍ– في مواجهة الجريمة من خلال مراقبة أي مسكليّات منحرفة تحصل بناءً على قواعد المعرفة والتنبؤ بأن هناك سلوكًا غير طبيعي هذا حسب دافينبورت (Davenport, 2017).
- **وأما في مجال البيئة:** أثبتت الدراسات أنَّ مكبات النفايات ومن خلال قيام مُستشعرات النظام بتقدير حجم النفايات الموجودة فيها، عندما يرتفع مستوى النفايات في المنطقة تقوم هذه المُستشعرات بإرسال البيانات إلى خوادم الإنترنت المرفقة في المنطقة، وهي –من ناحِيتها– تعطي إشارات بأن هذه المنطقة بحاجة إلى إزالة الفائض من هذه النفايات، بناءً على ذلك يتم تحريك عُمّال النظافة؛ لإزالتها عند الحاجة فقط، وليس بشكل يومي، هذا يعني أن آليّة عملها تعتمد –بالدرجة الأولى– على المستشعرات، فهذه التقنيات الذكيّة تفيد في تقليل الجهد المبذول وتساعد في توفير الحمايّة للإنسان من السموم وخطر الإصابة بمختلف الأمراض التي من المحتمل أن يتعرض لها حسب جوبتا وآخرون (Gupta & Others, 2018).

- ممّا سبق يتضح لنا أنَّ الذَّكاء الاصطناعي لا يعتمد في مجال عمله على جانب معين، إنما يتمتع بقدرة على العمل في مختلف الجوانب والمجالات إذا ما تمت برمجة النُّظُم الذكيّة بطريقة تتناسب مع طبيعة العمل؛ كي يتمكن من الاندماج وإدارة المواقف التي يتعرض لها، كما يتضح لنا أن أهمية الذكاء الاصطناعي تنبع من أهميته في القدرة على السيطرة على مجريات الأحداث داخل الشبكة من مُدْخلات البيانات ومُخْرجاتها عَبْرَ تفاعل كُلٍّ مُكَوِّنٍ مَعَ الآخر وقدرته على اتّخاذ القرارات في المواقف بناءً على المعرفة المتراكمة لديها، والتحكم في مجريات الأحداث كافَّةً على الشبكة، وعدم السماح بحدوث أيِّ خلل، إضافة إلى أنه يعمل على تخفيف العبء الواقع على الجهات العاملة في مجال التكنولوجيا؛ نظرًا لكثرة الإقبال على استخدامها، فمن شأنها أن تُقَلِّلَ من الوقت والجهد المبذول من هذه الطواقم البشريّة؛ ما يؤدي إلى تلاشي الأخطاء الَّتي من الممكن أن يقع فيها، والحصول على نتائجَ أعلى دقَّةً وكفاءةً، كما يعد مؤشر اتّجاه الدول إلى إدخال الذكاء الاصطناعي في ميادينها الحياتيّة كافة صفة أساسية في نجاحه وقدرته على التأثير في القرارات داخل الشبكة.

7.2.2 التجارب العالميّة والعربيّة والمحليّة في مجال الذكاء الاصطناعي:

في سبيل مُواكبة التطورات التكنولوجيّة التي يشهدها العالم في الآونة الأخيرة تتسابق الدول –فيما بينها– لإدخال أكبر قدر ممكن من التكنولوجيا لديها، وفيما يأتي عرض لبعض الدول التي عملت على إدخال برامج الذكاء الاصطناعي وأنظمته لديها واستخدامه:

- **تَجرِبة ألمانيا:** يشير بايبل (Bibel, 2020) وبريتبادما (Preetipadma, 2020) إلى أن ألمانيا كانت من الدول الأولى الحاضنة لبرامج الذكاء الاصطناعي وأنظمته، وأن تجربتها مع هذه التقنيات المتطوّرة ليست حديثة، إنما قديمة قِدَمَ نشأتها وولادتها، فهي تسعى لمواجهة التحديات التي تعوق عمليّة التطور ورفع مستوى كفاءة الكوادر البشرية، حيث كانت ألمانيا من الدول الرائدة والمتصدرة للمراكز الأولى في استخدام الدراسات والأبحاث والمشاريع التطبيقيّة المتعلقة بنظم الذكاء الاصطناعي في أوروبا.

  كما أشار ياكوبو وآخرون (Yakubu & Others, 2020) في دراسة أجريت في ألمانيا حول استخدام الذكاء الاصطناعي في حماية المعلومات الشخصيّة على أجهزة الحاسوب من الهجمات الإلكترونيّة التي تتعرض لها، فكانت أهميتها تنبع من تبني تطبيقات الذكاء الاصطناعي لحماية البيانات؛ لأنَّ الطرائق التقليدية لم تعد تجدي نفعًا، والعمل على توظيف الشرطة الرقميّة لزيادة الحمايّة والرقابة الأمنيّة المستمرة.

- **تَجرُبة المملكة العربية السعودية:** يذكر ميميش وآخرون (Memish & Others, 2021) أن المملكة العربية السعودية قامت بتأسيس ما يعرف بالهيئة السعودية للذكاء الاصطناعي؛ للإرتقاء بمستوى المملكة، فهي من الدول التي تحتل مراتب عليا في استخدام تقنيات الذكاء الاصطناعي وأنظمته في مختلف القطاعات؛ لكونها تتمتع ببنيّة تحتيّة كبيرة سرعت من عملية التحول الرقمي في عالم الذكاء الاصطناعي، وفي السياق نَفْسَهِ ذكرت (صحيفة الرياض، 2021) بتاريخ (05\04\2021م) على موقعها الرسمي صعود المملكة العربية السعودية إلى مراتب عليا في مجال الذكاء الاصطناعي على مستوى العالم، وليس على مستوى الدولة، وقد أطلقت ما يسمى بالمنصة الوطنيّة للذكاء الاصطناعي، فهي تسعى جاهدة لاستثمار كل ما يتعلق بتطبيق هذه البرامج والتقنيات الحديثة لديها، فهي تخدم مصالحها وتمنحها مزيدًا من التقدم والتطور الرقمي في جوانب حياتها المختلفة سواءٌ الاقتصاديّة أم الجنائيّة أم الترفيهيّة، في حين نشرت (صحيفة الوطن، 2020م) بتاريخ (28\10\2020) أن المملكة العربية السعودية قامت بنقلة نوعيّة فريدة من نوعها بدخولها إلى عالم الذكاء الاصطناعي واستخدامه في مختلف المجالات سواءٌ أكان ذلك في العالم الافتراضي أم في العالم الواقعي، بتوقيع اتِّفاقات ومذكرات تفاهم بينها وبين الدول الأخرى، إضافة إلى تدريب المهارات التي يمتلكها العاملون في هذا المجال وتطويرها بما يتناسب مع البرامج والأنظمة الموجودة لديها، وذكرت (صحيفة العين الإخبارية، 2021م) على موقعها الرسمي بتاريخ (08\02\2021م) أن المملكة العربية السعودية وقَّعَت اتفاقية تفاهم مع فيليبس العالمية؛ لتطوير القطاع الطبي والصحي وتعزيز استخدام تطبيقات الذكاء الاصطناعي في هذا المجال؛ لما تعطيه من نتائج فعّالة ودقيقة تساعد في علاج المرضى، وتُسْهِمُ بالارتقاء بمستوى الصحة لديها، كما يرى (بكر، 2020) أن المملكة العربية السعودية تسعى جاهدة إلى رفع مستوى الأمن والأمان للمواطن ولأنظمتها، من خلال تطبيق الذكاء الاصطناعي للحدِّ من الهجمات الإلكترونيّة التي تتعرض لها، وأن المملكة تشهد قمة عالميّة فريدة من نوعها بدخولها إلى عالم الذكاء الاصطناعي وتطبيق هذه الأنظمة التي تمّ توظيفها للكشف عن المجرمين الإلكترونيين الذين يقومون باستغلال الثغرات في الفضاء الإلكتروني والاحتيال، كما لديها القدرة على التنبؤ بالجرائم التي من المحتمل حدوثها في المستقبل.
- **تَجرُبة الإمارات:** أشار المرزوقي (Almarzooqi, 2019) في دراسة علميّة قام بها إلى أن دولة الإمارات نجحت في تجربة التقنيات الحديثة، فهي تسعى إلى رفع مستوى الكفاءة والمهارات لدى كواردها البشرية؛ لتمكينها من التعامل مع التقنيات الحديثة، كما تسعى الى تعزيز قدرات الإمارات في مجال التقنيات الحديثة، فمن خلال تجاربها مع الذكاء الاصطناعي أسَّسَتْ ما يُسمّى بوزارة الذكاء الاصطناعي، كما طبَّقَتْ الذكاء الاصطناعي في مختلف

قطاعاتها وتنمية مهارات الكوادر لديها؛ لتسهيل آليّة التعامل مع هذه التطبيقات الحديثة والتمكن من إدخال ثقافة الذكاء الاصطناعي في المجتمع الإماراتي (ماجد، 2018)، إضافة لما سبق يذكر (عبد الرحمن، 2019) أن هناك دراسة أخرى أجريت في دولة الإمارات استثمرت تطبيقات الذكاء الاصطناعي في العمل على اكتشاف جرائم الاحتيال الإلكترونيّة التي تحدث في البنوك والمؤسسات المحلية، واستخدام المجرمين المحترفين للهُوِيّات المزورة، إضافةً إلى غسيل الأموال، فكانت أهميتها تتمثّل في تبني الإمارات لتطبيقات الذكاء الاصطناعي في البنوك والمؤسسات، والتخفيف من جرائم الاحتيال التي كانت تُشَكِّلُ معضلة حقيقية تعاني منها، فنظم التعلم الآلي تمتلك القدرة على المتابعة المستمرة لمجريات الأحداث كافَّةً، دون كلل أو ملل، من خلال قواعد البيانات التي تحتوي على كم هائل من المعلومات، وتحليل المسلكيات المشبوهة عن المسلكيات غير المشبوهة.

إن الامارات –ضمن تجاربها في تطبيق الذكاء الاصطناعي– تمكنت من إلقاء القبض على (316) مطلوبًا من خلال تقنية التعلم الآلي بتركيب كاميرات على الشوارع العامة حيث تعتمد في مبدأ عملها على تقنيات وتطبيقات الذكاء الاصطناعي من خلال فرز صور الأشخاص المطلوبين للعدالة والأشخاص العاديين.

- **التَجرُبة المحليّة:** يرى (موسى، 2018) أن الحكومة الفلسطينة تسعى إلى تمكين المجتمع الفلسطيني في استخدام الذكاء الاصطناعي؛ لمواكبة التطور والتقدم في مجال التكنولوجيا ومواجهة المُعوقات التي تَحُدُّ من إمكانات المجتمع في التطور، حيث ذكر (جهاز الشرطة الفلسطينة، 2020م) أنَّ الحكومة الفلسطينيّة تقف على سلم التقدم والتطور من خلال دخولها عالم الذكاء الاصطناعي واعتمادها للخوذة الذكيّة في العمل الميداني لضباط الشرطة؛ لتسهل عملية القبض على الهاربين الفاريين من العدالة، كما تسعى الحكومة الفلسطينية –أيضًا– إلى جعل برامج الذكاء الاصطناعي وأنظمته فعّالة في مختلف قطاعاتها؛ لذلك أَوْلَت هذا المجال اهتمامًا كبيرًا.

نستنتج ممّا سبق أنه بالإمكان الاستفادة من الذكاء الاصطناعي في شتى المجالات وليس في مجال واحد؛ لذلك ومِنْ هنا تتسابق دول العالم؛ من أجل إدخال الذكاء الاصطناعي في مجالات عملها، وما نراه أن المجتمعات أصبحت حبيسة التكنولوجيا؛ لذا باتت تولي كثيرًا من الاهتمام في توظيف النظم الحديثة التي شكلت تغيّرًا جذريًّا في مختلف مناحي الحياة.

8.2.2 المُعوّقات التي تواجه تطبيق الذكاء الاصطناعي:

على الرغم من التطور الكبير الذي أحرزته التكنولوجيا في عصرنا الحالي فإنَّ هناك العديد من المُعوّقات التي تَعوقُ عملية تطبيق الذكاء الاصطناعي، لعل من أهمها ما يأي:

- **المُعوّقات البشرية:** بالرغم من أهمية نظم الذكاء الاصطناعي في المجتمع فإنَّ استحداثها وتطبيقها من الكوادر البشرية العاملة في هذه المجالات يشكل تحديًا وصعوبة، فهذه النظم لا تعتمد في مبدأ عملها على الطرائق التقليديّة المتعارف عليها، إنما بحاجة الى أشخاص ذوي خبرة ومهارة وكفاءة لتطبيقها، كما أنها بحاجة إلى المتابعة الدّائمة والتطوير المستمر؛ كي تستفيد مؤسسات المجتمع من الإمكانات التي تقدمها هذه النظم حسب وجهة نظر ماركو (Marko, 2017)، فقد تمّ تلخيص المُعوقات البَشرية حسب وجهة نظر كل من ويزل وهاجندورو (Wezal & Hagandor, 2019) في الآتي:
  - قلة المبرمجين المتخصصين في مجال التقنيات الذكيّة بالمقارنة مع حجم التنوع في برامج الذكاء الاصطناعي وأنظمته.
  - عدم قدرة المواد الأكاديميّة النظريّة على مواكبة التطور السريع للابتكارات التي تشهدها تقنيات الذكاء الاصطناعي.
  - قلة التدريبات التطبيقيّة في المواد النظريّة، إضافة إلى قلة التدريبات المهنية التي تمكن الكوادر البشرية من فهم برامج الذكاء الاصطناعي.

كما يشير (الشهري وعبدالله، 2001م) إلى أن الشح في عدد الموظفين ذات الكفاءة والمُتخصصين والحاصلين على مؤهلات علمية في هذا المجال من شأنها أن تعوقَ من عملية تطبيق هذه التقنيات الحديثة والاستفادة منها، فقد ذكرت (صحيفة البيان الإماراتية، 2019م) بتاريخ (04\11\2019) أن هناك معوقات تواجه الدولة في مرحلة تطبيق ما يسمى بالذكاء الاصطناعي داخل مجتمعها، خاصة أنها في هذه المرحلة الانتقاليّة تقفز من واقع الحياة التقليديّة إلى الحياة الرقميّة، فنقص الكفاءة والمهارات لدى الكوادر البشرية من أُولى العوائق التي واجهتها الإمارات، فضلًا عن الموازنات الماليّة الْمُخصَّصة لهذه التطبيقات وليدة العهد، فتطبيق هذه التقنيات يُكلف الدولة أموالًا باهظة، كما ذكرت (صحيفة المصراوي، 2021م) بتاريخ (05\10\2021م) أن أنظمة الذكاء الاصطناعي تلتقط نسبة ضئيلة من المسلكيات اللاأخلاقية والمؤذية التي يتعرض لها مستخدمو الشبكات الإلكترونيّة، من هنا تحتاج هذه الأنظمة إلى كوادر بشرية متخصصة ومؤهلة في هذا المجال، وقادرة على استخدام هذه النظم، وظيفتها تعزيز دور تلك الأنظمة، وذلك بتتبُّع جميع المحتويات المسيئة التي تلتقطها أنظمة الذكاء الاصطناعي، والعمل على مراقبة ما يتم نشره على فيسبوك وغيره من مواقع

التواصل الاجتماعي، فالمبرمج الذي يعمل في مجال الذكاء الاصطناعي ينبغي أن يكون على اطِّلاعٍ وإلمامٍ كاملَيْنِ بأدق التفاصيل المتعلقة بالنظم والبرمجيات الحديثة، إن إهمال هذه الناحية ستؤدي إلى عرقلة قدرته على التعامل مع هذه النظم، مما سبق نستنتج أن الخبرة والمعرفة في تقنيات الذكاء الاصطناعي تحتاج الى تدريبات خاصة وتطوير للقدرات والمهارات التكنولوجيّة لدى الأشخاص المؤهلين المتخصصين في هذا المجال، هذا ما أكده المبحوثين من خلال المقابلة التي أجريت معهم حيث أكدوا على أن وجود أشخاص غير متخصصين وغير حاصلين على مؤهلات علميّة تمنحهم القدرة على التعامل مع هذه التطبيقات في الوزارة من شأنها أن تشكل عائقًا كبيرًا أمام إمكانات الوزارة في جلب هذه التطبيقات وتطبيقها حتى وإن استطاعت استيراد المعدات والأجهزة المتعلقة بأنظمة الذكاء الاصطناعي وبرامجه؛ ما يعني تخزينها في المخازن لحين توفير الكفاءات المتخصصة القادرة على استخدامها، خاصة أن هذه البرامج والأنظمة تشكل بالنسبة للمجتمع الفلسطيني علمًا حديثًا جداً وضئيل الانتشار، وتختلف كليًّا عن البرامج والأنظمة التقليديّة المتوافرة في متناول اليد التي يمكن لأي مبرمج التعامل معها.

- **المُعوّقات التقنيّة:** إنَّ من أهم مُعوّقات تطبيق نظم الذكاء الاصطناعي هي الضُعف في إنشاء بِنًى تحتيّة صلبة قادرة على تحمُل هذه البرامج وتنوعها، فهي تتكون من مجموعة ضخمة من البيانات التي تحتاج إلى بِنًى تحتيّة، تشكل أرضية صلبة؛ لتتمكن من استيعابها، كما أن هذه البرامج الحديثة لا تستطيع أن تتكيف مع الْبِنى التحتيّة التي تستوعب البرامج القديمة والتقليدية المتعارف عليها، إنما تحتاج الى بيئة صلبة وقوية ترتكز عليها في عملها، إن ضعف البنى التحتيّة يُشكل أحد اكبر العوائق أمام استخدام تطبيقات الذكاء الاصطناعي حسب ماكيندريك (Mckendrick, 2018) وفوجيماكي (Fujimaki, 2020)، هذا ما أكده (مدير وحدة أمن المعلومات في وزارة الاتصالات وتكنولوجيا المعلومات،2021) خلال المُقابلة التي أجريت معه يوم الإثنين الموافق (28\09\2021)، حيث أكد على أن ضعف البنيّة التحتيّة في الوزارة يُشكل عائقًا أمام قدرتها على جلب هذه البرامج والأنظمة وتطبيقها، إن البنيّة التحتيّة المتوافرة في الوزارة غير قادرة على استيعاب التنوع في برامج الذكاء الاصطناعي، إن أساس تطوير الذكاء الاصطناعي مبني على وجود بنيّة تحتيّة صُلْبة، تستطيع تحمل التنوع في برامج الذكاء الاصطناعي وأنظمته، حيث إن كل مجال من مجالاته يحتاج لبيانات وخوارزميات تختلف عن الأخرى، فكلما تطورت البيانات والبرامج والتقنيات زاد حجم البيانات المخزنة؛ ما يستدعي وجود بِنْيَة تحتيّة صلبة ذات أساس قوي؛ كي تتمكن من الاستمرار في التطور والتقدم.
- **المُعوقات المآليّة:** إنَّ استحداث تقنيات الذكاء الاصطناعي وبرامجه والخدمات المستفادة منها من شأنها أن تتطلب موازنات مآليّة عآليّة؛ ما يستدعي من المؤسسات والدولة في المجتمع

توفير دعم مادي كبير، وتخصيص موازنات مآليّة ونفقات؛ كي تتمكن من جلب هذه البرامج نظراً لكلفتها المآليّة العآليّة حسب كيماري وشيفاسترا (Kimari & Shivastara, 2019)، كما أنَّ أيَّ مجتمع يسعى للتطور والتقدم بحاجة إلى وجود رأس مال، فأي إهمال في هذا الجانب يترك انعكاسات سلبيّة في عدم القدرة على اللحاق بكوكبة التطورات، فكلما ارتقى المجتمع بالتطورات التكنولوجيّة ازدادت الحاجة إلى تكاليفَ أعلى، إضافة إلى أن هذه النظم الحديثة تكلفتها باهظة بسبب ما تحتاجه من صيانة مستمرة وتطوير في برمجياتها حسب وجهة نظر ديفانبورت (Davenport, 2018).

إن ما يؤكد على ما سبق ما أشار إليه العاملون في وزارة الاتصالات وتكنولوجيا المعلومات، من خلال المُقابلة التي أجريت مَعهم يوم الثلاثاء الموافق (29\09\2021)، حيث أكدوا على أن بعض برامج الذكاء الاصطناعي تصل كُلفتها إلى مليون دولار؛ ما يشكل عائقًا كبيرًا جدًّا أمام قُدرة الوزارة على الحصول على مبالغ مآليّة كبيرة، مما سبق يتضح أن هناك أكثر من معوّق يرتبط كل منها بالآخر تَعوق تطبيق برامج الذكاء الاصطناعي، إن معظم هذه المعوّقات تؤثر في إمكانية المجتمع على مواكبة التطور في التكنولوجيا؛ لذا لا بُدَّ من العمل على إزالة العراقيل والمُعوّقات لتطوير المجتمع بما يتناسب مع متطلبات العصر ومن أجل تفعيل برامج الذكاء الاصطناعي بشكل صحيح.

3.2 الجرائم الإلكترونيّة:

1.3.2 مقدمة:

مَعْلومٌ أنَّ الطَّبيعةَ البشريَّة تميل إلى الخير والشر، وهذا ما يُفَسِّرُ لجوءَ بعضِ البشر إلى ممارسة الجريمة، التي من بينها استخدام التكنولوجيا والإنترنت ووسائل التواصل الاجتماعي بطُرُقِها السَّيِّئة والمؤذية، فقد أصبحت هذه الظاهرة المخالفة لما هو متعارف عليه في المجتمع لا تَخْدِمُ إلّا مصالح الجاني وتؤدّي إلى أضرار بالغة بالْمَجْنِيِّ عليه والدولة والبيئة المحيطة، وقدْ ولَّدَ هذا الاستخدام السيئ للتكنولوجيا ما يُسمّى بالجريمة الإلكترونيّة، التي يشكل فيها الفضاء الإلكتروني مسرح الجريمة، من خلالها تتكامل أركان الجريمة الإلكترونيّة، لكن ضررها يمتد إلى الحياة الواقعيّة والافتراضيّة في آن واحد.

فالجريمة الإلكترونيّة من القضايا التي يقف العالم أجمع أمام محاولة الحدِّ منها، فهذا النوع من الجرائم الْمُستَحْدَثة مُتعدِّدة الأشكال والأنماط تُلحق الضَّرر بدول العالم كافَّةً، فضلاً عن التفاوت في مدى تركيز كُلِّ دولة في الحد منها ومقاومتها والتخلُّص منها، بسَبِّبُ ما ينتج عنها من مشاكلَ اقتصاديَّةً واجتماعية، ونفسية، وسياسية، كلٌّ منها مرتبط بالآخر.

2.3.2 مفهوم الجريمة والجريمة الإلكترونيّة:

تكمن مفاهيم الجريمة والجريمة الإلكترونيّة في الآتي:

- **الجريمة لُغةً:** "التعدي والذنب والمكروه ويرجع أصل الكلمة إلى الجذر الثلاثي (جرم) يجرم جرمًا، وهي كل أمر إيجابي أو سلبي يعاقب عليها القانون، سواء كانت جنحة أم جناية أم مخالفة" (المجعم الوسيط، 2004: 118) ويقول الله سبحانه وتعالى في سورة (المائدة، الأية 8) "وَلَا يَجْرِمَنَّكُمْ شَنَآنُ قَوْمٍ عَلَىٰ أَلَّا تَعْدِلُوا".
- **الجريمة اصطلاحًا** "هي كل فعل غير مشروع صادر عن إرادة الجاني يقرر له القانون عقوبة أو تدابير احترازية" (الحسناوي، 2018: 21).
- **الجريمة بوصفها ظاهرة اجتماعية:** عرفها (مجيد، 2019: 17) على أنها "خروج الفرد عن القيم الاجتماعية والعادات المُتعارف عليها في المُجتمع، وممارسة الفرد سلوكيات تتعارض مع القيم السائدة في المُجتمع تَستوجب مُعاقبة الفاعل عليها".
- **الجريمة قانونياً:** عَرفها (بشير، 2009م) المُشار له في (الرواشدة والطراونة والضلاعين، 2020: 18) على أنها "كُل فعل مُخالف لأحكام قانون العقوبات وهو الذي يَتضمن الأفعال المُحرمة، ويحدد ما مقدار العقوبة المفروضة على اعتبار أن الجريمة عمل فيه ضرر على المجتمع لذلك فُرض العقاب على مُرتكبها".
- **الجريمة إجرائيًّا:** هي مَسكليات منافية لأخلاقيات المجتمعات وعاداتها وتقاليديها ومخالفة للقانون، يقوم بها شخص أو جماعة يشتركون في هدف معين؛ بغية إلحاق الضَّرر بغيرهم؛ بُغية الحصول على منفعة مادّيَّة أو رغبة في الانتقام.
- **إلكتروني لغة:** "اسم مَنْسُوبُ إِلَى الإِلِكْتُرُونِ، ويعني الشحنة الكهربائيّة السالبة التي تُعتبر جزء لا يتجزأ من الكهرباء" (معجم اللغة العربية المعاصرة، 2008: 111).
- **الجريمة الإلكترونيّة:** ينقسم مفهوم الجريمة الإلكترونيّة الى مقطعين الجريمة (Crime) والإلكترونيّة (Cyber) عرفها (لُطفي، 2019: 27) "أنها الجرائم المرتكبة عَبْرَ جهاز الكمبيوتر وغيرها من وسائل الاتِّصال الحديثة"، وعرّفها فرونزا (Frunza, 2016: 209) على أنَّها "كُلّ فعل ضار يتم من خلال وسائل تكنولوجية حديثة بما في ذلك الأجهزة الذكيّة والبرامج والاتصالات"، بينما عرفها (المؤتمر الدولي لمكافحة الجريمة، 2016) على أنها "كُلُّ سلوك إجرامي يرتكبه شخص أو مجموعة من الأشخاص يحترفون الإجرام؛ لتحقيق أهدافهم ضمن نطاق أكثر من دولة" وأقَرَّ قانون الجرائم الإلكترونيّة الفلسطيني رقم (28) لسنة (2020) على أنها "كل استعمال لوسائل التكنولوجيا في تهديد أو ابتزاز شخص آخر".

- **أما الجريمة الإلكترونيّة إجرائيًّا:** هي مجموعة من الأفعال والسلوكات المنحرفة التي من شأنها أن تُلحق الضَّرر بالشخص الذي وقع ضحية للجاني ومن حوله بأي جانب من جوانب حياته، تتم هذه الأفعال في الفضاء الإلكتروني، ويقوم خلالها الجاني بأعمال التزوير والابتزاز والاحتيال إما بدافع المَنفعة أو الانتقام، حيث تؤدي إلى أضرار كبيرة للأفراد والمجتمعات.

3.3.2 نَشأة الجريمة الإلكترونيّة:

كانت البداية الأولى للدخول إلى عالم التكنولوجيا وتقنيات المعلومات والاتصالات باختراع أول جهاز حاسوب عام (1940م)، فيما بعد انثبقت سلسة من التطورات المُتلاحقة لتَصميم أجهزة حاسوب، حتى وصل الإنسان إلى مَرحلة بدلًا من الاستخدام الإيجابي لهذه الآلة إلى استخدامها بطَريقة سَلبية ومُسيئة للأخلاق أخذت هذه المسلكيات مُسمى الجَريمة الإلكترونيّة، فكانت بداية ظهور الجرائم الإلكترونيّة في العالم الإلكتروني والواقعي ما بين عام (1960–1970)، إذ كانت هذه الجرائم لحداثتها تقتصر على أجهزة الحاسوب فقط، وبعد ربط الحواسيب والاتصالات مع بعضها عَبْرَ تقنيات المعلومات التي أصبحت تتطور مع مرور الوقت حيث بدأ المُجرمون باستغلالها، فمن خلالها تمّ اللجوء الى مختلف الأساليب الاحترافية الإجرامية لارتكاب الجرائم الإلكترونيّة (محمد، 2016م).

كما كان أول ظهور لأجهزة الحاسوب التي تَحتوي على شبكات الإنترنت والاتصالات التي تربط بين أنحاء العالم كافة، وجعلت العالم متقاربًا على الرغم من بعد المسافات في نهايات عام(1969م) حيث أنْشأتْهُ وزارة الدفاع الأمريكية، وفي فترة الثمانينات بدأ البشر بصناعة الفايروسات الإلكترونيّة واستخدامها لإلحاق الضرر بأجهزة الحاسوب والشبكات عَبْرَ ارتباطها بالإنترنت في المواقع الإلكترونيّة، حيث تمكَّنَ الشاب (موريس) عام (1988م) من نشر فيروس إلكتروني تَمكَّن من خلاله مُهاجمة آلافَ أجهزة الحاسوب عبر شبكة الإنترنت، الأمر الذي تسبب بأضرار بالغة ومخاسر كبيرة (الحسيناوي، 2018م)، كما عمل المُجرمون الإلكترونيون فيما بعد على تَطوير فايروسات لاستخدامها في ارتكاب الجرائم الإلكترونيّة وفي عام (2010م) تمّ تَطوير دودة إلكترونيّة (فايروس إلكتروني) الهدف منها اختراق وحدات التَحكُّم تُسمى (stuxnet worm) وهي دودة خبيثة تصيب أنظمة الويندوز وتلحق الضرر بها وتتسبَّب في إتلافها حسب فرونزا (Frunza, 2016).

وقد شهدت فترة التسعينات ازدهارًا مهولًا في حقل الجرائم المعلوماتيّة والتقنية وتغيّرًا في نطاقها ومفهومها وأحدثت شبكات الإنترنت والاتِّصالات تسهيلات لعملية دخول الأنظمة واقتحام شبكات المعلومات واستغلالها فأصبحت تضمُّ أعدادًا كبيرة من المستخدمين الرقميين في دول العالم المختلفة.

فالجريمة الإلكترونيّة تنقسم إلى قسمين:

- **القسم الأول:** يتكون من الشبكة بوصفه كائنًا إجراميًّا، مثل التطفل والتدمير والتعدي على الممتلكات.
- **القسم الثاني:** يتكون من ارتكاب الجرائم مثل الاحتيال والإثارة الجنسية والتجارة غير المشروعة وسرقة البنوك حسب كلوف (Clough, 2015).

4.3.2 أركان الجريمة الإلكترونيّة:

الجريمة الإلكترونيّة في مجملها العام هي جريمة كغيرها من الجرائم الأخرى تقوم على ثلاثة أركان أساسية، وإذا لم تتكامل هذه الأركان فلا يمكن اعتبارها جريمة، تتمثل تلك الأركان في:

- **الرُّكن القانوني (الشرعي):** يُقصد به أن يكون هناك نص في القانون يجعل من ارتكاب هذا الفعل جرمًا ويعاقب على إتيانه، ويشترط فيه أن يكون ساري المفعول في الوقت الذي اقترف فيه الجاني الفعل الإجرامي، والأصل في اكتمال أركان الجريمة الإلكترونيّة كافّةً معاقبة الجاني، بمعنى أنه بدون وجود نص قانوني مكتوب في القانون لا يُمكن اعتبار الفعل جريمة يُعاقب عليها أو فعلًا مخالفًا للعادات حسب ما هو متعارف عليه (الطيفي، 2019).
- **الرُّكن المادي:** يتمثل في الأداة أو الشيء الملموس التي يتم ارتكاب الجريمة من خلالها، فلا يمكن للجريمة الإلكترونيّة الاكتمال إلا بوجود جهاز ملموس يُشَكّلُ وسيطًا لدخول العالم الافتراضي؛ للقيام بالفعل الإجرامي في الفضاء الإلكتروني، فالعالم الرقمي يُعَدُّ مسرحًا للجريمة كما العالم الواقعي وللدخول إلى هذا العالم يستلزم وجود جهاز حاسوب، هذا الجهاز هو الأداة التي يتم من خلالها القيام بالجريمة؛ من أجل إلحاق الضرر والحصول على مكاسب مادية (مدين، 2020م)، بمعنى آخر أن اقتحام أجهزة الحاسوب أو شبكة الإنترنت للقيام بالسلوك الإجرامي الواقع على الضحية يُعَدُّ رَكيزة أساسية لاكتمال حدوث الفعل الإجرامي، هذا ما يَجعل من الجريمة الإلكترونيّة صعبة الإثبات (لطفي، 2019).
- **الرُّكن المَعنوي:** هذا الرُّكن يعني توافر الإرادة الكاملة للجاني بارتكاب جَريمة داخل شبكة الإنترنت أو جهاز الحاسوب وإلحاق الضرر بغيره، فالعبث والاطِّلاع على المعلومات الشخصيّة للفرد في شبكة الإنترنت والقَرصنة والاستغلال وتهكير الحاسبات وأي شكل من أشكال الجرائم التي تحصل داخل الشبكة بطريقة غير مشروعة يمثل الرغبة الموجودة والكامنة لدى الجاني من ارتكابها (الصبار، 2015).

5.3.2 عوامل ارتكاب الجرائم الإلكترونيّة:

هناك العديد من العوامل التي تدفع الفرد لممارسة الجريمة الإلكترونيّة، أهمّها ما يأتي:

- **الضغوط العامة:** تلعب الضغوط العامة دورًا مهما وكبيرًا في مدى إقبال أو عزوف الفرد عن ارتكاب الجرائم الإلكترونيّة الواقعة في محيط الفضاء الإلكتروني، فقد رأى كل من مازيرول وبوتيرنوستير (Mazerolle & Poternoster, 1994) حسب ما أشار إليه (البداينة، 2014م) أن الظروف المحيطة بالفرد في المجتمع وشعوره بالعجز في الحصول على أهدافه بالطرق المشروعة لها دورٌ كبيرٌ في زيادة نسبة إقباله على الجرائم الإلكترونيّة، إن عدم تحمله للضغوط الحياتية يدفعه للجوء إلى الفضاء الإلكتروني؛ من أجل القيام بمسلكيات منحرفة.
- نستنتج مما سبق أن الضغوط العامة المحيطة بحياة الفرد قد تكون الدافع الأساسي للجوء إلى ارتكاب الجرائم في الفضاء الإلكتروني، فعلى سبيل المثال إن ظهور فايروس كورونا بشكل مفاجئ عطل كثيرٍ من مرافق الحياة بالإضاقة إلى التغيُّر في ظروف الحياة الاجتماعية والاقتصادية والثقافية وازدياد نسبة البطالة بين أبناء المجتمع، كذلك أوقات الفراغ التي تتسبب في إزدياد نِسبة الجرائم الإلكترونيّة، فالفرد كلما تعرض لمزيد من المشاكل والظروف القاسية في حياته زادت من نسبة إقباله إلى الانحراف واتِّباع مسلكيات مخالفة لما هو متعارف عليه، من هنا عكست العوامل التي يتعرض لها الفرد وشهدها المجتمع في الآونة الأخيرة آثارًا سلبيّة، جعلت من الفضاء الإلكتروني وكْراً للقيام بمسكليات مُنحَرِفة، ومنافية للأخلاق ولقوانين المُجتمع، إما من أجل الحصول على المال، أو بدافع الانتقام، أو لتفريغ الغضب والضغوط الداخليّه.
- **ضُعف الرقابة الأمنيّة:** يؤكد بيريرا (Pereira, 2014) أنَّ ضعف الحماية الأمنيّة للتقنيات التكنولوجيّة الحديثة مُرتبط بارتكاب الجرائم في الفضاء الإلكتروني، فالجرائم الإلكترونيّة ما هي إلا مُحصلة الخَلل في معالجة هذه الثّغرات الأمنيّة التي تتسبب في استغلال الجناة لها وتمكنهم من ارتكاب المَسكليات المُنحرفة، والحصول على مطالبهم بطرائقَ غير مشروعة، فتُعزز لديه رغبة الإقبال مرات عديدة لارتكاب هذه الجرائم، في هذا السياق يتضح لنا أن ضعف الحماية الأمنيّة على مواقع الإنترنت واستغلال المجرمين والهاكرز للثغرات الأمنيّة تساهم في زيادة الجرائم الإلكترونيّة، لاسيما أن العالم الافتراضي أصبح مكتظّاً بمستخدميه من مختلف المناطق حيث إنَّ مختلف دول العالم تعمل على محاربة ظاهرة انتشار الجرائم الإلكترونيّة، لكن في فلسطين الحال مختلف خاصة مع سياسة التَّضييق التي تتبعها سلطات الاحتلال الإسرائيلي، التي تهدف إلى زيادة نسبة الجريمة وتفشي الفتن والفساد في المجتمع

الفلسطيني؛ لإضعاف الروابط الاجتماعية والتماسك الاجتماعي حيث تعمل على التضيق في جانبين:

- **الجانب الأول:** مَنع الجهات المُختصة في مجال التكنولوجيا الحصول على بعض المعلومات المُتعلقة بمواقع الجُناة على الشبكات الإلكترونيّة، وحجب الكثير من المواقع التي تَمنعهم من التَعرف على الجناة، إضافة إلى حجز الكثير من المُعدات الإلكترونيّة التي تُعد وسائل فعّالة لتقليل نِسبة الجرائم الإلكترونيّة.
- **الجانب الثاني:** عندما تتمكن الجهات المختصة من التوصُّل لموقع الجاني تعمل إسرائيل على منع وصول الجهات التنفيذية لإحضار الجاني كون الجاني موجودًا في مناطق تصنف على أنها (C)؛ ما يُشَكِّل مصدر راحة لهم بتوفير مكان معزول وبعيد عن إنفاذ القانون؛ إذ تُشَكِّل فرصةً لهم لارتكاب المسلكيات المنحرفة.

- **أوقات الفراغ:** إن للبيئة المحيطة بالفرد تأثيرًا كبيرًا في استغلال أوقات الفراغ بالشكل الصحيح، تحديداً وأن وقت الفراغ له صِلة بارتكاب الفرد للجرائم في الفضاء الإلكتروني، حيث إن البيئة التي يُمْضي فيها الفرد ساعات طويلة دون ممارسة أي نشاط ترويحي يشعره بالراحة والإيجابية تشكل خطوة أولى في ممارسة الجريمة والانحراف.

إن ما سبق يؤكد لنا أن وقت الفراغ له دورٌ كبيرٌ ومهمٌّ في دفع الجُناة لارتكاب الجرائم الإلكترونيّة فكثرة الأوقات التي تخلو من أي أنشطة أو أي اعمال تولد لدى الفرد التفكير في المسلكيات المنحرفة، خاصة في ظل ظروف التغيرات السريعة التي تَمر بها المُجتمعات في الآونة الأخيرة، جراء إنتشار وباء كورونا الذي دفع العالم إلى الإلتزام بالحجر المنزلي وعَدم الخروج، والاعتماد على الإنترنت في إتمام مختلف الأعمال؛ فأصبحت تُشكل هذه التَغيرات السريعة زيادة في أوقات الفراغ، إذ إنها تقيد حركة الفرد بشكل كامل، وانعدام الحياة في الخارج وانعدام الروابط الأسرية في الداخل ولَّد لدى الفرد الضغوط خاصة في ظل ضعف الترابط الأسري، وانغماس كل فرد في العائلة في حياته الشخصيّة؛ ما يدفعهم إلى اللجوء لوسائل التواصل الاجتماعي الْمَنْفذ الوحيد للبقاء على تواصل مع العالم الخارجي واستغلالها بشكل مسيء، حيث إن حاجتهم لوجود منفس قد يدفعهم لاستخدامها بشكل خاطئ وبحكم تواجدهم لأوقات طويلة في المنزل بالمُقارنة مع الأوقات التي كانوا يُمضونها في الخارج والقيام بمختلف الأنشطة الحياتية؛ ما يتسبب في كثرة المشاكل العائليّة التي تولد لديهم التفكير بمسلكيات مرفوضة اجتماعياً (الزعارير وأبو عبيلة وأبو الملحم، 2015).

هذا ما يعكس آثارًا سلبية على حياة الفرد والمجتمع، واستمرار إهدار الوقت لساعات طويلة على شبكة الإنترنت وإهمال البيئة المحيطة نتيجة قلة الوعي والجهل تلعب دوراً في تغير

مسلكياته والتراجع عن القيم الاجتماعية المتعارف عليها، وتصبح بمثابة روتين من الصعب التراجع عنها بعد انتهاء الجائحة؛ كونه تشرَّب هذه المسلكيات وتعوَّد عليها؛ الأمر الذي قد يتطلب الحاجة إلى جلسات تفريغ نفسي لإعادة تأهيله؛ ليتمكَّن من العودة إلى الأنشطة الحياتية القديمة، هذا الأمر الذي يفسر لنا ارتفاع نسبة الجريمة الإلكترونيّة فترة جائحة كورونا وفق ما أشار إليه (الهندي، 2020) مدير وحدة الجرائم الإلكترونيّة في المقابلة التي تمت معه يوم الثلاثاء بتاريخ (2020/10/20).

- **الحقد والكراهيّة:** يرى (الرواشدة، 2020م) أن توفر الرغبة بالانتقام يُعَدُّ دافعًا مؤثرًا في ارتكاب الجريمة الإلكترونيّة، فالتأثير السلبي للعلاقات الاجتماعية السابقة أو المنافسة أو العمل أو أي قطاع آخر يولِّد مشاعر الحقد والغضب الداخلية لدى الفرد ضد شخص ما أو مؤسسة، هذا بدوره يؤدي إلى ظهور أنماط إجرامية مستحدثة، فهذه المشاعر المكبوتة لدى الفرد تظهر على شكل سلوكات منحرفة تُرْتَكبُ في الفضاء الإلكتروني، إن ارتكاب الجاني للجرائم الإلكترونيّة بعدم قدرته على تحقيق أهدافه المرجوة وفق القوانين المقبولة والمتعارف عليها في المجتمع تتسبب في تراكم مشاعره المكبوتة داخليًّا تلك المشاعر تُولد لديه الرغبة للجوء إلى سلوكات يشكل قيامه بها إنحرافًا عن مسار المجتمع، فمثلًا تعرض الفرد للبطالة بشكل مفاجئ نتيجة فرض الحجر الصحي بعد أن كان على رأس عمله يجعله يلجأ إلى الجريمة الإلكترونيّة؛ للحصول على المال، أو بهدف إحداث خلل في توازن المجتمع بدافع الحقد والكراهية، تحديدًا في حال تعرضه لضغوطات ومتطلبات الحياة التي لا يقدر على تحقيقها.

6.3.2 خصائص الجريمة الإلكترونيّة:

تقوم الجرائم الإلكترونيّة على تِقْنيّاتٍ وأساليبَ حديثةٍ غيْرِ الجرائم التقليديّة المُتعارف عليها، فهي تتسم بمجموعة من الخصائص التي تميزها عن غيرها من الجرائم الأخرى، أهمّها ما يأتي:

- **عابرة للحدود والدول:** نظراً للانفتاح على العالم من خلال التكنولوجيا وشبكات الإنترنت أدَّتْ إلى الحد من إمكانية التحكم والسيطرة على مستخدميها، وأتاحت الفرص أمام المجرمين الإلكترونيين من ارتكاب الجرائم في الفضاء الإلكتروني؛ كون هذا النوع من الجرائم لا يقتصر ارتكابه داخل حدود دولة واحدة يوجد فيها كلا الطرفين في مكان معين، إنما تعداه ليتم ارتكابه في مختلف البلدان، فأصبحت الجريمة ترتكب في مكان والمجني عليه في مكان آخر (أي أن الجاني في الفضاء الإلكتروني باستطاعته ارتكاب جريمته في أثناء وجوده في دولة، وحدوثها في دولة أخرى)، هذا ما أكسبها طابع التنقل بين الحدود الدوليّة، خاصة أن الحدود في سماء العالم الرقمي غير مرسومة وغير واضحة (الهاشمي، 2019م)، فالجريمة الإلكترونيّة لا تتسم

بالطابع المحلي، إنما تتنقل بين الحدود والبلدان بكل سهولة، بخلاف الجريمة التقليديّة التي يلزم اكتمالها توافر الجاني والمجني عليه في المكان نفسه، فاليوم مع التطورات الهائلة التي تشهدها المجتمعات أصبحنا نعيش في عالم افتراضي يستطيع البشر على إثرها الاتصال والتواصل فيما بينهم أينما تواجدوا؛ ما أكسب هذه الجريمة التي أضحت من أخطر الجرائم التي تواجه العصر الحالي السهولة في ارتكابها أينما تواجد الجاني (مدين، 2020).

- **صعوبة إثباتها واكتشافها:** الإنسان كائن بشري ذكي دائمًا يسعى إلى اكتشاف الثغرات والحلول؛ للوصول إلى هدفه المطلوب، هذا ما يجعل من اكتشاف الجرائم الإلكترونيّة معضلة تواجه الدول؛ لأنَّ المجرم الإلكتروني يستخدمها بطريقة ذكيّة وفنيّة، ويسعى في أثناء ارتكاب جريمته عدم ترك أي أثر أو دليل على ارتكابه للجريمة فهو يرتكبها من عدة أماكن، ومن أجهزة إلكترونيّة غير شخصيّة، وبمختلف التقنيات المتطورة والحديثة التي تُسَهِّل عليه محو الدليل الذي يثبت إدانته (محمد، 2016م)، كما أن الجريمة الإلكترونيّة –بطبيعتها– غير مرئيّة، ويستطيع الجاني ارتكابها في أماكنَ مُغْلَقَةٍ بمعزل عن الآخرين يصعب الوصول إليها؛ ما يعني تمكن الجاني من إخفاء أي دليل ملموس خلفه؛ كونها تحصل داخل بيئة مكونة من البيانات، مثل قيام المجرم باستخدام جهاز حاسوب عام أو جهاز حاسوب لشخص آخر، وهذا ما يزيدها صعوبة اكتشافها خاصة أنها تتسم من الجرائم الناعمة التي لا تتطلب العنف والضرب واستخدام القوة الجسدية (لطفي، 2019م).
- **السرعة الهائلة في تنفيذ الجريمة الإلكترونيّة:** من ضمن الخصائص التي تتسم بها الجريمة الإلكترونيّة أنها تتم بِفِعْلِ أشخاص غير عاديين، لديهم الخبرة والمهارة في التعامل مع التكنولوجيا تمكنهم من ارتكابها بسرعة وسلاسة، وبطبيعة الحال الجريمة الإلكترونيّة تختلف عن الجريمة التقليديّة المتعارف عليها، لذا من الطبيعي أن نجد الاختلاف في فئات المجرمين، فهذا النوع من الجرائم يحتاج إلى الإلمام والاطِّلاع على تفاصيل وحيثيات التكنولوجيا الحديثة كافَّةً، ومختلف الثغرات من أجل استغلالها (مدين، 2020م).

7.3.2 أنواع الجرائم الإلكترونيّة في العالم بشكل عام وفلسطين بشكل خاص:

تصنف الجرائم الإلكترونيّة عامّةً ضمن مجموعة من الأنواع، لعل أهمها كما أشار (نصار، 2017) ما يأتي:

- الجرائم الماديّة منها (السطو على المصارف والبنوك، التجسس بأنواعه كافّة، التزوير).
- الجرائم الاقتصاديّة منها (النصب، الاحتيال، الرشوة، الابتزاز، التهديد).
- جرائم ضد الأشخاص منها (التشهير، الذم، القدح، الاستغلال الجنسي، سرقة المعلومات الشخصيّة، انتحال الشخصيّة).

بينما أشارت الدراسة التي أجراها كل من براشاك وآخرون (Prakash & Others, 2019) إلى أن أنواع الجرائم الإلكترونيّة تكمن في:

- جرائم النصب والسرقة الإلكترونيّة.
- جرائم القرصنة والاختراقات.
- الاحتيال.
- الاستغلال الجنسي.
- الجرائم المُرتكبة عَبْرَ الاختراقات والهكرز.

في حين أن أنواع الجرائم الإلكترونيّة المنتشرة في فلسطين، كما أشار إليها (جهاز الشرطة الفلسطينية، 2020) تتمثل في:

- الاحتيال.
- الاستغلال والابتزاز الإلكتروني.
- التهديد والقدح والذم والتشهير عبر مواقع التواصل الاجتماعي.
- إفساد الرابطة الزوجيّة من خلال مواقع التواصل الاجتماعي المختلفة مثل (الفيسبوك والتويتر والواتساب).

8.3.2 دور الذكاء الاصطناعي في مواجهة الجريمة الإلكترونيّة:

تُشير الأبحاث والدِّراسات التي تتعلق بتطبيق برامج الذكاء الاصطناعي في مواجهة الجرائم التي تَحدُث في الفضاء الإلكتروني ومواقع التواصل الاجتماعي التي باتت تشهد اكتظاظًا بالسكان، أنَّ السُّلطات والشركات والمؤسسات بدأت تعمل على صياغة خارطة عمل واضحة المعالم؛ للعمل من خلالها على تعزيز خدمات الذكاء الاصطناعي والاستفادة منها في مجال الجرائم الإلكترونيّة؛ لتسهل عملية اكتشاف مرتكبها، فنحن نرى في الآونة الأخيرة أن لهذه البرامج أدوارًا بالغة الأهميّة في اكتشاف الجريمة والتعرف إلى مرتكبيها بالصوت والصورة، بل وببصمة العين والصوت التي تفشل معها كل محاولات المجرمين المتصيدين في خداع الحاسب الآلي وشبكات الإنترنت في حال استخدمها، كما لها دور في التنبؤ بالجرائم. (محمد، 2016م).

إن ما يؤكد على ذلك دراسة (لخضر ونفيسة، 2018م) بعنوان "دور الذكاء الاصطناعي في مواجهة الجريمة الإلكترونيّة"، إنَّ هذه النظم الحديثة تعود بالفائدة للإنسان في مختلف المجالات الحياتيّة، بالإضافة إلى توفير الأمن والراحة النفسيّة للإنسان من خلال تعزيزها للرقابة والحمايّة الإلكترونيّة على المواقع والشبكات الإلكترونيّة واكتشاف عمليات القرصنة والتهكير التي يقوم بها المحترفون

والمتصيدون على الشبكات الإلكترونيّة، فضلًا عن قدرتها على التنبؤ بالهجمات الإلكترونيّة من خلال تحليل المعطيات الموجودة في الموقع، وتقييم الموقف حول ما إذا كانت تُشَكِّلُ خطرًا، وإتخاذ القرار المناسب لصد أي اختراق.

ففي مجال مواجهة الجرائم الإلكترونيّة أثبتت النظم الحديثة فاعليتها من خلال ما قدمه بعض العلماء من دراسات وأبحاث في التصدي للجرائم الإلكترونيّة، كما على النحو الآتي:

- إقتَرح شو وآخرون (Xu & Others, 2020) نظام يسمى بـ(MNTD) "هو نظام يتكون من خطوط أنابيب وظيفتها الكشف عن أحصنة طروادة"، يتم تدريب النظام على التنبؤ بأي هجمات إلكترونيّة تقوم بها هذه الأحصنة، ذلك بأخذ عينات عشوائية من أحصنة طروادة ومن ثم تطويرها بطريقة تمكنها من تصنيف الهجمات الإلكترونيّة التي تتعرض لها الشبكة الإلكترونيّة، بناءً على ما تقدم تم تجربة النظام فقد كانت نِسبة كَشف النظام للهجمات الإلكترونيّة (97%)، وعليه أثبت فاعليته بالإضافة إلى تفوقه على الأنظمة الإلكترونيّة الموجودة حاليا كافة.
- أما بهاسكير (Bhasker, 2015) قَدم نظام يُعرف بـ(LDA) يقوم على أساس الـ(Gibbs) "هو عبارة عن نظام يقوم بِتَصنيف البيانات التي يتم جمعها ومن ثم تحليلها إلى نتائج عاليّة الدقة"، حيث يعمل على أخذ عينات عشوائيّة في أثناء التجول المستمر داخل الشبكة ومن ثم تحليل ما إذا كان هناك مسلكيات منحرفة وغير طبيعيّة تحصل داخل الشبكة.
- في حين اقترح رنا وضاهر وجاغدل (Rana & Dhar & Jagdale, 2014) نظامًا خبيرًا يعمل على حِساب دَرجة الخطر (أي التنبؤ) في أثناء عمل المُستخدم داخل شبكة الإنترنت، لديه القدرة على التعرف على سلوك المستخدم المعتاد وأي تغير في سلوكه داخل الشبكة سيؤدي إلى ارتفاع درجة الخطورة في النظام، وعندما يتجاوز الدرجة المحددة مسبقاً داخل النظام يبدأ بإرسال إشارات إنذار بوجود مسلكيات مشبوهة تحصل داخل الشبكة.
- في حين عمل كل من رايت وآخرون (Wright & Others, 2011) على وضع نظام مبني على خوارزميات الاستشعار الإلكتروني لزيادة الأمان داخل الشبكة لتتمكن من الكشف السريع عن الهجمات التي تتعرض لها، إذ يعمل هذا النظام على بناء نموذج قاعدة ضبابية للشبكة من خلال تصميم خوارزمية للكشف عن أي مسلكيات منحرفة وتصنيف الهجمات الإلكترونيّة، حيث تمّ تجربته على (11) مجموعة مع (200000) من الحزم ذات السلوك الشاذ، كانت نِسبة الإنذرات الصحيحة (99.36%) ونِسبة الإنذارات الخاطئة (0.9%)، وعليه أثبت النظام فاعليته في التَصدي للهجمات الإلكترونيّة.

4.2 وزارة الإتصالات وتكنولوجيا المعلومات:

تُعَدُّ وزارة الاتِّصالات وتكنولوجيا المعلومات من أهم الوزارات التي تسعى لتقديم الخدمات التكنولوجيّة في المجتمع الفلسطيني، فهي الجسم المسؤول عن استخدام التكنولوجيا الحديثة ومواكبتها وإدارتها بشكل سليم؛ للارتقاء بالمجتمع، كما أنها تُعَدُّ المسؤولة عن مختلف التشريعات والقوانين والخطط وعن تقديم آخر التطورات لتنميّة الحكومة الإلكترونيّة وتفعيل الشراكة مع مختلف القطاعات الأخرى (وزارة الاتصالات وتكنولوجيا المعلومات، 2021م).

ولمّا كانت التكنولوجيا –في مختلف دول العالم– تشهد كثيرًا من التطورات في شتى مجالات الحياة كان لا بد من أن تعمل فلسطين جاهدة كي تواكب متطلبات العصر الحالي، وهذا يقع على عاتق وزارة الاتّصالات وتكنولوجيا المعلومات التي تعمل على الارتقاء بمستوى التكنولوجيا وعدم الوقوف على الطرق القديمة، إنما تطوير نظم تكنولوجية في فلسطين يمكنها من اللحاق بسلسلة التطورات التي يشهدها العالم اليوم؛ كي تتماشى مع التطورات كافةً التي تخوضها دول العالم، تقدم الوزارة خدماتها في ثلاثة قطاعات رئيسة حسب ما أشارت اليها (مديرة مكتب وزير الاتصالات وتكنولوجيا المعلومات، 2021م) من خلال المقابلة التي أجريت معها يوم الإثنين الموافق (2021\09\13)، تتمثل تلك القطاعات في:

- **قطاع البريد:** يمنح أذونات وتصاريح لأكثر من (12) بريدًا تابعًا للقطاع الخاص تمنح له هذه الأذونات الحق في التنقل بحريّة بين الدول.
- **قطاع تكنولوجيا المعلومات:** يمنح خدمات إلكترونيّة حديثة ومطورة لأكثر من (28) مؤسسة محلية.
- **قطاع الاتصالات:** منح (94) موافقة ترددية وخطوط نفاذ لاستخدامها فهو الجهة الرسميّة المُخوَّلة والمتخصصة بمنح التصاريح بما يتعلق في جانب التكنولوجيا.

1.4.2 رؤية وزارة الاتصالات وتكنولوجيا المعلومات:

ذَكرت (وزارة الاتصالات وتكنولوجيا المعلومات، 2017) أن رؤية الوزراة هي الارتقاء بمجتمع فلسطيني لديه القدرة على التقدم والتطور في شتى مجالات الحياة، تسعى للاستفادة من كلّ الإنجازات التكنولوجيّة التي حققتها حديثًا؛ كي تقوم بتطبيقها على أرض الواقع والاستفادة من نتائجها.

2.4.2 الأهداف الإستراتيجيّة لوزارة الإتصالات وتكنولوجيا المعلومات:

أشارت (الخطة الإستراتيجيّة للوزارة، 2017م) إلى مجموعة من الأهداف للقطاعات الثلاث في الوزارة تتمثل في:

- تعزيز العمل على تطوير البنيّة التحتيّة للحصول على بنيّة حديثة ذات جودة عآليّة، لديها القدرة على استكمال المتطلبات المطلوبة منها كافة، دون أي عراقيل وتطوير قطاع تكنولوجيا المعلومات.
- تأمين استخدام المواطنين لشبكات الإنترنت والاتصالات والاستفادة من مختلف الخدمات المُقدمة وتعزيز جودتها بأعلى المستويات.
- توظيف التكنولوجيا الحديثة؛ لتمكين فئات المجتمع كافَّةً من استخدامها بشكل آمن وفعال ويخدم مصالح المجتمع.
- العمل على تقويّة إمكانات العاملين في قطاع البريد وتكثيف الدورات التدريبيّة بمختلف أشكالها وتعزيز التوعية واستخدام البريد بأعلى مستوياته.
- تعزيز الاستخدام الآمن للتكنولوجيا؛ للحصول على تصفح آمن للمواطنين يحميهم من الوقوع ضحايا للمتصيدين.
- التشبيك بين الوزارة والجمهور لنشر الوعي ونشر الدورات التدريبيّة؛ للحصول على أجيال قادرة على التعامل مع التكنولوجيا الحديثة والمؤسسات الدوليّة للاطلاع على آخر تحديثات التكنولوجيا التي وصل إليها العالم للبقاء على اطِّلاع ودراية بها.

3.4.2 واقع قطاع الاتِّصالات وتكنولوجيا المعلومات في فلسطين:

إنَّ فَرْضَ سلطات الاحتلال الإسرائيلي كثيرًا من القيود على المجتمع الفلسطيني تُسْهِم بدرجة كبيرة في عرقلة تطور الوزارة في شتى مجالات عملها وتقديمها للخدمات في المجتمع، حيث إنَّ لفلسطين في هذا المجال خصوصيّة تختلف عن باقي الدول؛ إذ كانت ولا تزال مقيدة وإمكاناتها محدودة مقارنة مع دول العالم؛ لأنَّ الاحتلالَ الإسرائيليّ يمارسُ العديد من السياسات التي من شأنها أن تعرقل قدرة الوزارة على التنميّة وتطوير قدراتها وإمكاناتها، بالإضافة إلى حجز الأجهزة والمعدات، كل هذا يُشكل جزءًا من الواقع الذي يعيشه المجتمع الفلسطيني (وزارة الاتصالات وتكنولوجيا المعلومات، 2016م).

ولأهميّة هذا القطاع في مختلف دول العالم تولي الوزارة كثيرًا من الاهتمام به في سبيل التقدم وزيادة الخدمات المقدمة للمجتمع، حيث تسعى الوزارة إلى تقديم أفضل خدمات الرفاهيّة والتعليم والاستخدام الآمن لشبكات الإنترنت ومختلف الخدمات؛ كونها تُشكل المنفذ الوحيد للاطِّلاع على العالم الخارجي،

فهي تعمل جاهدة على اللَّحاق بعجلة التقدم والتطور التي قفز لها العالم في خطوات استباقية (وزارة الاتصالات وتكنولوجيا المعلومات،2017م).

لكن بالرغم من ضعف الإمكانات التي تعاني منها وزارة الاتصالات وتكنولوجيا المعلومات فإنها تؤدّي دورًا مهمًّا ورئيسًا في مواكبة التطور واستحداث برامج الذكاء الاصطناعي؛ للاستفادة منها فهي تعمل على تقديم الخدمات التكنولوجيّة الحديثة للمجتمع الفلسطيني، تأكيدًا على ذلك ما ذكرته (صحيفة وفا، 2021م) على موقعها الرسمي بتاريخ (09\06\2021م) أن الوزارة وقعت على اتفاقية مع شركة بيربوس لاستخدام أدوات الذكاء الاصطناعي وبرامجه المختلفة سعيًا منها للتطور في مجال النظم الذكيّة والارتقاء بمستوى التكنولوجيا المقدمة للمواطن، واستثمارها بأفضل شكل في فلسطين، وتوضيحًا لذلك فقد أكدت الوزارة من خلال الاحتفال باليوم العالمي لوزارة الاتّصالات وتكنولوجيا المعلومات بتاريخ (17\05\2021م) على ضرورة الاستثمار والعمل في مجال استخدام برامج الذكاء الاصطناعي في مختلف المجالات خاصة في قطاع التعليم، وذكرت (صحيفة معًا، 2021م) على موقعها الرسمي بتاريخ (06\10\2021م) أن الوزارة قامت بتنظيم ورشة عمل بعنوان "التكنولوجيا والذكاء الاصطناعي" تأكيدًا منها على سعيها بالنهوض بالمجتمع الفلسطيني والانتقال إلى الحكومة الرقميّة لتقديم أفضل الخدمات للمجتمع الفلسطيني، وذكرت أيضًا (وزارة الاتصالات وتكنولوجيا المعلومات، 2021م) من خلال موقعها الرسمي بتاريخ (03\04\2021م) أنها قامت بتنظيم مشروع يسمى بمليون طفل فلسطيني مبرمج؛ حتى تتمكن من نشر الذكاء الاصطناعي، وتعلم التقنيات الحديثة التي أصبحت تشكل أساس ارتقاء المجتمعات وتعليمهم على البرمجة؛ لإنتاج مبرمجين قادرين على فهم هذه البرامج الذكيّة وإدارتها بطريقة ذكية واستثمارها في سبيل الوطن، إضافة إلى أنها تمنحهم القدرة على مواجهة المشكلات التي من المحتمل أن يتعرضوا لها على الشبكة الإلكترونيّة، خاصة في ظل تطوير الهاكرز لقدراتهم في اختراق الثغرات الأمنيّة، كل ذلك من شأنه أن يعمل على حمايته من الوقوع فريسة للمجرمين الإلكترونيين ومواكبة مجريات التطور التي يعيشها العالم.

إضافة لما سبق ذكرت (صحيفة فلسطين، 2021م) بتاريخ (05\03\2021م) من خلال الورشة التي عقدتها وزارة الاتصالات وتكنولوجيا المعلومات على أهمية تهيئة البنيّة التحتيّة في فلسطين؛ كي تتمكن من استيعاب الكم الهائل من البيانات الضخمة الخاصة بتقنيات الذكاء الاصطناعي وبرامجه، ومِنْ ثَمَّ التكيُّف معها بناءً على قواعد المعرفة المتمثلة بمخزن المعلومات، كما ذكرت الوزارة على موقعها الرسمي في تاريخ (04\03\2021م) أنها عقدت ورشة عمل حول دور تقنيات الذّكاء الاصطناعي في تحسين الخدمات الحكوميّة، والعمل على تطوير قواعد البيانات ورفع مستواها في العمل؛ حتى تتمكن من استيعاب التنوع في تطبيقات الذكاء الاصطناعي، سعيًا منها للارتقاء بمستوى العمل الحكومي وتَسهيل حياة المواطن الفلسطيني.

5.2 النظريات المفسرة لممارسة الجرائم الإلكترونيّة:

هناك العديد من النظريات التي فسرت ممارسة الجرائم الإلكترونيّة، لعل من أهمّها ما يأتي:

- **نظريّة النشاط الرتيب:** نشأت هذه النظريّة في نهاية سبعينيات القرن الماضي عام (1979م)، ومن أهم روادها (كوهن – فيلسون)، وتقوم هذه النظريّة على وجود ثلاثة عناصر رئيسية لحدوث الجريمة هي:
  - الهدف (المجني عليه).
  - الرغبة (المجرم الراغب) (الجاني).
  - غياب الرقابة والحراسة (غياب القوانين.

حيث إنه ونتيجة التغيرات التي حصلت بعد الحرب العالميّة الثانية ظهر العديد من الأنماط الجديدة والنشاط الروتيني لحياة الفرد في المجتمع؛ ما أدى إلى الزيادة في معدل الجريمة فقامت هذه النظريّة بتفسير الجريمة وسبل الوقاية منها كلّاً متكاملًا فهي لم تَسْعَ لتفسير أسباب الميل الإجرامي لدى الأفراد باعتبار أنه موجود عند البعض من عامة الناس (الوريكات، 2013م).

وبتطبيق هذه النظريّة على الجرائم الإلكترونيّة نجد أن جميع هذه الجرائم تحدث في أماكن مغلفة ومنعزلة؛ ما يعني أن هذه الأماكن تكون خاليّة تمامًا من الرقابة والحراسة، ففي ظل غياب الرقابة والاعتقاد المُتشكل لدى الجاني أن الجريمة الإلكترونيّة يمكن أن يرتكبها في الخفاء، وفي أماكن منعزلة يتشكل لديه عوامل جذب لارتكاب هذا النوع من الجرائم مع توافر الضحية الضعيفة التي يستهدفها المجرمون لوجود تصور مُسَبَّق لديهم بأن الرقابة والحمايّة ضعفية، خاصة في ظل الانفتاح على العالم والتغير في أنماط الحياة الروتينية لدى الأفراد؛ ما يؤدي إلى تكامل العناصر الثلاثة الأساسيّة التي تقوم عليها نظريّة النشاط الرتيب كما تمّ الإشارة لها أعلاه.

مما سبق نستنتج أن حدوث الجريمة الإلكترونيّة وفق هذه النظريّة ما هو إلا نتاج تصور ونوع من عدم الاكتراث والاستهتار لدى المجرم فعندما ينغرس في ذهنه عدم توافر رقابة أمنية في الفضاء الإلكتروني بالإضافة إلى ضعفها في الواقع؛ بسبب التضييق من الجانب الإسرائيلي على الجهات المنفذة للقانون، ومنعهم من الوصول إلى مفتعلها في كلا الجانبين، هذا يدفعه إلى القيام باستغلال الثغرات الأمنيّة، فالجاني العالِمُ بالثغرات التي يمكن اختراق الأنظمة من خلالها وإخفاء الأدلة وكلّ تحركاته على الشبكة لعلمه أن الحماية على هذه الشبكات ضعيفة والتطبيقات الحديثة والذكيّة غير مفعلة لتقوم بتسجيل تحركاته وصد هجماته الإلكترونيّة، يتمادى في ممارسة الجريمة الإلكترونيّة؛ ما يؤدي إلى وقوع مزيد من الجرائم المرتكبة في

الفضاء الإلكتروني، ومن أجل الحد من ممارستها ومنعها في سبيل حماية مستخدمي شبكات الإنترنت من الوقوع فريسة للجناة ينبغي العمل على مواجهة العراقيل التي تقف عائقًا أمام تطبيق الذكاء الاصطناعي وأهمية العمل على تعزيز الرقابة والحماية من أجل تقليل الفرص أمام المجرمين من ممارسة الجريمة الإلكترونيّة.

- **نظريّة الفرصة والاختيار العقلاني:** نشأت نظريّة الفرصة عام (1959م) على يد العالمين (كلوارد واوهلن)، فقد افترضا أن الأشخاص يرغبون بتحقيق أهدافهم بالطرق المتاحة والمشروعة في مجتمعهم لكنهم في المقابل يواجهون عقبات شديدة أمام تحقيق أهدافهم المرجوة، وعندما لا تتوافر لديهم فرص للاقتراب من التقدم إلى الأمام فإنها تقودهم إلى الإحباط واليأس، فالفرص التي تتوافر لدى بعض الجماعات من خلال اتِّباع الأساليب غير المشروعة تدفعهم للجوء إليها في سبيل تحقيق هذه الأهداف (الزعبي، 2011).

ولمّا كانت هذه النظريّة ترتكز في منطلقاتها على أن الجاني يستغل الفرص لارتكاب الجريمة الإلكترونيّة يمكن القول إنَّ طبيعة الحياة في الوقت الحاضر القائمة على التكنولوجيا الحديثة أسهمت في توفير الفرص أمام المجرمين لارتكاب الجرائم الإلكترونيّة التي سببها العديد من المعوقات، فالفرصة تؤدّي دورًا كبيرًا في حدوث الفعل الإجرامي في الفضاء الإلكتروني، إن افتقار المواقع الإلكترونيّة للحمايّة الأمنيّة وضعف الرقابة تدفع الجناة وتعزز لديهم الرغبة في استغلال الثغرات، إن ما سبق يُشكل للجاني فُرَصًا سريعة للحصول على المنفعة بالطرق غير المشروعة، إنَّ زيادة نسبة الجرائم الإلكترونيّة في فلسطين خاصة في فترة إنتشار جائحة فايروس كورونا كان بسبب أن هذه الجائحة دفعت العالم الى استخدام خدمات الإنترنت في مجالات الحياة المختلفة بشكل أكبر مما كانت عليه في السابق.

فالحياة اليوم وفي ظل انتشار هذا الفايروس فُرض عليها الاعتماد وبشكل كبير على استخدام الإنترنت والبرامج ذات العلاقة به التي تستخدم بطريقة لا تتمتع بالرقابة المطلوبة من قبل الأهل ومؤسسات التنشئة الاجتماعيّة، فعدم وجود رقابة على شبكة الإنترنت والشعور باليأس والإحباط لدى المواطنين بسبب سياسة الإغلاق ومنع التجمعات تدفع الفرد إلى الخروج عن قواعد المجتمع المشروعة، فهو من خلالها قد يجد فيها فرصًا مناسبة في سبيل تحقيقه لأهدافه وغاياته التي قد تكون في البداية الهدف منها التسلية، لكن فيما بعد قد تتحول لممارسات إجراميّة، فالعقبات والضغوط العامة التي توضع أمام الأشخاص التي تعرقل تحقيقهم لأهدافهم ضمن الأطر المتاحة في المجتمع هي التي تُشَكِّلُ فرصًا لارتكاب الجرائم الإلكترونيّة تحديدًا في ظل انتشار الفايروسات المختلفة التي تشل الحياة كما نتج عن انتشار الفايروس اللعين (كوفيد-19)، إن ما يؤكد ذلك ارتفاع نسبة الجريمة في فلسطين خلال انتشار هذا الفايروس، تحديداً جرائم القتل التي لم تصل نسبتها في السنوات السابقة كما وصلت له عام (2020م)

فحسب إحصاءات (جهاز الشرطة الفلسطينية، 2021م) ارتفعت نسبة جرائم القتل ما يقارب (42%) في حين ازدادت خلال عام (2021م) لتصل نسبتها (69%).

مما سبق يتضح لنا أنه وبتطبيق هذه النظريّة على الجرائم الإلكترونيّة والذكاء الاصطناعي نجد أن الفرد الجاني المتصيد للفرص يلجأ إلى طرائق غير مشروعة للحصول على أهدافه، خاصة بعد تغلغل الطرائق الحديثة ووجود ثغرات في حماية العالم الالكتروني، فكلما كان هناك تحديات تواجه تطبيق نظم الذكاء الاصطناعي الحديثة زادت فرصة اغتنام الجاني للفرص في اللجوء لارتكاب الجرائم الإلكترونيّة في العالم الرقمي، بمعنى آخر هذه التحديات تُعد بمثابة حافز لدى الجاني لارتكاب المزيد من الجرائم الإلكترونيّة.

أما نظرية الإختيار العقلاني نشأت هذه النظريّة عام (1987م) من أهم روادها (رون كلاريك وكورينش)، تعتمد هذه النظريّة على المبادئ الأساسيّة لعلم الإجرام الكلاسيكي التي تنص على أن الناس يختارون بحرية سلوكهم، يرى منظور الاختيار العقلاني أن الجرائم هي نتيجة للخيارات العقلانيّة والمعتمدة على تحليل التكلفة والمنفعة وهكذا يقرر الأفراد أو تجدهم يقومون بارتكاب الجريمة من أجل المنفعة أو توسيع تلك المنافع والإقلال من التكاليف (وريكات، 2004).

ولمّا كانت نظريّة الاختيار العقلاني تقوم على أساس أن الجاني يرتكب الجريمة الإلكترونيّة بدافع الحصول على المنفعة والفائدة واستغلاله للفرص في ظل غياب الرقابة والحراسة، فإننا نستنتج من ذلك أنه بغياب الرقابة الأمنيّة وإمكانية ارتكاب هذه الجرائم في فترات زمنيّة مختلفة، يغتنم الجاني الفرصة على أساس المنفعة واللذة التي يحصل عليها بصورها المختلفة من ابتزاز أو سرقة بطاقات، أو بريد الكتروني، أو احتيال، وأي شكل من هذه الأشكال، أو حتى رغبة منه بالانتقام بدافع المتعة، وعليه نجد أنه كلما كانت الرقابة والحراسة ضعيفة أو معدومة في الفضاء الالكتروني مع المنفعة العائدة كانت نسبة الجريمة الإلكترونيّة في ازدياد.

إن ما سبق يوضح لنا أن هناك تقاطعًا ما بين نظريّة الفرصة ونظريّة الإختيار العقلاني ونظريّة النشاط الرتيب، هذا التقاطع يتمثل في محاولة تفسير إقبال الجناة بارتكاب الجريمة الإلكترونيّة، فالجاني يتّخذ القرار المناسب بناءً على الفرصة في ظل غياب الرقابة الأمنية والحراسة الضعيفة، فعندما تكون المواقع الإلكترونيّة غير محصنة فهي تسهم في انتشار الجرائم في الفضاء الإلكتروني.

- **نظريّة الضغوط العامة:** نشأت هذه النظريّة في منتصف الثمانينات على يد العالم (روبرت أجنيو)، ركز في نظريته على أن الظروف المحيطة بالفرد تؤدّي دورًا مهمًّا في مسلكياته، فهو يعدُّ أن تحمل الفرد لانسداد الفرص في تحقيقه لطموحاته وعدم قدرته على الحصول عليها تُشكل الفكرة الأساسية لانبثاق الضغوط لدى الفرد، فكل ما يتحمله الفرد من ظروف صعبة

ومحبطة وغير مشجعة تُشكل أساس هذه النظريّة، إضافة إلى أن تراكم الكبت والضغوط لدى الفرد تولد لديه فكرةً بأن المجتمع بأكمله ضده وأنه يستطيع تحقيق طموحاته بطرق غير مشروعة وأن المجتمع هو السبب في عدم حصوله عليها، هذا ما يؤدي الى ارتكابه مسلكيات منحرفة نتيجة عدم قدرته على تحمل هذه التراكمات (البداينة والخريشا، 2013م).

يتضح لنا مما سبق أنه وبحسب نظريّة الضغوط العامة وعلاقتها بالجرائم الإلكترونيّة والذكاء الاصطناعي أنَّ الفرد عندما يفتقر لكل ما يُشبع حاجاته ورغباته وطموحاته في المجتمع وتُغلق الأبواب في وجهه فإنه يلجأ إلى العالم الرقمي الذي يجد فيه مكانًا غير محصن بالحماية الكافية، ويعلم بالضعف في تطبيق التقنيات الذكيّة الحديثة التي من شأنها أن تؤمِّن الحراسة والحماية لمستخدمي أنظمة الحاسوب، فهو يجد فيها أسلوبًا ونمطًا مغريًا لتحقيق طموحاته خاصة في ظل ظروف انتشار فايروس كورونا واستمرار استكمال مناحي الحياة في الفضاء الإلكتروني، وفرض حظر التجول فإنه لا يجد أمامه إلّا العالم الرقمي وسيلةً لاشباع الحاجات العامة التي تعرض لها في حياته بسبب الضغوطات العامة.

إن ما سبق يوضح لنا أن هناك تقاطعًا بين كل من نظريّة الضغوط العامة ونظريّة النشاط الرتيب ونظريّة الفرصة، هذا التقاطع يتمثل في محاولة تفسير العلاقة بين الضغوط التي تدفع بالفرد للجوء إلى ارتكاب الجرائم في العالم الإلكتروني وضعف الرقابة الأمنية على المواقع والشبكات الإلكترونيّة التي يُشكل ضعفها ثغرات مغريّة للجناة، وعليه يرى المجتمع الفلسطيني ولخصوصيته أنه من الدول المُتَضررة؛ بِسبب ما يعاني الأفراد من ضغوطات محيطة به في جميع مناحي مثل انتشار جائحة كورونا التي أدت إلى زيادة الفقر والبطالة إضافة الى قلة الأنشطة الحياتيّة، والإحتلال الإسرائيلي الذي يساعد في دعم الجرائم الإلكترونيّة من خلال التضيق على الجهات المُختصة في الحصول على الأجهزة والمُعدات كل هذه العوامل مُجتمعة في هذه النظريات الثلاث تشكل عاملًا رئيسًا في ارتكاب الجرائم الإلكترونيّة.

- **النظريّة اللامعياريّة (الأنومي):** نشأت هذه النظريّة على يد العالم (إميل دوركايم) الذي افترض أنَّ سلوك أفراد المجتمع ما هو إلّا نتاج انعدام القدرة على تحقيق الغايات والأهداف، بناءً على ما هو متعارف عليه في المنظومة الاجتماعية، بالتالي تؤدي الى اختلال النظام والتوزان في المجتمع، وتدفع بالفرد إلى اللجوء لتحقيق ذلك بطرائق غير مشروعة، حيث إنَّ هذه الضغوطات الاجتماعيَّة ولَّدَتْ لديه حالة من الاضطراب تدفع به لارتكاب الجريمة، فهذه المسلكيات تُعَبِّرُ عن هدف معين في وقت لا تتوافر فيه الوسائل الشرعية لبلوغ هدفه المحدد (أبو عليان،2016م)، هذا ما يمكن ربطه مع نظريّة الفرصة التي تدفع الفرد لممارسة سلوكيات غير مقبولة مجتمعياً لتحقيق حاجاته وإشباعها.

يتضح لنا ممّا سبق أنه وبحسب نظريّة الأنومي فإن الفرد وشعوره بالحرمان والدونيّة والتشاؤوم وفقدان ثقته بنفسه تولد لديه صراعًا وضغوطًا وإختلالًا في التوازن في المجتمع والحياة؛ بسبب انتشار جائحة كورونا، إنَّ شعوره بالفراغ الكبير يدخله إلى عالم التكنولوجيا خاصة المواقع الإلكترونيّة التي تحتوي على المغريات التي لا يستطيع الحصول عليها على أرض الواقع؛ بسبب البطالة المُتفشية، وانسداد فرص العمل بالإضافة إلى عدم قدرته على الانحراف الأخلاقي في المجتمع، إن ما يُعزِّز ذلك التفكير المُشوش لديه حيث يرى فيه فُرصة لإثبات ذاته فضلًا عن ضعف الرقابة الوالدية المتمثلة في التربية والتوجهات الدينية وعدم اكتراث الوالدين في المشاكل المتعلقة بأبنائهم، فهم يلجأون إلى الإنترنت رغبة منهم في التخلص من هذه المشاكل والضغوط التي يعاني منها، كما أنه من الممكن أن يقع في مستنقع الإرهاب وممارسة العنف تجاه المجتمعات والقتل والتدمير من خلال الأفكار المتطرفة التي يبثها الإرهابي في عقله نتيجة الحقد والكراهية والضغوط الداخلية التي دفعت إلى اختلال في التوازن الفكري لديه.

في هذا السياق نجد أن المجتمعات هي التي تسهم في زيادة المشكلات وتفاقمها لدى الشباب، خاصة الشباب الذين يعانون من الضغوط والمشاكل والبطالة والفقر، فالجماعات الإرهابيّة تبحث عن الأشخاص اللّامعياريين في المجتمع؛ من أجل تحريضهم لممارسة السلوك المنحرف تجاه الجماعات من خلال الوقوع فريسة لدى المنظمات الإرهابية من خلال شبكات الإنترنت خاصة أن الشبكات الإلكترونيّة تفتقر لوجود حماية ذكية تكشف هذه المسلكيات غير الطبيعيّة.

- **نظريّة الردع:** قدمت المدرسة الكلاسيكيّة نظريّة في ردع السلوك الإجرامي وتنقسم إلى جانبين هما الردع الخاص والردع العام، حيث إنَّ الردع الخاص يتمثل في إنزال العقوبة بالجاني، والردع العام يتمثل في تطبيق العقوبة بالجاني؛ حتى يرتدع الآخرون من ذلك، إن الهدف من ذلك أن يكون الشخص –فيما بعد– قادرًا على اختيار مسلكياته في المجتمع بحرية مع الأخذ بعين الاعتبار الألم والعقاب والحبس (البداينة والخريشا، 2013م).

يتضح مما سبق أن الفرد يبعتد عن ارتكاب الجرائم الإلكترونيّة عند شعوره بالألم والعقاب، خاصة إذا تمّ تفعيل تطبيقات الذكاء الاصطناعي التي من شأنها أن تقوم بالكشف عن الجاني؛ ما يعزز شعور الإحباط لديه عندما يعلم أن هناك عقوبة صارمة وشديدة تجرم هذا الفعل، كما يمكن تطبيق الردع العام من خلال معرفة الأشخاص الآخرين أن الجاني الذي ارتكب جريمة إلكترونيّة تمت معاقبتة معاقبة شديدة الألم، فإنها تؤدي إلى زرع شعور من الخوف والتردد من القيام بهذه المسلكيات المنحرفة.

- **نظريّة الوصم:** نشأت هذه النظريّة على يد العالم (ليمرت) الذي ركز على أهمية التفاعل بين الأفراد في المجتمع، حيث إنَّ لتأثير الظروف الاجتماعية المحيطة دورًا في ردود الأفعال الصادرة عن الفرد، إن الفرد الذي يوصم بالوصمة المجتمعيّة يشعر بالنقص والدونيّة؛ ما يعني انحرافه عن المسلكيات المشروعة والمتعارف عليها الأمر الذي يؤدي إلى ممارسة الجريمة والانحراف. (الهسنياني والمعماري، 2012م).

يتضح مما سبق أن البيئة المحيطة بالفرد هي من تعطي صفة الوصم والمسؤولة عن عودة الجاني لارتكاب المسلكيات الإجراميّة وغير المشروعة في المجتمع، فالنظرة التي يرى فيها المجتمع الجاني هي من تدفعه لارتكاب هذه المسلكيات، حيث إنَّه عندما يفتقر لفرصة العودة بوصفه فردًا صالحًا في المجتمع والالتزام بالعادات والتقاليد المتعارف عليها يؤدي ذلك إلى ردود فعل سلبية نهايتها الانحراف والانعزال عن العائلة وأفراد المجتمع فيجد في الشبكات الإلكترونيّة فرصة للانتقام من المجتمع، لاسيما أن هذه الشبكات تفتقر إلى الحماية الأمنيّة، فالشاب الذي قام بمسلك مخالف للقوانين وتمت معاقبته، وأنهى الفترة المقررة للعقوبة، وتم إصلاحه وتأهيله في مراكز الإصلاح، بعد خروجه من مراكز الإصلاح إذا رأى أن المجتمع لا يزال ينظر إليه نظرة مجرم، ولا يسمح له بالعمل في وظيفة وتكوين عائلة من خلال الارتباط والزواج، كلُّ ذلك يؤدّي دورًا مهمًّا في شعوره بالدونيّة؛ ما يشكل لديه ضغوطاتٍ نفسيَّةً، ومن ثَمَّ من الممكن أن يقرر الانعزال عن المجتمع، واللُّجوء للانتقام من خلال الشبكات الإلكترونيّة حتى لو تمّ تعديل سلوكاته، هذا ما تم الإشارة له عند الحديث عن نظريّة الضغوط العامة.

- **النظريّة التكامُليّة:** نشأت هذه النظريّة على يد العالم (إنريكي فيري)، ركز في نظريته على أن الجريمة ليست محصلة عامل واحد فقط إنما هي نتاج تفاعل مجموعة من العوامل الداخليّة (النفسيّة والبيولوجيّة) والخارجية المحيطة به (الاجتماعية) هي من تدفع الفرد لارتكاب الجريمة (أبوعفيفة، 2013م).

نستنتج مما سبق أن الدافع وراء ارتكاب الجاني للجرائم الإلكترونيّة ليس دافعًا واحدًا، إنما مجموعة من الدوافع تتشابك مع بعضها بعضًا، بمعنى أنَّ هناك علاقةً بين السلوك الداخلي الصادر عن الجاني بسبب العوامل البيولوجيّة والظروف البيئيّة المحيطة به وبين ممارسة الجريمة، حيث إنَّ شعور الفرد بالإحباط والغضب والحقد وعدم القدرة على تحقيق رغباته وأهدافه ووجود بيئة مفككة يسودها الإهمال وعدم الاحتواء من الآخرين والدولة وقلة التفاعل الاجتماعي بين أفراد الأسرة، بالإضافة إلى انسداد الفرص التي كان لها تأثيرات سلبية على الأفراد في المجتمع، كل ذلك من شأنه أن يحفز الجينات الداخليّة لدى الجاني حيث إنَّ المتحكم في ردود أفعال الإنسان وتصرفاته هي الجينات التي من الممكن أن تكون ساكنة منذ

ولادته نتيجة عدم تعرضه لمواقف حياتية، خاصة إذا كان يعاني من (متلازمة كلاينفلتر) التي تعزز لدى الجاني الانعزال والاكتئاب، وظهور مشكلات نفسيّة تؤدي إلى اختلال توازنه النفسي، والابتعاد عن العالم الخارجي واللجوء إلى الفضاء الإلكتروني؛ نتيجة عدم قدرته على الاتصال والتواصل مع العالم الخارجي، وفي ظل وجود بيئة خصبة ومهيَّأة لانحراف الجاني، كلٌّ ذلك يتفاعل مع بعضه بعضًا؛ ليدفعه للقيام بمسلكيات إجرامية خطيرة من شأنها أن تلحق الضرر والأذى بالآخرين.

6.2 الدراسات السابقة وذات الصلة:

من خلال المسح الشامل للمكتبات والدراسة المستفيضة حول الموضوع تمّ العثور على عدد قليل من الدراسات السابقة وذات الصلة العربيّة والأجنبيّة التي ترتبط بالدراسة الحاليّة، لعل من أهم الدراسات العربية دراسة (العبيدي، 2020م)، دراسة (القحطاني، 2014م)، دراسة (البشير، 2010م)، دراسة (البلوي، 2009م)، دراسة (العنزي، 2003م)، دراسة (الشهري، 2001م) المشار لها في (العمري، 2004م)، دراسة (البشري، 2000م)، أما فيما يخص الدراسات الأجنبية فقط تمّ العثور على دراسة بلال وآخرون (Bilal & Others, 2019)، دراسة ايكنيم (Ekanem, 2019)، إضافة إلى دراسة كوسترا (Koostra, 2019)، دراسة تيواري وماهيشواري وبال (Tiwari & Maheshwary & Pal, 2018)، دراسة ويليامسون (Williamson, 2014) كما على النحو الآتي:

1.6.2 الدراسات العربية:

- دراسة (العبيدي، 2020م)، بعنوان "**دول الدليل الرقمي في الإثبات الجنائي في النظام السعودي**"، هدفت الدراسة التعرف إلى دور الدليل الرقمي في الإثبات الجنائي في النظام السعودي، لقد استخدم الباحث في هذه الدراسة المنهج الوصفي من خلال الاستقراء والتحليل والمقارنة، توصلت الدراسة إلى مجموعة من النتائج، من أهمها ضرورة وجود أدلة رقمية لأهميتها في الإثبات الجنائي، ووجود الأنظمة الذكيّة التي تُستخدم لمواجهة الجرائم الإلكترونيّة مهمة في إثبات الأدلة الجنائيّة، في حين أوصت الدراسة بضرورة مواكبة الإصدارات الجديدة من التكنولوجيا في مجال مواجهة الجرائم التي تحصل في الفضاء الإلكتروني، وأهمية العمل على توفير كوادر بشرية لديها القدرة على التعامل مع الأدلة التي يتم الحصول عليها من الشبكات الإلكترونيّة وضرورة المتابعة والاستمرار في مواكبة التحديثات المتعلقة بالحصول على الأدلة الرقميّة.
- دراسة (القحطاني، 2014م)، بعنوان "**تطوير مهارات التحقيق في الجرائم المعلوماتيّة**"، هدفت الدراسة التعرف إلى المعوّقات التي تحول دون تطوير مهارات التحقيق في الجرائم الإلكترونيّة، استخدم الباحث في هذه الدراسة المنهج الوصفي، وتكوَّن مجتمع الدراسة من جميع المحققين

والعاملين في الادّعاء العام في مدينة الرياض البالغ عددهم (256)، وبلغت العينة (156) محقق وعامل في الادّعاء العام، وتوصلت الدراسة إلى مجموعة من النتائج من أهمها قلة الخبرة المتوفرة لدى المحققين لإثبات الجرائم الإلكترونيّة، بالطرائق والأساليب الحديثة والتعامل مع برامج فحص الأدلة الرقميّة التي تساعد في عملية التحقيق، في حين أوصت الدراسة بضرورة الاستفادة من التجارب والخبرات الناجحة من الدول المتقدمة، والعمل على توفير الأجهزة والبرمجيات الحديثة من أجل مكافحة الجرائم الإلكترونيّة، بالإضافة إلى القيام بدراسات مستقبليّة من أجل الحدّ من المعوقات التي تحول دون تطوير التحقيق في الجرائم المعلوماتيّة.

- دراسة (البشير، 2010م)، بعنوان "**دور الدليل الرقمي في إثبات الجرائم المعلوماتيّة**"، هدفت الدراسة التعرف إلى استخلاص الدليل الرقمي ودوره في إثبات الجرائم المعلوماتيّة، واستخدم الباحث في هذه الدراسة المنهج الوصفي، ومنهج تحليل المضمون لتحليل بعض القضايا ذات العلاقة، وقد توصلت الدراسة إلى مجموعة من النتائج من أهمها أن مسرح الجريمة المعلوماتيّة يتشكل من الحواسيب وملحقاتها والأفراد والإنترنت (الشبكة العالميّة للمعلومات)، بالإضافة إلى أن الجرائم الإلكترونيّة تحتوي على أصناف مختلفة من الجرائم متعددة الأشكال وتوصلت إلى أن الجرائم الإلكترونيّة تتسبب في انهيار القطاع الخاص بالمستثمرين، فهي تستهدف غالبًا المؤسسات الكبرى، في حين أوصت إلى ضرورة العمل على الاهتمام بتطوير الدلائل الماديّة الرقميّة وإيجاد آليّة واضحة ومخطط لها لتوظيفها في عصر التكنولوجيا الحديثة.
- دراسة (البلوي، 2009م)، بعنوان "**التقنيات الحديثة في التحقيق ودورها في ضبط الجريمة**"، هدفت الدراسة التعرف إلى الأدلة الرقميّة والتقنيات الحديثة ودورها في حماية الحساب الآلي من الجرائم، واستخدم الباحث في هذه الدراسة المنهج الوصفي (الوثائقي)، وتوصلت الدراسة إلى مجموعة من النتائج، من أهمها أن هناك تقنيات واستراتيجيات وأجهزة متطورة يمكن استخدامها في التحقيق الجنائي، مثل أجهزة التحليل باستخدام الأشعة تحت الحمراء، وأجهزة المسح الطبقي للوثائق والمستندات، في حين أوصت الدراسة بأهميّة العمل على تدريب الكوادر البشرية العاملة لديها على التقنيات الحديثة واستخدامها بأعلى كفاءة، كذلك أوصت بضرورة العمل على فتح إدارات تمكن العاملين من استخدام التقنيات الحديثة بالإضافة إلى ضرورة تكثيف الدورات وورش العمل المتعلقة بالتكنولوجيا الحديثة في ضبط الجناة، كما أوصت بضرورة جلب أحدث الأجهزة والمعدات المتطورة وتوفير مخصصات ماليّة لذلك.
- دراسة (العنزي، 2003م)، بعنوان "**وسائل التحقيق في جرائم المعلومات**"، هدفت الدراسة التعرف إلى وسائل التحقيق في الجريمة المعلوماتيّة، ووضع نظام عام لحماية نظم المعلومات، واستخدم الباحث المنهج الوصفي، من خلال أسلوب المسح الاجتماعي بالعينة،

تكونت عينة الدراسة من (141) فردًا، وتوصلت الدراسة إلى مجموعة النتائج لعل من أهمها أن هناك برامج حماية تساعد في تحديد نوع الجريمة ووقت وقوعها وتتبع المُخترقين، بالإضافة إلى توفُّر برامج للكشف عن الفيروسات وأدوات مراقبة مستخدمي الشبكة، في حين أوصت الدراسة بضرورة العمل على زيادة الدورات والندوات للتعرف على أحدث الطرائق التي من شأنها أن تساعد في تحقيق أمن المعلومات، وأهمية العمل على التنسيق بين وزارة الداخلية والمؤسسات الأخرى الموفرة لنظم أمن المعلومات والشركات المزودة لخطوط الاتصالات ومزودي خدمة الإنترنت؛ لمساعدة الجهات الأمنيّة في ضبط تلك الجرائم ونوعيّة التطبيقات المُقدمة والأجهزة المستخدمة.

- دراسة (الشهري، 2001م) المشار لها في (العمري، 2004م)، بعنوان "**المعوقات الإداريّة في التعامل الأمني مع جرائم الحاسب الآلي**"، هدفت الدراسة التعرف إلى المعوقات الإداريّة في التعامل الأمني مع تلك الجرائم الحاسوبيّة، استخدم الباحث منهج المسح الاجتماعي، وقد تَكَوَّن مجتمع الدراسة من الضباط العاملين بجهاز الأمن العام بمدينة الرياض، في حين تكونت عينة الدراسة من (302) ضابط، توصلت الدراسة إلى مجموعة من النتائج، من أهمها نقص المعرفة بالحاسب الآلي ونقص المهارة في التعامل مع الإنترنت، إضافة إلى أن هناك نقصًا في الدورات التدريبيّة في مجال الأنظمة المعلوماتيّة، في حين أوصت الدراسة بوجوب عقد دورات لضباط الأمن في مجال أمن المعلومات والحاسب الآلي وشبكة الإنترنت، وأهميّة التوسع في العمل الآلي.
- دراسة (البشري، 2000م)، بعنوان "**الأدلة الجنائيّة الرقميّة مفهومها ودورها في الإثبات**"، هدفت الدراسة التعرف إلى إبراز دور الأدلة الجنائيّة الرقميّة والتعريف بخصائصها، وقد استخدم الباحث المنهج الوصفي، وتوصلت الدراسة إلى مجموعة من النتائج، من أهمها أهميّة الأدلة الجنائيّة الرقميّة لمواجهة الجرائم الإلكترونيّة وضرورة الارتقاء بمستوى منتسبي أجهزة العدالة الجنائيّة؛ حتى يكونوا قادرين على التعامل مع الأدلة الجنائيّة الرقميّة، في مواجهة الجرائم الإلكترونيّة، إضافة إلى أن استخدام الأدلة الجنائيّة الرقميّة يتوقف على إنشاء مختبرات الذكاء الاصطناعي، وتعميم الاستفادة منها؛ للتعامل مع الأدلة الجنائيّة الرقميّة، وجعل ثقافة الأدلة الرقميّة جزءًا من تكوين رجال تنفيذ القوانين والقضاء وتدريبهم، وأيضًا العمل على توعية الجمهور بدور الأدلة الجنائيّة الرقميّة في تحقيق العدالة، في حين أوصت الدراسة إلى أهمية العمل على توعية الجمهور بدور الأدلة الجنائيّة في تحقيق العدالة، فضلًا عن ضرورة تحقيق التعاون والتنسيق بين أجهزة العدالة وشركات تقنيات المعلومات، وأخيرًا أوصت بضرورة العمل على إنشاء مختبرات للذكاء الاصطناعي.

2.6.2 الدراسات الأجنبية:

- دراسة بلال وآخرون (Bilal & Others, 2019) بعنوان "**تأثير الذكاء الاصطناعي في الكشف عن الجرائم الإلكترونيّة**"، هدفت الدراسة التعرف إلى مدى تأثير تطبيقات الذكاء الاصطناعي في الكشف عن الجريمة الإلكترونيّة، استخدم الباحث المنهج الوصفي، وتكوَّن مجتمع الدراسة من العاملين كافَّةً في قطاع تكنولوجيا المعلومات في العراق، في حين تكوَّنت عينة الدراسة من (468) عاملًا في القطاع، وتوصلت الدراسة إلى مجموعة من النتائج، من أهمها أن هناك أهميّة كبيرة لتطبيقات الذكاء الاصطناعي في مواجهة الجريمة الإلكترونيّة، خاصة أن الشركات والمؤسسات أصبحت بحاجة مُلِحَّة لتوفير الحمايّة والأمان من أيٍّ هجمات إلكترونيّة تتعرض لها أنظمتها، في حين أوصت الدراسة بضرورة العمل على تطوير البنيّة التحتيّة في قطاع التكنولوجيا لزيادة تخزين البيانات، بالإضافة إلى ضرورة العمل على تطبيق الذكاء الاصطناعي في المؤسسات كافَّةً؛ لتوفير الحمايّة، وصدِّ الهجمات الإلكترونيّة في حال تعرضها لأي اختراقات؛ كونها تحتوي على معلومات سرِّيَّة وبيانات ضخمة، كما وأوصلت على تعزيز الدراسات المُتعلّقة بالذكاء الاصطناعي والجريمة الإلكترونيّة.
- دراسة ايكنيم (Ekanem, 2019) بعنوان "**الذكاء الاصطناعي كآليّة لمكافحة الجريمة في نيجيريا**"، هدفت الدراسة التعرف إلى كيفيّة عمل الذكاء الاصطناعي بآليّة مثآليّة لمكافحة الجريمة في نيجيريا وتحسين أداء ضباط الشرطة في التحقيق، استخدم الباحث منهج تحليل المضمون، ولتحقيق ذلك قام بالاعتماد على الكتب والصحف والمؤتمرات ومواد الإنترنت والدراسات ذات العلاقة في الموضوع، توصلت الدراسة إلى مجموعة من النتائج، من أهمها أهميّة الذكاء الاصطناعي في مواجهة الجريمة، والحد منها خاصة مع ارتفاع معدل الجريمة في نيجيريا، أكدت النتائج أن التحقيق في الجرائم أثبت نجاحًا من خلال الذكاء الاصطناعي، إضافة إلى نقص الخبرة والمهارة لدى ضباط الشرطة، في حين أوصت الدراسة بضرورة توسيع مجال العمل في تقنيات الذكاء الاصطناعي في مكافحة الجريمة بالإضافة إلى العمل على رفع الخبرة والكفاءة لدى المحققين.
- دراسة كوسترا (Koostra, 2019) بعنوان "**دعم استخدام الذكاء الاصطناعي في مراكز العمليات الأمنية**"، هدفت الدراسة التعرف إلى أي مدى يمكن دعم استخدام الذكاء الاصطناعي في مراكز العمليات الأمنيّة، استخدم الباحث منهج تحليل المضمون من خلال مراجعة الأدبيات، وتوصلت الدراسة إلى مجموعة من النتائج، من أهمها أنَّ استخدام الذكاء الاصطناعي بالفعل يساعد في رفع مستوى عمل الحكومة، بالإضافة إلى أن دعم الذكاء الاصطناعي في مراكز الأمن يساعد في أداء الأعمال بشكل أدق وكفاءة عآليّة، كما أكدت نتائج الدراسة أن أفضل تقنيات يمكن لمراكز العمليات الأمنيّة في هولندا استخدامها هي

الأنظمة الخبيرة والتعلم الآلي ومعالجة اللغات الطبيعيّة، في حين أوصت الدراسة بضرورة العمل على تبني مصطلح الذكاء الاصطناعي في المراكز الأمنيّة وضرورة تعزيز مهارات الموظفين في هذه المراكز، كما أكدت على أهميّة استخدام تقنيات الذكاء الإصطناعي.

- دراسة تيواري وماهيشواري وبال (Tiwari & Maheshwary & Pal, 2018) بعنوان "**تطبيق الذكاء الإصطناعي في الحد من هجمات الجرائم الإلكترونيّة**"، هدفت الدراسة التعرف إلى البحث وتقديم تقنيات وبرامج وتطبيقات في الذكاء الاصطناعي؛ من أجل حلِّ مشاكل الجرائم الإلكترونيّة؛ كونها لا تقتصر على منطقة معينة، استخدم الباحث منهج تحليل المضمون، ولتحقيق ذلك اعتمد على الكتب والصحف والمجلات والدراسات ذات العلاقة، وتوصلت الدراسة إلى مجموعة من النتائج، من أهمها أن إمكانات الذكاء الاصطناعي بالفعل لديها القدرة على مكافحة الجرائم الإلكترونيّة ومواجهتها، إضافة إلى أن الذكاء الاصطناعي يوفر تقنيات مختلفة مثل (النظم الخبيرة، الوكلاء الأذكياء، الشبكات العصبيّة)، توصلت إلى بناء هيكل للدفاع (CDS) من خلال تقنيات البرمجة؛ للكشف عن المتسللين الإلكترونيين، حيث إنهم في المستقبل قد يحاولون استخدام الطرائق المختلفة؛ من أجل اقتحام الشبكات والنظم، في حين أوصت الدراسة بأهميّة العمل على تعزيز بناء بنية للدفاع من أجل إزالة الاختراقات واستخدام المواد النظريّة والأكاديميّة في تطبيق مزيد من النظم ذات العلاقة.
- دراسة ويليامسون (Williamson, 2014) بعنوان "**تحديات ضبط المجرم الالكتروني**"، هدفت الدراسة إلى التعرف إلى التحديات التي تحول دون ضبط مجرمي الإنترنت، والقبض عليهم، استخدمت الدراسة منهج تحليل المضمون، ولتحقيق ذلك اعتمد على الكتب والصحف والمجلات والدراسات ذات العلاقة، وتوصلت الدراسة إلى مجموعة من النتائج لعل من أهمها قلة المعلومات في موضوع تحديّات ضبط مجرمي الإنترنت، وأن الأبحاث التي أُجْرِيَتْ على الموضوع اقتصرت على معرفة التاريخ، وكيفية الوصول وتحليل معلومات الحاسب الآلي ولم يتم اكتشاف معلومات دقيقة عن الإنترنت، في حين أوصت الدراسة بضرورة إجراء المزيد من الأبحاث والدراسات حول الإمكانات التي يتم من خلالها ضبط مجرمي الإنترنت وضرورة التعمق في البحث عن المعلومات.

3.6.2 ما يميّز الدراسة الحاليّة عن الدراسات السابقة وذات الصلة:

هناك عدد من النقاط التي تتمييز بها الدراسة الحآليّة عن الدراسات السابقة وذات العلاقة، من أهمها ما يأتي:

- تُعَدُّ هذه الدراسة من الدراسات النادرة التي تبحث حول موضوع المُعوقات التي تحول دون تطبيق الذكاء الاصطناعي في الحد من ممارسة الجريمة الإلكترونيّة في الضفة الغربية.
- مجتمع الدراسة يتكون من العاملين في وزارة الاتصالات والتكنولوجيا والمعلومات.
- تتميز هذه الدراسة عن الدراسات السابقة في أدوات جمع البيانات فهي اعتمدت على المقابلة أداةً لجمع البيانات، في حين أغلب الدراسات استندت على الاستبانة لجمع البيانات، إضافة إلى تحليل المضمون من خلال الرجوع للمصادر والمؤسسات الرسمية التي تحتوي على إحصائيات للجرائم الإلكترونيّة.

الفصل الثالث

المنهج والإجراءات

1.3 مقدمة:

يتناول هذا الفصل وصفًا مُفصلًا لمَنهج الدراسة وأداتها التي اُخْتيرتْ لإجراء الدراسة ولجمع البيانات، وكيفية التحقق من صدق الأداة، كذلك مجتمع الدراسة وعرضه الإجراءات المتبعة في التأكد من الخصائص الديموغرافيّة للعينة.

2.3 مَنهجيّة الدراسة:

استنادًا إلى طبيعة الدراسة وأهدافها، استخدمت الدراسة الحاليّة المنهج الوصفي بشقه الكيفي (النوعي) من خلال استخدام دليل المقابلة؛ كونه المنهج الأنسب لهذا النوع من الدراسات، بحكم أنّه من المناهج المهمَّة الذي يُعَبِّرُ كمًّا ونوعًا عن معطيات الدراسة، ولأنه يُعَدُّ طريقة علميّة منظمة لوصف النتائج وتحليلها وتفسيرها واستخلاصها.

3.3 مُجتمع الدراسة وعينته:

في الدراسة الحاليّة تمّ استخدام أسلوب المسح الاجتماعي الشامل، حيث تَكوَّن مُجتمع الدراسة من جميع العاملين في وزارة الاتصالات وتكنولوجيا المعلومات في مدينة رام الله والبيرة من فئة العاملين في تكنولوجيا المعلومات والاتصالات البالغ عددهم (50) حسب إحصائيات (وزارة الاتّصالات وتكنولوجيا المعلومات،2021)، الجدول رقم (1.3) يوضح الخصائص الديموغرافيّة لمُجتمع الدراسة.

جدول رقم (1.3): الخصائص الديموغرافيّة لمجتمع الدراسة

المتغير	المستوى	العدد	النسبة المئويّة %
الجنس	ذكر	23	46.0
	أنثى	27	54.0
العمر	أقل من 25 سنة	1	2.0
	25 – 35 سنة	38	76.0
	36 – 45 سنة	10	20.0
	أكثر من 46 سنة	1	2.0
المستوى التعليمي	ماجستير	9	18.0
	بكالوريوس	39	78.0
	دبلوم عالي	1	2.0
	دبلوم	1	2.0
القسم	أمن المعلومات	5	10.0
	أنظمة معلومات	1	2.0
	الاتصالات	5	10.0
	التطوير الفني	1	2.0
	الحاسوب الحكومي	8	16.0
	الحكومة الإلكترونيّة	13	26.0
	الدعم الفني	3	6.0
	الشكاوي	10	20.0
	المعلوماتيّة	1	2.0
	المقاسم	1	2.0
	جودة الخدمة	1	2.0
	هندسة الحاسوب	1	2.0
المسمى الوظيفي	دعم فني	1	2.0
	رئيس قسم الشبكات	1	2.0
	مبرمج	12	24.0
	مدير	7	14.0
	مهندس	29	58.0
عدد سنوات الخبرة في العمل	أقل من 10 سنوات	40	80.0
	10–20 سنة	4	8.0
	أكثر من 20 سنة	6	12.0
أماكن العمل التي عملت بها من قبل	قطاع خاص	33	66.0
	قطاع عام	3	6.0

	لم أعمل	14	28.0
عدد سنوات الخبرة السابقة	أقل من سنة	5	10.0
	سنة – أقل من 5 سنوات	20	40.0
	5 سنوات فأكثر	11	22.0
	لا يوجد خبرة	14	28.0
دورات خاصة بالذكاء الإصطناعي لها علاقة بتتبع الجرائم الإلكترونيّة	لا	49	98.0
	نعم	1	2.0

يُبَيِّنُ الجدول رقم (1.3) أنَّ عدد أفراد المجتمع من الذكور بلغ (23) بنسبة (46%) من أفراد المجتمع، فيما بلغ عدد الإناث (27) بنسبة (54%)، وقد يعود السبب في ذلك إلى أن الضبط المرتفع يُولِّدُ عِنْدَ الإناث الإصرار على إثبات الذات والتحدي لاكتساب التعليم والوظيفة، هذا يعني أن طبيعة التنشئة الاجتماعية في المجتمع الفلسطيني تؤدّي دورًا كبيرًا في تحديد مستوى الضبط عند الطرفين كليهما، فعندما تكون التنشئة الاجتماعية قائمة على أنَّ كل شيء متاح للذكور فمن الممكن أن يُوَلِّدَ لديهم الضبط المنخفض؛ ما يعني ممارستهم للجريمة على العكس من الإناث، فالتنشئة الاجتماعية لدى الإناث تقلل من فرصة ممارستهنّ للجريمة، في حين أن توزيع أفراد المجتمع حسب متغير العمر، نلاحظ أن عدد المبحوثين الذين تتراوح أعمارهم بين (25 – 35) سنة تمثل نسبة (76%) تليها الفئة العمرية بين (36 – 45) سنة، وتمثل نسبة (20%)، وفئة (أقل من 25) سنة تمثل (2%) وفئة (أكثر من 46) سنة تمثل (2%)، قد يعود السبب في ذلك إلى أن الفئات العمرية الشابة تكون في مقتبل العمر، ونسبة عطائها في العمل أكثر في هذه الفترة ما يدفع الوزارة إلى البحث عن هذه الفئات العمريّة؛ لتوظيفها بهدف الحصول على إنتاجيّة أكبر في العمل، وأما عن توزيع أفراد المجتمع حسب متغير المستوى التعليمي فإنَّ الجدول يُبَيِّنُ أن نِسبة (78%) من أفراد المجتمع هم من حَمَلَةِ درجة البكالوريوس بنسبة (39%) بينما حَمَلَةِ درجة الماجستير بلغ عددهم (9) بنسبة (18%)، في حين كانت نسبة حَمَلَةِ الدبلوم العالي (2%) بعدد مقداره (1) إضافة إلى عدد حَمَلَةِ الدبلوم بلغ عددهم (1) بنسبة (2%)، ونلاحظ أن هناك تفاوتًا بين نسبة حَمَلَةِ الدرجات العلميّة العليا والوسطى، وقد يعود السبب في ذلك إلى صعوبة التخصص الذي يتطلب كثيرًا من المهارات والقدرات الذهنيّة؛ لاستكمال المتطلبات الجامعيّة، إضافةً إلى ارتفاع تكلفة الدراسات العليا التي تعوق –في بعض الأحيان– قدرة الطلبة على الاستمرار في المسيرة التعليميّة، في حين أن توزيع أفراد المجتمع حسب متغير القسم يبين الجدول أن (26%) من أفراد المجتمع يعملون في قسم الحكومة الإلكترونيّة بعدد (13)، فيما كان عدد العاملين في قسم الشكاوي (10) بنسبة (20%) من أفراد المجتمع، في حين بلغ عدد العاملين في قسم الحاسوب الحكومي (8) بنسبة (16%)، وأما في قسم الاتصالات بلغ عدد العاملين (5) بنسبة

(10%)، وبلغ عدد العاملين في قسم أمن المعلومات (5) بنسبة (10%) فيما كان عدد العاملين في قسم الدعم الفني (3) بنسبة (6%)، ونلاحظ أن هناك تفاوتًا في أعداد العاملين في الأقسام، وقد يعود السبب في ذلك إلى الإختلاف في احتياج كل قسم لعدد الموظفين العاملين فيه، وأما توزيع أفراد المجتمع حسب متغير المسمى الوظيفي يبين الجدول أن نسبة (58%) من أفراد المجتمع مسامهم الوظيفي "مهندسون" بعدد (29)، وهذا يشكل أكثر من نصف أفراد مجتمع الدراسة وما نسبته (24%) مسماهم "مبرمجون" بعدد (12)، وما نسبته (14%) مسماهم "مدير"، بعدد (7)، وما نسبته (2%) مسماهم "رئيس قسم الشبكات" بعدد (1)، وما نسبته (2%) مسماهم "دعم فني" بعدد (1)، قد يعود السبب في ذلك إلى طبيعة التخصصات العلميّة التي تفرضها عندما ترغب في توظيف موظفينها، فهي توظف حسب التخصصات والقدرات العلمية، في حين أن توزيع أفراد المجتمع حسب متغير عدد سنوات الخبرة في العمل يبين الجدول أن نسبة (8%) من أفراد المجتمع لديهم خبرة عمل تزيد عن (20) سنة، في حين أنَّ (12%) من أفراد العينة لديهم سنوات خبرة بين (10–20)، سنة والباقي (80%) من أفراد المجتمع لديهم خبرة أقلّ من (10) سنوات، ونلاحظ أن هناك انخفاضًا في نسبة الموظفين أصحاب الخبرة القديمة، وقد يعود السبب في ذلك إلى أن الوزارة تحيل الكبار في السن إلى التقاعد، وتقوم بتوظيف موظفين جدد؛ ما يوضح السبب في ارتفاع نسبة الموظفين الذين تقل خبرتهم عن (10) سنوات، إضافة لحداثة الموضوع المدروس فإن سنوات الخبرة قليلة لدى الموظفين، وفيما يخص توزيع أفراد المجتمع حسب متغير أماكن العمل السابقة يبين الجدول أن نسبة (66%) من أفراد المجتمع كانوا يعملون في القطاع الخاص بعدد مقداره (33)، ونسبة الذين كانوا يعملون في القطاع العام (6%) بعدد مقداره (3)، بينما كانت نسبة الذين لم يكن لديهم عمل سابق (28 %) بعدد مقداره (14)، وأما عن توزيع أفراد المجتمع حسب متغير سنوات الخبرة في أماكن العمل السابقة فإنَّ الجدول يبين أن نسبة (22%) من أفراد المجتمع لديهم خبرة في أماكن عملهم السابقة تزيد عن (5) سنوات، بينما (40%) من أفراد المجتمع لديهم سنوات خبرة تتروح بين (سنة–أقل من 5 سنوات)، بينما (10%) من أفراد المجتمع يمتلكون خبرة تقل عن (سنة)، بعدد (5) والباقي (28%)، لا يمتلكون الخبرة، وأخيرًا فيما يخص توزيع أفراد المجتمع حسب متغير الالتحاق بدورات خاصة بتطبيقات الذكاء الاصطناعي لها علاقة بتتبع الجريمة الإلكترونيّة يبين الجدول أن نسبة (98%) من أفراد المجتمع لم يلتحق بدورات خاصة بتطبيقات الذكاء الاصطناعي لها علاقة بتتبع الجريمة الإلكترونيّة حيث كان عددهم (49) فردًا، في حين أن من التحق بالدورات كان مبحوثًا واحدًا بنسبة (2%) نلاحظ أن هناك تفاوتًا كبيرًا جداً في نسبة الموظفين الخاضعين لدورات خاصة بالذكاء الاصطناعي، على الرغم من الأهمية الكبيرة التي توليها الدول الأخرى في هذا الشأن قد يعود السبب في ذلك لندرة المتخصصين في مجال الذكاء الاصطناعي، إضافة إلى أن هذه الدورات تتطلب من الموظفين السفر لفترات خارج البلاد؛ ما يدفع الموظف إلى التفكير في الأسرة والالتزامات الحياتيّة التي تجبره في كثير من الأحيان

إلى رفض مثل هذا النوع من الدورات، إضافة إلى التكاليف العاليّة التي تحتاجها البنيّة التحتيّة الخاصة بهذه الدورات.

4.3 أدوات جمع البيانات:

استخدمت الدراسة الحاليّة دليل المقابلة أداةً لجمع البيانات حيث تمّ إعداد أسئلة المقابلة وعرضها على (6) من المحكمين من ذوي الاختصاص في العلوم الإنسانية، وتكنولوجيا المعلومات، ومِنْ ثَمَّ إجراء التعديلات اللازمة بناءً على ما تقدموا به من ملحوظات، لمزيد من التوضيح حول أسماء المحكمين أنظر/ ي ملحق رقم (2)، تكونت المقابلة من بعدين رئيسيين:

- **البعد الأول:** اشتمل على معلومات عامة عن المبحوثين من حيث (الجنس، العمر، المستوى التعليمي، القسم، المسمى الوظيفي، عدد سنوات الخبرة في العمل الحالي، أماكن العمل السابقة، عدد سنوات العمل الخبرة السابقة، هل تم الالتحاق بدورات خاصة بتطبيقات الذكاء الاصطناعي لها علاقة بتتبع الجرائم الإلكترونيّة).
- **البعد الثاني:** إشتمل على ثلاثة محاور رئيسية هي:
  - المحور الأول: ما دور الذكاء الاصطناعي في الكشف عن الجريمة الإلكترونيّة؟
  - المحور الثاني: ما آليّة عمل برامج الذكاء الاصطناعي المستخدمة في الوزارة لتتبع الجناة المرتكبين للجرائم الإلكترونيّة؟
  - المحور الثالث: ما المُعوقات التي تواجه تطبيق الذكاء الاصطناعي في الحد من ممارسة الجريمة الإلكترونيّة؟

5.3 صدق الأداة وثباتها:

تمَّ التَّحقُّقُ من صدق الأداة وثباتها من خلال تطبيقها على (5) من العاملين في الوزارة اللذين تمّ إستبعادهم فيما بعد من العينة النهائيّة، حيث تمّ التعديل على محاور الأداة بعد الإجابة عليها من قبل هؤلاء العاملين، وإخراجها بصورتها النهائيّة كما في ملحق رقم (1).

6.3 إجراءات الدراسة:

من أجل استكمال الدراسة تمّ القيام بمجموعة من الإجراءات، على النحو الآتي:

- تّم إخراج أداة الدراسة (دليل المقابلة) بصورتها النهائيّة بعد عرضها على المحكمين وتطبيقها على (5) من العاملين في الوزارة، حيث تمّ الأخذ بعين الاعتبار ما تم إبداؤه منهم من ملحوظات.

- تمّ الحصول على كتاب تسهيل مهمة من عمادة كليّة الآداب بجامعة القدس، من أجل مخاطبة وزارة الاتصالات وتكنولوجيا المعلومات لتسهيل مهمة إجراء المقابلات، وعليه تمّ الحصول على موافقة الوزارة.
- بعد الحصول على موافقة الوزارة تمّ إجراء المقابلات مع العاملين في قسم تكنولوجيا المعلومات والاتصالات.
- بعد ذلك تمّ تحليل أسئلة المقابلات والحصول على النتائج التي تمّ مناقشتها والتوصل من خلالها للاستنتاجات والتوصيات.

الفصل الرابع

عرض النتائج

1.4 مقدمة:

في هذا الفصل تمّ عرض أهم النتائج التي توصلت إليها الدراسة بإيراد نتائج أسئلة المقابلات من خلال جداول تبين أهم النقاط التي اتفق عليها أفراد المجتمع.

2.4 نتائج المحور الرئيسي الأول المُتعلق بدور الذكاء الاصطناعي في الكشف عن الجريمة الإلكترونيّة والحد منها:

نتائج تحليل إجابات المبحوثين حول الأسئلة ذات العلاقة بدور الذكاء الاصطناعي في الكشف عن الجريمة الإلكترونيّة والحد منها، تستعرضها الدراسة فيما هو آتٍ:

1.2.4 النتائج المتعلقة بوجود دور الذكاء الاصطناعي في الحد من الجريمة الإلكترونيّة:

في إطار إجابة الدراسة على السؤال البحثي "هل هناك دور للذكاء الاصطناعي في الكشف عن الجريمة الإلكترونيّة؟"، تم احتساب التكرارات والنسب المئويّة وجاءت النتائج كما في الجدول رقم (1.4).

جدول رقم (1.4): التكرارات والنسب المئويّة لإجابات المبحوثين حول وجود دور للذكاء الاصطناعي في الكشف عن الجريمة الإلكترونيّة

هل هناك دور للذكاء الاصطناعي في الكشف عن الجريمة الإلكترونيّة؟	التكرارات	النسبة المئويّة %
نعم	50	%100
لا	0	%0
المجموع	50	%100

تظهر النتائج في الجدول رقم (1.4) أن جميع أفراد مجتمع الدراسة البالغ عددهم (50) بنسبة (100%) أكدوا على أن هناك دورًا للذكاء الاصطناعي في الكشف عن الجريمة الإلكترونيّة والحد منها، يتجلى هذا الدور في أن خوارزميات التنبؤ وخورازميات التصنيف التي تعمل على تصنيف البيانات وتحليلها، وذلك من خلال المعطيات وقواعد البيانات المتوفرة لديها، كما أن لها دورًا في تسهيل عمليّة الكشف عن المجرمين، وتتبعهم عن طريق التوصل إلى أماكن وجودهم، والسرعة في الوصول إليهم، فضلًا عن دقة البيانات التي تعطيها هذه التطبيقات، بالإضافة إلى قدرتها على المراقبة المستمرة لكلّ المسلكيّات الَّتي تحدث داخل نطاق الشبكة، وبشكل عام أكد أغلب المبحوثين في الدراسة على الدور المهم للذكاء الاصطناعي في الكشف عن قضايا الابتزاز التي يتعرض لها الأطفال خاصة على مواقع التواصل الاجتماعي، وركز بعضهم على أهميته في الحالة الفلسطينيّة تحديداً مثلما ذكروا "أن وضع فلسطين الخاص يحتاج إلى تطبيقات الذكاء الاصطناعي؛ لتؤدّيَ دورًا في الكشف عن الجريمة الإلكترونيّة وتوأمة الذكاء الاصطناعي، بحيث يتمكن من التعرف إلى ما يسمى بالهندسة الاجتماعية التي تستخدم في مواقع التواصل الاجتماعي وهي عبارة عن طرق للاحتيال على الضحيّة، والحصول على معلومات متعلقة به".

في حين ركز البعض الآخر على أهميّة استخدام هذه التطبيقات في المجتمع الفلسطيني بالتركيز على سلبياتها نظراً للانتشار الواسع لاستخدام وسائل التواصل الاجتماعي بشكل سلبي، كما ينعكس في بعض المسلكيّات الاجراميّة، بينما ركز آخرون على دورها في المراقبة والحمايّة من الجرائم.

2.2.4 النتائج ذات العلاقة بمدى القبول المجتمعي للذكاء الاصطناعي:

في إطار إجابة الدراسة عن السؤال البحثي "من وجهك نظرك هل تشعر أن مدى الذكاء الاصطناعي مرتبط بمدى قبوله في المجتمع؟ كيف ولماذا؟"، تمّ احتساب التكرارات والنسب المئويّة وجاءت النتائج كما في الجدول رقم (2.4).

جدول رقم (2.4): التكرارات والنسب المئويّة لإجابات المبحوثين حول مدى الذكاء الاصطناعي مرتبط بمدى قبوله في المجتمع

هل تشعر أن مدى تطبيق الذكاء الإصطناعي مرتبط بمدى قبوله في المجتمع؟	التكرارات	النسبة المئويّة %
نعم	16	%32
لا	34	%68
المجموع	50	%100

تظهر النتائج في الجدول رقم (2.4) أن نسبة (68%) من أفراد المجتمع أكدوا على عدم ارتباط تطبيق الذكاء الاصطناعي بقبوله في المجتمع، بل هي تطبيقات تفرض على المجتمع حيث إن

الجوالات تستخدم الذكاء الاصطناعي دون إذن المستخدم، وتتخذ كثيرًا من القرارات دون إذنه، وكذلك ينظر المجتمع إليها من باب انتهاك الخصوصيات، لكن هذا الموضوع يصب في مصلحته فيما أكد (32%) من أفراد المجتمع أن تطبيق الذكاء الاصطناعي مرتبط بقبوله في المجتمع؛ لأنه يعمل على تحقيق الأمان والحماية، وتسهيل حياتهم وليس ضدهم، كما أن بعض أفراد المجتمع ليس على علم واطِّلاع بالتكنولوجيا وكيفية استخدامها، إضافة إلى رفض وخوف الأفراد في المجتمع من هذه التطبيقات نظرًا لانتهاك الذكاء الاجتماعي لخصوصياتهم (الاطِّلاع على معلوماتهم الشخصيّة كافَّةً)؛ ما يشعرهم بانعدام الخصوصيّة؛ لذا، وبناءً على ما سبق عند تطبيق تكنولوجيا حديثة في المجتمع يحتاج إلى قبول الناس لها، إضافة إلى أن تطبيق الذكاء الاصطناعي بحاجة الى موافقة عشائر المجتمع وعوائله.

3.2.4 النتائج حول واقع استخدام برامج الذكاء الاصطناعي في وزارة الاتصالات وتكنولوجيا المعلومات:

في إطار إجابة الدراسة على السؤال البحثي "هل يتم استخدام برامج الذكاء الاصطناعي في وزارة الاتصالات وتكنولوجيا المعلومات؟ ما أهم هذه البرامج؟ وما هي نطاقات استخدامها؟" تمّ احتساب التكرارات والنسب المئويّة وجاءت النتائج كما في الجدول رقم (3.4).

جدول رقم (3.4): التكرارات والنسب المئويّة لإجابات المبحوثين حول في استخدام وزارة الاتصالات وتكنولوجيا المعلومات لبرامج الذكاء الاصطناعي

هل يتم إستخدام برامج الذكاء الاصطناعي في وزارة الاتصالات وتكنولوجيا المعلومات؟	التكرارات	النسبة المئويّة %
نعم	43	%86
لا	6	%12
تطوير برامج الذكاء الاصطناعي في وزارة الاتصالات وتكنولوجيا المعلومات	1	%2
المجموع	50	%100
أهم تلك البرامج؟		
WAF	42	%84
UTM	26	%52
Fir wall	25	%50
F5	1	%2

يتضح من الجدول رقم (3.4) أنَّ الوزارة تستخدم تطبيقات الذكاء الاصطناعي فقد بلغت نسبة الإجابات بـ(نعم) (86%) بعدد مقداره (43)، وبلغت نسبة الإجابات بـ(لا) (12%)، بعدد مقداره (6)، كما يتضح من الجدول أعلاه أن أكثر تطبيقات الذكاء الاصطناعي استخداماً هي برنامج الـ(WAF) حيث حصل على (42) إجابة من أصل (50) بنسبة (84%) إضافة لبرنامج الـ(UTM) الذي حصل

على (26) بنسبة (52%) وبرنامج الـ(Fir wall) الذي حصل على (25) إجابة وهي تشكل (50%) من الاجابات، وبرنامج الـ(F5) الذي حصل على أقل عدد من الاستجابات من خلال إجابة مبحوث واحد فقط، في حين بلغ عدد الإجابات حول تطوير الوزارة لتطبيقات الذكاء الاصطناعي والتدريب عليها إجابة واحدة فقط.

4.2.4 النتائج حول مساهمة برامج الذكاء الاصطناعي في الحد من الجريمة الإلكترونيّة:

في إطار إجابة الدراسة على السؤال البحثي "هل تسهم برامج الذكاء الاصطناعي في الحد من الجريمة الإلكترونيّة؟"، تمّ احتساب التكرارات والنسب المئويّة وجاءت النتائج كما في الجدول رقم (4.4).

جدول رقم (4.4): التكرارات والنسب المئويّة لإجابات المبحوثين حول مساهمة برامج الذكاء الاصطناعي في الحد من الجريمة الإلكترونيّة

كيف تساهم برامج الذكاء الاصطناعي في الحد من الجريمة الإلكترونيّة؟	العدد	النسبة المئويّة %
تساهم في التقليل من نسبة الجريمة من خلال التنبؤ بوقوع الجريمة واكتشافها وسرعة اتخاذ القرار	26	%52
تساهم في صد الهجمات الإلكترونيّة	25	%50
توفير الحماية والأمان	11	%22
توفير أدلة للنيابة	9	%18
لا تساهم بشكل كلي إنما هناك ضرورة لوجود قوانين وعقوبات صارمة	6	%12
نشر الوعي والفكر لدى أفراد المجتمع بفعآليّة هذه التطبيقات في كشف الجريمة الإلكترونيّة	4	%8

يتضح لنا من الجدول أعلاه أن هناك أكثر من إجابة مُتاحة للمبحوثين، حيث نرى أن نسبة (52%) من أفراد المجتمع أكدوا على أن برامج الذكاء الاصطناعي تساهم في الحد من الجريمة الإلكترونيّة من خلال التنبؤ بالأحداث قبل وقوعها والسرعة في اتخاذ القرار في المواقف التي تتعرض لها، فيما أكد (50%) من أفراد المجتمع أن صد الهجمات الإلكترونيّة تسهم في الحد من الجريمة الإلكترونيّة، وأكد (22%) من أفراد المجتمع أن برامج الذكاء الاصطناعي تسهم في توفير الحمايّة والأمان وتوفير الأدلة للنيابة من خلال كشف تطبيقات الذكاء الاصطناعي للجريمة فقد حصلت على نسبة (18%)، وبلغت نسبة الإجابات على أن تطبيقات الذكاء الاصطناعي وحدها لا تُسْهِمُ بشكل كلي في الحد من الجريمة الإلكترونيّة، إنما هناك ضرورة لوجود قوانين وعقوبات صارمة (12%)، إضافة إلى نشر الوعي والفكر لدى أفراد المجتمع بوجود تقنيات حديثة، تعمل على الكشف عن الجرائم التي تحدث داخل الشبكة الإلكترونيّة، فقد حصلت على أقل عدد من الاستجابات بنسبة (8%).

5.2.4 النتائج حول كيفية ردع برامج الذكاء الاصطناعي للجناة:

في إطار إجابة الدراسة على السؤال البحثي "كيف يمكن أن تكون برامج الذكاء الاصطناعي رادعًا أمام الجناة لمنع ممارسة الجريمة الإلكترونيّة والحد منها؟"، تمَّ احتساب التكرارات والنسب المئويّة وجاءت النتائج كما في الجدول رقم (5.4).

جدول رقم (5.4): التكرارات والنسب المئويّة لإجابات المبحوثين حول آليّة ردع برامج الذكاء الاصطناعي للجناة

كيف يمكن أن تكون برامج الذكاء الاصطناعي رادع أمام الجناة؟	التكرارات	النسبة المئويّة %
من خلال التأثير في نفسية الجاني أنه مراقب إلكترونيا	35	%70
من خلال تعريض الجاني للمساءلة القانونية وإنزال أشد العقوبات عند كشفه	15	%30
يمكن أن تكون رادعًا بشكل جزئي	8	%16
من خلال تقيد حركة الجاني على الشبكة الإلكترونيّة بواسطة هذه التطبيقات	7	%14
من خلال نشر الوعي حول إمكانية الذكاء الاصطناعي على كشف الجرائم	6	%12

يتضح لنا من الجدول أعلاه أن هناك أكثر من إجابة مُتاحة للمبحوثين، كما ويتضح أن تطبيق الذكاء الاصطناعي يُسهم في ردع الجناة ومنعهم من ممارسة الجريمة الإلكترونيّة من خلال التأثير في نفسية الجاني أنه مراقب إلكترونيا طوال الوقت، فقد حصلت على (35) إجابة من أصل (50)، يليها تعريضه للمساءلة القانونية، وإنزال أشد العقوبات عند كشفه فقد حصلت على (15) إجابة، ثم يمكن أن تكون رادعًا بشكل جزئي فقد حصلت على (8) إجابات، في حين أن تقييد حركته على الشبكة الإلكترونيّة بوساطة هذه التطبيقات فقد حصلت على (7) إجابات، وأخيرًا نشر الوعي والتثقيف حول إمكانية تطبيقات الذكاء الاصطناعي على كشف الجرائم فقد حصلت على (6) إجابات.

3.4 نتائج المحور الرئيسي الثاني المُتعلق بآليّة عمل برامج الذكاء الاصطناعي لتتبع الجناة مرتكبي الجرائم الإلكترونيّة:

نتائج تحليل إجابات المبحوثين حول الأسئلة ذات العلاقة بآليّة عمل برامج الذكاء الاصطناعي لتتبع الجناة مرتكبي الجرائم الإلكترونيّة، تستعرضها الدراسة فيما هو آتٍ:

1.3.4 النتائج المُتعلقة بآليّات عمل برامج الذكاء الاصطناعي في تتبع الجناة:

في إطار إجابة الدراسة على السؤال البحثي "ما آليّة عمل برامج الذكاء الاصطناعي لتتبع الجناة المرتكبين للجريمة الإلكترونيّة؟"، تمّ احتساب التكرارات والنسب المئويّة، وجاءت النتائج كما في الجدول رقم (6.4).

جدول رقم (6.4): التكرارات والنسب المئويّة لإجابات المبحوثين حول آليّة عمل برامج الذكاء الاصطناعي في الوزارة لتتبع الجناة مرتكبي الجرائم الإلكترونيّة

ما آليّة عمل برامج الذكاء الاصطناعي المستخدمة في الوزارة لتتبع الجناة المرتكبين للجرائم الإلكترونيّة؟	التكرارات	النسبة المئويّة %
لا يوجد	50	%100
يوجد	0	%0
المجموع	50	%100

أظهرت نتائج الجدول أعلاه أن الوزارة تستخدم تطبيقات الذكاء الاصطناعي وبرامجه، لكن لا يوجد في الوزارة آليّة لعمل تلك البرامج والتطبيقات لتتبع الجناة المرتكبين للجرائم الإلكترونيّة، إن ما يؤكد على ذلك ما أشار له المبحوث في (مقابلة رقم 32) حيث أشار إلى أن "الوزارة تستخدم الذكاء الاصطناعي لكن لا يوجد آليّات متبعة في استخدامه".

2.3.4 النتائج المُتعلقة بإسهام آليّات عمل برامج الذكاء الاصطناعي في التخفيف من الجريمة الإلكترونيّة المرتكبة:

في إطار إجابة الدراسة عن السؤال البحثي "كيف تُسْهِم الآليات المتبعة في استخدام برامج الذكاء الاصطناعي في التخفيف من الجريمة الإلكترونيّة المرتكبة؟"، تم احتساب التكرارات والنسب المئويّة وجاءت النتائج كما في الجدول رقم (7.4).

جدول رقم (7.4): التكرارات والنسب المئويّة لإجابات المبحوثين حول مساهمة آليّات استخدام برامج الذكاء الاصطناعي في الوزارة في التخفيف من الجرائم الإلكترونيّة

كيف تساهم الآليات المتبعة في استخدام برامج الذكاء الاصطناعي في الوزارة في التخفيف من نسبة الجريمة الإلكترونيّة؟	العدد	النسبة المئويّة %
لا يوجد	50	%100
يوجد	0	%0
المجموع	50	%100

أظهرت نتائج الجدول أعلاه أن الآليات المتبعة في استخدام برامج الذكاء الاصطناعي في الوزارة لا تُسْهِمُ في التخفيف من نسبة الجريمة الإلكترونيّة المُرتكبة؛ لأنَّ جميع المبحوثين أجمعوا في السؤال السابق على أنه لا توجد آليّات متبعة في تطبيق الذكاء الاصطناعي.

3.3.4 النتائج المُتعلقة بآليّات عمل مقترحة لتتبع الجرائم الإلكترونيّة:

في إطار إجابة الدراسة عن السؤال في حال ضعف أو عدم توفر اليات تتبع للجرائم الإلكترونيّة ماذا تقترح/لتوفير أو تحسين آليات العمل في تتبع الجرائم الإلكترونيّة؟"، تمّ احتساب التكرارات والنسب المئويّة وجاءت النتائج كما في الجدول رقم (8.4).

جدول رقم (8.4): التكرارات والنسب المئويّة لإجابات المبحوثين حول المقترحات لتحسين آليّات العمل المتبعة في تتبع الجرائم الإلكترونيّة

ماذا تقترِح/ين لتوفير أو تحسين آليات العمل المُتبعة في تَتبع الجرائم الإلكترونيّة؟	التكرارات	النسبة المئويّة %
ضرورة توفير أجهزة الذكاء الاصطناعي لتتبع مرتكبي الجرائم الإلكترونيّة وملاحقتهم.	36	%72
ضرورة تدريب الموظفين وتطوير مهاراتهم وقدراتهم في التعامل مع برامج الذكاء الاصطناعي فقط.	27	%54
ضرورة تخصيص موازنات مآليّة مخصصة لقسم الذكاء الاصطناعي	15	%30
ضرورة تطوير أقسام مناسبة لتطبيق الذكاء الاصطناعي	13	%26
ضرورة إقرار قوانين حديثة ورادعة	8	%16
تطوير بنية تحتية مناسبة لحداثة تطبيقات الذكاء الاصطناعي	11	%22
مراعاة سرية وخصوصية المعلومات من الطواقم العاملة	2	%4
التعاون والتنسيق بين الوزارة والمؤسسات الأخرى العاملة في مجال الذكاء الاصطناعي	6	%12
الاطلاع على تجارب الدول السابقة في مجال تطبيق الذكاء الاصطناعي وملاحقة مرتكبي الجرائم الإلكترونيّة	1	%2

يتضح لنا من الجدول أعلاه أن هناك أكثر من إجابة مُتاحة للمبحوثين، حيث أظهرت النتائج كما في الجدول أعلاه أن غالبيّة إجابات المبحوثين تمركزت حول ضرورة توفير أجهزة الذكاء الاصطناعي لتتبع مرتكبي الجرائم الإلكترونيّة وملاحقتهم، حيث حصلت على (36) إجابة بنسبة (72%) وهي نسبة عاليّة، يليها ضرورة تدريب الموظفين وتطوير مهاراتهم وقدراتهم في التعامل مع برامج الذكاء الاصطناعي، فقط حصلت على (27) إجابة، يليها ضرورة توفير كوادر متخصصة في مجال الذكاء الاصطناعي فقد حصلت على (27) إجابة بنسبة (54%)، بالإضافة إلى ضرورة تخصيص موازنات مآليّة مخصصة لقسم الذكاء الاصطناعي حيث حصلت على (15) إجابة بنسبة (30%)، وضرورة تطوير أقسام مناسبة لتطبيق الذكاء الاصطناعي، فقد حصلت على (13) إجابة، بنسبة (26%)، وضرورة إقرار قوانين حديثة ورادعة حيث حصلت على (8) إجابات بنسبة (16%)، وتطوير بنية تحتية مناسبة لحداثة تطبيقات الذكاء الاصطناعي فقط حصلت على (11) إجابة بنسبة (22%)، بالإضافة إلى مراعاة الطواقم العاملة سرية المعلومات وخصوصيتها، فقد حصلت على (2) إجابة بنسبة (4%)، وضرورة التعاون والتنسيق بين الوزارة والمؤسسات الأخرى العاملة في مجال الذكاء

الاصطناعي، حيث حصلت على (6) إجابات بنسبة (12%)، بالإضافة إلى الاطلاع على تجارب الدول السابقة في مجال تطبيق الذكاء الاصطناعي وملاحقة مرتكبي الجرائم الإلكترونيّة فقد حصلت على (1) إجابة بنسبة (2%).

4.3.4 النتائج المُتعلقة بأكثر الجرائم المكتشفة بتطبيقات الذكاء الاصطناعي:

في إطار إجابة الدراسة على السؤال "ما أكثر الجرائم الإلكترونيّة التي تقوم تطبيقات الذكاء الاصطناعي في الوزارة باكتشافها؟"، تمّ احتساب التكرارات والنسب المئويّة وجاءت النتائج كما في الجدول رقم (9.4).

جدول رقم (9.4): التكرارات والنسب المئويّة لإجابات المبحوثين حول بأكثر الجرائم المكتشفة من الوزارة باستخدامها لتطبيقات الذكاء الاصطناعي

ما أكثر الجرائم الإلكترونيّة التي تقوم تطبيقات الذكاء الاصطناعي باكتِشافها في الوزارة؟	التكرارات	النسبة المئويّة %
جرائم الاختراق	39	%78
الفايروسات	18	%36
التهديدات والابتزاز	12	%24
البريد الوارد	8	%16
جرائم زراعة الملفات المشبوهة	1	%2
لا يوجد	7	%14

يتضح لنا من الجدول أعلاه أن هناك أكثر من إجابة مُتاحة للمبحوثين، حيث يتضح لنا أن أكثر الجرائم التي تقوم تطبيقات الذكاء الاصطناعي باكتشافها في الوزارة هي جرائم الاختراق حيث حصلت على (39) إجابة من أصل (50) بنسبة (78%)، وهي الأعلى نسبة بين الجرائم، يليها جرائم الفايروسات حيث حصلت على (18) إجابة بنسبة (36%)، ثم جرائم التهديدات والابتزاز حيث حصلت على (12) إجابة بِنسبة (24%)، يليها البريد الوارد حيث حصلت على (8) إجابات بِنسبة (16%)، بالإضافة إلى جرائم زراعة الملفات المشبوهة التي حصلت على (1) إجابة، في حين بلغ عدد الإجابات بعدم وجود جرائم تكتشفها تطبيقات الذكاء الاصطناعي (7) إجابات بنسبة (14%).

4.4 نتائج المحور الرئيسي الثالث المُتعلق بمُعوّقات تطبيق الذكاء الاصطناعي في الحد من ممارسة الجرائم الإلكترونيّة:

نتائج تحليل إجابات المبحوثين حول الأسئلة ذات العلاقة بالمُعوقات التي تواجه تطبيق الذكاء الاصطناعي في الحد من ممارسة الجرائم الإلكترونيّة، تستعرضها الدراسة فيما هو آت:

1.4.4 النتائج المُتعلقة بتطبيق الوزارة للذكاء الاصطناعي في الحد من الجرائم الإلكترونيّة.

في إطار إجابة الدراسة على السؤال البحثي "هل هناك معوقات تواجه تطبيق الوزارة للذكاء الاصطناعي في الحد من الجرائم الإلكترونيّة؟"، تمّ احتساب التكرارات والنسب المئويّة وجاءت النتائج كما في الجدول رقم (10.4).

جدول رقم (10.4): التكرارات والنسب المئويّة لإجابات المبحوثين حول المُعوقات التي تواجه تطبيق الوزارة للذكاء الاصطناعي في الحد من الجرائم الإلكترونيّة

هل هناك معوقات تواجه تطبيق الذكاء الاصطناعي في الحد من ممارسة الجريمة الإلكترونيّة في الوزارة؟	العدد	النسبة المئويّة %
نعم	50	%100
لا	0	%0

تظهر نتائج الجدول أعلاه أن هناك مُعوقات تواجِه تَطبيق الذكاء الاصطِناعي في الحد من ممارسة الجريمة الإلكترونيّة في الوزارة حيث أجمع جميع أفراد مجتمع الدراسة البالغ عددهم (50) بنسبة (100%) على وجودها.

2.4.4 النتائج المتعلقة بترتيب المُعوقات التي تواجه تطبيق الوزارة للذكاء الاصطناعي في الحد من الجرائم الإلكترونيّة.

في إطار إجابة الدراسة على السؤال البحثي "حول ترتيب والمُعوقات التي تواجه تطبيق الوزارة للذكاء الاصطناعي في الحد من الجرائم الإلكترونيّة حسب الأهميّة"، تمّ احتساب التكرارات والنسب المئويّة وجاءت النتائج كما في الجدول رقم (11.4).

جدول رقم (11.4): التكرارات والنسب المئويّة لإجابات المبحوثين حول ترتيب المُعوقات التي تواجه تطبيق الوزارة للذكاء الاصطناعي في الحد من الجرائم الإلكترونيّة حسب الأهميّة

الترتيب	رتب/ي المُعوقات التي تواجِه تَطبيق الذكاء الاصطِناعي في الحد من ممارسة الجريمة الإلكترونيّة في الوزارة حسب الأهميّة؟	العدد	النسبة المئويّة %
الأول	الاحتلال الإسرائيلي	22	%44
الثاني	ضعف البنيّة التحتيّة	16	%32
الثالث	ندرة المبرمجين والميزانية الماليّة	15	%30
الرابع	قلة الأبحاث	7	%14
الخامس	نطاق عمل المؤسسة	7	%14
السادس	عدم كفاية قاعدة البيانات	9	%18
السابع	عدد الكادر العامل	10	%20
الثامن	الوضع السياسي	7	%14
التاسع	جنس الكادر	36	%72

من خلال إجراء التحليل لنتائج أسئلة المقابلات فقد وضعَ المبحوثون في المرتبة الأولى حسب الأهميّة الاحتلال الإسرائيلي حيث حصلت على (22) إجابة من أصل (50) بنسبة (44%)، يليها في المرتبة الثانية ضعف البنيّة التحتيّة، حيث حصلت على (16) إجابات، بنسبة (34%) وجاءت في المرتبة الثالثة ندرة المبرمجين والميزانيّة الماليّة فقد حصلت على (15) إجابة بنسبة (30%)، وأما في المرتبة الرابعة فقد حصلت فيها قلة الأبحاث على (7) إجابات بنسبة (14%)، في حين أظهرت النتائج أن خامس المُعوقات التي تواجِه تَطبيق الذكاء الاصطِناعي في الحد من ممارسة الجريمة الإلكترونيّة في الوزارة من حيث الأهميّة هو نطاق عمل المؤسسة حيث حصلت على (7) إجابات بنسبة (14%)، أما عدم كفاية قاعدة البيانات فقد احتلت حسب وجهة نظر المبحوثين المرتبة السادسة بنسبة (18%)، في حين حصل عدد الكادر بنسبة (20%) حيث اختارها (10) من أفراد المجتمع ليكون الخيار السابع في المُعوقات التي تواجِه تَطبيق الذكاء الاصطِناعي في الحد من ممارسة الجريمة الإلكترونيّة في الوزارة، وأما المرتبة الثامنة فقد حصلت عليها فقرة الوضع السياسي بنسبة (14%)، حيث اختارها (7) من أفراد المجتمع، وأجمع (36) من المبحوثين على أن جنس الكادر في المرتبة الأخيرة، وفي ذيل الترتيب بنسبة (72%) أي أن جنس الكادر لا يؤدي دورًا في المُعوقات التي تواجِه تَطبيق الذكاء الاصطِناعي في الحد من ممارسة الجريمة الإلكترونيّة في الوزارة حسب الأهميّة.

3.4.4 النتائج المتعلقة بطرق التغلب على المُعوقات التي تواجه تطبيق الوزارة للذكاء الاصطناعي في الحدّ من الجرائم الإلكترونيّة.

في إطار إجابة الدراسة على السؤال البحثي "حول طرائق التغلب على المُعوقات التي تواجه تطبيق الوزارة للذكاء الاصطناعي في الحد من الجرائم الإلكترونيّة"، تمّ احتساب التكرارات والنسب المئويّة وجاءت النتائج كما في الجدول رقم (12.4).

جدول رقم (12.4) التكرارات والنسب المئويّة لإجابات المبحوثين حول طرائق التغلب على المُعوقات التي تواجه تطبيق الوزارة للذكاء الاصطناعي في الحدّ من الجرائم الإلكترونيّة

ما طرائق التغلب على هذه المُعوقات والصعوبات؟	العدد	النسبة المئويّة %
العمل على تطوير البنيّة التحتيّة	34	%68
العمل على توفير كوادر متخصصة وذات كفاءة عاليّة في مجال التعامل مع برامج الذكاء الاصطناعي	26	%52
العمل على توفير إمكانيات ماليّة من الدول المانحة والمؤسسات الداخلية والخارجية وتخصيصها حول كل ما يتعلق بتطبيق الذكاء الاصطناعي	26	%52
العمل على تدريب الموظفين وإعطائهم دورات وورشات عمل فعّالة.	24	%48
العمل على دعم الأبحاث والدراسات ذات العلاقة بالذكاء الاصطناعي وزيادتها وتتبع مرتكبي الجرائم الإلكترونيّة.	8	%16

يتضح من الجدول أعلاه أن أهم طرائق التغلب على المُعوقات التي تواجه تطبيق الذكاء الاصطناعي في الحد من ممارسة الجريمة الإلكترونيّة العمل على تطوير البنية التحتية، فقد حصلت على (34) إجابة بنسبة (68%)، يليها توفير كوادر متخصصة وذات كفاءة عاليّة في مجال التعامل مع برامج الذكاء الاصطناعي، حيث حصلت على (26) إجابة بنسبة (52%)، وأما فيما يخص توفير إمكانيات ماليّة من الدول المانحة والمؤسسات الداخلية والخارجية وتخصيصها حول كل ما يتعلق بتطبيق الذكاء الاصطناعي فقد حصلت على (26) إجابة أي بنسبة (52%)، وأما أهمية إجراء تدريبات ودورات وورشات عمل فعّالة للموظفين فقد حصلت على (24) إجابة بنسبة (48%)، في حين حصل العمل على دعم الأبحاث والدراسات ذات العلاقة بالذكاء الاصطناعي وزيادتها، وتتبع مرتكبي الجرائم الإلكترونيّة على (8) إجابات بنسبة (16%).

4.4.4 النتائج المُتعلقة باتجاهات المبحوثين حول العلاقة بين المتغيرات الديمغرافية وبين ممارسة الجريمة الإلكترونيّة:

نتائج إجابة السؤال البحثي:"ما إتجاهات المبحوثين حول العلاقة بين الخصائص الديمغرافية (الجنس، مكان السكن، عدد أفراد الأسرة، التحصيل العلمي، العمر) وبين ممارسة الجريمة الإلكترونيّة"؟

تشير نتائج إتجاهات المبحوثين إلى أن هناك علاقة بين المتغيرات الديمغرافية (الجنس، عدد أفراد الأسرة، مكان السكن، التحصيل العلمي، العمر) وارتكاب الجريمة الإلكترونيّة، لعل من أهم تلك المتغيرات العمر، فكلما قل العمر زادت نسبة الإقبال على ارتكاب الجرائم الإلكترونيّة، حيث حصلت على (36) إجابة من أصل (50) بنسبة (72%)، وأما فيما يخص الفئات العمرية فقد أظهرت النتائج أن الفئات الأصغر سنًّا هي الأكثر ميلًا لارتكاب الجرائم الإلكترونيّة، وفيما يخص مكان السكن حصلت على (27) إجابة بنسبة (54%)، أي أن الثقافة المرتبطة بمكان السكن تؤدّي دورًا في ارتكاب الجرائم الإلكترونيّة، وأما متغير التحصيل العلمي فقد حصل على (27) إجابة، بنسبة (54%) فزيادة التعليم والوعي والمعرفة بمثل هذه الجرائم لا شك أنَّ لها دورًا في الحد من الجرائم والكشف عنها أيضًا، وأما متغير الجنس فقد حصل على (26) إجابة بنسبة (52%) فالذكور حسب رأي المبحوثين أكثر ميلًا لارتكاب الجرائم الإلكترونيّة من الإناث، أمّا متغير عدد أفراد الأسرة فقد حصلت على (9) إجابات بنسبة (18%)، وهذا يدل على أنه كلما زاد عدد أفراد الأسرة قلت المتابعة وزادت المُتطلبات الماليّة زادت الجرائم الإلكترونيّة.

5.4.4 النتائج المتعلقة بجهات أخرى تطبق الذكاء الاصطناعي في الحد من ممارسة الجريمة الإلكترونيّة:

في إطار إجابة الدراسة على السؤال البحثي "هل لديك علم بمؤسسة أو وزارة أخرى تستخدم تطبيق الذكاء الاصطناعي في الحد من ممارسة الجريمة الإلكترونيّة؟"، تمّ احتساب التكرارات والنسب المئويّة وجاءت النتائج كما في الجدول رقم (13.4).

جدول رقم (13.4): التكرارات والنسب المئويّة لإجابات المبحوثين حول مؤسسات أو وزارات أخرى تستخدم تطبيق الذكاء الاصطناعي في الحد من ممارسة الجريمة الإلكترونيّة

هل لديك علم بمؤسسة أو وزارة أخرى محليّة تستخدم تطبيق الذكاء الاصطناعي في الحدّ من ممارسة الجريمة الإلكترونيّة؟	العدد	النسبة المئويّة %
وزارة الداخليّة	40	%80
نيابة الجرائم الإلكترونيّة	13	%26
الأجهزة الأمنيّة	6	%12
شركة جوال	3	%6
شركة الأمن المعلوماتي	2	%4

أظهرت نتائج الجدول أن جميع أفراد المجتمع لديهم علم بمؤسسة أو وزارة أخرى محليّة تستخدم تطبيق الذكاء الاصطناعي في الحد من ممارسة الجريمة الإلكترونيّة، لعل أهم مؤسسة تستخدمه هي وزارة الداخلية فقد بلغ عدد الإجابات (40) من أصل (50) بنسبة (80%)، يليها نيابة الجرائم الإلكترونيّة، فقد بلغ عدد الإجابات (13) بنسبة (26%)، يليها الأجهزة الأمنيّة حيث بلغ عدد الإجابات (6) بنسبة (12%)، إضافة إلى شركة جوال فقد بلغ عدد الإجابات (3) بنسبة (6%)، في حين بلغ عدد الإجابات لشركة الأمن المعلوماتي (2) بنسبة (4%).

6.4.4 النتائج المُتعلقة بالتعاون بين الوزارة والمؤسسات المحليّة والدوليّة في مجال الجرائم الإلكترونيّة:

في إطار إجابة الدراسة على السؤال البحثي "هل هناك تعاون وتنسيق بين الوزارة والمؤسسات المحليّة والدوليّة العاملة في مجال الجرائم الإلكترونيّة"؟، تم احتساب التكرارات والنسب المئويّة وجاءت النتائج كما في الجدول رقم (14.4).

جدول رقم (14.4): التكرارات والنسب المئويّة لإجابات المبحوثين حول التعاون بين الوزارة والمؤسسات المحليّة والدوليّة في مجال الجرائم الإلكترونيّة:

هل هناك تعاون وتنسيق بين الوزارة والمؤسسات المحليّة والدوليّة العاملة في مجال الجرائم الإلكترونيّة؟	العدد	النسبة المئويّة %
يوجد تعاون	46	%92
لا يوجد تعاون	4	%8
المجموع	50	%100

أكَّدَ جميع أفراد مجتمع الدراسة على وجود تعاون وتنسيق بين الوزارة والمؤسسات المحليّة والدوليّة العاملة في مجال الجرائم الإلكترونيّة والحد منها، لعل من أهم هذا التعاون التنسيق بين الوزارة والشرطة الفلسطينية ونيابة الجرائم الإلكترونيّة، إضافة إلى الاتصال والتواصل من فريق فلسطين للاستجابة لطوارئ الحاسوب في حال وقوع هجمات إلكترونيّة، فقد بلغت عدد الإجابات (46) من أصل (50)، أي بنسبة (92%) من المبحوثين، ويبدو ذلك جلياً من خلال فريق الاستجابة للطوارئ وهو فريق تابع لوحدة الأمن المعلوماتي يعمل على التدخل السريع في حال حدوث طارئ.

الفصل الخامس

مناقشة النتائج والتوصيات

1.5 مقدمة:

في هذا الفصل سيتم مناقشة نتائج الدراسة التي تمّ التوصل إليها بوصفها إجابةً عن الأسئلة التي طرحت، وهي تمثل مشكلة الدراسة والتوصل إلى عدد من الاستنتاجات التي على ضوئها وُضِعَتْ توصيات الدراسة.

2.5 مناقشة النتائج:

يمكن تلخيص نتائج الدراسة على النحو الآتي:

1.2.5 مناقشة نتائج المحور الرئيسي الأول: من وجهة نظرك/كِ هل هناك دور للذكاء الاصطناعي في الكشف عن الجريمة الإلكترونيّة والحد منها؟ وتفرعاته:

بعد تحليل نتائج المقابلات اتضح وجود دور للذكاء الاصطناعي في الحد من ممارسة الجريمة الإلكترونيّة، في ضوء ما أشار إليه المبحوثون في إجاباتهم، فقد أجمع المبحوثون على أن للذكاء الاصطناعي دورًا مهمًّا وقويًّا في مواجهة الجريمة الإلكترونيّة، فهذه التطبيقات تتكون من خورازميات التصنيف التي لها القدرة على تصنيف البيانات وخوارزميات التنبؤ، ثمّ تحليلها، وهي تمتاز بالاستباقية وتوقع الجريمة قبل حدوثها، تتفق هذه النتيجة مع دراسة ايكينيم (Ekanem, 2019) بعنوان "تطبيق الذكاء الاصطناعي كآليّة لمكافحة الجريمة في نيجيريا"، حيث أشارت إلى أهمية الذكاء الاصطناعي في مواجهة الجريمة الحاصلة في الفضاء الإلكتروني، كما أشارت إلى أن استخدام تطبيقات الذكاء الاصطناعي وبرامجه في مواجهة الجرائم أدى إلى نتائج واضحة وفعّالة على أرض الواقع، ودراسة (لخضر ونفيسة، 2018م) بعنوان "دور الذكاء الاصطناعي في مواجهة الجريمة الإلكترونيّة" حيث أشارت أن لهذه النظم دورًا في مواجهة الجرائم الإلكترونيّة وتحقيق الأمان والراحة للإنسان وحرية في

استخدام الإنترنت، كما أن لديها القدرة على التنبؤ والتحليل والتصنيف وفيما بعد اتخاذ القرار لصد الهجمات الإلكترونيّة، إضافة الى أن النتيجة تتفق كذلك مع دراسة كل من تيواري وماهيشواري وبال (Tiwari & Maheshwary & Pal, 2018) بعنوان "تطبيق الذكاء الاصطناعي في الحد من هجمات الجرائم الإلكترونيّة"، حيث أشارت أن لتطبيقات الذكاء الإصطناعي وأنظمته إمكانات كبيرة وذات فعآليّة عآليّة في التقليل من الهجمات التي تتعرض لها الشبكات الإلكترونيّة.

هذا ما يفسر إقبال المجتمعات في الآونة الأخيرة إلى تطبيق الذكاء الاصطناعي وبرامجه في مجال الحماية الأمنية، وحماية أنظمتها من الاختراقات والهجمات، بالإضافة إلى توظيفه في مواقع التواصل الاجتماعي من الشركات الكبرى القائمة على هذه المواقع؛ لما أثبتته هذه النظم من فاعلية في مواجهة الجرائم التي تحصل في الفضاء الإلكتروني والحد منها، فاليوم هو المتحكم في العالم واتجاهاته التكنولوجيّة، إن تطبيق الذكاء الاصطناعي في العالم الافتراضي يوفر بيئة سليمة وآمنة غير معرضة للاختراقات من المجرمين المتصيدين للضحايا؛ نظرًا لقدرة هذه التطبيقات على الكشف عن هوية المجرم وتحديد موقعه والعثور عليه والحصول على مجريات الأحداث كافَّةً، وخط سير الجاني على الشبكة، حيث إنَّ الفرص أمام الجاني تنعدم لارتكاب الجريمة الإكترونية، بحكم أنَّ هذه التطبيقات صممت خصيصًا للبحث والكشف عن أي مسلك غير طبيعي يحصل في إطار الشبكة، وذلك بإدخال كم هائل من البيانات والمعلومات المتعلقة بمختلف أنواع الجرائم التي من المحتمل أن تحصل؛ ما يكسبها المعرفة والمهارة للتعرف على أي جريمة تحصل داخل الشبكة الإلكترونيّة، ونظرًا للتغيرات الأخيرة التي تحصل في العالم التي أدت بالبشر الى الانتقال من العالم الواقعي إلى العالم الافتراضي نتيجة انتشار جائحة كورونا وما حصدته هذه الفترة من زيادة في الجرائم الإلكترونيّة المرتكبة، هنا تتضح أهميّة تفعيل دور هذه التطبيقات والبرامج الذكيّة في الكشف عن الجرائم وموقع الجناة خاصة أن ضعف الإمكانات التكنولوجيّة في فلسطين وعدم قدرة الجهات المختصة في كثير من الأحيان على اكتشاف موقع الجاني أصبحت تشكل مصدر راحة وأمان للجاني، هذا ما يسمى حسب نظريات علم الجريمة الفرصة.

أما فيما يخص ارتباط تطبيق الذكاء الاصطناعي بقبوله في المجتمع فقد أجمع (34) من المبحوثين أن تطبيق الذكاء الاصطناعي لا يرتبط بقبوله في المجتمع على أساس أن أفراد المجتمع ليسوا ملمين بالتطورات التكنولوجيّة الحديثة، فهذا النوع من التكنولوجيا يفضل أن يترك لجهات الاختصاص. هذا من جهة ومن جهة أخرى تم تصميم تطبيقات الذكاء الاصطناعي لتحقيق الرفاهية والأمان والحمايّة لأفراد المجتمع، كما أنها تساعد على تقليل الجهد والوقت في إتمام مختلف الأعمال بالشكل الّذي يجب أن تقوم به، إن هذه النتيجة منطقيّة؛ لأن تطبيقات الذكاء الاصطناعي والبرامج التكنولوجيّة الحديثة اخْتُرِعَتْ؛ لتسهيل حياة الإنسان، والارتقاء بمستوى المجتمعات؛ لمواكبة التطورات التي تمر بها

الدول، فهذه التطبيقات لها أدوار مهمة وواضحة في إنجاز الأعمال وإتمامها بسرعة ودقة عآليّة، كما لديها خاصية مهمة، وهي التنبؤ ليس فقط في مجال الجريمة الإلكترونيّة، إنما في مختلف الأعمال التي توضع في سبيل إنجازها، ومن ثَمَّ فإن الذكاء الاصطناعي وما يتم الحصول عليه من نتائج إيجابية على أرض الواقع يُعَدُّ من أهم الأسباب التي تجعل من رفض المجتمع لتطبيقه ليس شرطًا أساسيًّا.

ومن الطبيعي أن يرفضَ أفراد المجتمع إدخال نوع جديد من التكنولوجيا التي لم يسبق لهم أن سمعوا عنها، إضافة إلى أن الكثير من أفراد المجتمع ليسوا على اطِّلاع بالتكنولوجيا، أو على فهم ودراية بها وبكيفية استخدامها، وهذا أمر طبيعي فهي تكنولوجيا حديثة أُدْخِلَتْ إلى العالم فتلك التطبيقات تتقاطع مع عمل الجهات المختصة التي لديها القدرة والإمكانات العلميّة المكتسبة، من خلال الخبرات المتراكمة للتعامل معها وتوظيفها في مصلحة المواطن، ناهيك عن أنه يمكن تفادي انتهاك الذكاء الاصطناعي لخصوصية المعلومات وبيانات المواطنين من خلال الحفاظ على السرية التامة، وعدم الإدلاء بأي معلومة تتعلق بأي مواطن من الطواقم العاملة في مجال الذكاء الإصطناعي.

وتستخدم مواقع التواصل الاجتماعي الذكاء الاصطناعي دون الحاجة إلى أذونات المستخدمين، هذا ما أشارت إليه (صحيفة سي إن إن، 2019م) من خلال موقعها الرسمي بتاريخ (01\05\2019)، حيث أكدت أنه يتم مضاعفة استخدام الأنظمة والبرامج الذكيّة ذات العلاقة بالذكاء الاصطناعي؛ للحد من المحتويات الضارة والمنافية للأخلاق على الشبكات الإلكترونيّة، كما تقوم هذه الأنظمة بحذف هذه المحتويات بشكل تلقائي من مواقع التواصل الاجتماعي، بالإضافة إلى تدريب تطبيقات الذكاء الاصطناعي على فرز الفيدوهات كافّةً، وتصنيفها حول ما إذا كانت تحتوي على مقاطع غير أخلاقية أم لا، كما أشارت (صحيفة ميتا ال، 2020م) على موقعها الرسمي بتاريخ (29\11\2020) أن شركة فيسبوك من خلال تطبيقها لتقنيات الذكاء الاصطناعي أسهمت في حماية الضحايا من الوقوع فريسة للجناة الإلكترونين، وعملت على تدريب هذه التطبيقات من خلال التكرار في الصور ومقاطع الفيديو، وتحليل الكلام والكتابة إضافة للقطات الشاشة؛ ما يمنحها القدرة على التنبؤ بشكل أكبر وأدق وكشف المسلكيات المشبوهة التي تحصل داخل الشبكة.

وفيما يخص إمكانية الذكاء الاصطناعي في الحد من الجريمة الإلكترونيّة وردع الجناة، فقد أظهرت نتائج الدراسة –من خلال ما أجمع عليه المبحوثون– أن الذكاء الاصطناعي يتمتع بقدرة عآليّة في الكشف عن الجريمة الإلكترونيّة، بسرعة كبيرة، وبدقة عآليّة، ولا مجال للخطأ فيها، كما أن التأثير في نفسيّة المجرم بوجود تطبيقات لها القدرة على اكتشاف كل مسلك منحرف أو غير طبيعي على الشبكة يُشكل للجاني رادعًا وخوفًا من التعرض للمساءلة القانونية في ظل وجود قوانين صارمة تجرم مرتكبي الجرائم الإلكترونيّة.

نستنتج من هذه النتيجة أن ردع المجرمين بالوسائل التكنولوجيّة الحديثة التي بُرْمِجَتْ للكشف عن الجرائم تسهم بدرجة كبيرة في التأثير في نفس الجاني، وزرع نوع من التردد والخوف والقلق حيال ارتكاب أي مسلك منحرف في الفضاء الإلكتروني، من هنا تتوضح لنا فكرة نظريّة الردع التي ترى أن عقاب المجرم والتأثير عليه تؤدي إلى شعوره بالخوف، وتقلل من نسبة انخراطه في ارتكاب المسلكيات غير المشروعة، والمخالفة للعادات والتقاليد في المجتمع، حيث إن الردع يتمثل في جانبين: الجانبُ الأول الردع الخاص، المتمثل في نفسية الجاني وتردده وخوفه من ارتكاب الجريمة؛ ما يؤدي إلى عدم التفكير بأي مسلك مخالف في الشبكة الإلكترونيّة، فحالة الخوف والتردد التي يعيشها المجرم نتيجة الإمكانات التي تتمتع بها هذه التطبيقات واكتشاف تلك المسكليات وتسجيلها وتحويلها إلى دليل ملموس تؤدي إلى إدانته في النيابة والمحكمة، هذا من شأنه أن يدفع الجاني إلى الابتعاد عن هذه المسلكيات. أمّا الجانبُ الثاني (الردع العام) فإنه يعني انتقال ذلك للجناة الآخرين المقبلين على ارتكاب الجريمة الإلكترونيّة، فعندما يرى الآخرون أن هذه التطبيقات موجودة، وجاءت بنتائج إيجابية في الكشف عن المجرم فإنَّها تشكل رادعًا لهم؛ خوفًا من التعرض للكشف والعقاب، وذلك بغرس فكرة قدرة هذه التطبيقات –من خلال المستشعرات– التعرف على معلومات الجاني، إضافة إلى تسجيل كل حركة يقوم بها على الشبكة الإلكترونيّة وأن ذلك يشكل دليلًا على الجريمة غير المقبولة اجتماعيًّا؛ ما يعني التعرض لأقصى العقوبات من الجهات المختصة والمنفذة للقانون، إن تحكم هذه التطبيقات في الشبكة يؤدي إلى التقليل –بنسبة كبيرة– من ارتكاب الجرائم في الفضاء الإلكتروني التي أصبحت في الآونة الأخيرة منصة لكل من يرغب في القيام بأي مسلك مخالف للأخلاق والقوانين والعادات والتقاليد، هذا ما شهدته فترة انتشار الجائحة التي أدت الى زيادة نسبة استخدام التكنولوجيا والعالم الافتراضي، كما أن إفشال الهجمات الإلكترونيّة التي يقوم بها المجرمون على الفور واكتشافها تعمل على غرس نوع من اليأس، فالشعور الذي يتولد لدى الجاني أنه لا فرصة له في نجاح مشروعه الإجرامي يعزز لديه الابتعاد عن هذا النوع من الجرائم، وبلا عودة، هنا نلاحظ أنَّ دور تطبيقات الذكاء الاصطناعي فعّالة وقويّة في كشف الجاني من جهة، والضبط والتأثير في نفسيته من جهة أخرى، هذا يدفع مستخدمي الشبكة الإلكترونيّة وشبكات التواصل الاجتماعي إلى استخدامها بالشكل الصحيح بعيدًا عن إلحاق الضرر والأذى بالآخرين.

كما يمكن تفسير النتيجة السابقة في ضوء نظريّة الفرصة التي ترى أن الأفراد في المجتمع يلجأون إلى ارتكاب الجريمة الإلكترونيّة في ظل الفرص المتاحة لهم، باتباع الأساليب غير المشروعة مع توفُّر الرغبة في نفس الجاني، وعليه فإنَّ الفرص التي يغتنمها هي أساس نجاحه أو فشله، لذا وبناءً على ما سبق عندما يتم تطبيق برامج الذكاء الاصطناعي ونظمه سواء في مواقع التواصل الاجتماعي لحماية الضحايا أم في المؤسسات والبنوك والوزارات التي تكون عرضة أكثر للجرائم والسرقة، إضافة الى

ضرورة حفاظ هذه المؤسسات على سريّة المعلومات والبيانات الخاصة بها، هذا يساعد في انعدام الفرص أمام الجناة في استغلال الثغرات الأمنيّة، واختراق الجدار المتين الذي يحمي الشبكة الإلكترونيّة نظرًا للقدرات العآليّة التي تتمتع بها، تلك القدرات التي تعمل على تعميق الشعور لدى الجاني.

إن ارتكاب أي مسلك غير مشروع في الفضاء الإلكتروني يجعله عرضة للسجن والمساءلة القانونية، حيث تعمل هذه التطبيقات على إضعاف ثقة الجاني بنفسه؛ لأنه سيكون بحاجة إلى مواجهة تطبيقات الذكاء الاصطناعي التي تصدُّ أي هجمات إلكترونيّة، وتتخلَّص من أي مسلكيات مسيئة تحصل بشكل تلقائي بناءً على الخبرة والمهارة التي تمتلكها في هذا المجال، كما أنها تترك مشاعر إيجابية في نفوس أفراد المجتمع وتعزّز لديهم تقبل هذه التطبيقات، فالأثر الذي تتركه هذه التطبيقات في نفوس أفراد المجتمع قد تكون السبب الرئيس في السماح بقبولها في المجتمع وتراجع الجناة عن تعريض الناس للأذى والضرر، هذا ما يفسر دور الذكاء الاصطناعي وبرامجه في الحد من الجريمة الإلكترونيّة.

أما فيما يخص جانب إنفاذ القانون أكدت نسبة من إجابات المبحوثين بلغت (30%) أن الذكاء الاصطناعي وحده لا يكفي لردع المجرم، إنما هناك ضرورة مُلِحَّة لفرض القوانين الصارمة التي من شأنها أن تكون مُكمِّلًا لتطبيقات الذكاء الاصطناعي في ردع المجرم، فالجاني إذا لم يتعرض للعقوبة الصارمة والحبس بعد أن تكتشفه برامج الذكاء الاصطناعي فإن ذلك لا يجدي نفعًا، حيث إنَّ وجود قوانين تُجرِّم الأفعال المرتكبة في الفضاء الإلكتروني أمر مهمٌّ وضروري جدًّا، ومرتبط –بشكل مباشر– في ردع المجرم، وعدم إقباله على ارتكاب الجريمة الإلكترونيّة، تتفق هذه النتيجة مع نظريّة الوصم التي ترى أن ارتكاب الفرد لمسلكيات مخالفة لعادات المجتمع وتقاليده فإنها تَصِمُهُ ببعض الصفات التي تظلُّ ملاصقة له؛ لما يتعرض له من نَبْذِ أفراد المجتمع بعد اكتشافه، ومعاقبته، وسجنه، ولا يقتصر ذلك على الجاني فقط، إنما يتعداها لتشمل عائلته، وتعرضها للنظرة الدونية ومضايقات أفراد المجتمع، إضافة الى إلقاء اللَّوْم على عائلة الجاني؛ بسبب ضعف التنشئة الاجتماعية وضعف الرقابة الأبوية التي ولَّدَتْ لدى الجاني الضبط الاجتماعي المنخفض، تتقاطع هذه النتيجة مع النظريّة اللامعياريّة (الأنومي)، فعندما يتعرض الفرد لِنَبْذ الجتمع والبيئة المحيطة وانتقادهما؛ بسبب قيامه بمسلكيات منحرفة وغير مقبولة في المجتمع يؤدي ذلك إلى استمراره في ممارسة السلوكات المنحرفة نتيجة الضغوطات المجتمعية التي يتعرض لها، ونتيجة عدم قدرة الأهل والمجتمع على ضبط الفرد ضمن عادات المجتمع وتقاليده وأعرافه.

إن ما يؤكد على أهمية القانون في الحد من ممارسة الجريمة الإلكترونيّة، قيام دولة فلسطين بإصدار قانون الجرائم الالكترونيّة رقم (16) لسنة (2017) بشأن الجرائم الإلكترونية، وقرار بقانون رقم (10)

لسنة (2018) بشأن الجرائم الإلكترونية الخاص بالتعديل على قانون رقم (16) لسنة (2017)، فالتشريع السابق كان يُجرّم في الغالب المخالفات ضدّ الأصول والهويّات الماديّة دون الافتراضية، وبعد اعتراض مؤسسات المجتمّع المدني(المدنية والحقوقية) على الثغرات في الأساس القانوني للملاحقة القضائية كونها تمّس بالحقوق والحريات للمواطنين تمّ تداركه في القرار بالقانون (10) لسنة (2018)، وفي هذا المجال يرى (عبد الباقي، 2018) أن الإطار القانوني الموجود في فلسطين قبل إصدار قانون الجرائم الإلكترونية ليس كافياً لمكافحة إساءة استخدام الإنترنت والبيانات ونُظُم الكمبيوتر، لهذا لا بد من تطوير في تعريف الجرائم الرقمية، والدليل على ضرورة التطوير أنّ الشرطة الفلسطينية تشاركه هذا الرأي مُؤكِّدة أن القانون الجديد رقم (10) لسنة (2018) سيُمكِّن من التجريم الافعّال والملاحقة القضائية وجمع الأدلّة المُتعلِّقة بالجرائم الرقمية، حيث تمّثلت التعديلات على القانون رقم (16) لسنه (2017) بإلغاء النصوص العامة والفضفاضة بشكل صريح مثل المادة (15) لعدم استيفائها الشروط الاجرائية القانونية، وتحديد النائب العام وليس النيابة من يتخذ القرار بناءاً على قرار من المحكمة المختصة بالجرائم الإلكترونية، والمادة (30) والمادة (33) التي تمّنح الصلاحية للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي، ودون أمر من المحكمة المختصة بتفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة وضبط الأجهزة والأدوات والبيانات والمعلومات الإلكترونية، والتحفظ على كامل نظام المعلومات أو أي وسيلة من وسائل تكنولوجيا المعلومات من شأنها أنّ تساعد على كشف الحقيقة دون حضور المتهم أو حيازة الأجهزة لإجراءات التفتيش والضبط، والمادة (34، 40، 46) التي تتعارض مع الاتفاقيات الدولية والعربية بهذا الشأن وغيرها من النصوص التي تمّ تداركها في القانون رقم (10) لسنة (2018).

على أثر هذا القانون قامت النيابة العامة الفلسطينية باستحداث مكتب مكافحة الجرائم المعلوماتية "الإلكترونية"، إذ تمّ تخصيص أعضاء من النيابة العامة كمختصين لمتابعة قضايا الجرائم الإلكترونية وتدريبهم وإعدادهم للتعامل مع هذه الجرائم في كافة النيابات الجزائية في مختلف محافظات الوطن، وتتولى النيابة المختصة كجهة قانونية متابعة الطلبات المتعلقة بالجرائم الإلكترونية بالتعاون مع الشرطة والأجهزة الأمنيّة الأخرى ذات الاختصاص، وتتولى التواصل مع الجهات والمؤسسات والشركات المختصة فيما يتعلق بالجرائم الإلكترونية والاتصالات والحصول على الدليل الفني الالكتروني وربط الجناة فيه (براك وجراده، 2019).

وعلى الرغم مع وجود هذه القوانين الصارمة فيما يخص الجرائم الإلكترونية وما تمّ استحداثه من دوائر خاصة بالجرائم الإلكترونية، فقد أشارت الشرطة الفلسطينية إلى أنّ هناك تزايد في معدلات الجريمة الإلكترونية في فلسطين كما تمّ الإشارة له سابقاً، من هنا ومما سبق يمكننا التأكيد على تكامل كل الجهات مع بعضها بعضًا، فلكل منها دورٌ مُكَمِّلٌ للآخر، وهي ذات ارتباط مباشر بها، فتطبيقات

الذكاء الاصطناعي وظيفتها التوصل إلى موقع الجاني، وتسجيل مجريات الأحداث على الشبكة (إحضار الدليل)، أما دور القضاء والجهات المختصة فهو تنفيذ القانون، وإيقاع أشد العقوبات على الجناة مرتكبي الجرائم الإلكترونيّة؛ لتكون رداعًا للجاني ورادعًا للجناة الآخرين؛ لتجنب تعرضهم للموقف ذاته مرة أخرى، هنا يأتي الدور الأهم للتنشئة الاجتماعية السليمة، فهي المسؤول الأول والأخير عن غرس ثقافة السلام وحب الخير للآخرين، ومراقبة الأبناء؛ لعدم الانخراط والتعامل مع رفاق السوء، مِمَّن لهم تأثير مباشر على الأفراد، عَبْرَ استثارة الميول المنحرفة التي من المحتمل أن تكون موجودة لدى الجاني، هنا يمكن أن نؤكد على هذا التكامل بين الجهات جميعها من خلال النظريّة التكاملية التي ترى أن ممارسة الجريمة والحد منها لا يقف عند عامل واحد أو سبب واحد، وإنما عوامل كثيرة وأسباب متعددة، كذلك الحدّ منها ومكافحتها يحتاج لعدة أطراف وليس لطرف واحد.

2.2.5 مناقشة نتائج المحور الرئيسي الثاني: هل هناك آليات عمل متبعة في استخدام برامج الذكاء الاصطناعي في الوزارة لتتبع الجناة مرتكبي الجرائم الإلكترونيّة؟ ما هي تلك الآليات بشكل دقيق؟ وتفرعاته:

من خلال إجراء التحليل لنتائج المقابلات حول الآليّات المتبعة في الوزارة لتطبيق برامج الذكاء الاصطناعي لتتبع مرتكبي الجرائم الإلكترونيّة فقد أجمع المبحوثون على أن الوزارة لا تتبع آليّات معينة في تطبيق برامج الذكاء الاصطناعي على الرغم من إستخدامها له ولبرامجه، فقد أكد المبحوث في المقابلة رقم (32) أن الوزارة تستخدم الذكاء الاصطناعي لكن دون وجود آليّات محددة، بناءً على ذلك أكد المبحوثون على ضرورة التعاون؛ لطرح مجموعة من الآليات لاتباعها في تطبيق برامج الذكاء الاصطناعي والاستفادة من هذه النظم الحديثة التي تعود بالنفع والفائدة على المجتمع والمؤسسات.

يتضح لنا أن الوزارة تفتقر إلى وجود آليّات واضحة ومحددة لاتباعها في تطبيق برامج الذكاء الاصطناعي؛ إن ما يفسر لنا الضعف في تطبيق تلك البرامج أنها تكنولوجيا حديثة الولادة وضئيلة الانتشار في فلسطين؛ الأمر الذي يتطلب وضع آليات يمكن من خلالها العمل على تطبيق هذه البرامج، حيث أجمع المبحوثون على ضرورة وجود آليّات واضحة ومحددة من أهمها ضرورة توفير أجهزة الذكاء الاصطناعي؛ لتتبع مرتكبي الجرائم الإلكترونيّة وملاحقتهم، وضرورة تدريب الموظفين وتطوير مهاراتهم وقدراتهم في التعامل مع برامج الذكاء الاصطناعي، ضرورة توفير كوادر متخصصة في مجال الذكاء الاصطناعي، بالإضافة إلى تخصيص موازنات مآليّة مخصصة لقسم الذكاء الاصطناعي وتطوير أقسام مناسبة لتطبيق برامجه، وضرورة إقرار قوانين حديثة ورادعة، وتطوير بنيّة تحتيّة مناسبة لحداثة تطبيقات برامج الذكاء الاصطناعي وأنظمته، بالإضافة إلى مراعاة الطواقم العاملة سرية المعلومات وخصوصيتها، وضرورة التعاون والتنسيق بين الوزارة والمؤسسات الأخرى

العاملة في مجال الذكاء الاصطناعي، بالإضافة إلى الاطِّلاع على تجارب الدول السابقة في مجال تطبيق برامج الذكاء الاصطناعي وملاحقة مرتكبي الجرائم الإلكترونيّة.

هذا الأمر يعود بنا إلى ما أكده ايكينيم (Ekanem, 2019) في دراسته بعنوان "تطبيق الذكاء الاصطناعي كآليّة لمكافحة الجريمة" فقد أكد على ضرورة توسيع مجال العمل في تقنيات الذكاء الاصطناعي والعمل على رفع الخبرة والمهارة والكفاءة لدى العاملين، ودراسة (القحطاني، 2014) بعنوان "تطوير مهارات التحقيق في الجرائم المعلوماتيّة"، إذْ أكد على ضرورة الاستفادة من تجارب الدول السابقة وتوفير أجهزة وبرمجيات حديثة؛ لتتبع الجرائم الإلكترونيّة، إضافة لدراسة (البلوي، 2009) بعنوان "التقنيات الحديثة ودورها في ضبط الجريمة"، فقد أكدت على ضرورة إنشاء إدارات وأقسام خاصة وحديثة لاستخدام تقنيات الذكاء الاصطناعي وتكثيف الدورات التكنولوجيّة الحديثة.

يتضح لنا ممّا سبق أن العاملين في وزارة الاتِّصالات بحكم المؤهلات العلميّة الحاصلين عليها في مجال التكنولوجيا والهندسة التكنولوجيّة والبرمجيات، كذلك تصميم البرامج لديهم إمكانية وضع مقترحات لتخطي إفتقار الوزراة لوجود آليّات عمل واضحة لتطبيق برامج الذكاء الاصطناعي، حيث تُعَدُّ الأجهزة والمعدات من أهم الأمور الواجب توفُّرها لدى العاملين في الوزارة؛ من أجل البدء بالخطوات الأولى في تحديد آليّات للعمل من خلالها، فهناك ارتباط وثيق بين وجود هذه التطبيقات في متناول اليد على أرض الواقع والقدرة من خلالها على وضع خارطة للعمل بها، إذ إنَّ هذه الأجهزة والمعدات إلى جانب الخبرة والمؤهلات العلميّة، إضافة الى الدراسات النظريّة تعزز لدى العاملين المعرفة، لكن دون العمل على تطبيقها واستخدامها على أرض الواقع لا تجدي نفعًا، وبانفتاح العالم على بعضه بعضًا، وتسهيل عمليّة الاتصال والتواصل مع الدول الأخرى التي تمتلك مختلف الأجهزة والمعدات يمكن لنا توفير ما تفتقر إليه الوزارة، لكن وبسبب الاحتلال الإسرائيلي الذي يعمل على التضيق على الجانب الفلسطيني لمنع إدخالها إلى الأراضي الفلسيطينة، فهو لا يسيطر فقط على الحدود الجغرافية، إنما يتحكم بالمجريات كافَّةً، ويمنع المجتمع الفلسطيني من الدخول في سلسلة التطورات التكنولوجيّة التي يعيشها العالم اليوم. هذا من جهة، ومن جهة أخرى الكلفة العآليّة لهذه الأجهزة والمعدات، وما يترتب على إحضارها من مخصصات مآليّة مستمرة حيث إنه وبحكم حداثتها تُعَدُّ مكلفة جدًّا، إضافة إلى أنها تحتاج إلى صيانة مستمرة، وتغذية للبيانات والمعلومات؛ ما يستدعي ذلك توفير موازنات مآليّة إضافية تشكل عبئًا على الوزارة، تتفق هذه النتيجة مع دراسة (القحطاني، 2014) بعنوان "تطوير مهارات التحقيق في الجرائم المعلوماتيّة" التي أكدت على ضرورة توفير معدات وأجهزة وبرمجيات حديثة تساعد في الكشف عن الجرائم الإلكترونيّة.

أما فيما يخص توفير كوادر بشرية حاصلة على مؤهلات علميّة في مجال برامج الذكاء الاصطناعي وعلم البيانات، وما تمتلكه من خبرة ومهارة وتحويلها من نظريّة إلى تطبيقية تُعَدُّ من الآليات المهمة

التي يجب اتباعها؛ لتطبيق هذه النظم، وعدم وضعها في يد أشخاص غير مؤهلين فمن الضروري أن يكون هناك كادرٌ كفءٌ لديه الإلمام الكافي لتطبيقها، ناهيك عن ضرورة تدريب العاملين في الوزارة؛ لتفادي الوقوع في أخطاء فنيّة وتقنيّة أثناء تطبيقها، هذا ما أكدت عليه دراسة (العبيدي، 2020) بعنوان "دور الدليل الرقمي في الإثبات الجنائي في النظام السعودي" حيث أكدت على ضرورة استقطاب متخصصين موكل إليهم مهمة متابعة الشبكات الإلكترونيّة والحصول على الأدلة ومجريات الأحداث؛ من أجل مكافحة الجريمة الإلكترونيّة، إن ذلك يساعد على فتح أقسام للذكاء الاصطناعي، من خلالها يمكن اتباع الأساليب الحديثة، واكتساب مزيد من الخبرة والمهارة مع الممارسة المستمرة.

كما أكد المبحوثون على أن توفير مخصصات مآليّة تُعَدُّ من الآليات المهمة التي يجب أخذها بعين الأهميَّة؛ لتطبيق برامج الذكاء الاصطناعي؛ كونها حلقة الوصل بين الأجزاء كافَّة(الأجهزة – الكادر البشري – الصيانة – الدورات)، فكلما زاد الدعم المادي زادت قدرة الوزارة على تطبيق هذه البرامج الذكيّة، لذا يُعَدُّ من أهم الطرائق التي تساعد على تخطي المُعوقات التي تواجه الوزارة، من هنا تأتي أهمية التنسيق بين الوزارة والدول المانحة والمؤسسات المحليّة التي من شأنها أن تؤدّي دورًا أساسيًّا في توفير المال، إضافة إلى أننا لا نستطيع إغفال جانب السرية التامة في الحفاظ على المعلومات والبيانات الشخصيّة في سبيل تطبيق برامج الذكاء الاصطناعي، فهناك علاقة بين السرية وتطبيق هذه النظم؛ كون جميع المعلومات التي تتعلق بجميع المواطنين تتوافر لدى هذه التقنيات في قواعدها المعرفيّة، ويمكن للعاملين والتطبيقات الاطِّلاع عليها؛ ما يستدعي من الوزارة توفير كوادر مخصصة، لديها حرص تام على السريّة، إضافة لتوفير الراحة والأمان للمواطنين من خلال استخدام الشكبات الإلكترونيّة وقبولها في المجتمع، وتتفق هذه النتيجة مع دراسة (القحطاني، 2014م) بعنوان "تطوير مهارات التحقيق في الجرائم المعلوماتيّة" التي أكدت على ضرورة التزام التقنيين العاملين في مجال البرمجيات والتقنيات الذكيّة والتكنولوجيا الحديثة بالمحافظة على البيانات والمعلومات المتوفرة لديهم، وعدم العبث بها أو إظهارها.

كما أجمع المبحوثون على أهمية الاطِّلاع على تجارب الدول السابقة، فكما هو معروف نحن نعيش اليوم في عصر التكنولوجيا، وفلسطين من الدول حديثة العهد في مجال برامج الذكاء الاصطناعي ولا تزال تحتاج الكثير من الجهود المبذولة لمواجهة المعوّقات التي تحد من قدرتها على تطبيقه، إن التشبيك والاطِّلاع على تجارب الدول التي تستخدم هذه التقنيات الحديثة من شأنها أن تساعد العاملين في الوزارة الاستفادة من التجارب التي مرت بها، وتذليل التحديات التي تعاني منها الوزارة، إضافة الى أنها تساعد في الحصول على الخبرة والمهارة، وفتح آفاق جديدة لجلب موازنات مآليّة من الدول المانحة واستيراد أجهزة ومعدات، من هنا تأتي أهمية الاستفادة من تجارب الدول السابقة، خاصة أن دول العالم اليوم تتنافس في مجال التكنولوجيا والابتكارات الحديثة، كدولة الإمارات والسعودية التي

اطلقت ما يسمى (وزارة الذكاء الاصطناعي)، كما وعملت دول الإمارات على تطبيق برامج الذكاء الاصطناعي في مجال مكافحة الجرائم الإلكترونيّة للكشف عن جرائم الاحتيال من خلال نظم التعلم الآلي، هذا ما أكدت عليه دراسة (العبيدي، 2020) بعنوان "دور الدليل الرقمي في الإثبات الجنائي في النظام السعودي"، حيث أكدت على أهمية الاستفادة من تجارب الدول الأخرى وتعزيز المهارة والخبرة لديها، ودراسة (القحطاني، 2014م) بعنوان "تطوير مهارات التحقيق في الجرائم المعلوماتيّة"، التي أكدت على ضرورة الاستفادة من التجارب السابقة التي مرت بها الدول، وحققت من خلالها نجاحًا واضحًا في مجال برامج الذكاء الاصطناعي، فهو من التطبيقات الحديثة التي أثبت فعاليته في تتبع المجرمين الإلكترونين، خاصة في ظل التطور الذي تعيشه المجتمعات والتغيير في أنماط المعيشة والاعتماد –بشكل كبير– على استخدام التكنولوجيا ووسائل التواصل الاجتماعي التي أصبحت تشكل بؤر تجمع للمجرمين المتصيدين للجرائم، هذا ما يستدعي من العاملين في الوزارة مواكبة التطور والالتحاق بدورات مكثفة ومستمرة سواء على المستوى المحلي أم العالمي والتعلم منها، فكلما ازدادت المعرفة لدى المتخصصين زادت من قدرتهم على التعامل مع هذه البرامج، حيث إن آليات تطبيق برامج الذكاء الاصطناعي للحد من الجريمة الإلكترونيّة بحاجة إلى اهتمام كبير من جهات الاختصاص، فتطوير هذه النظم بحاجة إلى اهتمام وتركيز أكبر لتطبيقها؛ كونها تكنولوجيا جديدة بدأت تتغلغل في المجتمع الفلسطيني.

من الواضح أن الوزارة تستخدم برامج الذكاء الاصطناعي، لكن دون وجود آليّات محددة حيث يُعدُّ عدم وجود تلك الآليّات من أهم المُعوقات التي تواجه تطبيق برامج الذكاء الاصطناعي في الحد من الجريمة الإلكترونيّة حسب رأي المبحوثين، قد يعود السبب في ذلك إلى حداثة هذه البرامج وعدم وجود متخصصين فيها بدرجة عآليّة من الكفاءة؛ لتطبيقها ضمن آليّات محددة، لذا لا يمكن تحديد مساهمة هذه الآليّات في الحد من الجريمة الإلكترونيّة، لكن من الممكن لو تمّ القيام بدراسة الموضوع نفسه بعد عدة سنوات من التعامل مع برامج الذكاء الاصطناعي لدى الوزارة ولدى نفس المبحوثين أن تكون الإجابات مختلفة، ذلك بسبب أنه سيكون هناك آليّات متبعة للتعامل مع برامج الذكاء الاصطناعي تسهم في الحد من الجرائم الإلكترونيّة، تحديدًا مع وجود الخبرة التي سيتمتع بها المبحوثين.

وفيما يخص أكثر الجرائم التي تقوم تطبيقات برامج الذكاء الاصطناعي باكتشافها فقد حصلت جريمة الاختراق على أعلى درجة فقد أجمع عليها (39) من أصل (50) ، في حين جاءت جريمة نشر الفايروسات في المرتبة الثانية حيث حصلت على (18)، وجاء التهديد والابتزاز في المرتبة الثالثة، حيث حصلت على (12) إجابة، وفي المرتبة الرابعة البريد الوارد حيث حصل على (8) إجابات، وفي المرتبة الخامسة جرائم زراعة الملفات المشبوهة التي حصلت على (1) إجابة، نستنتج أن أكثر الجرائم التي تكتشفها الذكاء الاصطناعي هي الاختراقات وأدناها جرائم زراعة الملفات المشبوهة ذلك على

اعتبار أن هذه البرامج تحتاج إلى مهارة وخبرة عآليّة من الجناة المقبلين على ارتكاب الجرائم الإلكترونيّة.

من خلال ما سبق يمكننا أن نجزم أن تطبيقات الذكاء الاصطناعي فعّالة في اكتشاف الجرائم الإلكترونيّة، وقد يعود السبب في اكتشاف هذا النوع من الجرائم إلى طبيعة التطبيق الذي صمم خصيصًا لهذا النوع من الجرائم، وتغذيته بمجموعة من البيانات التي تكسبه الخبرة والمهارة، وتجعل منه أداة قادرة على التعامل مع الموقف الذي تتعرض له، حيث إنه –على سبيل المثال– يتم إدخال كل ما يتعلق بجريمة الابتزاز وكل دلالاتها، من خلالها يتمكن البرنامج التنبؤ بوجود مسلك غير طبيعي تتعرض له الضحيّة، إن ما يفسر هذه النتيجة استخدام جهاز الشرطة الفلسطينية للخوذة الذكيّة القائمة على تقنيات برامج الذكاء الاصطناعي، حيث تكمن وظيفتها في تحديد ما إذا كان المواطن مطلوبًا أم لا، من خلال خاصية التعرف على ملامح الشخص، بناءً على قاعدة بيانات، هنا يتم إدارج بيانات المطلوبين كافَّةً وصورهم؛ لتتمكن هذه الخوذة من كشف المطلوب في وقت وجهد أقل، نستنتج من ذلك أن لكل جريمة خوارزميات وبيانات خاصة يتم برمجتها وتصميمها من المبرمجين؛ لتتمكن هذه التطبيقات من اكتشاف الجريمة.

3.2.5 مناقشة نتائج المحور الرئيسي الثالث: هل هناك مُعوقات تواجِه تَطبيق برامج الذكاء الاصطِناعي في الحد من ممارسة الجريمة الإلكترونيّة في الوزارة؟ وتفرعاته:

من خلال إجراء التحليل لنتائج المقابلات اتَّضح وجود فروق في إجابات المبحوثين، فقد جاءت في المرتبة الأولى من حيث المُعوقات الاحتلال الإسرائيلي فقد حصلت على (22) إجابة من أصل (50)، يليها ضعف البنيّة والتحتيّة فقد حصلت على (16) إجابة، يليلها ندرة المبرمجين والميزانيّة المآليّة فقد حصلت على (15) إجابة، يليها قلة الأبحاث فقد حصلت على (7) إجابات، ثم نطاق عمل المؤسسة فقد حصلت على (11) إجابة، يليها عدم كفاية قاعدة للبيانات ذات صعوبة في تطبيق الذكاء الاصطناعي، فقد حصلت على (9) إجابات، ثم عدد الكادر العامل فقد حصلت على (7) إجابات، يليها نطاق عمل المؤسسة فقد حصلت على (11) إجابة، وأخيرًا جنس الكادر العامل فقد حصلت على (36).

مما سبق يتضح وجود مجموعة من المُعوقات التي تحول دون قدرة الوزارة على تطبيق برامج الذكاء الاصطناعي للحد من ممارسة الجريمة الإلكترونيّة، يُعَدُّ أحد أبرز المُعوقات التي تمنع الوزارة من إدخال برامج الذكاء الاصطناعي إلى الضفة الغربية الاحتلال الإسرائيلي والإجراءات الصعبة التي يفرضها؛ بهدف التضيق وزيادة الوقت المستغرق في استلام الوزارة وحصولها على البرامج والمعدات الإلكترونيّة، حيث إن ذلك ينصب في مصلحته؛ لزيادة الجرائم، ونشر الفساد، وعدم تمكين السلطات

والجهات المختصة من اكتشاف الفاعل في المجتمع الفلسطيني، كما أنه في كثير من الأحيان يمنع استيراد الكثير من التقنيات والبرامج التي تساعد المجتمع الفلسطيني في النهوض والارتقاء واللحاق بكوكبة التطورات التكنولوجيّة في العالم، هذا ما أكده المبحوث رقم (1) من خلال المقابلة التي أجريت معه، حيث أكد على أن الاحتلال الإسرائيلي يعوق مواكبة الوزارة للتطور بحجزه للمعدات والأجهزة لمدة تزيد عن ثلاثة أشهر، وفي بعض الأحيان حجزها وعدم الموافقة على إدخالها إلى أراضي الضفة الغربية، هذا ما يقف عائقًا أمام الوزارة ويؤثر على إمكاناتها في تطبيق هذه التقنيات التي من الممكن أن تساعد الجهات التنفيذية على تقليل نسب الجريمة الحاصلة، خاصة أن هذه التقنيات تساعد على التوصل لموقع الجناة وحل جزء كبير من القضية.

أما فيما يخص البنيّة التحتيّة بوصفها إحدى أهم المُعوقات التي تعوق الوزارة في تطبيق الذكاء الاصطناعي فالمجتمع الفلسطيني له خصوصية تختلف عن باقي دول العالم الأخرى؛ كون الاحتلال هو المتحكم الرئيس في فلسطين، وهذه البرامج والتقنيات تعتمد على البنى التحتية التي تستوعب كمًّا هائلًا من البيانات، خاصة أن البنيّة التحتيّة الحاليّة في الوزارة لا تكفي لاستيعاب التقنيات الحديثة؛ ما يشكل معضلة حقيقيّة في تطبيق الذكاء الاصطناعي، من هنا نستنتج أن سياسة الاحتلال الإسرائيلي لم تقف فقط في التضييق على الوزارة والحدّ من إمكانات شراء الأجهزة والمعدات، إنما تجاوز هذا التضيق إلى إضعاف البنيّة التحتيّة في فلسطين، فالبنيّة الحاليّة الموجودة غير قادرة على استيعاب التقنيات الحديثة، فهي بحاجة ماسة إلى تطوير؛ ليتمكن العاملون في الوزارة من مواءمتها مع التقنيات الحديثة، حيث إننا عندما نتحدث عن البنية التحتية فإننا لا نتحدث عن مساحة معينة، إنما نحتاج إلى قاعدة ضخمة من البيانات لها القدرة على استيعاب كم هائل من البيانات والمدخلات المتنوعة لمختلف أنواع الجرائم الحاصلة، إذْ إنَّ لكل جريمة مدخلات وأنظمة تختلف عن غيرها، فجريمة الابتزاز والتهديد تختلف عن جريمة السرقة والنصب والاحتيال من حيث مدخلاتها ودلالاتها والخوارزميات الخاصة بها، فمن المهم أن تعمل الوزارة جاهدة؛ لتخطي الضعف الذي يغطي البنيّة التحتيّة وتعزيز دورها؛ لما لها من دور كبير وأساسي في تطبيق برامج الذكاء الاصطناعي، وهذا ما أكدت عليه دراسة بلال وآخرون (Bilal & Others, 2019) بعنوان "تأثير الذكاء الاصطناعي في الكشف عن الجرائم الإلكترونيّة"، حيث أكدت على ضرورة العمل على تطوير البنية التحتية في المؤسسات العاملة في مجال التكنولوجيا؛ لتعزيز قدرتها على تخزين البيانات كون البنيّة التحتيّة تحتاج إلى مساحة كبيرة جدًّا لاستيعاب أكبر قدر من البيانات في قواعدها، كما أكَّدت دراسة تيواري وماهيشواري وبال (Tiwari & Maheshwary & Pal, 2018) بعنوان "تطبيق الذكاء الاصطناعي في الحد من هجمات الجرائم الإلكترونيّة"، حيث أكدت على ضرور العمل على تعزيز بناء بنيّة تحتيّة قوية؛ من

أجل الدفاع عن أي اختراقات تتعرض لها الشبكة، إذ إن وجود بنيّة تحتيّة قويّة تشكل الدرع الحامي من أي اختراقات.

كما يتضح من النتائج أن ندرة المبرمجين جاءت ضمن أبرز المُعوقات التي تواجه الوزارة، حيث إنَّ وجود أشخاص غير مؤهلين وغير ملمين بالتطورات التكنولوجيّة الحديثة من شأنه أن يزيد من الضعف في تطبيق برامج الذكاء الاصطناعي؛ إذْ إنَّ الشح في العاملين الحاصلين على مؤهلات علميّة في مجال برامج الذكاء الاصطناعي من الممكن أن يكون السبب فيه حداثة هذا العلم وانتشاره في دول العالم الأخرى، إضافة إلى صعوبة ظروف الحياة في المجتمع الفلسطيني، حيث إن الأشخاص الحاصلين على هذه التخصصات قد يلجأون إلى العمل في دول أخرى؛ لوجود فرص حياتيّة أفضل لهم في الخارج، مقارنة مع فلسطين، ناهيك عن البطالة المتفشيّة في المجتمع التي تدفع بهم للهجرة خارج البلاد، وهذا ما يجعل فلسطين تفتقر –بشكل واضح– إلى وجود كوادر بشرية تحمل تخصصات في مجال برامج الذكاء الاصطناعي، إضافة لما سبق فإن الشح في عدد الموظفين الخاضعين لدورات متعلقة ببرامج الذكاء الاصطناعي وتتبع الجرائم الإلكترونيّة في الوزارة، كل هذا يؤثر في تطبيق برامج الذكاء الاصطناعي، نرى أن هذه النتيجة جاءت مُحَصِّلةً لعدم التحاق العاملين في الوزارة بدورات متخصصة في الذكاء الاصطناعي وتتبع الجرائم الإلكترونيّة، وهو ما تم استنتاجه من خلال الجدول رقم (1.3)، فقد تبين وجود عدد ضئيل جدًّا في العاملين الخاضعين لدورات متعلقة ببرامج خاصة بالذكاء الاصطناعي.

إضافة الى أن نقص الكوادر البشريّة ذات الكفاءة والخبرة في الكثير من الأقسام في الوزارة بسبب إحالة الوزارة عدد كبير من الموظفين المتقدمين في السن الى التقاعد خلال السنوات الأخيرة يُشكل صعوبة كبيرة في إمكانيّة استثمار الأجهزة والمعدات والخبرات وتطبيق البرامج؛ ويؤثر على بعض الأقسام ويتسبب في تركها فارغة ويعوق من عملية فتح أقسام جديدة في المستقبل، هذا يستدعي من الوزارة البحث عن موظفين جدد ذوي كفاءة ومهارة عاليّة تناسب قدراتهم مع أماكن العمل التي سوف يشغلونها في المستقبل.

كما أوضحت نتائج المقابلات أن قلة الأبحاث تشكل إحدى المُعوقات المهمة التي تعوق قدرة الوزارة على تطبيق الذكاء الاصطناعي؛ بسبب ندرة استثمار الأكاديميين للأبحاث والدراسات التي تختص في مجالات وبرامج الذكاء الاصطناعي مثل (الشبكات العصبيّة – التعلم الآلي – النظم الخبيرة) وقدرتها على مواجهة الجريمة الإلكترونيّة فهي تشكل علم واسع وجديد والمجتمعات في الوقت الحالي بأمس الحاجة لها، وبسبب إهمال هذه الأبحاث وعدم إرفاقها في المناهج التعليمية واقتصارها فقط على على الدراسات العليا، كالماجستير والدكتوراه؛ ما يؤثر على تطبيق الذكاء الاصطناعي وبطء انتشاره في المجتمع.

في حين جاء الجنس كأدنى استجابة على اعتبار أنها أحد المُعوقات التي تعوق تطبيق الوزارة لبرامج الذكاء الاصطناعي في مواجهة الجريمة الإلكترونيّة، السبب في ذلك أنه في العصر الحالي المجتمع لا يفرق بين ذكر وأنثى نتيجة ذلك لم يعد هناك فرق بين الذكر والأنثى، فالعالم لم يُعطِ اهتمامًا لجنس دون الآخر لمن يشغل وظيفة معينة في العمل أو من يتعامل مع هذه التطبيقات، بمعنى أنه إذا توافرت لدى الجنسين الخبرة والمهارة والقدرة على التعامل مع هذه التطبيقات فليس هناك قيود لتطبيقها من الذكر دون الأنثى والعكس صحيح، بمعنى آخر أن تطبيقها لا يقتصر على جنس دون الآخر، لذا جاءت النتيجة منطقية حيث إنَّ تأثير الجنس على تطبيق برامج الذكاء الاصطناعي شبه معدوم وهو ما تتفق عليه النتائج السابقة.

أمّا فيما يخص طرائق التغلب على المُعوقات التي تواجه تطبيق الذكاء الاصطناعي في الحد من ممارسة الجريمة الإلكترونيّة فقد أجمع (34) من المبحوثين على أهميّة تطوير البنيّة التحتيّة، في حين أجمع (26) مبحوث على أهميّة توفير كوادر متخصصة وذات كفاءة عآليّة في مجال التعامل مع برامج الذكاء الاصطناعي، وأجمع (26) آخرين على ضرورة توفير إمكانات مآليّة من الدول المانحة والمؤسسات الداخلية والخارجية وتخصيصها حول كل ما يتعلق بتطبيق الذكاء الاصطناعي، وفيما يخص أهمية إجراء تدريبات ودورات وورشات عمل فعّالة للموظفين فقد حصلت على(24) إجابة، إضافة إلى ضرورة العمل على دعم الأبحاث والدراسات ذات العلاقة بالذكاء الاصطناعي وزيادتها، وتتبع مرتكبي الجرائم الإلكترونيّة، نلاحظ من النتائج أعلاه أن تطوير البنيّة التحتيّة تُعتبر من أبرز طرق التغلب على هذه المُعوقات والصعوبات، فكلما تم تطوير البنيّة التحتيّة وتعزيز قدرتها على استيعاب البيانات أدت إلى إزالة جانب مهم من العقبات التي تواجه تطبيق تلك البرامج، فهناك ارتباط بين البنيّة التحتيّة وتطبيق برامج الذكاء الاصطناعي على اعتبار أن برامج الذكاء الاصطناعي في آليّة عملها تعتمد على البنيّة التحتيّة، حيث إنه دون توفير بنيّة مناسبة من المستحيل تمكين هذه البرامج من العمل، من هنا تأتي أهمية تطويرها؛ كي تتمكن الوزارة من تطبيق برامج الذكاء الاصطناعي؛ كون البنية التحتية المصدر الأساسي لعمل هذه البرامج حيث إن تحسينها يساعد بدرجة كبيرة في الارتقاء بمستوى الخدمة المقدمة والحصول على نتائج أسرع وأدق، لذا تعدُّ البنية التحتية من أهم الطرائق التي يجب العمل على تطويرها، تتفق هذه النتيجة مع ما أشارت إليه نتائج دراسة كل من تيواري وماهيشواري وبال (Tiwari & Maheshwary & Pal, 2018) بعنوان "تطبيق الذكاء الاصطناعي في الحد من هجمات الجرائم الإلكترونيّة" حيث أكدت على ضرورة العمل على تعزيز بناء بنيّة للدفاع من أجل إزالة الاختراقات، ودراسة بلال وآخرون (Bilal & Others, 2019) بعنوان "تأثير الذكاء الاصطناعي في الكشف عن الجرائم الإلكترونيّة" التي أكدت على ضرورة العمل على تطوير البنيّة التحتيّة في قطاع التكنولوجيا لزيادة تخزين البيانات.

وتعدُّ الدورات وورشات العمل ذات العلاقة ببرامج الذكاء الاصطناعي والكشف عن الجريمة الإلكترونيّة من الأمور المهمة التي يجب على الوزارة العمل على توفيرها؛ لتتمكن من الحصول على مزيد من الخبرة والمهارة التي من شأنها جعل العاملين في الوزارة على قدر المسؤوليّة في استخدام برامج تطبيقات الذكاء الاصطناعي؛ كونه من العلوم الجديدة في المجتمع الفلسطيني، ويحتاج إلى مزيد من الخبرات والكفاءات، وعدم الوقوف على الخبرات السابقة التي لم تعد تجدي نفعًا في هذا المجال، كما تمكن الخبرة والمهارة التي يمتلكها الكفاءات والمتخصصون في مجال الذكاء الاصطناعي من إدارة البنيّة التحتيّة والتعامل مع تطبيقات الذكاء الاصطناعي؛ لمنع تفاقم الجرائم الإلكترونيّة، إن هذا التكامل بينها من أهم الطرائق للتغلب على المُعوقات التي تواجه تطبيق الذكاء الاصطناعي، تتفق هذه النتيجة مع دراسة تيواري وماهيشواري وبال (Tiwari & Maheshwary & Pal, 2018) بعنوان "تطبيق الذكاء الاصطناعي في الحد من الهجمات الإلكترونيّة" التي أكدت على أهمية توفير كوادر متخصصة وذات كفاءة عاليّة في مجال الذكاء الاصطناعي بالإضافة إلى تعزيز الدورات وورشات العمل والإمكانات الماليّة، ودراسة (البلوي، 2009) بعنوان "التقنيات الحديثة في التحقيق ودورها في ضبط الجريمة" التي أشارت إلى أهمية تدريب العنصر البشري على التقنيات الحديثة وكيفية استخدامها بأعلى كفاءة، ودراسة (الشهري، 2001) المشار لها في (العمري، 2004) بعنوان "المعوقات الإدارية في التعامل الأمني مع جرائم الحاسب الآلي" التي أشارت إلى أهمية عقد دورات لضباط الأمن في مجال أمن المعلومات والحاسب الآلي وشبكة الإنترنت، وأهمية التوسع في العمل الآلي، إضافة الى دراسة (العنزي، 2003) بعنوان "وسائل التحقيق في جرائم المعلومات" التي أكدت على أهمية زيادة الدورات والندوات للتعرف على أحدث الطرائق التي من شأنها أن تساعد في تحقيق أمن المعلومات.

أمّا فيما يخص العلاقة بين متغيرات (الجنس، عدد افراد الأسرة، مكان السكن، التحصيل العلمي، العمر) وارتكاب الجريمة الإلكترونيّة حصل متغير **العمر** على المرتبة الأولى فقد أجمع المبحوثون على علاقته بارتكاب الجريمة الإلكترونيّة حيث حصل على (36) إجابة من أصل (50)؛ ما يعني أن للعمر تأثيرًا في ارتكاب الجاني للجريمة الإلكترونيّة؛ فالشباب في المراحل العمرية الصغيرة أكثر ميلًا لارتكاب الجريمة الإلكترونيّة بالإضافة الى حب الفضول والطيش والتحدي الذي يتمتع به الشباب في هذه المراحل العمرية، بخلاف فئة كبار السن الذين يتميزون بالاستقرار وكثرة المسؤوليات والواجبات التي تدفعهم إلى عدم التفكير والتوجه الى الجرائم الإلكترونيّة، هذا يعني أن مرحلة الشباب مرحلة انتقاليّة تتسم بوجود تقلبات في حياة الشباب بالمقارنة مع الفئات العمرية الصغيرة جداً، والفئات العمرية الكبيرة التي تصنف بالناضجة، فهذه المراحل العمرية تتسم بعدم الاستقرار وقلة الالتزامات الحياتية خاصة أن الشباب في هذه المرحلة يمرون بالعديد من المواقف، منها العاطفية التي تعرضهم لبعض المشاكل التي قد تدفع بهم للانتقام واللجوء إلى الفضاء الإلكتروني، كما تؤدّي الظروف الاجتماعية كالحياة داخل المنزل والتفكك الاجتماعي وقلة الروابط الأسرية المبنية على التنشئة الصحيحة دورًا في

ممارسة الفرد للجرائم الإلكترونيّة، فعندما يصبح الفرد غير قادر على التميز بين ما هو مقبول اجتماعياً وما هو مرفوض، ويرغب في إثبات الذات بطرائق غير مشروعة يتجه إلى استخدام شبكات الإنترنت ومواقع التواصل الاجتماعي التي تعدُّ المُتنفَّس الوحيد في هذا المجال، إضافة إلى أن الشباب في هذه المراحل العمرية يعانون من صعوبة في الحصول على متطلبات المعيشة، فضلًا عن الظروف الاقتصادية الصعبة، خاصة ما شهدته فترة انتشار جائحة كورونا التي دفعت بهم إلى مواجهة صنفين من الظروف التي شكلت ضغوطًا عامة، تمثَّلَ الجانب الأول في انعدام القدرة على الحركة والجانب الثاني الخروج من المنزل؛ ما أدى إلى صعوبة التعايش وزيادة المشاكل العائلية؛ بسبب ضعف الروابط الأسرية قبل انتشار الجائحة، حيث أدت إلى العزلة عن المحيط الأسري ليجد نفسه يعيش في عالم إلكتروني هرباً من الواقع؛ ما يعزز لدى الجاني الرغبة في الانتقام والكراهية من خلال الشبكات الإلكترونيّة، ومن جانب آخر كان للجانب الاقتصادي تأثير واضح خاصة أن المجتمع الفلسطيني في ظل الظروف الطبيعية يعاني من مشكلة البطالة التي ازدادت بشكل فائق وملحوظ في فترة انتشار الجائحة، الأمر الذي أدى إلى هلاك الكثير من العائلات وانعدام قدرتها على توفير المال، هذا ما ولد شعور الحقد والكراهية وفقدان الانتماء واللجوء إلى الإنترنت بإعتباره الميدان الوحيد الذي يمكن من خلاله التعبير عن مشاعر الغضب والحصول على المال، هذا من شأنه أن يشكل دافعًا لقيامه بمسلكيات منحرفة ضد المجتمع وضد الدولة؛ من أجل التخلص من الضغوط التي ولدتها الظروف الصعبة التي عاشها؛ بسبب انتشار فايروس كورونا، فالشباب في هذه المراحل بحاجة إلى احتواء من الأسرة والدولة، حيث يمكن للفرد إشباع رغباته من خلال شبكة الإنترنت بسهولة؛ بسبب عدم توفر الرقابة وتوفر الفرصة له، هذا ما أشارت له كل من نظريّة النشاط الرتيب ونظريّة الفرصة، حيث أن غياب الرقابة والقوانين ووجود الفرصة تدفع الشباب لممارسة جريمتهم.

إضافة لما سبق لا نستطيع إغفال دور رفاق السوء في هذه المرحلة العمرية، فعندما يبدأ الشباب بإمضاء فترات زمنية طويلة مع الرفاق أكثر من الأسرة، هنا يبدأ تأثير هذه السلسة من العلاقات السيئة على الفرد، ويصبح من السهل التأثير على عقل الشباب، ودفعه لارتكاب الجرائم الإلكترونيّة، ناهيك عن أن نتائج الجرائم وجرائم التهديد والابتزاز لا تقتصر فقط على الفضاء الإلكتروني، إنما يمتد ذلك على أرض الواقع وتتحول إلى قتل وطعن وجرائم بأبشع صورها، تتقاطع هذه النتيجة مع أوقات الفراغ التي تُعَدُّ دافعًا في ارتكاب الجريمة الإلكترونيّة للفئات العمرية في مرحلة الشباب، فكثرة أوقات الفراغ في هذه المرحلة العمرية –خاصة أنها تخلو من أي أنشطة وأعمال– تدفع الشباب إلى حب التنافس والتحدي من خلال ارتكاب المسلكيات المنحرفة، وتعزز لديهم الفكر الإجرامي، وهذا ما شهدته فترة انتشار جائحة كورونا التي زادت من نسبة أوقات الفراغ لجميع أفراد المجتمع؛ ما أدى إلى زيادة نسبة الجريمة الإلكترونيّة؛ بسبب استخدامهم المتزايد لشبكة الإنترنت ومواقع التواصل الاجتماعي، هذا ما أكد عليه (الهندي، 2020) من خلال المقابلة التي أجريت معه يوم الثلاثاء الموافق (2020/10/20)

أن الجريمة الإلكترونيّة زادت في فترة انتشار الجائحة لدى الشباب؛ بسبب إمضاء أوقات طويلة، وعدم استثمارها في أنشطة حياتيّة مفيدة، على عكس الفئات العمريّة الناضجة التي تتسم بالاستقرار، وزيادة مسؤولياتها الحياتيّة التي تقلل من نسبة التفكير في أي مسلكيات منحرفة بالإضافة إلى أنها تتسم بالاتزان والنضج.

وفي المرتبة الثانية حصل متغير **مكان السكن** على (27) إجابة؛ ما يعني أن لمكان تواجد الجاني تأثيرًا في ارتكاب الجريمة الإلكترونيّة؛ فكما نعلم أن المدينة ذات انفتاح أكثر على التكنولوجيا مقارنة مع القرية، إضافة إلى أن القرية تتحكم فيها العادات والتقاليد والمجتمع العشائري الذي يُعاقب مرتكب الجريمة الإلكترونيّة الخارج عن القواعد المتعارف عليها، يمكن تفسير هذه النتيجة في ضوء نظريّة الوصم التي ترى أن ارتكاب الفرد لمسلك مخالف للضوابط المتعارف عليها تؤدي الى إلصاق التهمة بالجاني مدى الحياة، ووصمه بها عند خروجه عن القواعد المتعارف عليها في المجتمع؛ ما يعرضه إلى النبذ في البيئة التي يعيش فيها، ولا يقتصر ذلك فقط على الجاني، إنما يتعداها ليتم وصم أفراد عائلته كافّة؛ بسبب الفعل الذي قام به، لذا يبتعد الفرد الذي يعيش في القرية عن ارتكاب الجرائم الإلكترونيّة؛ للمحافظة على مكانته الاجتماعية وتجنب الانكسار والاستحقار من المجتمع، إضافة لما جاءت به النظريّة اللامعياريّة التي ترى أن عدم التوافق بين الفرص المتاحة والظروف المعيشية والضوابط الاجتماعية داخل القرية تعزز لدى الفرد الشعور بحالة من الضغط، وعدم الرضا عن الحياة في القرية التي تتحكم فيها العادات والتقاليد والعشائر بشكل واضح، كل ذلك ينمي المشاعر السلبية لدى الجاني، وتعزز لديه الرغبة في ترك القرية واللجوء إلى المدينة؛ لما تمتاز به من عزلة وقلة الروابط الاجتماعية التي تمكنه من القيام بالمسلكيات غير المشروعة، وإشباع رغباته دون قيود؛ ما يؤدي إلى انفتاحه بشكل غير صحيح على التكنولوجيا، واستخدامها بطرائق غير مشروعة، بالإضافة الى أن إجابات المبحوثين خلال المقابلات تمركزت حول المناطق الخارجة عن اختصاص وسيطرة السلطة التي تصنف بمناطق (C)، فهي تشكل وكرًا لارتكاب الجرائم الإلكترونيّة ومصدر أمان للجاني؛ نتيجة لسياسة الاحتلال الإسرائيلي التي تعوق من قدرة الأجهزة الأمنية على الوصول إلى موقع الجاني في كلا الجانبين، الجانب الأول الافتراضي من خلال تقييد حركة جهات الاختصاص في الحصول على مجريات الأحداث على الشبكة، والجانب الثاني الواقعي ففي حال تمّ التوصل لموقع الجاني إلكترونيًّا فالواقع يفرض قيودًا على الجهات المنفذة للقانون في حال وجود الجاني في مناطق خارجة عن السيطرة الفلسطينيّة، إن ذلك يشكل معضلة كبيرة خاصة أن سلطات الاحتلال الإسرائيلي في كثير من الأحيان لا تعطي تنسيقًا لبعض المناطق؛ ما يشكل مصدر أمان للجاني وفرصة كون ذلك ينصب في مصلحة الاحتلال لزيادة الفساد والجرائم بين أبناء المجتمع الفلسطيني، هذا ما يمكن تفسيره ضمن نظريّة الفرصة.

يمكن التأكيد مما سبق على أنه من الطبيعي أن يكون هناك اختلاف في الروابط الاجتماعية والعادات بين المدينة والقرية كون المدينة هي نقطة تجمع لفئات وثقافات وجنسيات وأعمار مختلفة من البشر، بالإضافة إلى أنها مراكز جذب للتكنولوجيا، وأول من يستقبل التحديثات الجديدة في التكنولوجيا، هذا ما أكده المبحوث في المقابلة رقم (8) أن برنامج الذكاء الاصطناعي الـ(Fir wall) الذي يعمل على توفير الحماية والأمان والوقاية من أي نوع من الهجمات الإلكترونيّة، "يتوفر فقط في مدينة رام الله ناهيك عن البرامج التكنولوجيّة الحديثة الأخرى التي تتوافر فيها"، فالطبيعة الجغرافية للمناطق وتصنيفاتها تؤثر في ارتكاب الجريمة الإلكترونيّة، حيث إن البيئة المحيطة بالفرد تؤثر بشكل كبير على تصرفاته ومسكلياته الإجرامية، فتنشئة الفرد بناءً على ما هو متعارف عليه في تلك المناطق تؤثر بشكل كبير على نفسيته وتنمي في نفسه التمرد وارتكاب المسلكيات المنحرفة، كما تدفعه إلى ارتكاب الجرائم الإلكترونيّة، فشعور الجاني أنه لا يخضع للقانون لعدم وجود رقابة أمنية وكثرة الكثافة السكانية في تلك المناطق التي تحوي مختلف أنواع البشر فضلًا عن صعوبة الوصول إلى تلك المناطق هي ذات ارتباط مباشر في ارتكاب الجريمة الإلكترونيّة، إن ما يؤكد ذلك نظريّة النشاط الرتيب التي ترى أن غياب الرقابة الأمنيّة والرغبة والهدف تجتمع في ارتكاب الجريمة الإلكترونيّة، حيث يمكن ربطها في حالة شعور الجاني بالطمأنينة حيال ارتكابه للجريمة الإلكترونيّة، نتيجة غياب الرقابة الأمنية، وتوفر الهدف؛ ما يؤدي إلى دفعه لارتكاب الجريمة الإلكترونيّة؛ لعلمه أنه في مناطق من المستحيل وصول الحماية الأمنية فيها، بالإضافة إلى عدم توفر تطبيقات الذكاء الاصطناعي يعطي فرصة للجاني لممارسة جريمته، ومن ثمَّ تعزز من إمكانية ارتكابه للجريمة الإلكترونيّة متكاملة الأركان، من هنا تتوضح فكرة وجود جريمة في مناطق دون الاخرى.

وجاءت في المرتبة الثالثة **الجنس** فقط حصل على (27) درجة لصالح الذكور ذلك؛ قد يعود السبب في ذلك أن الذكور أكثر جرأة وميلًا لارتكاب الجرائم الإلكترونيّة، بخلاف الأنثى التي م لا تميل لارتكاب الجريمة الإلكترونيّة، بحكم طبيعة المجتمع والعادات والتقاليد التي تقيّد من إمكانيتها على الإقبال لهذا النوع من الجرائم، خاصة أن المجتمع الفلسطيني مجتمع ذكوري بحت، وجاءت أقل درجة لصالح الإناث حيث حصلت على إجابة (1)، هذا في حال كانت تمتلك خبرة ومهارة كافية للتعامل مع التكنولوجيا الحديثة، تتفق هذه النتيجة مع نظريّة الوصم التي ترى أن ارتكاب الفرد لمسلك مخالف للضوابط المتعارف عليها تؤدي إلى إلصاق التهمة بالجاني مدى الحياة، فالأنثى في المجتمع الفلسطيني لا تميل لارتكاب الجريمة الإلكترونيّة، بحكم العادات والتقاليد والخوف من ملازمة التهمة والمسلكيات المنحرفة مدى الحياة، إضافة إلى النظرة الدونيّة من أفراد المجتمع لها؛ ما يولد لديها ضبط الذات وعدم الانحراف عما هو متعارف عليه في المجتمع، كما هو متمثل في النظريّة اللامعياريّة.

حيث إنَّ طبيعة التنشئة الاجتماعية في المجتمع الفلسطيني قائمة على الحياة الذكورية، وأن الرجل لا يعيبه شيء بعكس الفتاة التي يجب أن تكون على وعي ودراية بكل خطوة تقوم بها، فالذكر بحكم المسؤولية الملقاة على عاتقه من إعالة الإسرة من جهة، ومواجهة المواقف الحياتية كافّة من جهة أخرى تولد لدى الفتاة في المجتمع نوعًا من التردد والخوف من ارتكاب أي مسلك منحرف والخروج عن القواعد المتعارف عليها في المجتمع، وذلك تجنباً للانتقاد والنَّبْذ خاصة أن المجتمع الفلسطيني مجتمع محافظ، لا يقبل فكرة وجود فتاة في مراكز الإصلاح والتأهيل، أو في مراكز الشرطة، تتفق هذه النتيجة مع نظريّة الوصم التي ترى أن قيام الفرد لمسلك مخالف في المجتمع يعرضه للنبذ والوصم والنظرة الدونية، فالأنثى تفضل الالتزام بالمبادئ المتعارف عليها، وتقوم بكبت مشاعرها، ولا تُقدم على ارتكاب الجريمة، لأن ذلك يُعرضها للعنوسة؛ نتيجة السمعة التي تلتصق بها، وتدفع بأفراد المجتمع إلى عدم الاقتراب منها، كما أن طبيعة التربية في المجتمع الفلسطيني قائمة على زيادة الرقابة للأنثى من الوالدين، بخلاف الذكر الذي تقل الرقابة الولدية له، فتعزز من ارتكابه للجريمة.

فيما يخص النتيجة السابقة لا يمكن أن نتفق معها، فالمجتمعات في الوقت الحالي أصبحت أكثر انفتاحًا، وكلا الجنسين يستخدمان التكنولوجيا والعالم الإلكتروني بشقيه السلبي والإيجابي، وكلاهما إذا توافرت لديهم الخبرة والمهارة سيندفع إلى ارتكاب الجريمة وإخفاء أي أثر له على الفضاء الإلكتروني، فالجريمة الإلكترونيّة تختلف عن الجريمة التقليديّة، فهي تحتاج إلى قدرات ذهنيّة لارتكابها، إن ما يؤكد على ذلك ما أشارت إليه (صحيفة دنيا الوطن، 2019) بتاريخ (31\3\2019)، حيث أشارت أن معظم ضحايا الجرائم الإلكترونيّة هم من فئة الذكور، حيث شكلت نسبة الشكاوي الوارد لدى وحدة الجرائم الإلكترونيّة في جهاز الشرطة الفلسطينية الذكور(1447) مقابل (1034) من الإناث، وتتروح فئاتهم العمرية ما بين (18–25)، تتفق هذه النتيجة في ضوء نظريّة الضغوط العامة التي ترى أن الفرد وما يمر به من ظروف هي المحرك الأساسي لتصرفاته وردود فعله؛ ما يساهم في زيادة الجرائم الإلكترونيّة لدى الإناث في العديد من الأحيان أكثر من الذكور، فالأنثى عندما تشعر أنها غير قادرة على تحقيق رغباتها وطموحاتها في المجتمع بطرائق مشروعة نتيجة رفض المجتمع لها ولوجود حاجز العادات والتقاليد الذي يقيّد قدرتها على القيام برغباتها على أرض الواقع، أو نتيجة تعرضها لبعض الظروف التي تمنعها من مواجهتها على أرض الواقع؛ فإنها ستلجأ للعالم الافتراضي نظراً لما يقدمه لها من كسر للحواجز وإتاحة الفرصة في إشباع رغباتها المكبوتة التي أصبحت تتشكل على هيئة ضغوط هي السبب في انخراطها وممارستها للجرائم الإلكترونيّة، كما وتتقاطع هذه النتيجة مع متغير العمر؛ لتؤكد أن الفئات العمرية الصغيرة أكثر ميلًا لارتكاب الجرائم الإلكترونيّة، فالمجتمع الفلسطيني –كغيره من المجتمعات– يواكب التطورات وكل ما هو حديث في عالم التكنولوجيا؛ نتيجة الانفتاح على العالم

الافتراضي وتغير القيم والمفاهيم الاجتماعية المتوارثة في المجتمع، فالجريمة لم تعد تقتصر على أنثى أو ذكر، فكل منهما إذا توافرت لديه الميول الاجرامية يلجأ الى ارتكاب الجريمة الإلكترونيّة.

وفي المرتبة الرابعة تمركزت (27) من إجابات المبحوثين على وجود علاقة بين **التحصيل العلمي** وارتكاب الجريمة الإلكترونيّة، هذا يعني وجود تأثير للتحصيل العلمي على ارتكاب الجريمة الإلكترونيّة، هنا يمكننا القول إنَّ المتعلم يمارس الجريمة الإلكترونيّة نتيجة إلمامه واطّلاعه على التكنولوجيا بخلاف غير متعلم، إن عدم معرفته بالتكنولوجيا وكيفية استخدامها تبعده عن ارتكاب هذا النوع من الجرائم.

نتفق مع هذه النتيجة لأنَّ المجتمع الفلسطيني له خصوصية تختلف عن باقي الدول ذلك لضيق المنافذ وخيارات الحياة للمواطن الفلسطيني، ولصعوبة متطلبات الحياة نتيجة تضييق الاحتلال الإسرائيلي، فالمتعلم الحاصل على مؤهلات علميّة في مجال التكنولوجيا عندما يجد نفسه أمام واقع تنتشر فيه البطالة وظروف اقتصادية صعبة وقلة الاستثمار في المهارات الشابة؛ فإنَّ ذلك يؤدي إلى اندفاعه لارتكاب الجريمة الإلكترونيّة، ولعل ما يؤكد على ذلك نظريّة الضغوط العامة التي ترى أن ظروف الفرد المحيطة تؤدّي دورًا في مسلكياته وانسداد الفرص المحيطة لتحقيق رغباته وطموحاته، فعندما يفتقر المتعلم إلى أدنى فرص الحياة التي كان يطمح بها، ولا يستطع تطبيقها فذلك يؤدي إلى تراكم المشاعر الداخلية، وتفريغها بطرائق غير مشروعة في الفضاء الإلكتروني، فاجتماع العلم والخبرة مع الظروف القاسيّة تؤثّر في ذلك، أما غير المتعلم ونتيجة لقلة معرفته بالتكنولوجيا وضعف امتلاكه للمهارات التي تمكنه من استغلال الثغرات من الممكن أن يبتعد عن ارتكاب الجريمة في مجال الفضاء الإلكتروني مقابل ارتكابها على أرض الواقع.

نستنتج ممّا سبق أن للتحصيل العلمي تأثيرًا في ارتكاب الجريمة الإلكترونيّة حيث إن هذا النوع من الجرائم لا يمكن لأي شخص القيام به، أي أنه كلما كانت الجريمة الإلكترونيّة المرتكبة أكثر وأعلى دقة كان للتحصيل العلمي خاصة في مجال تكنولوجيا المعلومات تأثير أكبر، كما أن الأُمّيّ –بحكم الجهل وعدم الإلمام الكافي باستخدام التكنولوجيا– من الممكن أن يرتكب جريمة على شبكات التواصل الاجتماعي دون قصد أو وعي، حيث يقع فريسة لأشخاص لديهم القدرة على التأثير في الفرد، وتعزيز الرغبة لديه في ارتكاب الجريمة الإلكترونيّة.

وفي المرتبة الرابعة تمركزت (41) من إجابات المبحوثين على عدم وجود علاقة بين **عدد أفراد الأسرة** وارتكاب الجريمة الإلكترونيّة، بما يعني أن عدد أفراد الأسرة لا يؤثر في ارتكاب الجريمة من وجهة نظر المبحوثين، وتفسير ذلك أن الجريمة حاصل محصل إذا كان لدى الفرد ميول إجرامية فسوف يلجأ الى ارتكابها بصرف النظر عن عدد الأسرة كثيرًا كان أم قليلًا، تتفق هذه النتيجة مع نظريّة الاختيار العقلاني التي يمكن ربطها بحرية اختيار الفرد لسلوكاته، فعندما يشعر الفرد بالحقد والكراهية تجاه

العائلة أو الدولة؛ لعدم تلبيتها لاحتياجاته ورغباته وإشباعها، إضافة إلى غياب الرقابة الأمنية في مواقع التواصل الاجتماعي، يقوم بممارسة مسلكيات منحرفة ومرفوضة اجتماعيًّا.

على الرغم من النتيجة السابقة إلا أنه لا يمكن الإتفاق معها؛ فالتنشئة الاجتماعية الصحيحة القائمة على العادات والتقاليد والأخلاق هي الدرع الحامي للفرد بعدم ارتكاب جرائم إلكترونيّة، يعود ذلك في الأساس إلى بذرو التربية التي زرعها الوالدان في الأبناء، فزيادة عدد أفراد الأسرة يؤدي إلى فقدان السيطرة من الوالدين في إعطاء الأبناء حقهم في التربية، ويؤدي إلى تنشئة كل منهم على هواه، وما يتعلمه من محيطه؛ نتيجة إهمال الوالدين وضعف الرقابة الأبوية، خاصة إذا كانت الأسرة تعاني من ظروف اقتصادية سيئة فتؤدي بالأب والأم إلى الخروج لفترات طويلة من المنزل في سبيل الحصول على الرزق لإعالة أبنائهم، ومن جانب آخر فمن الممكن أن يندفع رب الأسرة الكبيرة إلى ارتكاب جريمة إلكترونيّة نتيجة الظروف الاقتصادية السيئة؛ ما يدفع الأب إلى القيام بذلك لتحسين الوضع الاقتصادي، يمكن تفسير هذه النتيجة من خلال نظريّة الضغوط العامة التي يتعرض لها الفرد في المجتمع؛ نتيجة عدم قدرته على إشباع رغباته بالطرائق المشروعة؛ ما يترك أثرًا سلبيًّا في نفس الجاني، وتعزز لديه الرغبة في ارتكاب الجريمة لانسداد الفرص أمامه في تحقيق أهدافه وطموحاته المنشودة، فعندما يكون لدى الأسرة دخل منخفض فإن الأب يتعرض لحالة من الضغوط والظروف الصعبة التي تجعل منه عاجزًا عن تأمين المال لإعالة الأولاد والأسرة؛ ما يؤدي إلى خروجه فترات طويلة من المنزل للعمل في أكثر من وظيفة، الأمر الذي يؤدي بنتائج سلبية على الأب وتولد لديه مشاعر حقد وغضب، كل هذه الضغوط التي يعيشها تجعل منه شخصًا متصيّدًا للفرص، وعرضة أكثر للإغراءات في سبيل الحصول على مزيد من المال، تتفق هذه النتيجة مع نظريّة الفرصة التي ترى أن غياب الرقابة الأمنيّة والفرصة المتاحة والهدف تعزز لدى الجاني الإقبال على ارتكاب الجريمة الإلكترونيّة، فعندما لا تسمح الفرص–على أرض الواقع– تأمين الرزق للعائلة فإنه يجد في العالم الافتراضي فرصة لا تعوض، يحصل من خلالها على ما يحتاج بغض النظر عن مشروعيَّة هذه الطرائق أم عدم مشروعيتها.

وأما فيما يخص المؤسسات الأخرى التي تستخدم الذكاء الاصطناعي في الحد من ممارسة الجريمة الإلكترونيّة فقد حصلت **وزارة الداخليّة** على أعلى درجة حيث بلغت عدد الإجابات (40) إجابة من أصل (50) إجابة، يليها في المرتبة الثانية **نيابة الجرائم الإلكترونيّة** حيث حصلت على (13) إجابة، إضافة **للأجهزة الأمنيّة** التي جاءت في المرتبة الثالثة حيث حصلت على (6) إجابات، **بينما جاءت شركة جوال** في المرتبة الرابعة فقد حصلت على (3) إجابات، وفي المرتبة الأخيرة **شركة الأمن المعلوماتي** حيث بلغ عدد إجاباتها (2)، إن النتيجة السابقة منطقيّة حيث إن وزارة الداخلية تسعى إلى تطبيق الذكاء الاصطناعي في مواجهة الجرائم الإلكترونيّة هذا ما أكده (الهندي، 2020) خلال

المقابلة التي أجريت معه أنه من خلال الاجتماعات التي تعقد مع القيّادة قي جهاز الشرطة الفلسطيني يتم التركيز على تعزيز تطبيق الذكاء الاصطناعي واستثماره في المجالات كافّةً، والحد منها، فقد دخل جهاز الشرطة الفلسطينية عالم الذكاء الاصطناعي من خلال استخدام الخوذة الذكيّة القائمة في مبدأ عملها على الذكاء الاصطناعي، والتعلم الآلي حيث إنها مرتبطة في عملها مع ما يسمى بالعمليات المركزيّة، وقدرتها على العمل الليلي من خلال تصنيف المطلوبين، كما حصلت الشرطة على قرار مجلس الوزارء بتطبيق الكاميرات القائمة على نظام الذكاء الاصطناعي والتتبع الذكي، إضافة إلى أن الشرطة الفلسطينيّة شريك إلى جانب النيابة والمحاكم والوزارة في تتبع الجرائم الإلكترونيّة، فكل منها مكمل للآخر في مجال اختصاصه، وهذا ما تؤكده النظريّة التكامليّة التي ترى أنَّ ممارسة الجريمة لا تقف عند سبب وعامل واحد، وإنما تعود إلى أسباب وعوامل متعددة، كما أن مكافحتها تحتاج إلى تعاون وتشبيك من عدة أطراف مكملة لبعضها بعضًا، هذا ما أكدته نتيجة التعاون بين الوزارة والمؤسسات الأخرى في مجال تتبع الجريمة الإلكترونيّة، حيث أكد المبحوثون أن هناك تعاونًا بين الوزارة والمؤسسات الأخرى في مجال تتبع الجريمة الإلكترونيّة والحد منها، إضافة الى أن هناك اتصالًا وتواصلًا من فريق فلسطين للاستجابة لطوارئ الحاسوب (الأمن المعلوماتي) في حال وقوع هجمات إلكترونيّة فقد بلغت عدد الإجابات (46) إجابة من أصل (50) إجابة.

مما سبق يمكن التأكيد على وجود ارتباط بين الوزارة والشرطة ونيابة الجرائم الإلكترونيّة وأهميّة التعاون بين الجهات الحكومية؛ لِلْحَدِّ من هذه الظاهرة الآخذة في الانتشار في ظل المُعوقات التي تواجهها، كما أكد المبحوثون على سعي الوزارة إلى مزيد من التعاون مع مختلف المؤسسات الأخرى، فهذا التنسيق يساعد على التوصل إلى الجناة والحد من الجريمة الإلكترونيّة كون الشرطة هي جهة تنفيذيّة والوزارة تحتوي على مبرمجين ومتخصصين، يساعدون في التوصل إلى موقع الجناة، فتقاطع هذا التعاون بينهم ما هو إلا للوصول إلى مصلحة المواطن وتوفير الاستخدام الآمن للشبكات الإلكترونيّة في المجتمع الفلسطيني، تتفق هذه النتيجة مع نتيجة دراسة (البشري، 2000) بعنوان "الأدلة الجنائيّة الرقميّة مفهومها ودورها في الإثبات" التي أكدت على ضرورة تحقيق التعاون والتنسيق بين أجهزة العدالة الجنائيّة والشركات المزودة للأجهزة والمعدات الإلكترونيّة والحديثة، إضافة إلى الاستثمار في تقنيات المعلومات، ودراسة (العنزي، 2003) بعنوان "وسائل التحقيق في جرائم المعلومات" التي أكدت على أهميّة العمل على التنسيق بين وزارة الداخلية والمؤسسات الأخرى الموفرة لنظم أمن المعلومات والشركات المزودة لخطوط الاتصالات ومزودي خدمة الإنترنت؛ لمساعدة الجهات الأمنيّة في ضبط تلك الجرائم، إضافة إلى نوعيّة وجودة التطبيقات المقدمة والأجهزة المستخدمة.

3.5 الإستنتاجات:

توصلت الدراسة إلى مجموعة من الاستنتاجات لعل من أهمها أنها أوضحت:

- أن للذكاء الاصطناعي دورًا قويًّا وفعالًا جدًّا في الكشف عن الجريمة الإلكترونيّة وصد الهجمات الإلكترونيّة التي تتعرض لها الشبكات، إضافة إلى دورها في التوصل إلى مرتكبي الجرائم الإلكترونيّة.
- أنه من الضروري العمل على سن قوانين وتشريعات متعلقة ببرامج الذكاء الاصطناعي وأنظمته، بالإضافة إلى تشديد القوانين على مرتكبي الجرائم الإلكترونيّة والتعامل معها بصرامة.
- أنَّ الاحتلال الإسرائيلي والبنية التحتية والموازنات المآليّة والكادر البشري هي أبرز المُعوقات التي تعوق عملية تطبيق الذكاء الاصطناعي في الحد من ممارسة الجريمة الإلكترونيّة.
- أن المجتمع الفلسطيني لا يزال بعيدًا كلَّ الْبُعْدِ عن التطور التكنولوجي، ولا يزال يحتاج إلى المزيد من الجهد في سبيل التوصل إلى التطور التكنولوجي.
- أن الوزارة تفتقر إلى وجود أقسام خاصة بالذكاء الاصطناعي، تحتوي على آليّات تعمل على الحد من الجرائم الإلكترونيّة.
- أن العاملين في الوزارة لديهم خبرة قليلة في الذكاء الاصطناعي وبرامجه ولديهم افتقار واضح الى الدورات التدريبية ذات العلاقة في برامج الذكاء الاصطناعي ومتابعة مرتكبي الجرائم الإلكترونيّة.
- أن الوزارة تسعى إلى التطور وتطبيق الذكاء الاصطناعي وأنه يتم تطبيقه ضمن الإمكانات المتوفرة لديها وهي ضمن برامج محدودة جدًّا.
- أن هناك تعاونًا وتنسيقًا بين الوزارة والمؤسسات الحكومية الأخرى الموجودة في المجتمع الفلسطيني.
- أن هناك ندرة وقلة في الأبحاث والدراسات ذات العلاقة بتطبيق الذكاء الاصطناعي في مواجهة الجريمة الحاصلة في الفضاء الإلكتروني.

4.5 التوصيات:

توصلت الدراسة إلى مجموعة من التوصيات التي من شأنها أن تساعد في تخطي المُعوقات التي تواجه تطبيق الذكاء الاصطناعي في الحد من ممارسة الجريمة الإلكترونيّة، لعل من أهم تلك التوصيات الآتي:

- العمل على تفعيل دور الذكاء الاصطناعي وتطبيقه في الكشف عن الجرائم المرتكبة في الفضاء الإلكتروني.
- العمل على سن قوانين وتشريعات تتوافق مع تطبيق الذكاء الاصطناعي.
- العمل على تطوير البنيّة التحتيّة بما يتناسب مع تطبيقات الذكاء الاصطناعي، بالإضافة الى توفير خبراء ومتخصصين لتطوير البنية التحتية في فلسطين.
- ضرورة العمل على غرس ثقافة الذكاء الاصطناعي بين أبناء المجتمع الفلسطيني واللحاق بسلسلة التطورات التكنولوجيّة الحديثة.
- ضرورة فتح قسم خاص يسمى (الذكاء الاصطناعي وتتبع الجرائم الالكتروني)؛ كي لا تتداخل أعمال مختلف والأقسام مع بعضها البعض.
- ضرورة وضع آليّة عمل مفصلة وواضحة للعمل من خلالها على تطبيق برامج الذكاء الاصطناعي.
- ضرورة العمل على تكثيف الدورات وورشات العمل ذات الفائدة للموظفين ونقل الخبرة والمهارة للآخرين؛ لتوسيع نطاق الاستفادة في هذا المجال.
- الاطِّلاع على تجارب الدول السابقة التي حققت نجاحًا في هذا المجال.
- التعاون والتنسيق مع الدول والمؤسسات المانحة التي تمتلك إمكانات في توفير موازنات ماليّة، وتوفير معدات وأجهزة ذات علاقة بتطبيق برامج الذكاء الاصطناعي وأنظمته.
- ضرورة فتح تخصص الذكاء الاصطناعي للبكالوريوس وأن لا تقتصر فقط على درجة الماجستير والدكتوراه.
- ضخ الخبرة والمعرفة المستمرة للعاملين في مجال الذكاء الاصطناعي لتمنية قدراتهم.
- توفير كوادر حاصلة على مؤهلات علميّة في مجال الذكاء الاصطناعي.
- تعزيز التعاون والتنسيق بين الوزارة والشرطة (وحدة الجرائم الإلكترونيّة).
- تعزيز الاهتمام بتطوير الأبحاث والدراسات الخاصة بالذكاء الاصطناعي وإرفاق مناهج تختص بالذكاء الاصطناعي في المدارس والجامعات.

قائمة المصادر المراجع

- القران الكريم.

المراجع العربية:

أولا: الكتب:

- أبو غزالة، طلال (2019). **العالم المعرفي المتوقد**، ط2، دار أبو طلال للترجمة والتوزيع والنشر: عمان.
- الأمين، مرتضى (2016). **التوثيق الإعلامي وتكنولوجيا المعلومات**، ط1، دار أمواج للنشر والتوزيع: عمان.
- البداينة، ذياب (2014). **الجرائم المُستحدثة في ظل المتغيرات والتحولات الإقليميّة والدوليّة**، كليّة العلوم التكنولوجيّة : عمان.
- البداينة، ذياب والخريشا، رافع (2013). **نظريات علم الجريمة**، ط1، دار الفكر للنشر والتوزيع: الأردن.
- براك، أحمد وجراده، عبد القادر (2019). **الجرائم الإلكترونية في التشريع الفلسطيني**، دار الشروق للنشر والتوزيع: رام الله.
- بنسون، ستيف وستانديج، كريج (2020). **نظم المعلومات**، ترجمة محمد مجدي وعزت محمود، ط1، مجموعة النيل العربية للنشر والتوزيع: القاهرة.
- الحسيناوي، علي (2018). **جرائم الحاسوب والانترنت**، ط1، دار اليازور للنشر والتوزيع: عمان.
- خليفة، إيهاب (2019). **مجتمع ما بعد المعلومات تأثير الثورة الصناعية الرابعة على الأمن القومي**، ط1، العربي للنشر والتوزيع: القاهرة.
- دهشان، يحيى (2019). المسؤولية الجنائية عن جرائم الذكاء الاصطناعي، ط1،جلة الشريعة والقانون لنشر والتوزيع: الامارات.
- الرواشدة، مصطفى (2020). **جرائم الإبتزاز الإلكتروني**، ط1، دار الكتاب الأكاديمي للنشر والتوزيع: عمان.
- الرواشدة، ولاء والطراونة، هناء والضلاعين، معتصم (2020). **علم الجريمة (المفهوم – الوقاية –العقاب)**، ط1، دار الخليج للنشر والتوزيع: الشارقة.

- الزعارير، أحمد وأبو عبيلة، مصطفى وأبو الملحم، محمد (2015). **مدخل إلى علم الجريمة**، ط1، دار البيروني للنشر والتوزيع: عمان.
- سليمان، نورهان (2020). **تكنولوجيا الاعلام**، ط1، مؤسسة حورس الدولية للنشر والتوزيع: الاسكندرية.
- الصبار، أيمن (2015). **المسؤوليّة الجنائيّة لمستخدمي شبكات التواصل الإجتماعي**، ط1، دار المنهل للنشر والتوزيع: عمان.
- الصمد، أسماء وكريمة، محمد (2020). **تطبيقات الذكاء الاصطناعي ومستقبل تكنولوجيا المعلومات**، ط1، دار المنهل للنشر والتوزيع: عمان.
- عفيفي، جهاد (2015). **الذكاء الاصطناعي والأنظمة الخبيرة**، ط1، دار المنهل للنشر والتوزيع: عمان.
- عمر، أحمد (2008). **معجم اللغة العربية المعاصرة**، ط1، عالم الكتب للنشر والتوزيع: القاهرة.
- العيد، وليد (2018). **الذكاء والذكاءات المتعددة**، ط1، دار الكتب العالمية للنشر والتوزيع: بيروت.
- الفاخري، سالم (2018). **سيكولوجيّة الابداع**، ط1، دار الكتاب الاكاديمي للنشر والتوزيع: عمان.
- كاظم، أحمد (2012). **مبادئ الذكاء الاصطناعي وتطبيقاته ومراحل تطوره**، ط3، جامعة الامام الصادق: العراق.
- لطفي، خالد (2019). **الدليل الرقمي ودوره في إثبات الجريمة المعلوماتيّة**، ط1، دار الفكر الجامعي للنشر والتوزيع: الإسكندرية.
- مجيد، سحر (2019). **الجرائم المستحدثة دراسة معمقة ومقارنة في عدة جرائم**، ط1، المركز العربي للنشر والتوزيع: القاهرة.
- محمد، جمال (2015). **نظم المعلومات**، ط1، دار المعتز للنشر والتوزيع: عمان.
- محمد، لينا (2016). **الجرائم الإلكترونيّة ماهيتها وطرق مكافحتها**، ط1، دار خالد الليحاني للنشر والتوزيع: مكة المكرمة.
- مدين، محمد (2019). **الجريمة الإلكترونيّة وتحديات الأمن القومي**، ط2، المصرية للنشر والتوزيع: القاهرة.
- مدين، محمود (2020). **فن التحقيق والاثبات في الجرائم الالكتروني**، ط1، دار المصري للنشر والتوزيع: القاهرة.
- مرق، سامح (2021). **كلام في العلم**، ط1، مركز المحروسة للنشر والتوزيع: القاهرة.

- المنجد، بشير (2020). **الآلة الذكيّة من ديكارت وحتى دماغ غوغل**، ط1، دار الكتب للنشر والتوزيع: لندن.
- موسى، عبدالله وبلال، أحمد (2019). **الذكاء الإصطناعي ثورة في تقنيات العصر**، ط1، دار الكتب المصرية للنشر والتوزيع: القاهرة.
- نصار، غادة (2017). **الإرهاب والجريمة الإلكترونيّة**، ط1، العربي للنشر والتوزيع: القاهرة.
- الهاد، محمد (2021). **الذكاء الاصطناعي ومعالمه وتطبيقاته وتأثيراته التنموية والمجتمعية**، ط1، الدار المصرية اللبنانية للنشر والتوزيع: القاهرة.
- الهاشيمي، رفد (2019). **الإرهاب الإلكتروني القانوني**، ط1، دار أمجد للنشر والتوزيع: عمان.
- وريكات، عايد (2004). **نظريات علم الجريمة**، ط1، دار الشروق للنشر والتوزيع: الأردن.
- ياسين، سعد (2018). **نظم المعلومات الإدارية**، ط1، دار اليازور العلمية للنشر والتوزيع: عمان.
- ياسين، سعد (2020). **الإدارة الإلكترونيّة**، ط1، دار اليازور للنشر والتوزيع: عمان.

ثانياً: المجلات والأبحاث:

- جباري، لطيفة (2017). دور نماذج الذكاء الإصطناعي في اتخاذ القرارات، **مجلة العلوم الإنسانيّة**، مجلد (1)، عدد (1)، ص ص (121 – 132).
- شهاب، أشرف (2018). الذكاء الاصطناعي بهاجم الذكاء الاصطناعي، **مجلة الاهرام**، مجلد (72)، عدد (213)، ص ص (72–75).
- الشهري، حسن (2009). قانون موحد لمكافحة الجرائم المعلوماتيّة، **المجلة العربيّة للأبحاث والعلوم الإنسانيّة والاجتماعية**، مجلد (1)، عدد (1)، ص ص (315–526).
- عبد الباقي، مصطفى (2018). التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين: دراسة مقارنة، **مجلة دراسات علوم الشريعة والقانون**، الجامعة الأردنية، مجلد (4)، عدد (45)، ص ص (284–299).
- لخضر، دولي ونفيسة، ناصري (2018). دور الذكاء الاصطناعي في مواجهة الجريمة الإلكترونيّة، **مجلة المؤشر**، مجلد(2)، عدد (2)، ص ص (52–57).

ثالثاً: الرسائل:

- البشير، سيدي محمد (2010). **دور الدليل الرقمي في إثبات الجرائم المعلوماتيّة– دراسة تحليلية تطبيقية**، رسالة ماجستير غير منشورة، جامعة نايف للعلوم الأمنية: الرياض.

- البلوي، سالم (2009). **التقنيات الحديثة في التحقيق الجنائي ودورها في ضبط الجريمة،** رسالة ماجستير غير منشورة، جامعة نايف للعلوم الأمنية: الرياض.
- العنزي، سليمان (2003). **وسائل التحقيق في جرائم المعلومات،** رسالة ماجستير غير منشورة، جامعة نايف للعلوم الأمنية: الرياض.
- القحطاني، عبد الله (2014). **تطوير مهارات التحقيق في مواجهة الجرائم المعلوماتيّة،** رسالة ماجستير غير منشورة، جامعة نايف للعلوم الأمنية: الرياض.

المراجع الأجنبية:

Firstly: Books:

- Joshi, Ameet (2019**). Machine Learning and Artifical Intelgence**, 1Ed, Springer Publishers :USA.
- Kumar, Praveen & Shree, Vidhya & Himremath, Lingayya & Rajandron, Sindhu (2019). **The Use of the Use of Modern Technology in Smart Waste Mangment and Recycling: Artificial Intelligence and Machine Learning**, 1Ed, Springer cham Publishers: Germany.
- Kimari, Neha & Shivastara, Narsh & Bhatele, Kirti (2019)**. The Role of Artifical intelligenc in cyber security**, 1Ed, IGI Global: Pennsylvania.
- Nathan, Ross (2019). **How Artifical Intelligenc Works,** 1Ed, Universty of the Westen: Cape.
- Alshahat, Adel (2018). **Adcanced Aplications for Artificial Neural Networkd**, 1Ed, National and Unviresity in Zagreb: Croatia.
- Nones, Amina & Anjali, Palepn & Wallac, Merrick (2017). **Artifical Intelligence,** 1Ed, Boston Uni: UK.
- Clough, Jonathan (2015). **Principles of Cybercrime**, 2Ed, Cambridge Universit, Cambridge: England.
- Cross, Micheal (2008). **Scene of the cyber crime**, 1Ed, syngress Publisher: USA.
- Louis, Jean (1987). **Problem Solving and Artifical Intelligence**, 2Ed, Prentice Hall Publisher, Michigan: USA.

Secondly: Journal:

- Memish, Ziad & Altuwajir, Majid& Almoeen, Abdulgader & Enani, Sarah (2021). The Saudi Data & Artificial Intelligence Authority (SDAIA) Vision: Leading the Kingdom's Journey toward Global Leadership, **Journal of Epidemiology and Global Health**, Vol (11), No (2), pp (140-142).
- Bibel, Wofgang (2020**).** On The Development of AL in Germany, **KL- Kunstlicne Intelligence**, Vol (34), No (2), pp (251-258).
- Yakub, Ismail & Shittu, Fatima & Job, Goteng & Aron, Achi & Atiku, Shidaawa (2020). Survey On Applications Of Artificial Intelligence in Cyber Security, **Iternational Journal of Scientifc and Technology Researsh**, Vol (9), No (10), pp (2277-8616).
- Hagando, Thilo & Wezel, Katharina (2019). Challenges for Artifical Intelligence or what can do**, Journal of Artifical intelligence and society,** Vol (2), No (35), pp (1-11).

- Davenport, Thamas & Kalakota, Ravi (2019). The potential for artificial intelligence in healthcare**, Futuer Journal**, Vol (6), No (2), pp (94-98).
- Gupta, Praveen & Shree, Vidhya & Hiremath, Lingayya & Rajandran, sindhu (2019). The Use of Modern Technology in Smart Waste Management and Recyling Artificial Intelligence and machine Learning, **Journal of King Saud University - Computer and Information Sciences**, Vol (35), No (5), pp (2072-2087).
- Supriyanto, Ganden & Widiaty, Isma & Abdullah, Ade & Yustiana, YR (2018). Application of expert system for education**, Article**, Vol **(**434), No (1), pp (1-4).
- Frunz, Marins (2016). Cyber crime, **Article,** Vol (1), No (1), pp (207-220).
- Gallo, cresenzio (2015). Artifical neural Network, **in the encyclopedia of information science and technology**, Vol (3), No (10), pp (6369-6378).
- Bhasker, Neeraja (2015). Genetic Algorithm Basea For Identification Of Cybercriminal Networks From Online social Media, **International Journal of Engineering & Technology**, Vol (3), No (15), pp (2278- 0181).
- Salekhov, Lailya & Nurgaliev, Albert & Zaripova, Rinata & Khakimullina, Nail (2013). The principles of Desiging an Expert System in Teaching, **Universal Journal of education Resear**, Vol (1), No (2), pp (42-47).
- Bilal, Alhayani & Mohammed, Husam & Chaloob, Ibrahim & Ahmed, Jehan (2020). Effectiveuss of Artifical Intelligence Techiniques Againt Cyber Security Risks Apply of It Indastry, **Article in International Journal of Artificial intelligence**, Vol (16), No (47), pp (2214- 7853).
- Dilek, Selma & Cakır, Hussein & Aiden, Mustafa (2015). Applications of artificial intelligence techniques to combating cyber crimes, **Article**, **International Journal of Artificial intelligence**, Vol (6), No (1), pp (21-39).
- Rana, Nikita & Dhar, Shivani & Jagdale, Priyanka & Javalkar, Nikhil (2014). Implementation Of An Expert System for the Enhancement Of E-Commerce Securit, **Article in international journal**, Vol (2), No (3), pp (49-53).
- Linda, Ondrej & Todd, Vollmer & Milos, Maric (2009). Neural Network based intrusion detection system for critical infrastructure, **Article In 2009 International joint conference on neural networks**, Vol (1), No (1), pp (1827 – 1834).

Third: Research:

- Xu, Xiaojun & Wang, Qi & Li, Huichen & Borisov, Nikita (2021). **Detecting AI Trojans Using Meta Neural Analysis**, Symposium on Security and Privacy, University of Illinois at Urbana-Champaign: Illinois.
- Crowder, James & Carbone, John (2020). **Artificial neural diagnostics and prognostics Self-soothing in cognitive systems**, Article in Artificial psychology, Springer Cham Publishers: Switzerland.
- Ekanem, David (2019). **Artificial Intelligence as Mechanism for Crime Control in Nigeri,** Master thesis, University of Uyo: Nigeria.
- Kooistra, Alex (2019). **Artifical Intelligence Supporting security operations Centers**, Master Thesis, University of Leiden campus den hag: Netherland.
- Williamson, Nancy (2014). **Challenges of catching the cyber criminal,** Doctoral dissertation, Utica College: New York.
- Pereira, Teresa (2014). **Challengs in information security**, Article ,University of Minho, Portugal,

المراجع إلكترونيّة:

- Fujimaki, Royhei (2020). **The (6) Challenges Of Implementing Artifical Intelligenc**, Internet Journal of Criminology, for more details the following link: https://www.americanmachinist.com/, Retrieved (2020/10/19) the hour (18:30) PM.
- Prakash, Febin & Sadawarti, Harsh & Baskar, Kala (2019). **Cyber Crime: Challenges & Its Classification**, Internet Journal, for more details the following link: https://www.researchgate.net/profile/Kala, Retrieved (2020/10/19), the hour (19:50) PM.
- Sharma, Aarushi (2019). **What are The Components Of Artificial Intelligence: How Artificial Intelligence Is Used**, Internet Journal, for more details the following link: https://medium.com/@Aarushi_Sharma/, Retrieved (2020/12/20), the hour (15:30) PM.

- وزارة الاتصالات وتكنولوجيا المعلومات (2021). **تقرير بعنوان** "**الذكاء الاصطناعي في فلسطين**" لمزيد من التوضيح انظراي للموقع الالكتروني ادناه:

https://www.mtit.gov.ps/index.php/c_home/showNew/2355، تم الاسترجاع في تاريخ (22-04-2021) الساعة (8:30) مساءً.

- صحيفة المصراوي (2021). **تقرير بعنوان** "**أنظمة الذكاء الإصطناعي تلتقط نسبة ضئيلة من المحتوى المسيء على فيسبوك**"، لمزيد من التوضيح أنظراي للموقع الالكتروني أدناه:

https://www.masrawy.com/news/news_publicaffairs/details/2021/10/5/2100903/%D9%85%D9، تم الاسترجاع في تاريخ (08\10\2021)، الساعة (5:59) مساءً.

- صحيفة البيان (2021). تقرير بعنوان "**الذكاء الاصطناعي يتنبأ بفيروسات قاتلة قادمة للبشر**"، لمزيد من التوضيح أنظر/ي للموقع الالكتروني أدناه:

https://www.albayan.ae/health/life/1، تم الاسترجاع في تاريخ (08\10\2021) الساعة (18:32) مساءً.

- صحيفة فلسطين (2021). تقرير بعنوان "**الجهات الحكومية بغزة تنظم ورشة عمل حول الذكاء الإصطناعي**"، لمزيد من التفاصيل أنظر/ ي للموقع الإلكتروني أدناه:

https://felesteen.news/post/84247، تم الإسترجاع في تاريخ (2021/10/09) الساعة الـ (19:00) مساءً.

- صحيفة معاً (2021). **تقرير بعنوان** "**ورشة عمل حول التكنولوجيا الجديدة والذكاء الإصطناعي**"، لمزيد من التفاصيل أنظر/ ي للموقع الإلكتروني أدناه:

https://www.maannews.net/news/l، تم الإسترجاع في تاريخ (2021/10/09) الساعة الـ (19:30) مساءً.

- صحيفة وفا (2021). تقرير بعنوان "**اتفاقية لتعزيز تكنولوجيا الاتصالات وإدخال أدوات الذكاء الإصطناعي في العمل الحكومي**"، لمزيد من التفاصيل أنظر/ ي للموقع الإلكتروني أدناه:
http://www.wafa.ps/Pages/Details/25931، تم الإسترجاع في تاريخ (2021/10/01) الساعة الـ (15:30) مساءً.
- صحيفة الرياض (2021). تقرير بعنوان "**إطلاق المنصة الوطنية للذكاء الاصطناعي**"، لمزيد من التفاصيل أنظر/ ي للموقع الإلكتروني أدناه:
https://www.alriyadh.com/1878964 تم الإسترجاع في تاريخ (2021/6/06) الساعة الـ (14:30) مساءً.
- صحيفة العين الإخبارية (2021). تقرير بعنوان "السعودية توسع اعتمادها على الذكاء الاصطناعي في الرعاية الصحية"، لمزيد من التفاصيل أنظر/ ي للموقع الإلكتروني أدناه:
https://al-ain.com/article/saudi-arabia-promotes-the-use-of-artificial-intell تم الإسترجاع في تاريخ (2021/06/04) الساعة الـ (12:30) ظهراً.
- صحيفة الجزيرة (2020). تقرير بعنوان "الذكاء الاصطناعي في عالم الجرائم المعلوماتية"، لمزيد من التفاصيل أنظر/ ي للموقع الإلكتروني أدناه:
https://www.al-jazirah.com/2020/20201025/ar5.htm تم الإسترجاع في تاريخ (2020/06/20) الساعة الـ (12:00) ظهراً.

المقابلات الشخصيّة:

- الهندي، سامر (2020). **عدد الجرائم الإلكترونيّة في الضفة من عام (2016-2021)**، المدير العام لوحدة الجرائم الإلكترونيّة في الضفة الغربيّة، مقابلة شخصيّة تمّ إجراءها يوم الثلاثاء الموافق (2020/10/20) الساعة الـ (11:30) صباحاً.
- مقابلة رقم 1 (2021)، **مُعوّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة**، مقابلة شخصيّة تمّ إجراءها يوم الإثنين الموافق (2021/09/20) الساعة الـ (10:10) صباحاً.
- مقابلة رقم 2 (2021)، **مُعوّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة**، مدير أمن المعلومات، مقابلة شخصيّة تمّ إجراءها يوم الإثنين الموافق (2021/09/20) الساعة الـ (10:45) صباحاً.

- مقابلة رقم 3 (2021)، **مُعوّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة**، مبرمج في قسم الحكومة الإلكترونيّة، مقابلة شخصيّة تمّ إجراءها يوم الإثنين الموافق (2021/09/20) الساعة الـ (12:30) ظهراً.
- مقابلة رقم 4 (2021)، **مُعوّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة**، الدعم الفني، مقابلة شخصيّة تمّ إجراءها يوم الإثنين الموافق (2021/09/20) الساعة الـ (2:00) ظهراً.
- مقابلة رقم 5 (2021)، **مُعوّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة**، مبرمج في قسم أنظمة المعلومات، مقابلة شخصيّة تمّ إجراءها يوم الثلاثاء الموافق (2021/09/21) الساعة الـ (8:30) صباحاً.
- مقابلة رقم 6 (2021)، **مُعوّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة**، مهندس في قسم الحاسوب الحكومي، مقابلة شخصيّة تمّ إجراءها يوم الثلاثاء الموافق (2021/09/21) الساعة الـ (10:30) صباحاً.
- مقابلة رقم 7 (2021)، **مُعوّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة**، مهندس في قسم الحاسوب الحكومي، مقابلة شخصيّة تمّ إجراءها يوم الثلاثاء الموافق (2021/09/21) الساعة الـ (12:30) ظهراً.
- مقابلة رقم 8 (2021)، **مُعوّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة**، مهندس في قسم الشكاوي، مقابلة شخصيّة تمّ إجراءها يوم الثلاثاء الموافق (2021/09/21) الساعة الـ (2:00) ظهراً.
- مقابلة رقم 9 (2021)، **مُعوّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة**، مهندس في قسم الشكاوي، مقابلة شخصيّة تمّ إجراءها يوم الأربعاء الموافق (2021/09/22) الساعة الـ (8:15) صباحاً.
- مقابلة رقم 10 (2021)، **مُعوّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله**

والبيرة، مهندس في قسم هندسة الحاسوب، مقابلة شخصيّة تمّ إجراءها يوم الأربعاء الموافق (2021/09/22) الساعة الـ (10:20) صباحاً.

- مقابلة رقم 11 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مهندس في قسم الحكومة الإلكترونية، مقابلة شخصيّة تمّ إجراءها يوم الأربعاء الموافق (2021/09/22) الساعة الـ (12:40) ظهراً.
- مقابلة رقم 12 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مهندس في قسم التطوير الفني، مقابلة شخصيّة تمّ إجراءها يوم الأربعاء الموافق (2021/09/22) الساعة الـ (1:40) ظهراً.
- مقابلة رقم 13 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مهندس في قسم الحكومة الإلكترونية، مقابلة شخصيّة تمّ إجراءها يوم الخميس الموافق (2021/09/23) الساعة الـ (8:20) صباحاً.
- مقابلة رقم 14 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مهندس في قسم الشكاوي، مقابلة شخصيّة تمّ إجراءها يوم الخميس الموافق (2021/09/23) الساعة الـ (9:30) صباحاً.
- مقابلة رقم 15 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مدير قسم الحكومة الإلكترونية، مقابلة شخصيّة تمّ إجراءها يوم الخميس الموافق (2021/09/23) الساعة الـ (12:30) ظهراً.
- مقابلة رقم 16 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مهندس في قسم الشكاوي، مقابلة شخصيّة تمّ إجراءها يوم الأحد الموافق (2021/09/26) الساعة الـ (8:30) صباحاً.
- مقابلة رقم 17 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مدير قسم الحكومة الإلكترونية، مقابلة شخصيّة تمّ إجراءها يوم الأحد الموافق (2021/09/26) الساعة الـ (10:30) صباحاً.

- مقابلة رقم 18 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مهندس في قسم الشكاوي، مقابلة شخصيّة تمّ إجراءها يوم الأحد الموافق (2021/09/26) الساعة الـ (12:40) ظهراً.
- مقابلة رقم 19 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مهندس في قسم الشكاوي، مقابلة شخصيّة تمّ إجراءها يوم الإثنين الموافق (2021/09/27) الساعة الـ (8:10) صباحاً.
- مقابلة رقم 20 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مهندس في قسم الاتصالات، مقابلة شخصيّة تمّ إجراءها يوم الإثنين الموافق (2021/09/27) الساعة الـ (9:45) صباحاً.
- مقابلة رقم 21 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مهندس في قسم الشكاوي، مقابلة شخصيّة تمّ إجراءها يوم الإثنين الموافق (2021/09/27) الساعة الـ (12:55) ظهراً.
- مقابلة رقم 22 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مهندس في قسم الشكاوي، مقابلة شخصيّة تمّ إجراءها يوم الإثنين الموافق (2021/09/27) الساعة الـ (2:15) ظهراً.
- مقابلة رقم 23 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مدير قسم الحاسوب الحكومي، مقابلة شخصيّة تمّ إجراءها يوم الثلاثاء الموافق (2021/09/28) الساعة الـ (8:30) صباحاً.
- مقابلة رقم 24 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مهندس في قسم الشكاوي، مقابلة شخصيّة تمّ إجراءها يوم الثلاثاء الموافق (2021/09/28) الساعة الـ (10:30) صباحاً.
- مقابلة رقم 25 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله**

والبيرة، مدير الحكومة الإلكترونيّة، مقابلة شخصيّة تمّ إجراءها يوم الثلاثاء الموافق (2021/09/28) الساعة الـ (12:30) ظهراً.

- مقابلة رقم 26 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مهندس في قسم الحكومة الإلكترونيّة، مقابلة شخصيّة تمّ إجراءها يوم الثلاثاء الموافق (2021/09/28) الساعة الـ (1:45) ظهراً.
- مقابلة رقم 27 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مدير قسم الحاسوب الحكومي، مقابلة شخصيّة تمّ إجراءها يوم الاربعاء الموافق (2021/09/29) الساعة الـ (8:10) صباحاً.
- مقابلة رقم 28 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مبرمج في قسم الحاسوب الحكومي، مقابلة شخصيّة تمّ إجراءها يوم الاربعاء الموافق (2021/09/29) الساعة الـ (10:30) صباحاً.
- مقابلة رقم 29 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مبرمج في قسم الحاسوب الحكومي، مقابلة شخصيّة تمّ إجراءها يوم الاربعاء الموافق (2021/09/29) الساعة الـ (12:30) ظهراً.
- مقابلة رقم 30 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مدير دائرة المشاريع في قسم الحاسوب الحكومي، مقابلة شخصيّة تمّ إجراءها يوم الخميس الموافق (2021/09/30) الساعة الـ (8:30) صباحاً.
- مقابلة رقم 31 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** رئيس قسم الشبكات، مقابلة شخصيّة تمّ إجراءها يوم الخميس الموافق (2021/09/30) الساعة الـ (11:30) صباحاً.
- مقابلة رقم 32 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مُبرمج في قسم الحاسوب الحكومي، مقابلة شخصيّة تمّ إجراءها يوم الأحد الموافق (2021/09/03) الساعة الـ (8:30) صباحاً.

- مقابلة رقم 33 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مُبرمج في قسم الحكومة الإلكترونيّة، مقابلة شخصيّة تمّ إجراءها يوم الأحد الموافق (2021/09/03) الساعة الـ (10:30) صباحاً.
- مقابلة رقم 34 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مُبرمج في قسم الحكومة الإلكترونيّة، مقابلة شخصيّة تمّ إجراءها يوم الأحد الموافق (2021/09/03) الساعة الـ (12:30) ظهراً.
- مقابلة رقم 35 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مُبرمج في قسم الحكومة الإلكترونيّة، مقابلة شخصيّة تم إجراءها يوم الاثنين الموافق (2021/09/04) الساعة الـ (8:10) صباحاً.
- مقابلة رقم 36 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مُبرمج في قسم الحكومة الإلكترونيّة، مقابلة شخصيّة تمّ إجراءها يوم الاثنين الموافق (2021/09/04) الساعة الـ (10:20) صباحاً.
- مقابلة رقم 37 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مهندس في قسم الحكومة الإلكترونيّة، مقابلة شخصيّة تمّ إجراءها يوم الاثنين الموافق (2021/09/04) الساعة الـ (12:20) ظهراً.
- مقابلة رقم 38 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مهندس في قسم الاتصالات، مقابلة شخصيّة تمّ إجراءها يوم الثلاثاء الموافق (2021/09/05) الساعة الـ (8:45) صباحاً.
- مقابلة رقم 39 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مهندس في قسم الاتصالات، مقابلة شخصيّة تمّ إجراءها يوم الثلاثاء الموافق (2021/09/05) الساعة الـ (11:15) صباحاً.
- مقابلة رقم 40 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله**

والبيرة، مهندس في قسم أمن المعلومات، مقابلة شخصيّة تمّ إجراءها يوم الثلاثاء الموافق (2021/09/05) الساعة الـ (1:18) صباحاً.

- مقابلة رقم 41 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مهندس في قسم أمن المعلومات، مقابلة شخصيّة تمّ إجراءها يوم الأربعاء الموافق (2021/10/06) الساعة الـ (9:10) صباحاً.
- مقابلة رقم 42 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مبرمج في قسم أمن المعلومات، مقابلة شخصيّة تمّ إجراءها يوم الأربعاء الموافق (2021/10/06) الساعة الـ (11:15) صباحاً.
- مقابلة رقم 43 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مهندس في قسم الإتصالات، مقابلة شخصيّة تمّ إجراءها يوم الأربعاء الموافق (2021/10/06) الساعة الـ (1:30) ظهراً.
- مقابلة رقم 44 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مبرمج في قسم الدعم الفني، مقابلة شخصيّة تمّ إجراءها يوم الخميس الموافق (2021/10/07) الساعة الـ (8:30) صباحاً.
- مقابلة رقم 45 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مهندس في قسم الإتصالات، مقابلة شخصيّة تمّ إجراءها يوم الخميس الموافق (2021/10/07) الساعة الـ (10:30) صباحاً.
- مقابلة رقم 46 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مهندس في قسم جودة الخدمة، مقابلة شخصيّة تمّ إجراءها يوم الخميس الموافق (2021/10/07) الساعة الـ (1:15) ظهراً.
- مقابلة رقم 47 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مبرمج في قسم أمن المعلومات، مقابلة شخصيّة تمّ إجراءها يوم الأحد الموافق (2021/10/10) الساعة الـ (8:15) صباحاً.

- مقابلة رقم 48 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مبرمج في قسم الشكاوي، مقابلة شخصيّة تمّ إجراءها يوم الأحد الموافق (2021/10/10) الساعة الـ (10:45) صباحاً.
- مقابلة رقم 49 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مهندس في قسم المقاسم، مقابلة شخصيّة تمّ إجراءها يوم الأحد الموافق (2021/10/10) الساعة الـ (12:45) صباحاً.
- مقابلة رقم 50 (2021)، **مُعوِّقات تطبيق الذَّكاء الاصطناعيّ في الحدِّ من ممارسة الجريمة الإلكترونيّة مِن وجهة نظر العاملين في وزارة الاتّصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة،** مهندس في قسم الحكومة الإلكترونية، مقابلة شخصيّة تمّ إجراءها يوم الأحد الموافق (2021/10/10) الساعة الـ (2:00) صباحاً.

الملاحق:

ملحق رقم (1): دليل المُقابلة في صورته النهائيّة

جامعة القدس
كليّة الدراسات العليا
برنامج علم الجريمة

أخي العزيز/ أختي العزيزة
تحيّة طيبة وبعد

<u>دليل المُقابلة</u>

تقوم الباحثة بإجراء دراسة بعنوان "**معوقات تطبيق الذكاء الإصطناعي في الحد من ممارسة الجريمة الإلكترونيّة من وجهة نظر العاملين في وزارة الإتصالات والتكنولوجيا والمعلومات في محافظة رام الله والبيرة**"، ذلك إستكمالاً لمتطلبات الحصول على درجة الماجستير في علم الجريمة من جامعة القدس، أرجو التكرم بالإجابة عن الأسئلة المُرفقة بما يتناسب مع وجهة نظركم، شاكرة لكم جهودكم وأمانتكم وحرصكم على إنجاح هذه الدراسة، علما بان إجاباتكم ستكون سريّة ولن تستخدم إلا لغايات البحث العلمي فقط.

مع الشكر والاحترام

الباحثة: كاترين أبو علان

إشراف الدكتورة: وفاء الخطيب

البعد الأول: البيانات الديموغرافيّة

- **الجنس: ( ) ذكر ( ) أنثى**
- **العمر بالسنوات: _____ سنة.**
- **التحصيل العلمي: _____.**
- **القسم: _____.**
- **المُسمى الوظيفي: _____.**
- **عدد سنوات الخبرة للعمل الحالي: _____.**
- **ما هي أماكن العمل التي عملت بها من قبل: _____.**
- **عدد سنوات الخبرة السابقة: _____.**
- **هل التحقت بدورات خاصة بتطبيقات الذكاء الإصطناعي لها علاقة بتتبع الجرائم الإلكترونيّة؟**

  نعم ( ) لا ( )
- **إذا كانت الاجابة نعم، كم عدد الدورات التي خضعت لها: _____.**

البعد الثاني: المحاور

المحور الرئيسي الأول وتفرعاته: من وجهة نظرك/كِ هل هناك دور للذكاء الإصطناعي في الكشف عن الجريمة الإلكترونيّة والحد منها؟

_____

_____

_____

- **من وجهة نظرك/كِ هل تشعر أن مدى تطبيق الذكاء الإصطناعي مرتبط بمدى قبوله في المجتمع؟ كيف ولماذا؟**

_____

_____

_____

- **هل يتم إستخدام برامج الذكاء الإصطناعي في وزارة الإتصالات وتكنولوجيا المعلومات؟ ما أهم تلك البرامج؟ وما هي نطاقات إستخداماتها؟**

_____

_____

_____

- **برأيك/ كِ كيف تساهم برامج الذكاء الإصطناعي في الحد من الجريمة الإلكترونيّة؟**

_____

_____

_____

- **كيف يمكن أن تكون برامج الذكاء الإصطناعي رادع أمام الجُناة لمنع ممارسة الجريمة الإلكترونيّة والحد منها؟**

_____

_____

_____

المحور الرئيسي الثاني وتفرعاته: هل هناك آليات عمل متبعة في إستخدام برامج الذكاء الإصطناعي في الوزارة لتتبع الجناة المرتكبين للجرائم الإلكترونيّة؟ ما هي تلك الآليات بشكل دقيق؟

_____

_____

_____

- **كيف تساهم الآليّات المتبعة في إستخدام برامج الذكاء الاصطناعي في الوزارة في التخفيف من نسبة الجريمة الإلكترونيّة المُرتكبة؟**

_____

_____

_____

- **في حال عَدم توفر آليّات تتبع للجرائم الإلكترونيّة، ماذا تَقترِح/ين لتوفير أو تحسين آليّات العمل المُتبعة في تَتبع الجرائم الإلكترونيّة؟**

_____

_____

_____

- **ما هي أكثر الجرائم الإلكترونيّة التي تقوم تطبيقات الذكاء الإصطناعي بإكتِشافها في الوزارة؟**

_____

_____

_____

المحور الرئيسي الثالث وتفرعاته: هل هناك مُعوقات تواجِه تَطبيق الذكاء الإصطناعي في الحد من ممارسة الجريمة الإلكترونيّة في الوزارة؟

( ) نعم ( ) لا

- **إذا كانت الإجابة نعم، رتب/ي هذه المُعوقات حسب الأهميّة من وجهة نظرك/ كِ، بحيث يكون الرقم الأصغر هو الأكثر صعوبة؟**

الرقم	المُعوقات	الترتيب
1	الإحتلال الإسرائيلي	
2	سنوات خبرة العاملين	

3	عدد الكادر العامل	
4	جنس الكادر	
5	الميزانية الماليّة	
6	الوضع السياسي	
7	عدم كفاءة الكادر العامل	
8	عدم كفاية قاعدة البيانات	
9	عدم توافر قاعدة للبيانات	
10	نطاق عمل المؤسسة	
11	ضعف البنيّة التحتيّة	
12	قلة الأبحاث	
13	ندرة المبرمجين المتخصصين	
مُعوقات أخرى أذكر/ي:		

- **ما هي طرق التغلب على هذه المُعوقات؟**

_____

_____

_____

- **ما إتجاهات المبحوثين حول العلاقة بين الخصائص الديمغرافية (الجنس، مكان السكن، عدد افراد الاسرة، التحصيل العلمي، العمر) وبين ممارسة الجريمة الإلكترونيّة؟**

_____

_____

_____

- **هل لديك/ كِ علم بمؤسسة أو وزارة اخرى محليّة تستخدم تطبيق الذكاء الاصطناعي في الحد من ممارسة الجريمة الإلكترونيّة؟**

_____

_____

_____

- **هل هناك تعاون وتنسيق بين الوزارة والمؤسسات المحليّة والدوليّة العاملة في مجال الجرائم الإلكترونيّة؟**

( ) نعم ( ) لا

- **إذا كانت الإجابة نعم، إشرح/ي ما نوع هذا التعاون؟**

_____

_____

_____

الباحثة: كاترين أبو علان

ملحق رقم (2): محكمي أداة الدراسة

الرقم	إسم المُحكم	الجامعة
1	د. عصام الأطرش	جامعة الإستقلال
2	د. رحاب السعدي	جامعة الإستقلال
3	د. محمد عساف	جامعة الإستقلال
4	د. محمد فرارجة	جامعة القدس
5	د. محمد عكه	جامعة فلسطين الأهليّة
6	د. عماد طميزي	جامعة فلسطين الأهليّة

ملحق رقم (3): نتائج المقابلات

البعد الأول: البيانات الديموغرافيّة للمبحوثين

رقم المقابلة	الجنس	العمر بالسنوات	المستوى التعليمي	القسم	المسمى الوظيفي	عدد سنوات الخبرة للعمل الحالي	أماكن العمل التي عملت بها من قبل؟	عدد سنوات الخبرة السابقة	هل التحقت بدورات خاصة بتطبيقات الذكاء الاصطناعي لها علاقة بتتبع الجرائم الإلكترونيّة	عدد الدورات
1	أنثى	27	بكالوريوس	أمن المعلومات	مهندس	3 سنوات	--	--	لا	--
2	ذكر	45	ماجستير	المعلوماتيّة	مدير	21 سنة	قطاع خاص	سنة	لا	التحقت بدورات عامة خاصة بالذكاء الاصطناعي
3	أنثى	32	بكالوريوس	الحكومة الإلكترونيّة	مبرمج	4 سنوات	وزارات اخرى	3 سنوات	لا	---
4	أنثى	41	دبلوم	الدعم الفني	دعم فني	21 سنة	-----	----	لا	---
5	أنثى	29	بكالوريوس	أنظمة معلومات	مبرمج	3 شهور	قطاع خاص	4 سنوات	لا	--
6	ذكر	31	بكالوريوس	الحاسوب الحكومي	مهندس	4 سنوات	---	---	لا	--
7	ذكر	30	بكالوريوس	الحاسوب الحكومي	مهندس	أقل من سنة	--	--	لا	--
8	ذكر	28	بكالوريوس	الشكاوي(ضبط الجودة)	مهندس	2 سنة	قطاع عام	سنة	لا	التحقت بدورة عامة خاصة بالذكاء الاصطناعي في PLC
9	أنثى	28	بكالوريوس	الشكاوي	مهندس	سنة	قطاع خاص	4 شهور	لا	--
10	أنثى	29	بكالوريوس	هندسة الحاسوب	مهندس	أقل من سنة	قطاع خاص	7 سنوات	لا	--
11	أنثى	32	بكالوريوس	الحكومة الإلكترونيّة	مهندس	اقل من سنة	قطاع خاص	9 سنوات	لا	--
12	أنثى	28	بكالوريوس	التطوير الفني	مهندس	2 سنة	قطاع خاص	2 سنة	لا	--
13	ذكر	26	ماجستير	الحكومة الإلكترونيّة	مبرمج	4 سنوات	قطاع خاص	سنة	لا	--
14	أنثى	28	بكالوريوس	الشكاوي	مهندس	4 سنوات	--	--	لا	--
15	ذكر	35	بكالوريوس	الحكومة الإلكترونيّة	مدير	11 سنة	قطاع خاص	سنة	لا	--
16	أنثى	30	بكالوريوس	الشكاوي	مهندس	سنة	قطاع خاص	7 سنوات	لا	--
17	أنثى	35	ماجستير	الحكومة الإلكترونيّة	مدير	11 سنة	قطاع خاص	سنة	لا	--
18	أنثى	25	بكالوريوس	الشكاوي	مهندس	3 سنوات	قطاع خاص	3 سنوات	لا	--
19	ذكر	24	بكالوريوس	الشكاوي	مهندس	اقل من سنة	--	--	لا	--
20	أنثى	28	ماجستير	الإتصالات	مهندس	اقل من سنة	--	--	لا	--
21	ذكر	25	بكالوريوس	الشكاوي	مهندس	2ونصف	--	--	لا	--
22	أنثى	45	بكالوريوس	الشكاوي	مهندس	11سنة	قطاع عام	3 سنوات	لا	--
23	ذكر	41	بكالوريوس	الحاسوب الحكومي	مدير	17سنة	--	--	لا	--
24	ذكر	27	بكالوريوس	الشكاوي	مهندس	3سنوات	قطاع خاص	5 سنوات	لا	دورات عامة في التعلم الالي
25	ذكر	40	بكالوريوس	الحكومة الإلكترونيّة	مدير	17سنة	قطاع خاص	سنة	لا	التحقت بورشات عامة خاصة بالذكاء الاصطناعي
26	أنثى	26	بكالوريوس	الحكومة الإلكترونيّة	مهندس	3ونصف	--	--	لا	--

27	ذكر	49	بكالوريوس	الحاسوب الحكومي	مدير	22 سنة	قطاع خاص	2 سنة	لا	--
28	ذكر	30	بكالوريوس	الحاسوب الحكومي	مبرمج	سنة	قطاع خاص	6 سنوات	لا	--
29	أنثى	30	بكالوريوس	الحاسوب الحكومي	مبرمج	4 سنوات	قطاع خاص	شهرين	لا	--
30	ذكر	45	بكالوريوس	الحاسوب الحكومي	مدير دائرة المشاريع	21 سنة	--	--	لا	--
31	أنثى	42	بكالوريوس	الدعم الفني	رئيس قسم الشبكات	6 سنوات	قطاع خاص	6 اشهر	لا	--
32	أنثى	30	بكالوريوس	الحاسوب الحكومي	مهندس	5 سنوات	--	--	لا	--
33	أنثى	30	بكالوريوس	الحكومة الإلكترونيّة	مبرمج	سنة ونص	قطاع خاص	5سنوات	لا	_
34	أنثى	26	بكالوريوس	الحكومة الإلكترونيّة	مهندس	اقل من سنة	برمجة تطبيقات	4 سنوات	لا	--
35	أنثى	30	دبلوم عالي	الحكومة الإلكترونيّة	مبرمج	سنة	قطاع خاص	6 سنوات	لا	--
36	ذكر	31	بكالوريوس	الحكومة الإلكترونيّة	مبرمج	3 سنوات	--		لا	--
37	أنثى	28	بكالوريوس	الحكومة الإلكترونيّة	مهندس	5 سنوات	قطاع خاص	سنة واحدة	لا	--
38	أنثى	30	بكالوريوس	الاتصالات	مهندس اتصالات	2ونص	قطاع خاص	سنة	لا	--
39	ذكر	28	ماجستير	الاتصالات	مهندس اتصالات	4 سنوات	قطاع خاص	3 سنوات	لا	--
40	ذكر	29	ماجستير	أمن المعلومات	مهندس	7 سنوات	قطاع خاص	سنة	لا	--
41	ذكر	37	ماجستير	أمن المعلومات	مهندس	11 سنة	قطاع خاص	3 سنوات	لا	--
42	ذكر	43	ماجستير	أمن المعلومات	مبرمج	3 سنوات	قطاع خاص	9 سنوات	نعم	دورات تتعلق بالذكاء الاصطناعي الشبكات العصبيّة الاصطناعية وعملت على مشروع اكتشاف التسلل مبني IDS على الشبكات الذكيّة ANN
43	أنثى	35	بكالوريوس	الاتصالات	مهندس	3 سنوات	قطاع خاص	7 سنوات	لا	--
44	ذكر	37	بكالوريوس	الدعم الفني	مبرمج	6 سنوات	قطاع خاص	7 سنوات	لا	التحقت بدورات عامة خاصة بالذكاء الاصطناعي
45	ذكر	28	بكالوريوس	الاتصالات	مهندس	5 سنوات	قطاع خاص	اقل من سنة	لا	التحقت بدورات عامة خاصة بالذكاء الاصطناعي
46	أنثى	29	بكالوريوس	جودة الخدمة	مهندس	5 سنوات	قطاع خاص	اقل من سنة	لا	--
47	أنثى	31	بكالوريوس	أمن المعلومات	مبرمج	2 سنة	قطاع خاص	3 سنوات	لا	--
48	أنثى	28	بكالوريوس	الشكاوي	مبرمج	2 سنة	-----	-------	لا	---
49	ذكر	35	ماجستير	المقاسم	مهندس	6 ونص	قطاع خاص	6 سنوات	لا	التحقت بدورات عامة بالذكاء الاصطناعي

50	ذكر	29	بكالوريوس	الحكومة الإلكترونيّة	مهندس	3 سنوات	قطاع خاص	3 سنوات	لا	--

البعد الثاني: نتائج المحاور

المحور الرئيسي الأول: ما دور الذكاء الإصطناعي في الكشف عن الجريمة الإلكترونيّة؟ يتفرع عنه

من وجهة نظرك/كِ هل هناك دور لبرامج الذكاء الإصطناعي في الكشف عن الجريمة الإلكترونيّة والحد منها؟	
مقابلة رقم (1)	نعم صحيح هناك دور، ذلك من خلال وجود العديد من البرامج التي تعمل على مبدأ الذكاء الاصطناعي في كشف المجرمين الإلكترونيين، خاصة مع تطوير هذه البرامج باستمرار فهي تساعد بدرجة كبيرة في هذا المجال، كما أن هذه البرامج تسهل عملية كشف أماكن تواجد الجناة وتساعد في سرعة الوصول إليهم، فضلاً عن أن برامج الذكاء الاصطناعي تقوم بعملية المراقبة المستمرة في حال حصول أي خلل داخل الشبكة فهي تعمل على صد الهجمات الإلكترونيّة والمسلكيات المنحرفة التي يقوم بها المجرمين، وتعمل على كشف المجرمين وتوفر كل الداتا الشخصيّة المتعلقة بهم.
مقابلة رقم (2)	نعم أكيد هناك دور، لأن وضع فلسطين يحتاج الى تطبيقات الذكاء الاصطناعي كونها تلعب دور في الكشف عن الجريمة الإلكترونيّة، وتوأمة الذكاء الاصطناعي بحيث يتمكن من التعرف على ما يسمى بالهندسة الاجتماعية التي تستخدم في مواقع التواصل الاجتماعي، هي عبارة عن طرق للاحتيال على الضحية والحصول على معلومات متعلقة بها، هذا أمر خطير جداً يمكن معالجته ذلك من خلال استخدام خوارزميات مصممة خصيصا في موضوع الذكاء الاصطناعي لأن الذكاء الاصطناعي في الأساس مبني على الخوارزميات. ونتيجة الدور الفعال والهام جدا لهذه التطبيقات يفضل تطبيقه للأطفال عند استخدامهم للإنترنت وتعرضهم للجرائم الإلكترونيّة كالإبتزاز، لدى تطبيقات الذكاء الإصطناعي القدرة على الكشف عن الجريمة من خلال معرفة او سماع كلمات مخالفة او غير طبيعية تبدأ بالتنبؤ بأن هناك جريمة يتعرض لها الأطفال، تحديداً بعدما تغلغلت التكنولوجيا في حياتنا حيث لا يمكن الإستغناء عنها ولا يمكننا السيطرة على أطفالنا في استخدامها واستخدام الانترنت.
مقابلة رقم (3)	نعم ذلك من خلال تجميع داتا معينة خاصة بالهجمات الإلكترونيّة، بالتالي يتم العمل على تجميع معلومات خاصة بالجريمة الإلكترونيّة ومن ثم العمل على تحليل هذه البيانات بناءاً على قيام تطبيقات الذكاء الاصطناعي بتصنيفها بشكل تلقائي بالإعتماد على قواعد البيانات، حيث تعطي نتيجة دقيقة وسريعة هذه النتيجة تعتمد على دقة إدخال البيانات. كما أن برامج الذكاء الاصطناعي تلعب دور هام من خلال التنبؤ بالمسلكيات المنحرفة التي تحدث في الشبكة، بالإضافة الى القدرة على اتخاذ القرارات هذا من شأنه يساعد في عملة الكشف عن الجريمة الإلكترونيّة والحد منها كونها توفر الحماية ضد أي هجمات إلكترونيّة.
مقابلة رقم (4)	نعم يأتي دور برامج الذكاء الاصطناعي في اكتشاف الجرائم التي تحصل داخل الفضاء الالكتروني من خلال قواعد البيانات هذه القواعد عبارة عن مهارات ومعارف يتم إدخالها في البينة التحتية، بناءً على ذلك تقوم البرامج بمعرفة هوية المجرم وتحديد مكانه من خلال قواعد البيانات، فهي تعمل على التصنيف والتحليل فتمكنها من الوصول إليه بسرعة ودقة عآليّة، كما أن هذه البرامج لديها القدرة على اكتشاف الجريمة الإلكترونيّة وصد الهجمات التي تتعرض لها الأنظمة، فتطبيقات الذكاء الاصطناعي لديها ما يسمى بالحساسات هي عبارة عن مستشعرات تعمل على مبدأ التنبؤ وظيفتها التقاط المسلكيات الغير طبيعية التي تحصل داخل الشبكة، هذا من شأنه أن يوفر بيئة امنة للمستخدم فكلما زاد تطبيق هذه البرامج كلما وفر بيئة امنة بعيدة عن تصيد المجرمين واستغلال الثغرات.
مقابلة رقم (5)	نعم هناك دور كبير لبرامج الذكاء الاصطناعي في الكشف عن الجريمة الإلكترونيّة ذلك من خلال وضع الإحتمالات المبكرة لجريمة معينة أي من خلال ادخال المعلومات المتعلقة بالجرائم الإلكترونيّة في قواعد المعرفة وبالرجوع إليها تتمكن من معرفة الجريمة، كذلك إمكانية اختراق خصوصية الأفراد بالتصنيف وتتبع الفرد لتتمكن من التوصل الى مكان الجاني ومعلومات مفصلة عنه. هذه الخاصية التي يمتاز بها من خلال استطاعته لتصنيف البيانات تساعد بشكل كبير في حل جزء كبير من الجريمة ،

	كما ان خوارزميات التنبؤ التي تعمل على مبدأ وضع الاحتمالات في مجال الجريمة الإلكترونيّة تساعد في سرعة ودقة اكتشاف الجريمة الإلكترونيّة.
مقابلة رقم (6)	نعم، بالتأكيد هناك دور مهم لهذه البرامج الحديثة والجديدة في المجتمع خاصة في مجال مكافحة الجريمة الإلكترونيّة والكشف عن المجرمين وتتبعهم على الشبكة، فعندما يتم ادخال داتا متخصصة لمقارنتها مع أي مسلكيات منحرفة يتشكل لهذه البرامج القدرة على التصنيف والمقارنة من خلال قواعد البيانات المتوافرة لديها، فتحليل البيانات له دور هام في الكشف عن الجريمة الإلكترونيّة حيث تعمل خوارزميات التنبؤ على التنبؤ حول أي إشكاليات من الممكن أن تحصل، بالتالي تمكنها من سرعة اكتشاف الجريمة واتخاذ القرار في المواقف التي تتعرض لها.
مقابلة رقم (7)	نعم بالتأكيد له دور من عدة زوايا، مثال على ذلك استخدام برامج الذكاء الاصطناعي في التحليل والمتابعة لدعم عمليات التحكم والمراقبة واتخاذ القرارات الدقيقة، فتحليل البيانات وتصنيفها حول ما اذا كانت مهمة أو غير مهمة تعزز اكتشاف الجرائم الإلكترونيّة، فالرقابة المستمرة على الشبكات توفر الحماية لها من أي هجمات إلكترونيّة، كما ويأتي دور هذه البرامج والتطبيقات في القدرة على اتخاذ القرارات المناسبة والدقيقة وذات الجودة العآليّة، فهذه الخبرات التي تتمتع بها برامج الذكاء الاصطناعي تساعد في مجال الجريمة الإلكترونيّة بدرجة عآليّة.
مقابلة رقم (8)	نعم من خلال أن أي تصرف يقوم به الجاني أو أي شخص آخر على الشبكة الإلكترونيّة مسجل ومراقب، إضافة إلى أن لهذه البرامج دور في التنبؤ بالجريمة قبل وقوعها أي الإستباقية في توقع الأحداث، فخوارزميات التنبؤ تساعد بدرجة كبيرة في مجال كشف الجريمة.
مقابلة رقم (9)	نعم ذلك من خلال خوارزميات خاصة بالأشخاص الذين يستخدمون المواقع وكمية استخدام هذه المواقع وأهداف استخدامها، فالذكاء الاصطناعي في الأساس يقوم على خوارزميات يتم من خلالها التحليل والتصنيف التي تساعد في الكشف عن أي جرائم تحدث داخل نطاق الشبكة، توفر هذه البرامج الحماية والرقابة المستمرة على كافة التحركات التي تحصل داخل مجال الشبكة، كما وأنها تكشف عن أي محاولة يقوم بها المجرمين الراغبين في التلاعب في معلومات الاخرين، فهي من تعطي إشارات إنذار حول وجود مسلك غير طبيعي، بمعنى أن أي مسلك مشبوه يحصل في الشبكة لهذه البرامج القدرة العآليّة على اكتشافها من خلال مميزاتها التي تمتاز بها.
مقابلة رقم (10)	نعم توفر برامج الذكاء الاصطناعي خوارزميات وبرامج تساهم في الحفاظ على أمن المعلومات المتناقلة عبر الشبكات الإلكترونيّة والكشف عن عمليات التلاعب والتجسس والإختراقات التي تتعرض لها الشبكات، إضافة الى أن لها القدرة على تصنيف البيانات من خلال قواعد المعرفة ما بين مهمة وغير مهمة لتتمكن من توفير الحماية، فضلاً عن قدرتها على اتخاذ القرارات في المواقف التي توضع فيها بناءاً على الخبرات السابقة التي حصل عليها.
مقابلة رقم (11)	نعم، ممكن تصميم برامج معينة تستطيع الكشف عن الجريمة الإلكترونيّة من خلال العمل على استخدام يوزرات لها بيانات معينة تثبت شخصيّة المستخدم لا تستخدم من قبل أشخاص آخرين وفي حال حاول أحد إختراق ذلك ترسل إشارات تحذيرية، وعليه تقوم بإتخاذ القرار حول هذا الخصوص، كما أنها تقوم بإكتشاف الحسابات الوهميّة التي يتم إنشاؤها بغرض إرتكاب الجرائم فهذه التطبيقات تقوم بمهمة المراقبة والحماية على مدار الـ 24 ساعة بالتالي تقلل من نسبة حصول مسلكيّات غير طبيعيّة.
مقابلة رقم (12)	نعم له دور حيث أن برامج الذكاء الاصطناعي تعتمد على الأنظمة المتطورة التي يمكن تدعيمها بالخبرات والمهارات التي تعمل على تصنيف المحتويات ما بين مهم وغير مهم وعليه تصبح لديها القدرة على تميز البيانات، بالتالي تتمكن من الكشف عن الجريمة الإلكترونيّة، وعندما تلاحظ تطبيقات الذكاء الاصطناعي وجود مسلكيات منحرفة فإنها تعمل على إتخاذ القرار في خصوصها وصدها كما وأنه يعمل على التنبؤ بوجود مسلك غير طبيعي من خلال الحساسات التي يحتوي عليها النظام.
مقابلة رقم (13)	أكيد إن برامج الذكاء الاصطناعي تتعمق في تحليل الداتا على السوشيال ميديا والمواقع الإلكترونيّة المتعلقة في تصميم مواقع وهمية تشكل خطورة ووكر للجرائم، فيتم استخدام برامج الذكاء الاصطناعي في مراقبة السلوكيات من أجل توفير الحماية، أما فيما يتعلق بالتنبؤ تتعلم برامج الذكاء الاصطناعي من التعلم الآلي بغض النظر عن تحديد ما ستقوم به في

	المستقبل، فهي تلعب دور في تحديد السلوكيات التي يقوم بها المستخدمين في الشبكة الإلكترونيّة بناءاً على مسلكياتهم في الماضي فتمكنه من التنبؤ إذا ما كان سيذهب الى إرتكاب مسلكيات إجرامية أم لا، بالإضافة الى القدرة العآليّة على التصنيف للبيانات والمدخلات من خلال مقارنة هذه البيانات بما هو متوافر لديه في قاعدة المعرفة ومن ثم العمل على تحليل ما اذا كانت هذه المسلكيات طبيعيّة ام لا.
مقابلة رقم (14)	نعم بالتأكيد هناك دور لبرامج للذكاء الاصطناعي في مجال الجريمة الإلكترونيّة، حيث أن برامج الذكاء الإصطناعي في الأساس عبارة عن خوارزميات تقوم على التنبؤ بوجود مسلكيات غير طبيعية تحصل داخل الشبكة فهي لديها خاصية الإستباقية، كما أنها تعمل على تصنيف البيانات من خلال المعطيات التي يتم إدخالها الى البرامج فتصبح لديها القدرة على العمل والتصنيف بناءاً على مقارنتها بما هو متوافر في قواعد المعرفة لديها، بالتالي تصبح لديها القدرة على تصنيف حول ما إذا كان المحتوى مهم أو غير مهم، فيتمكن من إكتشاف أي جرائم تحصل سواء اختراقات او تهديدات او ابتزاز فهذه البرامج الحديثة عبارة عن علم جديد.
مقابلة رقم (15)	نعم من خلال إعطائه دلائل الجريمة بالتالي يعطي الإحتمالات التي ممكن أن تحصل، إن استخدام تقنيات الذكاء الاصطناعي في مراقبة حركة المستخدمين داخل الشبكة تعطي نتائج فعّالة في الكشف عن الجريمة الإلكترونيّة كما وتعمل على اتخاذ القرار في المواقف التي تتعرض لها فهذه البرامج من خلال إدخال الخبرات والمهارات في قواعدها تصبح لديها القدرة على تصنيف البيانات وإعطاء الإحتمالات الممكنة، وما هي الإحتمالات غير المهمة التي يجب استثناؤها فهي تشكل جزء مهم في حل الجريمة الإلكترونيّة وتساعد المحققين في حل جزء كبير في التحقيق.
مقابلة رقم (16)	نعم من خلال اكتساب برامج الذكاء الاصطناعي للخبرات والمهارات التي تدخل في قواعد المعرفة، بالتالي تصبح لديها القدرة على التميز ما إذا كانت هذه المسلكيات طبيعية أم لا، كما أن خوارزميات التنبؤ لديها القدرة على التنبؤ بوجود مسلكيات إجرامية تحصل داخل الشبكة فهذه البرامج قادرة على الحد من الجرائم الإلكترونيّة بشكل كبير لا سيما اليوم لم تعد الطرق التقليدية تجدي نفعاً خاصة أننا نعيش في عالم التكنولوجيا ومن الواجب مواكبة هذه التطورات التي تعيشها المجتمعات.
مقابلة رقم (17)	نعم لأنه عندما يكون لدي برامج ذكاء اصطناعي أنا أستطيع عمل مزامنة وتنبؤ على السلوكيات الطبيعية أو غير الطبيعية، فعندما يحصل أي سلوك غير طبيعي يصبح بإمكاني تحديد هذه المسلكيات من خلال قيام برامج الذكاء الاصطناعي بإكتشافها، فمن خلال برامج الذكاء الاصطناعي يمكن مراقبة الشبكات على مدار الـ24 ساعة، بالتالي عندما يحصل أي مسلكيات او انحرافات داخل الشبكة فإنها تعطي إشارات إنذار أو تعمل على صد هذه الهجمات التي تتعرض لها فهذه النظم قائمة على التعلم الآلي وتستطيع أن تتعلم من كافة التجارب التي تمر بها، بالتالي تصبح لديها القدرة على اتخاذ القرارات فهذه التطبيقات والآليّة التي تعمل بها تساعد في اكتشاف الجرائم الإلكترونيّة كما أنها تعمل على التصنيف من خلال خوارزميات التصنيف التي تقوم بمقارنتها بما هو موجود لديها.
مقابلة رقم (18)	نعم من خلال التوعية ببرامج الذكاء الاصطناعي التي تعطي المواطن وعي أكثر حول وجود برامج الذكاء الاصطناعي ومساعدتها في الكشف عن الجريمة، فكلما كان الإنسان على وعي أكثر في استخدام وسائل التكنولوجيا كلما كان هناك وعي في كشف الجرائم فنحن اليوم في عصر التكنولوجيا عصر استحداث مختلف البرامج التكنولوجيّة التي تفيد المجتمع، حيث أن برامج الذكاء الاصطناعي تلعب دور في هذا المجال (إدخال الخبرات والمهارات في قواعد المعرفة) من ثم العمل على تصنيف البيانات بناءاً على المعيطات الى مهمة وغير مهمة، ممكن عمل بلوك على المعطيات الغير مهمة ووضعها في مكان معين حتى يتم النظر اليها، في هذه الحالة يتم التحكم حول ما اذا كان هناك رغبة في استقبالها أو رفضها بالتالي تحذف، كما أنها تساعد في الوصول للجاني كل هذه المميزات التي تتميز بها برامج الذكاء الاصطناعي لها دور في مجال الجريمة الإكترونية.
مقابلة رقم (19)	نعم فهي تعمل على تحليل البيانات وإعطاء النتائج فهي تركز على النقاط التي تشكل مركز لحصول الجريمة الإلكترونيّة، عند التنبؤ بحصول أي مسلكيات إجرامية فإنها تقوم بإرسال إشارات إنذار بأن هناك خلل سيحصل، كما وأنها لديها القدرة على الإستجابة الذاتية لأي طارئ فتعمل على إتخاذ القرار في حال حصول أي جريمة في الفضاء الإلكتروني، فهذه

	البرامج تستقبل البيانات ومن ثم تعمل على تحليلها، فهذه المميزات التي تتميز بها برامج الذكاء الاصطناعي تمنحها القدرة على تميز المسلكيات المنحرفة عن الطبيعية.
مقابلة رقم (20)	طبعا باستخدام خوارزميات خاصة ببرامج الذكاء الاصطناعي والنماذج المبكرة في التنبؤ بأي مسلك يحصل داخل الشبكة من خلال المراقبة المستمرة، كما أنها تقوم بمهمة التنصيف لبيانات الشبكة لتتمكن من توفير الحماية والمراقبة باستمرار، كل ذلك يتم من خلال برامج جاهزة معرفة على الجهاز بشكل مسبق لتقوم بمهمة الكشف عن المسلكيات الإجرامية.
مقابلة رقم (21)	نعم بشكل عام هي عبارة عن نافذة تسمح بالكشف عن أي جريمة، وتطوير سبل الحماية ضد أي هجمات، فبرامج الذكاء الاصطناعي لها بعض المخرجات منها توفير بنية آمنة تعمل على الحماية من الجريمة، فهي تساعد على التحليل بناءاً على المعطيات المتوافرة لديها، وتقلل من نسبة وقوع الجريمة بالإعتماد على المعطيات والبيانات والحصول عليها كمخرجات، فهذه البرامج في الأساس تقوم على مبدأ مهم أنه عند استخدام الشبكة تقوم على الإمساك بهذه البيانات ومن ثم تحليلها وتصنيفها واحدة تلو الأخرى، من أجل التعرف على المحتوى المهم والمحتوى غير المهم، كما أنها يمكن لها مراقبة استخدام الشبكة.
مقابلة رقم (22)	أكيد إن تبني هذه البرامج من قبل المؤسسات تساعد في سرعة الكشف عن الجريمة الإلكترونيّة وبدقة، فهناك الكثير من تطبيقات الذكاء الاصطناعي لديها القدرة على الكشف عن الجريمة الإلكترونيّة بعدة طرق منها الخوارزميات المتعلقة بالتصنيف فهي تلعب دور في القدرة على تصنيف البيانات وتحليلها حول ما إذا كانت تشكل خطر أم لا، وخوارزميات التنبؤ وهي بدورها تقوم بالتنبؤ بحصول اختراقات داخل الشبكة، فهذه البرامج هي من متطلبات العصر الحالي وهذه الخبرات التي يتم إدخالها تساهم بدرجة كبيرة في هذا المجال.
مقابلة رقم (23)	نعم بالتأكيد فتطبيقات الذكاء الاصطناعي تسهل من عملية التوصل الى الجاني بأسرع وقت ممكن وعدم فقدان أي دليل او أثر يتعلق بالجاني ذلك بتتبع مساره على الشبكة، كما أن هذه البرامج توفر بيئة أمنة لمستخدمي الإنترنت من الوقوع ضحايا للمجرمين، فهي تقلل الفرص أمامهم في ارتكاب الجرائم لقدرتها على كشفهم، فهذه البرامج تقوم على أساس البيانات التي تحتوي عليها في قواعدها وتقوم بتصنيف كافة المسلكيات ومن ثم التنبؤ بأي خطر يحدق بالمستخدم.
مقابلة رقم (24)	نعم من خلال إعداد برنامج متعلق بالـ(IB) والسيرفرات في أي موقع يرتكب فيها جريمة يمكن التوصل الى مفتعل الجريمة من خلالها، كما أنها تعمل على التنبؤ بالجرائم الإلكترونيّة من خلال توقع المسلكيات الغير طبيعية التي تحصل داخل الشبكة، مثلاً من خلال جهاز الحاسوب تستطيع برامج الذكاء الاصطناعي عمل بلوك على الجهاز لتحذره أن هناك اختراق ومسلك غير طبيعي قد حصل فمن خلال قدرته على التنبؤ والإستباقية وصد الهجمات يلعب دور كبير في الكشف عن الجريمة الإلكترونيّة أيا كان نوعها.
مقابلة رقم (25)	أكيد من خلال التتبع الآلي للأنظمة فالتتبع الآلي أفضل بكثير من التتبع الإنساني وعمليات مقارنة البيانات وتحليلها، فهي تقوم بها بشكل أسرع وأدق من الإنسان أي أنه لا مجال للخطأ فيها، ويتم الكشف عن الجريمة الإلكترونيّة من خلال التتبع الآلي للإستخدام في الشبكات والعمل على المقارنة كما قلت تتم هذه المقارنة من خلال تحليلها ضمن ما هو متوافر في قاعدة المعرفة فهي في الأساس تعتمد على الرجوع الى المعطيات من خلال التعلم المستمر واكتساب الخبرة والمهارة، كما وأنها تقدم المعلومة بشكل دقيق ولا مجال للخطأ فيها، بالتالي تمكنها من الكشف عن الجريمة الإلكترونيّة.
مقابلة رقم (26)	نعم هناك دور قوي لبرامج الذكاء الاصطناعي في الكشف عن الجريمة الإلكترونيّة حيث توظيف دول العالم الملايين في البحث وتطوير البنى التحتية وقواعد البيانات وتحليلها لزيادة القدرة على الكشف عن الجريمة التي يتم ارتكابها في الفضاء الإلكتروني، خاصة أن المخاطر الأمنية بدأت تزداد في الآونة الأخيرة وهذه البرامج لديها القدرة على الإستباقية في الأمور من خلال قواعد البيانات والعمل على منع حدوث المسلكيات الإجرامية فهي تعمل على تحصين الشبكة من خلال الإصتطدام بجدار الحماية وتقليل الفرصة في اختراق الثغرات، وتساعد في تسريع الحصول على المعلومة المتعلقة بالجريمة أو حتى الحصول على إنذار بوقوعها قبل حصولها من خلال التنبؤ بأن هناك خلل فبرامج الذكاء الاصطناعي تعمل على حل الجريمة واكتشافها من جذورها وليست بعد وقوعها وتصنيفها كجريمة، كما أنها تساعد في ردع الجناة خاصة عند الجاني بوجود هذه التطبيقات التي لديها القدرة على اكتشاف جرائمه.

مقابلة رقم (27)	نعم يوجد لها دور كبير في الكشف عن الجريمة والحد منها حيث أنها تقوم بتحديد حدوثها من خلال دقتها العآليّة في مكافحة الجريمة الإلكترونيّة خاصة في كشف المجرمين كونها لا تسمح بتدخل البشر إلا من خلال إدخال المعطيات وتزويدها بالخبرات والمهارات، فيما بعد تقوم هذه البرامج بتحديد المسلكيات المنحرفة بدقة والتنبؤ بأي مسلك سيحصل، ولا يقتصر دور برامج الذكاء الاصطناعي في مكافحة الجريمة الإلكترونيّة إنما في مختلف مجالات العدالة الجنائيّة والجرائم الواقعة وتقديم أدلة داعمة للقضاء بواسطة هذه البرامج، كما وأنها تلعب دور كبير في الجرائم الإلكترونيّة والتحقيقات الرقميّة الجنائيّة، بما فيها القدرة على ربط الأحداث مع بعضها البعض، والقدرة على التنبؤ بالجرائم فمعظم الجرائم الإلكترونيّة يتم التنبؤ بها قبل وقوعها من خلال برامج الذكاء الاصطناعي، فمن أهم ركائز برامج الذكاء الاصطناعي أنها تسرع من عملية الكشف عن الجريمة الإلكترونيّة كما أن التقدم في التكنولوجيا وتعليم الآلآت من خلال تطوير خوارزميات لديها إمكانيات نائبة عن البشر بالتنبؤ بالجرائم، كما أن التطبيقات والأجهزة الحديثة معظم عملها التعلم من تجاربها السابقة.
مقابلة رقم (28)	نعم من خلال الخوارزميات أي أنه عند إدخال كلمات معينة ومعطيات متعلقة بالجريمة الإلكترونيّة تتكون لديها في قواعد البيانات وتخزن من خلالها استقبالها لها وتتشكل لديها خبرة كافية للتعامل مع المسلكيات المنحرفة، حيث تصبح لديها القدرة على التنبؤ بكشف النية بإرتكاب الجريمة الإلكترونيّة أو إذا كان هناك مسلكيات منحرفة داخل الشبكة، هذه التطبيقات تقوم بتحليل البرامج الوهمية حيث أنه مع كثرة التجارب التي تمر بها تصبح لديها القدرة على تمييز أن هذا المسلك غير طبيعي، فالمستشعرات التي يعتمد عليها النظام ساعدت في الكشف عن الكثير من الجرائم الإلكترونيّة.
مقابلة رقم (29)	نعم لها دور مهم جداً في الكشف عن الجريمة الإلكترونيّة، فهذه البرامج يتم إدخال البيانات في قواعدها من قبل الإنسان وتستقبلها لتستخدمها فيما بعد في الكشف والتنبؤ بالتصرفات المشبوهة التي تحصل في الشبكة، فهي في كل تكرار تقوم بتعليم نفسها بنفسها وتتشكل لديها خبرة كافية، فتتطور وتصبح لديها قدرة سريعة ودقيقة في الكشف عن الجرائم الإلكترونيّة.
مقابلة رقم (30)	نعم لها دور كبير وتمتاز عن الطرق التقليدية بدقتها العآليّة في مكافحة الجريمة الإلكترونيّة كونها لا تسمح بتدخل العنصر البشري، إلا من خلال إدخال المعطيات وتزويدها بالبيانات والحالات المشابهة للمهمة المطلوبة منها، كي تتمكن من معرفة المسلكيات المشبوهة التي تحصل داخل الشبكة، وتقوم بتحديد تفاصيل الجريمة الإلكترونيّة وتحليلها والتنبؤ من خلال المستشعرات الحسية لديها وإعطاء إنذار بأن هناك جريمة ستقع في المستقبل، كل ذلك يتم من خلال البيانات الموجودة في قواعدها المعرفية من خلال استخدامها للخبرة والمهارة .
مقابلة رقم (31)	نعم فالخبرة والمهارة الكافية التي تحصل عليها هذه التطبيقات تمكنها من اكتشاف الجرائم، خاصة إذا تم إدخال العديد من الحالات المشابهة للجرائم التي حصلت فتتمكن خوارزميات التنبؤ بأن جريمة سوف تحدث، بالتالي تقوم المستشعرات الحسية بإرسال إشارات أن هناك مسلك غير طبيعي يحصل.
مقابلة رقم (32)	نعم وذلك من خلال التتبع السريع والوصول إلى الجرائم من خلال تطبيقات الذكاء الاصطناعي، حيث أن الجاني عند إقباله على ارتكاب الجريمة في الفضاء الإلكتروني يأخذ بالأسباب أن هذه التطبيقات لديها قدرة على الكشف عن الجريمة خاصة أن هذه البرامج تقوم بتتبع أي مسلك يتم داخل الشبكة والتنبؤ به بناءاً على تغذيتها بالبيانات والخبرات التي تمكنها من المراقبة المستمرة وتوفير البيئة الأمنة والحماية للبشكات.
مقابلة رقم (33)	بالتأكيد لها دور كبير حيث أن برامج الذكاء الاصطناعي بدأت تتغلل في كافة مجالات الحياة، ناهيك عن الإمكانيات الفعّالة التي تساعد في الكشف عن الجريمة الإلكترونيّة التي تحصل داخل نطاق شبكات الإنترنت حيث تم العمل على تطوير برامج الذكاء الاصطناعي لتصبح قادرة على تحليل كم هائل من البيانات بأعلى دقة وسرعة ممكنة، من خلال هذا التحليل تتمكن من تصنيف البيانات ذلك بالرجوع الى قواعد المعرفة ومن ثم تصنيف ما اذا كان هذا المحتوى ضار أم لا، وبناءً عليه تتمكن من اتخاذ القرار في حل المشاكل التي تتعرض لها بالتالي الكشف عن الجريمة الإلكترونيّة، كما أن هذه البرامج لها القدرة على التبؤ والإستباقية في الأحداث التي تحصل داخل الشبكة ذلك بالإستناد الى نماذج الخطورة .
مقابلة رقم (34)	نعم فالكثير من البرامج الذكيّة في العصر الحالي تعتمد على برامج الذكاء الاصطناعي، خاصة أن تطبيقات وبرامج الذكاء الاصطناعي قامت بأدوار مهمة في تحديد هوية الشخص وتحديد ما إذا كان هذا الشخص هو حقيقي أم مزيف بالتالي تكشف عن الجاني على الفور، كما أن هذه التطبيقات لها دور فعال وكبير في مجال الفحص واكتشاف العديد من عمليات

	النصب والاحتيال في المعاملات البنكية ذلك من خلال أنظمة تسمى (Security systems).
مقابلة رقم (35)	أعتقد ذلك حيث يمكن لبرامج الذكاء الاصطناعي تتبع سلوك وتصرفات البرامج الأخرى أو الهدف منها، واتخاذ القرار استنادا للخبرة والمهارة والتعلم من التجربة والخطأ من خلال إدخال العنصر البشري للبيانات فيما بعد تقوم بالتعلم المستمر بناءاً على التجارب التي تتعرض لها، فتصبح لديها القدرة على اتخاذ القرارات بناءاً على ما هو متوافر لديها، فهذا النوع من البرامج الحديثة وذات الدقة والمهارة العآليّة بإمكانها الكشف عن الجرائم التي تحصل في مجال الفضاء الالكتروني كما وأنها تقوم بالتنبؤ بالجرائم من خلال المستشعرات التي تحتوي عليها التي تساعدها في عملية إعطاء إنذارات حول حصول مسلكيات غير طبيعية.
مقابلة رقم (36)	نعم يوجد لبرامج الذكاء الاصطناعي دور في الكشف عن الجريمة بشكل عام والجريمة الإلكترونيّة بشكل خاص، فالجريمة بشكل عام من خلال استخدام البصمات فهي من أهم أساسيات الذكاء الاصطناعي حيث تساعد في سهولة وسرعة الكشف عن الجريمة الإلكترونيّة، كما أنه يتم من خلالها اكتشاف البصمات بسرعة ذلك بالإعتماد على الذكاء الاصطناعي، أما في الجريمة الإلكترونيّة فاليوم نعيش عالم السرعة ونعيش فترة التطور التكنولوجي فالطرق التقليدية نرى أنها أصبحت أقل نفعا بالتالي فإن برامج الذكاء الاصطناعي تلعب دور هام في الكشف عن الإختراقات التي تحصل في الفضاء الإلكتروني كما أنها تعمل على الحد من الجريمة الإلكترونيّة، ولدى هذه التطبيقات القدرة على تتبع مسار المجرم على الشبكة من خلال الأي بي، حيث يمكن من خلاله الحصول على كافة المعلومات التفصيلة حول المجرم وبأدق التفاصيل.
مقابلة رقم (37)	نعم بالتأكيد هناك دور هام جداً لبرامج الذكاء الاصطناعي والبرامج التابعة له في مجال مكافحة الجريمة الإلكترونيّة، فهذه البرامج الحديثة لا يقتصر مجال عملها في الجريمة الإلكترونيّة فقط إنما في مختلف المجالات فهذه البرامج عبارة عن خوارزميات يتم إدخالها من قبل البشر، تعمل على استلامها وتخزينها في قواعدها كي تتغذا عليها لتتمكن من التصرف في المواقف التي تتعرض لها، فهذه التطبيقات لها قدرة عآليّة في الكشف الدقيق عن الجرائم وصد الاختراقات التي تتعرض لها الشبكات، كما أنها لديها القدرة على التنبؤ بالجرائم بناءً على المستشعرات الحسية بالإضافة الى أن محاولات الدخول المتكررة تعطي إنذار بوجود خلل في هذا الموقع ومن المتوقع حصول جريمة، فكل ذلك يساعد بدرجة كبيرة في الكشف عن الجرائم الإلكترونيّة.
مقابلة رقم (38)	نعم أكيد هناك دور لهذه التطبيقات ذلك من خلال العمل على تحديد اللوكيشنات فهي أسرع وأسهل وأدق طرق تستخدمها برامج الذكاء الاصطناعي في التوصل الى الجاني من ثم كشف الجريمة المرتكبة، كما أن بناء وتحليل البيانات ونسبة توافر البيانات تمكن برامج الذكاء الاصطناعي من تحليل هذه المسلكيات وتصنيفها، مما يساعد في الكشف عن الجريمة الإلكترونيّة.
مقابلة رقم (39)	نعم حيث أن برامج الذكاء الاصطناعي من مخرجات العصر فهذه التطبيقات تساعد في الكشف عن الجريمة من خلال التنبؤ بالجرائم التي تتعرض لها الشبكة بناءاً على التكرارات كما أنها لديها إمكانية في صد الهجمات والإختراقات بالإضافة الى تتبع المجرمين السريع من خلال الاي بي.
مقابلة رقم (40)	نعم يوجد دور كبير لخدمات وبرامج الذكاء الاصطناعي في الكشف عن الجريمة الإلكترونيّة فهي تساهم في الكشف المبكر عن الجريمة الإلكترونيّة من خلال الإستباقية، وتقلل من أثر حدوث هذه الجرائم، وتساعد هذه التطبيقات عند حصول أي خلل داخل الشبكة على اتخاذ القرار في المواقف التي تتعرض لها لحظة وقوع الجريمة وليس بعد وقوعها.
مقابلة رقم (41)	نعم ذلك من خلال البرامج والتطبيقات التي يتم تحديثها بشكل دوري ومستمر وتغذيتها بالبيانات كي تتمكن من التعلم المستمر، للكشف عن الثغرات الأمنية في التطبيقات. كما وأنها تعمل على اتخاذ الإجراءات المناسبة في حال حصول أي جريمة على (Network).
مقابلة رقم (42)	نعم بكل تأكيد هناك دور لتطبيقات الذكاء الاصطناعي في كشف الجرائم التي تحصل على الشبكة، فالمستقبل متجه نحو برامج الذكاء الاصطناعي في كافة مناحي الحياة، لكن برامج الذكاء الاصطناعي دائما ما تعتمد على البيانات المتوفرة لديها فهذه التطبيقات تعمل على اتخاذ القرار المناسب حول المواقف التي تتعرض لها في الشبكة كما وأنها تعمل على التنبؤ بالمسلكيات المشبوهة لكن بغض النظرعن كافة هذه الأدوار التي تقوم بها، فتطبيق برامج الذكاء الاصطناعي مرهون

	بالبيانات وفي مجتمعنا بالتحديد المجتمع الفلسطيني يعاني من تبنى هذا النهج وصعوبة في جمع البيانات.
مقابلة رقم (43)	نعم التنبؤ بعدد المرات وتكرار عدد المرات ومحاولات الإختراق تعطي إنذار بوجود خلل في موقع معين فهذه التطبيقات وظيفتها تتبع أي حركة غير صحيحة تحصل داخل الشبكة من أجل توفير الحماية والأمان لها من أي جريمة الإلكترونيّة، هذا يساعد في اكتشاف الجرائم الإلكترونيّة فهذه البرامج لا تتعب بل تعمل على مدار الـ24 ساعة وتقوم بتوفير الحماية بشكل مستمر ولديها سرعة كبيرة في الكشف عن أي جريمة وبدقة عآليّة ولا مجال فيها لأي خطأ.
مقابلة رقم (44)	نعم يمكن لتطبيقات وبرامج الذكاء الاصطناعي عند ارتكاب الجريمة الإلكترونيّة العمل على اكتشاف الجريمة والتوصل لموقع الجاني من خلال برامج معينة ومخصصة تقوم على تحديد مكان الشخص المرتكب للجريمة بسرعة كبيرة من خلال ما يسمى بالأي بي، بالتالي ممكن من ذلك التوصل إليه وإحضاره، كما أنها تعمل على التنبؤ بوقوع الجريمة وعليه تتخذ قرار تلقائي بالتعامل مع الموقف من خلال المعيطات المتوافرة لديها في قواعدها المعرفية.
مقابلة رقم (45)	نعم بالتأكيد هناك دور مهم لذكاء الاصطناعي في مجال الجريمة الإلكترونيّة إذ يمكن لذكاء الاصطناعي من خلال المهارات التي يتمتع بها تسريع عملية اكتشاف موقع الجاني والحصول على أدق التفاصيل حول بياناته الشخصيّة كما نعلم أن هذه التطبيقات تتميز عن التطبيقات التقليدية المتعارف عليها فهي لديها القدرة على التنبؤ بالهمجات التي تتعرض لها الشبكات فهذه البرامج في الأساس تعتمد على مجموعة ضخمة من البيانات من خلالها تتعلم وتتخذ القرار.
مقابلة رقم (46)	نعم ان برامج الذكاء الاصطناعي مرتبطة بالمسلكيات البشرية أي أنها تقوم في الأساس على مبدأ العمل على السلوكيات البشرية، فهي عبارة عن برامج تعمل بطريقة تشبه طريقة عمل الدماغ البشري وهذا بدوره يساعد في قدرتها على اتخاذ القرار، فتتمكن من ذلك بناءً على الخبرة والمهارة المكتسبة، ويتمكن من استشعار التصرفات الغير طبيعية، كما أنها تتمكن من اكتشافها على الفور وبأدق النتائج.
مقابلة رقم (47)	أكيد هناك دور لبرامج الذكاء الاصطناعي في مجال كشف الجرائم المرتكبة خاصة أن العالم اليوم بدأ يتجه نحو برامج الذكاء الاصطناعي بشكل كبير أكبر من ذي قبل وأصبح التوجه في توفير الكثير من المعلومات وتوفير قواعد بيانات ضخمة تستند عليها وتساعدها في اتخاذ القرارات في المواقف التي تتعرض لها كما أن هناك توجه مهم نحو الـ(IOT) وهو اختصار لـ(Internet things) ذلك سعيا منها لجمع البيانات الضخمة وبناء قواعد ضخمة، فكل ذلك يساعد في الكشف عن الجريمة الإلكترونيّة بشكل كبير ومهم جداً، اذ نتمنى في المستقبل استخدام التكنولوجيا لتطوير الوضع القائم وإدخال العديد من البرامج والتطبيقات التي تساعد على اكتشاف الجرائم الإلكتروني بشكل أسرع وأدق.
مقابلة رقم (48)	نعم أرى أن هناك علاقة لتطبيقات الذكاء الاصطناعي في العمل على اكتشاف الجريمة الإلكترونيّة التي تحصل داخل الشبكة سواء من خلال تتبع السلوكيات الطبيعية أو غير الطبيعية كما يمكن التنبؤ بوجود مسلكيات منحرفة والعمل على إتخاذ القرار بشكل تلقائي وسريع، كل ذلك يتم بالإستناد على قواعد المعرفة فالذكاء الاصطناعي يتمكن من التعامل مع المواقف بناءاً على الخبرات المتوافرة لديه ومن ثم العمل على مقارنة ما هو متوافر لديه وتصنيف هذه المسلكيات حول ما إذا كانت طبيعية ومشبوهة أم لا، وله دور كبير في توفير الحماية وتحصين الأنظمة من المخترقين والمستغلين للثغرات.
مقابلة رقم (49)	نعم عن طريق نشر تطبيقات الذكاء الاصطناعي في الكشف عن الجريمة الإلكترونيّة من خلال الكشف عن التطبيقات في المواقع الإلكترونيّة التي من المحتمل أن تتعرض للإختراقات من قبل المجرمين، والتنبؤ بوقوع الجريمة من خلال ما يسمى بالمستشعرات وهي حساسات موجودة فيها النظام تستشعر وجود جرائم من خلال تخمين كلمات معينة تدل على الجرائم، ويتم ذلك بناءاً على لغة التعلم الآلي لتحليل وتصنيف البيانات.
مقابلة رقم (50)	نعم بالطبع لها علاقة كبيرة في الكشف عن الجريمة الإلكترونيّة وتساعد بدرجة كبيرة في الحد من الجرائم الإلكترونيّة حيث أن تطوير منظومة الأمن والأمان الإلكترونيّة تساعد بشكل كبير في الكشف عن الجريمة الإلكترونيّة والحد منها وتمنع حدوثها، ذلك لقدرة برامج الذكاء الاصطناعي على تحليل كميات هائلة من البيانات بسرعة عآليّة جدا مما يساعد في الكشف عن التهديدات الأمنية في الوقت الفعلي أو على الأقل التنبؤ بها استنادا الى نماذج المخاطر والمعطيات التي تحتوي عليها فتمكنها بهذه الطريقة من الكشف عن الجرائم التي تحصل.

من وجهة نظرك/كِ هل تشعر أن مدى تطبيق برامج الذكاء الإصطناعي مرتبط بمدى قبوله في المجتمع؟ كيف ولماذا؟	
مقابلة رقم (1)	نعم وذلك لأن المجتمع لا يمتلك الوعي والفهم الكافي، كما أنه يوجد في المجتمع رفض وتخوف من هذه التطبيقات نطراً لإنتهاك الذكاء الاصطناعي لخصوصياتهم أي بتوفير تكنولوجيا وبرامج الذكاء الاصطناعي يشعرهم بعدم الارتياح لإنتهاك الخصوصيات لديهم والإطلاع على بياناتهم.
مقابلة رقم (2)	لا عندما يستند الموضوع على قوانين وتشريعات من الدولة من خلالها يتم تنظيم عمل برامج الذكاء الاصطناعي في نفس الوقت يجب أن تراعي موضوع الخصوصية، بالتالي من المفترض أن يكون هناك توعية وثقافة حول الموضوع حتى يتمكن الناس من التعرف على برامج الذكاء الاصطناعي وأخذ فكرة عنه وعن عمله والفائدة التي يعود بها على المجتمع، وأنا أرى هناك توجهين يوجد توجه يوافق وتوجه ضد.
مقابلة رقم (3)	بالنظر الى طبيعة التطبيق الذي أرغب في بنائه، بإعتقادي أنه من جانب الفائدة والرفاهية والجهد سيفيد وسيتقبله المجتمع لكن من جانب أخر سيتم رفضه من قبل المجتمع كونه يعمل على جانب الخصوصية وانتهاك لخصوصيات البشر، لكن عند علم المجتمع أن هذه البرامج والتطبيقات لها فائدة على المجتمع وتنصب في مصلحتهم من المؤكد أنه سيلاقي قبول في المجتمع.
مقابلة رقم (4)	نعم أرى أن ذلك مرتبط بالمجتمع فإذا رفضه لا يمكن تطبيقه ذلك لأن وجود برامج تتغلل في خصوصيات الشخص ومعلوماته الشخصيّة لا يتقبلها الجميع خاصة أنها تندرج تحت مسمى انتهاك الخصوصيات، ولا يمكن فرضه إلا في حالة العموم ومصلحة المجتمع بشكل عام.
مقابلة رقم (5)	نعم يعتبر المجتمع الفلسطيني غير مقبل أو متوجه لاستخدام التكنولوجيا وبشكل خاص "برامج الذكاء الاصطناعي" فإن استخدام الذكاء الاصطناعي يعتبر ميزة لما توفر من حماية ورفاهية ووقت وجهد على الناس وفي نفس الوقت تحدي لأن المجتمع غير مدرك لأهمية هذا النوع من التكنولوجيا الحديثة في المجتمع.
مقابلة رقم (6)	لا، لا أرى أن تطبيق هذه البرامج مرتبط بالمجتمع ذلك لأنه ليس جميع افراد المجتمع على اطلاع بالتكنولوجيا ولديه الفهم الكافي أو حتى العلم بماهية برامج الذكاء الاصطناعي.
مقابلة رقم (7)	لا أرى أنه مرتبط أكثر بالتشريعات والقوانين التي يتم وضعها من قبل الدولة إضافة الى وجود قوانين لانه يُفرض على المجتمع خاصة أنه ينصب في مصالحهم.
مقابلة رقم (8)	طبعا أي شيء يحتاج الى تطبيق يحتاج في نفس الوقت الى وجود عشائر وعوائل في المجتمع الفلسطيني، بالتالي أرى أنه يحتاج الى القبول حتى يتسنى تطبيق نوع من الذكاء الاصطناعي.
مقابلة رقم (9)	لا، لا أرى أن لذلك علاقة يمكن استخدام برامج الذكاء الاصطناعي من غير معرفتهم لان هذه البرامج هي بالأساس تأتي لخدمة مصلحة المجتمع وليست ضدهم.
مقابلة رقم (10)	نعم يجب أن يتقبل المجتمع برامج الذكاء الاصطناعي ويسعى الى استخدامه، فهذه البرامج الحديثة فيها انتهاك للخصوصيات كونه يدخل في معلوماتهم للحصول على بيانات حولهم، لكن في ذات الوقت يجب على المجتمع أن يعي ان هذه التطبيقات تعمل لخدمتهم.
مقابلة رقم (11)	نعم من المهم العمل على نوع الثقافة لتعزيز فهم الناس ان هذه البرامج امنة وضرورة من أجل محو الجهل وقلة الوعي، بالتالي يصبح قبول من المجتمع وفهمه ان هذه البرامج تصب في مصلحة المجتمع.
مقابلة رقم (12)	بالعكس المجتمع بحاجة الى برامج الذكاء الاصطناعي ليساعدها في اتخاذ القرار لكن حسب المجال فانا أرى العكس حيث أن المجتمع سوف يتقبل فكرة برامج الذكاء الاصطناعي.
مقابلة رقم (13)	لا،المجتمع لا يتحكم بالتطور بل على العكس التطور هو الذي يتحكم بالمجتمع لان المجتمع غير مدرك ومقتنع وواعي للتكنولوجيا، بالتالي التكنولوجيا هي التي تجبر المجتمع على كل هذه الأمور.
مقابلة رقم (14)	لا أعتقد ان الدولة اذا قامت بوضع قوانين ناظمة لعمل الذكاء الاصطناعي فإن المجتمع لا علاقة له بالقبول او الرفض، في النهاية هذه البرامج تم تصميمها لخدمة مجالات الحياة في المجتمع وكي تتمكن المجتمعات من مواكبة التطورات.

مقابلة رقم (15)	المجتمع لا علم لديه لكن بالتأكيد يحتاج الى تنظيم من خلال قوانين فعندما يتم إدخال الذكاء الاصطناعي فإنها تخدم مصالحهم، فضلاً عن أن الكثير من تطبيقات الذكاء الاصطناعي منتشرة في المجتمع وهم لا علم لديهم بذلك.
مقابلة رقم (16)	نعم من المفترض أن يكون هناك تقبل من المجتمع في هذا الموضوع لأن في برامج الذكاء الاصطناعي انتهاك لخصوصيات الأفراد، بالتالي يجب أن يكون هناك قبول حتى يتم تطبيقه.
مقابلة رقم (17)	يعتمد على السياسات التي تفرضها الحكومة والدولة حيث يوجد سياسات تفرض على المجتمع سواء برضاه أو لا، فهذه السياسات تخدم المجتمع وتنصب في مصالحه وفي سبيل توفير حياة كريمة وامنة خاليّة من المشاكل أو أي اعتداءات.
مقابلة رقم (18)	لا المجتمع لن يرفض هذه البرامج لأن العصر الحالي هو عصر التكنولوجيا خاصة في ظل جائحة كورونا ازدادت الحاجة الى هذه البرامج، على الرغم من وجود الكثير من الفئات التي لا تتقبل هذه التكنولوجيا الحديثة المبينة على برامج الذكاء الاصطناعي التي تحتاج الى وقت لتقبلها.
مقابلة رقم (19)	يتقبل المجتمع فكرة وجود برامج حديثة بالأخص عندما يساعد في كشف الجرائم التي تحصل في الفضاء الإلكتروني وعندما يحقق لهم الحياة الأمنة والكريمة والرفاهية فإنه يتقبله.
مقابلة رقم (20)	لا لا علاقة للمجتمع في هذا الخصوص بمعنى هل عندما تقوم شركة معينة بإصدار موبايل جديد يتم سؤال المجتمع بقبوله؟ لا الشخص وحده له الحرية في الشراء أو عدم الشراء إذا كان لا يرغب في الأساس استخدام التكنولوجيا، بمعنى ان المجتمع سوف يتقبل ذلك بشكل تلقائي.
مقابلة رقم (21)	لا حتى لو لم يتقبل المجتمع ذلك من المفترض أن تقوم الدولة بفرضه سواء كان هناك موافقة من المجتمع أم لا لأنه يفيد مصالحهم وليس ضدهم.
مقابلة رقم (22)	لا يتم ذلك من خلال إقرار قوانين ناظمة تعمل على تنظيم هذا الموضوع وتلزم المجتمع بالقبول، لأن هذه التقنيات الحديثة هي تعمل لمصلحة المجتمع في الأساس.
مقابلة رقم (23)	لا لا علاقة فهذا علم حاصل محصل ولا علاقة للمجتمع في هذا الموضوع، قديماً المجتمع لم يكن يعلم بهذا الموضوع لكن حديثا أصبح هناك استعياب أكثر ومعرفة بوجود تطبيقات الذكاء اصطناعي.
مقابلة رقم (24)	لا فنحن موجودين في عالم التكنولوجيا، والمجتمع بدأ بالتعرف على التكنولوجيا بشكل أكبر في فترة كورونا وأصبح المعظم على إطلاع أكثر في مجال التكنولوجيا كونهم أقبلوا على أوقات فراغ أكثر بالتالي لديهم علم وتصور بأهمية وجودها.
مقابلة رقم (25)	أكيد قبول الناس شرط اساسي لإنتشار برامج الذكاء الاصطناعي فالتوعية شيء مهم في التغيير من خلال توعية المجتمع بتقبل برامج الذكاء الاصطناعي والوزارة لديها مركز يعمل على نشر الوعي بأهمية هذه البرامج.
مقابلة رقم (26)	لا لا أعتقد أن هناك ارتباط لأنه لا يشترط أن يكون المجتمع أجمع ملم بثقافة برامج الذكاء الاصطناعي وتطبيقه، بالتالي لا يرتبط بقبول أو رفض المجتمع وأنا أرى أنها تعمل في مصلحة المجتمع حيث تساعد في تحقيق الرفاهية لدى المجتمع وتساعد في الكشف عن الجرائم الإلكترونيّة وكذلك الجرائم العادية، إضافة إلى أنها تساعد في المجالات الإقتصادية.
مقابلة رقم (27)	لا فبرامج الذكاء الاصطناعي يتم فرضها على المجتمع، لأن في ذلك تسهيل لحياة الناس وتحقيق الرفاهية والوقت والجهد.
مقابلة رقم (28)	لا لا علاقة لذلك حيث أن برامج الذكاء الاصطناعي تُفرض في المجتمع غصب عنهم وليس بإرادتهم، لأنه ليس جميع الناس على إطلاع بالتكنولوجيا وعلى علم بها وبأهميتها.
مقابلة رقم (29)	لا يتم فرض برامج الذكاء الاصطناعي على المجتمع لأنه ليس شرط أن يقبل به المجتمع كافة حيث أنه يوجد فئات مع هذه التطبيقات وفئات ضدها رغم أنها صممت في الأساس لتسهيل حياة البشر.
مقابلة رقم (30)	لا أتوقع أن مدى تطبيق برامج الذكاء الاصطناعي مرتبط بمدى قبول المجتمع لكن تطبيقها يحتاج الى توجه عام من الدولة ومن ثم بناء القدرات وتخصيص الموازنات المآليّة اللازمة لتطبيقها.
مقابلة رقم (31)	نعم من المهم نشر الثقافة وإيصالها لكافة المستويات في المجتمع لأنه لا يوجد لدى الناس المعلومات الكافية حول أهمية وجود هذا النوع من التكنولوجيا الحديثة في المجتمع.

مقابلة رقم (32)	نعم تطبيقه يعتمد على قبوله من المجتمع خاصة أنه ليس جميع أفراد المجتمع موافق على ذلك كونهم غير مستوعبين أهمية تطبيقه، كما وأن هناك الكثير من الأشخاص من أصحاب المناصب التي لا تتقبل التكنولوجيا الحديثة.
مقابلة رقم (33)	أعتقد أن المجتمع من المفترض أن يتقبل فكرة وجود وتطبيق برامج الذكاء الاصطناعي لأنها تعود بالفائدة على المجتمع وتتغلل في شتى مجالات الحياة وليس مجال واحد فقط، كما وتسهل عليهم حياتهم وتوفر الوقت والجهد، وفي النهاية تطبيق هذا النوع من التكنولوجيا الحديثة مسؤولية الأفراد والجهات المختصة في مجال التكنولوجيا لأنها هي الجهات الوحيدة المختصة في هذا المجال خاصة أنه ليس جميع أفراد المجتمع على إطلاع كافي بتفاصيل التكنولوجيا.
مقابلة رقم (34)	نعم لكن لا يرتبط ارتباط قوي لأنه مع تطوير التكنولوجيا والأساليب الحديثة المستخدمة حالياً أصبح من السهل تقبل فكرة تطبيق برامج الذكاء الاصطناعي والبرامج الذكيّة.
مقابلة رقم (35)	لا بل تقع على عاتق العاملين في مجال برامج الذكاء الاصطناعي من خلال الاستخدام والدراسات والأبحاث وعكس النتائج على المجتمع بعد ذلك سيتم قبول هذه البرامج بسبب أهميتها وبناءً عليه يفرض على المجتمع.
مقابلة رقم (36)	بغض النظر هناك قبول أو رفض هذا شيء أساسي، حيث من المهم ومن الضروري مواكبة التكنولوجيا والإستفادة منها حيث أنه ليس جميع أفراد المجتمع على إطلاع وفهم ودراية بالتكنولوجيا، فأنا أرى أن يترك ذلك لجهات مختصة في هذا المجال كي يستفيد منها المجتمع.
مقابلة رقم (37)	من وجهة نظري أرى أن المجتمع يجب أن يتقبل هذه البرامج من جانب إن مدى قبولها مربوط بالمجتمع، بالتأكيد لأن برامج الذكاء الاصطناعي فيها انتهاك للخصوصيات لكن إذا انصب الموضوع في مصلحة المجتمع أرى انه لا لا علاقة لهم بالرفض أو القبول.
مقابلة رقم (38)	لا المجتمع ينظر إليها من باب انتهاك الخصوصيات لكن إذا نظرت لها من باب الفائدة فلا علاقة لهم على الإطلاق بالرفض فهي تعمل من أجل مصالحهم، لذا يجب العمل على نشر التوعية حول أهمية هذه التطبيقات.
مقابلة رقم (39)	لا تُفرض على المجتمع من خلال التشريعات والقوانين فتصبح شيء اجباري على المجتمع، فالمجتمع عندما يرى أن هناك تشريعات وقوانين تنص على استخدام برامج الذكاء الاصطناعي فإنه يتقبلها حتى لو كان هناك رفض من بعض أفراد المجتمع.
مقابلة رقم (40)	نعم يجب أن يكون هناك قبول من المجتمع لأنه يعمل على تحقيق الأمان والحماية وتسهيل حياتهم وليس ضدهم.
مقابلة رقم (41)	لا خاصة أن ثقافة برامج الذكاء الاصطناعي في المجتمع غير منتشرة.
مقابلة رقم (42)	لا، ليس بالضرورة فإن فرض مثل هذا النهج يحتاج الى سياسات تحدد استخدامها لكن في مجتمعنا من الصعب تطبيقه لضعف البنى التحتية.
مقابلة رقم (43)	نعم حيث لا يجوز انتهاك خصوصيات المجتمع بدون موافقته، بالتالي إذا كان هناك انتهاك للخصوصيات يجب أن يقبل في البداية المجتمع بذلك.
مقابلة رقم (44)	بشكل عام لا علاقة للمجتمع في ذلك لكن إذا مس خصوصيات المجتمع طبعا يجب أن يكون هناك قبول لكن إذا كان لا يمس خصوصياتهم من الطبيعي ان أقوم بتطبيقه لكن انا أرى أنها تعدي على الخصوصيات.
مقابلة رقم (45)	لا علاقة للمجتمع في هذا الخصوص انما يفرض عليهم بحكم متغيرات المجتمع، فالمجتمع لا يتحكم بها انما تفرض عليه كونها احد متطلبات العصر الحالي.
مقابلة رقم (46)	ليس بدرجة أساسية لانه يتم توظيفه في الأساس من قبل الدولة وأصحاب القرار والقوانين الناظمة لهذا الموضوع في البداية يجب على القانون ان يقبل تطبيقات وبرامج الذكاء الاصطناعي وهل نتائجها فعّالة ام لا.
مقابلة رقم (47)	لا اكيد في الغالب المجتمع غير واعي بالتكنولوجيا وهذه التطبيقات تقوم بخدمة مصلحة المجتمع، ولان المجتمع في الأساس يجب ان يعلم ما هي التكنولوجيا وكيفية استخدامها.
مقابلة رقم (48)	لا لا أرى أن هناك علاقة لافراد المجتمع بقبول برامج الذكاء الاصطناعي أو رفضها، فالمجتمع تُفرض عليه هذه التطبيقات والبرامج لانها في النهاية تعمل لمصلحة المجتمع ولتوفير الحماية والارتقاء به ولا تعمل ضده أو ضد مصالحه

مقابلة رقم (49)	لا لا علاقة لذلك بل هي تفرض على المجتمع، نحن نعلم أن الجوالات تستخدم الذكاء الاصطناعي من دون اذن المستخدم وهناك الكثير من الأشياء تقوم باتخاذ القرار عنه دون اذن منه، بالتالي هو يفرض عليه لمصلحته .
مقابلة رقم (50)	من وجهة نظري لا يوجد مجتمع لا يقبل تطبيق برامج الذكاء الاصطناعي لان فوائد تطبيقها تعود على المجتمع وتقوم بتسهيل معظم الأمور التي تشكل ضغط على البشرية مثل اتمتة بعض الخدمات لكن يعتمد هذا التطبيق بشكل مباشر على الجهات الفاعلة والمؤسسات العاملة في نطاق التكنولوجيا لمواكبة التطور والعمل عليه وأيضا يعتمد على توفير الإمكانيات اللازمة لتطبيقه.
هل يتم إستخدام برامج الذكاء الإصطناعي في وزارة الإتصالات وتكنولوجيا المعلومات؟ ما أهم تلك البرامج؟ وما هي نطاقات إستخداماتها؟	
مقابلة رقم (1)	نعم يستخدم برنامج الـ(WAF) وهو اختصار لـ (Web Application Firwall) حيث يعمل على مبدأ (Machine Learining) ذلك من أجل تعليم السياسة الخاصة للمواقع من قبل أشخاص موثوقين وعمل تكرار للحركات اللازمة، ومنع أي حركة أخرى غريبة ومشبوهة بعد التعليم بمعنى صد الهجمات التي تتعرض لها الشبكات.
مقابلة رقم (2)	نعم يتم استخدام برامج الذكاء الاصطناعي في الوزارة وهي: برنامج (WAF) هو عبارة عن برنامج يستخدم مجال التعلم الآلي وهو أحد مجالات الذكاء االاصطناعي، يعمل كجدار حماية من أي اختراق ويعمل على صد الهجمات الإلكترونيّة بشكل سريع وتلقائي.
مقابلة رقم (3)	نعم تستخدم الوزارة برامج تعلم آلي كما الآتي: برنامج (WAF) وبرنامج (UTM) وبرنامج (Fir wall) وهي.
مقابلة رقم (4)	نعم تستخدم: برنامج (WAF) وبرنامج (UTM) وبرنامج (Fir wall).
مقابلة رقم (5)	نعم وهي: برنامج (WAF) وبرنامج (UTM) وبرنامج (Fir wall).
مقابلة رقم (6)	نعم يتم استخدام برامج قائمة على التعلم الآلي وهي: برنامج (WAF) وبرنامج (UTM) وبرنامج (Fir wall).
مقابلة رقم (7)	حسب معلوماتي لا يتم استخدامها.
مقابلة رقم (8)	لا لا يتم استخدامها.
مقابلة رقم (9)	لا يتم استخدام الطرق التقليدية في الوزارة.
مقابلة رقم (10)	نعم يتم استخدام برامج الذكاء الاصطناعي خاصة في مجال الحماية، حيث يتم استخدامه في أمن الشبكات، وأمن المعلومات وأمن البيانات، إضافة إلى أنه يتم استخدامها لحماية أنظمة الوزارة، لعل من أهم هذه البرامج: برنامج (Fir wall) وبرنامج (WAF) هذه البرامج تعتمد على التعلم الالي.
مقابلة رقم (11)	نعم تستخدم الوزارة بشكل عام برامج الذكاء الاصطناعي، اما في مجال الامن تستخدم برنامج (WAF) وتعتمد على التعلم الالي، وتستخدم منظومة الدفع الالكتروني على نطاق واسع.
مقابلة رقم (12)	نعم حيث يتم استخدام كل من: برنامج (WAF) وبرنامج (UTM) وبرنامج (Fir wall)، تستخدم هذه البرامج في مجال الحماية الأمنية، كما وتستخدمها الوزارة في فلترة أي هجوم الكتروني، وتعمل بناءً على المعلومات بتصنيف وتحليل الهجمات بالتالي توفر الحماية للشبكات.
مقابلة رقم (13)	نعم فهي تستخدم كل من: برنامج (WAF) وبرنامج (UTM) وبرنامج (Fir wall)، هذه البرامج تعتمد على الذكاء الاصطناعي (التعلم الالي) وتقوم بحماية الشبكات والبيانات.
مقابلة رقم (14)	نعم يتم استخدام: برنامج (Fir wall) وبرنامج (WAF)، هي برامج ذات نطاق محدود، كلا التطبيقان من تطبيقات الذكاء الاصطناعي أي

	تعمل على مبدأ التعلم الآلي وتشكل حماية وامن لشبكات الإلكترونيّة.
مقابلة رقم (15)	لا تستخدم الوزارة أي من تطبيقات وبرامج الذكاء الاصطناعي.
مقابلة رقم (16)	نعم تستخدام الوزارة: برنامج (WAF) وبرنامج (UTM).
مقابلة رقم (17)	نعم بالتأكيد تستخدام الوزارة: برنامج (WAF) وبرنامج (UTM) والـ (F5)، هذه البرامج في الخلفية الخاصة بها مكونة من الذكاء الاصطناعي وتعتمد على التعلم الالي فهي تقوم بالتعلم من هذه الحركات التي توضع في قواعد البيانات لديه ليتعلم منها، بالتالي يصبح لديه علم ان هذه الحركات طبيعية وهذه غير طبيعية وعليه يقوم بحساب درجة الملسكيات فيه ليتم ما اذا تم قبوله أو لا، حيث أن هذه البرامج ذات نطاق محدود.
مقابلة رقم (18)	نعم تستخدم الوزارة برامج الذكاء الاصطناعي في معظم أنظمتها خاصة في البورتل الرئيسي وفي الايميلات وهي ذات نطاق واسع جدا حيث يتم تعديل واستحداث هذه البرامج كل فترة، اما في مجال الحماية وامن المعلومات تستخدم: برنامج (WAF) وبرنامج (UTM) وبرنامج (Fir wall)، فالوزارة تعمل على التشبيك والتعاون مع المؤسسات الأخرى من أجل حماية أمنها من أي هجمات واختراقات تتعرض لها.
مقابلة رقم (19)	نعم تستخدم الوزارة برامج على مستوى عالي، هذه البرامج توفر الحماية من أي اختراقات وهجمات إلكترونيّة وهي: برنامج (WAF) وبرنامج (UTM)، تعمل هذه البرامج على مبدأ التعلم الآلي في الذكاء الاصطناعي وهي ذات نطاق واسع الاستخدام فهي تمكن من تعديلها وتطويرها كل فترة.
مقابلة رقم (20)	نعم تستخدم برامج فلترة الايميلات.
مقابلة رقم (21)	نعم يتم استخدامها وهي: برنامج (WAF) وبرنامج (UTM)، هذه البرامج تعمل على توفير الحماية والأمان والوقاية من أي نوع من الهجمات الإلكترونيّة، ويمكن التعديل على هذه البرامج واستحداثها.
مقابلة رقم (22)	نعم يتم استخدامها وهي: برنامج (WAF) وبرنامج (UTM)، تعتمد في عملها على التعلم الالي وهي احد فروع الذكاء الاصطناعي الذي يقوم بتحليل وتصنيف الهجمات والبيانات.
مقابلة رقم (23)	نعم يتم استخدام: برنامج (WAF) وبرنامج (UTM) وبرنامج (Fir wall)، هذه البرامج تعتمد على التعلم الالي ذات نطاق محدود كونها يتم شرائها من الخارج، وهي برامج ذات جودة عآليّة.
مقابلة رقم (24)	نعم تستخدم برنامج واحد هو: برنامج (WAF)، وهو برامج عالمي ذو نطاق واسع يمكن استحداثه وتطويره.
مقابلة رقم (25)	نعم يتم استخدام برامج حماية امنية لشبكات هي: برنامج (WAF) وبرنامج (UTM) وبرنامج (Fir wall)، هي برامج ذكاء اصطناعي تستخدم التعلم الالي، فهذه البرامج يتم استيرادها وشراءها من الخارج ذات جودة ودقة عآليّة جدا ونطاق استخدامها واسع.
مقابلة رقم (26)	نعم يتم استخدام بعض تطبيقات الذكاء الاصطناعي في الوزارة وهي تطبيقات ذات جودة عآليّة وتصنف على مستوى عالمي فهي: برنامج (WAF) وبرنامج (Fir wall)، هذه البرامج تستفيد من الخبرات والمهارات من خلال التعلم الالي، فهي تعمل على توفير الحماية والأمان والوقاية من أي هجمات إلكترونيّة.
مقابلة رقم (27)	لا يوجد استخدام لبرامج الذكاء الاصطناعي في الوزارة.
مقابلة رقم (28)	نعم يتم استخدام برامج حماية امنية للشبكات هي:

	برنامج (WAF)، وبعض المستشعرات العامة في الوزارة.
مقابلة رقم (29)	نعم كما وانها مسؤولة عن القطاعات الأخرى ذات العلاقة حيث ان الوزارة تقوم بتوزيع خدمات هذه البرامج للقطاعات الشريكة، هذه البرامج هي: برنامج (WAF) وبرنامج (UTM) وبرنامج (Fir wall)، تعد هذه البرامج برامج ذكاء اصطناعي تستخدم التعلم الالي.
مقابلة رقم (30)	لا لكن في نفس الوقت يتم حاليا تطوير برامج تدريبية لكن لم يتم استخدامها بعد.
مقابلة رقم (31)	نعم تستخدم الوزارة برامج الذكاء الاصطناعي وبرامج حماية وصد الاختراقات تشكل جدار حماية، حيث تستخدم: برنامج (WAF) وبرنامج (UTM) وبرنامج (Fir wall)، لكن لا اعلم نطاق استخدامها.
مقابلة رقم (32)	نعم يتم استخدام برنامج (WAF) وهو عبارة عن برنامج يعمل على مبدا التعلم الالي من خلال ادخال الخبرات والمهارات ويعمل كجدار حماية ونطاق استخدامه بسيط فهذه البرامج مستوردة.
مقابلة رقم (33)	نعم تستخدم الوزارة برامج الذكاء الاصطناعي منها: برنامج (WAF) وبرنامج (UTM) وبرنامج (Fir wall)، هذه البرامج تستخدم الذكاء الاصطناعي (التعلم الالي) وتعمل على توفير الحماية وتستخدم كجدار حماية، تعتبر هذه برامج عالمية ذات استخدام عالي الدقة والسرعة وذات نطاق واسع.
مقابلة رقم (34)	نعم يتم استخدامها في الكشف عن محاولات الاختراق التي تحصل، من بين هذه البرامج: برنامج (WAF) وبرنامج (Fir wall).
مقابلة رقم (35)	نعم يتم استخدام: برنامج (WAF) وبرنامج (UTM) وبرنامج (Fir wall)، حيث يتم استخدامها ضد الهجمات الإلكترونيّة.
مقابلة رقم (36)	نعم أكيد تستخدم الوزارة برامج الذكاء الاصطناعي في أنظمتها وكافة مرافقها كما ويتم استخدامها في برامج الاتصالات، وتستخدم في مجالات الحماية والامن كبرامج الـ (WAF – UTM– FirWall)، جميعها تعمل على مبدأ التعلم الالي وتوفر الحماية والأمان ضد أي تهديدات كما ان الوزارة تقدم برامجها للعديد من الوزارة والقطاعات الأخرى لحمايتها من الاختراقات والانتهاكات التي تحصل، لكن هذه البرامج باهظة الثمن ويتم استيرادها من الخارج فتحدد نطاق استخدامنا لها.
مقابلة رقم (37)	نعم يتم استخدام: برنامج (WAF) وبرنامج (UTM) وبرنامج (Fir wall)، هذه البرامج تُعتبر برامج حماية وجدار من أجل صد الاختراقات فهي تشكل بمثابة جدران، أي اكثر من جدار في كل مرة يحاول فيها الفايروس أو الهكر إختراق النظام في كل مرة يصتطدم بكل جدار حتى يتم التخلص منها.
مقابلة رقم (38)	حسب الإمكانيات المتوافرة حاليا في الوزارة لا يتم استخدامها.
مقابلة رقم (39)	نعم يتم استخدام: برنامج (WAF) وبرنامج (Fir wall)، وهي برامج حماية عالمية، تسعى الوزارة الى احضار برامج ذكاء اصطناعي تعمل على تحليل التحركات التي تحصل داخل الشبكات.
مقابلة رقم (40)	نعم برنامج (WAF) وهو عبارة عن برنامج يقوم بصد الهجمات الإلكترونيّة، يعمل على مبدأ التعلم الآلي.
مقابلة رقم (41)	نعم يوجد جهاز تتبع للهجمات الإلكترونيّة وهو الـ (WAF) وهو برنامج يعمل على صد الهجمات وتتبعها.
مقابلة رقم (42)	نعم بالتأكيد تستخدم الوزارة برامج الـ (WAF) الذي يقوم بصد الهجمات الإلكترونيّة.
مقابلة رقم (43)	ليس من صلاحياتي الإفتاء حول ما اذا كانت الوزارة تستخدم الذكاء الاصطناعي ام لا.
مقابلة رقم (44)	نعم يتم استخدام: برنامج (WAF) وبرنامج (UTM) وبرنامج (Fir wall)، هذه البرامج ذات أهمية كبيرة في الحماية من الاختراقات وصد أي هجمات تتعرض لها، كما ان هناك الكثير من المؤسسات والقطاعات التي تقوم بالتشبيك مع الوزارة من اجل حماية برامجها وحماية نفسها من أي اختراقات.
مقابلة رقم (45)	نعم يتم استخدام:

	برنامج (WAF) وبرنامج (UTM) وبرنامج (Fir wall).
مقابلة رقم (46)	نعم يتم استخدام: برنامج (WAF) وبرنامج (UTM) وبرنامج (Fir wall)، لان موضوع الذكاء الاصطناعي جديد الى حد ما على القطاع لا تستغربي ان لا تكون الكثير من البرامج مفعلة خاصة ان هذه البرامج بحاجة الى الكثير من الموازنات.
مقابلة رقم (47)	نعم من خلال تتبع المواقع الإلكترونيّة مثل: برنامج (WAF) وبرنامج (Fir wall)، هذه البرامج تفي بالغرض كطريقة تنظيم عمل ال Network والـ Traffic on بالإضافة الى إمكانية احضار العديد من البرامج التي تقوم بتحليل الحركات على الشبكات، التي سيتم احضارها بشكل أساسي ورسمي وفق المرحلة القادمة لزيادة عدد التطبيقات والمواقع الإلكترونيّة المستضافة لدى الوزارة.
مقابلة رقم (48)	نعم يتم استخدام برامج الذكاء الاصطناعي في الحماية من الهجمات الإلكترونيّة وتتبع المواقع مثل برنامج (WAF) فهو برنامج يعمل كجدار حماية على الشبكات.
مقابلة رقم (49)	نعم يستخدم برنامج (WAF)، الذي يقوم بإدخال الأمور التي تتعلق بالتنبؤ فيما يسمى بانظمة التشغيل والاستهلاك المتوقع.
مقابلة رقم (50)	لا يتم استخدامه.

برأيك/ كِ كيف تساهم برامج الذكاء الإصطناعي في الحدّ من الجريمة الإلكترونيّة؟	
مقابلة رقم (1)	تعمل هذه البرامج على الحد من الجريمة الإلكترونيّة من خلال نشر الفكر والوعي لدى أفراد المجتمع بوجود برامج ذكاء اصطناعي وتقنيات حديثة وخاصة تعمل على كشف كل جريمة يتم إرتكابها من قبل المجرمين بوقت أقصر وأسرع، فهذا بحد ذاته يحد من الجريمة تمنع الأخرين من الاقدام على ارتكابها.
مقابلة رقم (2)	يساهم في حماية الضحية من الوقوع فريسة للمجرم الالكتروني، كما ويساهم في حماية المؤسسات والبنوك وكافة القطاعات من أي جرائم تتعرض لها، ويساهم في التنبؤ بالجريمة الإلكترونيّة والاستباقية في التنبؤ بالاحداث، فهو يقلل من نسبة الجريمة ويمنعها من الزيادة في المجتمع.
مقابلة رقم (3)	يساهم في قدرته بالتنبؤ بشكل مسبق باي مسلكيات تحصل بالتالي يستطيع ان يأخذ قرار في منع الجريمة، كما يمكن له ان يمنع حدوثها من خلال ارسال إشارات انذار بان هناك خطر يواجه المستخدم، هذه الإنذارات تعمل على مبدأ الحساسات التي يحتوي عليها النظام، بالتالي في كل مرة يتم فيها الكشف عن الجريمة أو صد أي هجمة تتعرض لها الأنظمة هذا يعني تقليل نسبتها في المجتمع، فالخبرة الكافية في التعامل مع الاحداث تجعل برامج الذكاء الاصطناعي قادرة على التعامل مع أي موقف تتعرض له، إضافة الى قدرة هذه البرامج على توفير الحماية والأمان.
مقابلة رقم (4)	بالتأكيد يساهم بدرجة كبيرة، فعندما يتم الإمساك بشخص معين من الممكن لها أن تشكل رادع للمجرمين الاخرين خوفا من التعرض للعقوبة، فهذه التطبيقات وظيفتها اكتشاف أي مسلك غير طبيعي يحصل في الشبكة وصدها في نفس اللحظة أو إعطاء انذار بان هناك جريمة او مسلك غير طبيعي يحصل، خاصة أن معظم الجرائم تأتي وتكون قد حصلت ، فهي تحد منها لانها تعمل على صدها في نفس الوقت وليست بعد وقوعها، بالتالي تقلل بشكل كبير من نسبتها سواء المجرمين نفسهم بعدم عودتهم لارتكاب الجرائم هذا يعني أن والجريمة نفسها تقل.
مقابلة رقم (5)	يساهم من خلال العمل على وضع احتمالات معينة داخل البرامج مثل وضع بيانات عن نوع من الجرائم التي تمكن تطبيق الذكاء الاصطناعي من تتبعه واكتشافه، فان استخدام تطبيقات الذكاء الاصطناعي تساهم بدرجة كبيرة في هذا المجال كونها عندما تقوم باكتشاف الجريمة كل مرة تقوم بنفس العمل وتعمل على تقليل نسبتها في المجتمع.
مقابلة رقم (6)	من خلال الاستغلال الجيد لهذه البرامج في مكافحة الجريمة والكشف عنها بالتالي تقلل منها وتؤثر على نفسية الجاني في علمه أن هذه البرامج فعّالة الكترونيا فهي تقوم بمراقبة كافة المسلكيات في الشبكة، فعندما تكون نسب الخطأ والانذارات اقل في هذه التطبيقات تقدم أفضل النتائج وسرعة في اتخاذ القرارات مما يعني أن نسبة الجريمة ستنخفض تلقائيا، وتوفر الراحة والاطمئنان للمجتمع واغلاق الفرص امام الجاني.
مقابلة رقم (7)	بالتأكيد يساهم بدرجة كبيرة، فعندما يتم الإمساك بشخص معين من الممكن لها ان تشكل رادع للمجرمين الاخرين خوفا من

	التعرض للعقوبة، فهذه التطبيقات وظيفتها اكتشاف أي مسلك غير طبيعي يحصل في الشبكة وصدها في نفس اللحظة أو إعطاء انذار بان هناك جريمة او مسلك غير طبيعي يحصل، خاصة أن معظم الجرائم تأتي وتكون قد حصلت ، فهي تحد منها لانها تعمل على صدها في نفس الوقت وليست بعد وقوعها، بالتالي تقلل بشكل كبير من نسبتها سواء في المجرمين أنفسهم بعدم العودة لارتكاب الجرائم أو الجريمة التي ستنخفض.
مقابلة رقم (8)	عندما يقوم المجرمين بالدخول من اجل ارتكاب جريمة والبرنامج يقوم بصده وحماية الشبكة وكافة هذه التفاصيل تساعد بدرجة كبيرة في موضوع الحد من الجريمة الإلكترونيّة خاصة ان هذه البرامج ذات جودة عآليّة فمن الطبيعي ان تساعد على التخفيف من حجم الجرائم المرتكبة فعندما يتم تصميم برامج ذات علاقة في مراقبة المسلكيات التي تحصل داخل الشبكة باستمرار فان ذلك يحد من هذه الظاهرة.
مقابلة رقم (9)	تساهم بدرجة كبيرة من خلال علم الجاني بوجود مثل هذه البرامج والتطبيقات التي تشكل له رادع، فالجاني في الأساس لا يقبل على ارتكاب الجريمة الإلكترونيّة الا لعلمه انه لن يتم اكتشافه وتحديد موقعه فعندما يتم نشر ان هذه البرامج ساهمت الى حد كبير في كشف اكثر من جريمة في الفضاء الالكتروني فإن نسبة الاقبال على الجرائم الإلكترونيّة ستنخفض بشكل تدريجي فتكرار صد الهجمات والتجسس والاختراقات هي اكبر حد من الجريمة الإلكترونيّة.
مقابلة رقم (10)	تساهم في توفير ادلة أكثر للنيابة وتساعد على تتبع المعلومات والجرائم والكشف عن موقع الجريمة الإلكترونيّة ووقتها وتسلسل الاحداث داخل الشبكة وكذلك البيانات، من خلال ما يسمى بالـ (GPS) حيث يوفر الذكاء الاصطناعي برامج لحماية أمن المعلومات والشبكات والتصدي لجرائم الاختراق والسرقات.
مقابلة رقم (11)	ذلك من خلال كل مرة يتم فيها صد الهجمات وكشف الجريمة تقل نسبتها، واعتقد انها تساهم في الحد من خلال الإمكانيات التي يتمتع بها الذكاء الاصطناعي في كشف الجريمة والتعرف على هوية الجاني، فمن خلال معرفة هويته تساعد في الوصول على أدوات الجريمة فضلاً عن ان الكثير من تطبيقات الذكاء الاصطناعي تساعد على توفير الحماية من أي اختراقات وهجمات إلكترونيّة مفاجئة.
مقابلة رقم (12)	عندما يتوافر في الأساس أنظمة للكشف عن الجرائم بالتالي تصبح عملية احباط للمجرم الالكتروني فهو في كل مرة يحاول فيها ارتكاب جريمة تحبط كل اعماله الاجرامية، مثلا فيسبوك تعمل على اتخاذ القرار لحذف المنشورات المسئة للاخلاق بالتالي تقلل من نسبة الانخراط في ارتكاب الجريمة وعلى هذا المبدأ تساهم في الحد من الجريمة.
مقابلة رقم (13)	اعتقد انها لا تساهم بدرجة كبيرة في الحد من الجريمة الإلكترونيّة انما تساهم بنسبة (40%)، فهذه التطبيقات لها قدرة على التصنيف والتحليل وتحديد المسلكيات الطبيعة عن غير الطبيعية لكن هذا لا يكفي نهائيا فقط، ان القيام بكشف الجريمة الإلكترونيّة بحاجة الى اتخاذ إجراءات قانونية صارمة بحق من يرتكب هذه الجرائم لتكون مكمل لدور الذكاء الاصطناعي، فمن المهم للحد من هذه الظاهرة العمل على سن القوانين والتشريعات.
مقابلة رقم (14)	في اعتقادي ان هذه البرامج تساهم بدرجة عآليّة في الحد من الجريمة الإلكترونيّة في جانب المجرم نفسه وجانب الجريمة والتقليل منها، فعلى مستوى المجرم فإن هذه التطبيقات في كل مرة يسعى الجاني الى ارتكاب جريمته تقوم هذه التطبيقات باتخاذ القرار بصد الهجمات والاختراقات ومنع حدوثها كما وانها تتنبا بوقوعها، أما في مجال الجريمة ففي كل مرة يتم صد الهجمات ومراقبة المسلكيات والتحركات على الشبكة بالتأكيد ستنخفض حتى لو لم تنخفض فانها لن تزيد.
مقابلة رقم (15)	من خلال عدد المرات التي يتم فيها اكتشاف الجريمة ففي كل مرة يتم فيها الكشف عن الجريمة ومن ثم صدها تعمل على التقليل من احتمآليّة زيادة المسلكيات المنحرفة كما انها تضعف من الفرصة امام مرتكبي الجرائم الإلكترونيّة في كل محاول لهم في القيام بجرائم فهذه البرامج فعّالة وتعمل على احباط كافة أساليبه ضمن البديهي بهذا الشكل يمكن ان تساعد في الحد من الجريمة الإلكترونيّة.
مقابلة رقم (16)	أرى انها تساهم الى حد كبير في التقليل من الجريمة التي يتم ارتكابها في الفضاء الالكتروني فعندما يتم نشر هذه البرامج في السوشيال ميديا وهي المواقع الأكثر اكتظاظ بالناس فانها تعمل بشكل دقيق على صد الهجمات التي يتعرض لها المستخدمين من خلال الحساسات عند الشعور باي حركات مشبوهة، فهذه البرامج في كل مرة يتم فيها صد الاختراقات والهجمات من شانها ان تعمل على الحد من هذه الظاهرة، بالتالي فهي تضعف الفرص امام الجناة وامام الأشخاص

	الاخرين في التفكير في ارتكاب الجرائم الإلكترونيّة او الحاق الضرر لعلمه ان هذه البرامج ستصد أي تصرف يقوم بها.
مقابلة رقم (17)	حسب اين ارغب في تطبيقها، مثلا هل ارغب في تطبيقها على السوشيال ميديا بالتالي انا هنا اخذ منها بشكل كبير جدا، فانا أرى في تطبيقها من هي الجهة المستفيدة ومما لا شك فيه ان هذه البرامج تعمل على التقليل من نسبة الجريمة الإلكترونيّة في كل مرة يتم فيها اكتشاف مسلكيات منحرفة وغير طبيعية على الشبكة.
مقابلة رقم (18)	تساهم بدرجة كبيرة من خلال العمل على تحديد موقع الجاني ومكان تواجده ومساره على الشبكة وما هي كل التحركات التي قام بها على الشبكة فهذه البرامج لديها القدرة على تحديد الجريمة وكشفها، بالتالي فان هذه البرامج بهذه الطريقة تساهم في الحد من الجريمة الإلكترونيّة ، كما انها لديها قدرة على التنبؤ بالجريمة الإلكترونيّة أي الاستباقية فتصدها او تحذر بوجودها.
مقابلة رقم (19)	من خلال التوعية بوجود هذا النوع من البرامج الجديدة فعندما يتم نشر الوعي بين افراد المجتمع بوجودها فان ذلك يشكل لدى الجناة بان كافة الجرائم التي سيسعون الى ارتكابها ستكون معروفة وفي ذات الوقت تشكل مصدر راحة للمواطن، هذا برأيي في حد ذاته مساهمة في الحد من الجريمة الإلكترونيّة في المجتمع.
مقابلة رقم (20)	عن طريق البرامج التي يتم بناؤها والتنبؤ بالجرائم الإلكترونيّة وتتبع الشبكة، او اذا كانت الشبكة عرضة للاختراق من قبل مجرمين بناءً عليها تعمل على تحليل الـ (IB) وتحليل المسار فيها يصبح عندي معطيات واضحة وادلة واضحة من اجل الكشف عن الجريمة بالتالي نقلل منها.
مقابلة رقم (21)	بشكل عام كل برنامج له بيانات عن المشتركين ويكون موجودة لديه في قواعده فاي شخص يرغب في ارتكاب جريمة إلكترونيّة أو مسلك غير طبيعي فان هذه البرامج داخل الشبكة تقوم باكتشافه أي انها تساعد بدرجة كبيرة في الحد من الجريمة من خلال ان كل حركة مراقبة ومسجلة بالتالي تحبط جريمته في حال ممارسته لها.
مقابلة رقم (22)	نعم تساهم في الحد منها من خلال دقة هذه البرامج وقدرتها العآليّة على كشف الجريمة الإلكترونيّة فهي تعمل على افشال محاولات المجرمين في اختراق الأنظمة او أي نوع من الجرائم الإلكترونيّة، بالتالي تقلل من نسبة وقوعها، كما انها تساهم في زيادة الحماية والرقابة الأمنية.
مقابلة رقم (23)	كلما كان هناك فكرة وتصور لدى الجناة بوجود تطبيقات خاصة بالذكاء الاصطناعي تعمل على كشف الجريمة وتوضيح ما هي هذه البرامج كلما كان هناك إنخفاض في نسبة المقبلين على ارتكاب الجريمة الإلكترونيّة نظرا لان فرص الجناة في ارتكاب الجريمة شبه معدومة فهي بهذه الطريقة تعمل على الحد منها.
مقابلة رقم (24)	نعم اكيد تساهم بدرجة عآليّة انا عندما أقوم بتصميم برامج تعمل على الحساسات والمشتسعرات من خلال تعليمها على الاحداث والمسلكيات غير الطبيعية واكسابها الخبرة فهي تعمل على الحد من الجريمة الإلكترونيّة، كما وانها تعمل على تقييد حركة المجرمين على الشبكة بالتالي تضعف الفرصة امام الجناة.
مقابلة رقم (25)	من خلال التتبع الالي للمسلكيات المنحرفة لان التتبع الالي يكون اسرع وادق، إن برامج الذكاء الاصطناعي هي برامج يمكن لها ان تتعلم بنفسها من خلال مجموعة من الخبرات والمهارات حيث تصبح لديها القدرة على استخلاص ان هناك مسلكيات غير طبيعية تحصل داخل الشبكة كما وانها تعمل على افشال المحاولات التي يقوم بها المجرمين فانا أرى انها بهذه الطريقة تساهم بدرجة كبيرة في الحد من الجريمة الإلكترونيّة.
مقابلة رقم (26)	من الممكن رصد الهجمات الإلكترونيّة ومنع أي دخول غير معروف وغير موثوق فيه فهذه التضيقات لها أهمية كبيرة في الحد من الجريمة الإلكترونيّة فعند تطبيق هذه البرامج يمكن التقليل من فرص المجرمين العبث في المعلومات كما وانها تساهم في الحفاظ على امن البيانات من التعديل عليها او العبث بها واشياء أخرى.
مقابلة رقم (27)	تساهم في الحد من الجرائم الإلكترونيّة من خلال التنبؤ بوقوع الجريمة ومتى قبل حدوثها، هذا ما يسمى بالخطوط الاستباقية لمنع الجريمة قبل حدوثها حيث ان هناك خوارزميات مبنية على مبدأ التنبؤ تقوم بالتنبؤ بوقوع الجريمة الإلكترونيّة، بالتالي فيما بعد تقوم بارسال إشارات انذار بوجود مسلكيات مشبوهة كل ذلك يساعد في الحد من الجريمة ومساعي المجرمين الالكترونين.
مقابلة رقم (28)	هذه البرامج عندما يتم تصميمها هي تصمم من اجل التصدي للجرائم الإلكترونيّة فيتم ادخال جميع الحالات المشابهة

	للجرائم وانواعها بالتالي تكون وظيفتها في الشبكة التصدي للجرائم الإلكترونيّة طوال الوقت فهي تقوم بمراقبة كافة المسلكيات والحركات وفي كل مرة يحاول فيها الجاني القيام بجريمة تصده وتضعف فرصة ارتكابه للجريمة، وهذا ما يساعدها في الحد من الجريمة الإلكترونيّة
مقابلة رقم (29)	تساعد هذه التطبيقات من خلال قدرتها على كشف تسلسل حركة الجاني على الشبكة من الحصول على الأدلة الكافية والواضحة من اجل عرضها على النيابة والمحاكم كون أن برامج الذكاء الاصطناعي تقوم بتسجيل كافة التحركات على الشبكة فهي تساهم في دعم موضوع محاكمة المجرمين واستكمال الإجراءات القانونية بحقهم، بالتالي تحد من اقبال المجرمين وعليه تقل نسبة الجريمة.
مقابلة رقم (30)	من خلال تطوير خوارزميات قادرة على الحد من الجريمة الإلكترونيّة حيث ان معظم الموازنات في الدولة تصرف على الجانب الأمني واهم نوعين في الخوارزميات هي : - خوارزميات التصنيف. - خوارزميات التنبؤ، يمكن من خلالهما الحد من الجريمة بشكل كبير جدا.
مقابلة رقم (31)	يمكن من خلال العمل على تصميم برامج قادرة على التصنيف والتنبؤ بوقوع الجرائم فهي بذلك تشكل عنصر احباط للمجرمين الالكترونين.
مقابلة رقم (32)	يمكن الحد من الجريمة الإلكترونيّة من خلال ردع الجاني وقدرة هذه التطبيقات على مساعدة المؤسسات الاستفادة منها من اجل التقليل من حجم الجرائم نظرا لما تتميز به من مميزات في التصدي للهجمات الإلكترونيّة.
مقابلة رقم (33)	هذا النوع من البرامج التي ظهرت بشكل كبير في الأونة الأخيرة ليست كالتكنولوجيا التقليدية والمتعارف عليها، انما برامج لديها القدرة على ما يسمى بالتبؤ هذه القدرات تعطيها الاستباقية في التنبؤ بالاحداث والمسلكيات المنحرفة داخل الشبكة، ومع تكرار كل اكتشاف للجريمة الإلكترونيّة يتم الحد من نسبتها في المجتمع بحيث لا يصبح هناك زيادة في اعدادها، كما وأنه عندما يتم تأمين المؤسسات والشركات والبنوك وكافة القطاعات ببرامج الحماية والأمان فانها ستقلل الفرص أمام المجرمين في ارتكاب الجرائم الإلكترونيّة وعدم مقدرتهم على استغلال الثغرات في مساعيهم الاجرامية، فهذه البرامج تعمل على صد الهجمات الإلكترونيّة والتخلص منها بشكل تلقائي مما يوفر الحماية من أي جريمة.
مقابلة رقم (34)	تساهم من خلال الكشف عن الكثير من الاعمال الغير قانونية مثلا كعملية النصب والاحتيال من قبل الهاكرز التي تتم بطريقة عشوائية فهذه التطبيقات الحديثة اي الانظمة المزودة بالذكاء الاصطناعي تعمل على كشف الكثير من تلك العمليات وكذلك يمكن من خلالها تحديد هوية الجاني ومعرفة الشبكة التي يتم استخدامها في الدخول الى النظام ان كانت حقيقة او وهمية، إن ما سبق جميعه يلعب دور مهم في الحد من الجريمة خاصة انه يتم الكشف عن الجاني.
مقابلة رقم (35)	من خلال الكشف المبكر عنها والحد منها وحماية الجاني من الوقوع فريسة للمجرمين الالكترونين، فضلاً عن الحماية من خطر التهديدات الأمنية مما يدفع بالجاني الى العزوف عن ارتكاب الجرائم الإلكترونيّة كما انه من اهم عناصر الحد من الجريمة الإلكترونيّة التنبؤ بوقوع الجريمة وصدها او إعطاء انذار بوجود خلل في هذا الموقع.
مقابلة رقم (36)	إن نظام الكشف عن البرامج الضارة واي تهديدات تتعرض لها الشبكات تعمل على التقليل من نسبة الجريمة الإلكترونيّة من خلال اكتشاف هذه الجرائم، فهذه النظم الحديثة التي تعمل على أساس الحساسات من شانها ان تعمل على صد أي هجمات إلكترونيّة فهي تقلل من فرصة المجرم لاستخدام الأساليب التقليدية خاصة ان هذه البرامج تستخدم قدرات عآليّة وذات دقة عآليّة وسرعة في الكشف عن الجرائم الإلكترونيّة.
مقابلة رقم (37)	من خلال تصميم خوارزميات التنبؤ لدى هذه الخوارزميات القدرة على التنبؤ بالجريمة الإلكترونيّة ومن ثم الكشف عنها وكشف هوية الجاني وكافة تفاصيله، بالإضافة الى السرعة في اجراء هذه العملية.
مقابلة رقم (38)	بالأساس الذكاء الاصطناعي يساهم في مختلف المجالات ماذا لو كان هذا المجال هو مجال الامن وحماية الشبكات، إن إحتواء هذه التطبيقات على خوارزميات خاصة تمكنها من الكشف عن الجريمة ولديها مستشعرات قادرة على التنبؤ بوقوع جريمة، كل هذا يساهم في الحد من ممارسة الجريمة بدرجة كبيرة، ولمنع الهجمات التي يقوم بها الهاكزر يتم التضيق على تحركاتهم واستغلالهم للثغرات على الشبكة.

مقابلة رقم (39)	تساهم من خلال التصنيف والتحليل لكافة المسلكيات المنحرفة التي تحدث داخل الشبكة فأي مسلك غير مقبول وغير طبيعي يحصل داخل الشبكة تعمل على اكتشافها، وهذا بدوره يساعد في التقليل من نسبة الجريمة الإلكترونيّة.
مقابلة رقم (40)	من خلال الكشف المبكر عن الجريمة الإلكترونيّة ومن خلال تتبع الجرائم وتتبع المسلكيات التي يقوم بها المواطنين على شبكة الانترنت، بالتالي في كل مرة يتم فيها ارتكاب جريمة من قبل أي شخص فانها تعمل على صد هذه الهجمات والاختراقات او العمل على إعطاء إشارات انذار بوجود مسلك مشبوه في الشبكة.
مقابلة رقم (41)	من خلال تعلم الاحتمالات الصحيحة والاحتمالات غير الصحيحة، بناءً على ذلك تقوم باتخاذ القرار المناسب لما سيكون مستقبلا ذلك عن طريق استخدام خوارزميات تحليلية بناءً على عدد ودقة النتائج واتخاذ القرار في جريمة معينة.
مقابلة رقم (42)	ان تعزيز قدرة برامج الذكاء الاصطناعي في التنبؤ وتحليل اكتشاف الجرائم الإلكترونيّة، كما وانها عندما تقوم بمراقبة كافة المسلكيات التي تحصل داخل الشبكة وتعمل على صدها والتوصل الى موقع الجاني والحصول على معلومات مفصلة عنه من خلال البيانات والتعرف على تسلسل حركته داخل الشبكة ومعاقبته، لا شك في ان ذلك يسهم في الحد من انتشارها بشكل كبير،
مقابلة رقم (43)	تساهم بالحد من الجريمة الإلكترونيّة من خلال قدرتها على التنبؤ الأمني لاي مسلكيات غير طبيعية تحصل داخل الشبكة ففي كل محاولة تقوم فيها هذه التطبيقات باكتشاف الجرائم الإلكترونيّة تقلل من فرص المجرمين على ارتكاب هذه المسلكيات مرة أخرى.
مقابلة رقم (44)	هذه البرامج ممكن ان تكون مساهمة في الحد من الجريمة الإلكترونيّة من خلال قدرة برامج الذكاء الاصطناعي على كشف الجريمة ومكافحة الفيروسات وصدها ومساهمتها في حماية الافراد الضحايا من الوقوع فريسة من قبل المجرمين الالكترونين، كما وانها تقلل الفرص امام المجرم في ارتكاب جريمته خاصة انها تقوم بكشف هويته وأماكن تواجده.
مقابلة رقم (45)	كون هذه البرامج تعمل على نظام التعلم الالي فهي تتعلم من التجارب السابقة وتبدأ بتكوين مجموعة من الخبرات والمهارات في قواعدها المعرفية بناءً عليها تقوم باتخاذ القرارات بخصوص الجرائم التي تتعرض لها فعندما تحصل أي انتهاكات واختراقات تقوم هذه البرامج بالتصدي لها ومنع أي هجوم من الممكن ان يتعرض له، فإنها بذلك تقلل من نسبة الجرائم الإلكترونيّة ومن انتشارها.
مقابلة رقم (46)	الذكاء الاصطناعي يساعد في حل جزء من الجريمة وكشف الجريمة والحصول على ادلة، لكن الذكاء الاصطناعي لا قدرة له على العلم باسباب الجريمة يمكن لي ان أقوم بتوظيفه في حل الجريمة بعد وقوعها والعمل على تتبع المجرم لكن هو لا يعلم بنوايا الناس، انا افضل ان يتم العمل على الحد من هذه الظاهرة من خلال نوايا الناس لانه اهم وفي كل الأحوال المجرم المصمم على ارتكاب الجريمة الإلكترونيّة سيقوم بارتكابها باي شكل من الاشكال.
مقابلة رقم (47)	تساهم بشكل ما في مراحل التتبع لاي حدث امني او اختراقات او جريمة إلكترونيّة حيث ان لديها القدرة على تتبيع الاحداث والأشخاص، ومعرفة السلوك العام للمواطنين ضمن السياسات العامة، والعمل على نشر الوعي ونشرات التوعية التي تصدر من مختلف المنظمات المجتمعية من اجل توعية المواطن وتدريبه على استخدام التكنولوجيا بالطريقة الصحيحة .
مقابلة رقم (48)	يساهم في الحماية الصحيحة من الوقوع فريسة للمجرم الالكتروني، ويساهم في حماية المؤسسات والبنوك وكافة القطاعات الأخرى من استغلال الثغرات فيها، إضافة إلى أنه يساهم في التنبؤ بالجريمة الإلكترونيّة والاستباقية بالاحداث والعمل على منع وقوع الجرائم.
مقابلة رقم (49)	الجريمة الإلكترونيّة من خلال تطبيقات الذكاء الاصطناعي يتم تتبعها واحضار الجاني والعثور عليه بطريقة اسهل واسرع ضمن أدوات متوافرة في هذه التطبيقات من خلال مثلا برنامج (WAF) يمكن لنا الحصول على معلومات فهذه التطبيقات هي التي توفر لي المعلومات التفصيلية والدقيقة وتتبع حركة ومسار المجرم ومن ثم التوصل إليه، بالتالي تساعد في حل جزء من الجريمة الإلكترونيّة ويمكن لهذا الجزء الحد من الجريمة الإلكترونيّة.
مقابلة رقم (50)	يتميز الذكاء الاصطناعي عن الابتكارات الأخرى بخاصية الاستباقية أي استباق حصول الأمور وليس فقط التفاعل مع الحدث فيمكنه في الامن الالكتروني تنبؤ الاختراقات ومنع حدوثها بالإضافة الى تأمين الأنظمة من أي عيوب يمكن ان

	يستخدمها المخترقون وأيضا يساعد الامن الالكتروني المالي مثل التوقيع الالكتروني في الحد من اختراقات البيانات الخاصة، ويتميز الذكاء الاصطناعي في الامن الالكتروني بسرعة ردة الفعل من مواجهة أي خطر الكتروني بشكل تلقائي وسريع في أي وقت وضد أي تهديد محتمل بفاعلية اكبر من ردة فعل الكادر البشري الذي يصله انذار اختراق.
كيف يمكن أن تكون برامج الذكاء الإصطناعي رادع أمام الجُناة لمنع ممارسة الجريمة الإلكترونيّة والحد منها؟	
مقابلة رقم (1)	من الممكن عمل توعية وتثقيف عن ما هو الذكاء الاصطناعي وما هي البرامج التي تندرج في مجال عمله، وعن مدى قدرة الذكاء الاصطناعي الكشف عن الجريمة الإلكترونيّة ومرتكبيها والتوصل الى موقعهم، وان كل حركة هي مسجلة على الشبكة، كما انها برامج سريعة ودقيقة، كل ذلك يُدخل المجرمين الى دائرة الخوف من ارتكاب جريمة والتفكير جيداً قبل ممارستها.
مقابلة رقم (2)	من خلال نشر هذه التقنيات والتطبيقات على الاعلام، والقيام بعمل نشرات إعلامية للناس انه تم استحداث برامج تطبيقات ذكاء اصطناعي مختصة في تتبع المجرمين الالكترونين واي شخص يقدم على هذا العمل سوف يتم اكتشافه وهو مراقب طوال الوقت في حال قرر القيام بمسلكيات إجرامية، كما وانه سيتعرض للمساءلة القانونية عند الإمساك به من خلال برامج الذكاء الاصطناعي، بالتالي فان ذلك من شأنه ان يمنعه من العودة لارتكاب الجريمة الإلكترونيّة لكن يجب ان تكون العقوبة صارمة بحق كل من يكرر هذه المسلكيات، ويوجد سياسة تم اعدادها مؤخرا بخصوص امن المعلومات ممكن تكون رادع للتخفيف من انتشار الجرائم الإلكترونيّة
مقابلة رقم (3)	عند علم الجاني انه مراقب طوال فترة استخدامه للشبكة من المؤكد أنه لن يعود الى ارتكاب الجريمة فانه عندما يعلم بوجود هذه البرامج وقدرتها على مراقبة كافة تصرفاته واي حركة غريبة يقوم بها تقوم باصطياده فانه سيعزف عن ارتكاب جريمته. فضلا عن ان هذه البرامج ذات خبرة ومهارة في كل مرة يحاول فيها القيام بالملسكيات الاجرامية فانها تعمل على صده كما انه يحتاج الى اكتساب خبرات ومهارات اعلى من هذه التطبيقات حتى يتمكن من التفوق عليها، فالجاني يعتمد على الطرق التقليدية المعروفة، والأشخاص الملمين الملم كامل بالتكنولوجيا وبادق تفاصيلها نادرين جدا بالتالي كل ذلك يعرضه للمحاكمة والسجن ولن يعود الى ارتكاب الجريمة.
مقابلة رقم (4)	كما ذكرت في حال الكشف عن شخص مارس جريمة ممكن ان يسبب ذلك الخوف للمجرمين الاخرين من التعرض للمحاكم والمساءلة القانونية، لكن ليس شرطا ممكن بعض المجرمين تشكل لديهم تحدي وفضول اكثر في اختراق الأنظمة ، اعتقد انه لو ان كل الناس ارتدعت كانت الجرائم كافة انتهت من المجتمع أي انا أرى ان مثلها مثل أي جريمة موجودة في المجتمع.
مقابلة رقم (5)	من الممكن أن تكون رادع من خلال تقليل صلاحيات الجناة في التنقل بين المواقع، كما الرقابة المستمرة لهم من قبل هذه التطبيقات يساعد في الحد من حركتهم وتصرفاتهم داخل الشبكة، فهذه الصلاحيات المحدودة لهم وتقييد حركتهم داخل الشبكة هي أكبر عامل ليعلم أن جريمته لن تنجح، بالتالي يؤدي الى ضعف الاقبال الى ارتكاب هذا النوع من الجرائم لعلمه انه مراقب وسوف يتم اكتشافه فيما بعد، وتعريضه فيما بعد للمحاكم والنبذ في المجتمع.
مقابلة رقم (6)	الردع يمكن من خلال توظيف هذه التطبيقات في سرعة اكتشاف الجريمة والقدرة على تحليل البيانات والمعطيات المتوافرة، فهذه البرامج تعمل على صد الاختراقات وتشكل حماية من أي تلاعب وتجسس أو مسلكيات منحرفة، بالتالي فان تكرار صد الهجمات تساعد في عدم عودة الجاني الى ارتكاب الجريمة الإلكترونيّة.
مقابلة رقم (7)	كما ذكرت في حال الكشف عن شخص ممكن ان تسبب الخوف للمجرمين الاخرين ويشعروف بالخوف من التعرض للمحاكم والمساءلة القانونية، لكن ليس شرطا ممكن بعض المجرمين تشكل لديهم تحدي وفضول اكثر في اختراق الأنظمة ، اعتقد لو ارتدعت كل الناس كانت الجرائم كافة انتهت من المجتمع أي انا أرى ان مثلها مثل أي جريمة موجودة في المجتمع.
مقابلة رقم (8)	عند علم الجاني ان كل عملية مسجلة على الشبكة وان البرامج الخاصة بالذكاء الاصطناعي فعّالة، وان أي تصرف يقوم به على الشبكة هو مسجل حيث تقوم هذه التطبيقات بالتنبؤ بمسلكياته وصدها، بالتالي يكون لديه علم انه سوف يتم

	اكتشافه مما يعني عدم نجاح جريمته، وهكذا تشكل له رادع في عدم اقباله مرة أخرى على ارتكاب الجريمة.
مقابلة رقم (9)	ان اقبال المجرم على ارتكاب الجرائم الإلكترونيّة ما هي الا لعلمه ان الرقابة ضعيفة فعند علمه بان هناك برامج تم جلبها وتصميمها لتتبع الجرائم الالكتروني وتتبع الأنشطة على الشبكة فانها تشكل افضل وسيلة لردع المجرمين، وعند شعوره ان هذه البرامج تراقبه الكترونيا وان كافة تحركاته مسجلة في الشبكة لن يقوم بالجريمة الإلكترونيّة فهي بالنسبة له وسيلة حاسمة لاكتشافه ومن ثم تعرضه للمساءلة القانونية كما وان حركته داخل الشبكة مقيدة ومحدودة ولا وسيلة لارتكاب جريمة.
مقابلة رقم (10)	من خلال الكشف عن موقع الجناة كما وانها تكشف عن هويتهم الحقيقة ومكان ممارسة الجريمة والطرق المستخدمة من قبل الجناة في اختراق واختلاس وسرقة البيانات، فعندما يتم الكشف عن كل ذلك فان الجاني لن يعود الى ارتكاب الجريمة الإلكترونيّة مرة أخرى.
مقابلة رقم (11)	رادع بشكل جزئي لكن هناك حاجة الى وجود قوانين من اجل معاقبة المجرمين كون أن هذه البرامج لوحدها لا تكفي، لان المجرم الراغب بارتكاب الجريمة سيعمل على ارتكابها واكتشاف الثغرات لن تشكل رادع للجاني الا اذا كانت هناك تطبيقات ذكاء اصطناعي حديثة بالإضافة الى وجود قوانين وتشريعات صارمة عند تعرضه للمساءلة القانونية لضمان عدم عودته للجريمة، فالتطبيقات لوحدها لا تكفي لردع.
مقابلة رقم (12)	كون الجاني يعلم بوجود برامج وتطبيقات ذكاء اصطناعي حديثة فمن الصعب عليه القيام بأي مسلكيات منحرفة داخل الشبكة، بالتالي اذا أراد التغلب عليها عليه ان يعمل على ابتكار مهارات وطرق جديدة وهؤلاء الأشخاص قلة بالمقارنة مع مجمل الناس، كما ان هذه البرامج من خلال عملها تعمل على كشف المجرم وأماكن تواجده أينما كان ومعلومات عنه فهي تعرضه للمساءلة القانونية.
مقابلة رقم (13)	بعد اكتشاف المجرم وجريمته بوجود الأدلة على ذلك تتم محاكمته حسب الأصول وليس فقط بالكشف عن الجريمة، صحيح أن هذه البرامج هي من تكشف عن الجريمة بأكملها لكن بعد اكتشاف الجريمة نحن بحاجة الى متابعة من اجل ضمان عدم عودة المجرم الى ارتكاب الجريمة الإلكترونيّة، وبحاجة كذلك الى قوانين مشددة لمعاقبة من يقوم بهذه المسلكيات الاجرامية.
مقابلة رقم (14)	الجاني اذا وجد ان هناك وسائل تراقب أي تصرف يحصل داخل الشبكة وان أي محاولة سيقوم بها من اجل ارتكاب جريمة في الفضاء الالكتروني ستفشل فإنه سيفكر اكثر من مرة قبل الاقدام على ارتكاب الجريمة، كما وان شعوره أن هذه التطبيقات في كل مرة ستكشف أساليبه وفي نفس الوقت ستكشف هويته مما يعني تعريضه للسجن والعقوبات، هذا يعني الردع لجعل الجاني يفكر اكثر من مرة قبل ارتكاب الجريمة خاصة وان اساليبه القديمة لم تعد تجدي نفعا في ظل وجود برامج الذكاء الاصطناعي.
مقابلة رقم (15)	اكيد ستكون رادع، عند علمه بوجود تطبيقات ذكاء اصطناعي ستقل ثقته بالقيام بجريمته الإكترونية لان لديه علم انه سيتم اكتشافه على الفور، بالتالي لن يجازف في هذا الخصوص، فيتشكل لديه فكر بان كافة محاولاته ستفشل بسبب أن هويته الحقيقة ستتكشف مما يعني تعرضه للمحاكم وبطبيعة الحال هذا اكبر رادع له.
مقابلة رقم (16)	في كل مرة يحاول فيها الجاني ارتكاب الجريمة الإلكترونيّة فإن هذه البرامج لديها القدرة على صد الهجمات الإلكترونيّة، بالتالي يستدعي من الجاني ابتكار أساليب جديدة وحديثة كي يتمكن من التفوق على برامج الذكاء الاصطناعي، وفي الأساس هؤلاء الأشخاص قلة في المجتمع كون هذه البرامج في الأصل حديثة وغير منتشرة، بالتالي تضعف فرصة الجاني في ارتكاب جريمة إلكترونيّة وتجعله يفقد الامل في نحاج مشروعه الاجرامي.
مقابلة رقم (17)	عند علمه ان تصرفه لمسلكيات غير طبيعية او قيامه باي جريمة إلكترونيّة كلها تحت الرقابة فمن الطبيعي انه سيقلل من الجريمة الإلكترونيّة هذا بحد ذاته شكل من اشكال الردع وردع بالنسبة للجاني، هذا يعني أنه سيقوم باللجوء الى طرق أخرى من اجل ارتكاب الجريمة الإلكترونيّة لكن هذه التطبيقات تحتاج الى أساليب ومهارات اعلى، بالتالي تضعف فرصة الجاني في ارتكاب جريمته الإكترونية، وفي النهاية عند معرفة الجاني أن هذه البرامج ستكشفه وستكشف جريمته وستعرضه للمحاسبة سوف يرتدع.
مقابلة رقم (18)	المجرم مهما كانت جريمته كاملة لا بد ان يترك دليل عندما يفكر الجاني أنه من خلال هذه التطبيقات اذا قام بارتكاب جريمة فانه سوف تعرف هويته وتتكشف جريمته سيكون ذلك رادع له في مجال ارتكاب الجريمة الإلكترونيّة وفي الغالب إن

	لقوة هذه التطبيقات دور في اغلاق كافة الطرق والوسائل امامه في التفكير للقيام بمسلكيات إجرامية.
مقابلة رقم (19)	انا اعتقد انها رادع قوي جدا للجناة في عدم اقبالهم لارتكاب الجريمة الإلكترونيّة، فالقدرة التي تتميز بها هذه التطبيقات والتقنيات تزرع في نفوسهم الخوف والقلق من ان كل جريمة يتم ارتكابها ستكون مسجلة ومكشوفة، بالتالي يرى انه لا امل من ذلك فعندما يتشكل لديه خوف فهذا بحد ذاته اصبح رادع.
مقابلة رقم (20)	ستكون رادع من خلال انها تشكل لهم رهبة وخوف خاصة ان كان المجرم يعلم بوجود برامج ستشكل هذه البرامج رادع له، واخذ حيطة وحذر اكثر أي انه يأخذ احتياطه قبل القيام بالجريمة الإلكترونيّة.
مقابلة رقم (21)	هذه السياسات والمعايير تحددها اليات معينة من خلال العمل على استحداث برامج جديدة، عندما أقوم بجلب برامج جديدة تعمل على توفير الحماية وصد الهجمات والاختراقات، بالتالي لا فرصة للجاني في ارتكاب الجريمة الإلكترونيّة هذا ما يزرع في اذهان الافراد ان هناك تطبيقات توفر الحماية والأمان للمواطن ولا فرصة لنجاح جريمة الجاني وحتى اذا استطاع ارتكاب جريمة فان هذه التطبيقات قادرة على الوصول الى موقعه والحصول على معلوماته وتعرضه للمحاسبة القانونية.
مقابلة رقم (22)	من خلال علم المجرمين بوجود مثل هذه التطبيقات والبرامج ولا يرتدع الا اذا شعر ان كافة محاولاته باءت بالفشل خاصة عندما يرى الجاني انه لا جدوى من تكرار جريمته، بالإضافة الى العمل على نشر التوعية والتثقيف بوجود برامج الذكاء الاصطناعي كي تعزز شعور المواطن بالأمان وتضعف ثقة الجاني بقدرته على ارتكاب الجريمة.
مقابلة رقم (23)	ستكون رادع عند علم الجاني ان هذه التطبيقات موجودة في كل مكان، وانه حتى لو ارتكب جريمة إلكترونيّة كل اساليبه وطرقه مكشوفة ولا مجال لاخفاءها.
مقابلة رقم (24)	عندما يقبل المجرم على ارتكاب جريمة إلكترونيّة ويرى ان الضحية استشعر ان هناك حركة غير طبيعية حصلت وحاول ان يتفاداها وقامت التطبيقات بكشفه بالتالي فان الجاني سيعزف عن ارتكاب الجريمة الإلكترونيّة كما انه عندما يشعر انه سوف يتعرض للمساءلة القانونية فانه يتردد من القيام بالجريمة.
مقابلة رقم (25)	لانه سيشعر انه مراقب الكترونيا طوال الوقت لا مجال ان يتبع أي مسلكيات إجرامية أخرى، ولا يوجد احتمال كما العنصر البشري الذي يتعب وينام هذه البرامج والتطبيقات لا تتعب ولا تنام فهي تعمل على مدار الساعة، من هنا يتوصل الجاني انه لا فرصة من القيام بجريمته خاصة ان هذه التطبيقات هي ذات تقنيات وجودة عآليّة.
مقابلة رقم (26)	تتيح البرامج رصد التغيرات فورا وهذا يمنع ويضع الجاني تحت المجهر حيث تكشف هذه البرامج فورا عن قيام أي جاني بارتكاب جريمة إلكترونيّة، فيشعر الجاني ان اقباله على الجريمة الإلكترونيّة اصبح بلا جدوى وان هذه التطبيقات ستقوم باكتشافه على الفور وتقوم بتتبع مساره وتسلسل مجريات الاحداث التي قام بها على الشبكة.
مقابلة رقم (27)	لا يمكن لهذه التطبيقات التي تعتمد على الذكاء الاصطناعي ان تكون رادع بالكامل للمجرمين لان المجرمين كلما زادت التقنيات المتبعة كلما زادت طرق التحايل لديهم، وتشكل لديهم كنوع من التحدي للتحايل على هذه التطبيقات واستغلال أي ثغرة من اجل ارتكاب الجريمة، لكن بالطبع برامج الذكاء الاصطناعي تساهم في كشف جزء كبير من الجرائم الإلكترونيّة.
مقابلة رقم (28)	بما ان العالم متجه للحياة التكنولوجيّة فاذا كانت وسائل التواصل الاجتماعي تحتوي على تطبيقات الذكاء الاصطناعي في الكشف عن أي تصرف مسيء او جريمة إلكترونيّة فان ذلك سوف يساعد في التقليل من التهديدات التي تتعرض لها الشبكات من المجرمين.
مقابلة رقم (29)	ستشكل رادع للمجرمين الإلكترونيين من خلال زرع الخوف في نفوسهم من المسائلة القانونية نتيجة كشف هذه التطبيقات لكافة المسلكيات الاجرامية التي قام بها على الشبكة خاصة انها لديها قدرة على التنبؤ بالهجمات أي الاستباقية والعمل على صد أي اختراق تتعرض له الشبكات.
مقابلة رقم (30)	من خلال الخوارزميات المطورة يمكن التقليل من نسب الجرائم الالكتروني وردع المجرمين واخص هنا خوارزميات التنبؤ بتصرفات وسلوكيات الجناة في الواقع الافتراضي، بناءً على هذه التنبؤات التي تتميز بها هذه التطبيقات يعمل الجاني على اخذ الاحتياطات اللازمة ولا يقوم بالجريمة الإلكترونيّة.
مقابلة رقم (31)	عندما يتم نشر الورشات التوعوية للمواطنين بوجود تطبيقات ذكاء اصطناعي لديها خصائص تقوم بالكشف عن المجرمين

	وتعمل على توفير الحماية والأمان لمستخدمي الانترنت، فان ذلك يزرع في نفس المجرمين انه لن ينجح في ارتكاب الجريمة الإلكترونيّة.
مقابلة رقم (32)	عندما يتم محاسبة الجاني والحكم عليه بناءً على فعله الاجرامي نتيجة كشف تطبيقات الذكاء الاصطناعي لجريمته وبناءً على قدرتها على تحليل وتصنيف البيانات والتوصل الى موقع الجاني فإنها تعمل على صد الاختراقات واي جريمة تتعرض لها الشبكات وتعمل على تعزيز الخوف في نفس الجاني من المعاقبة نتيجة كشف هذه التطبيقات له.
مقابلة رقم (33)	من وجهة نظري أنه في كل مرة يتم اكتشاف الجاني من قبل هذه البرامج ومع كل مرة يتم فيها صد الاختراقات والانتهاكات فإنها تعرض الجاني للمحاكم والنيابة والإجراءات القانونية من أجل محاكمته وسلب حريته، حيث لا مفر له من ذلك، هذا من شأنه أن يقلل الفرص أمام المجرم من الاقبال مرة أخرى على ارتكاب هذا النوع من الجرائم، أيضا يجب في كل مرة يتم فيها اكتشاف الجاني بواسطة برامج الذكاء الاصطناعي العمل على نشر الاخبار كي تكون رادع أمام غيره من المجرمين ليصبح لديهم تخوف في ارتكاب الجريمة الإلكترونيّة، وهنا يتحقق الردع العام والخاص.
مقابلة رقم (34)	من خلال المسائلة القانونية واستخدام نتائج هذه البرامج التي تعتمد على الذكاء الاصطناعي في كشف الجرائم الإلكترونيّة كدليل اتهام لشخص الجاني امام المحاكم القانونية وتعرضه للعقاب على اثرها، إضافة الى عمل محكمة إلكترونيّة وتعزيز دور الحكومات الإلكترونيّة في كافة الدول.
مقابلة رقم (35)	فقط تكون رادع من خلال استخدام الدليل الذي قامت تطبيقات الذكاء الاصطناعي باكتشافه ومن ثم محاكمة المعتدي بالدليل وتعرضه للعقوبات الشديدة سيرتدع بهذا الشكل فقط، خاصة انه سيصبح عنده تصور ان الرقابة الأمنية فعّالة ضد أي مخاطر تواجه الشبكات والمستخدمين.
مقابلة رقم (36)	عند علم الجاني بوجود مثل هذه البرامج فانه من الطبيعي عندما يرغب بارتكاب جريمة إلكترونيّة سيقوم بالتفكير عدة مرات قبل الاقبال على ارتكاب الجريمة، والجاني كي يتمكن من التفوق على أساليب الذكاء الاصطناعي بحاجة الى مهارات وتقنيات اعلى من تلك التي يمتلكها.
مقابلة رقم (37)	يمكن لهذه البرامج ان تكون رادع قوي امام الجناة كون الجناة لم يرتدعوا من الطرق التقليدية فعند تطبيق برامج الذكاء الاصطناعي سيصبح لدى الجناة معرفة علم بوجود هذه الحماية الأمنية على الشبكات الأمر الذي سيضعف من تفكيرهم بالاقبال على الجرائم لعلمهم ان كل شي مراقب الكترونيا وواضح ومسجل ولا مجال لارتكاب جريمة إلكترونيّة مخفية.
مقابلة رقم (38)	عندما يظهر انذار لشخص ما ان هناك دخول غير طبيعي او غير صحيح يحصل سيكون اكبر رادع امام المجرمين ان هذه الأساليب فشلت ويستدعي منهم البحث عن أساليب جديدة كي يتمكن من اختراق هذه التقنيات المنتشرة كما انها تعرضهم للمحاكم والنيابة والسجن.
مقابلة رقم (39)	وجود التطبيقات القائمة على الذكاء الاصطناعي في الفضاء الالكتروني بحد ذاتها رادع للمجرم الراغب في ارتكاب جريمة والمعرفة بوجود هذه التطبيقات اهم من التطبيقات بحد ذاتها كي تشكل رادع قوي ومتين امام المجرمين بعدم ارتكاب ملسكيات إجرامية وتعطي المواطن الراحة والاطمئنان.
مقابلة رقم (40)	من الممكن ان تقوم برامج الذكاء الاصطناعي في الحد من الجريمة الإلكترونيّة من خلال قدرتها على كشف الجريمة قبل وقوعها هذا يتسبب في ردع المجرمين بسبب علمهم ان كل جريمة تحصل في الفضاء الالكتروني هي مسجلة ومراقبة ولا فائدة من الجرائم التي يقوم بها كما وانها ستعرضهم للمحاكمة.
مقابلة رقم (41)	عندما يتم تتبع الجناة من خلال تطبيقات الذكاء الاصطناعي فان المجرمين يتكون لديهم علم ومعرفة بهذه التطبيقات وان هناك برامج وظيفتها تتبع الجناة هذا من شأنه ان يعمل على الحد من ارتكاب الجريمة الإلكترونيّة.
مقابلة رقم (42)	كما سبق ان تعزيز فرص كشف الجريمة وتحديدها قبل وقوعها عند اقدام المجرمين على ارتكابها قد يشكل رادع للحد من الجريمة الإلكترونيّة كون الجاني قد جرب بنفسه ان يقوم بجريمة وقد قامت هذه التطبيقات بصدها.
مقابلة رقم (43)	عندما اعلم انا كمجرم انا كافة التصرفات التي أقوم بها هي مراقبة ومحفوظة في السجلات إن هذا بحد ذاته رادع بعدم التفكير بالجريمة مرة أخرى.

مقابلة رقم (44)	عند استخدام برمجيات الذكاء الاصطناعي وتحديد مكان الجاني سيؤثر ذلك على غيره من المجرمين ويستبب في ردعهم فهي تشكل لديهم الخوف من القاء القبض عليهم، في المقابل يوجد من المجرمين المطلعين بدرجة عآليّة على البرامج التكنولوجيّة فهي لا تشكل لهم رادع انما حب التحدي والفضول في سبيل اختراقها.
مقابلة رقم (45)	تشكل رادع لحد ما وليست بشكل كبير، في الأساس هذه الجرائم تعمل على حل جزء من الجريمة ليس بأكملها لكن اذا الشخص كانت التنشئة الاجتماعية لديه ضعيفة ومسلكياته منحرفة فإن الجاني سوف يسعى الى ارتكاب الجريمة في الواقع الافتراضي بأي شكل من الاشكال بغض النظر إذا توافرت برامج ذكاء اصطناعي ام لا.
مقابلة رقم (46)	بالتأكيد تساهم بشكل كبير في حال سهلت اكتشاف المجرم وكيفية حصول الجريمة من الممكن ان تشكل رادع امام الجاني بالتالي خيارات المجرم تقل واساليبه تقل لانه في كل الأحوال سوف يتم اكتشافه، هذا يعني أنه سيصبح لديه فهم انه لا جدوى من ارتكابه للجريمة الإلكترونيّة.
مقابلة رقم (47)	نعم ممكن ان تكون رادع قوي حيث أنه يعيش الشخص يشعر ان ضمن بنية تحتية قائمة على بعض السياسات العامة التي تتعلق بأمن المؤسسات ومعلوماتها، كما وان هذه التطبيقات المبنية على الذكاء الاصطناعي ستكون رادع اما بالنسبة للمواطن العادي ستكون بمثابة قوانين رادعة تراقب عمل المواطن او اقدامه على ارتكاب جريمة إلكترونيّة او أي استفزاز في الفضاء الالكتروني، وكذلك سرعة اكتشاف الجريمة عن طريق هذه البرامج ستكون رادع للشخص عن وللأخرين معاً.
مقابلة رقم (48)	عندما تقوم هذه التطبيقات باكتشاف المجرم الالكتروني من خلال التعرف على تفاصيل هويته فانها تكشف المجرم وتعرضه للمساءلة القانونية والمحاكم وكل ذلك يكون موثق بالدليل لان كل تصرف يتم داخل الشبكة تعمل تطبيقات الذكاء الاصطناعي على تسجيلها وهذا بحد ذاته رادع قوي جدا.
مقابلة رقم (49)	عند علمه ببرامج تراقب الشبكة الإلكترونيّة وتعمل على تتبع أي حركة موجودة، فعلى الأقل اذا رغب بارتكاب جريمة إلكترونيّة هو بحاجة الى مهارة عآليّة جدا وخبرة كبيرة كي يتمكن من القيام بذلك وحتى هذا الشيء موجود عند قلة من الناس.
مقابلة رقم (50)	تكون هذه البرامج القائمة على الذكاء الاصطناعي من وجهة نظري فعّالة في حال تمّ كشف هوية المجرم ومحاسبته قانونيا والقصد هنا كشف هوية المجرم عن طريق هذه البرامج ومحاسبته قانونيا بذلك قد تمنع وترهب أي شخص اخر من محاولة القيام باي جريمة الكترونيا خوفا من الكشف عن هويته ومحاسبته.

المحور الرئيسي الثاني: ما آليّة عمل برامج الذكاء الإصطناعي لتتبع الجناة مرتكبي الجرائم الإلكترونيّة؟ يتفرع عنه

هل هناك آليّات عمل متبعة في إستخدام برامج الذكاء الإصطناعي في الوزارة لتتبع الجناة المرتكبين للجرائم الإلكترونيّة؟ ما هي تلك الآليّات بشكل دقيق؟	
مقابلة رقم (1)	لا يوجد.
مقابلة رقم (2)	لا يوجد.
مقابلة رقم (3)	لا يوجد.
مقابلة رقم (4)	لا يوجد.
مقابلة رقم (5)	لا يوجد.
مقابلة رقم (6)	لا يوجد.
مقابلة رقم (7)	لا يوجد.
مقابلة رقم (8)	لا يوجد.
مقابلة رقم (9)	لا يوجد.
مقابلة رقم (10)	لا يوجد.
مقابلة رقم (11)	لا يوجد.

مقابلة رقم (12)	لا يوجد.
مقابلة رقم (13)	لا يوجد.
مقابلة رقم (14)	لا يوجد.
مقابلة رقم (15)	لا يوجد.
مقابلة رقم (16)	لا يوجد.
مقابلة رقم (17)	لا يوجد.
مقابلة رقم (18)	لا يوجد.
مقابلة رقم (19)	لا يوجد.
مقابلة رقم (20)	لا يوجد.
مقابلة رقم (21)	لا يوجد.
مقابلة رقم (22)	لا يوجد.
مقابلة رقم (23)	لا يوجد.
مقابلة رقم (24)	لا يوجد.
مقابلة رقم (25)	لا يوجد.
مقابلة رقم (26)	لا يوجد.
مقابلة رقم (27)	لا يوجد.
مقابلة رقم (28)	لا يوجد.
مقابلة رقم (29)	لا يوجد.
مقابلة رقم (30)	لا يوجد.
مقابلة رقم (31)	لا يوجد.
مقابلة رقم (32)	الوزارة تستخدم الذكاء الاصطناعي لكن لايوجد آليات متبعة في استخدامها
مقابلة رقم (33)	لا يوجد.
مقابلة رقم (34)	لا يوجد.
مقابلة رقم (35)	لا يوجد.
مقابلة رقم (36)	لا يوجد.
مقابلة رقم (37)	لا يوجد.
مقابلة رقم (38)	لا يوجد.
مقابلة رقم (39)	لا يوجد.
مقابلة رقم (40)	لا يوجد.
مقابلة رقم (41)	لا يوجد.
مقابلة رقم (42)	لا يوجد.
مقابلة رقم (43)	لا يوجد.
مقابلة رقم (44)	لا يوجد.
مقابلة رقم (45)	لا يوجد.
مقابلة رقم (46)	لا يوجد.
مقابلة رقم (47)	لا يوجد.
مقابلة رقم (48)	لا يوجد.

مقابلة رقم (49)	لا يوجد.
مقابلة رقم (50)	لا يوجد.
كيف تساهم الآليّات المتبعة في إستخدام برامج الذكاء الاصطناعي في الوزارة في التخفيف من نسبة الجريمة الإلكترونيّة المُرتكبة؟	
مقابلة رقم (1)	لا يوجد اليات.
مقابلة رقم (2)	لا يوجد.
مقابلة رقم (3)	لا يوجد.
مقابلة رقم (4)	لا يوجد.
مقابلة رقم (5)	لا يوجد.
مقابلة رقم (6)	لا يوجد.
مقابلة رقم (7)	لا يوجد.
مقابلة رقم (8)	لا يوجد.
مقابلة رقم (9)	لا يوجد.
مقابلة رقم (10)	لا يوجد.
مقابلة رقم (11)	لا يوجد.
مقابلة رقم (12)	لا يوجد.
مقابلة رقم (13)	لا يوجد.
مقابلة رقم (14)	لا يوجد.
مقابلة رقم (15)	لا يوجد.
مقابلة رقم (16)	لا يوجد.
مقابلة رقم (17)	لا يوجد.
مقابلة رقم (18)	لا يوجد.
مقابلة رقم (19)	لا يوجد.
مقابلة رقم (20)	لا يوجد.
مقابلة رقم (21)	لا يوجد.
مقابلة رقم (22)	لا يوجد.
مقابلة رقم (23)	لا يوجد.
مقابلة رقم (24)	لا يوجد.
مقابلة رقم (25)	لا يوجد.
مقابلة رقم (26)	لا يوجد.
مقابلة رقم (27)	لا يوجد.
مقابلة رقم (28)	لا يوجد.
مقابلة رقم (29)	لا يوجد.
مقابلة رقم (30)	لا يوجد.
مقابلة رقم (31)	لا يوجد.
مقابلة رقم (32)	لا يوجد.
مقابلة رقم (33)	لا يوجد.

مقابلة رقم (34)	لا يوجد.
مقابلة رقم (35)	لا يوجد.
مقابلة رقم (36)	لا يوجد.
مقابلة رقم (37)	لا يوجد.
مقابلة رقم (38)	لا يوجد.
مقابلة رقم (39)	لا يوجد.
مقابلة رقم (40)	لا يوجد.
مقابلة رقم (41)	لا يوجد.
مقابلة رقم (42)	لا يوجد.
مقابلة رقم (43)	لا يوجد.
مقابلة رقم (44)	لا يوجد.
مقابلة رقم (45)	لا يوجد.
مقابلة رقم (46)	لا يوجد.
مقابلة رقم (47)	لا يوجد.
مقابلة رقم (48)	لا يوجد.
مقابلة رقم (49)	لا يوجد.
مقابلة رقم (50)	لا يوجد.

في حال عَدم توفر آليّات تتبع للجرائم الإلكترونيّة، ماذا تَقترِح/ين لتوفير أو تحسين آليّات العمل المُتبعة في تَتبع الجرائم الإلكترونيّة؟	
مقابلة رقم (1)	من خلال العمل على: - توفير البرامج اللازمة التي تعمل على تتبع الجريمة وتطويرها. - توفير طاقم متخصص في برامج الذكاء الاصطناعي والجريمة الإلكترونيّة. - إعطاء التعليم والدورات والورشات اللازمة من اجل افادة المجتمع استخدام البرامج بطريقة صحيحة من اجل الاستفادة منها في هذا المجال.
مقابلة رقم (2)	من خلال العمل على: - التركيز على استيراد برامج ومعدات تعزز موضوع الذكاء الاصطناعي وتتبع المجرمين الالكترونيين. - مراعاة الخصوصية والسرية. - تتبع الجرائم الإلكترونيّة المنتشرة ومراقبتها وتطبيق تقنيات الذكاء الاصطناعي عليها. - تأسيس قسم خاص للذكاء الاصطناعي.
مقابلة رقم (3)	من خلال العمل على: - توفير فريق متخصص. - ضرورة الاستفادة من تجارب الدول الأخرى في هذا المجال. - نقل الخبرة والمهارة. - جلب برامج متعلقة بالجريمة الإلكترونيّة تكون برامج الذكاء الاصطناعي من بينها.
مقابلة رقم (4)	من خلال العمل على: - سن قوانين صارمة تتعلق بالجرائم الإلكترونيّة، بالإضافة لبرامج الذكاء الاصطناعي التي ستكون مكملة لبعضها البعض.

	- من خلال العمل على توفير ورشات بخصوص برامج الذكاء الاصطناعي وتوظيفه في تتبع الجرائم الإلكترونيّة . - العمل على تطبيق تطبيقات وبرامج الذكاء الاصطناعي التي تقوم بتتبع الجرائم الإلكترونيّة.
مقابلة رقم (5)	من خلال العمل على: - تطوير البنية التحتية لمثل هذا النوع من البرامج. - وضع كوادر متخصصة في التعامل مع هذا النوع من البرامج، يفضل أن يكونو من الحاصلين على تخصصات ضمن دائرة الذكاء الاصطناعي. - تكثيف الدورات المتعلقة بالجريمة الإلكترونيّة. - جلب الأجهزة لمتابعة نشاط وحركة المجرمين على الشبكات. - نشر الوعي والتثقيف بوجود هذه البرامج.
مقابلة رقم (6)	من خلال العمل على: - جلب متخصصين في مجال الذكاء الاصطناعي. - توفير ورشات عمل حول برامج الذكاء الاصطناعي وتتبع الجرائم الإلكترونيّة. - جلب الأجهزة والمعدات ذات الجودة العآليّة في مجال الذكاء االاصطناعي. - توظيف هذه الأجهزة في المراقبة الأمنية.
مقابلة رقم (7)	من خلال العمل على: - سن قوانين صارمة تتعلق بالجرائم الإلكترونيّة، إضافة الى برامج الذكاء الاصطناعي التي ستكون مكملة لبعضها البعض. - من خلال العمل على توفير ورشات بخصوص برامج الذكاء الاصطناعي وتوظيفه في تتبع الجرائم الإلكترونيّة . - العمل على تطبيق تطبيقات برامج الذكاء الاصطناعي التي تقوم بتتبع الجرائم الإلكترونيّة.
مقابلة رقم (8)	من خلال العمل على : - زيادة عدد المبرمحين في مجال الذكاء الاصطناعي. - زيادة الورشات والدورات المخصصة في هذا المجال. - تطوير البنية التحتية. وفي النهاية هذه البرامج عبارة عن خوارزميات يقوم البشر بتصميمها وتطويرها
مقابلة رقم (9)	من خلال العمل على: - استحداث أنظمة ذكاء اصطناعي لتتبع الجرائم الإلكترونيّة قبل وقوعها وليس بعد وقوعها لان معظم الجرائم المتوافرة تكتشف بعد وقوعها وليس قبل وقوعها. - تخصيص موازنات مآليّة للبرامج والمعدات والكوادر المتخصصة في مجال الذكاء الاصطناعي والجريمة الإلكترونيّة.
مقابلة رقم (10)	من خلال العمل على: - الحصول على احدث وأقوى برامج عالمية للحفاظ على امن الشبكات والمعلومات. - استحداث برامج تتبع الهاكرز والـ(Anti virus) مثل برامج الـ(Croundstriks).
مقابلة رقم (11)	من خلال العمل على: - وضع خطة شاملة. - جلب الخبراء والمختصين في هذا المجال. - إعطاء الموظفين المتواجدين دورات أكثر بالتالي يكون العمل مخصص في هذا المجال. - الحصول على برامج عالمية في مجال مواجهة الجرائم الإلكترونيّة خاصة تلك البرامج التي تعتمد على برامج الذكاء الاصطناعي في التصدي للمخترقين.

مقابلة رقم (12)	من خلال العمل على: - وضع خطة تشمل كافة نواحي العمل في هذا المجال. - دعم وتطوير البنية التحتية. - استقطاب كافة الخبراء والمتخصصين في مجال الجريمة الإلكترونيّة والذكاء الاصطناعي.
مقابلة رقم (13)	من خلال العمل على: - وضع سياسات وقوانين من أجل متابعة هذه الأمور تكون ذات مواصفات عالمية. - جلب معدات وأجهزة من اجل متابعة الحركات التي تحدث على الشبكات. - الحصول على موازنات مآليّة من اجل الاستمرار في جلب الأجهزة والمعدات الحديثة. - تخصيص كوادر متخصصة في مجال الذكاء الاصطناعي كي تتمكن من التعامل مع هذه البرامج.
مقابلة رقم (14)	من خلال العمل على: - تحسين البنية التحتية (فاالبنية التحتية أساس عمل برامج الذكاء الاصطناعي). - شراء مختلف البرامج ذات العلاقة بتتبع المجرمين واي نشاطات ومسلكيات إجرامية تحصل داخل الشبكة. - توفير كادر متخصص عامل في هذا المجال.
مقابلة رقم (15)	من خلال العمل على: - فتح مراكز برامج الذكاء الاصطناعي والجريمة الإلكترونيّة. - استقطاب الكوادر العاملة في مجال الذكاء الاصطناعي. - تخصيص موازنات مآليّة كون هذه البرامج تتطلب مبالغ مآليّة.
مقابلة رقم (16)	من خلال العمل على: - جلب الموازنات المآليّة من اجل جلب المبرمجين والمتخصصين في مجال الذكاء الاصطناعي وتتبع الجرائم التي تحصل في الواقع الافتراضي. - فتح اقسام في هذا المجال. - تطوير البنية التحتية من اجل تمكينها من استقبال التنوع في برامج الذكاء الاصطناعي. - شراء أجهزة ومعدات خاصة برامج الذكاء الاصطناعي. - شراء المعدات والأجهزة من خلال الموازنات المآليّة.
مقابلة رقم (17)	تأتي على أكثر من مستوى: - الجانب التقني أي الأشخاص المتخصصين ممن لهم دور في الرقابة والطرق اليدوية. - الجانب المتعلق بالتشريعات التي تحمي المواطن من الجرائم الإلكترونيّة، فمن المهم تخصيص وحدات ضمن النظام القضائي تشمل القانون والعقوبات. - العمل على فتح وحدات متعلقة ببرامج الذكاء الاصطناعي ومتابعة الجريمة الإلكترونيّة. - العمل على جلب الفنيين إلى جانب المتخصصين ببرامج الذكاء الاصطناعي.
مقابلة رقم (18)	من خلال العمل على: - التوعية وطمئنة المواطن ان هناك سرية في استخدام تطبيقات الذكاء الاصطناعي، وأن هذه البيانات والمعلومات ليست في متناول يد الجميع. - العمل على استحداث برامج ذكاء اصطناعي. - وضع موازنات مآليّة لهذه البرامج كونها تحتاج الى مبالغ مآليّة. - العمل على توفير بنية مناسبة لهذه البرامج لتصبح قادرة على استعياب التنوع في الأجهزة والبرامج. - العمل على توفير المبرمجين المتخصصين في مجال الذكاء الاصطناعي.
مقابلة رقم (19)	من خلال العمل على:

	- تطوير البنية التحتية لانها المكان الذي يحتوي على البيانات. - اعتماد متخصصين في مجال الذكاء الاصطناعي. - تكثيف الدورات المتعلقة ببرامج الذكاء الاصطناعي والجريمة الإلكترونيّة. - جلب الأجهزة المعتمدة على برامج الذكاء الاصطناعي من اجل توظيفها في تتبع الجرائم الإلكترونيّة.
مقابلة رقم (20)	من خلال العمل على: - تدريب متخصصين في مجال الجرائم الإلكترونيّة، وان يكون التدريب مكثف. - فتح قسم خاص ببرامج الذكاء الاصطناعي وممارسة الجريمة الإلكترونيّة ليكون خط الدفاع الأول.
مقابلة رقم (21)	من خلال: - الاعتماد على المزامنة الفورية وتنظيمها من قبل جهات الاختصاص. - العمل على فتح اقسام مخصصة في هذا المجال. - توفير الكوادر المتخصصة لهذه المزامنة.
مقابلة رقم (22)	انا اقترح انه يجب العمل على وضع خطة تشمل كل من : - العمل على فتح قسم خاص ببرامج الذكاء الاصطناعي لتتبع الجرائم الإلكترونيّة. - ضرورة توفير كوادر حاصلة على اختصاص ببرامج الذكاء الاصطناعي. - شراء معدات وأجهزة لتطبيق برامج الذكاء الاصطناعي. - توفير موازنات مآليّة في مجال شراء الأجهزة وتكثيف الدورات للعاملين في هذا المجال.
مقابلة رقم (23)	في الأساس مفهوم الذكاء الاصطناعي غير واضح في المجتمع لذلك اقترح: - ان يتم العمل على توضيع مفهوم الذكاء الاصطناعي. - ومن ثم العمل على وضع اقتراحات من أجل تطبيق برامج الذكاء الاصطناعي.
مقابلة رقم (24)	من خلال العمل على: - تطوير البنية التحتية. - توفير برامج متنوعة في البنية التحتية. - شراء تطبيقات ذكاء اصطناعي خاصة بتتبع الجرائم الإلكترونيّة وذات جودة عآليّة. - تخصيص جزء من الموازنات المآليّة لهذه البرامج.
مقابلة رقم (25)	لا بد من: - التشبيك مع المؤسسات الداخلية والخارجية. - جلب الموازنات المآليّة لانه من خلال الموازنات المآليّة المخصصة يمكن جلب كوادر مخصصة في مجال الذكاء الاصطناعي. - توفير الدورات وارسال المتخصصين فيها كي يتمكنوا من امتلاك الخبرة والمهارة ما يكفي لتعامل مع هذه البرامج وتطويرها باستمرار. - توفير الرقابة على الشبكات باستمرار. - شراء برامج الذكاء الاصطناعي المصممة في تتبع الجرائم الإلكترونيّة.
مقابلة رقم (26)	من خلال: - التثقيف حول أهمية برامج الذكاء الاصطناعي. - إرسال فريق مخصص للإلتحاق في دورات وورشات عمل ممولة. - تطوير المهارات والخبرات في مجال تطبيق الذكاء الاصطناعي لتتبع الجرائم الإلكترونيّة. - توفير موازنات مآليّة.
مقابلة رقم (27)	من خلال:

	- تحسين اليات العمل في تتبع الجرائم الإلكترونيّة حيث يجب ان يكون هناك حرفية ومتابعة دورية. - لا بد من وجود اليات وبرامج بان يتم فحص الأنظمة بشكل دوري وتوثيق النتئائج للاستفادة منها، والرجوع اليها عند الحاجة للتعلم منها في التنبؤ وفهم الأسباب لتكون اكثر دقة في تتبع الجرائم الإلكترونيّة.
مقابلة رقم (28)	من خلال العمل على: - نشر التوعية المجتمعية بعدم سوء استخدام التكنولوجيا وطمئنة الناس بان هذه التطبيقات تستخدم لمصلحتهم. - تفعيل دور القضاء الفلسطيني واعتماد الاخذ بالدليل. - توعية دور في مراقبة أبناؤهم أثناء استخدام التكنولوجيا. - جلب المتخصصين في مجال الذكاء الاصطناعي. - توفير دورات مخصصة في هذا المجال وتكثيفها لتعزيز المهارات والخبرات.
مقابلة رقم (29)	من خلال: - زيادة الدورات المتخصصة في مجال برامج الذكاء الاصطناعي. - فتح اقسام مخصصة لهذا المجال. - توفير برامج الذكاء الاصطناعي. - توفير الموازنات المآليّة.
مقابلة رقم (30)	لابد من فرض البرامج والتدريب اللازم في مجال برامج الذكاء الاصطناعي حتى يتسنى تطبيقها في مكافحة الجريمة الإلكترونيّة.
مقابلة رقم (31)	من خلال: - تعزيز البنية التحتية. - العمل على تدريب كوادر كي تتمكن من العمل مع برامج الذكاء الاصطناعي. - الحصول على موازنات مآليّة من الدول المانحة.
مقابلة رقم (32)	من خلال العمل على: - استحداث برامج لتتبع الجرائم الإلكترونيّة لكن بحاجة الى موازنة مآليّة. - تدريب الكوادر العاملة في هذه البرامج كونها حديثة وتحتاج الى خبرة ومهارة. - تكثيف الدورات الداخلية والخارجية بهذا الخصوص كي يتمكن العاملين في هذا المجال من الالمام والاطلاع على كامل البرامج.
مقابلة رقم (33)	اقترح عدة أمور يمكن اتباعها ومن ثم تعميمها كالتالي: - أن يكون هناك قوانين رادعة وعقوبات صارمة على مرتكبي الجرائم الإلكترونيّة وليس فقط الاعتماد على البرامج بل يجب ان تكون مكملة لبعضها البعض. - جلب معدات وأجهزة تعتمد على الذكاء الاصطناعي وكشف الجريمة الإلكترونيّة. - الحرص على السرية التامة في هذا المجال عند استخدام برامج الذكاء الاصطناعي خاصة ان هذا النوع من البرامج يحتوي على معلومات الأشخاص. - تأسيس قسم خاص ببرامج الذكاء الاصطناعي وتتبع الجريمة الإلكترونيّة. - العمل على تدريب الكوادر البشرية لتتمكن من الحصول على اعلى درجة من الخبرة والمهارة في التعامل مع الذكاء الاصطناعي.
مقابلة رقم (34)	من خلال: - تزويد كافة المؤسسات بالبرامج الذكيّة التي تعمل على اكتشاف الثغرات الإلكترونيّة والهجمات الإلكترونيّة من الخارج. - تدريب موظفين متخصيين في استخدام هذه البرامج بشكل كبيرة.

	- إعطاء المتخصصين في هذا المجال دورات وورشات عمل. - اختيار افضل البرامج المستخدمة في تتبع الجرائم الإلكترونيّة، والعمل على تشفيرها.
مقابلة رقم (35)	من خلال: - العمل مع ذوي الخبرة في هذا المجال. - توفير فريق متخصص للعمل فقط في مجال الذكاء الاصطناعي وتتبع الجرائم الإلكترونيّة.
مقابلة رقم (36)	العمل على: - توعية المجتمع بأهمية الذكاء الاصطناعي وتعريفه به. - مواكبة احدث التكنولوجيا واستحداث أجهزة ومعدات ذكاء اصطناعي للمواقع التي تحتاج الى حماية من الجرائم الإلكترونيّة. - توفير كادر مخصص لهذا المجال. - العمل على تطوير الرقابة الأمنية على الشبكات.
مقابلة رقم (37)	أرى انه يجب العمل كالتالي: - ضرورة وجود قانون لمعاملة مرتكبي الجرائم الإلكترونيّة يكون صارمة. - توفير كادر مخصص للعمل في منظومة الذكاء الاصطناعي. - تطوير قسم خاص ببرامج الذكاء الاصطناعي كي يتمكن الكادر المخصص من تتبع وملاحقة مرتكبي الجرائم الإلكترونيّة.
مقابلة رقم (38)	من خلال: - تطوير البنية التحتية المخصصة لذلك. - تطوير الترددات الخاصة بتتبع مرتكبي الجرائم الإلكترونيّة. - توفير أشخاص متخصصين يحملون مؤهلات علميّة في مجال الذكاء الاصطناعي. - تكثيف الدورات وورشات العمل.
مقابلة رقم (39)	من خلال: - توفير كوادر مناسبة لهذا المجال. - ضرورة العمل على توفير إتفاقيات مع شركات التواصل الإجتماعي. - نشر التوعية والتثقيف بين المواطنين. - توفير هذه التخصصات وفتح أقسام لها لتتبع المجرمين الإلكترونين. - إحضار برامج لتتبع المجرمين الإلكترونين.
مقابلة رقم (40)	من خلال: - جلب متخصصين في مجال الذكاء الاصطناعي لتتبع الجرائم الإلكترونيّة. - العمل على رفع كفاءة العاملين في هذا المجال من خلال تكثيف الدورات وورشات العمل. - زيادة الخبرة والمهارة في مختلف تطبيقات الذكاء الاصطناعي.
مقابلة رقم (41)	من خلال: - استخدام برامج الذكاء الاصطناعي في ملاحقة المجرمين. - توفير التمويل المناسب. - توفير التدريب المناسب للمتخصصين في مجال الذكاء الاصطناعي.
مقابلة رقم (42)	من خلال: - تشجيع الدراسات المتعقلة بالذكاء الاصطناعي. - توفير كواد متخصصة.

	- التنسيق مع جهات الإختصاص.
مقابلة رقم (43)	من خلال: - وضع قوانين ناظمة لهذا الموضوع. - وضع كوادر مدربة في مجال الجريمة الإلكترونيّة والذكاء الاصطناعي. - جلب برامج متعلقة في تتبع المجرمين الالكترونين لتسهل عملية ملاحقتهم.
مقابلة رقم (44)	من خلال: - تطوير برامج الحماية والانتي فايروس ضمن تطبيقات الذكاء الاصطناعي. - استخدام البرامج المرخصة والعالمية، لملاحقة مرتكبي الجرائم الإلكترونيّة. - جلب الكوادر المتخصصة القادرة على التعامل مع هذه البرامج.
مقابلة رقم (45)	من خلال: - تطبيق برامج فلترة الفايروسات. - وضع خطط واضحة للعمل مع تطبيقات الذكاء الاصطناعي. - وضع فريق متخصص في مجال برامج الذكاء الاصطناعي وملاحقة الجناة. - تطوير برامج الذكاء الاصطناعي من قبل فريق متخصص حيث يعمل على استحداثها باستمرار. - تطوير الرقابة الأمنية في هذا المجال.
مقابلة رقم (46)	من خلال: - تعزيز أنظمة الرقابة. - تعزيز الجهات الداعمة لبرامج الذكاء الاصطناعي. - تعزيز ورشات العمل والندوات المتعلقة بملاحقة مرتكبي الجرائم باستخدام برامج الذكاء الاصطناعي. - زيادة عدد الكوادر العاملة في هذا المجال.
مقابلة رقم (47)	من خلال: - توفير كوادر عاملة + متخصصين على علم ودراية من ناحية اجتماعية وامنية ومن ناحية تخصصات امن المعلومات. - الرجوع الى جهة واحدة والتنسيق مع الجهات المختصة والتعاون بينها في حل الجريمة والوصول لها، مثل لجان المراة ووحدة الجرائم الإلكترونيّة ووزارة الاتصالات والشرطة.
مقابلة رقم (48)	من خلال: - العمل على احضار اشخاص ذو خبرة ومتخصصين في هذا المجال. - تشكيل فريق خاص للعمل مع برامج الذكاء الاصطناعي. - شراء أجهزة ومعدات لتتبع المجرمين الالكترونين، فكل منها مكمل للاخر.
مقابلة رقم (49)	من خلال: - تجهيز بنية تحتية. - تجهيز معدات وبرامج خاصة بانظمة الذكاء الاصطناعي وملاحقة مرتكبي الجرائم الإلكترونيّة. - مراقبة الجريمة الإلكترونيّة في كافة انحاء البلاد، البدء بالمناطق التي توجد فيها بؤر تجمع للجرائم الإلكترونيّة. - بالإضافة الى نشر الوعي حول موضوع الذكاء الاصطناعي ومرتكبي الجرائم الإلكترونيّة. - تدريب الجهات المختصة في التعامل معها واعطائهم الصلاحيات للتعامل في هذا الخصوص.
مقابلة رقم (50)	اقترح عدة أمور يجب القيام بها أو تعميمها منها: - يجب وضع سياسات دولية تفرض عقوبات صارمة على مرتكبي جرائم الانترنت اذا يتطلب ذلك تدخل دولي نظرا لخطورة الامر.

	- الاعتماد على أساليب وتقنيات متطورة للتمكن من الكشف عن هوية مرتكب الجريمة الإلكترونيّة والاستدلال عليه بأسرع وقت. - الحرص على سرية المعلومات الخاصة بالعناوين الإلكترونيّة كالحسابات البنكية والبطاقات الائتمانية وغيرها. - تجنب تحميل أي برامج مجهولة المصدر. - تأسيس منظمة خاصة لمكافحة الجرائم الإلكترونيّة مثل (وحدة الجرائم الإلكترونيّة في كل من الشرطة الفلسطينية والنيابة العامة) ولكن يجب تدريبها بأعلى المستويات وتوفير كافة البرامج اللازمة.

ما هي أكثر الجرائم الإلكترونيّة التي تقوم تطبيقات وبرامج الذكاء الإصطناعي بإكتِشافها في الوزارة؟	
مقابلة رقم (1)	- الاختراقات أو محاولات الاختراق خاصة الـ (ATTACH DDOS). - الفايروسات.
مقابلة رقم (2)	- الاختراقات. - التهديدات.
مقابلة رقم (3)	- السوشيال ميديا. - الابتزاز. - اختراق الهواتف الذكيّة. - التهديدات. - الإختراقات.
مقابلة رقم (4)	- الاختراقات. - الفايروسات. - البريد الوارد.
مقابلة رقم (5)	- الاختراقات. - التهديدات.
مقابلة رقم (6)	- التهديدات - الهجمات إلكترونيّة - الإختراقات
مقابلة رقم (7)	- لا يوجد
مقابلة رقم (8)	- الاختراقات. - الهجمات إلكترونيّة.
مقابلة رقم (9)	من خلال نظام الحماية التقليدي هي : - الاختراقات. - التهديدات.
مقابلة رقم (10)	- الاختراقات. - التصدي للهاكرز.
مقابلة رقم (11)	- الاختراقات. - التهديدات.
مقابلة رقم (12)	- الاختراقات. - التهديدات.
مقابلة رقم (13)	- الإختراقات ومحاولات الإختراق.

	- التهديدات.
مقابلة رقم (14)	- الإختراق. - الهجمات إلكترونيّة.
مقابلة رقم (15)	- الإختراق. - التهديد. - الهجمات إلكترونيّة.
مقابلة رقم (16)	- الإختراق.
مقابلة رقم (17)	- لا أعلم.
مقابلة رقم (18)	- تتبع البريد. - الإختراقات.
مقابلة رقم (19)	- الإختراق.
مقابلة رقم (20)	- اختراق الايميلات.
مقابلة رقم (21)	- الإختراقات. - تتبع بريد. - الفايروسات.
مقابلة رقم (22)	- الإختراقات. - التهديدات.
مقابلة رقم (23)	- محاولات الاختراق. - الفايروسات.
مقابلة رقم (24)	- الاختراق.
مقابلة رقم (25)	- الاختراق.
مقابلة رقم (26)	- لا اعلم.
مقابلة رقم (27)	- لا يوجد.
مقابلة رقم (28)	- الإختراقات. - الفايروسات. - البريد الوارد.
مقابلة رقم (29)	- الإختراقات. - الفايروسات.
مقابلة رقم (30)	- لا يوجد.
مقابلة رقم (31)	- الإختراقات. - الفايروسات.
مقابلة رقم (32)	- الاختراقات. - تتبع البريد. - الفايروسات.
مقابلة رقم (33)	- الاختراقات - الفايروسات
مقابلة رقم (34)	- الوصول الى المعلومات الشخصيّة.

	- الإختراقات.
مقابلة رقم (35)	- لا يوجد.
مقابلة رقم (36)	- تتبع الهاكرز. - الاختراقات. - الفايروسات. - تتبع البريد.
مقابلة رقم (37)	- الاختراقات. - الفايروسات.
مقابلة رقم (38)	- لا يوجد.
مقابلة رقم (39)	- الاختراقات.
مقابلة رقم (40)	- الإختراقات. - الفايروسات. - الهجمات الإلكترونيّة.
مقابلة رقم (41)	- لا يوجد.
مقابلة رقم (42)	- لا يوجد.
مقابلة رقم (43)	- الإختراقات.
مقابلة رقم (44)	- الإختراقات. - تتبع البريد. - الفايروسات.
مقابلة رقم (45)	- الإختراقات. - الفايروسات.
مقابلة رقم (46)	- الإختراقات. - تتبع البريد. - الفايروسات.
مقابلة رقم (47)	- جرائم الاختراقات جرائم زراعة الملفات المشبوهة. - جرائم سرقة البيانات.
مقابلة رقم (48)	- الفايروسات. - التهديدات.
مقابلة رقم (49)	- الاختراقات. - التهديدات التي تتعرض لها الشبكات.
مقابلة رقم (50)	- الاختراق. - الفايروسات الإلكترونيّة بأنواعها.

المحور الرئيسي الثالث: ما المُعوقات التي تواجه تطبيق الذكاء الإصطناعي في الحد من ممارسة الجرائم الإلكترونيّة؟ يتفرع عنه

هل هناك مُعوقات تواجِه تَطبيق الذكاء الإصطِناعي في الحد من ممارسة الجريمة الإلكترونيّة في الوزارة؟ **( ) نعم ( ) لا** **إذا كانت الإجابة نعم، رتب/ي هذه المُعوقات حسب الأهمية من وجهة نظرك/ كِ، بحيث يكون الرقم الأصغر هو الأكثر صعوبة؟**	
مقابلة رقم (1)	1 الاحتلال الإسرائيلي. 2 الوضع السياسي. 3 ضعف البنية التحتية. 4 قلة الأبحاث. 5 الميزانية المآليّة. 6 سنوات خبرة العاملين. 7 عدد الكادر العامل. 8 عدم كفاءة الكادر العامل. 9 عدم كفاية قاعدة البيانات. 10 ندرة المبرمجين المتخصصين. 11 عدم توافر قاعدة للبيانات. 12 نطاق عمل المؤسسة. 13 جنس الكادر. مُعوقات أخرى : الاهتمام بموضوع الذكاء الاصطناعي.
مقابلة رقم (2)	1 نطاق عمل المؤسسة. 2 ندرة المبرمجين المتخصصين. 3 الاحتلال الاسرائيلي. 4 ضعف البنية التحتية. 5 قلة الأبحاث. 6 سنوات خبرة العاملين. 7 عدد الكادر العامل. 8 الميزانية المآليّة. 9 الوضع السياسي. 10 عدم كفاءة الكادر العامل. 11 عدم توافر قاعدة للبيانات. 12 عدم كفاية قاعدة البيانات. 13 جنس الكادر.
مقابلة رقم (3)	1 ضعف البنية التحتية. 2 قلة الأبحاث. 3 عدم توافر قاعدة البيانات. 4 عدم كفاية قاعدة البيانات. 5 الميزانية المآليّة. 6 سنوات خبرة العاملين.

	7 الاحتلال الإسرائيلي. 8 عدم كفاءة الكادر العامل. 9 عدد الكادر العامل. 10 ندرة المبرمجين المتخصصين. 11 نطاق عمل المؤسسة. 12 الوضع السياسي. 13 جنس الكادر
مقابلة رقم (4)	1 ضعف البنية التحتية. 2 قلة الأبحاث. 3 الوضع السياسي. 4 الاحتلال الاسرائيلي. 5 سنوات خبرة العاملين. 6 نطاق عمل المؤسسة. 7 عدد الكادر العامل. 8 عدم كفاية قاعدة البيانات. 9 ندرة المبرمجين المتخصصين. 10 الميزانية المآليّة. 11 عدم توافر قاعدة للبيانات. 12عدم كفاءة الكادر العامل. 13 جنس الكادر.
مقابلة رقم (5)	1 قلة الأبحاث. 2 نطاق عمل المؤسسة. 3 عدم توافر قاعدة للبيانات. 4 ضعف البنية التحتية. 5 الوضع السياسي. 6 ندرة المبرمجين المتخصصين. 7 الميزانية المآليّة. 8 جنس الكادر. 9 عدد الكادر العامل. 10 سنوات خبرة العاملين. 11 الاحتلال الإسرائيلي. 12 عدم كفاءة الكادر العامل. 13 عدم كفاية قاعدة البيانات.
مقابلة رقم (6)	1 ندرة المبرمجين المتخصصين. 2 ضعف البنية التحتية. 3 عدم توافر قاعدة للبيانات. 4 عدم كفاية قاعدة البيانات. 5 سنوات خبرة العاملين.

	6 عدد الكادر العامل. 7 قلة الأبحاث. 8 الميزانية المآليّة. 9 الوضع السياسي. 10 عدم كفاءة الكادر العامل. 11 الاحتلال الإسرائيلي. 12 جنس الكادر. 13 نطاق عمل المؤسسة.
مقابلة رقم (7)	1 ضعف البنية التحتية. 2 قلة الأبحاث. 3 الاحتلال الاسرائيلي. 4 الوضع السياسي. 5 سنوات خبرة العاملين. 6 نطاق عمل المؤسسة. 7 عدد الكادر العامل. 8 عدم كفاية قاعدة البيانات. 9 ندرة المبرمجين المتخصصين. 10 الميزانية المآليّة. 11 عدم توافر قاعدة للبيانات. 12 عدم كفاءة الكادر العامل. 13 جنس الكادر.
مقابلة رقم (8)	1 الاحتلال الإسرائيلي. 2 ضعف البنية التحتية. 3 قلة الأبحاث. 4 ندرة المبرمجين المتخصصين. 5 سنوات خبرة العاملين. 6 الوضع السياسي. 7 الميزانية المآليّة. 8 عدم توافر قاعدة للبيانات. 9 عدم كفاية قاعدة البيانات. 10 عدد الكادر العامل. 11 نطاق عمل المؤسسة. 12 عدم كفاءة الكادر العامل. 13 جنس الكادر.
مقابلة رقم (9)	1 الاحتلال الإسرائيلي. 2 الوضع السياسي. 3 الميزانية المآليّة. 4 سنوات خبرة العاملين.

	5 عدد الكادر العامل. 6 ضعف البنية التحتية. 7 جنس الكادر. 8 عدم كفاءة الكادر العامل 9 ندرة المبرمجين المتخصصين. 10 قلة الأبحاث. 11 عدم توافر قاعدة البيانات. 12 عدم كفاية قاعدة البيانات. 13 نطاق عمل المؤسسة (ليست صعوبة)
مقابلة رقم (10)	1 الاحتلال الإسرائيلي. 2 الميزانية المآليّة. 3 عدد الكادر العامل 4 الوضع السياسي. 5 ضعف البنية التحتية. 6 عدم كفاية قاعدة البيانات. 7 عدم توافر قاعدة للبيانات. 8 نطاق عمل المؤسسة. 9 عدم كفاءة الكادر العامل. 10 قلة الأبحاث. 11 سنوات خبرة العاملين. 12 ندرة المبرمجين المتخصصين. 13 جنس الكادر.
مقابلة رقم (11)	1 ضعف البنية التحتية. 2 سنوات خبرة العاملين. 3 الميزانية المآليّة. 4 قلة الأبحاث. 5 عدم كفاية قاعدة البيانات. 6 الاحتلال الإسرائيلي. 7 عدد الكادر العامل. 8 عدم كفاءة الكادر العامل. 9 ندرة المبرمجين المتخصصين. 10 عدم توافر قاعدة البيانات. 11 الوضع السياسي. 12 نطاق عمل المؤسسة. 13 جنس الكادر.
مقابلة رقم (12)	1 الميزانية المآليّة. 2 ضعف البنية التحتية. 3 سنوات خبرة العاملين.

	4 عدد الكادر العامل. 5 قلة الأبحاث. 6 ندرة المبرمجين المتخصصين. 7 نطاق عمل المؤسسة. 8 عدم توافر قاعدة للبيانات. 9 عدم كفاية قاعدة للبيانات. 10 الوضع السياسي. 11 الاحتلال الإسرائيلي. 12 عدم كفاءة الكادر العامل. 13 جنس الكادر.
مقابلة رقم (13)	1 ضعف البنية التحتية. 2 عدم توافر قاعدة للبيانات. 3 عدم كفاية قاعدة البيانات. 4 الميزانية المآليّة. 5 الوضع السياسي. 6 قلة الأبحاث. 7 عدم كفاءة الكادر العامل. 8 ندرة المبرمجين المتخصصين. 9 سنوات خبرة العاملين. 10 نطاق عمل المؤسسة. 11 الاحتلال الإسرائيلي. 12 عدد الكادر العامل. 13 جنس الكادر.
مقابلة رقم (14)	1 ضعف البنية التحتية. 2 الميزانية المآليّة. 3 ندرة المبرمجين المتخصصين. 4 عدد الكادر العامل. 5 سنوات خبرة العاملين. 6 الاحتلال الإسرائيلي. 7 الوضع السياسي. 8 عدم توافر قاعدة للبيانات. 9 عدم كفاية قاعدة البيانات. 10 عدم كفاءة الكادر العامل. 11 نطاق عمل المؤسسة. 12 قلة الأبحاث. 13 جنس الكادر.
مقابلة رقم (15)	1 قلة الأبحاث. 2 ضعف البنية التحتية.

	3 عدم توافر قاعدة للبيانات. 4 ندرة المبرمجين المتخصصين. 5 عدم كفاية قاعدة البيانات. 6 الميزانية المآليّة. 7 عدم كفاءة الكادرة العامل. 8 سنوات خبرة العاملين. 9 عدد الكادر العامل. 10 الاحتلال الإسرائيلي. 11 الوضع السياسي. 12 نطاق عمل المؤسسة. 13 جنس الكادر. ملاحظات أخرى: البيئة التشريعية.
مقابلة رقم (16)	1 الاحتلال الإسرائيلي. 2 الوضع السياسي. 3 الميزانية المآليّة. 4 عدم كفاية قاعدة البيانات. 5 عدم توافر قاعدة للبيانات. 6 عدم كفاءة الكادر العامل. 7 نطاق عمل المؤسسة. 8 ضعف البنية التحتية. 9 ندرة المبرمجين المتخصصين. 10 قلة الأبحاث. 11 سنوات خبرة العاملين. 12 عدد الكادر العامل. 13 جنس الكادر.
مقابلة رقم (17)	1 ضعف البنية التحتية. 2 الوضع السياسي. 3 الاحتلال الإسرائيلي. 4 قلة الأبحاث. 5 نطاق عمل المؤسسة. 6 عدم توافر قاعدة للبيانات. 7 عدد الكادر العامل. 8 عدم كفاية قاعدة البيانات. 9 عدم كفاءة الكادر العامل. 10 الميزانية المآليّة. 11 سنوات خبرة العاملين. 12 ندرة المبرمجين المتخصصين. 13 جنس الكادر.

مقابلة رقم (18)	1 الاحتلال الإسرائيلي. 2 ضعف البنية التحتية. 3 الوضع السياسي. 4 عدم توافر قاعدة للبيانات. 5 الميزانية المآليّة. 6 عدم كفاية قاعدة البيانات. 7 عدم كفاءة الكادر العامل. 8 نطاق عمل المؤسسة. 9 سنوات خبرة العاملين. 10 قلة الأبحاث. 11 ندرة المبرمجين المتخصصين. 12 عدد الكادر العامل. 13 جنس الكادر.
مقابلة رقم (19)	1 ضعف البنية التحتية. 2 قلة الأبحاث. 3 ندرة المبرمجين المتخصصين. 4 الميزانية المآليّة. 5 سنوات خبرة العاملين. 6 عدد الكادر العامل. 7 عدم كفاية قاعدة البيانات. 8 عدم توافر قاعدة للبيانات. 9 نطاق عمل المؤسسة. 10 جنس الكادر. 11 عدم كفاءة الكادر العامل. 12 الوضع السياسي. 13 الاحتلال الإسرائيلي.
مقابلة رقم (20)	1 ندرة المبرمجين المتخصصين. 2 ضعف البنية التحتية. 3 عدم كفاءة الكادر العامل. 4 سنوات خبرة العاملين. 5 عدم كفاية قاعدة البيانات. 6 عدم توافر قاعدة البيانات. 7 قلة الأبحاث. 8 عدد الكادر العامل. 9 الاحتلال الإسرائيلي. 10 الوضع السياسي. 11 الميزانية المآليّة. 12 نطاق عمل المؤسسة.

	13 جنس الكادر.
مقابلة رقم (21)	1 الاحتلال الإسرائيلي. 2 الوضع السياسي. 3 الميزانية المآليّة. 4 قلة الأبحاث. 5 سنوات خبرة العاملين. 6 نطاق عمل المؤسسة. 7 ضعف البنية التحتية 8 عدم توافر قاعدة للبيانات. 9 عدد الكادر العامل. 10 عدم كفاءة الكادر العامل. 11 عدم كفاية قاعدة البيانات. 12 ندرة المبرمجين المتخصصين. 13 جنس الكادر.
مقابلة رقم (22)	1 الاحتلال الإسرائيلي. 2 الوضع السياسي. 3 عدم كفاية قاعدة البيانات. 4 عدم توافر قاعدة للبيانات. 5 نطاق عمل المؤسسة. 6 ضعف البنية التحتية. 7 قلة الأبحاث. 8 سنوات خبرة العاملين. 9 عدد الكادر العامل. 10 جنس الكادر. 11 الميزانية المآليّة. 12 عدم كفاءة الكادر العامل. 13 ندرة المبرمجين المتخصصين.
مقابلة رقم (23)	1 الاحتلال الإسرائيلي. 2 ضعف البنية التحتية. 3 الميزانية المآليّة. 4 الوضع السياسي. 5 جنس الكادر. 6 سنوات خبرة العاملين. 7 عدد الكادر العامل. 8 عدم توافر قاعدة للبيانات. 9 عدم كفاءة الكادر العامل. 10 عدم كفاية قاعدة البيانات. 11 ندرة المبرمجين المتخصصين.

	12 نطاق عمل المؤسسة. 13 قلة الأبحاث.
مقابلة رقم (24)	1 الاحتلال الإسرائيلي. 2 ضعف البنية التحتية. 3 الميزانية المآليّة. 4 الوضع السياسي. 5 عدم كفاية قاعدة البيانات. 6 عدم توافر قاعدة للبيانات. 7 نطاق عمل المؤسسة. 8 عدد الكادر العامل. 9 سنوات خبرة العاملين. 10 قلة الأبحاث. 11عدم كفاءة الكادر العامل. 12 ندرة المبرمجين المتخصصين. 13 جنس الكادر.
مقابلة رقم (25)	1 الميزانية المآليّة. 2 عدم كفاءة الكادر العامل. 3 الاحتلال الإسرائيلي. 4 عدد الكادر العامل. 5 عدم كفاية قاعدة البيانات. 6 عدم توافر قاعدة للبيانات. 7 قلة الأبحاث. 8 ندرة المبرمجين المتخصصين. 9 سنوات خبرة العاملين. 10 ضعف البنية التحتية . 11 نطاق عمل المؤسسة. 12 الوضع السياسي. 13 جنس الكادر.
مقابلة رقم (26)	1 الاحتلال الإسرائيلي. 2 الوضع السياسي. 3 الميزانية المآليّة. 4 ضعف البنية التحتية. 5 عدم كفاية قاعدة البيانات. 6 عدم توافر قاعدة للبيانات. 7 سنوات خبرة العاملين. 8 ندرة المبرمجين المتخصصين. 9 عدم كفاءة الكادر العامل. 10 عدد الكادر العامل.

	11 قلة الأبحاث. 12 جنس الكادر. 13 نطاق عمل المؤسسة.
مقابلة رقم (27)	1 الاحتلال الإسرائيلي. 2 الوضع السياسي. 3 الميزانية المآليّة. 4 ضعف البنية التحتية. 5 عدم كفاية قاعدة البيانات. 6 عدم توافر قاعدة للبيانات. 7 عدد الكادر العامل. 8 سنوات خبرة العاملين. 9 عدم كفاءة الكادر العامل. 10 نطاق عمل المؤسسة. 11 ندرة المبرمجين المتخصص. 12 قلة الابحاث. 13 جنس الكادر.
مقابلة رقم (28)	1 الاحتلال الإسرائيلي. 2 الوضع السياسي. 3 قلة الأبحاث. 4 الميزانية المآليّة. 5 عدم توافر قاعدة للبيانات. 6 ندرة المبرمجين المتخصصين. 7 ضعف البنية التحتية. 8 سنوات خبرة العاملين. 9 نطاق عمل المؤسسة. 10 عدم كفاءة الكادر العامل. 11 عدد الكادر العامل. 12 عدم كفاية قاعدة البيانات. 13 جنس الكادر.
مقابلة رقم (29)	1 الاحتلال الإسرائيلي. 2 الوضع السياسي. 3 الميزانية المآليّة. 4 ضعف البنية التحتية. 5 عدد الكادر العامل. 6 عدم توافر قاعدة للبيانات. 7 عدم كفاية قاعدة البيانات. 8 سنوات خبرة العاملين. 9 عدم كفاءة الكادر العامل.

	10 نطاق عمل المؤسسة. 11 ندرة المبرمجين المتخصص. 12 قلة الابحاث. 13 جنس الكادر
مقابلة رقم (30)	1 الميزانية المآليّة. 2 ندرة المبرمجين المتخصصين. 3 عدد الكادر العامل. 4 الاحتلال الإسرائيلي. 5 قلة الأبحاث. 6 ضعف البنية التحتية. 7 سنوات خبرة العاملين. 8 عدم كفاءة الكادرة العامل. 9 عدم كفاية قاعدة البيانات. 10 الوضع السياسي. 11 عدم توافر قاعدة للبيانات. 12 نطاق عمل المؤسسة. 13 جنس الكادر.
مقابلة رقم (31)	1 الاحتلال الإسرائيلي. 2 الوضع السياسي. 3 الميزانية المآليّة. 4 قلة الأبحاث. 5 سنوات خبرة العاملين. 6 نطاق عمل المؤسسة. 7 ضعف البنية التحتية. 8 عدم توافر قاعدة للبيانات. 9 عدد الكادر العامل. 10 عدم كفاءة الكادر العامل. 11 عدم كفاية قاعدة البيانات. 12 ندرة المبرمجين المتخصصين. 13 جنس الكادر.
مقابلة رقم (32)	1 الاحتلال الإسرائيلي. 2 الوضع السياسي. 3 ضعف البنية التحتية. 4 الميزانية المآليّة. 5 ندرة المبرمجين المتخصصين. 6 عدم كفاية قاعدة البيانات. 7 عدم توافر قاعدة بيانات. 8 نطاق عمل المؤسسة.

	9 عدد الكادر العامل. 10 قلة الأبحاث. 11 سنوات خبرة العاملين. 12 جنس الكادر. 13عدم كفاءة الكادر العامل.
مقابلة رقم (33)	1 الاحتلال الإسرائيلي. 2 الوضع السياسي. 3 الميزانية المآليّة. 4 عدم توافر قاعدة للبيانات. 5 عدم كفاية قواعد البيانات. 6 ضعف البنية التحتية. 7 ندرة المبرمجين المتخصصين. 8 قلة الأبحاث. 9 سنوات خبرة العاملين. 10عدد الكادرة العامل. 11عدم كفاية الكادر العامل. 12 نطاق عمل المؤسسة. 13 جنس الكادر.
مقابلة رقم (34)	1 الاحتلال الإسرائيلي. 2 ضعف البنية التحتية. 3 الوضع السياسي. 4 قلة الأبحاث. 5 الميزانية المآليّة. 6 سنوات خبرة العاملين. 7 عدم كفاءة الكادر العامل. 8 ندرة المبرمجين المتخصصين. 9 عدم كفاية قاعدة البيانات. 10 عدم توافر قاعدة للبيانات. 11 عدد الكادر العامل. 12 نطاق عمل المؤسسة. 13 جنس الكادر.
مقابلة رقم (35)	1 ندرة المبرمجين المتخصصين. 2 عدد الكادر العامل. 3 الميزانية المآليّة. 4 عدم كفاءة الكادر العامل. 5 سنوات خبرة العاملين. 6 نطاق عمل المؤسسة. 7 الاحتلال الإسرائيلي.

	8 الوضع السياسي. 9 قلة الأبحاث. 10 ضعف البنية التحتية. 11 عدم توافر قاعدة للبيانات. 12 عدم كفاية قاعدة البيانات. 13 جنس الكادر.
مقابلة رقم (36)	1 قلة الأبحاث. 2 ضعف البنية التحتية. 3 نطاق عمل المؤسسة. 4 ندرة المبرمجين المتخصصين. 5 عدم توافر قاعدة للبيانات. 6 الاحتلال الإسرائيلي. 7 الميزانية المآليّة. 8 سنوات خبرة العاملين. 9 عدم كفاءة الكادر العامل. 10 عدم كفاية قاعدة البيانات. 11 الوضع السياسي. 12 عدد الكادر العامل. 13 جنس الكادر. مُعوقات أخرى: عدم وجود اليات لطريقة تطبيق الذكاء الاصطناعي.
مقابلة رقم (37)	1 الاحتلال الإسرائيلي. 2 الوضع السياسي. 3 ضعف البنية التحتية. 4 عدم كفاية قاعدة البيانات. 5 الميزانية المآليّة. 6 عدد الكادر العامل. 7 ندرة المبرمجين المتخصصين. 8 عدم توافر قاعدة للبيانات. 9 سنوات خبرة العاملين. 10 عدم كفاءة الكادر العامل. 11 قلة الأبحاث. 12 نطاق عمل المؤسسة. 13 جنس الكادر.
مقابلة رقم (38)	1 قلة الأبحاث. 2 ندرة المبرمجين المتخصصين. 3 عدم كفاءة الكادر العامل. 4 نطاق عمل المؤسسة. 5 سنوات خبرة العاملين.

	6 ضعف البنية التحتية. 7 عدم كفاية قاعدة البيانات. 8 عدم توافر قاعدة للبيانات. 9 عدد الكادر العامل. 10 الوضع السياسي. 11 الاحتلال الإسرائيلي. 12 جنس الكادر. 13 الميزانية المآليّة.
مقابلة رقم (39)	1 الميزانية المآليّة. 2 ندرة المبرمجين المتخصصين. 3 قلة الأبحاث. 4 ضعف البنية التحتية. 5 الاحتلال الإسرائيلي. 6 الوضع السياسي. 7 عدد الكادر العامل. 8 سنوات خبرة العاملين. 9 عدم كفاءة الكادر العامل. 10 نطاق عمل المؤسسة. 11 عدم توافر قاعدة للبيانات. 12عدم كفاية قاعدة البيانات. 13 جنس الكادر.
مقابلة رقم (40)	1 الاحتلال الإسرائيلي. 2 ضعف البنية التحتية. 3 الميزانية المآليّة. 4 قلة الأبحاث. 5 نطاق عمل المؤسسة. 6 سنوات خبرة العاملين. 7 ندرة المبرمجين المتخصصين. 8 عدم توافر قاعدة للبيانات. 9 عدم كفاية قاعدة البيانات. 10 عدم كفاءة الكادر العامل. 11 عدد الكادر العامل. 12 الوضع السياسي. 13 جنس الكادر.
مقابلة رقم (41)	1 الميزانية المآليّة. 2 عدم كفاءة الكادر العامل. 3 نطاق عمل المؤسسة. 4 ضعف البنية التحتية.

	5 قلة الأبحاث. 6 سنوات خبرة العاملين. 7 ندرة المبرمجين المتخصصين. 8 عدم توافر قاعدة للبيانات. 9 عدم كفاية قاعدة للبيانات. 10 عدد الكادر العامل. 11 جنس الكادر. 12 الوضع السياسي. 13 الاحتلال الإسرائيلي.
مقابلة رقم (42)	1 الميزانية المآليّة. 2 ضعف البنية التحتية. 3 عدم كفاية قاعدة البيانات. 4 قلة الأبحاث. 5 الاحتلال الإسرائيلي. مُعوقات أخرى : عدم توفر (Dataset) محليّة تُناسب المجتمع الفلسطيني هي اكبر معيق.
مقابلة رقم (43)	1 سنوات خبرة العاملين. 2 ضعف البنية التحتية. 3 عدد الكادر العامل. 4 ندرة المبرمجين المتخصصين. 5 عدم كفاءة الكادر العامل. 6 قلة الأبحاث. 7 عدم كفاية قاعدة البيانات. 8 عدم توافر قاعدة للبيانات. 9 الميزانية المآليّة. 10 نطاق عمل المؤسسة. 11 الوضع السياسي. 12 جنس الكادر. 13 الاحتلال الإسرائيلي.
مقابلة رقم (44)	1 الاحتلال الإسرائيلي. 2 ضعف البنية التحتية. 3 الوضع السياسي. 4 سنوات خبرة العاملين. 5 عدم كفاءة الكادر العامل. 6 ندرة المبرمجين المتخصصين. 7 عدم كفاية قاعدة البيانات. 8 عدم توافر قاعدة للبيانات. 9 نطاق عمل المؤسسة. 10 قلة الأبحاث.

	11 عدد الكادر العامل. 12 الميزانية المآليّة. 13 جنس الكادر.
مقابلة رقم (45)	1 ندرة المبرمجين المتخصصين. 2 عدم كفاية قاعدة البيانات. 3 عدم كفاءة الكادر العامل. 4 الميزانية المآليّة. 5 عدم توافر قاعدة للبيانات. 6 نطاق عمل المؤسسة. 7 قلة الأبحاث. 8 ضعف البنية التحتية. 9 عدد الكادر العامل. 10 سنوات خبرة العاملين. 11 الوضع السياسي. 12 الاحتلال الإسرائيلي. 13 جنس الكادر.
مقابلة رقم (46)	1 ندرة المبرمجين المتخصصين. 2 ضعف البنية التحتية. 3 عدم كفاءة الكادر العامل. 4 الميزانية المآليّة. 5 قلة الأبحاث. 6 عدم توافر قاعدة للبيانات. 7 عدم كفاية قاعدة البيانات. 8 سنوات خبرة العاملين. 9 الوضع السياسي. 10 الاحتلال الإسرائيلي. 11 عدد الكادر العامل. 12 جنس الكادر. 13 نطاق عمل المؤسسة. مُعوقات أخرى: عدم توافر مواد تتعلق بالذكاء الاصطناعي والجريمة الإلكترونيّة.
مقابلة رقم (47)	1 ضعف البنية التحتية . 2 ندرة المبرمجين المتخصصين. 3 عدم كفاية قاعدة البيانات. 4 عدم كفاءة الكادر العامل. 5 الميزانية المآليّة. 6 سنوات خبرة العاملين. 7 عدد الكادر العامل. 8 جنس الكادر.

	9 نطاق عمل المؤسسة. 10 قلة الأبحاث. 11 الوضع السياسي. 12 الاحتلال الإسرائيلي. 13 عدم توافر قاعدة للبيانات.
مقابلة رقم (48)	1 ندرة المبرمجين المتخصصين 2 ضعف البنية التحتية. 3 سنوات خبرة العاملين. 4 الميزانية المآليّة. 5 عدم كفاية قاعدة البيانات. 6 عدد الكادر العامل. 7 الاحتلال الإسرائيلي. 8 الوضع السياسي. 9 قلة الأبحاث. 10 نطاق عمل المؤسسة. 11 عدم كفاءة الكادر العامل. 12عدم توافر قاعدة البيانات. 13 جنس الكادر.
مقابلة رقم (49)	1 قلة الأبحاث. 2 ضعف البنية التحتية. 3 عدم كفاءة الكادر العامل. 4 الميزانية المآليّة. 5 سنوات خبرة العاملين. 6 ندرة المبرمجين المتخصصين. 7 عدم توافر قاعدة البيانات. 8 عدم كفاية قاعدة البيانات. 9 عدد الكادر العامل . 10 الاحتلال الإسرائيلي. 11 الوضع السياسي. 12 نطاق عمل المؤسسة. 13 جنس الكادر.
مقابلة رقم (50)	1 الاحتلال الإسرائيلي. 2 الوضع السياسي. 3 الميزانية الماليّة. 4 عدم كفاية قاعدة البيانات. 5 عدم توافر قاعدة للبيانات. 6 ضعف البنيّة التحتيّة. 7 قلة الأبحاث.

	8 ندرة المبرمجين المتخصصين. 9 سنوات خبرة العاملين. 10 عدد الكادر العامل. 11 عدم كفاءة الكادر العامل. 12 نطاق عمل المؤسسة. 13 جنس الكادر.

ما طرق التغلب على هذه المُعوقات؟	
مقابلة رقم (1)	من خلال: - توفير الدورات اللازمة. - تخصيص كادر مختص في مجال الذكاء الاصطناعي. - العمل على التشبيك والتواصل من اجل التعاون مع المؤسسات الأخرى. - توفير ميزانية مآليّة عآليّة للعمل على تطوير البنية التحتية.
مقابلة رقم (2)	من خلال: - الاهتمام ببرامج الذكاء الاصطناعي بشكل عام. - الاطلاع على تجارب الدول السابقة التي توظف برامج الذكاء الاصطناعي في خدمات الجرائم والتعليم وغيرها. - العمل على جلب واستقطاب المتخصصين في مجال الذكاء الاصطناعي من خلال الجامعات والطلبة المتخصصين في هذا المجال. - تحويل المشاريع الى منتجات شرط ان تكون هذه المشاريع ذات العلاقة ببرامج الذكاء الاصطناعي وتتبع المجرمين. - العمل على تطوير البنية التحتية كي تتحمل التنوع في برامج الذكاء الاصطناعي.
مقابلة رقم (3)	سأذكر بعض الطرق بغض النظر عن معيقات الاحتلال الإسرائيلي. - العمل على توفير مقومات في البنية التحتية. - يجب ان تكون هذه التطبيقات متصلة بالانترنت على مدار الـ (24) ساعة، كل ذلك يحتاج بالتأكيد الى موازنات مآليّة . - من الضروري العمل على الحصول على الموازنات المآليّة لتخصصيها لهذا الجانب. - العمل على تفعيل دورات متخصصة في برامج الذكاء الاصطناعي وليست عامة. - يجب أن يتوفر اشخاص قادرين على التعامل مع الداتا والبيانات والمعرفة بآليّة عمل هذه البرامج.
مقابلة رقم (4)	سأذكر بعض الطرق بغض النظر عن معيقات الاحتلال الإسرائيلي. - العمل على وضع بنية تحتية متنوعة تتمكن من استعياب كافة التنوعات في برامج الذكاء الاصطناعي . - العمل ضمن نطاق مؤسسي. - ضرورة الاطلاع على تجارب الدول السابقة. - ضرورة زيادة الأبحاث في هذا المجال.
مقابلة رقم (5)	سأذكر بعض الطرق بغض النظر عن معيقات الاحتلال الإسرائيلي. - توفير البنية التحتية اللازمة لتطبيق منظومة وبرامج الذكاء الاصطناعي. - توفير قواعد البيانات وحجم الداتا اللازمة لاستيعابها من قبل قواعد البيانات. - توفير الميزانية المآليّة من الضروري العمل على توفير موازنات مخصصة لهذه البرامج والتطبيقات.

	- توفير كادر عامل يمتلك الخبرة في هذا المجال. - العمل على دعم الأبحاث اللازمة في هذا المجال.
مقابلة رقم (6)	- يجب العمل على جلب متخصصين فقط في مجال الذكاء الاصطناعي. - يجب توفير قاعدة بيانات للعمل ضمنها. - العمل على تطوير البنية التحتية حتى تتمكن من استيعاب التنوع في برامج الذكاء الاصطناعي
مقابلة رقم (7)	- العمل على وضع بنية تحتية متنوعة تتمكن من استيعاب كافة التنوعات في برامج الذكاء الاصطناعي . - العمل ضمن نطاق مؤسسي. - ضرورة الاطلاع على تجارب الدول السابقة. - بالإضافة الى ضرورة زيادة الأبحاث في هذا المجال.
مقابلة رقم (8)	- العمل على تطوير البنية التحتية. - إعطاء الدورات للموظفين. - العمل على زيادة عدد المبرمجين المتخصصين في مجال الذكاء الاصطناعي والجريمة الإلكترونيّة. - العمل على تأهيل المؤسسات الشريكة في هذا الخصوص. - التوعية لكافة العاملين والمجتمع بأهمية برامج الذكاء الاصطناعي في هذا المجال.
مقابلة رقم (9)	- العمل على تكثيف تدريب الكادر. - تجربة البرامج باليد وعلى فترات من اجل التأكد من فعآليّة تطبيقات وبرامج الذكاء الاصطناعي. - العمل على التشبيك والتعاون مع مؤسسات أخرى وإدخال شركاء للعمل معا في هذا المجال.
مقابلة رقم (10)	- الحصول على إمكانيات خدمات الانترنت وان تكون واسعة وقوية. - التخلص من قيود الاحتلال. - توفير ميزانية مآليّة عآليّة لبرامج الذكاء الاصطناعي حيث يتم استخدامها في شراء برامج متطورة . - تدريب كوادر متخصصة للعمل عليها.
مقابلة رقم (11)	- العمل على توفير بنية تحتية. - زيادة مهارة العاملين. - العمل على توفير مخصصات مآليّة من اجل صرفها على الدورات لاكتساب الخبرة والمهارات اللازمة. - استقطاب المتخصصين الخبراء في مجال الذكاء الاصطناعي.
مقابلة رقم (12)	- العمل على تطوير البنية التحتية. - الحصول على الدعم المالي من الدول المانحة. - يمكن التغلب على هذه المُعوقات من خلال الحصول على ميزانيات مآليّة ودعم مالي من اجل صرفها على المخصصات المتعلقة ببرامج الذكاء الاصطناعي، فكل منها مكمل للاخر فعند الحصول على موازنات مآليّة يمكن تطوير البنية التحتية وتوفير مبرمجين وشراء برامج وتطبيقات للذكاء الإصطناعي .
مقابلة رقم (13)	- تطوير البنية التحتية، لانها تعتمد على البيانات هذه البيانات اذا لم تتوفر لا يمكن استخدام التعلم الالي والقيام بتتبع الجريمة الإلكترونيّة. - العمل على توفير قاعدة بيانات لانه لا سيطرة لدينا على البيانات في فلسطين.
مقابلة رقم (14)	- من الضروري تطوير البنية التحتية. - الحصول على الدعم المادي من خلال الدول المانحة والشركاء . - توفير كوادر متخصصة. - العمل على فتح تخصصات متعلقة ببرامج الذكاء الاصطناعي.
مقابلة رقم (15)	- العمل على تعزيز الأبحاث.

	- العمل على وضع بيئة تشريعية. - العمل على تطوير البنية التحتية كي تصبح قادرة على استعياب التنوع في برامج الذكاء الاصطناعي. - استقطاب متخصصين في مجال الذكاء الاصطناعي.
مقابلة رقم (16)	- ممكن العمل على توفير موازنات مآليّة لتكون كل منها مكمل للاخر.
مقابلة رقم (17)	- الحصول على موازنات مآليّة. - العمل على تحسين البنية التحتية. - بناء القدرات للطواقم الفنية والمهارات والخبرات. - العمل على ضرورة تعزيز الأبحاث المتعلقة ببرامج الذكاء الاصطناعي وتتبع الجرائم الإلكترونيّة.
مقابلة رقم (18)	- العمل على تعزيز الدورات. - العمل على زيادة التوعية ببرامج الذكاء الاصطناعي. - التوعية بالجرائم الإلكترونيّة وبرامج الذكاء الاصطناعي على مواقع التواصل الاجتماعي. - التشبيك مع المؤسسات الأخرى في هذا المجال. - العمل على تخصيص موازنات مآليّة خاصة ببرامج الذكاء الاصطناعي.
مقابلة رقم (19)	- تحسين البنية التحتية في الوزارة. - دعم الأبحاث والدراسات في هذا المجال فهي تشكل أهمية كبيرة. - توفير دعم وموازنات مآليّة لصرفها على البحوث العلمية وشراء بنية تحتية.
مقابلة رقم (20)	- العمل على تعزيز التخصصات ذات العلاقة ببرامج الذكاء الاصطناعي. - زيادة تأهيل الكوادر العاملة عن طريق تدريبها وزيادة الخبرة والمهارة لديها في هذا الخصوص. - جلب المتخصصين في مجال برامج الذكاء الاصطناعي.
مقابلة رقم (21)	- توفير طرق تمويل والحصول على تمويل خارج، كون التمويل مكمل لباقي المُعوقات اذ انه عندما تتوافر الموازنات المآليّة تتوافرالابحاث والدراسات.
مقابلة رقم (22)	- العمل على توفير بنية تحتية من اجل تنوع البرامج. - العمل على تكثيف الأبحاث والدراسات المتعلقة بهذا الخصوص ونشر الوعي حول أهمية برامج الذكاء الاصطناعي.
مقابلة رقم (23)	- العمل على ارسال فريق متخصص في برامج الذكاء الاصطناعي لاخذ دورات داخلية وخارجية في مجال برامج الذكاء الاصطناعي والجرائم الإلكترونيّة. - التشبيك مع المؤسسات الأخرى العاملة من اجل تتبع الجرائم الإلكترونيّة. - توفير ميزانية مآليّة عآليّة للعمل على تطوير البنية التحتية.
مقابلة رقم (24)	- العمل على محاولة تطوير البنية التحتية من خلال الموازنات المآليّة. - العمل على تخصيص موازنات والبحث عن الدول المانحة التي تساعد في هذا الخصوص.
مقابلة رقم (25)	- توفير الموازنات المآليّة للبحث العلمي. - توفير دورات متخصصة وحديثة للعاملين في مجال الذكاء الاصطناعي وبرامجه. - توفير كادر متخصص في هذا المجال.
مقابلة رقم (26)	- بعيداً عن الوضع السياسي والاحتلال الإسرائيلي. - ضرورة توفير موازنات مآليّة لتطوير البنية التحتية. - تطوير الكادر من ناحية عملية. - توفير قواعد بيانات والتدريب عليها لتحليل البيانات. - فتح التخصصات ذات العلاقة بسبب وجود ندرة بهذه التخصصات.

مقابلة رقم (27)	- توفير موازنات مآليّة. - زيادة عدد الدورات التخصصية. - زيادة عدد الكوادر المتخصصة في هذا المجال.
مقابلة رقم (28)	- وجود اتفاقيات بين شركات عالمية والوزارة مع شركات التجسس والاختراقات. - وجود صلاحيات اكثر في مجال الجرائم الإلكترونيّة. - تعزيز الدورات المتعلقة ببرامج الذكاء الاصطناعي والجريمة الإلكترونيّة.
مقابلة رقم (29)	- التشبيك مع المؤسسات الأخرى في مجال تتبع الجرائم الإلكترونيّة. - تطوير البنية التحتية. - الحصول على الدعم والموازنات المآليّة من الدول المانحة كون هذه البرامج كلفتها عآليّة.
مقابلة رقم (30)	- وجود توجه في هذا الخصوص من اعلى المستويات. - توفير المخصصات المآليّة اللازمة. - الشراء والتدريب لهذه البرامج.
مقابلة رقم (31)	- التشبيك مع المؤسسات الخارجية والداخلية في مجال الذكاء الاصطناعي والجريمة الإلكترونيّة.
مقابلة رقم (32)	- تخطي حاجز الاحتلال الإسرائيلي الذي يتحكم في كافة البرامج والتكنولوجيا الحديثة ويعيق من عملية التطور. - تخصيص فريق كامل لهذه النظم الذكيّة. - العمل على التشبيك مع المؤسسات ذات العلاقة من اجل مواكبة احدث التطورات أي كي تكون متكاملة. - على الشركات المزودة لخدمة الانترنت أن تشدد الرقابة الأمنية.
مقابلة رقم (33)	سأذكر بعض الطرق بغض النظر عن معيقات الاحتلال الإسرائيلي. - العمل على توفير موازنات مآليّة من الدول المانحة والمؤسسات للقيام بـ (الدورات – شراء البرامج – توفير كوادر بشرية متخصصة – تطوير البنية التحتية). - من الضروري العمل على تطوير البنية التحتية لتتمكن من استيعاب برامج الذكاء الاصطناعي. - ضرورة العمل على تكثيف الدورات وورشات العمل الخاصة ببرامج الذكاء الاصطناعي والجريمة الإلكترونيّة. - توفير الأبحاث العلمية.
مقابلة رقم (34)	- توزيد البنية التحتية بالاساسات اللازمة لتلك البرامج. - العمل على تدريب الكوادر العاملة في الوزارة والمؤسسات. - اعتماد تخصص الجرائم الإلكترونيّة والذكاء الاصطناعي كتخصص جامعي يدرس في الجامعات والمعاهد. - زيادة الوعي بين الناس عن أهمية الكشف عن الجريمة الإلكترونيّة وخطورتها.
مقابلة رقم (35)	- زيادة الخبرة والتخصص في هذا المجال. - العمل على زيادة وتفعيل هذا النوع من التخصصات في الجامعات الفلسطينية. - ضرورة زيادة نسبة الكوادر العاملة في هذا المجال. - كما ان الميزانية المآليّة تلعب دور في هذا الخصوص.
مقابلة رقم (36)	- العمل على استيراد الكفاءات والمبرمجين النادرين. - الحصول على الموازنات المآليّة كونها مكملة لبعضها البعض، فعندما تتوافر الموازنات المآليّة يمكن تخصيص دورات وورشات عمل. - شراء أجهزة ومعدات عالميّة لخاصة ببرامج الذكاء الاصطناعي.
مقابلة رقم (37)	- ضرورة العمل على توفير بنية تحتية تتحمل حجم البيانات. - العمل على توفير موازنات مآليّة لهذه التطبيقات والبرامج. - العمل على تدريب الكواد المتخصصة لرفع الكفاءة والمهارة.

مقابلة رقم (38)	- العمل على الاستثمار في البنية التحتية لتصبح قوية. - وجود كادر متخصص في هذا المجال. - جلب خبرات متخصصة وليست عامة.
مقابلة رقم (39)	- من خلال وضع خطة شاملة لتوضيح آليّة العمل في برامج الذكاء الاصطناعي مع كافة الأطراف.
مقابلة رقم (40)	- جلب الخبراء والمتخصصين في مجال الذكاء الاصطناعي. - ضرورة دعم البحث العلمي. - فتح تخصصات الذكاء الاصطناعي.
مقابلة رقم (41)	- توفير المخصصات المآليّة. - توفير الكادر الفني. - اعتماد سياسة الذكاء الاصطناعي. - توفير بنية تحتية.
مقابلة رقم (42)	بغض النظر عن صعوبة الاحتلال: - ضرورة توفير موازنات مآليّة عآليّة. - توفير بنيّة تحتيّة. - تطوير الأبحاث والدراسات المتعلقة بالذكاء الاصطناعي والجريمة الإلكترونيّة.
مقابلة رقم (43)	- تطوير البينيّة التحتيّة. - تطوير مهارات العاملين حتى تتناسب مع تطور الذكاء الاصطناعي. - جلب الكوادر المتخصصة في مجال الذكاء الاصطناعي والجريمة الإلكترونيّة. - زيادة عدد الكوادر المتخصصة في مجال الذكاء الاصطناعي.
مقابلة رقم (44)	بغض النظر عن إعاقة الاحتلال الإسرائيلي: - من المهم العمل على تطوير البنية التحتية. - استقطاب المتخصصين النادرين في مجال الذكاء الاصطناعي وليست التخصصات العامة. - العمل على رفع كفاءة الكوادر العاملة من خلال تدريبهم واكسابهم الخبرة والمهارة العآليّة للتعامل مع هذه البرامج.
مقابلة رقم (45)	- تطوير استراتيجية عالمية وخاصة من اجل تطبيق برامج الذكاء الاصطناعي. - تحديد الأهداف والاولويات. - تطوير البنية التحتية اللازمة لاستيعاب برامج الذكاء الاصطناعي، فمن خلال البنية التحتية يمكن ادخال تنوع لبرامج الذكاء الاصطناعي.
مقابلة رقم (46)	- العمل على مبادرة وزارة التربية في اعتماد هذا التخصص في المناهج وإقرارها في الجامعات الفلسطينية. - تدريب الكوادر العاملة في مجال الذكاء الاصطناعي. - العمل على تطوير البنية التحتية. - توفير المتخصصين في هذا المجال.
مقابلة رقم (47)	- التوعية بتخصص امن المعلومات. - احضار خبراء وموظفين متخصصين في هذا المجال. - العمل على تحديد دورات تدريبية تساعد في صقل شخصيّة الموظفين في هذا المجال. - تطوير البنية التحتية.
مقابلة رقم (48)	- ضرورة زيادة الخبرة والمهارة في العمل مع هذه التطبيقات. - ضرورة توفير موازنات مآليّة من أجل ارسال المتخصصين في دورات مستمرة، ومن أجل شراء أجهزة ومعدات ذكاء اصطناعي.

مقابلة رقم (49)	- تعزيز البحوث العلمية المتعلقة في موضوع الذكاء الاصطناعي والجريمة الإلكترونيّة. - القيام ببحوث استطلاعية وتحديد التحديات والفرص. - العمل على تطوير البنية التحتية بناءً على الأبحاث. - جلب المتخصصين في هذا المجال.
مقابلة رقم (50)	سأذكر بعض النقاط بدون صعوبة الاحتلال: - توفير ميزانية مناسبة للقيام بالامور المتعلقة بالذكاء الاصطناعي والجريمة الإلكترونيّة. - توفير قواعد بيانات. - توفير كفاءات للعمل على هذه المنظومة. - توفير كافة البرامج اللازمة لعمل هذه المنظومة. - تدريب الكادر على احدث التقنيات بشكل مستمر، ذلك لمواكبة التطور ومعرفة كل جديد.

ما إتجاهات المبحوثين حول العلاقة بين الخصائص الديموغرافيّة (الجنس، مكان السكن، عدد افراد الاسرة، التحصيل العلمي، العمر) وبين ممارسة الجريمة الإلكترونيّة؟	
مقابلة رقم (1)	تؤثر بعض الخصائص الديموغرافيّة على ممارسة الجريمة الإلكترونيّة من خلال: - الجنس: لا علاقة له بارتكابها. - مكان السكن + عدد افراد الاسرة: لها علاقة بارتكاب الجريمة نتيجة عدم توافر سبل الحياة والمعيشة اللازمة مثل المال. - التحصيل العلمي: من الممكن ان يؤدي عدم المعرفة والتعلم الى انصياع المجرم لارتكاب الجريمة الإلكترونيّة. - العمر: الفئات العمرية الصغيرة اكثر ميلا لارتكاب الجريمة الإلكترونيّة من الفئات الكبيرة.
مقابلة رقم (2)	- الجنس: الذكور اكثر ميلا كونهم أجرأ من الاناث، فالاناث ينصعنّ للعادات والتقاليد اكثر من الشباب. - مكان السكن: ممارسة الجريمة الإلكترونيّة في المخيم اكثر من المدينة فالقرية تحكمها العادات والتقاليد أكثر من المدينة. - عدد افراد الاسرة: لا علاقة لذلك بممارسة الجريمة الإلكترونيّة. - التحصيل العلمي: لا علاقة لذلك فهي هواية اكثر من كونها مؤهل علمي وحسب التنشئة الاجتماعية بغض النظر عن كافة المتغيرات. - العمر: الفئات العمرية الكبيرة لا تمارس الجريمة بحكم العائلة والمسؤوليات والاستقرار اما الفئات الأصغر هي اكثر ميلا.
مقابلة رقم (3)	- الجنس: لا علاقة له بممارسة الجريمة الإلكترونيّة . - مكان السكن: له علاقة حيث ان المناطق الخارجة عن اختصاص السلطة والمعروفة بمناطق (C) يكون فيها نسبة ارتكاب الجريمة الإلكترونيّة اكثر، اما فيما يتعلق بالقرى إن ارتكاب الجرائم فيها اقل كون أن القرية خاضعة للعادات والتقاليد، اذا خالف الفرد العادات والتقاليد سيتعرض للنبذ والانتقاد ويتعرض للمشاكل، من جهة أخرى التكنولوجيا تصل الى القرية ابطئ من المدينة، لذا المدينة اكثر انفتاح على التكنولوجيا من القرية. - عدد افراد الاسرة: لا علاقة لذلك في ممارسة الجريمة الإلكترونيّة. - التحصيل العلمي: ان الغير متعلم ليس كالمتعلم فالمتعلم عنده وعي اكثر بالتكنولوجيا فمن الممكن ان يميل الى ارتكاب الجرائم الإلكترونيّة . - العمر: ان المراحل العمرية الصغيرة اكثر اندفاع الى ارتكاب الجرائم الإلكترونيّة بدافع الفضول والطيش.
مقابلة رقم (4)	- الجنس: له علاقة بالتأكيد، فالذكور أكثر ميلا الى ارتكاب الجرائم الإلكترونيّة من الإناث. - مكان السكن: لا أرى أن لمكان السكن علاقة بارتكاب الجريمة الإلكترونيّة . - التحصيل العلمي: لا علاقة له على الاطلاق

	- العمر : لا علاقة له. مما سبق نلاحظ ان كافة المتغيرات لا علاقة لها بارتكاب الجريمة الإلكترونيّة سوا متغير الجنس.
مقابلة رقم (5)	- (الجنس + مكان السكن) برأيي أن لها دور كبير أي ان الشباب اكثر ميلا الى ارتكاب الجرائم الإلكترونيّة وطبيعة المجتمع الفلسطيني محكومة بالعادات والتقاليد لذا الفتاة في المجتمع الفلسطيني تتعرض للانتقاد اكثر من الشاب، وفيما يخص مكان السكن المناطق التي يوجد فيها انفتاح اكثر على التكنولوجيا تجعله اكثر عرضه لاكتساب الخبرة والمهارة، فالمدينة بما أن العادات والتقاليد فيها أسهل من القرية هذا يعني ان ارتكاب الجرائم الإلكترونيّة في القرية اصعب بحكم العشائر والعادات. - أما ما تبقى من المتغيرات لا أرى أن لها علاقة في ارتكاب الجريمة الإلكترونيّة.
مقابلة رقم (6)	لا أرى ان لاي من هذه المتغيرات علاقة بارتكاب الجرائم الإلكترونيّة.
مقابلة رقم (7)	- الجنس: له علاقة بالتأكيد فالشباب أكثر ميلا لإرتكاب الجرائم الإلكترونيّة. - عدد افراد الاسرة: لا علاقة. - مكان السكن: لا أرى أن لمكان السكن علاقة بارتكاب الجريمة الإلكترونيّة . - التحصيل العلمي: لا علاقة له على الاطلاق - العمر : لا علاقة له. لا أرى لكافة المتغيرات علاقة بارتكاب الجريمة الإلكترونيّة سوا متغير الجنس.
مقابلة رقم (8)	- الجنس: الذكور يميلون اكثر للعدوانية وارتكاب الجريمة الإلكترونيّة. - مكان السكن: يتأثر من خلال وجود مناطق حصلت على تقنيات تكنولوجية على العكس من المناطق الأخرى التي لا تحتوي على هذه البرامج مثلا الـ (Fir wall) موجود فقط في رام الله ولا يوجد مثله في أي منطقة أخرى. - عدد افراد الاسرة: لا علاقة له بارتكاب الجريمة الإلكترونيّة. - التحصيل العلمي: بالتأكيد هناك علاقة من خلال ان الفرد الذي لديه دراية وعلم يدخل في هذا المجال والذي لا يعلم في هذا المجال لا يقوم بارتكاب الجريمة نتيجة خبرته القليلة. - العمر : ان فئة الشباب ميالين اكثر الى الجرائم الإلكترونيّة من الفئات العمرية الكبيرة حيث ان فترة المراهقة اكثر اقبال لإرتكاب الجرائم.
مقابلة رقم (9)	الجريمة تعتمد على التنشئة الاجتماعية، ومن جانب الجنس الشباب اكثر جرأة وميل لارتكاب الجريمة الإلكترونيّة، أما فيما يخص الطبيعة البشرية فالأشخاص الذين يعانون من امراض نفسية هم اكثر ميلا لارتكاب الجرائم الإلكترونيّة. ولا علاقة لكل من (مكان السكن، التحصيل العلمي، عدد افراد الاسرة، العمر) بارتكاب الجريمة الإلكترونيّة انما التنشئة هي أساس كل شي اذا كانت التربية سليمة فإن الفرد لن يقدم على ارتكاب الجريمة.
مقابلة رقم (10)	فقط مكان السكن له علاقة بارتكاب الجريمة الإلكترونيّة خاصة المناطق التي تفتقر لمقومات الحياة وتعاني من الفقر والبطالة، فهذه الظروف الصعبة تدفع المواطنين لارتكاب الجرائم الإلكترونيّة ، اما ما تبقى فلا علاقة له بارتكاب الجرائم الإلكترونيّة.
مقابلة رقم (11)	- الجنس: الذكور اكثر ميلا للجريمة لكن حسب هدف الشخص من الجريمة. - مكان السكن: تلعب دور من خلال المنطقة فثقافة الشخص تلعب دور في التنشئة الاجتماعية. - عدد افراد الاسرة:لا علاقة لها بارتكاب الجريمة الإلكترونيّة. - التحصيل العلمي: لا علاقة له. - العمر: سن الشباب اكثر ميلا لارتكاب الجرائم الإلكترونيّة.
مقابلة رقم (12)	- الجنس: الذكر اكثر ميلا للجريمة في المجتمع فالشباب اكثر ميلا للمسلكيات الاجرامية في الفضاء الالكتروني لالمامهم اكثر في هذا المجال لان عندهم حب للاختراق والتحدي. - مكان السكن: القرية أقل لأن الانترنت فيها ضعيف بعكس المدينة يكون فيها الإنترنت أقوى وفيها انفتاح اكثر على

	التكنولوجيا من القرية. - عدد افراد الاسرة لا علاقة لذلك. - التحصيل العلمي: بالتأكيد اذا كان الشخص متخصص في هذا المجال يصبح لديه الخبرة والعلم بالثغرات خاصة اذا كانت لديه ميول إجرامية حيث يعمل على استغلالها في ارتكاب الجرائم. - العمر: الفئات العمرية الأقل وعيا اكثلا ميلا لارتكاب الجريمة الإلكترونيّة بدافع الفضول عندما يكبر في العمر تزداد لديه المسؤوليات.
مقابلة رقم (13)	- الجنس: كلاهما بنفس المستوى لا علاقة لذلك بارتكاب الجريمة، هذا يعتمد على الشخص نفسه. - مكان السكن : نسبة الجريمة الإلكترونيّة في المدينة اكثر لانها على انفتاح اكثر اما القرية كونها تخضع ويحكمها العادات والتقاليد يقل فيها نسبة ممارسة الجريمة الإلكترونيّة. - عدد افراد الاسر: لا علاقة لذلك. - التحصيل العلمي: كلما زادت الخبرة والمهارة كلما زاد الاقبال على ارتكاب الجريمة الإلكترونيّة. - العمر: بالتأكيد سن الشباب اكثر ميلا لممارسة الجريمة الإلكترونيّة.
مقابلة رقم (14)	لا أرى ان هناك علاقة بين هذه الخصائص وارتكاب الجريمة الإلكترونيّة فالذي يرغب بارتكاب الجريمة سيرتكبها بغض النظر عن المتغيرات.
مقابلة رقم (15)	- الجنس: الذكر مندفع الى ارتكاب الجريمة الإلكترونيّة اكثر من الاناث. - مكان السكن: المناطق الخارجة عن اختصاص السلطة يتم فيها ارتكاب الجريمة الإلكترونيّة بكل اريحية. - عدد افراد الاسرة: لا علاقة لذلك. - التحصيل العلمي: كلما زاد التحصيل العلمي كلما زادت المعرفة والانخراط في ارتكاب الجريمة الإلكترونيّة. - العمر: فترة الشباب والمراهقة تزداد فيها ممارسة الجرائم.
مقابلة رقم (16)	- الجنس: الذكور ذو ميل اكثر لارتكاب الجرائم الإلكترونيّة. - مكان السكن: له علاقة فالمناطق الخارجة عن اختصاص السلطة تكون بمثابة امان للجاني. - عدد افراد الاسرة: كلما زاد عدد افراد الاسرة كلما ازدادت نسبة ارتكاب الجريمة وضعفت التنشئة الإجتماعية. - التحصيل العلمي: الغير متعلمين اكثر ميلا لارتكاب الجريمة الإلكترونيّة. - العمر: مرحلة الشباب والاعمار الأصغر غالبا اكثر ميلا لارتكاب الجريمة.
مقابلة رقم (17)	- الجنس: مرتبط اكثر بالشباب فهم اكثر اقبال لممارسة الجريمة من الاناث. - مكان السكن: يؤثر فالمخيمات لديها ميل لارتكاب الجريمة الإلكترونيّة، لاعتقادهم انهم غير خاضعين لنطاق السلطة. - عدد افراد الاسرة: لا علاقة لذلك. - التحصيل العلمي: كلما زاد التحصيل العلمي كلما قل ارتكاب الجريمة الإلكترونيّة ونسبة الغير متعلمين يرتكبون جرائم إلكترونيّة أكثر من المتعلمين كونهم منشغلين في الأبحاث والحياة اليومية والعمل. - العمر: الأشخاص المستقرين في الحياة يكونوا اقل ارتكاب للجرائم والفئة العمرية (18–30) يكون لديهم عدم استقرار وميل للجريمة الإلكترونيّة.
مقابلة رقم (18)	- الجنس: الذكور أجرأ في موضوع ممارسة الجرائم الإلكترونيّة والإبتزاز الإلكتروني. - مكان السكن: لا علاقة. - عدد افراد الاسرة: كلما كان عدد افراد الاسرة أكبر كلما قل الاقبال على ارتكاب الجريمة الإلكترونيّة. - التحصيل العلمي: من اجل ارتكاب جريمة يجب ان يكون الفرد ذو خبرة ومهارة بالتكنولوجيا ويجب ان يكون لديه قاعدة معرفة، الشخص الذي يمتلك سنوات خبرة ومهارة ومتخصص كلما زادت سنوات الخبرة لديه كلما كان هناك اقبال اكثر على ارتكاب الجرائم الإلكترونيّة.

	- العمر: لا علاقة.
مقابلة رقم (19)	- الجنس: لا علاقة لذلك من يرغب بارتكاب جريمة يقوم بها بغض النظر عن الجنس. - مكان السكن: المناطق الغير مراقبة امنيا هي مصدر اكبر وذات علاقة في الاقبال على ارتكاب الجرائم الإلكترونيّة. - عدد افراد الاسرة: لا علاقة لذلك من يرغب بارتكاب جريمة يقوم بها بغض النظر. - التحصيل العلمي: بالتأكيد ان كل من يرتكب جريمة إلكترونيّة وهو غير حاصل على مؤهل علمي من المحتمل ان يقوم بها نتيجة جهله وعدم المامه بالتطور التكنولوجي وفي الجانب المقابل من لديه الخبرة والمهارة من الممكن ان يندفع الى ارتكاب الجريمة بدافع الانتقام أو ميول داخلية تدفعه للقيام بذلك. - العمر: كلما زاد العمر كلما قلت نسبة الاقبال على الجريمة الإلكترونيّة نتيجة الوعي والاستقرار وكلما قل العمر كلما زاد الطيش والفضول وعدم النضوج.
مقابلة رقم (20)	- الجنس: الذكور أكثر ميلاً لممارسة الجريمة من الاناث. - مكان السكن: ان للموقع والمنطقة تأثير في تصرفات الشخص، فالانسان وليد البيئة التي ينشا فيها. - عدد افراد الاسرة: لا علاقة لها. - التحصيل العلمي: الانسان كلما زاد مؤهله العلمي وزادت الثقافة لديه كل ما قلت نسبة ممارسة الجريمة لديه. - العمر: من عمر (16–30) يكون الفرد اكثر اندفاعية لارتكاب الجرائم الإلكترونيّة فكلما تقدم الانسان في العمر كلما اصبح ناضج اكثر.
مقابلة رقم (21)	عبارة عن سلوك شخصي بغض النظر عن الجنس او العمر او التحصيل العلمي او عدد افراد الاسرة فهي تعود للتنشئة الاجتماعية.
مقابلة رقم (22)	- عدد افراد الاسرة: كلما زاد عدد افراد الاسرة كلما قل نطاق الاشراف على الأبناء ومستخدمي الانترنت. - لا علاقة لاي من هذه المتغيرات سوى عدد افراد الاسرة خاصة اذا كان الوضع الاقتصادي سيء وكل منهم يعيش على هواه نتيجة التفكك الاسري.
مقابلة رقم (23)	لا علاقة لهذه المتغيرات بارتكاب الجريمة الإلكترونيّة انما هي ذات دافع شخصي.
مقابلة رقم (24)	- الجنس: لا علاقة كلا الطرفين يمارس الجريمة الإلكترونيّة. - مكان السكن: نوعا ما له علاقة على مستوى الدولة خاصة اننا في دولة احتلال ولا يوجد هناك فرص للحياة. - عدد افراد الاسرة: أيضا لا علاقة له بهذا الموضوع. - التحصيل العلمي: الشخص الدارس للبرمجيات يكون اكثر ميلا لارتكاب الجريمة الإلكترونيّة. - العمر: له علاقة حيث ان الشباب في فترة المراهقة اكثر ميلا لارتكاب الجريمة في الفضاء الالكتروني.
مقابلة رقم (25)	- الجنس: الشباب اكثر ميلا لممارسة الجريمة الإلكترونيّة. - مكان السكن: لا علاقة له فالجريمة يمكن ارتكابها في كل مكان. - عدد افراد الاسرة: ممكن لكن بنسبة ضعيفة جدا كلما زاد عدد افراد الاسرة كلما زاد الإهمال من قبل الاهل. - التحصيل العلمي: كلما زاد التحصيل العلمي كلما قلت الجريمة الإلكترونيّة. - العمر: الشباب في فترة المراهقة اكثر اندفاعية من الكبار في السن.
مقابلة رقم (26)	- الجنس: الفتيات يملنّ اكثر الى ارتكاب الجريمة الإلكترونيّة في حال كنّ يمتلكنّ الخبرة والمهارة بسبب ما يتعرضنّ له في المجتمع. - عدد افراد الاسرة: لا اعتقد ان هناك علاقة وثيقة. - مكان السكن: لا علاقة. - التحصيل العلمي: لا يلعب دور. - العمر : اعتقد ان معظم الجرائم الإلكترونيّة ترتكب في عمر صغير بسبب انفتاحهم على التكنولوجيا.

مقابلة رقم (27)	بشكل عام هذه المتغيرات الديمغرافية مرتبطة مع الجريمة بشكل عام. - عدد افراد الاسرة كلما كان عدد افراد الاسرة اكبر والحالة الاجتماعية متردية والدخل منخفض كلما زادت ممارسة الجريمة الإلكترونيّة.
مقابلة رقم (28)	- عدد افراد الاسرة: اذا كان هناك فقر من الطبيعي ان يكون هناك اقبال على ارتكاب الجرائم الإلكترونيّة. - مكان السكن: المدينة يوجد فيها انفتاح اكثر من القرية . - اما ما تبقى لا علاقة له بارتكاب الجريمة الإلكترونيّة.
مقابلة رقم (29)	أرى انها مرتبط بميول الجاني نفسه وليست بالمتغيرات
مقابلة رقم (30)	لا يوجد علاقة لهذه المتغيرات مع ارتكاب الجريمة الإلكترونيّة.
مقابلة رقم (31)	- فقط الجنس والعمر فعندما يكون الشباب في مرحلة المراهقة والطيش يتكون لديهم حب الفضول والتحدي بدافع الاثبات. - اما ما تبقى لا علاقة له بارتكاب الجريمة الإلكترونيّة.
مقابلة رقم (32)	الجريمة حاصلة بغض النظر عن كافة المتغيرات والخصائص المتعلقة بالجاني. الجنس: اعتقد ان الشباب ميالون اكثر الى ارتكاب الجريمة الإلكترونيّة. - مكان السكن: لا اعتقد ان هناك علاقة. - عدد افراد الاسرة: عندما يكون عدد افراد الاسرة كبير فان المشاكل تزيد والرقابة الابوية تقل، بالتالي يكون هناك احتمال لاقبالهم لارتكاب الجرائم الإلكترونيّة في المقابل عندما يكون عدد افراد الاسرة صغير الأمر الذي يتسبب في زيادة الدلال مما يعني ارتكاب الجرائم الإلكترونيّة. - التحصيل العلمي: الأشخاص من الفئة المتعلمة خاصة الأنظمة المتعلقة بالحاسوب يمكن ان يكون لديه قدرة عآليّة على ارتكاب جريمة إلكترونيّة. العمر: المرحلة العمرية الصغيرة اكثر ميلا للجريمة الإلكترونيّة
مقابلة رقم (33)	أرى أن الجنس وعدد افراد الاسرة لا يوجد لها علاقة بارتكاب الجريمة الإلكترونيّة. اما فيما يخص مكان السكن اعتقد ان المناطق الخارجة عن اختصاص السلطة تشكل مصدر امان للجاني مما يعني ارتكاب الجريمة الإلكترونيّة. أما متغير التحصيل العلمي أرى أنه كلما قل التحصيل العلمي كلما زاد إقبال الفرد على ارتكاب الجريمة الإلكترونيّة. العمر ان الفئات العمرية الصغيرة أكثر طيشا من غيرها.
مقابلة رقم (34)	- الجنس وعدد افراد الاسرة : لا علاقة لها. - التحصيل العلمي: يمكن ان يكون سبب أساسي في ارتكاب الجرائم الإلكترونيّة من قبل المتخصصين في عمليات الاختراق والسيطرة على الشبكات. - مكان السكن:تزداد الجرائم الإلكترونيّة بين سكان المدينة اكثر من القرية خاصة على مواقع التواصل الاجتماعي، - العمر : المراهقين اكثر ارتكاب للجريمة الإلكترونيّة من البالغين.
مقابلة رقم (35)	- الجنس: الذكر اكثر ميلا لممارسة الجريمة الإلكترونيّة. - التحصيل العلمي العالي اكثر ميلا لممارسة الجريمة. - مكان السكن وعدد افراد الاسرة لا علاقة لها . - العمر: الفئات العمرية الصغيرة أكثر ميلا للطيش والتحدي.
مقابلة رقم (36)	- لا علاقة لاي منها في ارتكاب الجريمة سوى الوضع الاقتصادي السيء هو من يدفع المجرم لارتكاب الجريمة الإلكترونيّة.
مقابلة رقم (37)	- الجنس: كلا الجنسين اذا سمحت لهم الفرصة بارتكاب جريمة سيقومون بها بغض النظر عن الجنس. - مكان السكن: الأماكن الخارجة عن اختصاص السلطة تكون اكثر الأماكن عرضة لارتكاب الجرائم الإلكترونيّة.

	- عدد افراد الاسرة: لا علاقة لذلك فالذي يرغب بارتكاب جريمة يقوم بها بغض النظر عن عدد أفراد اسرته. - التحصيل العملي: كلما زاد التحصيل العلمي كلما قلت نسبة اقباله على ارتكاب الجريمة الإلكترونيّة، لعلمه انه سوف يتم اكتشافه. - العمر: كلما قل العمر كلما كانت نسبة الاقبال اكبر.
مقابلة رقم (38)	- الجنس: من وجهة نظري الجريمة الإلكترونيّة مرتبطة اكثر في الشباب كونهم اكثر ميلا للجريمة الإلكترونيّة. - مكان السكن: الجرائم تحصل دائما في المدن بحكم الانفتاح وقلة العادات والتقاليد عكس القرية التي تتحكم فيهم العادات والعشائر اكثر من المدينة. - عدد افراد الاسرة: لا علاقة لها. - التحصيل العلمي: كلما كان على فهم ودراية بمجال التكنولوجيا كلما زادت نسبة ارتكابه للجريمة. - العمر: كلما قل العمر كلما كان هناك طيش وتحدي وفضول.
مقابلة رقم (39)	- الجنس: الشباب اكثر ميلا من الفتيات اللواتي لا علاقة لهن بارتكاب الجريمة الإلكترونيّة. - مكان السكن: المدن تتجه للجريمة اكثر نتيجة للانفتاح عكس القرى لا بحكم العادات والتقاليد والرقابة اكثر على الناس كما ان المناطق خارج حدود السلطة الفلسطينية هي وكر لارتكاب الجرائم الإلكترونيّة. - عدد افراد الاسرة: لا علاقة له. - التحصيل العلمي: المتعلم لا يستطيع الاقبال على ارتكاب الجريمة الإلكترونيّة والغير متعلم يذهب لإرتكابها بدون خوف. - العمر: كلما كان العمر اصغر كلما كان عنده طيش أكثر عكس العمر الأكبر الي يزيد معه الإقبال على الجريمة الإلكترونيّة.
مقابلة رقم (40)	لا أرى علاقة، من وجهة نظري المجرم يرتكب جريمته بغض النظر عن هذه المتغيرات او غيرها.
مقابلة رقم (41)	لا يوجد علاقة بين هذه المتغيرات وارتكاب الجريمة الإلكترونيّة.
مقابلة رقم (42)	لا أرى ان لها علاقة بالجريمة الإلكترونيّة فهي ذات علاقة بالجريمة العادية المرتكبة على ارض الواقع بعكس الجريمة الإلكترونيّة.
مقابلة رقم (43)	- الجنس: الشباب اكثر ميلا لارتكاب الجريمة الإلكترونيّة خاصة في قضايا ابتزاز الفتيات على المواقع الإلكترونيّة. - مكان السكن: لا أرى ان هناك علاقة. - عدد افراد الاسرة: لا أرى ان هناك علاقة. - التحصيل العلمي: ممكن اذا كان هناك أناس مختصة في التكنولوجيا وفيما بعد لظروف ما دخل الى عالم الاجرام الالكتروني. - العمر: الفترة التي تسمى بالمراهقة تزيد من إقبال الشباب على ارتكاب الجريمة الإلكترونيّة.
مقابلة رقم (44)	- الجنس: ان طبيعة المجتمع تدفع الشباب ان يكون اكثر جراة من الاناث، لذلك أرى ان الشباب اكثر ميلا للجريمة الإلكترونيّة. - مكان السكن: اختلاف طبيعة السكن تلعب دور في التنشئة الاجتماعية بالتالي اذا كانت التنشئة قوية فهي تحمي من الاندفاع لارتكاب الجريمة الإلكترونيّة. - عدد افراد الاسرة: متعلقة اكثر بالوضع الاقتصادي وحسب الظروف المعيشية التي يتعرض لها. - التحصيل العلمي: لا علاقة. - العمر: الفئة العمرية هي اكبر دور في هذا المجال، فالفئات العمرية الصغيرة هي اكثر ميلا لارتكاب الجريمة الإلكترونيّة.
مقابلة رقم (45)	- الجنس: طبيعة الشباب اجرأ ولديهم حب المغامرة والفضول فهم اكثر ميلا للجريمة الإلكترونيّة. - مكان السكن: لا علاقة له.

	- عدد افراد الاسرة: لا علاقة له. - التحصيل العلمي: التحصيلات العليمة الأعلى هي على ارتباط وثيق بارتكاب الجريمة الإلكترونيّة. - العمر: له علاقة بالتأكيد نسبة الجريمة فقط لدى فئات الشباب حيث أن كبار السن والأطفال لا يلجأون الى ارتكاب الجريمة الإلكترونيّة ولا يستطيعون القيام بها.
مقابلة رقم (46)	- الجنس: حسب نوع الجريمة، فالجريمة الإلكترونيّة يكيل لها الشباب اكثر من الانثى التي لديها نوع من التخوف بحكم المجتمع والعادات والتقاليد. - مكان السكن: له دور من خلال انه في الغالب المدينة لا احد يعرف الاخر معزول عن الترابط الاجتماعي، لذلك يقوم بارتكاب الجريمة فيها اما القرية الترابط الاسري فيها اكبر ولا يمكن ان يقدم على هذا العمل لذلك تصبح عائق امام تطبيقه. - عدد افراد الاسرة: ارتباط غير مباشر لانه يؤثر على المستوى المادي والمعيشي للاسرة، ممكن اذا كان عدد افراد الاسرة كبيرة ان يتسبب في الفقر بالتالي يندفع للجريمة الإلكترونيّة. - التحصيل العلمي:علاقة عكسية وارتكاب الجريمة كلما كان التحصيل العلمي اكبر كلما قل ارتكاب الجريمة الإلكترونيّة. - العمر: البعض يميل لمسلكيات الجرائم الإلكترونيّة في فترة المراهقة.
مقابلة رقم (47)	- علاقة ترابطية حيث بحكم الجنس ومكان السكن هناك العديد من العوامل التي تقدم على ارتكاب الجريمة الإلكترونيّة، مثلا الذكور اكثر اقداما على ارتكاب الجريمة بشكل عام والسكن الريفي يساعد بشكل كبير على الاختفاء ومراقبة الضحية من بعيد. - وكذلك العمر والتحصيل العلمي يساعد في حال معرفة الشخص باليات الاختراق وافتعال الجرائم الإلكترونيّة.
مقابلة رقم (48)	- الجنس: بحكم العادات والتقاليد في المجتمع العربي الشباب اكثر جرأة وانفتاح، بالتالي الشباب اكثر اقبال على ارتكاب الجرائم الإلكترونيّة. - مكان السكن: لا علاقة لذلك بالجريمة الإلكترونيّة. - التحصيل العلمي: كلما زاد التحصيل العلمي كلما زادت نسبة ارتكاب الجريمة الإلكترونيّة. - عدد افراد الاسرة: لا علاقة له نهائيا في ارتكاب الجريمة الإلكترونيّة. - العمر: نعم هناك علاقة فالاعمار الصغيرة لديها حب الفضول والتحدي والطيش بعكس الاعمار الكبيرة التي تميل اكثر الى الاستقرار في الحياة.
مقابلة رقم (49)	- الجنس: لا علاقة للجنس في ارتكاب الجريمة الإلكترونيّة. - مكان السكن: نعم البيئة تعكس حيث أن السكن الذي تربى ونشأ داخله الفرد في ظل عدم وجود القانون من البديهي ان يمارس فيه الجريمة الإلكترونيّة. - عدد افراد الاسرة: نعم بالتأكيد مع العدد الكبير يتم فقدان السيطرة، حيث يؤدي ذلك لممارسة الأفراد للجرائم نتيجة ضعف التنشئة والرقابة الابوية. - التحصيل العلمي: زيادة الثقافة والعلاقات الاجتماعية تقلل من نسبة الانخراط في ارتكاب الجريمة الإلكترونيّة. - العمر: كلما زاد العمر كلما قلت الجرأة في ارتكاب الجريمة الإلكترونيّة وأصبح لديه مسؤوليات والتزامات ولديه رادع اكثر.
مقابلة رقم (50)	- الجنس: لا اعتقد ان للجنس علاقة في ارتكاب الجريمة الإلكترونيّة. - مكان السكن: من الممكن ان يساعد في بعض الأماكن التي لا يوجد فيها أي عقوبات ولا يوجد فيها تتبع للجرائم الإلكترونيّة. - عدد افراد الاسرة: لا اعتقد ان هناك علاقة. - التحصيل العلمي: يساعد بشكل كبير في بعض الأحيان هذه الجرائم خاصة تخصص تكنولوجيا المعلومات لانه

	على اطلاع اكبر بهذه المواضيع. - العمر: ليس له أي علاقة في ارتكاب الجريمة الإلكترونيّة، أتوقع مرحلة الشباب تحصل فيها نسبة الجرائم اكثر بسبب الطيش والتحدي.

هل لديك علم بمؤسسة أو وزارة آخرى محليّة تستخدم تطبيق الذكاء الاصطناعي في الحد من ممارسة الجريمة الإلكترونيّة؟	
مقابلة رقم (1)	نعم، المخابرات، النيابة العامة، الأمن الوقائي وحدة السايبر.
مقابلة رقم (2)	نعم، وزارة الداخلية.
مقابلة رقم (3)	نعم، نيابة الجرائم الإلكترونيّة.
مقابلة رقم (4)	نعم، وزارة الداخلية
مقابلة رقم (5)	نعم، وزارة الداخلية، ونيابة الجرائم الإلكترونيّة.
مقابلة رقم (6)	نعم، وزارة الداخلية.
مقابلة رقم (7)	نعم، وزارة الداخلية.
مقابلة رقم (8)	نعم، وزارة الداخلية.
مقابلة رقم (9)	نعم، الشرطة الفلسطينية، نيابة الجرائم الإلكترونيّة.
مقابلة رقم (10)	نعم، جميع الوزارات تمتلك برامج ذكاء اصطناعي لحماية شبكاتها من الاختراق لكن في مجال تتبع الجرائم الإلكترونيّة ، وزارة الداخلية ونيابة الجرائم الإلكترونيّة.
مقابلة رقم (11)	نعم، وزارة الداخلية.
مقابلة رقم (12)	نعم، المخابرات.
مقابلة رقم (13)	نعم، الأجهزة الأمنية.
مقابلة رقم (14)	نعم، وزارة الداخلية ، نيابة الجرائم الإلكترونيّة.
مقابلة رقم (15)	نعم، الأجهزة الأمنية بشكل عام، الشرطة كان لها عمل مع الاوربيين في هذا المجال.
مقابلة رقم (16)	نعم، وزارة الداخلية.
مقابلة رقم (17)	نعم، وزارة الداخلية.
مقابلة رقم (18)	نعم، الشرطة الفلسطينية، الأجهزة الأمنية بشكل عام، نيابة الجرائم الإلكترونيّة، شركة جوال كذلك الامر.
مقابلة رقم (19)	نعم، وزارة الداخلية.
مقابلة رقم (20)	نعم، نيابة الجرائم الالكتروني، وزارة الداخلية.
مقابلة رقم (21)	الوزارة مرتبطة مع الشرطة والنيابة والمخابرات.
مقابلة رقم (22)	نعم، الشرطة وحدة الجرائم الإلكترونيّة، نيابة الجرائم الإلكترونيّة.
مقابلة رقم (23)	نعم، نيابة الجرائم الإلكترونيّة، الشرطة.
مقابلة رقم (24)	نعم، وزارة الداخلية.
مقابلة رقم (25)	نعم، وحدة الجرائم الإلكترونيّة، ونيابة الجرائم الإلكترونيّة
مقابلة رقم (26)	نعم، الشرطة الفلسطينية.
مقابلة رقم (27)	نعم، وزارة الداخلية.
مقابلة رقم (28)	نعم، المباحث العامة، المخابرات، جوال عند سرقة الكود، الامن الوقائي.
مقابلة رقم (29)	لايوجد.
مقابلة رقم (30)	نعم، وزارة الداخلية.

مقابلة رقم (31)	نعم، وزارة الداخلية.
مقابلة رقم (32)	السايبر، الامن الوقائي، الشرطة، وحدة الجرائم الإلكترونيّة.
مقابلة رقم (33)	نعم، وحدة الجرائم الإلكترونيّة في جهاز الشرطة.
مقابلة رقم (34)	نعم، شركات الامن المعلوماتي مثل (Cystack).
مقابلة رقم (35)	نعم، الشرطة الفلسطينية.
مقابلة رقم (36)	نعم، شركة جوال تقوم بحماية الأنظمة الخاصة بها من المجرمين، الشرطة والامن الوقائي.
مقابلة رقم (37)	نعم، وحدة الجرائم الإلكترونيّة.
مقابلة رقم (38)	لا يوجد.
مقابلة رقم (39)	نعم، وزارة الداخلية، نيابة الجرائم الإلكترونيّة.
مقابلة رقم (40)	نعم، وحدة الجرائم الإلكترونيّة.
مقابلة رقم (41)	لا يوجد معلومة مؤكدة.
مقابلة رقم (42)	على حد علمي فقط الشركات التي تقدم خدمات الكشف عن التسلل (IDS) لدى المؤسسات الكبيرة مثل البنوك.
مقابلة رقم (43)	نعم، وزارة الداخلية.
مقابلة رقم (44)	نعم، وزارة الخارجية، الأجهزة الأمنية.
مقابلة رقم (45)	نعم، وزارة الداخلية.
مقابلة رقم (46)	نعم، وحدة الجرائم الإلكترونيّة من المؤكد انها تستخدم الذكاء الاصطناعي، ونيابة الجرائم الإلكترونيّة.
مقابلة رقم (47)	نعم، من الممكن ان تكون وحدة الجرائم الإلكترونيّة.
مقابلة رقم (48)	نعم، الشرطة الفلسطينية.
مقابلة رقم (49)	نعم، الشرطة الفلسطينية.
مقابلة رقم (50)	نعم، يوجد وحدة خاصة في فلسطين تسمى وحدة الجرائم الإلكترونيّة وهي تابعة للأجهزة الأمنية وتقوم بشكل كبير في الحد من هذه الجرائم على المستوى المحلي.

هل هناك تعاون وتنسيق بين الوزارة والمؤسسات الأخرى المحليّة والدوليّة العاملة في مجال الجرائم الإلكترونيّة؟
( ) نعم ( ) لا
إذا كانت الإجابة نعم، إشرح/ي ما نوع هذا التعاون؟

مقابلة رقم (1)	نعم، تعاون الشرطة والجرائم الإلكترونيّة للعمل على القبض على المجرمين الالكترونين في اسرع وقت ممكن.
مقابلة رقم (2)	نعم، شكلت الوزارة فريق الامن المعلوماتي في مجال حصول أي جريمة إلكترونيّة، كما وانها تسعى الى وضع بنود تتعلق بقوانين الجرائم الإلكترونيّة لتخفيف نسبة انتشارها واطلاع الناس على بنود هذه القوانين.
مقابلة رقم (3)	نعم، من خلال فريق الاستجابة لطوارئ (امن المعلومات) يوجد لديهم تعاون مع المؤسسات الأخرى في حال حصول أي جريمة في الشبكة.
مقابلة رقم (4)	نعم، في حال حصول أي جريمة أو أي اختراق يتم تشكيل فريق متخصص يّسمى فريق الاستجابة للطوارئ للبحث في الموضوع الحاصل.
مقابلة رقم (5)	نعم، يوجد في الوزارة ما يسمى بفريق الاستجابة للطوارئ يتم التنسيق معه في حال حصول أي طارئ من أجل تتبع مسار المجرم والتحقيق في الجريمة.
مقابلة رقم (6)	نعم، من خلال الاتصال والتواصل مع الوزارات الأخرى كي تتم معالجة أي اختراق او تهديدات او مسلكيات غير طبيعية.
مقابلة رقم (7)	نعم، في حال حصول أي جريمة أو أي اختراق يتم تشكيل فريق متخصص يسمى بفريق الاستجابة للطوارئ للبحث في الموضوع الحاصل.
مقابلة رقم (8)	نعم، هناك ما يسمى بفريق الاستجابة للطوارئ وهو فريق تابع لوحدة الامن المعلوماتي يعمل على التدخل السريع في حال

	حصول أي طارئ او تلاعب او تجسس.
مقابلة رقم (9)	نعم، من خلال العمل على التعاون من قبل الوزارة مع وزارة الداخلية والاتصال والتواصل فيما بينها في المتابعة للجرائم، بالإضافة الى وزارات أخرى شريكة.
مقابلة رقم (10)	نعم، فريق الامن المعلوماتي يقوم بالاستجابة السريعة لأي طارئ في حال حصول أي جريمة إلكترونيّة من خلال التعاون مع وزارة الداخلية.
مقابلة رقم (11)	لا يوجد تعاون.
مقابلة رقم (12)	نعم، فريق الاستجابة للطوارئ من خلال تشكيل لجنة تحقيق مع المؤسسات الخارجية لتتبع الجريمة الإلكترونيّة.
مقابلة رقم (13)	نعم، يوجد تعاون مع الأجهزة الأمنية في تتبع الجرائم الإلكترونيّة عند وقوع جريمة إلكترونيّة.
مقابلة رقم (14)	نعم، فريق الاستجابة للطوارئ هو على اتصال وتواصل مع المؤسسات التي تتعرض لاي جرائم واختراقات.
مقابلة رقم (15)	نعم، وحدة امن المعلومات مهمتها التواصل مع المؤسسات الخارجيّة والداخليّة للتنسيق في مجال الجريمة الإلكترونيّة.
مقابلة رقم (16)	نعم، فريق الامن المعلوماتي يقوم بالتواصل مع المؤسسات الداخلية والأجهزة الأمنية.
مقابلة رقم (17)	لا يوجد.
مقابلة رقم (18)	نعم، الشرطة ونيابة الجرائم الإلكترونيّة، فكل منهما مكمل للاخر في تتبع الجرائم الإلكترونيّة والتعاون في الكشف عن الجريمة المرتكبة.
مقابلة رقم (19)	نعم، من خلال الاتصال والتواصل مع المؤسسات الأخرى في حال حصول أي اختراق او جريمة إلكترونيّة.
مقابلة رقم (20)	نعم، من خلال التعاون مع الأجهزة الأخرى، ففي حالة حصول أي جريمة بحاجة الى تتبع وتحقيق يتم تشكيل فريق يقوم بالاتصال والتواصل مع المؤسسات الأخرى.
مقابلة رقم (21)	نعم هناك تعاون مستمر مع الأجهزة الأمنية في تتبع الجرائم والكشف عنها.
مقابلة رقم (22)	نعم، يتم التعاون من قبل الوزارة والشرطة وكافة المؤسسات الشريكة في تتبع أي مسلكيات إجراميّة.
مقابلة رقم (23)	نعم، من خلال التعاون من قبل فريق الامن المعلوماتي مع الشرطة في تتبع المجرمين الالكترونين والكشف عنهم بأسرع وقت ممكن.
مقابلة رقم (24)	نعم فريق الاستجابة للطوارئ هو على تواصل باستمرار مع المؤسسات الخارجيّة والداخليّة في مجال تتبع الجرائم.
مقابلة رقم (25)	نعم، امن المعلومات هي نقطة اتصال على المستوى العالمي وهناك انفتاح على الأجهزة الأمنية في سبيل مواجهة الجريمة الإلكترونيّة.
مقابلة رقم (26)	نعم، الشرطة شريك مع الوزارة في مواجهة الجرائم الإلكترونيّة بالإضافة الى نيابة الجرائم الإلكترونيّة.
مقابلة رقم (27)	نعم، هناك تعاون من خلال تشكيل فريق تقني تابع لوحدة الامن السيبراني يتم من خلاله التعاون مع أي مؤسسة في الكشف وتحليل الاختراقات الأمنية.
مقابلة رقم (28)	نعم، يتم التعاون مع الشرطة ونيابة الجرائم الإلكترونيّة من خلال فريق متخصص يعمل على التحقيق والكشف عن الجريمة الإلكترونيّة.
مقابلة رقم (29)	لا، لا يوجد.
مقابلة رقم (30)	نعم، التعاون بين فريق الامن المعلومات وباقي الوزارات الأخرى من اجل التحقيق في جريمة حصلت.
مقابلة رقم (31)	نعم، التنسيق بين الجهات المختصة في هذا المجال الشرطة، حيث يوجد هناك تعاون وتنسيق فيما بينها لملاحقة مرتكبي الجرائم الإلكترونيّة.
مقابلة رقم (32)	نعم، (الشرطة، نيابة الجرائم الإلكترونيّة، وحدة الجرائم الإلكترونيّة)، من خلال التنسيق مع هذه المؤسسات كونها شريك مع الوزارة لوجود مركز التدخل السريع في الوزارة الذي يعمل على التتبع لاي جريمة.
مقابلة رقم (33)	نعم، قامت الوزارة بتخصيص فريق يسمى بوحدة الاستجابة للطوارئ يقوم بالاتصال والتواصل مع وحدة الجرائم الإلكترونيّة في حال حصول أي انتهاكات او اختراقات ، بالإضافة الى الاستجابة لطوارئ في حال حصول أي جرائم في المؤسسات

	والقطاعات الحكومية.
مقابلة رقم (34)	نعم، يتم الاتفاق بين الوزارة والمؤسسات الأخرى الخاصة بحماية امن المعلومات والشبكات بغرض تزويدها ببرامج خاصة بالذكاء الاصطناعي والعمل على التدريب عليها.
مقابلة رقم (35)	نعم، يتم التعاون من قبل الوزارة والشرطة في التحقيق في الجرائم الإلكترونيّة لملاحقة وتتبع المجرمين.
مقابلة رقم (36)	نعم، يتم التعاون من قبل الوزارة مع الشرطة ونيابة الجرائم الإلكترونيّة والشراكة بين الجميع، ففي حال حصول أي اختراق وتهديدات يقوم فريق الاستجابة للطوارئ بمساعدة هذه المؤسسات.
مقابلة رقم (37)	نعم، يتم هذا التنسيق من خلال الوحدة التي قامت الوزارة بتشكيلها وهي فريق الاستجابة للطوارئ عند حصول أي جريمة إلكترونيّة.
مقابلة رقم (38)	لا يوجد.
مقابلة رقم (39)	نعم، اعلم ان هناك تنسيق بين الامن المعلوماتي والجرائم الإلكترونيّة والحصول على البيانات والمعلومات والمشاكل التقنية ومعالجة المشاكل التي يتعرض لها المجتمع.
مقابلة رقم (40)	نعم يتم التنسيق لزيادة المعلومات والخبرات في هذا المجال، كما انه يتم التنسيق مع الجهات الدوليّة والتي تتعامل مع الامن المعلوماتي.
مقابلة رقم (41)	نعم، حول الإفادة بخصوص التقنيات المستخدمة في المؤسسات المحلية، الايضاح حول العناوين المتعلقة بامن الانترنت، التواصل مع الجهات الدولية والتي تتعامل مع الامن المعلوماتي.
مقابلة رقم (42)	نعم، يتم التعاون بين الجهات الحكومة في تتبع الجرائم مع الوزارة، بالإضافة الى الجهات الدوليّة الرسمية.
مقابلة رقم (43)	نعم، من خلال التنسيق مع الوزارات التي تكون فيها الداتا بيس مشتركة مع الوزارة، وفريق الاستجابة لطوارئ في حال حصول أي جريمة اختراقات وتهديدات.
مقابلة رقم (44)	نعم، عند حدوث أي خلل يتوجه فريق مختص من الوزارة لفحص ما هي الجريمة الإلكترونيّة وكشف المجرم والتحقيق مع الشرطة.
مقابلة رقم (45)	نعم، التعاون بسيط في بعض التشريعات والقوانين فقط.
مقابلة رقم (46)	الوزارة شريك مع النيابة والشرطة خاصة ان وحدة الامن المعلوماتي عمله يتمحور في الجريمة الإلكترونيّة وعند حصول أي اختراقات تشكل فريق ليباشر العمل في هذا الموضوع.
مقابلة رقم (47)	نعم، لكن التعاون قليل وبسيط، التعاون بين الشرطة والوزارة في الجرائم الإلكترونيّة، لكن هناك ضرورة لتعاون مع مختلف الجهات والمؤسسات الأخرى، حيث يجب ان يكون التعاون بين لجان المراة ووحدة الجرائم الإلكترونيّة والشرطة ووزارة الاتصالات.
مقابلة رقم (48)	نعم، من خلال تعاون فريق الاستجابة للطوارئ مع الشرطة في حال حصول أي جريمة واذا تعرضت أي مؤسسة أو قطاع حكومي لأي خلل او اختراق او أي جريمة.
مقابلة رقم (49)	التعاون بين الشرطة ووزارة الاتصالات في حال تم أي اختراق او هجوم يتم التواصل مع فريق في الوزارة من اجل التحقيق وحل الإشكاليّة.
مقابلة رقم (50)	نعم، يوجد في وزارة الاتصالات وتكنولوجيا المعلومات مركز فلسطين للاستجابة لطوارئ الحاسوب حيث يعمل على مساعدة في تتبع الجرائم الإلكترونيّة، أيضا التعاون مع الأجهزة الأمنية الفلسطينة لحل المشاكل المتعلقة بالجرائم الإلكترونيّة.

فهرس الملاحق:

فهرس الجداول:

فهرس المحتويات: