أكاديمية الإمارات
للهوية والجنسية
Emirates Academy
of Identity and Citizenship

الهيئة الاتحادية للهوية
والجنسية والجمارك وأمن المنافذ
FEDERAL AUTHORITY FOR IDENTITY,
CITIZENSHIP, CUSTOMS & PORT SECURITY

مجلة الإمارات للبحث العلمي

(فصلية - علمية – محكمة)

تصدر عن أكاديمية الإمارات للهوية والجنسية
مركز البحث العلمي والابتكار

الإصدار الرابع 2025

أكاديمية الإمارات
للهوية والجنسية
Emirates Academy
of Identity and Citizenship

الهيئة الاتحادية للهوية
والجنسية والجمارك وأمن المنافذ
FEDERAL AUTHORITY FOR IDENTITY,
CITIZENSHIP, CUSTOMS & PORT SECURITY

مجلة الإمارات للبحث العلمي

(فصلية - علمية – محكمة)

تصدر عن أكاديمية الإمارات للهوية والجنسية

مركز البحث العلمي والابتكار

رقم الرخصة : AD-M.L-000031

الإصدار الرابع 2025

كلمة رئيس المجلس الاستشاري لأكاديمية الامارات للهوية والجنسية:

(معرفة تصنع المستقبل)

تواصل الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ مسيرتها الريادية في دعم منظومة البحث العلمي وتطوير الكفاءات الوطنية، تجسيدًا لتوجيهات القيادة الرشيدة الرامية إلى ترسيخ مكانة دولة الإمارات العربية المتحدة مركزًا عالميًا للمعرفة والابتكار، ومجتمعًا يقوم على الاستدامة والتميز المؤسسي

وفي هذا الإطار، يسرنا أن نحتفي بإصدار العدد الرابع من مجلة الإمارات العلمية، التي تمثل إحدى المبادرات النوعية للهيئة في مجال نشر المعرفة المؤسسية، ودعم الابتكار البحثي، وترسيخ ثقافة الاستدامة في العمل الأكاديمي والإداري. وتأتي المجلة استمرارًا للنجاحات التي حققتها الإصدارات السابقة في تقديم أبحاث ودراسات علمية رصينة تواكب التوجهات الاستراتيجية للهيئة، وتخدم أولويات الدولة في مجالات التحول الرقمي، والذكاء الاصطناعي، والأمن الوطني والسيبراني، وجودة الخدمات.

إن مجلة الإمارات العلمية لا تُعد منبرًا للنشر فحسب، بل هي منصة وطنية لتبادل المعارف والخبرات بين الباحثين والمفكرين، ومصدر للإلهام العلمي والفكري، وبيئة محفزة على الإبداع والتميز، تتيح للباحثين المساهمة في تطوير الأداء المؤسسي ودعم اتخاذ القرار المبني على المعرفة. وقد حرصت هيئة التحرير على الالتزام بأعلى معايير الجودة الأكاديمية والنزاهة العلمية

وفي الختام، أتوجه بخالص الشكر والتقدير إلى جميع الباحثين والمراجعين وأعضاء هيئة التحرير على جهودهم المخلصة التي أسهمت في إنجاز هذا الإصدار، سائلين الله تعالى أن يوفقنا جميعًا لخدمة وطننا الغالي، وأن يجعل من هذه المجلة منارة علمية تُسهم في تعزيز مكانة الإمارات الريادية في ميادين البحث والمعرفة.

اللواء/ سهيل سعيد الخييلي

مدير عام الهيئة الاتحادية للهوية

والجنسية والجمارك وأمن المنافذ

رئيس المجلس الأستشاري لأكاديمية الامارات للهوية والجنسية

- سياسة النشر

مجلة الإمارات للبحث العلمي هي مجلة فصلية علمية محكمة متخصصة في مجالات القانون ونظم العدالة الجنائية، والإدارة والإستراتيجية، والعلوم الاجتماعية وعلوم الأمن الوطني والأمن السيبراني والذكاء الاصطناعي. وتهدف المجلة إلى تنمية آفاق علمية جديدة لتبادل المعرفة وعرض التجارب العلمية والعملية الحديثة في المجالات التي تنسجم مع توجهات دولة الإمارات العربية المتحدة ورؤيتها وقيمها وتنسجم كذلك مع أهداف الهيئة الاتحادية للهوية والجنسية، وخدمة المجتمع الإماراتي وتعزيز الأمن والسلامة على المستوى الوطني والإقليمي والدولي. وتستهدف المجلة الأكاديميين، والباحثين ومراكز البحوث المتخصصة، والمؤسسات الحكومية ذات الصلة.

تسمح سياسة النشر في المجلة بنشر البحوث والدراسات التالية:

- البحوث التجريبية والتي تعتمد على واقع تطبيقي عملي.
- تحليل وتقييم للمفاهيم والأساليب النظرية التي يمكن تطبيقها.
- دراسات لحالات تعني بتجارب عملية واستخلاص الدروس المستفادة منها.
- دراسات مقارنات لقضايا معاصرة محلية وإقليمية ودولية.
- تحليل وتقييم لأدبيات البحث للبحوث والدارسات المعاصرة بما يفيد في تطوير وتحديث النظريات والمفاهيم في المجالات المحددة.
- تطوير نماذج وأطر نظرية جديدة تساهم في فهم أفضل للظواهر البحثية مع بيان الدلالات التطبيقية لها.

كذلك تسمح سياسة النشر في المجلة بنشر المقالات القصيرة التي تأخذ صورة ملاحظات علمية على بحوث أو دراسات أو أوراق عمل قدمت في مؤتمرات أو ندوات علمية متخصصة أو عرض تقييمي لكتب أو ملخصات لرسائل علمية (ماجستير / دكتوراه).

طريقة تقديم البحوث والمقالات للنشر

تقبل البحوث والدراسات المقدمة باللغات العربية والإنجليزية فقط وترسل إلى

البريد الإلكتروني RecearchCenter@icp.gov.ae باسم رئيس تحرير مجلة الإمارات للبحث العلمي». ويرفق مع البحث إقرار موقع من المؤلف بأن البحث المقدم للنشر لم يُنشر من قبل وأنه لن يقدم لأي جهة حتى تنتهي إجراءات التحكيم.

الاشتراطات الشكلية للنشر

ينبغي على المؤلف التزام بالشروط الشكلية التالية قبل تقديم البحث:
أن يحتوي البحث على:

- صفحة غلاف تتضمن عنوان البحث، واسم المؤلف، ووظيفته، والمؤسسة التي يعمل فيها، وعنوانه ورقم هاتفه والبريد الإلكتروني باللغتين العربية والإنجليزية.
- ملخص البحث على أن لا يتجاوز 250 كلمة باللغتين العربية والإنجليزية
- مقدمة البحث
- مشكلة الدراسة وتساؤلاتها
- أهمية الدراسة
- أهداف الدراسة
- فرضيات الدراسة (إن وجدت)
- الإطار النظري والدراسات السابقة
- منهجية الدراسة
- مجتمع الدراسة وعينتها
- تحليل البيانات واختبار الفرضيات
- النتائج والتوصيات
- الملاحق (إن وجدت)

قائمة المراجع

1. ألا تتجاوز عدد صفحات البحث 100 صفحة ولا تقل عن 50 صفحة بما في ذلك المراجع والملاحق.
2. مواصفات الطباعة: نوع الخط (Times New Roman) ، حجم الخط 14 ، الهوامش

4 سم في أعلى وأسفل وعلى جانبي الصفحة.

3. الجداول والصور: تأخذ كل الجداول والصور أرقاما متسلسلة تدرج أسفل الجدول/الصورة مع رقم الجدول/الصورة والاسم والمصدر.
4. المراجع في المتن يشار إلى جميع المراجع في متن البحث مع ضرورة الإشارة إلى الاسم الأخير للمؤلف (العائلة) وسنة النشر بين قوسين الكندي، 2025).
5. قائمة المراجع: تدرج قائمة للمراجع في نهاية البحث مرتبة هجائي حسب أسم المؤلف مع ضرورة استكمال كل البيانات الببليوجرافية لكل مصدر.

- تحكيم البحوث والمقالات المقدمة للنشر

يتم تحكيم البحوث والدراسات وفقاً للمعايير الأكاديمية المعروفة وبموجب نماذج للتحكيم والتقييم المعتمدة في الأكاديمية. ومن أهم المعايير المستخدمة في تقييم البحوث والدراسات التحقق من مدى أصالتها والإسهام الذي تقدمه من ناحية علمية وعملية. ويتم التحكيم من أستاذة متخصصين ممن لهم رصيد متميز من الإنتاج والبحث والعلمي. وتخضع البحوث المقدمة للنشر للإجراءات التالية

1. فحص أولي يجريه أعضاء هيئة التحرير.
2. تقييم سري يجريه ثلاثة محكمين للبحوث التي اجتازت الفحص الأولي.
3. تقرير صلاحية البحوث والدراسات المقدمة للنشر بواسطة المحكمين.
4. إرسال تقرير المحكمين للمؤلف يحتوي على نتيجة التحكيم وقرار هيئة التحرير خلال مدة أقصاها 3 أشهر من تاريخ تسليم البحث.
5. في حالة قبول نشر البحث، يتم إخطار المؤلف بالنشر وتاريخه.

حقوق النشر

محتويات الإصدار الرابع:	
دور الذكاء الاصطناعي في تحقيق العدالة الجنائية الدكتور/ محمد الأمين البشرى محجوب	1
دور تقنيات الذكاء الاصطناعي في تحقيق المواجهة الاستباقية لجرائم البيئة السيبرانية (دراسة استقرائية تحليلية) الدكتور/ أحمد عبدالله أحمد الجراح	2
أثر وسائل التواصل الاجتماعي على أداء الموظفين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ من وجهة نظر العاملين الباحثة / سهيلة راشد خميس النقبي	3
تعزيز الوعي بالأمن السيبراني لدى موظفي الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ بشأن التهديدات والهجمات السيبرانية وتأثيرها على الأصول والممتلكات الرقمي المهندس / محمد أحمد سعيد الزعابي	4

الفهرس

بحث بعنوان:

دور الذكاء الاصطناعي في تحقيق العدالة الجنائية

الدكتور/ محمد الأمين البشرى محجوب
أستاذ العدالة الجنائية
أكاديمية الإمارات للهوية والجنسية

ملخص البحث

أصبح موضوع الذكاء الاصطناعي في السنوات القليلة المنصرمة من أهم موضوعات البحث العلمي، وأكثرها حظاً في أجندة المؤتمرات واللقاءات العلمية والاجتماعات الحكومية والقطاع الخاص. ويعزى ذلك للتأثيرات الكبيرة التي فرضتها تقنيات الذكاء الاصطناعي على حياة الناس والأعمال والعمليات اليومية للقطاعين العام والخاص بما في ذلك مجال الجريمة والأمن ونظم العدالة الجنائية. ورغم الانتشار الواسع لاستخدامات الذكاء الاصطناعي، يقتصر هذا البحث على تأثيراته على نظم العدالة الجنائية لارتباط الجريمة الوثيق بالمجتمع ومعاملاته

يقع هذا البحث في اربعة فصول وهي:

- **الفصل الأول:** تمهيد للبحث يتناول موضوع ومشكلة البحث وأهدافه وأهميته، علاوة على تعريف لمصطلحات البحث وعرض للدراسات السابقة الداعمة للبحث.
- **الفصل الثاني:** يتناول استخدامات الذكاء الاصطناعي وتأثيراته على الجريمة والمجرمين وضحايا الجريمة وطرق وأساليب ارتكاب الجرائم.
- **الفصل الثالث:** يعنى باستخدامات الذكاء الاصطناعي وتأثيراته على العدالة الجنائية وعمليات أجهزة نظام العدالة، كالشرطة والأمن والنيابة العامة والمحاكم الجنائية والمؤسسات العقابية والإصلاحية.
- **الفصل الرابع:** يتضمن نتائج البحث وتوصياته المعززة بمقترحات عملية من شأنها أن تدعم الخطط الاستباقية اللازمة لمواجهة تحديات الذكاء الاصطناعي في سياق الجريمة والعدالة الجنائية.

خلص البحث إلى نتائج راشدة أهمها:

1. تعريف الذكاء الاصطناعي بأنه حقل من حقول المعرفة يهدف إلى صناعة آلات قادرة على القيام بمهام مطابقة تماماً للمهام التي تحتاج إلى ذكاء الإنسان).

كما عرف البحث ثلاث تقنيات تتفرع عن الذكاء الاصطناعي وهي تعلم الآلة، التعلم

العميق، الذكاء الاصطناعي المولد

2. أوضح البحث أن النمو المتسارع في استخدامات الذكاء الاصطناعي سوف تصحبه مخاطر وتأثيرات سالبة خاصة في مجالات الأمن، والاقتصاد العالمي، والنزوح الوظيفي مع التركيز على نماذج من التأثيرات السالبة مثل إحلال مكان البشر في الوظائف، والانحياز والتمييز بين الناس. انتهاك الخصوصيات من خلال استخدامات الذكاء الاصطناعي أمنياً ومعضلة الأخلاقيات.

3. كشف البحث تأثيرات الذكاء الاصطناعي على الجريمة ونظم وأجهزة العدالة الجنائية في ثلاثة محاور وهي:

- محور الوقاية من الجريمة والانحراف والمخاطر الأمنية، حيث أكد البحث أن الذكاء الاصطناعي أداة فاعلة في الوقاية من الجريمة والانحراف من خلال التنبؤ بالجريمة والمخاطر الأمنية التي يسببها البشر أو القوى القاهرة. خلص البحث إلى أن تحليل البيانات الكبيرة بواسطة تقنيات الذكاء سوف يساعد على التنبؤ بالمناطق الساخنة جنائياً وأمنياً، التعرف على الأشخاص المحتمل ارتكابهم الجريمة، التعرف على الأشخاص المحتمل تعرضهم للجريمة واتخاذ تدابير استباقية لحمايتهم، مكافحة الفساد والإرهاب الدولي وغسل الأموال والاتجار بالبشر.

- محور اكتشاف الجرائم والتحقيقات الرقمية، حيث يمكن تتبع المجرمين وضبطهم والتحقيق معهم بتقنيات الذكاء الاصطناعي من عدة زوايا، منها تحليل الصور والآثار والأدلة الرقمية، مضاهاة الصور، قراءة السلوكيات ولغة الجسد.

- محور القضاء الجنائي وأجهزة العدالة الجنائية وعملياتها، حيث أصبح من الممكن - بفضل الذكاء الاصطناعي- تحقيق العبء على المحاكم الجنائية في حفظ وتوثيق وتحليل الأدلة وضمان النزاهة واستبعاد التأثيرات البشرية العاطفية عن قرارات المحاكم وأجهزة الشرطة والنيابة.

4. بيّن البحث أهمية التشريعات الداعمة لاستخدامات الذكاء الاصطناعي في العدالة

الجنائية، موفراً نماذج من المعاهدات الدولية والتشريعات الوطنية خاصة في دول المجلس الأوروبي والمملكة المتحدة. مؤكداً ضعف التشريعات الجنائية الحاكمة للذكاء الاصطناعي بشقيها الشكلي والموضوعي في الدول النامية والدول العربية على وجه الخصوص.

5. خلص البحث إلى أن كثافة استخدامات الذكاء الاصطناعي في الحياة وتوفر تقنياته وبرامجها اللينة والصعبة في أسواق العالم المفتوحة يساعد على إساءة استخدام تقنيات الذكاء الاصطناعي. وقد ظهرت مقدمات لاستغلال المجرمين في ارتكاب الجرائم المالية والغش والاحتيال والاختراقات السيبرانية وتضليل العدالة الجنائية بصناعة أدلة جنائية رقمية كاذبة.

6. قدم البحث قائمة بالجرائم المحتمل ارتكابها باستخدام الذكاء الاصطناعي وهي جرائم تقليدية معززة بالذكاء الاصطناعي، والجرائم السيبرانية، والجرائم الجنسية الافتراضية واحتراق المعاملات المصرفية والحسابات البنكية.

- طرح البحث توصيات غير تقليدية، ذات صبغة مستقبلية تمّكن الأجهزة المعنية بمواجهة الجريمة وتحقيق العدالة الجنائية من حسن استخدام الذكاء الاصطناعي والحد من مخاطره، منها:

1. التأهيل العلمي للعاملين في الشرطة والقضاء في مجال الذكاء الاصطناعي، وذلك بإدماج علوم الذكاء الاصطناعي في مناهج كليات القانون ومعاهد وأكاديميات الشرطة والأمن (للباحثين منهاج مصمم كمساق تعليمي جامعي للراغبين في الإدماج).

2. تكليف مراكز البحوث الشرطية والأمنية والقضائية لتبني خطط مستقبلية للبحث العلمي في مجال الذكاء الاصطناعي واستخداماته والمشاركة المكثفة في المؤتمرات العلمية الدولية، وتبادل الخبرات والمشاريع البحثية المشتركة مع الدول المتقدمة، خاصة الولايات المتحدة الأمريكية، والصين واليابان.

3. إنشاء كليات للأمن السيبراني والذكاء الاصطناعي في الجامعات، معززة بمختبرات الذكاء الاصطناعي ومختبرات الأدلة الرقمية (نموذج: كلية الأمن السيبراني والذكاء الاصطناعي- في جامعة طوكيو للهندسة)، وذلك لتأهيل كفاءات عالية من المبرمجين القادرين على توطين صناعات الذكاء الاصطناعي ببرامجه الصعبة واللينة.
4. تأثيرات الذكاء الاصطناعي تأثيرات أفقية تهم كافة عناصر المجتمعات، ولذلك فإن الموصي به تبني مجلس وزراء الداخلية العرب استراتيجية عملية لتوعية المجتمعات العربية بتقنيات الذكاء الاصطناعي وإيجابياته ومخاطره.
5. مقترح لتأهيل وبناء القدرات لأجهزة العدالة الجنائية في الذكاء الاصطناعي العاملة في مواجهة الجريمة.

كلمات مفتاحية:

- ◊ الذكاء الاصطناعي laicfiitrA ecnegilletnI.
- ◊ تعلم الآلة enihcaM gninraeL.
- ◊ التعلم العميق peeD gninraeL.
- ◊ الذكاء المولد evitareneG IA.
- ◊ نظام العدالة الجنائية lanimirC ecitsuj.

الفصل الأول

الإطار العام للبحث

موضوع البحث

أصبح موضوع الذكاء الاصطناعي في السنوات الخمس المنصرمة من أهم موضوعات البحث العلمي، وأكثرها حظاً في أجندة المؤتمرات واللقاءات العلمية والاجتماعات الحكومية والقطاع الخاص. ويعزى ذلك للتأثيرات الكبيرة التي فرضتها تقنيات الذكاء الاصطناعي على حياة الناس والأعمال والعمليات اليومية للقطاعين العام والخاص، بما في ذلك مجال الجريمة والأمن ونظم العدالة الجنائية. يعتبر هذا الموضوع ذا أهمية بالغة بسبب التحديات العديدة والفرص الواسعة التي يمكن أن يوفرها في هذا السياق. الذكاء الاصطناعي يعمل على تطوير الحلول والأدوات التكنولوجية لمكافحة الجريمة وزيادة مستوى الأمن والسلامة العامة بفضل القدرات التحليلية والتنبؤية المتقدمة التي يتمتع بها. بفضل تقنيات الذكاء الاصطناعي يمكن للسلطات المختصة اكتشاف النقاط الضعيفة في نظام الأمن وتعزيزها، وتحليل البيانات الكبيرة لتوفير معلومات قيمة تساهم في القبض على المجرمين ومنع الأعمال الإجرامية، بالإضافة إلى ذلك، يمكن استخدام التقنيات الذكية والذكاء الاصطناعي في توقع الجرائم وتحليل نمط السلوك الإجرامي للحد من الجريمة وتعزيز الأمن العام. يعد استخدام التكنولوجيا والذكاء الاصطناعي في مكافحة الجريمة وتحقيق العدالة الجنائية نقلة نوعية حرجة وحساسة. فهو ليس مجرد أداة تحفيز فحسب، بل يمكن أن يعمل كمساعد حقيقي للسلطات المختصة في مكافحة الجريمة وتحقيق العدالة الاجتماعية وخفض النفقات المالية على أجهزة نظام العدالة الجنائية. كما يمكن للذكاء الاصطناعي أن يلعب دوراً حاسماً في تحليل البيانات الكبيرة والتنبؤ بالأزمات والكوارث الطبيعية وتقديم الحلول الاستباقية. باستخدام الخوارزميات المتقدمة في تحليل الأدلة والبيانات المتعلقة بالجرائم يمكن الكشف عن العلاقات بين عناصر الجريمة وضحايا الجريمة وجمع الأدلة الجنائية وصناعة الأدلة الرقمية.

ومن جهة أخرى تشير الدراسات الحديثة العلمية إلى أن يكون للذكاء الاصطناعي تأثير كبير على زيادة فرص ارتكاب الجرائم في المجال الإلكتروني. حيث يمكن لتطبيقات الذكاء الاصطناعي الابتكارية والمتقدمة أن تساعد بشكل كبير في عمليات التجسس والاختراق الإلكتروني. بالإضافة إلى ذلك، يمكن للجرائم السيبرانية أن تستفيد بشكل كبير من استخدام تقنيات الذكاء الاصطناعي للوصول إلى معلومات حساسة وتنفيذ هجمات إلكترونية متقدمة وفاعلة للغاية. ومع تطور التقنيات الحالية وسرعة التقدم في مجال الذكاء الاصطناعي ووفرة منتجاته في الأسواق المفتوحة لعامة الناس، قد تزداد الجرائم السيبرانية ويصعب اكتشافها، حيث يمكن أن يتم استخدام تقنيات الذكاء الاصطناعي لتضليل الأنظمة الأمنية وتشويه البيانات وتخفيض مستوى توقعات الكشف عن الجرائم المرتكبة. وهذا بالتأكيد يشكل تحدياً كبيراً للمجتمعات والمؤسسات والأفراد الذين يعملون في مواجهة هذه التهديدات المستمرة والمتطورة. لذلك، ينبغي لنا أن نكون في حالة تأهب وأن نعمل على تعزيز قدراتنا في مواجهة الجرائم السيبرانية المعززة بتقنيات الذكاء الاصطناعي. وعلى الصعيد الدولي، ينبغي تطوير التعاون مع المؤسسات والخبراء في مجال الأمن السيبراني من خلال العمل المشترك والتنسيق الدولي الوثيق، لتأمين بيئة الإنترنيت ومكافحة الجرائم السيبرانية التي تستهدف حقوقنا وسلامتنا الرقمية على نطاق واسع ومستدام

هناك نطاق واسع للاستفادة المشروعة من تقنيات الذكاء الاصطناعي وتعلم الآلة، مثل مكافحة الجريمة، والتحقيقات الجنائية[1]، والتحقيقات الرقمية، وصناعة الأدلة الرقمية، وتحليل الجريمة وتحليل إحصاءاتها، بالإضافة إلى التنبؤ بالجريمة وإدارة نظم العدالة الجنائية وفي المقابل يصاحب هذا التطور المتنامي لتطبيقات الذكاء الاصطناعي تحديات مواجهة الجرائم المرتكبة بتقنيات الذكاء الاصطناعي، وغير ذلك من المهددات الأمنية التي تتم بتقنيات الذكاء الاصطناعي. وتمتد التأثيرات السلبية للذكاء الاصطناعي إلى إنشاء الاستخدامات التقليدية والحاسب الآلي والوسائط الذكية

1 -Keith J. Howard and Matthys Maas (2020) Artificial Intelligence and Crime: A primer for Criminologists. Crime Maas, Sage.

للرقمنه، علاوة على احتمالات أضرار الذكاء الاصطناعي على حياة الإنسان من خلال اختراق عملياته وحركة النقل الجوي، وبرامج المركبات ذاتية القيادة Autonomous Vehicles وغيرها من المعاملات الافتراضية النافعة.[2] ومع مراعاة هذه (المساحات الشاسعة التي تشملها تطبيقات الذكاء الاصطناعي يركز موضوع هذا البحث على تأثيرات الذكاء الاصطناعي على الجريمة والعدالة الجنائية، من حيث طرق ارتكابها واتجاهاتها المستقبلية وأساليب مواجهتها وصولاً إلى مرئيات تقلل من فرص استغلال الذكاء الاصطناعي في ارتكاب الجرائم، وتعزز الاستفادة من الذكاء الاصطناعي في مكافحة الجريمة وتحقيق العدالة الجنائية وتطوير عملياتها

مشكلة البحث وتساؤلاته

تشكل الجريمة بصفة عامة ظاهرة اجتماعية تستوجب الدراسة والمعالجة بصفة مستمرة ولعل دخول الذكاء الاصطناعي عالم الجريمة أمرٌ يستحق الوقوف عنده، بحثا في التأثيرات الإيجابية والسالبة لذلك

الذكاء الاصطناعي ناتج من نتائج علوم الحاسب الآلي، أداة هذا العصر. كما أن التمكن من معارف وعلوم الذكاء الاصطناعي يتطلب التمكن من علوم الحاسب الآلي، وتملك مفاصلها من البرامج الصعبة واللينة. فالدول العربية وهي تتسابق نحو تطبيقات الذكاء الاصطناعي في معاملات حرجة تتعلق بأمنها القومي واقتصادها لم تولِ الاهتمام اللازم بنشر ثقافته وتطوير وتعميم دراساته وسن تشريعاته، والتحكم في نطاقات استخدامه وتوطين صناعاته من البرامج الصعبة واللينة. للذكاء الاصطناعي جوانب إيجابية غير محدودة كما أن له جوانب ضارة غير محدودة قد تفوق الإيجابيات. وعندما نتناول تقنيات الذكاء الاصطناعي بالدراسة علينا أن نستصحب معها مجموعة التقنيات الحديثة المتفرعة عن الذكاء الاصطناعي، وهي تعلم الآلة Machine Learning، والتعلم العميق Deep Learning، وتنقيب البيانات Data Mining والذكاء الاصطناعي المولد Generated Artificial Intelligence. في مجال الجريمة على سبيل المثال للذكاء

2- Doo won Jeong (2020) Artificial Intelligence Security threats, Crime, and Forensics: Taxonomy and Open issues.Digital objects identifier 10, 1109. IEEE Access.

الاصطناعي دور إيجابي في مكافحة الجريمة ومنع وقوعها والتنبؤ بها كما له مخاطر على أمن الدولة والجرائم عامة والجرائم المالية على وجه الخصوص في البيئة العالمية للاقتصاد والتجارة المحكومة بتقنيات المعلومات والاتصالات الفضائية. إن المشكلة التي يعالجها هذا البحث، وإن كان قاصرا على الجريمة، فهي مدخل لمشكلات الذكاء الاصطناعي ومتفرعاته في الحياة العامة في ظل غياب المعرفة والتعلم المجتمعي. فالمجتمع العربي في الغالب ما زال يعيش الأميّة المعلوماتية، الأمر الذي يجعله عرضة لجرائم يستخدم فيها الذكاء الاصطناعي. كما أن لمعظم الدول العربية بنيات هشة للمعلومات والاتصالات الإلكترونية، علاوة على افتقارها لصناعات البرامج الحاسوبية اللينة والصعبة، الأمر الذي يضع جل مقدراتها من المعلومات وأسرارها الاقتصادية والاجتماعية والأمنية في أيدي الغير. لا تقتصر مشكلة البحث على معالجة المخاطر المحتملة لاستخدامات الذكاء الاصطناعي فحسب، بل تمتد المشكلة إلى معالجة القدرات المهنية والجاهزية التقنية للاستفادة من فضائل الذكاء الاصطناعي في تفسير ظاهرة الجريمة وتحليلها والتنبؤ بها والتنبؤ بالمتغيرات الأمنية بالتنقيب في البيانات الكبيرة وتحليل المعلومات الاستخباراتية وإدارة نظم العدالة الجنائية

يطرح موضوع البحث تساؤلات عديدة أهمها:

1. ما هو الذكاء الاصطناعي؟
2. ماهي اتجاهات ونطاقات استخدام الذكاء الاصطناعي في الحاضر والمستقبل؟
3. ماهي تأثيرات الذكاء الاصطناعي على الجريمة والأحداث الأمنية؟
4. ماهي متطلبات الجاهزية لمواجهة تحديات الذكاء الاصطناعي؟
5. كيف يمكننا الاستفادة المثلى من تقنيات الذكاء الاصطناعي في الوقاية من الجريمة والأحداث الأمنية وتحقيق العدالة الجنائية؟

أهمية البحث وأهدافه

في الأعوام القليلة الماضية لاحظنا نمو التقنيات المعلوماتية والواعدة وتأثيرها بإحداث تغيير في نظم حياة الإنسان وأعماله ومعاملاته. وتبرز من خلال تلك التقنيات خمس مصطلحات جديدة هي الذكاء الاصطناعي (AI)، الذكاء الاصطناعي المولد (GAI)، تعلم الآلة (ML)، التعلم العميق (DL) وتنقيب البيانات. تستخدم هذه المصطلحات في الغالب كمرادفات، إلا أنها ليست كذلك بل هي متفرعات عن الذكاء الاصطناعي. وتكمن أهمية هذا البحث في

1. يتجه العالم اليوم نحو تسخير الذكاء الاصطناعي في كافة الأعمال والمعاملات العامة والخاصة، الأمر الذي يخلق بيئة تنمو فيها الجرائم السيبرانية المعتمدة على الذكاء الاصطناعي. ولا شك أن التعامل مع تلك الجرائم يقتضي بناء نظام عدالة جنائية قائمة على الذكاء الاصطناعي.
2. الحاجة إلى جسر الهوة المعرفية بين الموارد البشرية العاملة في أجهزة العدالة الجنائية وبين الكفاءات العاملة بتطبيقات الذكاء الاصطناعي
3. الاسهام في مراجعة القوانين الجنائية التقليدية لتغطية تطبيقات الذكاء الاصطناعي
4. مواكبة الأهمية التي تحظى بها تقنيات الذكاء الاصطناعي ونموها وتطورها المتسارع في ظل تباطؤ جهود التعليم التقني الشامل وغياب إستراتيجيات لبناء القدرات والتوعية الأمنية في هذا المجال.
5. التوعية الأمنية وبناء القدرات في تقنيات الذكاء الاصطناعي لا تقتصر على فئات ومهن محددة، بل يجب أن تمتد وتشمل أفراد المجتمع كافة، خاصة وقد أصبحت هذه التقنيات ووسائطها الذكية بين أيدي عامة الناس.
6. تكمن أهمية هذا البحث في كونه مبادرة تطرح مشكلات الذكاء الاصطناعي وتأثيراته على الجريمة والعدالة الجنائية والأزمات الأمنية بصفة عامة، وذلك من

خلال الدعوة إلى نشر ثقافة الذكاء الاصطناعي وتحدياته وابتكار مناهج تعليمية مواكبة لبيئة الذكاء الاصطناعي.

ومن المؤمل أن يسهم هذا البحث في تحقيق الأهداف التالية:

- التعريف العام بالذكاء الاصطناعي
- بيان استخدامات الذكاء الاصطناعي واتجاهاتها المستقبلية.
- التعريف بالتأثيرات الضارة للذكاء الاصطناعي على ارتكاب الجريمة
- بيان استخدامات الذكاء الاصطناعي في عمليات العدالة الجنائية مثل اكتشاف الجرائم، التحقيق الجنائي، المحاكمات الجنائية، الأدلة الرقمية والمؤسسات العقابية.
- بلورة توصيات ومقترحات عملية قابلة للتنفيذ لبناء قدرات عناصر أجهزة نظام العدالة الجنائية في مجال الذكاء الاصطناعي.

منهجية البحث

يلاحظ أن البحوث والدراسات المتوفرة حول الذكاء الاصطناعي، خاصة تلك التي نقوم بمراجعتها في هذا البحث اتبعت منهجاً وصفياً وتحليليا لتقنيات وتطبيقات الذكاء الاصطناعي. كما يلاحظ بوضوح أن البحوث والدراسات التي تنفذ في هذا المجال تتسم بالشراكة وتنوع الخبرات من حيث خبرة الباحثين وجنسياتهم. حيث نجد كثيراً من البحوث أُعدّت بمشاركة بين باحثين من الولايات المتحدة الأمريكية والصين واليابان. في تقديرنا أن هذا الاتجاه المنهجي في دراسات وأبحاث الذكاء الاصطناعي اتجاه مستحدث وسليم، وذلك لأسباب عدة أهمها:

- معرفة أن الذكاء الاصطناعي باب من أبواب المعرفة المفتوحة على حقول علمية متنوعة. وإن كانت معرفة تقنية المعلومات والاتصالات ووسائطها الذكية هي الأساس، إلا أن تطبيقات الذكاء الاصطناعي تستوجب البحث فيها بجوانبها القانونية والاقتصادية والاجتماعية والأمنية.

- تطبيقات الذكاء الاصطناعي ممتدة عبر الفضاء الافتراضي إلى جميع الدول والمجتمعات، الأمر الذي يفرض علينا دراسة آثارها في مختلف دول العالم لتبادل الخبرات ومعالجة مؤشرات القصور أو الخلل في التطبيقات والحد من المخاطر قبل إنشائها.
- يعتبر تحليل التطبيقات العلمية لتقنيات الذكاء الاصطناعي واستنباط إيجابياتها وجوانب قصورها هو المدخل لدرء المخاطر وضمان سلامة تلك التقنيات بالقدر الذي يطمئن الإنسان الذي أصبح اليوم يتوجس خيفة من معطيات الذكاء الاصطناعي.

وبناءً على ما تقدم يُتبع في هذا البحث المنهج الوصفي التحليلي وضمان شراكة بين الخبرات القانونية والإدارية وكفاءات علوم المعلومات والاتصالات الإلكترونية. ويقوم الوصف والتحليل في هذا البحث على مراجعة وتحليل الدراسات السابقة والمؤلفات الحديثة في هذا المجال، والاطلاع على مخرجات المؤتمرات والندوات العلمية الدولية. ولتعزيز مدخلات هذا البحث قام الباحثان بالمشاركة في مؤتمر إستكهولم الدولي الثامن عشر لعلم الإجرام الذي عقد في العاصمة السويدية خلال الفترة من 10-13-يونيو-2024. وقد كان اليوم الثاني للمؤتمر ثرياً بالبحوث والدراسات وأوراق العمل التي ركزت على تقنيات الذكاء الاصطناعي وتأثيراتها على الجريمة وأجهزة نظام العدالة الجنائية. وحاول الباحثون، وهم من كبار علماء علم الإجرام، إيجاد تفسير لظاهرة الجرائم التي يستخدم فيها الذكاء الاصطناعي والجرائم المرتكبة ضد تقنيات الذكاء الاصطناعي من منظور علم الإجرام وعلم ضحايا الجريمة[3] وما زال الباحثون في مجال علم الإجرام يبحثون عن نظريات جديدة تفسر الجرائم ذات العلاقة بتقنيات الذكاء الاصطناعي.

ينقسم هذا البحث إلى:

- **الفصل الأول:** تمهيد للبحث يتناول موضوع ومشكلة البحث وأهدافه وأهميته، علاوة على تعريف لمصطلحات البحث وعرض للدراسات السابقة الداعمة للبحث.

3 - The national council for crime prevention (2024) The Stockholm criminology symposium – Stockholm, bra-publications.

- **الفصل الثاني**: يناقش استخدامات الذكاء الاصطناعي وتأثيراته على الجريمة والمجرمين وضحايا الجريمة وطرق وأساليب ارتكاب الجرائم.
- **الفصل الثالث:** يُعنى باستخدامات الذكاء الاصطناعي وتأثيراته على العدالة الجنائية وعمليات أجهزة نظام العدالة، كالشرطة والأمن والنيابة العامة والمحاكم الجنائية والمؤسسات العقابية والإصلاحية.
- **الفصل الرابع:** خاتمة البحث بالنتائج والتوصيات ومقترح خريطة طريق لبناء قدرات الموارد البشرية العاملة في نظم العدالة الجنائية ومكافحة الجريمة بالقدر الذي يواكب مستقبل استخدامات الذكاء الاصطناعي.

تعريف مصطلحات البحث

لحداثة موضوع الذكاء الاصطناعي يحتوي هذا البحث عدداً من المصطلحات التي قد تكون حديثة للقارئ العادي. وبرغم تناقل ألسنة عامة الناس لعدد من هذه المصطلحات، إلا أنهم لا يقفون عند مفاهيمها السليمة. وقد يكون ضروريا للباحثين في هذا المجال أن يتفقوا حول مقاصد المصطلحات ذات العلاقة بالذكاء والتي تتكاثر وتتجدد بخطوات متسارعة. ومن تلك المصطلحات اللازمة لهذا البحث ما يلي

◊ الذكاء الاصطناعي:

الذكاء الاصطناعي (Artificial Intelligence) ويرمز له في هذا البحث بـ AI، هو حقل دراسي يهدف إلى صناعة آلات قادرة على القيام بمهام مطابقة تماما للمهام التي تحتاج إلى ذكاء الإنسان، مثل التعرف على الأصوات، وصناعة القرار، وفهم اللغات الطبيعية، وصناعة البيانات وتحليلها. ويتفرع عن الذكاء الاصطناعي أفرع منها تعلم الآلة، والتعلم العميق، وتنقيب البيانات والذكاء الاصطناعي المولد[4].

◊ تعلم الآلة:

تعلم الآلة Machine Learning، ويشار إليه في هذا البحث بـ (ML) هو فرع الذكاء

4 Jeremy Thorpe (2024) Crimes of the Future-Using AI – powered tools to identify suspects-Amazon – UK.

الاصطناعي الذي يركز على تطوير اللوغريثمات التي يمكنها التعلم من البيانات وصناعة التنبؤات أو القرارات المبنية على ذلك التعلم، أي ال (ML) هي الطريقة التي تمكّن الآلة من التعلم من التجارب كما يتعلم الإنسان. وتصنف لوغريثمات ال (ML) إلى أنواع هي: التعلم المدهش، والتعلم غير المدهش وتعلم إعادة التطبيق

- **التعلم العميق:**

التعلم العميق (Deep Learning) ويرمز له في هذا البحث بـ (DL) وهو فرع ال (ML) الذي يركز على تطوير الشبكات العصبية الاصطناعية التي يمكنها التعلم من البيانات الهائلة، ويمكن استخدام نماذجها للتعرف على أنماط البيانات، مثل الأيقونات والتعرف على اللغات والطبيعية والروبوتات

- **نظام العدالة الجنائية:**

نظام العدالة الجنائية[5] هو مجموعة عمليات قبل وقوع الجريمة أو أثناء وقوعها أو بعد وقوعها تنظمها أحكام القانون الجنائي، وتضطلع بها أجهزة الشرطة، والنيابة العامة، والقضاء الجنائي والمؤسسات الإصلاحية والعقابية

عرض الدراسات السابقة

على الرغم من حداثة الطفرة في تقنيات الذكاء الاصطناعي وإنشاء تطبيقاتها، حظي الذكاء الاصطناعي باهتمام الباحثين والخبراء المتخصصين في تكنولوجيا المعلومات والاتصالات، الأمر الذي وفر العديد من البحوث والدراسات والمؤلفات والكثير من اللقاءات العلمية والمؤتمرات الدولية التي أثرت المكتبات بالعلوم والمعارف المتجددة حول الذكاء الاصطناعي واستخداماته وتحدياته الأمنية

فيما يلي نقدم عدداً من تلك البحوث والدراسات لعلها تدعم مدخلات هذا البحث ومخرجاته، وهي على النحو التالي:

1. دراسة (فاني رهنستروم)[6] حول مدى قدرة الذكاء الاصطناعي في التنبؤ بالجريمة

5- Mohamed Elamin El Bushra (2024) Introduction to Criminal justice. Abu Dhabi. Emirates Academy for Identity and Citizenship.

6 - Fanny Rehnstrom (2021) How Capable is (AI) in Crime Prediction and prevention. Orebro University Press.

ومنعها. تكونت هذه الدراسة من مراجعة لتسع أدبيات تناولت مدى كفاءة التقنيات الحديثة في التنبؤ بالجريمة ومدى قدرتها على منع الجريمة قبل وقوعها. قدمت الدراسة تعريفاً للذكاء الاصطناعي وفروعه بالقول «إن الذكاء الاصطناعي يمكن وصفه بطريقتين مختلفتين هما،

أولا: وصف الذكاء الاصطناعي بأنه علم يهدف إلى اكتشاف الذكاء ويطور له آلات ذكية

ثانيا: وصف الذكاء الاصطناعي بأنه علم للوصول إلى طرق لحل المشكلات المعقدة التي لا يمكن حلها بدون ذكاء

وأضاف « فاني « لتعريفه هذا تصنيف الذكاء الاصطناعي من حيث قدراته إلى ثلاث درجات، ضعيف وقوي وفائق

وركزت هذه الدراسة على تطبيقات الذكاء الاصطناعي في مجال الجريمة ونظم العدالة الجنائية والاعتبارات الأخلاقية المتصلة بالذكاء الاصطناعي. وقد خلصت دراسة « فاني» إلى نتائج مشجعة لدور الذكاء الاصطناعي في التنبؤ بالجريمة،

إذ إن خمساً من الدراسات التسع التي تمت مراجعتها أكدت كفاءة وسلامة دور الذكاء الاصطناعي في التنبؤ بالجريمة، بينما هناك ثلاث دراسات فضلت كفاءة تعلم الآلة (ML) وتنقيب البيانات (DM) على كفاءة الذكاء الاصطناعي في التنبؤ بالجريمة وغيرها من الأحداث الأمنية. أما في مجال منع الجريمة فلم يجد «فاني» سوى دراسة واحدة أيّدت قدرة الذكاء الاصطناعي في منع الجريمة، وهي دراسة « كالدول»

2. دراسة « هايوارد ومعاس» 7حول الذكاء الاصطناعي والجريمة أولا لعلماء علم الاجرام. اتبعت هذه الدراسة على ذات المنهجية التي اتبعها « فاني ريهنستروم « باستناده على حقول علمية مقنعة مثل تعلم الآلة ML وتعلم إعادة التطبيق

7 - Keith J. Hayward and Matthys Maas (2020) Artificial Intelligence and Crime: A Primer for Criminologists Crime Media Culture. Sage.

والتعلم DL. استهدفت الدراسة لفت انتباه علماء علم الإجرام إلى ظاهرة الذكاء الاصطناعي وعلاقته بالجريمة والمجرم والعوامل والأسباب وراء الظاهرة. تشير هذه الدراسة إلى علم الإجرام وعلم ضحايا الجريمة والتفسيرات التقليدية التي قدمتها نظريات علم الإجرام مركزة على الظروف الاجتماعية والاقتصادية للفئات الضعيفة كعوامل رئيسية للجريمة والانحراف. بيد أن الذكاء الاصطناعي المؤثر على الجريمة ليس بأيدي الفئات الاجتماعية الضعيفة، بقدر ما هو بأيدي أفراد من الطبقات المتوسطة والطبقات الغنية التي حصلت على التعليم والعلوم المعلوماتية ووسائطها الذكية. وهنا يدعو كل من» هايوارد ومعاس» علماء علم الإجرام إلى البحث عن نظريات مواكبة تفسر ظاهرة استخدام الذكاء الاصطناعي في ارتكاب الجرائم. وتضيف هذه الدراسة من جهة أخرى إلى التأثيرات الإيجابية التي يمكن أن يحدثها الذكاء الاصطناعي في تحول عمليات الشرطة والعدالة الجنائية من جمودها التاريخي إلى عصرنا هذا، الأمر الذي ينبغي النظر إليه من نوافذ نظريات علم الإجرام وعلم ضحايا الجريمة وعلوم الأمن والعدالة الجنائية.

3. دراسة « كالدول وآخرين»[8] حول جرائم المستقبل الممكنة بالذكاء الاصطناعي، ممهدة لهذا الموضوع بعرض لنشأة ومسيرة تقنيات الذكاء الاصطناعي وطفرتها في السنوات الأخيرة.

راجعت هذه الدراسة عدداً كبيراً من الأدبيات التي وثقت خلال الفترة ما بين عامي 2015 و2020. وخلصت هذه الدراسة من تلك الأدبيات إلى تعريف ثمانية عشر من المهددات الأمنية المستقبلية للذكاء الاصطناعي، مع التأكيد أن ستة من بين تلك المهددات تشكل خطراً واسعاً على المجتمعات وهي:

- المحتويات الكاذبة.
- المركبات بدون قائد.

8 - Caldwell J.T. Andrews, T. Tanya and Griffin (2020). AI. Enabled Future Crimes. London: BMC available at : www.Creativecamons . org- revised 202024-5-.

- الروبوتات.
- البايومتركيات.
- العملات المشفرة.
- الصناعة الآلية للبرامج اللينة.

4. دراسة «دوون جونق»[9] حول التهديد الأمني للذكاء الاصطناعي والجريمة والفحص التقني الشرعي. تشير هذه الدراسة إلى أن الذكاء الاصطناعي المتقدم أصبح ضرورياً في جميع المعاملات الاقتصادية والاجتماعية العامة منها والخاصة، بما في ذلك علوم الحاسب الآلي، وهندسة الأمن، وعلم الإجرام، وعلم الاجتماع، وعلم الروبوتات. أوضحت الدراسة أن التعلم العميق DL دفع بدراسات الذكاء الاصطناعي إلى رفع قدرات تقنياته إلى القيام بالتحكم والتحليل لبيانات ضخمة من الصور والتقارير الطبية والتسجيلات الصوتية والتعرف على اللغات. قدمت هذه الدراسة تحليلا لخصائص جرائم الذكاء الاصطناعي وتحدياتها وصعوبات مواجهتها بأدوات المختبرات الجنائية التقليدية.

توصلت هذه الدراسة إلى أن الانتشار الواسع لتقنيات الذكاء الاصطناعي وتطبيقاتها مدعاة لنمو في أضرارها على الإنسان، الأمر الذي يستوجب تبني استراتيجيات مواكبة، خاصة فيما يتصل بنظم العدالة الجنائية الذكية وتنمية قدرات موظفي

5. دراسة «جون بايرز»[10] بعنوان (الذكاء الاصطناعي) المسائل القانونية العملية الصادرة في طبعتها الثالثة، وهي من أكثر الدراسات التي حظيت باهتمام المختصين في مجال الذكاء الاصطناعي. وقد وردت هذه الدراسة كمرجع في عدد من البحوث والمؤلفات التي تمت مراجعتها في هذا العمل لمواكبة التطبيقات العملية الواقعية للذكاء الاصطناعي ومستجداتها مع التركيز على الجوانب القانونية والأخلاقية.

9 - Doown Jeong (2020) Artificiality Intelligence Security Threats, Crime and Forensics: Taxonomy and Open Issues. IEEE Access.

10 - John Buyers (2023) AI: The Practical Legal Issues (3md, ed) Law Brief Publishing.

تناقش هذه الدراسة في مقدمتها نظم الذكاء الاصطناعي، وتخصص أكثر من عشرة فصول لعناصر الذكاء الاصطناعي واستخداماته. منها:

- أخلاقيات الذكاء الاصطناعي.
- الذكاء الاصطناعي المولد.
- قانون المجلس الأوروبي للذكاء الاصطناعي.
- البيانات الكبيرة والذكاء الاصطناعي.
- الملكية الفكرية والذكاء الاصطناعي.
- الذكاء الاصطناعي والجريمة.
- تأثيرات الذكاء الاصطناعي على الأسواق والتنافسية.

6. بحوث ودراسات ندوة إستكهولم الدولية لعلم الإجرام فيما يتصل بالذكاء الاصطناعي والجريمة: أفردت ندوة إستكهولم[11] الدولية الثامنة عشرة للعام 2024 يوماً كاملاً لعرض ومناقشة تأثيرات الذكاء الاصطناعي على الجريمة وعلى عمليات أجهزة العدالة الجنائية بصفة عامة ـ وكان من أهم الدراسات التي عرضت وناقشها الحضور ما يلي:

(1) - دراسة « ماري أنيان [12]» بعنوان الذكاء الاصطناعي والأمن. طرحت هذه الدراسة قضايا واقعية تم فيها استخدام الذكاء الاصطناعي وتقنيات التعلم العميق في تحليل وتوجيه المتغيرات السياسية في دول عظمى مثل فرنسا وبريطانيا وألمانيا. وكشفت الدراسة نتائج تلك الاستخدامات على المتغيرات السياسية في انتخابات بريطانيا وانتخابات البرلمان الأوروبي لعام 2024 وفوز اليمين الفرنسي فيها وما تبع ذلك الفوز من متغيرات في السياسة الداخلية الفرنسية

11 - تعتبر ندوة إستكهولم الدولية لعلم الإجرام أهم الملتقيات العلمية في مجال الجريمة والعدالة الجنائية. تنظم هذه الندوة سنويا في إستكهولم عاصمة السويد وتقدم فيها بحوث حديثة بجانب بحوث جائزة علم الإجرام السنوية التي تقدر قيمتها بـ (700 ألف دولار) .

12 - Marie Enema (2024) Artificial Intelligence and National Security: Criminology Symposium Papers. Bra Publication.

وفي إحدى القضايا كشفت الدراسة استخدام الذكاء الاصطناعي وتقنيات تعلم الآلة والذكاء الاصطناعي المولد في تحليل مجريات حرب أوكرانيا والتنبؤ بمخاطرها وحجمها ونهايتها، إلا أن الدراسة أوضحت بالأرقام فشل الذكاء الاصطناعي في قراءة الحرب موضحة أن الخسائر المالية والاقتصادية والعمر الزمني للحرب لم تكن سليمة.

(2) دراسة « بارتلوميج أورزياك[13] » حول الذكاء الاصطناعي والعدالة الجنائية في بولندا: نطاق وقواعد استخداماته. عرضت هذه الدراسة قضايا جنائية نجحت فيها أجهزة العدالة الجنائية، خاصة الشرطة والنيابة في جمع الأدلة للاتهام والدفاع بتقنيات الذكاء الاصطناعي وذلك من خلال حصر وتحليل كم كبير من الآثار والمكالمات الهاتفية والصور والبيانات الصحفية وإفادات الشهود، وترجمة كل ذلك إلى أرقام أنتجت أدلة قوية ومحوسبة لا يتطرق إليها الشك فيما يعرف بالأدلة الرقمية المصنفة Artificial Digital Evidence. وخلصت الدراسة إلى أن نجاحات الشرطة والنيابة في حسن استخدام الذكاء الاصطناعي استوجبت إجراء تعديلات في الدستور والقانون الجنائي لترشيد ووضع قواعد عامة لعمليات استخدام الذكاء الاصطناعي الأمر الذي تقوم به وزارة العدل الآن

(3) دراسة « كارلا فأردت [14]» بعنوان الذكاء الاصطناعي والجريمة: قراءة البيانات السرية. وقد تناولت هذه الدراسة المشكلات والضغوط التي تواجهها حكومات بعض الدول الأوروبية من الاختراقات المنفذة بالذكاء الاصطناعي على قواعد البيانات الشخصية للأفراد والتي تحتفظ بها الحكومات وأجهزتها الأمنية والصحية والتعليمية. وقدمت الدراسة نماذج من شكاوى الأفراد الذين كُشِفت بياناتهم الشخصية ونُشرت عبر وسائط الإعلام الاجتماعي وما نجم عنها من خسائر

13 - Bartlomiej Oreziak (2024) Artificial Intelligence Justice in Poland: Use Case Stockholm Criminology Symposium. Bra Publication 132024-6-.

14 - Klava Faldt (2024) AI and Crime: Secret Data Reading. Stockholm Criminology Symposium Papers. University of Gothenburg Publication.

(4) دراسة « مارتن بولدت[15] « بعنوان التنبؤ بالمناطق الساخنة القائم على خرائط البيانات واستخدام تقنيات الذكاء الاصطناعي. تناولت الدراسة تقييم محاولات استخدام تقنيات الذكاء الاصطناعي في التنبؤ بالمناطق الساخنة جنائياً وأمنياً. وقدمت الدراسة تجارب ناجحة، خاصة في رسم خرائط المناطق الساخنة للجريمة المنظمة واتجاهات أنشطتها.

(5) دراسة حول علم الإجرام السيبراني والتحقيق الرقميand Cyber criminology Digital Investigation لمعدّها « شيك شوي كنق» الذي تناول الجريمة السيبرانية من منظور علم الإجرام[16] . موضحاً مفهوم علم الإجرام السيبراني والتمييز بينه وبين علم الإجرام التقليدي. تم في هذه الدراسة مراجعة تعريف الجريمة السيبرانية وأنماطها المستحدثة وتعريف الجرم السيبراني والضحية السيبرانية فاتحاً بذلك الطريق أمام تطوير نظريات جديدة تفسّر أسباب الجريمة السيبرانية ورسم صورة لشخصية المجرم السيبراني بالقدر الذي يعين على التحقيق وجمع الأدلة الرقمية اللازمة لتحقيق العدالة الجنائية

(6) دراسة حول تحقيقات الجريمة السيبرانية Cybercrime Investigation ل « رايس انتوني وآخرين « [17]، يسلط هذا البحث الضوء على الأساليب الحديثة والمتطلبات الخاصة للأدوار والمهام الخاصة بالتحقيق السيبراني موزعاً تلك الأدوار على رجال إنفاذ القانون من الشرطة ومأموري الضبط القضائي ووكلاء النيابة العامة. يشرح البحث بتفصيل الإجراءات القانونية والفنية الخاصة بالتفتيش والضبط وحجز وتأمين الأدلة

15 - Marten Boldt (2024) A Data-drivingraph – based for hot spots Prediction: Use of Artificial Intelligence Stockholm Criminology Symposium Bra. Publication.

16 - Eoghan Casey, Digital Evidence and Computer Crime, London: AcademicPress,2000, P.260
Kyung-shick. Cyber criminology and Digital Investigation, FBI Scholarly Publishing.

17 Anthony Reyes, Kevin O'Shea, JIM Steele. Jon R. Hansen, Benjamin R. Jean and Thomas Ralph. Cyber Crime Investigations: Bridging the Gaps between Security Professionals Law Enforcement and Prosecutors. Syngress. Publishing 2015

(7) دراسة حول الجريمة الرقمية والإرهاب الرقمي لـ « روبرت تايلور وفرتش »[18] تتناول الدراسة الجريمة الرقمية وأنماطها المختلفة من عدة زوايا مع التركيز على أبعادها ومستجداتها واتجاهاتها المستقبلية. وتسلط الدراسة الضوء على كيفية انتقال عصابات الجريمة المنظمة من الأنشطة الإجرامية التقليدية إلى الأنشطة الإجرامية الرقمية، الأمر الذي شكّل تعقيدات في التحقيق وضبط الحياة.

معطيات الدراسات السابقة

مع معطيات التطور السريع في تطبيقات الذكاء الاصطناعي، يتسابق الباحثون وخبراء تقنية المعلومات والاتصالات الإلكترونية وحماة الأمن السيبراني في اللحاق بتلك التطبيقات ومواكبتها بالبحوث والدراسات التي تكشف مشكلاتها، والتعرف على نقاط الضعف وفرص معالجة إساءة استخدام تقنيات الذكاء الاصطناعي، علاوة على التعريف بالممارسات الفاضلة للذكاء الاصطناعي

يلاحظ في البحوث والدراسات والمؤلفات المنشورة التي قمنا بمراجعتها في سياق هذا البحث أنها أخذت اتجاهين:

- اتجاه يركز على طرح دراسات وأوراق عمل لتجارب وتطبيقات واقعية لاستخدامات الذكاء الاصطناعي مع بيان نتائجها وتحدياتها، خاصة في الجوانب القانونية الحاكمة لتلك الاستخدامات.
- اتجاه نظري يُعنى بدراسة تطبيقات الذكاء الاصطناعي ومقارنتها على نطاق واسع تمتد أحيانا عبر الحدود الدولية، تحسبا لعولمة استخدامات الذكاء الاصطناعي.

تعلمنا الدراسات السابقة، في مجال الذكاء الاصطناعي، طرق ومناهج بحث جديدة صبغتها بالالتزام بالتخصصات الدقيقة والشراكة بين الباحثين والخبراء والمهنيين، بحيث يسهم كل واحد منهم بعصارة تجربته وخبرته العملية. ولا تقتصر هذه الشراكة على دولة أو جنسية أو جنس واحد، بل تمتد الشراكة عبر الحدود والقارات. وقد تبين أن من

18 - Robert W, Taylor, Eric J. Fritsch, and John Liederbach. Digital Crime and Digital Terrorism. London, Pearson.2015

أفضل البحوث التي قمنا بمراجعتها بحوث ودراسات تم إعدادها بالشراكة بين باحثين من الصين والولايات المتحدة الأمريكية واليابان[19] من جهة أخرى، تسعى بحوث ودراسات الذكاء الاصطناعي إلى الفحص والتحليل العميق للتجارب والاستخدامات ومدى مراعاتها للحريات الشخصية والأخلاقيات المهنية وقيم المجتمعات.

أما من ناحية إساءة استخدام تقنيات الذكاء الاصطناعي فقد نبهت الدراسات السابقة إلى جرائم العنف والتطرف الفكري والراديكالية المعززة بتقنيات الذكاء الاصطناعي. كما كشفت الدراسات السابقة أن جرائم مستحدثة تُرتكب باستخدام تقنيات الذكاء الاصطناعي، مثل جرائم إنتاج ونشر المحتويات الكاذبة وتزوير الأدلة الجنائية وصناعة أدلة رقمية تدحض حقائق الجريمة وتضير بالعدالة الجنائية

حظيت الجرائم المالية المتأثرة بتقنيات الذكاء الاصطناعي باهتمام بالغ من قبل الباحثين، خاصة فيما يتصل بطرق ارتكابها واكتشافها والتحقيق فيها بما يُعرف بالتحقيقات المالية الرقميةDigital Financial Investigations، لم تهمل الدراسات السابقة النقد المؤسسي لتقنيات الذكاء الاصطناعي بتقديم نماذج حيّة من الأخطاء والفشل الناجم عن الذكاء الاصطناعي في التنبؤ وقراءة المستقبل وتقييم الأحداث الأمنية، مثل تقدير تطورات حرب أوكرانيا وخسائرها وانعكاساتها على الدول الأوروبية.

19 - Reza Montasari et.al (2023) Opcit.

الفصل الثاني

استخدامات الذكاء الاصطناعي وتأثيراته

حول الذكاء الاصطناعي

قبل الخوض في استخدامات الذكاء الاصطناعي ينبغي الإشارة إلى « ألان تورينق» لكونه أول من صاغ عبارة الذكاء الاصطناعي خلال جهوده الذكية في حل شفرات ألمانيا النازية أثناء الحرب العالمية الثانية، ووثق تلك العبارة في ورقة أعدّها عام 1950 تناولت المقاربة بين ذكاء الإنسان والحاسب الآلي

تفيد معظم الدراسات [20] بأن نشأة الذكاء الاصطناعي يعود إلى منتصف القرن العشرين، وتحديداً إلى عام 1956 تاريخ مؤتمر « دارتموث» الذي نظمه كل من « جون مكارثي « و « مارفن منسكي « و»ناثنيال روتشتر «، حيث اقترح فيه الباحثون تصميماً آليّاً لمحاكاة ذكاء البشر، ومن ثم تطورت أبحاث الذكاء الاصطناعي سريعاً في السنوات التالية لمؤتمر « دارتموث « مما أفرز عدة تقنيات مثل التفكير الرمزي والأنظمة الحديثة لتمكين الآلة من اتخاذ القرارات وحل المشكلات. وفي الثمانينيات من القرن العشرين ظهر مفهوم تعلم الآلة كنهج جديد للذكاء الاصطناعي.

عرّف « منسكي»[21] الذكاء الاصطناعي بأنه (علم تمكين الآلات من القيام بأشياء تتطلب ذكاءً إذا قام بها الإنسان)

"AI is the science of making machines do things that would require intelli-gence if done by men."

أما « بلمان «[22] فقد عرف الذكاء الاصطناعي بأنه (أتمتة الأنشطة المرتبطة بتفكير الإنسان، أي أنشطة اتخاذ القرار، وحل المشكلات، والتعلم، والتصنيع والألعاب وغيرها).

20 - Keith J. Haward and Matthys Maas (2020) Artificial and Crime: A Primer for Criminologists. Crime Media Culture. Sage.

21 - Minsky M (1968) Semantic Information Processing. MIT Press. Cambridge.

22 - Bellman R (1978) An Introduction to AI: Can Computer thin R? Boyd and faster. San Francisco.

“AI is the automation of activities that we associate with human thinking, activities such as decision- making, problem solving, learning, creating, game playing, and so on”.

في عام 2016، وصف « نلسون» الذكاء الاصطناعي بأنه ((نشاط مسخّر لجعل الآلات أذكياء، والذكاء هو الكفاءة التي تمكّن أي كيان من القيام بوظائفه بدقة وبعد نظر في مجاله))

“Activity devoted to making machines intelligent, and intelligence is that quality that enables an entity to function appropriately and with foresight in its environment”.

ومن جهة أخرى نظم « رسل ونورفق» [23] تعريفات الذكاء الاصطناعي في أربع مجموعات: تفكير بشري، وأداء بشري، وتفكير عقلاني وأداء عقلاني.

“Definitions of AI are four categories: Thinking humanly, acting humanly, thinking rationally and acting rationally”.

يصنف بعض الباحثين الذكاء الاصطناعي من حيث المعايير إلى ذكاء اصطناعي ضعيف وذكاء اصطناعي قوي وذكاء اصطناعي خارق، بينما يصنف البعض الآخر الذكاء الاصطناعي الضعيف من حيث الوظائف إلى:

- الآلات القادرة على ردة الفعل.
- الآلات محدودة الذاكرة.
- آلات تفهم الحالة العقلية للبشر.
- الآلات القادرة على فهم الذات [24].

23 - Russel S, Norvig P, (2016) AI: A Modern Approch. Pearson Education Limited, Essex.

24 - Ira Goel (2023) Introduction; AI and AI Governance. Amazon UK. ISBN 9798871709382-P.28.

تتفرع تقنيات الذكاء الاصطناعي المتطورة سريعاً إلى:

1. تعلم الآلة.
1. التعلم العميق.
2. رؤية الحاسب الآلي.
3. نظم الروبوتات.
4. نظم مقدمة للتوصيات.

استخدامات الذكاء الاصطناعي في العالم الواقعي

شهدت السنوات القليلة الماضية توسعاً ملحوظاً في استخدامات الذكاء الاصطناعي في العالم الواقعي أو الحقيقي Real World، خاصة في المعاملات الاجتماعية والاقتصادية والخدمات العامة والخاصة[25]. وقد انعكس هذا التوسع في الإحصاءات الموثقة التي توقعت عائداتها المالية بمبلغ (126) مليار دولاراً عام 2025. كما وضح من تقارير «قارتنر»[26] أن37% من المنظمات قد استخدمت الذكاء الاصطناعي بأي شكل من الأشكال في عملياتها وخدماتها بنمو تجاوز (270 %)، ومن جهة أخرى أكدت تقارير «حلول سيرفيون الدولية»[27] توقعات نمو تجارة البرامج اللينة للذكاء الاصطناعي Ai Software بمعدل (95%) عام 2025.

في ضوء هذا الانتشار المتسارع لتطبيقات الذكاء الاصطناعي، نتناول في هذا الفصل عرضاً لأهم مجالات استخدام الذكاء الاصطناعي، علماً بأن تعدد مجالات تطبيقات الذكاء الاصطناعي في الحياة العامة والخاصة يضاعف احتمالات استخدام الذكاء الاصطناعي في الجريمة. لا شك أن مرتكبي الجريمة والجانحين يسعون دائماً إلى استغلال الفرص والثغرات التقنية في التطبيقات لتحقيق أهدافهم[28].

25 - Lui HY (2021) " Ai challenges and the Inadequacy of human rights protection" criminal Justice Ethics 40:222-.

26 - Jennifer Garfinkel (2019) Gartner Survey of more than 3000 CIOs. Orlando. Gartner Symposium ITXPO 2019.

27 - Serverion Global Solutions.www.serverion.com.

28- Reed Hostings and Erin Meyer (2024) No Rules Rules: Netflix and the Culture of Reinvention Publications.WH Allen Puplications.

لأهمية استخدامات الذكاء الاصطناعي في الحياة اليومية[29] ولاحتمالات تعرضها لاختراقات أمنية وجنائية نورد هنا نماذج منها للتعريف وهي

1. **مساعدات الصوت:** مساعدات الصوت المتوفرة على هاتفك الذكي أو على جهازك المنزلي الذكي مدعوما بالذكاء الاصطناعي.
2. **الأجهزة المنزلية الذكية:** بفضل الذكاء الاصطناعي، يمكن لأجهزة تنظيم الحرارة في منزلك تلقائياً ضبط نظام التدفئة والتهوية وتكييف الهواء، بينما يمكن للكاميرات تنبيه المستهلكين إلى وجود أشخاص أو سيارات أو طرود مشبوهة.
3. **الملاحة والسفر:** أصبحت الخرائط الورقية شيئاً من الماضي. يمكن أن تعمل الاتجاهات التي تم إنشاؤها بواسطة الذكاء الاصطناعي على تحسين وقت السفر أو استهلاك الوقود.
4. **الموارد البشرية:** كما هو معروف تتم معظم عمليات التوظيف عبر الإنترنت هذه الأيام. تتم عمليات الاختيار عبر الانترنت باستخدام إذن الصوت والكاميرا لجهاز المرشح. هنا يتم رفع دعوى قضائية ضد تطبيق الذكاء الاصطناعي عند اكتشاف أي نوع من السلوكيات الخاطئة وأشياء أخرى كثيرة. كما أنه يستخدم للكشف عن شخصية أي مرشح في بعض الحالات، علاوة على استخداماته تخطيط وادارة الموارد البشرية.
5. **الزراعة:** أصبح الذكاء الاصطناعي جزءاً من الزراعة وحياة المزارعين، يتم استخدامه للكشف عن عوامل مختلفة، مثل كمية الماء والرطوبة، وكمية العناصر الغذائية الناقصة، وما إلى ذلك في التربة. هنالك أيضاً آلة تستخدم الذكاء الاصطناعي لاكتشاف مكان نمو الأعشاب الضارة، ومكان التربة غير الخصبة، وما إلى ذلك.
6. **سلسلة التوريد:** تساعد خوارزميات الذكاء الاصطناعي في تحليل المخزون وإعداده

29 - Tom Taulti (2019) Artificial Intelligence Basics: Anon-Technical Introduction.Apress. IsBN-13:978-1484250273.

للحفاظ على مخزون سلسلة التوريد على الرغم من أنها ليست جديدة، إلا أنها تساعد المزارعين في مجال الزراعة على ضمان تلبية المتطلبات بأقل قدر من الخسارة.

7. **إدارة الآفات:** يمكن لخوارزمية الذكاء الاصطناعي تحليل البيانات من مصادر متعددة لتحديد الإنذارات المبكرة للمزارعين المعنيين. تتيح هذه التقنية أيضاً استخدامات أقل للمبيدات الحشرية الضارة من خلال توفير أفضل الموارد لإدارة الآفات.

8. **التنبؤ:** بمساعدة الذكاء الاصطناعي أصبح تحليل توقعات الطقس ونمو المحاصيل أكثر ملاءمة في مجال الزراعة، وتساعد الخوارزميات المزارعين على زراعة المحاصيل من خلال اتخاذ قرارات تجارية فاعلة.

9. **خدمة المتعاملين:** تقدم تقنيات الذكاء الاصطناعي في مجال خدمة المتعاملين وتقديم خدمات حكومية شفافة.

10. **تجربة التسوق واكتشاف التقييمات المزيّفة:**

تحول الناس الآن نحو التسوق عبر الإنترنت ومن المرجح أن يصل حجم السوق إلى (71) تريليون دولاراً بين (2022-2028)، وللذكاء الاصطناعي دور مهم للغاية في ذلك من خلال تقديم توصيات وعروض قابلة لكل شخص لاستهداف شرائح محددة وزيادة المبيعات. أشار أحد التقارير إلى أن 9 من كل 10 أشخاص يميلون إلى مراجعات العملاء أولاً قبل تقديم أي طلب فعلياً[30].

11. **التعليم:** كان تنظيم وإدارة القطاعات التعليمية بالكامل يتم من خلال المشاركة البشرية حتى خلال بعض سنوات مضت، ولكن في هذه الأيام أصبح القطاع التعليمي أيضا تحت تأثير تطبيقات الذكاء الاصطناعي، فهو يساعد أعضاء هيئة التدريس وكذلك الطلاب من خلال تقديم توصيات المقرر الدراسي، وتحليل بعض البيانات والقرارات المتعلقة بالطالب.

12. **الترفيه:** يعتبر استخدام تطبيقات الذكاء الاصطناعي في مجال الترفيه هو الأكثر

30 - Linda Jereige (2024) Artificial Intelligence in Everyday life. Independently published. ISBN:13979-B328308137.

رواجاً في العالم اليوم.

13. **الفلك:** في السنوات الأخيرة قام تطبيق الذكاء الاصطناعي أيضاً بتوسيع نطاق تطبيقه في مجال علم الفلك. يستخدم الذكاء الاصطناعي للتحقيق في عمليات اندماج المجرّات والنجوم للتنبؤ بمستقبل البشر.

14. **روبوتات الدردشة:** روبوتات الدردشة يتم تعريفها على أنها أداة تُستخدم للرد على النص المقدم في الدردشة كمدخلات، وفيه يرسل العميل أو المستخدم الاستعلام حسب حاجته، ويعطي الشات روبوت المخرجات الأنسب لتقديم الحل الأفضل وفقاً للمدخلات.

15. **الصحة والعناية الطبية:** حققت تطبيقات الذكاء الاصطناعي في الخدمات الإنسانية تقدماً كبيراً في مجال الصحة والعناية الطبية، ومن ذلك

اكتشاف الأدوية وتنظيم استعمالاتها.

16. **الأمن الوطني:** تأخذ أجهزة الأمن الوطني، في كثير من دول العالم، قدراً كبيراً من تطبيقات الذكاء الاصطناعي في تنفيذ عملياتها ومنها، على سبيل المثال لا الحصر:

- كشف الاحتيال المالي
- المراقبة عن بعد
- تساعد خوارزميات الذكاء الاصطناعي في اكتشاف الأشياء
- التحليل التنبؤي
- تحليل السلوك وإيماءات الجسم

17. **أمن البيانات:** أحد الاهتمامات الرئيسية لأي شركة تكنولوجيا الاحتفاظ بالمعلومات حول بيانات اعتماد العديد من المستخدمين، وهي معلومات سرية للشركة. هناك

العديد من تطبيقات الذكاء الاصطناعي التي يتم استخدامها للحفاظ على أمان هذه البيانات، ومنع أي نوع من التهديدات والهجمات الضعيفة.

مخاطر وتأثيرات سالبة للذكاء الاصطناعي

توسعت تطبيقات واستخدامات الذكاء الاصطناعي في الحياة اليومية، ابتداءً من عمليات الترفيه والتعليم والخدمات الإنسانية وانتهاءً بالأمن والدفاع والرعاية الصحية. وليس هناك من ينكر أن كل تلك الاستخدامات تصحبها مخاطر وتأثيرات سالبة، لا ينبغي ترك فرص الخطأ فيها لصلتها الوثيقة بحياة الإنسان. فيما يلي نورد نماذج من المخاطر والتأثيرات السالبة المحتملة لاستخدامات الذكاء الاصطناعي، توطئة للانتقال إلى انعكاساتها على الجريمة والمجرمين وضحايا الجريمة، ومن أهم تلك المخاطر والتأثيرات السالبة ما يلي:

1. **الافتقار إلى الشفافية:**

يمكن لتقنيات الذكاء الاصطناعي أن تؤدي إلى التحيزات المجتمعية بسبب الافتقار إلى الشفافية الناجم عن التعلم الآلي، وتصميم خوارزميات معقدة قد لا تكون مفهومة لعامة الناس. وللحد من ذلك ينبغي الاستثمار في تطوير خوارزميات شفافة وغير متحيّزة.

2. **مخاوف على الخصوصية:**

غالباً ما تجمع تقنيات الذكاء الاصطناعي كميات كبيرة من البيانات الشخصية وتحلّلها، مما يثير مشكلات تتعلق بخصوصية البيانات وأمنها. للتخفيف من مخاطر الخصوصية يجب علينا الدعوة إلى قوانين صارمة لحماية البيانات وممارسات آمنة للتعامل مع البيانات.

3. **المعضلات الأخلاقية:**

ويشكّل غرس القيم الأخلاقية في أنظمة الذكاء الاصطناعي، وخاصة في سياقات صنع القرار ذات العواقب الوخيمة تحدياً كبيراً. يجب على الباحثين والمطورين إعطاء

الأولوية للآثار الأخلاقية لتقنيات الذكاء الاصطناعي لتجنب الآثار المجتمعية السلبية.

4. المخاطر الأمنية:

ومع تزايد تطور تقنيات الذكاء الاصطناعي، تتزايد أيضاً المخاطر الأمنية المرتبطة باستخدامها واحتمال إساءة استخدامها. يمكن للقراصنة والجهات الفاعلة الخبيثة تسخير قوة الذكاء الاصطناعي لتطوير هجمات إلكترونية أكثر تقدماً، وتجاوز التدابير الأمنية واستغلال نقاط الضعف في الأنظمة. كما يثير صعود الأسلحة المستقلة التي تعتمد على الذكاء الاصطناعي المخاوف بشأن مخاطر الدول المارقة، أو الجهات الفاعلة غير الحكومية التي تستخدم هذه التكنولوجيا - خاصة عندما ننظر في الخسارة المحتملة للسيطرة البشرية في عمليات صنع القرارات الحاسمة

5. تركيز القوة:

إن هيمنة عدد صغير من الشركات الكبرى والحكومات على تطوير الذكاء الاصطناعي يمكن أن يؤدي إلى تفاقم عدم المساواة والحد من التنوع في تطبيقات الذكاء الاصطناعي، لذا يُعدُّ تشجيع تطوير تطبيقات الذكاء الاصطناعي اللامركزي والتعاوني أمراً أساسياً لتجنب تركيز السلطة

6. تقدم الاعتماد على الذكاء الاصطناعي:

قد يؤدي تطور الذكاء الاصطناعي والاعتماد المفرط على تقنياته إلى تخلف في قدرات البشر بفقدانه فرص الإبداع والابتكار وتراجع التفكير النقدي. ولكن قد يكون في تحقيق قدر من التوازن بين اتخاذ القرارات بمساعدة الذكاء الاصطناعي والتدخل البشري أمراً حيوياً للحفاظ على قدرات الإنسان على المدى البعيد.31

7. النزوح الوظيفي والمهني:

ينظر البعض إلى عدم الاستقرار الوظيفي والمهني على أنه خطرٌ قد ينجم عن استخدامات الذكاء الاصطناعي، خاصة أن هناك صعوبة في التنبؤ بمثل هذا التأثير في

31 - Stuart Russell and Peter Norvig (2021) Artificial Intelligence: Amodern Approach.Pearson Publications. ISBN-13:978.1292401133-

ضوء تسارع تقدم تقنيات الذكاء الاصطناعي وتعلم الآلة.[32]

8. المخاطر والتأثيرات على الاقتصاد العالمي:

أصبح الاقتصاد العالمي موضع اهتمام دول وشعوب العالم في ظل عولمة عملياته، وتشابك المصالح والمعاملات المالية عبر الإنترنت التي تواجه تحديات الجريمة السيبرانية. أوضحت الدراسات المعنية بأمن الاقتصاد العالمي عن نتائج غير متفائلة[33]. وعززت تلك بالنتائج الإحصائية التي وثقتها منظمة الشرطة الجنائية الدولية (إنتربول). وقد أوضحت قراءات الشرطة الجنائية أن الجرائم الاقتصادية المرتكبة أو المتأثرة بالذكاء الاصطناعي موزعة على العالم وهي

- التلاعب في الاستثمارات.
- الاحتيال.
- الغش في المدفوعات.
- اختراقات الإنترنت.

استخدامات الذكاء الاصطناعي وتأثيراتها على ارتكاب الجرائم

من المتوقع أن يتواصل الصراع بين الأشرار والخيريين في استخدام الذكاء الاصطناعي. سوف تسعى المنظمات الإجرامية إلى استغلال الذكاء الاصطناعي وتقنياته المستحدثة في تنفيذ الجرائم. خاصة جرائم المال والجرائم السياسية. من جهة الأخرى سوف تعمل أجهزة العدالة الجنائية على تسخير تقنيات الذكاء الاصطناعي في الوقاية من الجريمة واكتشاف ما يقع منها[34]. وقد تتفوق المنظمات الإجرامية على أجهزة العدالة الجنائية بفضل إمكانياتها المالية وسهولة حركتها خارج نطاق الشرعية، بينما قد تظل أجهزة العدالة الجنائية متأخرة بسبب الإمكانات المالية والتقيد بالإجراءات القانونية غير

32 - Fathi Salih Khalid (2023) The Future of Human Resource Management in the Ero of Artificial Intelligence. Barcode Publishing house.

33 - Eben Estehuizen (2023) The A-Z of Ai use cases: An overiew of 63 ways that change the world. Business Development and Enterpreriership Books.

34 - Interpol Innovative Center. (2023) Chat GPT: Impact on Law enforcement. www, interpol.int/en.

المواكبة لسرعة تطور تقنيات الذكاء الاصطناعي [35].

الذكاء الاصطناعي، كأي نشاط من أنشطة المجتمع أو كأي عمل من أعمال أجهزة العدالة الجنائية لمكافحة الجريمة، يتطلب تجنب التأثير على حقوق الإنسان أو خصوصيات أي فرد من أفراد المجتمع، سواء كان متهماً أو مجرماً أو ضحية جريمة. ويشمل ذلك الحقوق المُعترف بها والمقررة في القانون الدولي. وينبغي أن تكون التشريعات الوطنية المنظمة لاستخدامات الذكاء الاصطناعي استباقية تتقدم على ابتكاراته. كما يجب على أجهزة نظام العدالة إشراك خبراء في القانون الدولي الإنساني وخبراء الأخلاقيات المهنية في مراجعة وتقييم تطبيقات الذكاء الاصطناعي في كافة عمليات مكافحة الجريمة ومعاملة المذنبين. وقد لاحظنا في الدراسات السابقة تطبيقات واقعية لدول متقدمة أقدمت على تطبيق الذكاء الاصطناعي في قضايا جنائية، ومن ثم أدركت مخالفة تلك التطبيقات للقوانين ومن ثم شرعت في تعديل دستورها[36]. ومع امتداد استخدامات الذكاء الاصطناعي إلى كثير من عمليات حياتنا اليومية تصبح الشرعية ضرورية لحوكمة الذكاء الاصطناعي واستخداماته في كافة القضايا والمنازعات المدنية منها والشرعية ، إلا أن للشرعية في مجال الجريمة والعدالة الجنائية أهمية خاصة لاتساع نطاق استخداماتها، ابتداءً بتنظيم حركة السير والمرور مروراً بالتنبؤ بالجريمة والوقاية منها وانتهاءً بعمليات المحاكم الجنائية والمؤسسات العقابية والإصلاحية [37]، علماً بأن عمليات مكافحة الجريمة ونظم العدالة الجنائية وأجهزتها تقع تحت الرقابة اللصيقة للجان الأمم المتحدة المتخصصة بحقوق الإنسان وسلامة عمليات أجهزة العدالة الجنائية في هذا السياق، وتعزيزاً لتدابير سلامة استخدامات الذكاء الاصطناعي أصدر معهد الأمم المتحدة الإقليمي لبحوث الجريمة والعدالة بالتعاون مع منظمة الشرطة الجنائية الدولية دليلاً ينظم مسؤوليات أجهزة إنفاذ القانون تجاه تقنيات الذكاء الاصطناعي

35 Bartlomiej Oreziak (2024) OP cit.

36 - B. Oreziak (2024) OP. Cit.

37 - B. Custers (2022) Opcit.

وابتكاراتها [38]. تضمن هذا الدليل مبادئ عامة لابتكارات الذكاء الاصطناعي تعالج مسائل الشرعية، وتقليل الضرر، واستقلالية الإنسان والعدالة.

إذاً، تكون الشرعية محوراً مهماً لاستخدامات الذكاء الاصطناعي في مجال الجريمة من حيث الوقاية منها ومكافحتها وتحقيق العدالة بشأنها. وعليه ينبغي مراجعة التشريعات الوطنية الإقليمية والدولية للتعرف على ما توافر منها لحوكمة استخدامات الذكاء الاصطناعي، أولا من حيث الاستفادة منها في تحقيق العدالة الجنائية ومكافحة الجريمة، وثانياً من حيث مساءلة إساءة استخدام الذكاء الاصطناعي وتقنياته في ارتكاب الجرائم وانتهاك حقوق الإنسان [39]. كما أن المسائل القانونية والأخلاقية لاستخدام الذكاء الاصطناعي [40] تعتبر من التحديات والعقبات في استخدام الذكاء الاصطناعي خاصة في مكافحة الجريمة من أهم الجوانب التي يجب مراعاتها، حيث تشمل هذه التحديات القضايا الأخلاقية والقانونية التي تتعلق بالخصوصية والأمان أثناء استخدام التكنولوجيا. بالإضافة إلى ذلك، تظهر الضغوط الاجتماعية والسياسية المرتبطة بتطبيقات الذكاء الاصطناعي في مجال مكافحة الجريمة كعوامل معقدة يجب معالجتها بعناية واحتراس. ينبغي توخي الحذر أيضاً في مواجهة التحديات التي قد تنشأ من التمييز العنصري والتحيز الجندري نتيجة لاستخدام التكنولوجيا، حيث يجب توفير استراتيجيات تصحيحية تضمن عدم حدوث اي تمييز غير مبرر، أو تحيّز غير مقصود في استخدام تطبيقات الذكاء الاصطناعي في مكافحة الجريمة. لذلك، فإن هناك حاجة ملحة لتواجد إرادة صادقة للتعامل مع هذه التحديات المعقدة، والبحث عن حلول مبتكرة وشاملة للتأكد من أن تكنولوجيا الذكاء الاصطناعي المستخدمة لمكافحة الجريمة تعمل بفاعلية وبشكل عادل لجميع الأفراد أو المجتمعات. ومن أهم تلك التحديات ما يلي:

---

38 -United Nations Interregional Crime and Justice Research Institution (2024). Responsible AI innovation in Law Enforcement (AI Tool Kit). Published by INTERPOL. (Funded by EU).

39 -Gellers (2021) Rights for robots: Artificial Intelligence, animal and environmental Law. Tylor and Trancis, Abingdn

40-Omar Santos and Peter Radanlier (2024) Beyond the Algorithm: AI, Security, Privacy and Ethics. Addison-Wesley.

1. التمييز العنصري والتحيز الجندري
2. التحديات الأخلاقية والقانونية
3. الخصوصية والأمان
4. التلاعب بالبيانات السرية

عليه، هنالك فرص ثمينة لاستخدام الذكاء الاصطناعي في ارتكاب الجرائم والإخلال بالأمن العام والسلامة العامة وانتهاك حقوق الإنسان، وربما تعريض العالم للدمار الشامل. ومما يدعم تلك الفرص ما يلي:

1. توفر تقنيات الذكاء الاصطناعي وبرامجها المتطورة ووسائطها الذكية المعروضة في الأسواق دون ضوابط تحكمها.
2. القدرة المالية المتوفرة للأفراد لاقتناء تلك التقنيات ووسائطها الذكية.
3. المنافسة المفتوحة بين الشركات المطورة لتقنيات الذكاء الاصطناعي وقدرتها على تسويق منتجاتها بتسهيلات تسهم في انتشارها.
4. تحفيز الذكاء الاصطناعي وابتكارات الشباب وصغار السن على التعلم الذاتي للخوارزميات، والتسابق في إنتاج وتطوير برامج وحلول في التعلم الآلي تمكنهم من إحداث اختراقات قد تكون خطيرة. وقد تكون تلك الاختراقات جرائم يكتسبون من ورائها، وقد تكون لمجرد التسلية وإثبات القدرات الشخصية.
5. كثرة استخدامات الذكاء الاصطناعي في معاملاتنا وحياتنا اليومية توفر فرصا لمرتكبي الجرائم. وكلما زادت تطبيقات الذكاء الاصطناعي زادت فرص إساءة الاستخدام.[41]

في تقديرنا، على ضوء نتائج البحوث الحديثة، قد يكون للذكاء الاصطناعي تأثير كبير على زيادة فرص ارتكاب الجرائم في المجال الإلكتروني، حيث يمكن لتطبيقات الذكاء الاصطناعي الابتكارية والمتقدمة أن تساعد في عمليات التجسس والاختراق

41 - Matt Greenwood (2024) Artificial Intelligence: A practical Guide to using Ai in everyday life ochre land Publishing.

الإلكتروني، بالإضافة إلى ذلك يمكن للجرائم السيبرانية أن تستفيد بشكل معقد من استخدام تقنيات الذكاء الاصطناعي للوصول إلى معلومات حساسة وتنفيذ هجمات إلكترونية متقدمة وفاعلة. ومع تطور التقنيات الحالية وسرعة التقدم في مجال الذكاء الاصطناعي، يزداد تعقيد الجرائم وصعوبات اكتشافها بصفة عامة، حيث يمكن أن يتم استخدام تقنيات الذكاء الاصطناعي لتضليل الأنظمة الأمنية وتشويه البيانات، وتخفيض مستوى توقعات الكشف عن الجرائم المرتكبة، وهذا بالتأكيد يشكل تحدياً للمؤسسات والأفراد الذين يعملون في مجال الأمن السيبراني لمواجهة هذه التهديدات المستمرة والمتطورة، لذلك ينبغي لنا أن نكون في حالة تأهب، وأن نعمل بقوة على تعزيز قدراتنا في مواجهة الجرائم المتعلقة بتقنيات الذكاء الاصطناعي. وعلى الصعيد الدولي يجب أن تتعاون الدول والمؤسسات والخبراء في مجال الأمن السيبراني من أجل ضمان الحماية الشاملة والفاعلة ضد هذه التهديدات الناشئة والخطيرة. فمن خلال العمل المشترك والتنسيق الدولي الوثيق، يمكننا تحقيق تقدم حقيقي في تأمين بيئة الإنترنت ومكافحة الجرائم التي تستهدف سلامتنا الرقمية على نطاق واسع ومستدام

يمكن أن يؤدي تطور التكنولوجيا والتقدم السريع في مجال الذكاء الاصطناعي إلى زيادة فرص ارتكاب الجرائم، حيث يمكن للمجرمين الاستفادة من تطبيقات الذكاء الاصطناعي في ارتكاب الجرائم دون ترك أي أثر رقمي وبشكل أكثر كفاءة، على سبيل المثال يمكن استخدام تطبيقات الذكاء الاصطناعي في تشفير البيانات وتجنب الكشف عن هوية المجرمين، وارتكاب الجرائم بصور مخفية، مما يعني أنه قد يصبح من الصعب على السلطات رصد وتحديد هوية المجرمين

بالإضافة إلى ذلك يمكن تطوير تقنيات الذكاء الاصطناعي لتفادي أنظمة الأمن وكسر القوانين بكل فاعلية، حيث يمكن أن تتكيّف هذه التطبيقات الذكية مع أي تحديثات أو تطورات في تقنيات الكشف عن الجرائم، وبهذا يصبح الكشف عن الجرائم المرتبطة بتقنيات الذكاء الاصطناعي تحدياً أمنياً وقانونياً أكبر، حيث يجب على السلطات العمل بجد لتطوير تقنيات جديدة وتحديث القوانين لمنع الاستغلال المتطور للذكاء

الاصطناعي في ممارسة الجرائم

تعتبر الجرائم المرتبطة بتطبيقات الذكاء الاصطناعي من أكثر أنواع الجرائم تطوراً مع التقدم التكنولوجي، حيث يمكن للمجرمين استخدام الذكاء الاصطناعي لتنفيذ أنشطتهم الإجرامية بشكل أكثر ذكاء ودقة. أحد الأمثلة المعروفة لهذا النوع من الجرائم هو استخدام تقنيات التلاعب بالبيانات للقيام بعمليات احتيالية، واختراق الأنظمة الأمنية والملفات الخاصة للشخصيات الهامة

وتؤكد بعض الدراسات الحديثة أن الجرائم السيبرانية التي يعاني منها العالم اليوم هي الأكثر تأثراً بالذكاء الاصطناعي؛ بما توفره التقنيات المتطورة لتعلم الآلة من خوارزميات تخفي الحقائق والصور والأدلة الجنائية.[42]

وقد لاحظنا خلال الأعوام الخمسة الماضية ارتفاعاً في الجرائم السيبرانية المرتكبة بطرق وأساليب معقدة، ومن أبرز نماذج تلك الجرائم:[43]

- هجمات « وانا كراي» التي ضربت (200000) جهاز حاسب آلي في (150) دولة عام 2017.
- تسجيل (1600) هجمة سيبرانية يومياً في المملكة العربية السعودية عام 8102.
- تعرّض هواتف نقالة لهجمات سيبرانية في الدول العربية بلغ عددها (86000) في دولة الإمارات، (220000) في مصر، (16000) في المملكة العربية السعودية و (150000) في سلطنة عمان خلال النصف الأول من العام 2022.
- هجمات سيبرانية سيطرت على مرافق حيوية في بعض الدول، حصل فيها الجناة على مبالغ ضخمة كفدية.44 وقد حجبت الدراسات أسماء تلك الدول.

---

42 - Nathali Rebe (2024) Artificial Intelligence: Crime, war and Justice Ethics. International Press. ISBN: 131804414842-978-.

43 - Ftima Khiralla (2022) Statistics of Cyber Crime From2016 to2020) International Journal of Computer Science Network'volum 9(5)2022).

44 - Gabriel Hallery (2018) Liability for crimes Involving Artificial Intelligence system Springer Publishing

من المتوقع أن تتضاعف تأثيرات مثل هذه النماذج من الجرائم السيبرانية متى تم تعزيز أساليبها بالذكاء الاصطناعي.

من الجرائم التقليدية والجرائم السيبرانية المتوقع تفاقمها وتضخيم خسائرها المالية ومخاطرها الأمنية باستخدام الذكاء الاصطناعي ما يلي:

1. نظم الاتصال لأبراج المراقبة الجوية وإعطاء أوامر من شأنها أن تسبب كوارث جوية.
2. استخدام بطاقات ائتمان مزورة لتمويل العمليات الإرهابية.
3. اختراق النظم المصرفية وتحويل الأموال.
4. تزييف العملات.
5. استخدام الهاتف النقال للإنترنت بأسماء مشفرة.
6. إرسال فيروسات تعطّل نظم المعلومات الحكومية.
7. الدخول على أنظمة المستشفيات وتعديل بيانات المرضى (جرعات علاج أعلى) بما يسبب الوفاة.
8. اختراق أنظمة الدولة وإعطاء أوامر بإصدار شيكات أو تمويل أموال للأفراد مما يضرّ الاقتصاد القومي.
9. إتلاف نظم الضرائب الحكومية.
10. التلاعب بنظم القطارات السريعة مما يؤدي إلى الاصطدامات.
11. الاستيلاء على نظم الاتصالات أو تعطيلها.
12. الاستيلاء على الاتصالات الفضائية ونشر بيانات مضللة.
13. الاعتداءات السياسية الإلكترونية.
14. اختراق وتتبع أنظمة الحكومات.
15. ميدان الحروب الرقمية.
16. جرائم القتل عن بعد.
17. جرائم إشانة السمعة.
18. اختراق إجراءات الانتخابات البرلمانية والرئاسية.

19. التسبب في حوادث مرور للمركبات المسيّرة.

20. تفجير المباني والمنشآت الحيوية عن بعد.45

ودعماً لما تقدم حول تأثيرات الذكاء الاصطناعي على ارتكاب الجريمة، تم استطلاع آراء (850) من الموظفين العاملين في مجال الخدمات والمعاملات الرقمية في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ في دولة الامارات العربية المتحدة للوقوف على آرائهم في هذا الشأن. وكانت النتيجة كالآتي

82.7 % من العينة أفاد بتأثير كبير على ارتكاب الجريمة

13 % من العينة أفاد بتأثير متوسط

4.3 % من العينة أفاد بتأثير ضئيل للذكاء الاصطناعي على الجريمة

45 - Bart Custers et al. opcit.

الفصل الثالث

دور الذكاء الاصطناعي في تحقيق العدالة الجنائية

يُقصد بنظام العدالة الجنائية العمليات والإجراءات والقوانين التي تنظم التعامل مع مرتكبي الجرائم وضحايا الجريمة، والأشياء المتعلقة بالجريمة في مراحل ما قبل ارتكاب الجريمة وأثناء ارتكاب الجريمة وبعد ارتكاب الجريمة، علاوة على الأجهزة الحكومية والأهلية المُناط بها تنفيذ القوانين الجنائية

عمليات وإجراءات العدالة الجنائية هي مكافحة الجريمة، واكتشاف ما يقع منها والتحقيق فيها ومحاكمة الجناة وتأهيل المذنبين وإنصاف الضحايا. أما الأجهزة المُناط بها تنفيذ عمليات وإجراءات العدالة الجنائية فهي أجهزة الشرطة والأمن والنيابة العامة، والمحاكم الجنائية والمؤسسات العقابية التي تعمل وفقاً للدستور والقوانين الجنائية والقوانين الخاصة المنظمة لتلك الأجهزة

ظلت نظم العدالة الجنائية تقوم بدورها منذ القدم، وفقاً لما توافر لها من إمكانات وموارد تطورت عبر التاريخ حتى بلغت مرحلة التقنيات الحديثة، والتحول الرقمي وأتمتة بعض عملياتها. وتأتي الآن مرحلة الذكاء الاصطناعي وإدخاله في العديد من عمليات الحياة اليومية، وعمليات العدالة الجنائية، حيث أصبح ضالعاً في مفاصل تلك العمليات.

للذكاء الاصطناعي آثار إيجابية بدأت تنعكس تدريجياً على نظم العدالة الجنائية من حيث الوقاية من الجريمة، والاكتشاف والتحقيق الجنائي، والمحاكمات الجنائية ومعاملة المذنبين في المؤسسات العقابية، وفيما يلي بيان لتلك الآثار

1. تأثيرات الذكاء الاصطناعي على الوقاية من الجريمة:

تعتبر الوقاية من الجريمة وانحراف الأحداث أهم وظائف نظام العدالة الجنائية وأقلها تكلفة وأكثرها إسعاداً للمجتمعات[46]. الوقاية من الجريمة هي أكبر نجاح يمكن أن تحققه الشرطة. وبما أن منع الجريمة قبل وقوعها يحتاج إلى تحليل بيانات هائلة

46 - Karen M. Erons (2013) Crime Prevention: Acritical introduction. sage publications.

حول الأشخاص والأشياء والظروف الاجتماعية، والتي كان من الصعب على الشرطة الاستفادة منها، أصبح الآن بفضل الذكاء الاصطناعي معالجة تلك البيانات الضخمة والوصول إلى الأشخاص الذين يخططون لارتكاب الجرائم، وكذلك التعرف على ضحايا الجريمة المحتملين، ومن ثم اتخاذ خطوات استباقية للوقاية وحماية الضحايا.

لقد أثبت الذكاء الاصطناعي تأثيرات موثّقة على الأنشطة الوقائية وخفض تكاليفها وجودة مخرجاتها ومن ذلك

أولاً ـ التنبؤ بالجريمة:

إن التنبؤ بالجريمة والانحراف واكتشاف الفئات الضعيفة المعرضة للجريمة، وكشف احتمالات المهددات الأمنية من أهم المهام وأكثرها صعوبة. فالتنبؤ ليس «رجماً بالغيب»، بل هو بحث وتحليل علمي لبيانات تاريخية كبيرة الحجم والوصول إلى حقائق معززة بالأرقام الدقيقة.[47]

ينظر الباحثون إلى دور الذكاء الاصطناعي في التنبؤ بالجريمة قبل وقوعها بوقت كافٍ، وهو أفضل دور ينبغي تطويره وتعزيزه بكافة الإمكانات، ولذا يعمل الباحثون في هذا المجال بقدر كبير من الجدية ويحققون تقدماً.[48]

ابتكر الباحثون في جامعة شيكاغو الأمريكية تقنية ذكاء اصطناعي قادرة على التنبؤ بالجرائم قبل أسبوع من حدوثها بمعدل من الدقة تجاوز 90%. قام فريق الباحثين المكون من الأستاذ «تشادوباداياي» والبروفسور «جيمس إيفانز»، والبروفسور «فيليب ديك» باستخدام البيانات التاريخية للجريمة المتاحة في سجلات الشرطة والقضاء في التنبؤ بالأحداث المستقبلية في مناطق حضرية محددة تبلغ مساحتها (10000) قدم مربع، وتمت قراءة هذه البيانات مع بيانات مماثلة في ثماني مدن أمريكية باستخدام تقنيات الذكاء الاصطناعي؛ للوصول إلى أنماط من الجرائم والتنبؤ بوقوعها في مناطق محددة وفي وقت معلوم مع كشف لصفات المجرمين المحتملين، وكذلك صفات

47 - Emirates Acdemy for Identity and Citizenship. (2022) Abu Dhabi: EAIC Publications.

48 - M.BOLDT (2024) Dp.cit.

الضحايا المحتملين والأشياء المستهدفة من الجناة

وتستخدم الشرطة اليابانية حالياً تقنية الذكاء الاصطناعي وفق نموذج مماثل لنموذج جامعة شيكاغو، وذلك فيما يتصل بتصميم وإدارة عمليات الشرطة الميدانية ودورياتها التي يتم إدارتها من غرفة المعلومات المركزية، وبإرشادات الذكاء الاصطناعي تتحرك دوريات الشرطة تلقائياً إلى المناطق الساخنة وتحول دون وقوع الجريمة.[49]

إن البيانات الكبيرة سابقة الذكر لا تقف في حدود اتخاذ القرارات أو وضع تدابير لمواجهة جريمة بعينها، بل تمتد إلى مساحات واسعة من الأنشطة الإجرامية والتحديات الأمنية والكوارث والأزمات القاهرة؛ الأمر الذي يستوجب دمج الذكاء الاصطناعي في كافة عمليات الشرطة والأمن، خاصة في مجال جرائم الإرهاب الدولي والجريمة المنظمة عبر الوطنية والجرائم السيبرانية والغش المالي.[50]

ثانياً ـ تحليل البيانات وتحديد المناطق الساخنة:

المناطق الساخنة Hot spots هي أجزاء محددة من منطقة جغرافية، قد تكون أكثر تضرراً من الجريمة والمهددات الأمنية لأسباب اجتماعية أو اقتصادية أو بيئية. ويشكل تحديد المناطق الساخنة وسيلة للتخطيط الاستباقي لعمليات الشرطة والأمن.[51]

ثالثاً ـ توزيع خدمات الشرطة والأمن:

يعتبر تحليل البيانات وتحديد النقاط الساخنة السالف بيانه هو مدخل أجهزة الشرطة والأمن في توزيع خدماتها وفقاً لاحتياجات المجتمعات المحلية وأولوياتها. كما أن تحديد النقاط الساخنة بتقنيات الذكاء الاصطناعي يوفر ربطاً بين كل منطقة ساخنة وظروفها من جهة، وبين خدمات الشرطة والأمن اللازمة من حيث كمِّها ونوعها وآلياتها.

رابعاً ـ رعاية الأحداث والفئات الضعيفة:

الأطفال وصغار السن والفئات الضعيفة في المجتمع، كالنساء والعجزة، هم الأكثر

49 - Hamid Jahankhani (2022) Policing in the Era of Ai and smart societies. Springer publications.

50- Christian Nwasike (2018) the Role Ai can play in Identifying and Flagging Financial Crimes. Kindle store.

51 - Emirate Academy for Identity and Citizenship (2022) Mapping Hot spots. Abu Dhabi: EAIC publications.

عرضة للتضرر من الجريمة، وهم الأقل قدرة على مواجهة المتغيرات الأمنية الحرجة. وفي ظل تطور تقنيات المعلومات والاتصالات الإلكترونية وانتشار ظاهرة اختراقات وسائط التواصل الاجتماعي قد تتعرض هذه الفئات الضعيفة لجرائم وانتهاكات لحقوقهم. وهنا يأتي دور الذكاء الاصطناعي في حماية هذه الفئات الضعيفة عن طريق حصرهم والتعرف على ظروفهم، وبالتالي متابعتهم وتوعيتهم والتدخل عند الضرورة لمساعدتهم.[52]

خامساً ـ مكافحة الفساد:

يشكل الفساد الإداري والمالي عبئاً على كثير من المجتمعات، خاصة في الدول النامية التي تضررت مواردها ومدخلات التنمية فيها بالفساد وسوء الإدارة. وبما أن عمليات وجرائم الفساد تُرتكب بدرجة عالية من السرية ونُهَج احتيالية يصعب كشفها يُنظر اليوم للذكاء الاصطناعي كأداة من أدوات مكافحة الفساد.

وقد أُفسِح المجال فعلاً لتقنيات الذكاء الاصطناعي للإسهام في مكافحة الفساد[53] إذ قام باحثون بتطوير نماذج حاسوبية تعتمد على شبكات عصبية اصطناعية بإمكانها أن تحدد المناطق والميادين والأعمال التي من المحتمل أن تنتشر فيها جرائم الفساد. وتمتد دور هذه النماذج إلى تتبع الأموال العامة ومشاريع التنمية وإجراءات تنفيذها بعيداً عن تدخل البشر

سادساً ـ مكافحة الإرهاب وغسل الأموال:

لم تحقق الجهود الوطنية والدولية النتائج المنشودة في مكافحة الإرهاب الدولي وغسل الأموال والاتجار بالبشر، برغم قناعة المجتمع بخطورة هذه الظواهر الإجرامية، وهنالك دراسات وبحوث تُجرى للوقوف على مدخلات وممكنات هذه الجرائم، وجمع بيانات ضخمة يتم تحليلها بتقنيات الذكاء الاصطناعي للتنبؤ بجرائم الإرهاب الدولي وغسل الأموال، والاتجار بالبشر وربطها ببعضها البعض، ومن ثم ربطها جغرافياً ومجتمعيّاً بالقدر

52 - Emirates Academy for Identity and Citizenship (2022), Ibid.

53 - 2 F.L Qureshi (2024) combatting corruption and Inefficiency in Pakistan power sector - Amazon Media EU.S..

الذي يساعد على صناعة القرارات الاستباقية التي تحول دون وقوع تلك الجرائم.[54]

2. تأثيرات الذكاء الاصطناعي على التحقيقات الجنائية:

حظيت التحقيقات الجنائية باهتمام أجهزة نظام العدالة الجنائية وأجهزة الشرطة والنيابات العامة على وجه الخصوص، باعتبار التحقيقات الجنائية هي مدخل العدالة الجنائية الناجزة والداعمة لتحقيق أهدافها.[55]

مع تطور أجهزة العدالة الجنائية الوقائية، شاهدنا أيضاً تطور الطرق والأساليب الفنية للتحقيقات الجنائية ومواكبتها لأساليب ارتكاب الجريمة وأنماطها.

في سبعينيات القرن العشرين ظهرت المختبرات الجنائية كنقلة علمية في اكتشاف الجرائم وتحليل الأدلة الجنائية واستنطاق مسرح الجريمة.[56] ومع بداية القرن الحادي والعشرين بدأت الدعوة إلى تطوير مختبرات الأدلة الجنائية المعززة بالذكاء الاصطناعي بهدف صناعة الأدلة الجنائية الرقمية بجمع وتحليل البيانات والمعلومات بتقنيات الذكاء الاصطناعي.[57] لقد كانت محاولات استخدام الذكاء الاصطناعي في مجال العدالة الجنائية متقدمة على كثير من الاستخدامات الراهنة للذكاء الاصطناعي. ومع تحديات جرائم تقنية المعلومات والاتصالات الإلكترونية وموجهات المعاهدات الدولية والتشريعات الوطنية التي عَرّفت وجرّمت الجرائم السيبرانية، ظهرت أساليب التحقيقات الجنائية الرقمية. (1) والتحقيقات الرقمية هي الإجراءات القانونية لفحص أجهزة الحاسب الآلي وملحقاتها وشبكات الإنترنت ووسائط الإعلام الاجتماعي، أو أية أوعية أخرى تُخزّن فيها الملفات الرقمية، ومن ثم استرجاع تلك المحتويات الرقمية وتحليلها واستنباط الأدلة الرقمية منها، واستخدامها في تحقيق العدالة الجنائية أو المدنية أو الشرعية أو الإدارية.[58]

54 - 1 Richard Bingley (2024) Combatting Cyber Terrorism: A Guide to Understanding cyber threat Landscape and Incident Response. IT Governance publishing.

55 - Institute for career Research (2024) Carees in forensic science. Amazon Media EU. S.

56- Marilyn T. Miller (2018) Crime scene investigation Laboratory Manual.Sage publications.

57 - Lan Walden, (2007) Computer Crime and Digital Investigations. New York: Oxford University press.

58 - 2 Mishera R.C (2005) Cyber Crime in The New Millerium. Delhi: Saujanya Books.

إن التحول الرقمي في المعاملات واعتماد عامة الناس على التعامل عبر الإنترنت وانتشار ما يعرف بالجرائم الرقمية، والإرهاب الرقمي والاختراقات السيبرانية؛ أصبح للتحقيقات الرقمية والأدلة الرقمية أهمية في الاكتشاف والتحقيق وضبط المجرمين. ولا شك أن تقنيات الذكاء الاصطناعي هي التي تفتح الآن الباب للتحقيقات الرقمية والأدلة الرقمية [59] لتأخذ مكانها المتقدم في عمليات نظم العدالة الجنائية

وعلى الرغم من الصعوبات المالية والمعوّقات القانونية وتراجع الكفاءات المهنية، تسعى أجهزة العدالة الجنائية إلى مضاعفة استخدام تقنيات الذكاء الاصطناعي في مختلف عمليات نظام العدالة الجنائية، وفي مختلف مراحل الجريمة، ابتداءً من قبل الحدث الإجرامي أو أثناء الحدث أو بعد الحدث. وفيما يلي نماذج من استخدامات الذكاء الاصطناعي في العدالة الجنائية:[60]

1. التحليل الرقمي:

تسمح تقنيات الذكاء الاصطناعي للشرطة بالتحليل الرقمي للصور وتحديد الأشخاص والأشياء، وفحص مسرح الجريمة وجمع الآثار، علاوة على تعديل وتوضيح الصور والأشياء غير الواضحة بما يساعد على التحقق من هوية الأشخاص

2. تحليل الحمض النووي:

وبالرغم من وجود معرفة الحمض النووي الشرعي منذ ثمانينيات القرن الماضي، إلا أن الذكاء الاصطناعي يسمح الآن للمختبرات الجنائية باكتشاف ومعالجة الحمض النووي ذات المستوى المنخفض أو غير القابلة للحياة. كما أصبح من الممكن بالذكاء الاصطناعي فك رموز كميات كبيرة من ملفات الحمض النووي والوصول إلى الحمض النووي للفرد

59- 1 Digital Evidence encompasses any and all digital data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator.

60- [2] Bart Custers and Eduard Fosch (2022) Law and Artificial Intelligence. springer. ASSERPress ISBN - 978 -945-522-6265-.

3. التعرف على الطلقات النارية:

تساعد تقنيات الذكاء الاصطناعي على فحص الطلقات النارية بطرق أكثر دقة مما كان معمولاً بها في المختبرات. فالذكاء الاصطناعي يكشف نمط الطلقات النارية ومصادرها واتجاهاتها وأصواتها ويُحدد موقع مطلق الطلقة

4. مضاهاة صور وجوه الأشخاص الذين يقومون بإحداث تغييرات على الوجه والتعرف على الصورة الأصلية.
5. تحليل بيانات ضخمة يتم جمعها من مسرح الجريمة وترجمتها إلى حقائق رقمية تشكّل أدلة مقبولة.
6. اكتشاف الاختراقات السيبرانية التي تؤثر على إجراءات التحقيقات الجنائية.
7. تعزيز رسالة التصنيف الحسابي Message digest algorithm، وهي مجموعة من الأحرف والأرقام المركبة بطريقة حسابية يمكن ترجمتها إلى كود محدد بالأرقام أشبه بقراءة بصمات الأصابع الرقمية Digital fingerprint.
8. حفظ وتأمين إجراءات التحقيق والأدلة الجنائية خلال جميع مراحل عمليات العدالة الجنائية بعيداً عن التأثيرات البشرية أو تعرضها للضياع والتلف.
9. المراقبة عن بعد للأشخاص والأشياء موضع التحقيقات الجنائية.
10. قراءة سلوك الإنسان ولغة الجسد أثناء الاستجواب والمقابلات مع المتهمين والشهود.[61]

3. تأثيرات الذكاء الاصطناعي على المحاكم الجنائية:

وفقاً لقوانين الإجراءات الجزائية، للمحاكم الجنائية مراحل معقدة من عمليات التقاضي، منها مرحلة الاتهام، الادعاء والتحقيقات القضائية الأولية ومراحل المحاكمات، والاستئنافات التي يتم فيها التدوين والتدقيق للشهادات والمرافعات وحصر الأدلة الجنائية، ومن ثم توصيف المعطيات بما يتواءم مع نصوص القانون. كل ذلك يمكن الآن تنفيذه بتقنيات الذكاء الاصطناعي مما يوفر العدالة ويُبعد فرص تحيز البشر

61 - 1 UDUAK Michael (2022) Forensic Investigation and Digital Footprint: Application of Genetics of finger print.

العاطفي في قرارات القضاء.[62]

لقد أصبح من المألوف استخدام تقنيات الذكاء الاصطناعي في المحاكم في كثير من دول العالم، العدالة الناجزة تستوجب سرعة الفصل في القضايا. وبما أن ضخامة المعلومات والبيانات التي تُعرض في قاعات المحاكم وبلورتها وفق القوانين تأخذ الوقت والجهد من المحاكم،[63] أصبح الآن بفضل الذكاء الاصطناعي من الممكن رصد وتحليل ما يجري في قاعات المحاكم وبلورتها وفق القانون في وقت وجيز يُعزز مقتضيات العدالة الناجزة

لم يكن استخدام الذكاء الاصطناعي في المحاكم الجنائية أمراً مفاجئاً، بل بدأ دخول التقنيات الرقمية إلى نظام العدالة الجنائية قبل عقدين من الزمان، تحت إطار نظام العدالة الإلكترونية القائمة على دمج التقنيات الحديثة في نظام العدالة الجنائية بصور متعددة، مثل تقديم خدمات المحاكم إلكترونياً واستخدام تقنيات الاتصالات الإلكترونية داخل قاعات المحاكم وتسوية المنازعات. وقد بلغ استخدام تقنيات المعلومات والاتصالات الإلكترونية مداه بدخول تقنيات الذكاء الاصطناعي مجال المحاكم الجنائية فيما عرف بالعدالة الجنائية الرقمية Digital criminal Justice والعدالة الجنائية التنبؤية Predictive criminal Justice التي تساعد المحاكم في تحليل السوابق القضائية والبيانات الاجتماعية لأطراف الجريمة وتقييم الأدلة الجنائية

من المؤمل أن تتقدم استخدامات الذكاء الاصطناعي في القضاء الجنائي إلى الاستفادة منه في البحث القانوني بإنشاء قواعد للبيانات القانونية الضخمة السارية على مستوى مختلف دول العالم.[64]

3. تأثيرات الذكاء الاصطناعي على عمليات المؤسسات العقابية:

شرعت بعض الدول في تطوير برامج الرعاية اللاحقة لنزلاء المؤسسات العقابية

62 - John Sammons and Lars Daniel (2017) Digital forensics Trail Graphic: Teaching the Jury through Effective use of Visuals. Sold by Amazon uk.

63 - 1 B. Clusters et.al (2022) P.410.

64 - 2 Emmanuel John Lutwick (2024) Ai and the Justice system: A strong Case. ISBN - 13: 978 – 1738309818.

باستخدام تقنيات الذكاء الاصطناعي بتحليل البيانات الكبيرة لنزلاء السجون وظروفهم توجهاتهم. وبناءً على نتائج تلك التحليلات يتم التأهيل والهندسة الاجتماعية بالقدر الذي يساعد المُفرّج عنه على الاندماج في المجتمع والانخراط في سوق العمل، مما يساعدهم في عدم عودتهم للجريمة. ولكن الأهم من ذلك هو استخدام الذكاء الاصطناعي في إدارة السجون، خاصة فيما يتصل بحسن توزيع النزلاء وفقاً لسلوكياتهم وتنظيم جداولهم اليومية ورصد تحركاتهم داخل السجون بالصوت والصورة عن بعد.[65] من أفضل تطبيقات الذكاء الاصطناعي هي التطبيقات الإدارية داخل المؤسسات العقابية للتعامل مع نزلاء السجون الخطرين والمصابين بأمراض معدية، وذلك باستخدام الروبوتات في خدمة النزلاء ومراقبتهم عن قرب والإبلاغ عن حالاتهم الصحية. وقد تم تطبيق نماذج من الخوارزميات في استخدام المسيرات والسيارات الصغيرة بدون قائد بشري في بعض الدول المتقدمة وحققت النجاح.[66]

65 - 1 Martha Henderson and Dena Hanley (2019) Correctional Administration and change Management. CRC Press.

66 - Ministry of Justice (2023) (white paper: correctional Institutions in Japan) Treatment of offenders in Central Fuchu prison. Japanese Government publications.

الفصل الرابع

النتائج والتوصيات

أولاً: نتائج البحث

وفقاً للأهداف التي طرحها البحث في فصله التمهيدي، نستطيع القول إن البحث قد حقق تلك الأهداف وتوصل إلى نتائج طيبة، ليس بسبب جهد الباحثين فحسب، بل بسبب توفر الدراسات والبحوث العلمية الحديثة والمواكبة للمستجدات المتسارعة لتقنيات الذكاء الاصطناعي، وبفضل ما يقدم في المؤتمرات بواسطة الذكاء الاصطناعي بالقدر الذي يمكّن من الحضور والمشاركة عن بعد. على سبيل المثال بلغ عدد المؤتمرات واللقاءات العلمية الدولية المنفذة عن بعد في كل من الولايات المتحدة الأمريكية والهند (304) مؤتمرات خلال النصف الأول من العام 2024. فيما يلي نوجز أهم النتائج التي توصل إليها هذا البحث وهي

1. من بين التعريفات المقدمة للذكاء الاصطناعي، وما يتفرع عنه من تقنيات بلغات مختلفة، توصل البحث إلى صياغة تعريف الذكاء الاصطناعي كالآتي:

(الذكاء الاصطناعي هو حقل من حقول المعرفة يهدف إلى صناعة آلات قادرة على القيام بمهام مطابقة تماماً للمهام التي تحتاج إلى ذكاء الإنسان)

كما عرّف البحث ثلاث تقنيات تتفرع عن الذكاء الاصطناعي وهي:

- تعلم الآلة.
- التعلم العميق.
- الذكاء الاصطناعي المولد.

2. حصر البحث مجالات استخدام الذكاء الاصطناعي في العالم الحقيقي موضحاً كيفية تسخير الذكاء الاصطناعي في العمليات والمعاملات الاجتماعية والاقتصادية والصناعية، بواسطة الجماعات والأفراد وخدمات القطاعين العام والخاص، مؤكداً

التقدم الإيجابي لتقنيات الذكاء الاصطناعي في مجالات الترفيه، والتعليم، والصحة والعناية الطبية والعلوم والأمن والدفاع.

3. سوف تصحب استخدامات الذكاء الاصطناعي مخاطر وتأثيرات سالبة خاصة في مجالات الأمن، والاقتصاد العالمي، والنزوح الوظيفي مع التركيز على نماذج من التأثيرات السالبة بعينها وهي:

- إحلال مكان البشر في الوظائف.
- انتهاك الخصوصيات من خلال استخدامات الذكاء الاصطناعي أمنياً.
- معضلة الأخلاقيات.
- العزلة الاجتماعية.
- تناول البحث بالفحص والمراجعة العميقة تأثيرات الذكاء الاصطناعي على الجريمة ونظم وأجهزة العدالة الجنائية في ثلاثة محاور على النحو التالي:

1. محور الوقاية من الجريمة والانحراف والمخاطر الأمنية، حيث أكد البحث أن الذكاء الاصطناعي أداة فاعلة في الوقاية من الجريمة والانحراف من خلال التنبؤ بالجريمة والمخاطر الأمنية التي يسببها البشر أو القوى القاهرة.

خلص البحث إلى أن تحليل البيانات الكبيرة بواسطة تقنيات الذكاء سوف يساعد على:

- التنبؤ بالمناطق الساخنة جنائياً وأمنياً.
- التعرف على الأشخاص المحتمل ارتكابهم الجريمة.
- التعرف على الأشخاص المحتمل تعرضهم للجريمة واتخاذ تدابير استباقية.
- مكافحة الفساد والإرهاب الدولي وغسل الأموال والاتجار بالبشر.

2. محور اكتشاف الجرائم والتحقيقات الرقمية، حيث يمكن تتبع المجرمين وضبطهم والتحقيق معهم بتقنيات الذكاء الاصطناعي من عدة زوايا، منها تحليل الصور والآثار والأدلة الرقمية، مضاهاة الصور، قراءة السلوكيات ولغة الجسد.

3. محور القضاء الجنائي وأجهزة العدالة الجنائية وعملياتها، حيث أصبح من الممكن بفضل الذكاء الاصطناعي تخفيف العبء على المحاكم الجنائية في حفظ وتوثيق وتحليل الأدلة، وضمان النزاهة واستبعاد التأثيرات البشرية العاطفية عن قرارات المحاكم وأجهزة الشرطة والنيابة.
4. بيّن البحث أهمية التشريعات الداعمة لاستخدامات الذكاء الاصطناعي في العدالة الجنائية، موفراً نماذج من المعاهدات الدولية والتشريعات الوطنية خاصة في دول المجلس الأوروبي والمملكة المتحدة. مؤكداً ضعف التشريعات الجنائية الحاكمة للذكاء الاصطناعي بشقيها الشكلي والموضوعي في الدول النامية والدول العربية على وجه الخصوص.
5. حول مستقبل الذكاء الاصطناعي في عمليات الشرطة والأمن، خلص البحث إلى أن استمرار تقدم تقنيات الذكاء الاصطناعي وتطورها، سيكون له تأثيرات كبيرة على مستقبل الشرطة وأجهزة الأمن الأخرى، ومراكزها التنسيقية على المستويات الإقليمية والدولية.

من المتوقع أن تنشأ منصات لمعلومات الذكاء الاصطناعي تسمح بالتعاون متعدد الوسائط خاصة فيما يتصل بمراقبة خدمات الشرطة في الوقت الفعلي والكشف عن التزييف العميق، ومراقبة مواقع الخلل في خدمات الصحة والأدوية وانتشار الأوبئة والأمن البيئي

6. خلص البحث إلى أن كثافة استخدامات الذكاء الاصطناعي في الحياة وتوفر تقنياته وبرامجها اللينة والصعبة في أسواق العالم المفتوحة تساعد على إساءة استخدام تقنيات الذكاء الاصطناعي. وقد ظهرت مقدمات لاستغلال المجرمين في ارتكاب الجرائم المالية، والغش والاحتيال والاختراقات السيبرانية وتضليل العدالة الجنائية بصناعة أدلة جنائية رقمية كاذبة.
7. قدم البحث قائمة بالجرائم المحتمل ارتكابها باستخدام الذكاء الاصطناعي، وهي جرائم تقليدية معززة بالذكاء الاصطناعي، والجرائم السيبرانية، والجرائم الجنسية الافتراضية

واختراق المعاملات المصرفية والحسابات البنكية.

ثانياً: التوصيات

يركز هذا البحث على توصيات غير تقليدية، ذات صبغة مستقبلية تمكّن الأجهزة المعنية بمواجهة الجريمة وتحقيق العدالة الجنائية من حسن استخدام الذكاء الاصطناعي والحد من مخاطره، وهي كالآتي:

1. التأهيل العلمي للعاملين في الشرطة والقضاء في مجال الذكاء الاصطناعي، وذلك بإدماج علوم الذكاء الاصطناعي في مناهج كليات القانون ومعاهد وأكاديميات الشرطة والأمن (للباحث منهاج مصمم كمساق تعليمي جامعي للراغبين في الإدماج).
2. تكليف مراكز البحوث الشرطية والأمنية والقضائية لتبني خطط مستقبلية للبحث العلمي في مجال الذكاء الاصطناعي واستخداماته، والمشاركة المكثفة في المؤتمرات العلمية الدولية، وتبادل الخبرات والمشاريع البحثية المشتركة مع الدول المتقدمة، خاصة الولايات المتحدة الأمريكية، والصين واليابان.
3. إنشاء كليات للأمن السيبراني والذكاء الاصطناعي في الجامعات، معززة بمختبرات الذكاء الاصطناعي ومختبرات الأدلة الرقمية (نموذج: كلية الأمن السيبراني والذكاء الاصطناعي- في جامعة طوكيو للهندسة)، وذلك لتأهيل كفاءات عربية عالية من المبرمجين قادرين على توطين صناعات الذكاء الاصطناعي ببرامجه الصعبة واللينة في الدول العربية؛ للتحكم على تسويق وحيازة منتجات الذكاء الاصطناعي كمتطلب من متطلبات الأمن القومي العربي.
4. تأثيرات الذكاء الاصطناعي تأثيرات أفقية تهم كافة عناصر المجتمعات، عليه من الموصي به تبني استراتيجية عملية لتوعية المجتمعات بتقنيات الذكاء الاصطناعي وإيجابيات ومخاطره.
5. تصور مبدئي لبناء القدرات للموارد البشرية العاملة في مواجهة الجريمة.

المراجع:

1. Keith J. Hayward and Matthias Maas (2020) Artificial Intelligence and Crime: A primer for Criminologists. Crime Maas, Sage.
2. Doo won Jong (2020) Artificial Intelligence Security threats, Crime, and Forensics: Taxonomy and Open issues. Digital objects identifier 10, 1109. IEEE Access.
3. The national council for crime prevention (2024) The Stockholm criminology symposium – Stockholm, bra-publications.
4. Jeremy Thorpe (2024) Crimes of the Future-Using AI – powered tools to identify Suspects-Amazon – UK.
5. Jon Adams (2024) AI Foundations of Generative AI: Easy to Read Guide – Green Mountain Computing.
6. Mohamed Elamin El Bushra (2024) Introduction to Criminal justice. Abu Dhabi. Emirates Academy for Identity and Citizenship.
7. Fanny Rainstorm (2021) How Capable is (AI) in Crime Prediction and prevention. Orebro University Press.
8. Keith J. Hayward and Matthias Maas (2020) Artificial Intelligence and Crime: A Primer for Criminologists Crime Media Culture. Sage.
9. Caldwell J.T. Andrews, T. Tanya and Griffin (2020). AI. Enabled Future Crimes. London: BMC available at \: www.Creativecamons. Org- revised 20-5-2024.

10. Down Jong (2020) Artificiality Intelligence Security Threats, Crime and Forensics: Taxonomy and Open Issues. IEEE Access.

11. Reza Mont sari, Victoria Carpenter and Anthony J. Masys. (2023) Digital Transformation in Policing: The Promise, Perils and Solution – springer. ISBN 978-3-031-09693-8.

12. Bart Custers, Eduard Frisch and Villanova (2022). Law and Artificial Intelligence: Regulating AI in Legal Practice, Asser Press. ISBN 978-94-6265-5225.

13. John Buyers (2023) AI: The Practical Legal Issues (3md, ed) Law Brief Publishing.

14. Ira Goel (2023) Introduction: AI and AI Governance. Printed by Amazon KDP.

15. Sydney Kramer (2024) Financial Crime AI: Harnessing Technology for Improved Fraud Detection – Amazon UK Publication.

16. Bufonid Ambert (2024) AI and Financial Crimes: How is improving Detection and Prevention. Amazon UK Publications.

17. Marie Enema (2024) Artificial Intelligence and National Security: Criminology Symposium Papers. Bra Publication.

18. Bartlomiej Oreziak (2024) Artificial Intelligence Justice in Poland: Use Case Stockholm Criminology Symposium. Bra Publication 13-6-2024.

19. Klava Faldt (2024) AI and Crime: Secret Data Reading. Stockholm Crimi-

nology Symposium Papers. University of Gothenburg Publication.

20. Marten Bolt (2024) A Data-drivingraph – based for hot spots Prediction: Use of Artificial Intelligence Stockholm Criminology Symposium Bra. Publication.

21. Eagan Casey, Digital Evidence and Computer Crime, London: Academic Press, 2000, P.260 Kyung-shick. Cyber criminology and Digital Investigation, FBI Scholarly Publishing.

22. Anthony Reyes, Kevin O'Shea, JIM Steele. Jon R. Hansen, Benjamin R. Jean and Thomas Ralph. Cyber Crime Investigations: Bridging the Gaps between Security Professionals Law Enforcement and Prosecutors. Syngress. Publishing 2015.

23. Darren R. Hayes. A practical Guide to Computer Forensics Investigations Pearson Education 2015.

24. Robert W, Taylor, Eric J. Fritsch, and John Lieder Bach. Digital Crime and Digital Terrorism. London, Pearson.2015.

25. Vasu, E-Crimes and Remedies. Delhi: Saujanya Books ,2005.

26. EURI, Briefing. No,34. E-Crime: New opportunity for partnership, 2002.M, Bri.

27. Reza Mont sari et.al (2023) op cit.

28. Keith J. Howard and Matthias Maas (2020) Artificial and Crime: A Primer

for Criminologists. Crime Media Culture. Sage.

29. Minsky M (1968) Semantic Information Processing. MIT Press. Cambridge.

30. Bellman R (1978) An Introduction to AI: Can Computer thin R? Boyd and faster. San Francisco.

31. Russel S, Nerving P, (2016) AI: A Modern Approach. Pearson Education Limited, Essex.

32. John Buyers (2023) AI: the practical Legal issues. Law Brief Publishing. ISBN-978-1-916698-14-7.

33. Ira Goel (2023) Introduction; AI and AI Governance. Amazon UK. ISBN 9798871709382-P.28.

34. A Aymen EL Amri (2024) Generative AI for the Rest of Us: your Future Decoded. Independently Published. ISBN13: 979-8322977049.

35. Harold Pearson (2022) Chat GPT Millionaire Bible: How AI Can Build you a Million-Dollar Business to become financially Free- Independently published. ISBN13:979-8858225690.

36. Interpol Innovative Center. (2023) Chat GPT: Impact on Law enforcement. www.Interpol.int/en.

37. Bartlomiej Oreziak (2024) OP cit.

38. B. Oreziak (2024) OP. Cit.

39. 39- B. Custers (2022) Op cit.

40. United Nations Interregional Crime and Justice Research Institution (2024). Responsible AI innovation in Law Enforcement (AI Tool Kit). Published by INTERPOL. (Funded by EU).

41. Gellers (2021) Rights for robots: Artificial Intelligence, animal and environmental Law. Tylor and Francis, Abingdon.

42. Custers (2022) op cit P.542.

43. Moritz Moser Bohm (2024) Navigating the Future of AI-the EU Act, www.pylhagoras-Solution.com.

44. Ai for Developing Countries Forum (2024) AI Justice for AU. AIFOD Vienna Forum Declaration.

45. Omar Santos and Peter Radanlier (2024) Beyond the Algorithm: AI, Security, Privacy and Ethics. Addison-Wesley.

46. Keith J. Hayward and M, Maas (2020) Op cit.

47. David Foster (2023) Generative Deep Learning: Teaching Machines to Paint, Write, Compose and Play. O Reilly Media Publication.

48. Christopher M. Bishop and Hugh Bishop (2023) Deep Learning: Foundations and Concepts. Springer Publications.

49. Shared Grande and Christian Ehl (2023) Generative AI: The Future of Everything. Independently Publishing.

50. Panchal Gupta (2023) Botnets and AI Uses' Black hat conference Paper Mandalay Bay Convention Center.

51. Lui HY (2021) "Ai challenges and the Inadequacy of human rights protection" criminal Justice Ethics 40:2-22.

52. Jennifer Garfinkel (2019) Gartner Survey of more than 3000 CIOs. Orlando. Gartner Symposium ITXPO 2019.

53. Server ion Global Solutions.www.serverion.com.

54. Reed Hosting's and Erin Meyer (2024) No Rules: Netflix and the Culture of Reinvention Allen Publications.

55. Kyle Balmer and Harminder Toor (2023) Chat GPT Business. Prompt Playbooks. Kindle Ed.

56. Joshua Arvin Lat (2021) Machine Learning:80 Proven recipes for date scientists and developers to perform machine learning experiments. Rackt Pup.

57. Shikhar Kwatra and bunny Kau struk (2024) Generative Ai with Amazon Bedrock: Build, scale and secure generative Ai Applications.

58. Tom Taulti (2019) Artificial Intelligence Basics: Anon-Technical Introduction.Apress. IsBN-13:978-1484250273.

59. Linda Jeering (2024) Artificial Intelligence in Everyday life. Independently published. ISBN:13-979B328308137.

60. Stuart Russell and Peter Norvig (2021) Artificial Intelligence: A modern Approach. Pearson Publications. ISBN-13:978-1292401133.

61. Fathi Salih Khalid (2023) The Future of Human Resource Management in the Ero of Artificial Intelligence. Barcode Publishing house.

62. Eben Estehuizen (2023) The A-Z of Ai use cases: An overiew of 63 ways that change the world. Business Development and Enterpreriership Books.

63. Matt Greenwood (2024) Artificial Intelligence: A practical Guide to using Ai in everyday life ochreland Publishing.

64. Nathalie Reba (2024) Artificial Intelligence: Crime, war and Justice Ethics. International Press. ISBN: 13-978-1804414842.

65. Ftima Khiralla (2022) Statistics of Cyber Crime From2016 to2020) International Journal of Computer Science Network'volum 9(5)2022).

66. Gabriel Halley (2018) Liability for crimes Involving Artificial Intelligence system Springer Publishing

67. Bart Custers et al. op cit.

68. Karen M. Eros (2013) Crime Prevention: Acritical introduction. Sage publications.

69. Emirates Academy for Identity and Citizenship. (2022) Abu Dhabi: EAIC Publications.

70. M. BOLDT (2024) op.cit.

71. Hamid Jahankhani (2022) Policing in the Era of Ai and smart societies. Springer publications.

72. Christian Nwasike (2018) the Role Ai can play in Identifying and Flagging Financial Crimes. Kindle store.

73. Emirate Academy for Identity and Citizenship (2022) Mapping Hot spots. Abu Dhabi: EAIC publications.

74. Emirates Academy for Identity and Citizenship (2022), Ibid.

75. F.L. Qureshi (2024) combatting corruption and Inefficiency in the Pakistan Power Sector - Amazon Media EU S.

76. Richard Bingley (2024) Combatting Cyber Terrorism: A Guide to Understanding cyber threat Landscape and Incident Response. IT Governance publishing.

77. Institute for career Research (2024) Careers in forensic science. Amazon Media EU. S.

78. Marilyn T. Miller (2018) Crime scene investigation Laboratory Manual. Sage publications.

79. Lan Walden, (2007) Computer Crime and Digital Investigations. New York: Oxford University press.

80. Mishera R.C (2005) Cyber Crime in the New Millerium. Delhi: Saujanya Books.

81. Digital Evidence encompasses any and all digital data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator.

82. Bart Casters and Eduard Foch (2022) Law and Artificial Intelligence. Springer. ASSER Press ISBN - 978 -94-6265-522-5.

بحث بعنوان:

دور تقنيات الذكاء الاصطناعي في تحقيق المواجهة الاستباقية لجرائم البيئة السيبرانية (دراسة استقرائية تحليلية)

الدكتور/ أحمد عبدالله أحمد الجراح

أستاذ القانون العام

أكاديمية الإمارات للهوية والجنسية

الملخص

تناولت هذه الدراسة موضوع المواجهة الاستباقية للجرائم السيبرانية في ظل ما يشهده العالم من تطور متسارع في التقنيات الرقمية، وما أفرزته البيئة السيبرانية من تهديدات مستحدثة ومعقدة تمس أمن المعلومات والبنى التحتية الحيوية للهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ بشكل خاص ولباقي مؤسسات الدولة. ولذلك هدفت الدراسة إلى توضيح مفهوم المواجهة الاستباقية لهذه الجرائم، واستعراض مدى الاستفادة من الوسائل الحديثة والتقنيات التنبؤية في التصدي لها، مع التركيز على دور الذكاء الاصطناعي في رصد الجرائم السيبرانية، وتحليل أنماط الهجمات والاختراقات المرتبطة بهذه التقنيات، وقياس كفاءة وفعالية الآليات الإجرائية المتبعة في مواجهتها

واعتمدت الدراسة على المنهج الاستقرائي والتحليلي لقراءة الواقع وتحليل التدابير المعمول بها، مع تقييم مدى توافقها مع المستجدات التكنولوجية والتهديدات الرقمية المتطورة. وسعت الدراسة إلى تقديم رؤية علمية تسهم في بناء منظومة أمنية استباقية متطورة، قادرة على حماية أمن الدولة ومؤسساتها من أخطار الجرائم الإلكترونية. وقد ارتكز التحليل على دراسة العلاقة بين تطور الذكاء الاصطناعي، ومساهمته في التنبؤ بالتهديدات، وتقديم حلول وقائية مدروسة تعزز قدرة أجهزة إنفاذ القانون.

وقد كشفت نتائج الدراسة عن أن الوقاية الاستباقية أصبحت خياراً استراتيجياً لا غنى عنه في السياسة الجنائية الحديثة، بالنظر إلى سرعة تنفيذ الجرائم السيبرانية وصعوبة اكتشاف مرتكبيها. كما أظهرت نتائج الدراسة أن استخدام الذكاء الاصطناعي في تحليل البيانات الضخمة، ورصد التهديدات، والتنبؤ بمواقع وأوقات وقوع الجريمة، يعزز من كفاءة الأجهزة الأمنية في التصدي للجرائم الرقمية، ويسهم في تقديم أدلة رقمية دقيقة تدعم العمل القضائي. وتبين أن الاختراقات والهجمات السيبرانية باتت تشكل تهديدًا وجوديًا على الأمن القومي، وهو ما يستدعي بناء استراتيجيات استباقية شاملة.

واستناداً إلى تلك النتائج، قدمت الدراسة مجموعة من التوصيات العملية، أبرزها: ضرورة تطوير وحدات متخصصة للتحليل التنبئي داخل الهيئة، وإنشاء منظومة وطنية متكاملة لرصد التهديدات السيبرانية في الزمن الحقيقي، إلى جانب تعزيز التعاون بين القطاعين العام والخاص، وإطلاق برامج تدريبية متقدمة للعاملين في مجال الأمن السيبراني. وتهدف هذه التوصيات إلى بناء منظومة أمنية مرنة ومتطورة قادرة على مجابهة التهديدات المستجدة بكفاءة

الكلمات المفتاحية:

الذكاء الاصطناعي، المواجهة الاستباقية، الجرائم السيبرانية.

Abstract

This study addresses the issue of proactive confrontation of cybercrimes in light of the rapid advancements in digital technologies and the emergence of complex, unprecedented threats posed by the cyber environment, which endanger information security and the critical infrastructure of states. Accordingly, the study aimed to clarify the concept of proactive confrontation of such crimes, examine the extent to which modern tools and predictive technologies are utilized to counter these threats, with a particular focus on the role of artificial intelligence in monitoring cybercrimes, analyzing attack patterns associated with these technologies, and evaluating the efficiency and effectiveness of the procedural mechanisms employed in combating them.

The study adopted both inductive and analytical approaches to examine the current reality and analyze the measures in place, assessing their alignment with technological developments and evolving digital threats. It sought to provide a scientific vision that contributes to building an advanced proactive security system capable of protecting the state's security and institutions from the risks of cybercrime. The analysis focused on exploring the relationship between the advancement of artificial intelligence, its contribution to threat prediction, and the provision of well-considered preventive solutions that enhance the capacity of law enforcement agencies.

The study's findings revealed that proactive prevention has become an indispensable strategic choice in modern criminal policy, given the speed at

which cybercrimes are committed and the difficulty of identifying perpetrators. The results also showed that utilizing artificial intelligence in big data analysis, threat detection, and crime location and timing prediction enhances the efficiency of security agencies in addressing digital crimes and provides precise digital evidence to support judicial processes. It was further evident that cyber intrusions and attacks have become an existential threat to national security, necessitating the development of comprehensive proactive strategies.

Based on these findings, the study presented a set of practical recommendations, most notably: the need to develop specialized predictive analysis units within law enforcement agencies, establish an integrated national system for real-time cyber threat monitoring, strengthen cooperation between the public and private sectors, and launch advanced training programs for cybersecurity personnel. These recommendations aim to build a flexible and advanced security system capable of effectively addressing emerging threats.

Keywords: artificial intelligence, proactive confrontation, cybercrimes.

مقدمة

في ظل التطور التكنولوجي الهائل في مجال تقنية المعلومات والاتصال واقتصاد المعرفة، وفي ظل الانفتاح المعلوماتي ظهرت أشكالاً عدة لجرائم البيئة السيبرانية وتوسع إطارها في الوقت الحاضر، كتوظيف البرامج المتطورة وتكنولوجيا الحوسبة السحابية وإنترنت الأشياء والبيانات الضخمة وخوارزميات الذكاء الاصطناعي في إحداث خلل واضطراب يهدد أفراد المجتمع وأمن مؤسساته، وتوظيف أدوات ذكية لإلحاق الضرر بالبُنى المعلوماتية للأشخاص والاتصالات وتعطيل الأجهزة والهيئات الحكومية والمرافق الاستراتيجية، بالإضافة إلى جرائم المحتوى التي تؤدي إلى التحريض ونشر المعلومات الزائفة، ونشر الشائعات التي تضر بمكانة وهيبة الدولة ومؤسساتها (عضيبات، 2023)

ويلاحظ أن التقدم التكنولوجي الهائل الذي وفرته الثورة المعلوماتية أحدث نقلة إيجابية نوعية في مسيرة البشرية، ولكنه في المقابل وفر أدوات تقنية مكنت المجرمين والعصابات المنظمة من ارتكاب العديد من الجرائم الإلكترونية التي تصاعد خطرها بشكل كبير على نحو يفرض ضرورة التعاون الجماعي لمواجهتها، حيث أصبحت الجرائم الإلكترونية أخطر من الجرائم التقليدية، نظراً لما تتميز به من سرعة الانتشار، وعدم السيطرة عليها وصعوبة إثباتها، كما لم تعد الوسائل التقليدية للكشف عن الجرائم صالحة في معظمها مع الجرائم التي ترتكب في البيئة السيبرانية (الجمل، 2018)

فالأصل أنه في أغلب أنواع الجرائم تكون الإجراءات العادية كافية لمواجهة الظاهرة الإجرامية، لكن استثناءً وفي بعض الحالات فإن اللجوء إلى إتباع إجراءات استباقية يكون فعالاً في الحد من آثار الظاهرة الإجرامية وسرعة السيطرة عليها، وذلك من خلال جمع البيانات حولها ووضع الخطط الكفيلة بالتقليل من أضرار الجرائم التي قد ترتكب في المستقل، حيث يكون استباقها أفضل من رد الفعل بعد ارتكابها والتبليغ عنها، بحيث أن يتم ذلك في إطار من الشرعية (روابح، 2020).

ومن هذا المنطلق، برزت أهمية الوقاية الجنائية الحديثة باعتبارها أحد الأساليب

الفعالة في السياسة الجنائية المعاصرة، حيث لم تعد مكافحة الجريمة تقتصر على الردع والعقاب بعد وقوع الفعل الإجرامي، بل امتدت لتشمل استراتيجيات وقائية تستند إلى التنبؤ بالمخاطر الإجرامية ومعالجتها قبل أن تتحول إلى واقع فعلي. وتقوم هذه الاستراتيجيات على استخدام التقنيات الحديثة في الرصد والتحليل، مثل أنظمة التحليل التنبؤي والذكاء الاصطناعي، بما يعزز قدرة الجهات المعنية على التدخل في الوقت المناسب وفق إطار قانوني يوازن بين حماية الأمن العام وضمان الحقوق والحريات (كاظم، 2024)

يسعى هذا البحث تقديم رؤية تحليلية استشرافية توضح الدور المحوري الذي تلعبه تقنيات الذكاء الاصطناعي في بناء منظومات امنية استباقية قادرة على رصد التهديدات والتنبؤ بها ، وتقديم حلول وقائية مدروسة تقلل من المخاطر السيبرانية .

وترتبط هذه الرؤية ارتباطا وثيقا باختصاصات الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ، باعتبار ان الهيئة مسؤولة عن حماية البيانات الشخصية، وتأمين المنافذ الحدودية، وضبط وتسجيل حركة الاشخاص والسلع. وتعتمد تحقيق أهدافها المؤسسية بشكل متزايد على منظومات رقمية تحتاج الى اعلى معايير الامان والاستجابة الاستباقية للتهديدات. لذلك تأتي اهمية هذا البحث من كونه يسهم في تقديم توصيات علمية وعملية تدعم المتطلبات المتجددة للهيئة بهدف حماية الامن الوطني وضمان استقرار المجتمع والدولة

- **مشكلة الدراسة:**

شهد العالم خلال العقود الأخيرة تحولاً جذرياً بفعل الثورة الرقمية الهائلة، التي أعادت تشكيل ملامح الحياة في شتى المجالات، وأسهمت في بروز أنماط جديدة ومعقدة من الجرائم. فقد أفرزت البيئة الرقمية وفي مقدمتها الفضاء السيبراني، بيئة خصبة لارتكاب الجرائم الإلكترونية، التي لم تعد مقتصرة على أعمال تقليدية كاختراق الأنظمة أو سرقة البيانات، بل تطورت لتشمل جرائم قائمة على استخدام تقنيات ذكية متقدمة، تتصدرها برمجيات الذكاء الاصطناعي، وهو ما جعل هذه الجرائم تمثل تهديداً

وجودياً لأمن المعلومات، بما في ذلك أمن مؤسساتها الحيوية والقطاعات الاقتصادية والاجتماعية كافة

وفي ظل هذا الواقع المتسارع، أضحت الجرائم السيبرانية القائمة على التقنيات الذكية، ولا سيما المدعومة بالذكاء الاصطناعي التوليدي، من أبرز التحديات الأمنية المعاصرة والمستقبلية. حيث أصبحت المؤسسات الأمنية تواجه نمطًا جديدًا من المجرمين الذين يوظفون هذه التقنيات المتقدمة في تنفيذ أنشطة غير مشروعة تتسم بالدقة والسرعة والقدرة على إخفاء الآثار الرقمية، مما يعقد من مهام الرصد والتحقيق والملاحقة. ومن هنا، تبرز الحاجة الماسة إلى تطوير منظومة متكاملة من الآليات والإجراءات الإجرائية الوقائية والاستباقية، القائمة على استثمار إمكانات الذكاء الاصطناعي، ليس فقط في كشف الجرائم بعد وقوعها، وإنما في رصد مؤشرات ارتكابها وتحليل الأنماط السلوكية الرقمية، بما يُمكّن من إحباط الهجمات الإلكترونية قبل تنفيذها، وتقليل آثارها المحتملة على أمن الدولة واستقرارها.

وتتمثل مشكلة الدراسة في غياب إطار إجرائي متكامل يوظف بفعالية التقنيات الذكية، وفي مقدمتها الذكاء الاصطناعي التوليدي، في المواجهة الاستباقية للجرائم الإلكترونية، بما يحدّ من الأخطار الناجمة عنها، ويعزز من قدرات المنظومة الأمنية في حماية الفضاء السيبراني. ويُثير هذا الواقع تساؤلاً حول مدى كفاية التدابير الحالية، وسبل تطويرها بما ينسجم مع حجم التهديدات الرقمية المستقبلية

- **تساؤلات الدراسة:**

يتمثل التساؤل الرئيسي لهذه الدراسة في: ما مدى فعالية المواجهة الاستباقية لجرائم البيئة السيبرانية المدعومة بتقنيات الذكاء الاصطناعي في الحد من الاختراقات والهجمات السيبرانية وحماية أمن المعلومات والبنى التحتية الحيوية للدولة؟ ويتفرع عنه التساؤلات الآتية

1. ما المقصود بالمواجهة الاستباقية لجرائم البيئة السيبرانية، وما هي أبعادها

ومكوناتها الرئيسية؟

2. إلى أي مدى يمكن الاستفادة من الوسائل الحديثة في التنبؤ بجرائم البيئة السيبرانية، وما هي أبرز هذه الوسائل؟
3. ما الدور الذي تؤديه تقنيات الذكاء الاصطناعي في رصد جرائم البيئة السيبرانية، وكيف تسهم في تعزيز الأمن السيبراني؟
4. ما هي أنماط الاختراقات والهجمات السيبرانية المرتبطة بتوظيف تقنيات الذكاء الاصطناعي، وما مدى كفاءة وفعالية الآليات الإجرائية المتبعة في مواجهتها؟

- **أهمية الدراسة:**

- **الأهمية العلمية:** تنبع الأهمية العلمية لهذه الدراسة من طبيعة موضوعها الذي يتناول أحد أبرز التحديات المعاصرة في ميدان الأمن السيبراني، والمتمثل في الجرائم الإلكترونية المدعومة بتقنيات الذكاء الاصطناعي. وتسهم الدراسة في إثراء المعرفة العلمية المتخصصة من خلال تسليط الضوء على الدور المحوري للإجراءات الإجرائية الاستباقية في التصدي لهذه الجرائم، واستكشاف آليات توظيف الذكاء الاصطناعي التوليدي كأداة متقدمة لرصد وتحليل التهديدات الرقمية قبل وقوعها. وتمثل الدراسة إضافة علمية نوعية، نظراً لندرة الدراسات العربية التي تناولت هذا الموضوع بالدراسة والتحليل، في ظل تسارع تطورات الثورة المعلوماتية، وظهور تقنيات ذكية ذات أثر بالغ على أمن المعلومات وحماية البنى التحتية الحيوية للدول.

- **الأهمية علمية:** أما على الصعيد العملي، فتكتسب الدراسة أهميتها من الحاجة الماسة إلى تقديم رؤى وتوصيات علمية قابلة للتطبيق تُمكن الجهات الأمنية والجهات المعنية، وصُناع ومتخذي القرار في المؤسسات الأمنية، من وضع سياسات وإجراءات أمنية استباقية فعالة للحد من مخاطر الهجمات السيبرانية والتقليل من آثارها السلبية. وتأتي هذه الدراسة لتدعم جهود بناء منظومة أمنية متطورة قادرة على حماية مؤسسات الدولة الحيوية، وضمان استقرارها في مواجهة التهديدات الإلكترونية المتزايدة التي باتت تمثل تهديداً فعلياً للأمن الوطني الشامل.

- **أهداف الدراسة:**

1. توضيح مفهوم المواجهة الاستباقية لجرائم البيئة السيبرانية.
2. الوقوف على مدى الاستفادة من الوسائل الحديثة في التنبؤ بجرائم البيئة السيبرانية.
3. استعراض دور تقنيات الذكاء الاصطناعي في رصد جرائم البيئة السيبرانية.
4. تحليل أنماط الاختراقات والهجمات السيبرانية المرتبطة بتوظيف تقنيات الذكاء الاصطناعي، والكشف عن مدى كفاءة وفعالية الآليات الإجرائية المتبعة في مواجهتها.

- **منهجية الدراسة:**

تعتمد هذه الدراسة على منهجين علميين متكاملين، هما: المنهج الاستقرائي والمنهج التحليلي. إذ يستند المنهج الاستقرائي إلى تتبع وتحليل المعطيات المرتبطة بالآليات والتدابير الاستباقية المعمول بها حاليًا في مواجهة الجرائم الإلكترونية في البيئة السيبرانية، مع رصد مدى توافقها مع المتغيرات التكنولوجية المستجدة. ويستخدم المنهج التحليلي في دراسة مدى فاعلية هذه التدابير والإجراءات في ضوء التطورات الهائلة في مجال تقنيات وبرامج الذكاء الاصطناعي، وما أفرزته من أنماط إجرامية متقدمة تصاعد خطرها على أمن المعلومات والبنى التحتية الحيوية للدولة. وتسعى الدراسة من خلال هذا الإطار المنهجي إلى تقديم تقييم علمي موضوعي للسياسات والإجراءات الأمنية المعتمدة، واقتراح رؤى عملية تسهم في بناء منظومة استباقية متطورة قادرة على حماية المصالح الوطنية، وصون أمن المجتمع ومؤسساته الأمنية والحكومية من أخطار الهجمات السيبرانية

- **المفاهيم الإجرائية للدراسة:**

- **المواجهة الاستباقية:** يقصد بها في هذه الدراسة التدابير والإجراءات القانونية والفنية التي يتم اتخاذها بشكل وقائي ومبكر باستخدام الوسائل التقنية الحديثة، وعلى رأسها تقنيات الذكاء الاصطناعي، بهدف رصد مؤشرات الجرائم السيبرانية قبل وقوعها، وتحليلها، والتصدي لها بما يحد من آثارها السلبية على أمن المعلومات والمصالح الحيوية للدولة.

- **الجرائم السيبرانية:** يقصد بها في هذه الدراسة كل سلوك غير مشروع يُرتكب عبر الفضاء السيبراني باستخدام التقنيات الرقمية أو الذكاء الاصطناعي، ويستهدف اختراق أو الإضرار بالأنظمة المعلوماتية أو البنى التحتية الحيوية، أو المساس بأمن المعلومات والبيانات الخاصة بالدولة أو الأفراد أو المؤسسات.

- **الدراسات السابقة:**

1. **دراسة Gurşu (2025) :** هدفت هذه الدراسة إلى استكشاف فعالية دمج الذكاء الاصطناعي مع استخبارات المصادر المفتوحة (OSINT) لرصد التهديدات السيبرانية بشكل استباقي، في بيئة تجريبية تحاكي شبكات دولية بما في ذلك بيئات الاتحاد الأوروبي وتركيا. اعتمدت الدراسة على تحليل بيانات تدفق الشبكة باستخدام خوارزميات تعلم آلي مثل Random Forest وLSTM وIsolation Forest، إلى جانب معالجة لغوية للبيانات المأخوذة من الإنترنت المظلم. أظهرت النتائج أن النظام نجح في تحقيق دقة عالية في الكشف المبكر، وتقليل معدلات الإيجابيات الكاذبة، وكشف أنماط هجمات جغرافية معقدة لا يمكن رصدها بسهولة بالأساليب التقليدية. وأوصت الدراسة بضرورة توسيع استخدام OSINT المدعوم بالذكاء الاصطناعي لتعزيز الرصد في الوقت الحقيقي، مع تحديثات مستمرة للنماذج المستخدمة لمواكبة تطور أساليب المهاجمين.
2. **دراسة (Smith 2025):** هدفت هذه الدراسة إلى تحليل وقياس أثر الذكاء الاصطناعي الوكيل (agentic AI) في دعم ممارسات الأمن السيبراني في بيئات مؤسساتية بالولايات المتحدة والمملكة المتحدة. ركزت الدراسة على كيفية مساهمة agentic AI في مراحل الإدراك، التفكير، اتخاذ القرار، والتنفيذ عند مواجهة التهديدات الرقمية. اعتمدت الدراسة على المنهج النظري المدعوم بتحليل سيناريوهات عملية ودراسات حالة لشركات تكنولوجيا وأمن معلومات كبرى. بينت النتائج أن هذه التقنيات عززت قدرة المؤسسات على الاستجابة الفورية للتهديدات، لكنها أظهرت أيضاً مخاطر جديدة مثل تحيز الخوارزميات وإمكانية ظهور سلوكيات

غير متوقعة. أوصت الدراسة بضرورة صياغة أطر حوكمة واضحة وآليات رقابية تقنية للحد من الآثار الجانبية للاعتماد المفرط على الذكاء الاصطناعي الوكيل.

3. **دراسة (Ferrag 2024):** هدفت هذه الدراسة إلى عرض أهم التطبيقات الأمنية ونقاط الضعف المرتبطة بنماذج اللغة الكبيرة (LLMs) التوليدية في الأمن السيبراني، ضمن مراجعة دولية شملت تجارب من أوروبا، الولايات المتحدة، ودول آسيوية. اعتمدت الدراسة على تحليل منهجي ونقدي لنتائج 42 نموذجاً من نماذج الذكاء التوليدي في مجالات كشف التسلل، التحليل الشرير، وتوليد استجابات تلقائية للحوادث. أظهرت النتائج أن هذه النماذج تقدم دقة كبيرة في التنبؤ بالهجمات وصياغة تقارير أمنية شاملة، لكنها في المقابل عرضة لهجمات مثل حقن الأوامر وتسمم البيانات، ما يجعلها أداة مزدوجة الحافة. أوصت الدراسة بتعزيز سلامة هذه النماذج باستخدام تقنيات مثل RLHF وأساليب hardening لتقليل المخاطر المحتملة.

4. **دراسة (Tripathi 2024):** هدفت هذه الدراسة إلى تحليل الاتجاهات الحديثة في مجال الذكاء الاصطناعي والأمن السيبراني، مركزة على بيئات التطبيق في الهند ودول جنوب شرق آسيا. وتحديد أبرز التحديات والفرص في هذا المجال للعام 2024. اعتمدت الدراسة على تحليل نظري مدعوم بإحصائيات قطاعية وشهادات خبراء من القطاعين العام والخاص. أظهرت النتائج أن المؤسسات في هذه الدول بدأت في تبني أنظمة ذكاء اصطناعي لتعزيز قدراتها الوقائية، لكنها تواجه معوقات تتعلق بنقص الكفاءات البشرية التقنية وصعوبة دمج الأنظمة الجديدة مع البنى التحتية القديمة. أوصت الدراسة بضرورة تعزيز التعاون بين القطاعين، واستثمار الجهود في بناء القدرات البشرية المتخصصة في الذكاء الاصطناعي والأمن السيبراني.

5. **دراسة (Islam 2024):** ركزت هذه الدراسة على تطبيق الذكاء الاصطناعي في إدارة الاستخبارات التهديدية للقطاعات الحيوية بدول مثل سنغافورة وماليزيا. اعتمدت الدراسة على تحليل بيانات واقعية من مؤسسات عاملة في قطاعات

الكهرباء، المياه، والاتصالات، واستخدمت تقنيات تعلم آلي ومعالجة لغوية في الزمن الفعلي لتحليل التهديدات. أظهرت النتائج أن دمج الذكاء الاصطناعي في هذه الأنظمة أدى إلى تقليل زمن الاستجابة للهجمات بشكل ملحوظ، وزيادة دقة التنبؤ بالمخاطر. أوصت الدراسة بضرورة تطوير أطر معيارية مشتركة لدعم التعاون بين مختلف القطاعات الحيوية، وتوسيع نطاق استخدام الذكاء الاصطناعي في مجالات أخرى.

6. **دراسة (Farzaan 2024):** سعت هذه الدراسة على تصميم نظام ذكي متكامل للكشف عن الحوادث السيبرانية والاستجابة لها في بيئات الحوسبة السحابية، مع التركيز على دول أوروبا الغربية والولايات المتحدة. استخدمت الدراسة خوارزميات تعلم عميق، مثل الشبكات العصبية وشجرة القرار، لتحليل حركة الشبكة والبرمجيات الضارة داخل بيئات Google Cloud وAzure. وأظهرت نتائج الدراسة أن النظام المقترح حقق دقة مرتفعة (90٪ في تصنيف التهديدات و96٪ في تحليل البرمجيات الضارة)، مع مرونة عالية في التوسع باستخدام الموارد السحابية. أوصت الدراسة بتطوير النظام ليشمل بيئات إنترنت الأشياء والأنظمة اللاسلكية، مع ضرورة تعزيز آليات التحديث التلقائي للخوارزميات الدفاعية.

- **التعليق على الدراسات السابقة:**

تتفق الدراسات السابقة بشكل عام مع الدراسة الحالية في تأكيد أهمية توظيف تقنيات الذكاء الاصطناعي في تعزيز قدرات المواجهة الاستباقية للجرائم السيبرانية، وفي التركيز على فعالية الأنظمة الذكية في الكشف المبكر عن التهديدات الرقمية والحد من آثارها. كما تشترك الدراسات السابقة مع الدراسة الحالية في إبراز الحاجة إلى دمج الذكاء الاصطناعي مع أنظمة أمنية تقليدية ومتقدمة، بما في ذلك أنظمة استخبارات التهديدات مثل دراسة Islam (2024)، ودراسة Gurşu (2025). وتوافقت كذلك على ضرورة وضع أطر ومعايير تنظيمية لضبط استخدام الذكاء الاصطناعي في الأمن السيبراني، كما في دراسة Smith (2025) وأهمية بناء القدرات البشرية لدعم

هـذه التقنيـات Tripathi (2024).

فـي المقابـل، تختلـف هـذه الدراسـات عـن الدراسـة الحاليـة فـي نطـاق التركيـز والمنظـور التحليلـي؛ إذ ركـزت معظـم الدراسـات علـى اسـتعراض نمـاذج تقنيـة أو تحليـل حـالات تطبيقيـة جزئيـة فـي قطاعـات معينـة (مثـل البنيـة التحتيـة للطاقـة، أو الحوسـبة السـحابية، أو بيئـات قطـاع خـاص)، بينمـا تتبنـى الدراسـة الحاليـة منظـوراً أوسـع وأشـمل مـن حيـث سـعيها إلـى تحليـل الآليـات الإجرائيـة الاسـتباقية فـي ضـوء تطـورات الـذكاء الاصطناعـي وتقييـم مـدى فعاليتهـا فـي حمايـة أمـن المعلومـات والبُنـى التحتيـة الحيويـة للدولـة علـى المسـتوى الوطنـي فـي دولـة الإمـارات، مـع اسـتعراض بعـض التجـارب الدوليـة، كمـا تنفـرد الدراسـة الحاليـة بدمـج البعـد القانونـي والإجرائـي الأمنـي بشـكل واضـح عنـد تقييـم تلـك الآليـات.

وتتميـز الدراسـة الحاليـة عـن الدراسـات السـابقة بأنهـا لا تكتفـي بتحليـل النمـاذج التقنيـة أو مراجعـة التطبيقـات المعتمـدة، بـل تسـعى إلـى تقديـم إطـار متكامـل للمواجهـة الاسـتباقية يربـط بيـن الجانـب التقنـي والجانـب الإجرائـي القانونـي، مـع التركيـز علـى البيئـة الأمنيـة فـي دولـة الإمـارات العربيـة المتحـدة بوجـه خـاص. كمـا تقـدم الدراسـة الحاليـة رؤيـة تحليليـة نقديـة للثغـرات القائمـة فـي التدابيـر الأمنيـة الحاليـة، وتطـرح مقترحـات عمليـة تسـهم فـي بنـاء منظومـة وقائيـة وطنيـة قـادرة علـى مواجهـة التهديـدات السـيبرانية المتنامية والمدعومـة بالـذكاء الاصطناعـي، وهـو مـا يمثـل إضافـة نوعيـة ومبتكـرة فـي مجـال الدراسـات العربيـة ذات الصلـة

- **خطة الدراسة:**

المبحث الأول: التقنيات الاستباقية لمواجهة جرائم البيئة السيبرانية

◊ **المطلب الأول:** مفهوم المواجهة الاستباقية وجرائم البيئة السيبرانية

◊ **المطلـب الثانـي:** الاتجاهـات التكنولوجيـة الحديثـة فـي التنبـؤ ورصـد جرائـم البيئـة السـيبرانية

المبحث الثاني: تعزيز أنظمة الذكاء الاصطناعي للكشف عن الجرائم السيبرانية

◊ **المطلب الأول:** الاختراقات والهجمات السيبرانية

◊ **المطلب الثاني:** تطبيقات الذكاء الاصطناعي في كشف الجرائم السيبرانية

الخاتمة (النتائج والتوصيات)

قائمة المراجع

المبحث الأول

التقنيات الاستباقية لمواجهة جرائم البيئة السيبرانية

تمهيد:

أصبحت التقنيات الحديثة تلعب دوراً حاسماً في تطوير استراتيجيات وسياسات الأمن السيبراني لمواجهة التهديدات الناتجة عن جرائم البيئة السيبرانية، ومنها استراتيجيات التحول من حالة الاستجابة إلى الحالة الاستباقية، حيث يتم التركيز فيها على الكشف المبكر عن التهديدات ومنعها قبل حدوثها، وأصبحت التقنيات المتقدمة تساهم في تحليل سجلات الأحداث والبيانات الضخمة لتحديد السلوك غير العادي والتهديدات المحتملة في البيئة السيبرانية بهدف الكشف عن الثغرات الأمنية والتهديدات المستقبلية المحتملة، بالإضافة إلى إنشاء نماذج تنبؤية لتحليل سلوك المجرمين في البيئة السيبرانية، وتحديد الأهداف المحتملة والأنماط الإجرامية المستحدثة (Patel,2023).

وعليه، فإنه باستخدام التقنيات الحديثة والمتطورة يمكن للأجهزة الشرطية تعزيز أمن الأنظمة السيبرانية وزيادة قدرتها على التصدي للجرائم المحتملة والمستقبلية في البيئة السيبرانية بطريقة استباقية. ولتوضيح ذلك سيتم تناول هذا المبحث من خلال المطلبين التاليين

- **المطلب الأول:** مفهوم المواجهة الاستباقية وجرائم البيئة السيبرانية.
- **المطلب الثاني:** الاتجاهات التكنولوجية الحديثة في التنبؤ ورصد جرائم البيئة السيبرانية.

المطلب الأول

مفهوم المواجهة الاستباقية وجرائم البيئة السيبرانية

إن الوقاية من الجريمة منهج جديد في السياسة الجنائية المعاصرة، لاسيما في ظل تزايد ارتكاب الجرائم في البيئة السيبرانية التي أصبحت تشكل خطراً على الفرد والمجتمع، وتتميز بكونها سريعة التنفيذ، وتتم بواسطة الأجهزة والتقنيات التي يصعب معها إثباتها أو اكتشاف مرتكبيها، لذا استوجب على الأجهزة الأمنية أن تكون سباقة في تعزيز منظومة الأمن السيبراني لتحقيق الفاعلية والكفاءة في مواجهة جرائم البيئة السيبرانية بكل أبعادها وأنواعها المستحدثة (كاظم، 2024).

ولتوضيح مفهوم المواجهة الاستباقية وجرائم البيئة السيبرانية، سيتم تناول هذا المطلب كالتالي

- **الفرع الأول: مفهوم المواجهة الاستباقية للجريمة.**
- **الفرع الثاني: مفهوم جرائم البيئة السيبرانية.**

الفرع الأول

مفهوم المواجهة الاستباقية للجريمة

كثيراً ما يترادف مصطلحي «الوقاية» و«الاستباقية» في سياق وضع الخطط الاستراتيجية طويلة المدى، حيث يرمز للمصطلحين في اللغة العربية بدلالتين قريبتين في المعنى، إذ نجد أن «الوقاية» تعني الحماية من الأخطار القادمة، أما «الاستباقية» فهي توقع خطوات أو سيناريوهات قادمة لوضع حلول لها. وبالتالي فإن الاستباقية خطوة تسبق الوقاية. أما الاستباقية في قاموس (Oxford, 2008) يقصد بها فعل شيء يمنع حدث معين من الوقوع أو التحضير له (سامي، 2020).

وعلى المستوى الاصطلاحي، فإنه تجدر الإشارة إلى أن ظهور مصطلح «الاستباقية» تزامن مع تطور الفكر الاستراتيجي الأمريكي عقد أحداث 11 سبتمبر 2001، وتبلور هذا المصطلح بالتزامن مع العقيدة الاستراتيجية الأمنية الأمريكية القائمة على التوقع والاحتواء والردع (مصباح، 2020)

ويلاحظ أن أغلب التعاريف لمصطلح «الاستباقية» ترتبط بالمفاهيم الأمنية العسكرية على وجه الخصوص، إذ يوجد مصطلح «الحرب الوقائية» وهو نوع من الحروب الهجومية دون الرد على هجوم مماثل، بما يرمز لاستخدام القوة كأداة دفاعية لدفع المخاطر (الحمادي، 2018).

وفي علم إدارة الشرطة يتم تعريف المواجهة الاستباقية بأنها نهج يركز على المستقبل الأمني، وخلق الأفكار الجديدة، ويكون هذا النهج بمثابة الإنذار المبكر للمشكلات الأمنية للعمل على تفاديها أو الحد من عواقبها، ويجب على المنظمة الأمنية أن تكون منفتحة على الفرص وتستغلها من خلال ميزة الاستباقية الناتجة عن التفاعل المستمر للمعلومات وتستجيب لها بشكل فعال (أبو حجير، 2019)

يتضح من تحليل التعريفات أن مفهوم الاستباقية قد نشأ بالأساس في السياقات العسكرية والأمنية التقليدية، حيث ارتبط بمفاهيم مثل «الحرب الوقائية» التي تعبّر عن

توجيه ضربات استباقية لدرء أخطار محتملة قبل وقوعها، حتى وإن لم يكن هناك هجوم فعلي مسبق. ويظهر ذلك كيف أن الاستباقية كانت تمارس تاريخياً كأداة دفاعية تقوم على استخدام القوة المبكرة لاحتواء المخاطر. ومع تطور العلوم الأمنية، ولا سيما في مجال إدارة الشرطة، تطوّر المفهوم ليأخذ بعدًا أكثر شمولية واستشرافية، فلم يعد مقتصراً على القوة، بل أصبح يعبر عن نهج إداري متكامل قائم على استبصار المستقبل، والتفاعل المستمر مع المعلومات، وصياغة استجابات ذكية تتيح منع التهديدات أو الحد من آثارها قبل وقوعها

ويبرز هذا التطور المفاهيمي أن الاستباقية لم تعد مجرد عمل وقائي محدود بنطاق عسكري، بل غدت ميزة استراتيجية تُمكن المنظمات الأمنية من تعزيز مرونتها في مواجهة المخاطر المستحدثة، لاسيما في البيئة الرقمية المعقدة. ويكشف ذلك عن الحاجة إلى إعادة تعريف المواجهة الاستباقية في ضوء التحديات السيبرانية المعاصرة، لتشمل الأبعاد التقنية والإجرائية والقانونية، والاستفادة من تقنيات الذكاء الاصطناعي بما يعزز قدرة الجهات الأمنية على توقع التهديدات السيبرانية والتعامل معها بكفاءة.

وبالتطرق للمعنى القانوني لمصطلح «المواجهة الاستباقية» يلاحظ أنه يشير إلى مجموعة من التدابير الوقائية، إذ يتم إضفاء الطابع القانوني عليها، وهي عملية وضع إجراءات تمنع فرد معين أو جماعات من ارتكاب فعل غير قانوني يتم تحديده من طرف المشرع لمواجهة الخطر الإجرامي المحتمل (العيداني، 2023). وهي مجموعة من التدابير والإجراءات التي يقرها المشرع، والتي بدورها تحول دون حدوث الجريمة، وهذه الإجراءات تعد جزء من السياسة الجنائية المناهضة للأسباب والعوامل التي تهيئ فرص ارتكاب الجريمة بصفتها ظاهرة اجتماعية تنتج عن عوامل ذاتية وأخرى بيئية يمكن اتخاذ تدابير وإجراءات وقائية للحد من خطورتها أو تحجيمها (الأعرج، 2022).

يستنتج الباحث مما تقدم أن مصطلح المواجهة الاستباقية يتميز بنوع من المطاطية، بحيث أنه علمياً يعد أحد مصطلحات الاستشراف المستقبلي نوعاً ما، أما عملياً فإن

بداياته كانت في المجال العسكري تحديداً بهدف منع وردع أي أخطار محتملة، وامتد هذا المصطلح إلى المنظمات الريادية التي تسعى إلى تحقيق الريادة التنافسية في مجال عملها. وعليه فإن ظهور مصطلح المواجهة الاستباقية للجريمة في مجال الأمن السيبراني ليس بغريب، كونه أحد المجالات المرتبطة بالأمن في الوقت الحالي الذي هو المجال الحيوي للمصطلح بالأساس، وهو ما اتجهت إليه الدول والمؤسسات الأمنية إلى وضع مجموعة من الاستراتيجيات الاستباقية لمواجهة الجريمة في البيئة السيبرانية.

ويعرف مصباح (2020) المواجهة الاستباقية للجريمة بأنها التصور الشامل للأهداف التي تكون قائمة في ذهن المخطط الأمني من أجل تحقيق الأمن والسلامة والاستقرار داخل المجتمع، وتعني كافة الوسائل والإجراءات الاحترازية التي يتم اتخاذها من قبل الدولة بسلطاتها المختلفة وأفراد المجتمع لغرض الوقاية الاستباقية من الجريمة وتأمين الضبط الاجتماعي وتوفير الرعاية المتكاملة لأفراد المجتمع. ويشير فيصل (2019) إلى أن الأساس الموضوعي للمواجهة الاستباقية للجريمة يكمن في تحييد الخطورة الإجرامية، والتي يقصد بها احتمال إقدام شخص على ارتكاب الجريمة

وتستهدف المواجهة الاستباقية تحديد الأساليب والوسائل المؤدية إلى تحقيق الأمن والسلامة في االمجتمع، مع إعطاء البعد الأمني لعتملية التنمية بكافة صورها، أي أن تتضمن المواجهة الاستباقية خطط التنمية الاجتماعية والاقتصادية والثقافية خططاً وقائية من الجريمة، بحيث تتم عملية الوقاية من الجريمة على أساس أنها جزء من السياسة الاجتماعية العامة وليس بشكل منعزل عنها، وذلك من أجل تحقيق الهدف الوقائي المتمثل في الشعور بالأمن والأمان في المجتمع (المصمودي، 2023).

من خلال ما سبق يمكن استنتاج تعريفاً للمواجهة الاستباقية للجريمة بأنها الدور الاستباقي للمشرع والجهات الأمنية والقضائية المختصة باعتماد مجموعة من الخطط والاستراتيجيات المستقبلية والوسائل والإجراءات التقنية والتشريعية الكفيلة لتأمين المصالح المحمية للأشخاص عن طريق تحييد الخطورة الإجرامية والتقليل من أضرار

الجرائم التي قد ترتكب في المستقل، حيث يكون استباقها أفضل من رد الفعل بعد ارتكابها والتبليغ عنها، بحيث أن يتم ذلك في إطار من الشرعية القانونية.

الفرع الثاني

مفهوم جرائم البيئة السيبرانية

يشير مصطلح «السيبرانية» الذي أضيف للأمن إلى خصوصية معينة له، لأنه ربما لارتباطه بحماية شبكات المعلومات الحاسوبية، والمواقع الإلكترونية، والأنظمة المعلوماتية، وشبكة الإنترنت، والبرامج المعلوماتية في الفضاء السيبراني من الهجمات السيبرانية، حتى أصبح يطلق على الأمن السيبراني بأنه قانون حماية الشبكات وأنظمة تكنولوجيا المعلومات والاتصالات (Naik,2022)

وباستقراء نص المادة (1) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية، يتضح أن المشرع الإماراتي لمن يتطرق إلى تعريف الأمن السيبراني صراحة على سبيل التحديد، إلا أنه أشار إلى تعريف «السيبراني» في الفقرة (5) من المادة (1) من المرسوم بقانون المشار إليه، بأنه: «كل ما يتعلق بالشبكات المعلوماتية الحاسوبية، وشبكة الإنترنت، والبرامج المعلوماتية المختلفة، وكل الخدمات التي تنفذها»، وتم تعريف «إلكتروني» في الفقرة (25) من ذات المادة بأنه: «ما يتصل بالتكنولوجيا الكهرومغناطيسية لإنشاء ومعالجة وتخزين وتبادل واستخدام نظم المعلومات الإلكترونية والبرامج المعلوماتية والمواقع الإلكترونية والشبكة المعلوماتية وأي وسيلة من وسائل تقنية المعلومات». وعليه، يتضح للباحث أن المشرع الإماراتي ميز بين «السيبراني»، و«الإلكتروني» في مجال تصنيف الجرائم الإلكترونية، وربما يكون مصطلح الإلكتروني أشمل وأعمق من السيبراني، حيث أن الإلكتروني يشكل كل ما يتعلق بالتكنولوجيا الكهرومغناطيسية أو الكهروضوئية أو الرقمية أو المؤتمتة أو ما شابه ذلك، أما السيبراني فيشمل كل ما يتعلق بالشبكات المعلوماتية والحاسوبية وشبكة الإنترنت والبرامج المعلوماتية المختلفة. ومن هذا المنطلق يمكن القول بأن كل جريمة

سيبرانية تعد جريمة إلكترونية، ليس كل جريمة إلكترونية تعتبر جريمة سيبرانية.

يعرف الأمن السيبراني بأنه أمن الشبكات والمعلومات والبيانات، والأنظمة المعلوماتية، والأجهزة المتصلة بالإنترنت، وهو المجال الذي يتعلق بإجراءات ومعايير ومقاييس الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات أو الحد من آثارها (فوزي، 2020). كما يعرف الأمن السيبراني بأنه نظام الدفاع ضد الهجمات الإلكترونية للأجهزة والشبكات والبرامج والعديد من أشكال البيانات المتصلة بالإنترنت، وذلك من خلال اتخاذ تدابير تمنع الوصول إلى البيانات الحساسة أو تحويلها أو حذفها أو التسبب في تعطيل ممارسات الأعمال القياسية (محسوب، 2022).

أما جرائم البيئة السيبرانية، فإنها من الجرائم التي تباينت واختلف تسمياتها، وتطورت بتطور التقنيات المرتبطة بها، حيث أطلق عليها في البداية مصطلح «إساءة استخدام الكمبيوتر»، ثم «جرائم الهاكرز»، وبعدها «جرائم الإنترنت والكمبيوتر»، وصولاً إلى الجرائم السيبرانية (عبدالعال، 2022)

ويلاحظ الباحث من خلال الإطلاع على التعريفات المختلفة للجريمة السيبرانية، أن الوقوف على تعريف لها يتوقف في المقام الأول على الغرض من استخدام المصطلح، فالجريمة السيبرانية الأساسية تتمثل في عدد محدود من الأعمال التي تمس بسرية البيانات أو النظم الحاسوبية وسلامتها من الاختراقات أو نحو ذلك. أما الأعمال المنفذة بواسطة الحواسيب والتي تهدف إلى تحقيق مكاسب شخصية أو مالية أو إحداث أضرار، والتي تندرج كلها ضمن نطاق أوسع من معنى مصطلح الجريمة السيبرانية، فلا يمكن تطويعها بسهولة لتنطوي ضمن تعاريف قانونية لمصطلح واحد وجامع

ونتيجة لحداثة جرائم البيئة السيبرانية وطورها، فإن فقهاء القانون لم يستقروا على تعريف واحد لهذه الجريمة، فقد عرفها الجمل (2018) بأنها «الجريمة التي تتم بواسطة الكمبيوتر أو أحد وسائل التقنية الحديثة على كمبيوتر أو أحد وسائل التقنية الحديثة الأخرى، مع ضرورة توفر شبكة اتصال فيما بينهما». وعرفها الدريني (2021) بأنها «نشاط

إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة، كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود». وعرفها عضيبات (2023) بأنها «السلوك غير المشروع أو المنافي للأخلاق أو غير المسموح به المرتبط بالشبكات المعلوماتية، وهي جرائم العصر الرقمي التي تطال المال والمعرفة والثقة والسمعة، وهي كلها تنفذ عن طريقة التقنية». وقد اتجه جانب من الفقه إلى اعتماد التعريف الذي تبنته منظمة التعاون الاقتصادي والتنمية Organization for Economic Co-operation and De-velopment (OCDE) في عام 2003 حيث عرفت الجريمة السيبرانية بأنها «كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات أو نقلها أو التعدي عليها» (مصباح، 2020).

يتضح للباحث أن التباين في تعريفات الجريمة السيبرانية يعكس مدى تعدد الأبعاد والسمات المميزة لهذا النمط المستحدث من الجرائم، والذي لا يزال في طور التشكل من منظور الفقه القانوني. ويلاحظ أن معظم التعريفات ركزت على ركن الوسيلة التقنية، سواء كانت الجريمة ترتكب باستخدام الحاسب الآلي أو أي وسيلة تقنية حديثة، مع توافر عنصر الاتصال الشبكي كشرط لازم (كما ذهب الجمل، 2018). في حين أضافت تعريفات أخرى، مثل تعريف الدريني (2021) وعضيبات (2023)، أبعاداً أوسع، شملت ليس فقط الوسيلة التقنية بل أيضاً طبيعة السلوك، وغاياته، ومدى تأثيره على القيم المحمية قانوناً مثل المال والمعرفة والسمعة والثقة. أما تعريف منظمة التعاون الاقتصادي والتنمية، فقد جاء أكثر شمولية، بإبرازه الطبيعة غير المشروعة أو غير الأخلاقية للسلوك، واتصاله بمعالجة البيانات أو نقلها أو التعدي عليها. ويكشف هذا التنوع في التعريفات عن غياب اتفاق فقهي حاسم حول تحديد إطار جامع مانع للجريمة السيبرانية، بما يعكس صعوبة الإحاطة الكاملة بطبيعة هذه الجرائم في ظل تطورها السريع وتعدد صورها وتقنياتها. وهو ما يبرز الحاجة إلى صياغة تعريف قانوني حديث ومرن يأخذ في اعتباره خصوصية الفضاء السيبراني، وتعدد الأهداف والوسائل التي ترتكب ضدها الجريمة

وعليه، يمكننا استنتاج تعريف شامل لجريمة البيئة السيبرانية بأنها: كل سلوك إجرامي عمدي أو غير مشروع يرتكب باستخدام التقنيات الحاسوبية الحديثة، أو الشبكات الإلكترونية، أو أنظمة التشغيل، أو البرمجيات المتطورة، أو أي من أدوات التكنولوجيا الرقمية، ويكون من شأن هذا السلوك استهداف البيانات أو المعلومات الحساسة أو ذات الطبيعة الاستراتيجية، بقصد الحصول عليها أو تعديلها أو نسخها أو إتلافها أو التلاعب بها، أو المساس بسريتها أو سلامتها أو توفرها، أو إيذاء الأفراد أو المؤسسات، أو الإضرار بالأنظمة المعلوماتية، أو المساس بالبنى التحتية الحيوية لمؤسسات الدولة، أو التعدي على حقوق الملكية الفكرية والاقتصادية، سواء ارتكبت الجريمة داخل الحدود الوطنية أو عبر الفضاء السيبراني

المطلب الثاني

الاتجاهات التكنولوجية الحديثة في التنبؤ ورصد جرائم البيئة السيبرانية

إن منع الجريمة بطريقة استباقية قبل أن تقع هو الغاية المنشودة لأي سياسة جنائية، ولذلك فإن الأجهزة الأمنية تحرص على استخدام المعطيات التكنولوجية المتاحة لسرعة الكشف عن الجريمة أو التنبؤ بها، وذلك بما أتاحته من إمكانيات جعلت تصدي الأجهزة الأمنية للجريمة أسهل وأدق من ذي قبل، كما أتاحت الوسائل المستحدثة إمكانية التنبؤ بالجريمة قبل وقوعها، وهو ما أخذت به العديد من الدول المتقدمة، علاوة على بعض الدول العربية التي قطعت شوطاً كبيراً في مجال الأخذ بالتكنولوجيا الحديثة في تعزيز الأمن والأمان، ومنها دولة الإمارات العربية المتحدة (عبد الحميد، 2019)

وترجع أهمية استخدام التقنيات الحديثة في العمل الأمني إلى دورها الفعال في تعزيز أداء العنصر البشري، بالإضافة إلى تعزيز قدرة هذه التقنيات على اكتشاف مواطن الخطر، ومن ثم سرعة القيام بعمليات المواجهة بالسرعة المناسبة ورفع الكفاءة وزيادة السيطرة والتحكم (البحيري، 2019)

وللوقوف على دور الاتجاهات التكنولوجية الحديثة في التنبؤ ورصد جرائم البيئة السيبرانية، سيتم تناول هذا المطلب على النحو الآتي

- **الفرع الأول:** مفهوم التنبؤ بالجرائم وأهميته في العمل الأمني.
- **الفرع الثاني:** دور الشرطة الاستباقية في التنبؤ ورصد الجرائم السيبرانية.

الفرع الأول

مفهوم التنبؤ بالجرائم وأهميته في العمل الأمني

يلاحظ إن مواجهة الشرطة للجرائم المختلفة، لا يمكن أن يعتمد على مهارة أو خبرة مسئول أو قائد، فسرعة إيقاع الجرائم السيبرانية على وجه الخصوص، وتعقدها وصعوبة إثباتها، وتشابكها، إلى جانب العديد من المتغيرات التي تخرج عن السيطرة، تجعل من المحتم الاعتماد على التنبؤ المستقبلي لتلك الجرائم عن طريق الاستعانة بالأساليب العلمية الحديثة في الإدارة والسيناريوهات المعدة لذلك، إلى جانب توظيف التكنولوجيا الحديثة في التنبؤ بها (Plotnek,2021).

وتم تعريف التنبؤ من وجهة نظر من يقومون بالملاحظة التدريجية وحساب معاملات الارتباط والانحدار بأنه «تقدير لما يمكن أن تكون عليه المشاهدات أو الظواهر إذ لم تتغير العوامل المؤثرة أو إذا تغيرت بالأسلوب والمعدل المتوقع» (الشامسي، 2022). وتم تعريف التنبؤ من وجهة الاعتماد على البيانات المتاحة بأنه «لا يعني في الحقيقة ما سيحدث في المستقبل تماماً، ولكنه يعني أننا سنصل إلى أقرب صورة لما يمكن أن يقع مستقبلاً اعتماداً على بيانات ومعلومات الماضي وما يلاحظ في الحاضر وباستخدام معادلة تبين الاتجاه العام لظاهرة معينة لاستخدامها للحصول على قيماً للمتغيرات في المستقبل» (الحسبان، 2022). يتضح من هذين التعريفين أنهما قدما صورة واقعية للتنبؤ، حيث اتضح أن التنبؤ لا يقر بما سيحدث في المستقبل تماماً، ولكنه يقدم صورة تقريبية من منطلق معطيات وبيانات الماضي والحاضر على افتراض أن هناك بعض المتغيرات تؤثر على الموقف الأمني

وعليه، يتضح من التعريفات السابقة أن التنبؤ لا يعني تقديم صورة محددة لما سيحدث في المستقبل، ولكنه مجرد مؤشرات لما ستبدو عليه الأحداث في الفترة القادمة

وفي ضوء التنبؤ بجرائم البيئة السيبرانية، فإن التحليلات التنبؤية تعد إحدى

استراتيجيات إنفاذ القانون لتحقيق الوقاية من وقوع الجريمة، ويتم ذلك من خلال جمع وتحليل البيانات متعددة المصادر، على أن تقوم الأساليب التنبؤية بتحديد الأنماط الإجرامية في البيئة السيبرانية، وإصدار التوصيات حول الأماكن التي يحتمل أن تقع فيها الجريمة السيبرانية، ويستتبع ذلك قيام الأجهزة الأمنية بتتبع حركة الجريمة، ومتابعة تغيراتها بمرور الوقت، ومن الممكن اكتشاف الأنماط الإجرامية والاتجاهات الجديدة غير المعروفة أو غير المتوقعة من الجرائم التي ترتكب في البيئة السيبرانية (الدريني، 2021).

حيث تشمل إجراءات التنبؤ بجرائم البيئة السيبرانية من خلال «رصد التهديدات والاستجابة لها» ثم جمع المعلومات عن التهديدات السيبرانية، وعمليات التصدي لها والتحليلات الجنائية، مما يتيح للأجهزة الأمنية إمكانية الحصول على رؤية متكاملة عن مشهد التهديدات المتطور باستمرار مع بيانات استباقية وعملية لمساعدته على اتخاذ قرارات وتنفيذ عمليات استجابة مدروسة (المصمودي، 2023)

وفي ضوء ما سبق، يمكن للباحث استنتاج أن التحليل التنبئي في البيئة السيبرانية يمثل أداة استراتيجية محورية في تعزيز قدرة أجهزة إنفاذ القانون على مواجهة الجرائم الرقمية بأسلوب استباقي وفعال، إذ لم تعد المواجهة الأمنية تقتصر على رد الفعل بعد وقوع الجريمة، بل باتت تعتمد على استثمار إمكانات الذكاء الاصطناعي والتحليلات المتقدمة لرصد التهديدات الناشئة، واكتشاف الأنماط الإجرامية الجديدة وغير المتوقعة، وتحديد مناطق الخطورة المحتملة قبل وقوع الجريمة. ويكشف هذا التوجه عن تحول جوهري في فلسفة العمل الأمني تجاه الجرائم السيبرانية، حيث أصبح جمع وتحليل البيانات من مصادر متعددة، وربطها بآليات اتخاذ القرار، أمراً بالغ الأهمية لتحقيق الوقاية وحماية البنية التحتية المعلوماتية للدولة. ومن هنا، تظهر الحاجة الماسة إلى تطوير منظومة أمنية متكاملة توظف التحليلات التنبؤية بشكل ممنهج، وتدمجها مع الإجراءات الإجرائية والقانونية، لضمان سرعة الاستجابة ودقة التصدي للتهديدات الرقمية في بيئة سيبرانية تتسم بالتعقيد والديناميكية المستمرة

ويعود السبب في استخدام التكنولوجيا الحديثة في التنبؤ بجرائم البيئة السيبرانية والوقاية منها – من وجهة نظرنا - إلى الحاجة الماسة لتفعيل قدرات البحث الجنائي للمواجهة الاستباقية لجرائم البيئة السيبرانية؛ لما تتسم به أنظمة التنبؤ من سرعة ودقة في الكشف عن تلك الجرائم، وكذلك المساهمة في تقديم أدلة قوية إلى جهات القضاء حول الجرائم المرتكبة، إلى جانب توفير معلومات ودلائل إلى الأجهزة الأمنية لكشف مرتكبي الجرائم السيبرانية المعقدة والعابرة للحدود

الفرع الثاني

دور الشرطة الاستباقية في التنبؤ ورصد الجرائم السيبرانية

يعد العمل الشرطي الاستباقي أسلوباً حديثاً لتنفيذ القانون، وقد تم استخدامها عند أول ظهور لها في المملكة المتحدة عام 1990م في مواجهة الجرائم المنظمة والخطيرة، وقد حثت النتائج الواعدة التي ظهرت في السنوات الأخيرة الجهات المختصة بإنفاذ القانون على توسيع نطاق المنهجية الاستباقية ليشمل نواحي إدارة الشرطة كنموذج عمل شامل، حيث يرتكز العمل الشرطي الاستباقي على التقييم والتجميع الممنهج للبيانات والمعلومات الإستراتيجية من خلال عملية تحليلية محددة تحولها إلى نتائج تحليلية إستراتيجية وتشغيلية تعمل كأساس لعملية صنع القرار المستند إلى دليل (Hughes,2019).

وللشرطة الاستباقية دورة تتكون من (6) خطوات قياسية لتحويل البيانات والمعلومات الأمنية الصريحة إلى معلومات أمنية إستراتيجية هادفة وموجهة لهدف ما، حيث تبدأ الخطوات بأحد القرارات أو التكليفات متبوعاً بمرحلة تخطيطية يشترك بعدها المحللون الأمنيون في جمع البيانات والمعلومات التي يجب تقييمها وفقاً لنظام تقييم معمول به، والخطوة التالية هي مرحلة المعالجة الفعلية والتي تبدأ بفحص البيانات والمعلومات المتاحة وهيكلتها، ومن ثم وضعها ضمن قاعدة بيانات، بعد ذلك يتم تحليل البيانات والمعلومات مما ينتج عنه الخروج بنتيجة للاستخبارات يتم مشاركتها مع الطرف الموكل

(القائد أو المحقق أو من يوكل إليه أمور التحليل الأمني) (Atymtayeva,2020)

حيث يعتبر جمع المعلومات للقيام بتنفيذ إجراءات أمنية استباقية عملية صعبة، فبينما يتحتم على المحللين والمخططين الأمنيين ضمان جمع بيانات كافية ودقيقة تغطي كافة جوانب المشكلة الأمنية أو الجريمة السيبرانية المطلوب تحليلها، سيكون عليهم أيضاً تجنب البيانات الزائدة وجمع معلومات غير ضرورية أو غير مناسبة، ولعل ما يشكل أهمية في هذه الخطوة هو دراية فريق العمل الأمني الاستباقي بكافة المصادر والهيئات التي يتم اختيارها لمهمة تجميع البيانات ومدى صلتها وسهولة الوصول إليها والاعتماد عليها، بالإضافة إلى الإلمام بأي قيود قانونية وشروط تنطبق على استخدام أنواع مختلفة من مصادر المعلومات، حيث تعتمد خطة تجميع البيانات على تعريف المهمة الأمنية، سواء كانت مواجهة استباقية لجريمة مرتكبة في البيئة السيبرانية أو مواجهة أحداث أمنية أخرى

يتضح للباحث أن العمل الشرطي الاستباقي يمثل نقلة نوعية في فلسفة إنفاذ القانون، حيث لم يعد يقتصر على الاستجابة للوقائع الإجرامية بعد وقوعها، بل أصبح يعتمد على منهجية علمية دقيقة تقوم على التقييم المنهجي للبيانات وتحويلها إلى استخبارات أمنية قابلة للتنفيذ. ويتبين أن نجاح المواجهة الشرطية الاستباقية، خاصة في الجرائم السيبرانية، يرتبط بقدرة الأجهزة الأمنية على تحقيق التوازن بين شمولية البيانات ودقتها من جهة، وتجنب التضخم المعلوماتي غير المجدي من جهة أخرى، إذ يتطلب ذلك من فرق العمل الاستباقي مهارات متقدمة في تحديد المصادر المناسبة، وضمان مصداقية وسلامة المعلومات المجمعة، مع الالتزام بالضوابط القانونية التي تحكم استخدامها. ومن هنا، يظهر بوضوح أن العمل الشرطي الاستباقي في البيئة السيبرانية لا يقتصر على الجانب الفني أو التقني، بل يتطلب تكاملاً بين البعد التحليلي، والإطار القانوني، والبنية المؤسسية الداعمة للتنفيذ على أرض الواقع.

وجدير بالذكر أن أجهزة الشرطة حول العالم تعاني مما قد يطلق عليه «تسونامي

البيانات Tsunami Of Data»، ويمكن خلال هذا الكم الهائل من تداول البيانات أن تكون المعلومات ذات الصلة بحدث أمني أو جريمة معينة معرضة بشكل متزايد لخطر الفقدان أو التلف، وهنا تظهر قيمة الأنظمة التنبؤية والتحليلات المنطقية الذكية Logical Analysis[67] التي تساعد الأجهزة الأمنية على فهم الظواهر الإجرامية وتقييم فعالية أساليب مكافحة الجريمة، حيث يمكن لتلك الأنظمة تحليل الوسائط الاجتماعية لكشف الروابط بين الأحداث والأفراد والأماكن والمركبات، فضلاً عن التقارير الآلية وتحديد أولويات توزيع الدوريات الأمنية للتعامل مع الأحداث المتوقعة (Chen,2020)

وفي إطار ذلك توجد العديد من البرامج التي تعتمد على التكنولوجيا الحديثة في التنبؤ بالجرائم، نذكر منها ما يلي

1. برنامج «هانش لاب HunchLab» للتنبؤ بالجرائم:

في عام 2013 قامت شرطة سانتا كروز بكاليفورنيا في الولايات المتحدة الأمريكية بالتعاون مع معهد دراسات الأمن الوطني باستحداث برنامج «هانش لاب Hunch-Lab» الذي يطبق خوارزميات تعلم الآلة والذكاء الاصطناعي للتنبؤ بانتشار أنواع من الجرائم، وتشمل هذه البيانات سجلات للبلاغات العامة عن الجريمة، وطلبات النجدة من الشرطة، والمواقع الجغرافية وتعتمد تقنية تعلم الآلة والذكاء الاصطناعي في هذا البرنامج على مجموعات من المتغيرات التي من شأنها أن تتنبأ على وجه الدقة بمواقع وأوقات حدوث الجريمة، ويمنح هذا النظام ثقلاً لأثر وتكرار حدوث أنواع الجرائم، ومدى فاعلية الدوريات الشرطية في منع حدوثها. كما تسمح أدوات البرنامج بتعديل أولويات دوريات الشرطة، من خلال إضافة قيود معينة، مثل عدد الضباط المتاحين أو المدة التي يستغرقها الضباط في المواقع المتنبأ بها في مقابل المدة التي يستغرقونها في

67 - التحليل المنطقي: هو التحليل الذي يساعد في اكتشاف وتفسير بيانات لها قيمة خاصة في المناطق الغنية بالمعلومات المسجلة، وتعتمد هذه التحليلات على التطبيق المتزامن للإحصاءات وبرمجة الحاسب الآلي وبحوث العمليات لقياس الأداء، حيث قد تطبق المنظمات التحليل المنطقي للبيانات التجارية بهدف تحسين أداء الأعمال والقدرات التنافسية التنبؤية وفي اتخاذ القرارات الصائبة. وتشير التحليلات الأمنية إلى تكنولوجيا المعلومات المتطورة لجمع وتحليل الأحداث الأمنية لفهم وتحليل الأحداث التي تشكل أكبر المخاطر. أنظر «التحليل المنطقي للبيانات»، متاح على الرابط: https://kalamfalsfa.wordpress.com/2020/03/28/ep58_logical_analysis/ تاريخ الاطلاع: 2024/11/6م

الاستجابة للبلاغات (Boccio,2019).

يتضح للباحث أن برنامج «هانش لاب» يعكس تجربة رائدة في توظيف الذكاء الاصطناعي لتحليل البيانات الشرطية والتنبؤ بمواقع الجرائم وأوقاتها بدقة، مما أسهم في تحسين توزيع الدوريات ورفع كفاءة الاستجابة الأمنية. ويوضح هذا النموذج أهمية بناء قرارات أمنية على أدلة وبيانات علمية، مع مراعاة المتغيرات التشغيلية مثل عدد الضباط وسرعة الانتشار. وتستلهم دراستي من هذا النموذج ضرورة تطوير أنظمة مماثلة في البيئة السيبرانية، تراعي خصوصية الجرائم الرقمية وطبيعتها العابرة للحدود، بما يعزز من قدرات المواجهة الاستباقية ويحقق حماية فعالة للبنى المعلوماتية الحيوية.

2. برنامج «بريدبول PredPol» للتنبؤ بالجرائم المحتملة:

في عام 2018 قامت شرطة لوس أنجلوس بالتعاون مع جامعة كاليفورنيا بإنشاء قاعدة بيانات أمنية ضخمة تحت مسمى «بريدبول PredPol» أو الشرطة التنبؤية وتعميمه على (50) إدارة وقسم شرطة، بهدف تحليل البيانات واستخلاص النتائج وإيجاد الارتباطات بين كميات كبيرة من البيانات التي لا يمكن للمحللين البشريين أن يتعاملوا معها، وعليه يتم إمداد أصحاب القرار معلومات عالية الدقة بتوقع الأوقات والأماكن التي يحتمل وقوع الجرائم فيها، وتحسين قرارات توزيع قوات الشرطة، مما ساهم في خفض نسبة ارتكاب جرائم العنف في الشوارع بنسبة 25%، ويعتمد هذا البرنامج على ثلاثة متغيرات، ألا وهي: نوع الجريمة، وتاريخ ووقت حدوثها، وموقعها، كما يقوم البرنامج بتطبيق خوارزميات تعلم الآلة والذكاء الاصطناعي للتنبؤ بانتشار أنواع الجرائم، وتشمل هذه البيانات سجلات للبلاغات العامة عن الجريمة وطلبات النجدة من الشرطة، وتعديل أولويات انتشار دوريات الشرطة من خلال إضافة قيود معينة، مثل عدد الضباط المتاحين أو المدة التي يستغرقها الضباط في المواقع المتنبأ بها في مقابل المدة التي يستغرقونها في الاستجابة للبلاغات (Chen,2020).

يتضح للباحث أن برنامج «بريدبول PredPol» يعتبر نموذجاً متقدماً لتطبيق الذكاء

الاصطناعي في العمل الشرطي، حيث أتاح تحليل كميات ضخمة من البيانات واستخلاص أنماط يصعب على المحللين البشريين التعامل معها، ما ساعد في تحسين توزيع القوات الأمنية وخفض جرائم العنف بشكل ملموس. ويبرز هذا النموذج أهمية الاستفادة من خوارزميات تعلم الآلة في التنبؤ بالمخاطر الأمنية المستقبلية

وفي عام 2018 دشنت القيادة العامة لشرطة أبوظبي منظومة مركز المدينة الآمنة، والتي تأتي ضمن أنظمة أمنية ومرورية تقوم على أسس التكامل والترابط، ضمن التقنيات التكنولوجية المتطورة، وتعد المدينة الآمنة مركزاً معلوماتياً متطوراً للتنبؤ الأمني والتصدي للجريمة، والرقابة الأمنية وتوزيع الدوريات، ورصد المركبات المطلوبة من خلال البرامج التي تقوم بتحليل البيانات المرورية باستمرار، وتعمل المدينة الآمنة كمركز استشعار مبكر من خلال ارتباطها مع المنظومة الوطنية للإنذار المبكر، وترسل التحذيرات للجمهور حول المخاطر والمهددات قبل وبعد وقوعها، باستخدام نظامي الاستشعار والبث والإرسال، في إرسال الرسائل المتغيرة والتحذيرية بتشكل الضباب والحوادث الجسيمة، وإغلاق الطرق، وذلك عبر الشاشات والرسائل عبر الهواتف المتحركة

(www.emaratalyoum.com).

يتضح للباحث أن المدينة الآمنة لشرطة أبوظبي تمثل نموذجاً متقدماً في توظيف التكنولوجيا الحديثة والذكاء الاصطناعي في العمل الأمني الاستباقي، حيث جمعت بين التنبؤ الأمني، وإدارة المخاطر، والرقابة المرورية ضمن منظومة متكاملة قائمة على تحليل البيانات الضخمة. ويبرز هذا النظام أهمية التكامل بين مراكز المعلومات والمنظومات الوطنية للإنذار المبكر لضمان سرعة الاستجابة للأحداث، وحماية الأرواح والممتلكات. ويتطلب ذلك تطوير حلول مماثلة في الفضاء السيبراني، قادرة على الاستشعار المبكر بالتهديدات الرقمية، وبناء استراتيجيات وقاية استباقية فعالة.

المبحث الثاني

تعزيز أنظمة الذكاء الاصطناعي للكشف عن الجرائم السيبرانية

تمهيد:

اتضح دور تقنيات الذكاء الاصطناعي في تطوير استراتيجيات الأمن السيبراني، والحد من الجرائم المرتكبة عبر البيئة السيبرانية من خلال الكشف عن التهديدات والاختراقات باستخدام تقنيات التعلم العميق وتحليل البيانات للكشف عن التهديدات السيبرانية والاختراقات المحتملة، ومراقبة الأنشطة غير المشروعة في الشبكة وتحليلها للكشف المبكر عن التهديدات والاستجابة السريعة، كما أن لتقنيات الذكاء الاصطناعي القدرة على تحليل ومعالجة البيانات الضخمة المتعلقة بالأمن السيبراني واستخلاص المعلومات الهامة من سجلات الأحداث والتقارير الأمنية وغيرها من المصادر والمعلومات الأمنية المتنوعة لتحليل الأنماط واكتشاف الثغرات والتهديدات المحتملة (البابلي، 2020).

وللتعرف على كيفية تعزيز أنظمة الذكاء الاصطناعي للكشف عن الجرائم السيبرانية، سيتم تناول هذا المبحث من خلال المطلبين التاليين

- **المطلب الأول:** الاختراقات والهجمات السيبرانية.
- **المطلب الثاني:** تطبيقات الذكاء الاصطناعي في كشف الجرائم السيبرانية.

المطلب الأول

الاختراقات والهجمات السيبرانية

تعتبر الاختراقات والهجمات السيبرانية من بين أهم المخاطر التي تواجه الأمن السيبراني، فضلاً عن كونها قد تقوم بتسريب معلومات سرية للدولة، إنها قد تلحق الضرر بمؤسسات ومرافق الدولة، أو خلق جانب من الفوضى وزعزعة الاستقرار والأمن بالدولة على كافة الأصعدة.

وخلال هذا المطلب سنوضح مفهوم الاختراقات والهجمات السيبرانية، والتعرف على أنواع وأساليب تنفيذ الهجمات السيبرانية، وذلك من خلال الفرعين التاليين:

- **الفرع الأول:** مفهوم الاختراقات والهجمات السيبرانية.
- **الفرع الثاني:** أنواع وأساليب تنفيذ الهجمات السيبرانية.

الفرع الأول

مفهوم الاختراقات والهجمات السيبرانية

الهجمات السيبرانية هي هجمات يتم تنفيذها بواسطة أجهزة الحاسوب عبر شبكات الانترنت والاتصالات الرقمية بهدف تغيير أو تعطيل برامج أو تدمير معطيات أو سرقة معلومات أو اختراق أنظمة التحكم والأوامر، والعمل على إحداث أضرار في أنظمة وبرامج وأجهزة الطرف الآخر وتعطيلها عن العمل، وغالباً ما تستهدف هذه الهجمات البنية التحتية للدول، ومحاولة إحداث أكبر الأضرار بها، وإصابتها بالشلل التام، كي تعجز عن تقديم الخدمات للسكان (داود، 2022)

كما يعرف الهجوم السيبراني بأنه عمل متعمد يقوم به مجرم إلكتروني أو أكثر لسرقة البيانات أو تلفيق المعلومات أو تعطيل الأنظمة الرقمية لأفراد أو منظمات بأكملها من خلال هجمات الأمن السيبراني، ويحصل مجرمو الإنترنت على وصول غير قانوني وغير مصرح به إلى واحد أو أكثر من أجهزة الكمبيوتر ليتم استخدامها فيما بعد وفقاً لأهدافهم الإجرامية (حسن، 2020)

يمكن للباحث استنتاج أن الهجمات السيبرانية لم تعد مجرد أفعال إجرامية تقنية عابرة، بل أصبحت تمثل أحد أخطر التهديدات الممنهجة الموجهة ضد أمن الدول واستقرارها، نظراً لاستهدافها المباشر للبنى التحتية الحيوية ومحاولتها شل قدرة الأنظمة والمؤسسات على تقديم الخدمات الأساسية للسكان. ويظهر تحليل التعريفات السابقة أن هذه الهجمات تتسم بتعدد صورها وأهدافها، حيث تتراوح بين سرقة البيانات وتلفيق المعلومات وتعطيل الأنظمة إلى السعي المتعمد لإحداث أضرار استراتيجية تطال الأمن القومي. كما يؤكد ذلك الحاجة إلى تطوير سياسات أمنية واستراتيجيات استباقية متقدمة تقوم على التنبؤ المبكر بهذه الهجمات، ورصدها وتحليلها بشكل دقيق، بما يتيح للأجهزة الأمنية التعامل معها بفعالية، والحد من آثارها المدمرة على

الأمـن الوطنـي والاقتصـادي والاجتماعـي

والهدف الرئيسي للهجوم السيبراني هو تدمير المعلومات المهمة وإلحاق خسائر بالدول ومؤسساتها، حيث تختلف أهداف الهجمات السيبرانية من شخص لآخر، ومن منظمة إلى أخرى، فعلى سبيل المثال يهاجم العديد من المتسللين الأفراد أجهزة الكمبيوتر الخاصة بالمؤسسات أو الأفراد الآخرين للحصول على مزايا مالية. وقد تسرق بعض المؤسسات التي ترعاها الحكومة المعادية معلومات تساهم في تدمير إمكانيات أو تضر بجاهزيته وقدرته على الاستعداد (النقبي، 2022).

وما يجعل الهجوم السيبراني ناجحاً هو الاختراقات الفنية الرئيسية التالية: (القضاة، 2022)

1. **خرق السرية:** يحدث خرق السرية عندما تكون المعلومات الشخصية للبيانات المقدمة لعملاء المؤسسة بموجب اتفاقيات لحماية سرية بيانات معينة، ثم يتم الإفصاح عنها إلى طرف ثالث دون الحصول على موافقة من العميل، وقد يهاجم المتسلل بيانات العميل المخزنة على خادم تابع لمؤسسة ما، ويتم ذلك من خلال طرق متعددة للوصول إلى المعلومات، والتي تم تقديمها للمؤسسة وفق اتفاقية حماية السرية، مما قد يؤدي إلى إلحاق خسائر مالية بالعميل، والشعور بعدم الأمان. ويحدث خرق السرية في بعض الأحيان من خلال القرصنة الإلكترونية للبيانات السرية الممثلة في (الملكية الفكرية، معلومات الهوية الشخصية، معلومات بطاقة الائتمان، معلومات الحساب المصرفي، المعلومات الصحية الشخصية، الأسرار التجارية).
2. **خرق التوافر (الإتاحة):** يحدث خرق الإتاحة عندما يتعذر على المستخدم المصرح له الوصول إلى الخدمات عبر الإنترنت أو المعلومات الشخصية المصرح له، وتتم الأنشطة الخبيثة الرئيسية المستخدمة لتعطيل توفر الخدمات أو المعلومات من خلال اختراق الشبكة بمجرد أن ينجح المتسلل في التطفل على الشبكة، فإنه ينشئ أدوات للسيطرة على الخوادم بشكل غير قانوني، ويرفض الوصول المصرح به

للمستخدمين الشرعيين إلى الموارد أو الخدمات، وتشمل المصادر الرئيسية لخرق التوافر في فشل عمل الأجهزة والبرامج.

يتضح للباحث مما تقدم أن نجاح الهجمات السيبرانية لا يرتبط فقط بوجود ثغرات تقنية، بل يقوم على استغلال نقاط ضعف حرجة تمس جوهر أمن المعلومات، وهي السرية والتوافر، إذ يمثل خرق السرية انتهاكاً خطيراً لثقة الأفراد والمؤسسات، ويؤدي إلى خسائر مالية ومعنوية جسيمة، بينما يعكس خرق التوافر تأثير الهجوم على استمرارية تقديم الخدمات، مما يحدث شللاً في الأنشطة الحيوية ويهدد الأمن المجتمعي والاقتصادي. ويبرز ذلك الحاجة إلى تطوير حلول استباقية متكاملة لا تكتفي بالكشف عن الهجمات بعد وقوعها، بل تركز على تعزيز قدرة الأنظمة على الصمود ومنع استغلال هذه الاختراقات منذ البداية، عبر تقديم تصور علمي وعملي لدور الذكاء الاصطناعي في تحقيق هذه الغاية.

وتتنوع الأدوات التي يتم من خلالها تنفيذ الهجمات السيبرانية، حيث تشمل الفيروسات أو «الديدان الإلكترونية»، والتطبيقات السرية المعروفة تحت مسمى «الأبواب الخلفية» أو برامج «حجب الخدمة» وغيرها من البرمجيات الفيروسية التي تستهدف زعزعة أو شل الهدف أياً كان، سواء أكانت فرداً أم مجموعة من الأفراد أم منظمة أو وكالة حكومية أو جهة رسمية (المعايطة، 2020).

كما تتنوع الجهات التي تقف وراء ظاهرة تنامي الاختراقات والهجمات السيبرانية على الصعيد العالمي في الآونة الأخيرة، وتشمل ما يلي: (عبد العال، 2022)

1. الدول التي تمتلك قدرات تقنية وتكنولوجية متطورة تتيح لها توظيفها في القيام بهجمات سيبرانية في مواجهة خصومها سواء لأغراض عسكرية (تدمير منشآت – وقف مشروعات) أو تجسسية كالحصول على معلومات أو إحداث تدمير في البنية التحتية الأساسية، كشبكات الكهرباء والمياه والمواصلات والاتصالات.
2. عصابات الجريمة المنظمة، والتي غالباً ما تلجأ إلى الهجمات السيبرانية للحصول

على فدية مالية، وتلجأ في ذلك إلى اختراق أنظمة المعلومات التي تدير الخدمات الأساسية في بعض الدول، لمساومتها للحصول على مبالغ مالية.

3. القراصنة من الأشخاص العاديين والذين يمتلكون مهارات تقنية فائقة، يتم توظيفها في الحصول على مبالغ مالية أو في اختراق الأمن المعلوماتي للدول، والحصول على معلومات حساسة.

يتضح للباحث مما سبق أن الهجمات السيبرانية تتسم بتعدد أدواتها وتنوع الجهات الفاعلة التي تقف وراءها، مما يعقّد من جهود المواجهة الأمنية ويتطلب مقاربات أكثر شمولية واستباقية، إذ إن استخدام أدوات متقدمة مثل الفيروسات، والديدان الإلكترونية، والأبواب الخلفية، وبرامج حجب الخدمة، يعكس مدى تطور الوسائل التقنية التي تستهدف تعطيل أو شل البنى التحتية، وإلحاق الأضرار بالأفراد والمؤسسات على حد سواء. كما يرى الباحث أن تنوع منفذي الهجمات السيبرانية بين دول تمتلك قدرات تقنية متقدمة، وعصابات الجريمة المنظمة، والقراصنة الأفراد ذوي المهارات العالية، يُظهر الطبيعة المركبة للتهديدات السيبرانية وامتدادها عبر مستويات متعددة، بدءًا من الهجمات ذات الطابع العسكري والسياسي، وصولًا إلى الهجمات ذات الطابع المالي أو التجسسي

ومن هنا يمكن للباحث التأكيد على أن فعالية المواجهة الأمنية لهذه التهديدات لا يمكن أن تتحقق إلا من خلال بناء منظومة متكاملة تستند إلى التحليل التنبئي، وتوظيف الذكاء الاصطناعي لرصد أنماط الهجمات وأدواتها، مع التفرقة بين طبيعة الجهات المهاجمة ودوافعها، كما تؤكد هذه المعطيات ضرورة تبني استراتيجيات أمنية مرنة قادرة على التكيف مع التهديدات المتغيرة، وتطوير قدرات استباقية شاملة تجمع بين البعد التقني، والإجرائي، والقانوني لتعزيز أمن المعلومات وحماية البنى التحتية الحيوية.

الفرع الثاني

أنواع وأساليب تنفيذ الهجمات السيبرانية

هناك عدة أنواع للهجمات السيبرانية، بصفة عامة، لعل أبرزها ما يلي:

1. التجسس باستخدام الفيروسات، وذلك بهدف سرقة المعلومات السرية التي لم يتم تأمينها بشكل صحيح، والتي يمكن أن يتم اعتراضها أيضا وقرصنتها، والمثال على ذلك الهجوم السيبراني الذي تعرضت له الولايات المتحدة الأمريكية في شهر ديسمبر 2020، والذي نجح في اختراق مؤسسات حيوية وحساسة كوزارات الدفاع والخارجية والخزانة والتجارة والطاقة والأمن الداخلي، وعدداً من الوكالات الفيدرالية الرسمية ومراكز الأبحاث والمنظمات غير الحكومية. وتكمن خطورة هذه النوعية من الهجمات أنها تمثل تهديداً كبيراً وجدياً للأمن القومي للدول المختلفة، المتقدمة منها والنامية، خاصة أن الهدف منها يكون في الأغلب هو اختراق نظم حماية وتأمين الشبكات الإلكترونية لهذه المؤسسات، والتجسس عليها ونقل المعلومات منها بواسطة استخدام برامج خبيثة (النقبي، 2022).
2. استهداف البنى التحتية الحساسة كمحطات الطاقة وتوزيع المياه وأنابيب النفط والاتصالات ووسائل النقل والمستشفيات، بهدف تعطيلها التام عن العمل، والمثال على ذلك الهجوم السيبراني الذي استهدف خط أنابيب نفط «كولونيال بايبلاين» في الساحل الشرقي بالولايات المتحدة في شهر مايو 2021، وأدى إلى نقص واسع النطاق في إمدادات الطاقة بجميع أنحاء الولايات المتحدة، خاصة أن هذا الخط ينقل ما لا يقل عن 45 % من البنزين والديزل والكيروسين الأمريكي من مصافي التكرير في خليج المكسيك إلى الساحل الشرقي للولايات المتحدة. ووفقا للشرطة الفيدرالية، فقد نفذت مجموعة «دارك سايد DarkSide» الإجرامية هذا الهجوم السيبراني باستخدام برنامج فدية (القضاة، 2022).
3. الهجمات السيبرانية التي تستهدف المنشآت ذات الطابع العسكري كالمحطات

النووية والأقمار الصناعية ومحاولة تخريبها وإحداث أكبر ضرر بها (محسوب، 2022).

يتضح للباحث أن الهجمات السيبرانية باتت تمثل تهديداً استراتيجياً متصاعداً يتجاوز مجرد الاختراقات التقنية التقليدية، لتصبح أداة ضغط وإضرار مباشر بالبنى التحتية الحيوية للدول ومؤسساتها العسكرية والمدنية. ويظهر تنوع هذه الهجمات بين - التجسس الإلكتروني، وتعطيل المنشآت الحيوية، واستهداف المرافق العسكرية الحساسة - أن البيئة السيبرانية تحولت إلى مسرح صراع معقد ذي أبعاد أمنية واقتصادية وسياسية عميقة. كما تؤكد الأمثلة الواقعية، كالهجوم على وزارات ومؤسسات أمريكية في 2020، والهجوم على خط أنابيب النفط في 2021، أن هذه التهديدات ليست نظرية، بل تشكل مخاطر عملية قائمة قادرة على إحداث شلل وظيفي وخسائر جسيمة

ومن هنا، تبرز الحاجة الماسة إلى تبني استراتيجيات استباقية متقدمة، تعتمد على الذكاء الاصطناعي لرصد هذه التهديدات في مراحلها المبكرة، والتعامل معها بكفاءة قبل تحولها إلى أزمات أمنية شاملة، كما تظهر أهمية أن تكون المواجهة متكاملة، تجمع بين البعد التقني، والبعد القانوني، والسياسات الوقائية، لضمان حماية المصالح الوطنية وصون أمن المعلومات والبنى التحتية الحيوية للدولة

وغالباً ما يكون تأثير الهجمات السيبرانية مدمراً، وقد يؤدي إلى إحداث شلل تام في البنية التحتية للدول في المجالات والقطاعات التي ترتبط بحياة البشر، وخاصة في مجالات الصحة العامة وشبكات الكهرباء والمياه والاتصالات والنقل، إذ أن قيام دولة بهجوم سيبراني على واحدة من هذه القطاعات كفيل بتوقف الحياة بشكل كامل، لاسيما في ظل صعوبة معرفة الجهات التي تقف وراء الهجوم السيبراني، وأن عمليات التحقيق الجنائي في هذه الهجمات تستغرق وقتاً طويلاً، وغالباً تنتهي دون معرفة الجهة التي تنفذها، وهذا يرجع إلى أن هذه الهجمات السيبرانية تندرج ضمن الحروب الخفية التي تقتحم الأنظمة الإلكترونية وتسبق العمل الأمني (فوزي، 2020).

وتتنوع الهجمات السيبرانية والأساليب المتبعة من قبل المجرمين الإلكترونيين،

وذلك من أجل تحقيق أهدافهم في الوصول إلى الأنظمة والشبكات أو تعطيلها باستخدام الطرق والوسائل التقنية المبتكرة، ومن أهمها ما يلي (سامي، 2020)

1. **البرامج الضارة Malware:** يشير البرنامج الضار إلى أي نوع من البرامج بصرف النظر عن طريقة تكوينه أو تشغيله، وهو مصمم لإلحاق الضرر بجهاز الكمبيوتر أو السيرفر أو الشبكة الداخلية، وتندرج الفيروسات المتنقلة والفيروسات كلها تحت البرامج الضارة، ولا يميزها عن بعضها البعض سوى الوسائل التي يتم استخدامها لإنشائها ونشرها. وقد تتسبب هذه الهجمات في تعطيل الشبكة، أو تمكن المهاجم من الوصول حتى يتمكن من التحكم في النظام المعلوماتي أو الشبكة المعلوماتية عن بعد.
2. **التصيد الاحتيالي Phishing:** التصيد تقنية يستخدمها مجرمو الفضاء الإلكتروني في إرسال رسائل بريد إلكتروني لخداع المستهدف من أجل القيام ببعض الأعمال الضارة، وربما يتم خداع المستلم في تنزيل برنامج ضار متخفي في صيغة مستند هام، على سبيل المثال، أو مطالبته بالنقر فوق أحد الروابط التي تقوم بتوجيهه إلى موقع إلكتروني زائف، حيث يتم سؤاله عن معلومات حساسة مثل أسماء المستخدمين وكلمات المرور الخاصة بالحسابات البنكية. والكثير من رسائل البريد المتصيدة تكون بدائية إلى حد ما ويتم إرسالها إلى الآلاف من الضحايا المحتملين، ولكن بعض رسائل البريد الإلكتروني يتم صياغتها وإرسالها بشكل خاص إلى أفراد مستهدفين ذوي قيمة لمحاولة الحصول على معلومات مفيدة منهم.
3. **هجوم حجب الخدمات Denial Of Service:** هجوم حجب الخدمات هو أسلوب استخدام القوة الغاشمة لمحاولة إيقاف تشغيل بعض الخدمات عبر الإنترنت. على سبيل المثال، قد يقوم المهاجمون بإرسال الكثير من البيانات إلى أحد مواقع الويب أو الكثير من الطلبات إلى إحدى قواعد البيانات والتي تتسبب في ملئ تلك الأنظمة وتعطيلها عن العمل.
4. **هجمات الرجل في المنتصف Man In The Middle:** هجوم الرجل في المنتصف

طريقة ينجح بها المهاجمون في إقحام أنفسهم سراً بين المستخدم وخدمة الويب التي يحاولون الوصول إليها. على سبيل المثال، ربما يقوم المهاجم بإعداد شبكة Wi-Fi مزودة بشاشة تسجيل مصممة بشكل يحاكي إحدى شبكات الفنادق، وبعد أن يقوم المستخدم بتسجيل الدخول يمكن أن يجمع المهاجم أي معلومات يرسلها المستخدم، ويشمل ذلك كلمات المرور الخاصة.

5. **هجمات Zero-Day :** هي عبارة عن ثغرات في البرامج لم يتم حلها إلى الآن وسميت كذلك لأنه بمجرد إصدار حزمة، يتناقص كل يوم عدد الأجهزة المفتوحة المعرضة للهجوم أثناء تسجيل المستخدم تحديثات الأمان.

يتضح للباحث أن تعدد أساليب الهجمات السيبرانية وتنوع تقنياتها يعكس الطبيعة الديناميكية والمتطورة للتهديدات الرقمية، ويزيد من تعقيد المواجهة الأمنية المطلوبة للتصدي لها، فمن البرامج الضارة التي تستخدم لتعطيل الأنظمة أو السيطرة عليها، إلى التصيد الاحتيالي الذي يستغل الثغرات البشرية، وصولاً إلى هجمات القوة الغاشمة كحجب الخدمة، وهجمات الرجل في المنتصف التي تستهدف سرية الاتصال، وحتى هجمات «اليوم صفر» التي تستغل الثغرات غير المكتشفة بعد، كلها تظهر أن الجرائم السيبرانية لا تستهدف فقط الأنظمة التقنية في المؤسسات العامة والحيوية، بل تمس مباشرة سرية المعلومات وسلامة البيانات واستمرارية تقديم الخدمات

ويبرز من هذا التنوع أن المواجهة الأمنية التقليدية القائمة على الحلول الجزئية لم تعد كافية، بل تستلزم نهجاً استباقياً متكاملاً يعتمد على التنبؤ، وتحليل الأنماط، وتوظيف الذكاء الاصطناعي لرصد التهديدات قبل وقوعها، كما تؤكد هذه المعطيات الحاجة إلى تطوير بيئة أمنية قادرة على التكيف مع تطور الهجمات، تجمع بين الحلول التقنية المتقدمة، والضوابط القانونية، والسياسات الوقائية

وفي ظل التصاعد المتزايد للهجمات السيبرانية، فمن المتوقع ظهور تهديدات سيبرانية تستهدف في المقام الأول عوالم الواقع الافتراضي والتقنيات وعالم

الميتافيرس، خاصة وأن درجة وتطور أمان العديد من هذه المنصات الجديدة غير موثوق بها وسيظل التهديد الأول لها هو عدم وعي المستخدمين بالمخاطر المحتملة لهجمات وحيل القراصنة لسلب بياناتهم وأموالهم (عضيبات، 2023)

يتضح للباحث مما تقدم أن الاختراقات والهجمات السيبرانية تشكل تهديداً متعاظماً للأمن والاستقرار، حيث أصبح الفضاء السيبراني بيئة خصبة لارتكاب الجرائم الإلكترونية ونشر الشائعات والتأثير على الأوضاع الاقتصادية والاجتماعية في الدولة، مما يتسبب في حدوث خسائر وأضرار هائلة على المؤسسات، كون الجرائم المرتكبة في البيئة السيبرانية أصبحت مهدداً حقيقياً لأمن المعلومات والبيانات الخاصة والعامة في كافة المجالات الحيوية بالدولة.

المطلب الثاني

تطبيقات الذكاء الاصطناعي في كشف الجرائم السيبرانية

رغم ما حققته تطبيقات الذكاء الاصطناعي من تقدم في الكشف عن التهديدات والجرائم السيبرانية، إلا أن الطرق التقليدية المستخدمة في الأمن السيبراني، والتي تعتمد بشكل أساسي على العنصر البشري لا تزال لها دور وفاعلية في الوقت الراهن مع وجود بعض الفروق في مدة ودقة إنجاز المهام، حيث يتميز الذكاء الاصطناعي بالمرونة والقدرة على التعلم والتكيف بشكل مستمر، واستيعاب البيانات الجديدة بسرعة تسهل عملية الكشف عن الخطر والاستجابة له، في حين أن الأنظمة التقليدية تعتمد على تحليل وتدقيق البيانات بشكل أساسي، والتي تتطلب وقتاً طويلاً للغاية وتحتاج إلى خبراء مميزين، كما أن الأنظمة التي يعتمدون عليها هؤلاء الخبراء، في تحديد السلوك والتوقعات للتهديدات الجديدة تحتاج إلى عملية تأهيل للتكيف مع أي تطورات جديدة (البابلي، 2020).

وللتعرف على دور تطبيقات الذكاء الاصطناعي في كشف وحماية البيئة السيبرانية، سيتم تناول هذا المطلب من خلال الفرعين التاليين

- **الفرع الأول:** أدوار الذكاء الاصطناعي في مجال مكافحة الجرائم السيبرانية.
- **الفرع الثاني:** تقنيات الذكاء الاصطناعي ودورها في تحليل الجريمة السيبرانية.

الفرع الأول

أدوار الذكاء الاصطناعي في مجال مكافحة الجرائم السيبرانية

يسعى الذكاء الاصطناعي إلى زيادة القدرة على التفكير الفائق وتحليل البيانات وتعزيز القدرات والمساهمات البشرية بشكل كبير، بل إنه يتفوق على الذكاء البشري في مجال تعزيز قوة الأمن السيبراني، إذ أنه مع تزايد الهجمات السيبرانية على المعلومات التي يصعب على فرق الأمن السيبراني ملاحقتها بالدقة المطلوبة، كان من الضروري استخدام تطبيقات الذكاء الاصطناعي في التصدي لتلك التهديدات، لما يتميز به الذكاء الاصطناعي من قدرة فائقة على مراقبة البيانات والكشف عن القيم المتطرفة التي تشير إلى احتمال وجود اختراقات معلوماتية، مما جعل الذكاء الاصطناعي حليفاً لبرامج الأمن السيبراني وإحباط مجموعة واسعة من الجرائم الخبيثة (النقبي، 2022)

وتتمثل أهم أدوار الذكاء الاصطناعي في مجال مكافحة الجرائم السيبرانية في الآتي: (القضاة، 2022)

1. الكشف عن التهديدات والاختراقات باستخدام تقنيات التعلم العميق وتحليل البيانات للكشف عن التهديدات السيبرانية والاختراقات المحتملة، ومراقبة الأنشطة غير المشروعة والسلوكيات الغريبة في الشبكة وتحليلها للكشف المبكر عن التهديدات والاستجابة السريعة لها.
2. القدرة على تحليل ومعالجة البيانات الضخمة المتعلقة بالأمن السيبراني، واستخلاص المعلومات الهامة من سجلات الأحداث والتقارير الأمنية وغيرها من المصادر لتحليل الأنماط واكتشاف الثغرات والتهديدات المحتملة.
3. تعزيز الاستجابة الآلية، بحيث يكون جزءًا من نظام الاستجابة الآلي بناءً على تحليلات وتقييمات يقوم بها لاتخاذ إجراءات آلية لمواجهة الهجمات والتهديدات دون تدخل بشري، وتوفير تحليلات وتوصيات دقيقة لدعم اتخاذ القرار الأمني بشأن مكافحة الجرائم.

4. القدرة على التعلم والتكيف بناءً على التجارب والمعلومات الجديدة، وتطوير النماذج التنبؤية باستخدام تقنيات التعلم الآلي لتحليل سلوك المهاجمين وتحديد الأهداف للهجمات السيبرانية المحتملة، وكيفية اتخاذ الإجراءات الوقائية للحد من جرائم البيئة السيبرانية.

يتضح للباحث أن الذكاء الاصطناعي أصبح يمثل ركيزة أساسية في بناء منظومة أمن سيبراني استباقية متقدمة، قادرة على مواجهة التهديدات الرقمية المتزايدة بتعقيداتها وديناميكيتها، إذ تتضح أدواره المحورية في قدرته على الكشف المبكر عن التهديدات والاختراقات عبر تقنيات التعلم العميق، وتحليل الكم الهائل من البيانات لرصد الأنماط غير المألوفة واستباق الهجمات قبل وقوعها. كما يظهر الذكاء الاصطناعي قيمة مضافة في دعم عمليات التحليل واتخاذ القرار، من خلال تقديم توصيات دقيقة، وإتاحة استجابة آلية فعالة دون الحاجة إلى تدخل بشري مباشر، مما يعزز سرعة التصدي للجرائم السيبرانية

كما يتضح من ذلك أيضاً أن المواجهة الناجحة للجرائم السيبرانية لا يمكن أن تتحقق بالاعتماد على الحلول التقليدية وحدها، بل تتطلب دمج تقنيات الذكاء الاصطناعي ضمن استراتيجية شاملة تقوم على التعلم المستمر، وتحليل السلوكيات التهديدية، وتطوير النماذج التنبؤية بشكل دائم

كما تعتبر تطبيقات الذكاء الاصطناعي أدوات قوية وفعالة لحماية الأنظمة والشبكات من الهجمات السيبرانية، حيث تساهم في تحقيق الآتي: (الأعرج، 2022)

1. الكشف عن التهديدات: يمكن للذكاء الاصطناعي تحليل كميات هائلة من البيانات بسرعة وكفاءة عالية مما يسمح له بالكشف عن التهديدات الناشئة والبرامج الضارة، كما يقوم بتحليل الأنماط الغير معتادة التي قد تشير إلي أي هجوم سيبراني محتمل.
2. التصدي للتهديدات: يمكن للذكاء الاصطناعي اتخاذ إجراءات تلقائية للتصدي للتهديدات مثل حظر البرامج الضارة أو عزل الأنظمة المصابة مما يقلل من الأضرار.

3. **التنبؤ بالتهديدات:** يمكن للذكاء الاصطناعي تحليل البيانات السابقة والأنماط الحالية للتنبؤ بالتهديدات المستقبلية مما يسمح باتخاذ الإجراءات الوقائية بما يتناسب مع التهديدات المتوقعة.
4. **التكيف مع التهديدات المتطورة:** يطور دائماً استراتيجيات دفاعية متقدمة لمواجهه التطور في الهجمات السيبرانية المستقبلية.
5. **تحليل السلوك:** يستخدم لمراقبة سلوك المستخدم وفهم أنماط السلوك الإجرامي في البيئة السيبرانية، وذلك للكشف عن السلوكيات الشاذة التي قد تشير إلي نشاط سيبراني ضار.
6. **تحليل نقاط الضعف وتقييم المخاطر:** يساعد الذكاء الاصطناعي في تحليل نقاط الضعف في الأنظمة والشبكات بشكل دقيق ويقدم تقييم شامل للمخاطر الأمنية ويصلح الثغرات تلقائياً أو يقدم توصيات للإصلاح ولتوفير أمن سيبراني.
7. **التحقق من الهوية:** يحسن دقة التحقق من الهوية باستخدام تقنيات مثل التعرف علي الوجه والتعرف علي الصوت والكشف عن محاولات انتحال الهوية بشكل أكثر فعالية.
8. **حماية البيانات:** الكشف عن محاولات سرقة البيانات والاختراقات وتشفير البيانات الحساسة وتأمينها من الوصول الغير مصرح به.
9. **مكافحة التصيد الاحتيالي:** تحليل رسائل البريد الإلكتروني ومواقع الويب للكشف عن محاولات الاحتيال والتصيد الاختراقي.

وعليه، يتضح للباحث مما سبق أنه عن طريق توظيف تقنيات الذكاء الاصطناعي، فإن المؤسسات الأمنية تكون قادرة على تعزيز مواجهة التهديدات السيبرانية والتصدي للهجمات المتطورة منها، حيث اتضح أن تقنيات الذكاء الاصطناعي تساهم بشكل فعال في توفير حماية للأنظمة من الهجمات والاختراقات السيبرانية، والتعرف على نقاط الضعف في الأنظمة وبالتالي الاستجابة للجرائم المحتملة، ما يساعد في اتخاذ القرار المناسب أثناء البحث والتحليل للهجمات السيبرانية بصورة أشمل وأدق.

الفرع الثاني

تقنيات الذكاء الاصطناعي ودورها في تحليل الجريمة السيبرانية

للذكاء الاصطناعي تطبيقات متعددة، وتوظيف تطبيقاته في المجال الأمني ومكافحة الجرائم أصبح ضرورة ملحة للأجهزة الأمنية المتطورة، كونها تساهم في سرعة التحليل وحل المشاكل، كما يشمل القدرة على التفكير المجرد وسرعة التعلم واتخاذ القرارات. لذا يعمل الباحثون في علوم الأدلة الجنائية على تطوير الأنظمة للاستفادة من القدرة الهائلة التي تقدمها أدوات الذكاء الاصطناعي في تحليل بيانات الجرائم، والتنبؤ بكيفية حدوثها واكتشاف مرتكبيها (الفليطي، 2023).

وتعمل تقنيات الذكاء الاصطناعي على تحليل الجرائم السيبرانية من خلال الآتي:

1. **تحليل البيانات الضخمة:**

وذلك من خلال الربط التقني بين أعمال مكافحة الجرائم السيبرانية والبيانات الضخمة المتوفرة لدى أجهزة إنفاذ القانون، وجعلها من أبواب البحث عن أدلة رقمية للجرائم المرتكبة، وهذه العملية تكون منذ بداية مرحلة تقديم البلاغ وإتاحة خيار تقديمه إلكترونياً وعبر تطبيقات معينة، ويتم تطويرها وتحديثها بشكل دوري، ويتم بعد ذلك مرور البلاغ في مراحل تدقيق وتصفيته للتأكد من صحته وعدم كونه بلاغاً كيدياً، وبعدها في حال التثبت تتم مرحلة البحث والاستدلال عن معلومات البلاغ والمشتبه بهم ومقدم البلاغ وجمع أكبر قدر ممكن من المعلومات عنهم، وتتم على أثرها مرحلة المقارنة والتحليل وجمع الأدلة الرقمية وفحصها من قبل تقنيات الذكاء الاصطناعي (حسن، 2020)

يتضح من ذلك أن تحليل البيانات الضخمة يمثل أحد الأعمدة الجوهرية في تعزيز قدرات المواجهة الاستباقية للجرائم السيبرانية، من خلال دمجه في جميع مراحل التعامل مع البلاغات بدءاً من تقديمها إلكترونياً وحتى فحص الأدلة الرقمية. ويُظهر هذا التكامل بين أنظمة البلاغات الرقمية، وتقنيات التدقيق والتحقق، وآليات البحث والتحليل المدعومة بالذكاء الاصطناعي، حيث أصبح استثمار البيانات الضخمة أداة

استراتيجية أساسية في الكشف عن الجرائم السيبرانية، وتحديد هوية المشتبه بهم، واستخلاص الأدلة الرقمية بشكل منهجي ودقيق. ويؤكد ذلك الحاجة إلى تطوير بنية تحتية متقدمة لإدارة البيانات الضخمة في المجال الأمني، بما يُسهم في بناء منظومة فعالة للوقاية من التهديدات الرقمية ومكافحتها.

2. التحليل الرقمي للأنظمة الجنائية:

هي عملية يتم بها الربط بين العلوم الجنائية وعلوم الحاسوب والشبكات وانترنت الأشياء والوسائط الرقمية ينتج على أثرها أدلة رقمية لوقائع إجرامية وقعت في البيئة السيبرانية، ويستخدم في هذه العملية جميع البيانات المتوفرة لدى جهات إنفاذ القانون كقوائم الأشخاص المشتبه بهم أو المبلغ عنهم في قضايا أخرى والجهات الأخرى كالصحية والاجتماعية، ويهدف التحليل الجنائي الرقمي للحفاظ على الأدلة الرقمية وتحديدها والحصول عليها وتوثيقها (الأسيوطي، 2020)

يتضح من ذلك أن التحليل الرقمي للأنظمة الجنائية يشكل ركيزة أساسية في منظومة مواجهة الجرائم السيبرانية، نظراً لدوره في الربط بين العلوم الجنائية التقليدية وعلوم الحاسوب والشبكات والوسائط الرقمية، بما يعزز من قدرة جهات إنفاذ القانون على استخلاص الأدلة الرقمية من وقائع إجرامية معقدة في البيئة السيبرانية، ويبرز هذا التحليل أهمية التكامل بين مصادر البيانات المتعددة، سواء من الملفات الجنائية أو السجلات الصحية والاجتماعية، بهدف بناء تصور شامل حول الجريمة والمشتبه بهم.

3. تقنيات اتخاذ القرارات الاستباقية:

هي نماذج تعزز من قدرة الذكاء الاصطناعي في اتخاذ القرارات الحاسمة، والتعامل الأمثل مع القضايا الغامضة في وقت قصير وقياسي، وذلك من خلال تحليل العمليات الحسابية المكثفة المتوفرة من خلال وقائع إجرامية سابقة، والنتائج التي ترتبت على تلك الوقائع لتقديم قرارات أفضل وأدق وتقليل نسبة الخطأ في القرار، وهذه العملية تسمى بعملية «سلاسل ماركوف» وهي عملية تحكم عشوائية ذات وقت منفصل

تستخدم لنمذجة صنع القرار في مشاكل التحسين عند عدم التيقن، وهناك العديد من التطبيقات التي تساعد الذكاء الاصطناعي على اتخاذ القرارات منها: «النظم الخبيرة والشبكات العصبية»، وهذه التطبيقات تتميز بقدرتها على معالجة البيانات والإشارات وتقديم الحلول التقنية المبنية على الخبرات السابقة والدمج بين المشاركة التقنية والمشاركة الإنسانية المتمثلة في الخبرات السابقة في مكان واحد مما يعود بالأثر على القرارات التي يتم اتخاذها، وبالتالي تعزيز القدرة على التنبؤ بالمتغيرات التي قد تحدث في مجالات عديدة (راشد، 2020)

يتضح من ذلك أن تقنيات اتخاذ القرارات الاستباقية القائمة على الذكاء الاصطناعي تمثل أحد أعمدة المواجهة الحديثة للجرائم السيبرانية، نظراً لقدرتها على تقديم حلول دقيقة وسريعة لمشكلات معقدة تتسم بعدم اليقين، ويبرز استخدام نماذج مثل سلاسل ماركوف والنظم الخبيرة والشبكات العصبية كيف أصبح الذكاء الاصطناعي أداة استراتيجية لتحليل الوقائع السابقة، ونمذجة القرارات في ضوء المعطيات المتاحة، والحد من احتمالية وقوع أخطاء بشرية في مواجهة القضايا الغامضة. كما تؤكد هذه التقنيات أهمية التكامل بين المعرفة التقنية والخبرة الإنسانية في صنع القرار الأمني، بما يُعزز القدرة على التنبؤ بالمتغيرات والتعامل معها بمرونة وفاعلية في مواجهة الجرائم السيبرانية

4. تحديد مواقع ارتكاب العمليات الإرهابية:

ساهمت تقنيات الذكاء الاصطناعي تم تطوير نماذج تساهم في التنبؤ وتحديد مواقع ارتكاب الهجمات الإرهابية وتوقيتها، ففي عام 2015 على سبيل المثال ادعت شركة تكنولوجية ناشئة (PredictifyMe) في الولايات المتحدة أن نموذجها الذي يحتوي على أكثر من 170 نقطة بيانات كان قادراً على التنبؤ بالهجمات الانتحارية بدقة 72 %. كذلك اعتمدت بعض النماذج الأخرى على بيانات المصادر المفتوحة للأفراد الذين يستخدمون الوسائط الاجتماعية والتطبيقات على هواتفهم المحمولة، ومن بينها نظام التعرف على الأحداث في وقت مبكر (EMBERS) الذي يدمج نتائج مختلف النماذج

التنبؤية المنفصلة من أجل التنبؤ بأحداث الاضطرابات المدنية (صالح، 2022).

يتضح من ذلك أن تطبيقات الذكاء الاصطناعي في تحديد مواقع وتوقيت العمليات الإرهابية تمثل نقلة نوعية في العمل الأمني الاستباقي، إذ أسهمت هذه التقنيات في تعزيز قدرة الأجهزة الأمنية على التنبؤ بالأحداث قبل وقوعها، والحد من آثارها المدمرة.

5. خوارزميات الذكاء الاصطناعي:

تُعرف الخوارزميات Algorithms بمفهومها العام على أنها مجموعة من الخطوات الرياضية والمنطقية والمتسلسلة اللازمة لحل مشكلة ما، تختلف باختلاف تفكير من يتولى مهمة حل المشكلة، ويمكن تشبيهها إلى حدٍ كبير بلوحة إشارات المرور، إذ توضع مجموعة من الخطوات والقواعد لكيفية التحكم باللوحة وصولاً إلى المرحلة التي يظهر فيها الضوء المناسب وفق الشرط المحقق. ففي عام 2018 طورت شركة التواصل الاجتماعي «فيسبوك Facebook» ابتكار «Facebook Deepfake» وهي خوارزمية تغلبت على جميع المعايير السابقة لخوارزميات الحاسوب من خلال قدرتها على التعرف على الوجوه البشرية، ووفي الواقع أخذنا نشهد مؤخراً ابتكار خوارزميات فائقة الذكاء مثل خوارزميات شبكات التواصل الاجتماعي المختلفة، وربما كانت الخوارزمية التي تعتمدها منصة «تيك توك Tok-tok» مثالاً جيداً عليها، حيث أن التطبيق يرشح المحتوى للمستخدم بناءً على مجموعة من العوامل المتعلقة بسلوكه على التطبيق، بدءً من الموقع الجغرافي والاهتمامات الشخصية، وصولاً إلى طريقة التفاعل مع المحتوى الذي يراه الشخص. ولذلك فإن الأجهزة الأمنية باستطاعتها الاستفادة من البيانات الضخمة، وتوظيف مجموعة من الخوارزميات التي توفر البيانات الضخمة تدفقاً ثابتاً من البيانات المتعددة الوسائط الضرورية وفهم الوضع الأمني ووضع الحلول الممكنة للقضايا واتخاذ القرارات الصائبة (الشحي، 2022)

يتضح من ذلك أن خوارزميات الذكاء الاصطناعي أصبحت أداة محورية في دعم جهود المواجهة الاستباقية للجرائم السيبرانية، لما توفره من قدرة متقدمة على تحليل البيانات المتدفقة والمتعددة الوسائط، واستنباط الأنماط السلوكية المعقدة، بما

يمكن الأجهزة الأمنية من بناء تصور أدق وأشمل حول الوضع الأمني والتعامل مع القضايا الرقمية بكفاءة عالية

الخاتمة

في ضوء ما تناولته هذه الدراسة من تحليل مستفيض لدور الذكاء الاصطناعي في المواجهة الاستباقية للجرائم السيبرانية، أمكن التأكيد على أن الجرائم الرقمية باتت تمثل أحد أخطر التهديدات المعاصرة للأمن الوطني، نظراً لطبيعتها المعقدة، وتنوع أدواتها، وتعدد الجهات المنفذة لها. كما أظهرت الدراسة أن الحلول الأمنية التقليدية لم تعد كافية لمواجهة هذه التهديدات، مما يستدعي ضرورة تبني مقاربات حديثة تقوم على استثمار التقنيات الذكية، والتحليلات التنبؤية، وإدارة البيانات الضخمة، لضمان رصد التهديدات مبكراً، والتعامل معها بكفاء. وعليه، فقد تم التوصل إلى النتائج والتوصيات الآتية

أولاً: النتائج

1. إن الوقاية من الجريمة منهج جديد في السياسة الجنائية المعاصرة، لاسيما في ظل تزايد ارتكاب الجرائم في البيئة السيبرانية التي أصبحت تشكل خطراً على الفرد والمجتمع، وتتميز بكونها سريعة التنفيذ، وتتم بواسطة الأجهزة والتقنيات التي يصعب معها إثباتها أو اكتشاف مرتكبيها، لذا استوجب على الأجهزة الأمنية أن تكون سباقة في تعزيز منظومة الأمن السيبراني لتحقيق الكفاءة في مواجهة جرائم البيئة السيبرانية بكل أبعادها وأنواعها المستحدثة.
2. أهمية تحديث الاجراءات والمعايير الامنية بما يتناسب مع تسارع تطور التقنيات والهجمات، وهذا يتوافق مع احتياجات الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ في تطوير منظومتها الرقمية وتأمين بيانات المواطنين والمقيمين والوافدين عبر الحدود..
3. تعتبر الاختراقات والهجمات السيبرانية من بين أهم المخاطر التي تواجه الأمن السيبراني، فضلاً عن كونها قد تقوم بتسريب معلومات سرية للدولة، إنها قد

تلحق الضرر بالهيئة الاتحادية للهوية والجنسية والجمارك وامن المنافذ وبمؤسسات ومرافق الدولة، أو خلق جانب من الفوضى وانعدام الأمن بالدولة على كافة الأصعدة.

4. تشمل إجراءات التنبؤ بجرائم البيئة السيبرانية من خلال «رصد التهديدات والاستجابة لها» ثم جمع المعلومات عن التهديدات السيبرانية، وعمليات التصدي لها والتحليلات الجنائية، مما يتيح للأجهزة الأمنية إمكانية الحصول على رؤية متكاملة عن مشهد التهديدات المتطور باستمرار مع بيانات استباقية وعملية لمساعدته على اتخاذ قرارات وتنفيذ عمليات استجابة مدروسة.

5. يرجع السبب في استخدام التكنولوجيا الحديثة في التنبؤ بجرائم البيئة السيبرانية والوقاية منها إلى الحاجة الماسة لتفعيل قدرات البحث الجنائي للمواجهة الاستباقية لجرائم البيئة السيبرانية؛ لما تتسم به أنظمة التنبؤ من سرعة ودقة في الكشف عن تلك الجرائم، وكذلك المساهمة في تقديم أدلة قوية إلى جهات القضاء حول الجرائم المرتكبة، إلى جانب توفير معلومات ودلائل إلى الأجهزة الأمنية لكشف مرتكبي الجرائم السيبرانية المعقدة والعابرة للحدود.

6. لتقنيات الذكاء الاصطناعي والاستخدام الامثل لها يسهم في سرعة الاستجابة وتقليل الاضرار، لا سيما في قطاع الجمارك وامن المنافذ الذي يتعرض لمحاولات متكررة من الجرائم السيبرانية العابرة للحدود.

ثانياً: التوصيات

1. تطوير وحدات متخصصة للتحليل التنبئي داخل أجهزة إنفاذ القانون في الهيئة، تعمل على توظيف خوارزميات الذكاء الاصطناعي لمعالجة البيانات الضخمة واستباق أنماط الجرائم السيبرانية، مع تزويدها بالبنية التقنية والكوادر البشرية المؤهلة، لضمان قدرتها على إصدار تقارير استباقية دقيقة تدعم صنع القرار الأمني.

2. إنشاء منظومة وطنية موحدة لرصد التهديدات السيبرانية في الزمن الحقيقي، ترتبط

بها الجهات الأمنية والقضائية والقطاعات الحيوية، بحيث تعتمد هذه المنظومة على تحليل فوري للبيانات متعددة المصادر، بما يتيح اكتشاف التهديدات العابرة للحدود والتعامل معها بكفاءة من خلال خطط استجابة سريعة ومدروسة.

3. إصدار دليل إجرائي موحد لمواجهة الجرائم السيبرانية، يتضمن آليات تشغيلية معيارية لكيفية التعامل مع البلاغات الرقمية، وآليات التحقق من صحتها، ومنهجية جمع الأدلة، وإجراءات التنسيق بين الجهات المعنية، مع تحديث هذا الدليل دورياً لمواكبة تطور أنماط الجرائم وتقنياتها.

4. تفعيل التعاون التقني بين القطاعين العام والخاص في مجال الأمن السيبراني، من خلال إنشاء شراكات استراتيجية مع الشركات التقنية الكبرى ومراكز البحث العلمي، لتبادل الخبرات، وتطوير برمجيات ذكية مخصصة لرصد التهديدات الرقمية وتقديم حلول عملية مبتكرة لمواجهتها.

5. إطلاق برامج تدريبية متقدمة إلزامية للعاملين في الهيئة الاتحادية للهوية والجنسية والجمارك وامن المنافذ، تركز على بناء القدرات الفنية للتحليل الجنائي الرقمي، واستخدام تقنيات الذكاء الاصطناعي والنظم الخبيرة، لضمان قدرتهم على التعامل مع الهجمات السيبرانية بكفاءة، واستثمار التكنولوجيا في جمع وتحليل الأدلة الرقمية لدعم الإجراءات القضائية.

قائمة المراجع

أولاً- المراجع باللغة العربية:

- إبراهيم، علي أحمد (2022). تطبيقات الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية، الرياض: دار الفيصل الثقافية للنشر والتوزيع.
- الأعرج، ماجد (2022). بناء نموذج ذكاء اصطناعي لتعزيز الإجراءات الوقائية للحد من الجريمة في المجتمع الأردني، المجلة العربية للنشر العلمي، العدد (44).
- الجمل، حازم (2018). الحماية الجنائية للأمن الإلكتروني، القاهرة: دار النهضة العربية.
- الحمادي، خالد (2018). إسهامات منصات التواصل الاجتماعي في تعزيز الأمن ومواجهة الجريمة، الشارقة: مركز بحوث الشرطة.
- الدريني، أشرف محمد (2021). جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات الخاصة بالدولة، مجلة روح القوانين، كلية الحقوق، جامعة المنصورة، العدد 95 (2).
- روابح، فريد (2020). التحري الجنائي المسبق وأثره في الحد من الجريمة المحتملة، مجلة الميزان للدراسات القانونية، جامعة العلوم الإسلامية، العدد 3 (9).
- عضيبات، أنس (2023). تفعيل دور تطبيقات الذكاء الاصطناعي في رصد الجرائم، المجلة العربية للدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، العدد 39 (2).
- العيداني، محمد (2023). دور الذكاء الاصطناعي في مجابهة الجرائم الإلكترونية، مجلة الدراسات القانونية والاقتصادية، العدد 9(2).
- المصمودي، سليم (2023). الاتجاهات الحديثة للوقاية من الجريمة في العصر الرقمي، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، العدد 4 (2).
- مخيمر، رضا محمد (2023). مدى تأثير التكنولوجيا الحديثة على السياسة الجنائية

في ضوء قانون تقنية المعلومات، دراسة تحليلية مقارنة، القاهرة، مجلة الشريعة والقانون، العدد 49 (2).

- المنذري، محمد راشد (2021). توظيف تقنيات الذكاء الاصطناعي في استشراف مستقبل الأحداث الأمنية، دراسة تطبيقية على القيادة العامة لشرطة أبوظبي، رسالة ماجستير غير منشورة، أبوظبي: كلية الشرطة.
- موسى، مصطفى (2015). دليل التحري عبر شبكة الإنترنت، القاهرة: دار الكتب القانونية.
- سامي، محمد (2020). دور الاستراتيجيات الاستباقية في مواجهة الهجمات السيبرانية، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد (4)، العدد (7).
- كاظم، رامي (2024). دور السياسة الوقائية في مواجهة الإجرام المنظم، مجلة كلية القانون والعلوم السياسية بالجامعة العراقية، العدد (25).
- مصباح، محمود (2020). المواجهة الاستباقية في السياسة الجنائية المعاصرة، مجلة جامعة تكريت، المجلد (2) العدد (7).
- فيصل، نسيمة (2019). سياسة الوقاية والمنع من الجريمة، مجلة البحوث والدراسات القانونية بكلية الحقوق والعلوم السياسية بجامعة بسكرة، المجلد (15)، العدد (1).
- فوزي، إسلام (2020). الأمن السيبراني، الأبعاد الاجتماعية والقانونية، المجلة الاجتماعية القومية، المجلد (56)، العدد (2).
- أبو حجير، طارق (2019). القيادة الإستراتيجية ودورها في إدارة المخاطر والأزمات، دراسة تطبيقية على المؤسسات الحكومية، أطروحة دكتوراه غير منشورة، مصر: جامعة قناة السويس، كلية التجارة.
- الباشري، أكرم (2018). الريادة الإستراتيجية مدخل معاصر، عمان: دار الرضوان للنشر.
- انطوان، حتو (2018). الريادة الإستراتجية في منظمات الأعمال، بيروت: المطبعة الشرقية.

- محسوب، بهاء (2022). الأمن السيبراني ودوره في تحقيق الاستدامة الأمنية في دولة الإمارات العربية المتحدة، الشارقة: أكاديمية الشارقة للعلوم الشرطية.
- النقبي، باسم (2022). تطوير قدرات الأمن السيبراني لتحقيق الاستدامة بدولة الإمارات العربية المتحدة، الشارقة: أكاديمية الشارقة للعلوم الشرطية.
- عبد العال، عصام الدين (2022). الحماية الجنائية للنظام السيبراني الخاص بمؤسسات دولة الإمارات العربية المتحدة ومرافقها الحيوية من الجرائم السيبرانية، الشارقة: أكاديمية الشارقة للعلوم الشرطية.
- الأسيوطي، أيمن (2020). الجوانب القانونية لتطبيق الذكاء الاصطناعي، أطروحة دكتوراه غير منشورة، القاهرة: جامعة القاهرة.
- حسن، حياة (2020). الفضاء الإلكتروني وتحديات الأمن العالمي، الجزائر: مجلة العلوم القانونية والسياسية، جامعة البليدة، المجلد (12)، العدد (1).
- الشامسي، راشد (2022). النظم الخبيرة كأحد أدوات الذكاء الاصطناعي ودورها في التنبؤ بالأزمات الأمنية، رسالة ماجستير غير منشورة، دبي: أكاديمية شرطة دبي.
- المعايطة، صالح (2020). الأمن الوطني بين مؤشرات التهديد التقليدية والحروب الرقمية والحشد الإلكتروني، أبوظبي: مركز الإمارات للدراسات والبحوث الإستراتيجية.
- راشد، طارق (2020). الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي، مجلة القانون والاقتصاد، جامعة القاهرة، العدد 92.
- الحسبان، عماد (2022). إدارة الشرطة الحديثة وتكنولوجيا الذكاء الاصطناعي، عمان: دار الخليج.
- البابلي، عمار (2020). دور أنظمة الذكاء الاصطناعي في التنبؤ بالجريمة، الشارقة: مجلة الفكر الشرطي، المجلد 28، العدد 110.
- البحيري، عمرو (2019). أثر تطبيقات الذكاء الاصطناعي على رفع كفاءة الأداء

الأمني، أطروحة دكتوراه غير منشورة، القاهرة: أكاديمية الشرطة.

- عبد الحميد، ممدوح (2019). الشرطة الاستخباراتية، العمل الشرطي القائم على الذكاء الاصطناعي وتحليل المعلومات، القاهرة: دار النهضة العربية.
- القضاة، محمد (2022). دور الاستراتيجيات الوطنية في مواجهة تحديات الأمن السيبراني في دول مجلس التعاون الخليجي، الشارقة: أكاديمية الشارقة للعلوم الشرطية.
- داود، حارث (2022). هجمات الفضاء الإلكتروني والاستراتيجية الوطنية، الشارقة: أكاديمية الشارقة للعلوم الشرطية.

ثانياً- المراجع باللغة الإنجليزية:

- Rajesh, S. (2021). Recognition and prevention of cyberharassment in social media using classification algorithms, Journal of Business Research, Vol.104.
- Eman, K. (2021). A case study of rural crime and policing in Pomurje region in Slovenia. Journal of Rural Studies, Vol. 85.
- Plotnek, J. (2021). Cyber terrorism: A homogenized taxonomy and definition, Journal of Computers and Security, Vol. 102.
- Samtani, S. (2023). Secure Knowledge Management and Cybersecurity in the Era of Artificial Intelligence. Information Systems Frontiers, Vol. 25(2).
- Patel, H. (2023). The Future of Cybersecurity with Artificial Intelligence (AI) and Machine Learning (ML), Journal of Advanced Research in Computer

and Communication Engineering, Vol. 101.

- Naik, Mehta. (2022). The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review, Journal of Complex & Intelligent Systems, Vol. 8(2).
- Atymtayeva, K. (2020). Building a Knowledge Base for Expert System in Information Security, Department of Computer Engineering, Kazakh-British Technical University, adfa, (232/).
- Boccio, C.M. (2019). The Influence Of Psychopathic Personality Traits, Low Self-Control, And Non-Shared Environmental Factors On Criminal Involvement, Youth Violence Juv, Justice, American Association For Correctional And Forensic Psychology Criminal Justice And Behavior, Vol. 19.
- Chen, S.; Plouffe, (2020). The Willy Encyclopaedia Of Personality And Individual Differences: Personality Process And Individual Differences, Vol. Iii, 3rd Ed.; John Wiley & Sons Ltd.: Hoboken, Nj, Usa.
- Hughes, G. (2019). Neighborhoods policing and community safety; researching instabilities of the local governance of crime, Criminology and criminal justice in the contemporary UK, 7 (4).
- Gurşu, S., & Can, O. (2025). Proactive cyber threat detection using AI and open-source intelligence. Journal of Cybersecurity Applications, 12(2), 45–62.
- Smith, A., & Jones, B. (2025). Transforming cybersecurity with agentic

AI to combat emerging threats. Computers & Security, 98, 103456.

- Ferrag, M. A., Alwahedi, F., Battah, A., Cherif, B., Mechri, A., Tihanyi, N., … Debbah, M. (2024). Generative AI in cybersecurity: A comprehensive review of LLM applications and vulnerabilities. arXiv preprint arXiv:2405.12750.
- Tripathi, P. (2024). AI and cybersecurity in 2024: Navigating new threats and unseen opportunities. International Journal of Computer Trends and Technology, 72(8), 26–32. https://doi.org/10.1444522312803//IJCTTV72I8P105
- Islam, S. A. M., Bari, M. S., Sarkar, A., Obaidur, A. J. M., & Paul, R. (2024). AIpowered threat intelligence: Revolutionizing cybersecurity with proactive risk management for critical sectors. Journal of Artificial Intelligence General Science, 7(1), 1–18. https://doi.org/10.60087/jaigs.v7i01.291
- Farzaan, M. A. M., Ghanem, M. C., ElHajjar, A., & Ratnayake, D. N. (2024). AIenabled system for efficient and effective cyber incident detection and response in cloud environments. arXiv preprint arXiv:2404.05602.

ثالثاً- المواقع الإلكترونية:

- الفليطي، سيلنيا (2023). العدالة التنبؤية بتقنيات الذكاء الاصطناعي، متاح على الرابط الإلكتروني: https://political-encyclopedia.org/dictionary.
- صالح، مروة (2022). سيادة القانون كمفهوم رئيسي في النظام البيئي الرقمي، متاح على الرابط الإلكتروني: https://www.unesco.org/en/articles/rule-law-key-concept-digital-ecosystem-during-internet-governance-forum-interview-12.
- الشحي، صفية (2022). أخلاقيات الخوارزميات، متاح على الرابط الإلكتروني:

بحث بعنوان:

أثر وسائل التواصل الاجتماعي على أداء الموظفين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ من وجهة نظر العاملين

الباحثة / سهيلة راشد خميس النقبي
باحث أكاديمي
الهيئة الاتحادية للهوية والجنسية والجمارك وامن المنافذ

ملخص البحث

تبرز هذه الدراسة الدور المتنامي لوسائل التواصل الاجتماعي في تشكيل الأداء الوظيفي داخل الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ، وهي من المؤسسات الرئيسية في الدولة. تهدف الدراسة إلى استكشاف تأثيرات استخدام وسائل التواصل الاجتماعي من وجهة نظر الموظفين، مع التركيز على كيفية تأثير هذه الوسائل على جودة العمل والأداء الوظيفي. تعتمد الدراسة على منهج وصفي كمي، حيث شملت عينة مكونة من 331 موظفًا من الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ النتائج التي خلصت إليها الدراسة تشير إلى وجود علاقة إيجابية بين استخدام وسائل التواصل الاجتماعي وتحسين التواصل والتعاون بين الموظفين، مما ينعكس بدوره على تحسين الأداء الوظيفي وزيادة الرضا الوظيفي. من ناحية أخرى، أبرزت الدراسة أيضًا بعض التأثيرات السلبية المتمثلة في التشتت وفقدان التركيز، مما يستلزم تطوير استراتيجيات فعّالة لإدارة استخدام هذه الوسائل بشكل يحقق التوازن بين فوائدها ومخاطرها.كما أشارت الدراسة إلى وجود فروق ذات دلالة إحصائية في استخدام وسائل التواصل الاجتماعي تبعًا لمتغيرات ديموغرافية مثل العمر، الخبرة، والمستوى التعليمي، مما يدعو إلى إجراء مزيد من البحوث لفهم هذه الديناميكيات بشكل أعمق.في ختامها، توصي الدراسة بضرورة صياغة سياسات واضحة وفعّالة تنظم استخدام وسائل التواصل الاجتماعي في بيئات العمل، بما يخدم أهداف المؤسسة ويدعم أداء الموظفين بشكل شامل

المقدمة

في في عصر التحول الرقمي، ومع تسارع نهضة الحياة الرقمية، أصبحت وسائل التواصل الاجتماعي جزءاً لا يتجزأ من إيقاع الحياة اليومية على المستويين الشخصي والمهني. وتعتبر هذه الوسائل أدوات فعالة للتواصل الفوري وتبادل المعلومات بين الأفراد والمؤسسات في عملياتها، ويمكن لتلك الوسائل أن تساعد في تحسين أداء الموظفين وزيادة الإنتاجية من خلال توفير مواقع سهلة الاستخدام لتبادل المعرفة والتعاون والاتصالات الداخلية (nalpaK & nielneaH, 0102).

وتعتبر دولة الإمارات العربية المتحدة من الدول الرائدة عالمياً بتكنولوجيا الأشياء في مختلف قطاعاتها، بما في ذلك جهاتها الحكومية والتي تعتبر الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ من الجهات الرائدة في تقديم خدماتها بالتحول الرقمي من خلال أحدث التقنيات في الذكاء الاصطناعي والذي يزيد من كفاءتها المؤسسية وتحسين جودة الخدمات المقدمة للمواطنين والمقيمين، وتلعب دورًا حيويًا في الحفاظ على الأمن القومي

يساعد استخدام وسائل التواصل الاجتماعي على تحسين التواصل الداخلي بين الموظفين وزيادة الكفاءة التشغيلية وزيادة سعادة الموظفين (الحسيني، 8102). خلال السنوات الأخيرة من هذا القرن، حدثت تحولات كبيرة في طريقة تفاعل الأفراد والمنظمات مع التكنولوجيا، فأصبحت وسائل التواصل الاجتماعي مثل koobecaF و rettiwT وnIdekniL وmargatsnIa جزءًا لا يتجزأ من الأدوات المستخدمة في بيئة الأعمال، حيث أشارت كثير من الدراسات أن استخدام وسائل التواصل الاجتماعي في المنظمات يعمل على تحسين التواصل بين الموظفين ويسهل الوصول إلى المعلومات والموارد (idranoeL, namsyuH, & dleifnietS, 3102). ومن الأمثلة على ذلك هو قدرة منصات مثل nIdekniL على مساعدة الموظفين في إنشاء شبكات مهنية قوية، في حين أن استخدام koobecaF وrettiwT يمكن أن يعزز التواصل الداخلي والتعاون بين مختلف الفرق.

وستكشف هذه الدراسة كيف سيؤثر استخدام وسائل التواصل الاجتماعي على أداء الموظفين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ، وكيف يمكن أن يؤدي استخدام وسائل التواصل الاجتماعي إلى تعزيز فعالية التواصل بين الموظفين وزيادة سرعة وكفاءة تبادل المعلومات وتحسين التنسيق بين الادارات المختلفة. وقد جاء اختياري لموضوع هذا البحث استنادًا إلى خلفيتي الأكاديمية، حيث إنني حاصلة على درجة البكالوريوس في إدارة الأعمال ودرجة الماجستير في الموارد البشرية، وهو ما أتاح لي الإلمام بالجوانب التنظيمية والإدارية المرتبطة بموضوع الدراسة. إن هذه الخلفية العلمية وفرت منظورًا متكاملاً يساعد في تناول الإشكالية البحثية بصورة منهجية، كما تدعم القدرة على الربط بين الأسس النظرية والتطبيقات العملية ذات الصلة.

المبحث الأول

الإطار العام للدراسة والإطار النظري

المطلب الأول: الإطار العام للدراسة

مشكلة البحث

تحظى وسائل التواصل الاجتماعي بأهمية متزايدة في الحياة اليومية وبيئات الأعمال، حيث أصبحت هذه الوسائل أداة مهمة للتواصل الفعال وتبادل المعلومات بين الأفراد والجماعات. وفي الجهات الحكومية مثل الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ، تلعب هذه الوسائل دوراً رئيسياً في تحسين الكفاءة التشغيلية وتسهيل تنفيذ المهام اليومية من خلال تحسين الاتصالات الداخلية ومع ذلك، هناك تحديات مرتبطة باستخدام هذه الوسائل بفعالية مثل إدارة الوقت، والحفاظ على التركيز، وضمان أمن المعلومات والذي يأثر في نهاية الأمر على أداء الموظفين.

فالدراسة تتمحور مشكلتها في معرفة أثر وسائل التواصل الاجتماعي على أداء الموظفين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ من وجهة نظر الموظفين.

اسئلة البحث

- ما وجهة نظر العاملين من استخدام وسائل التواصل الاجتماعي في مكان العمل؟
- ما اثر استخدام وسائل التواصل الاجتماعي على تحسين جودة العمل والأداء الوظيفي من وجهة نظر العاملين؟
- هل يوجد فروق ذو دلالة احصائية لمستوى استخدام وسائل التواصل الاجتماعي في مكان العمل من وجهة نظر العاملين وفقا لمتغير (النوع الاجتماعي، الخبرة، المستوى التعليمي)؟

أهداف البحث

- التعرف على وجهة نظر العاملين في استخدام وسائل التواصل الاجتماعي على الإنتاجية في مقر العمل.
- تحديد تأثير استخدام وسائل التواصل الاجتماعي في تحسين جودة العمل والأداء الوظيفي.
- تحليل الفروق والأدلة الإحصائية في استخدام وسائل التواصل الاجتماعي بناءً على المتغيرات الديموغرافية.

حدود الدراسة

- **الحدود المكانية:** الهيئة الاتحادية للهوية والجنسية والجمارك وامن المنافذ
- **الحدود الزمانية:** العام الحالي 4202- 5202
- **الحدود البشرية:** جميع العاملين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ
- **الحدود الموضوعية:** استخدام وسائل التواصل الاجتماعي وأثرها على أداء الموظفين في الهيئة الاتحادية للهوية والجنسية والجمارك و امن المنافذ

محددات الدراسة:

تُعَدُّ دراسة تأثير وسائل التواصل الاجتماعي على أداء الموظفين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ من الجوانب المهمة لفهم الديناميات التنظيمية. ومع ذلك، تواجه هذه الدراسة قيودًا عديدة تؤثر على عمق ونتائج البحث. أولاً، تقتصر العينة المستهدفة على موظفي الهيئة فقط، مما قد يؤثر على تعميم النتائج على شريحة أكبر من الموظفين في المؤسسات الحكومية الأخرى، كما قد يكون عدد الإستجابات لإستطلاع الرأي المعمم على موظفي الهيئة قليل مقارنة بالعدد الإجمالي لموظفيها. علاوةً على ذلك، تُشير بعض الدراسات السابقة إلى تأثيرات متباينة لوسائل التواصل الاجتماعي، مثل تأثيرها الإيجابي على تعزيز التواصل ورفع الروح

المعنوية، في حين تظهر دراسات أخرى علاقة سلبية تتعلق بالإلهاءات وتدهور الإنتاجية (ayahS siraF demmahoM, 9102). بالإضافة إلى ذلك، قد تؤثر الظروف الاجتماعية والاقتصادية في المنطقة على استخدام وسائل التواصل الاجتماعي ونتائجها (rD. ilA-lA liqaoM nib dhaF, 8102). لذلك، من الضروري توخي الحذر عند تفسير النتائج، والاعتراف بأن هناك عوامل متعددة قد تلعب دورًا في أداء الموظفين (5591-40)

المطلب الثاني

منهجية الدراسة وإجراءاتها

منهجية البحث

ستتبع الدراسة منهج البحث الوصفي (الكمي) التحليلي لجمع البيانات وتحليلها. حيث يعرف المنهج الوصفي على انه هو منهج بحثي يهدف إلى وصف الظواهر وجمع البيانات المتعلقة بها بشكل دقيق، ومن ثم تحليل هذه البيانات للوصول إلى استنتاجات مبنية على الأدلة، هذا المنهج يساعد في تقديم صورة شاملة وواضحة للظواهر المدروسة من خلال تحليل البيانات التي تم جمعها بطرق وصفية وتحليلية (yarG, evorG, & dnalrehtuS, 8102)

مجتمع الدراسة وعينتها (المشاركين)

سيتم تطبيق أداة الدارسة على عدد من المشاركين (331) ممن مازالوا يعملون على رأس عملهم في الهيئة التحادية للهوية والجنسية والجمارك وأمن المنافذ.

أداة الدراسة

تستخدم الدراسة الحالية الاستبانة كأداة رئيسية لجمع البيانات وستتضمن جزئين رئيسيين هما:

الجزء الاول : (البيانات) المعلومات الديموغرافية.

الجزء الثاني: حيث سيتضمن محورين: -

- **المحور الاول:** ما وجهة نظر العاملين من استخدام وسائل التواصل الاجتماعي في

مكان العمل؟ وعدد الأسئلة (7).

- **المحور الثاني:** ما أثر استخدام وسائل التواصل الاجتماعي على تحسين جودة العمل والأداء الوظيفي من وجهة نظر العاملين؟ وعدد الأسئلة (8).

تحليل البيانات التي سيتم الحصول عليها:

سيتم استخدام برنامج الحزمة الاحصائية ((lecxe في تحليل بيانات الدراسة.

الصدق والثبات

لضمان صلاحية أداة الدراسة، تم التحقق من صدق الاستبانة بعرضها على مجموعة من المحكمين المتخصصين في مجال البحث للتأكد من وضوح العبارات وملاءمتها لقياس أبعاد الدراسة، وقد أُجريت التعديلات اللازمة بناءً على ملاحظاتهم، مما وفر صدق المحتوى للاستبانة. كما تم التحقق من ثبات الأداة باستخدام الأساليب الإحصائية المتعارف عليها.

المطلب الثالث

الإطار النظري والدراسات السابقة

مراجعة الأدبيات

يرتكز البحث على نظريات متعددة حول الاتصال التنظيمي وتأثير التكنولوجيا على الأداء الوظيفي. تشير دراسة الحسيني (8102) إلى أن تكنولوجيا المعلومات، بما في ذلك وسائل التواصل الاجتماعي، تلعب دورًا محوريًا في تحسين الأداء الوظيفي من خلال تعزيز التواصل الفعال وتوفير منصات لتبادل المعرفة. بالإضافة إلى ذلك، تُظهر دراسة الناصري (9102) أن الاتصال الإداري الجيد يمكن أن يؤدي إلى تحسين كبير في أداء الموظفين ورفع مستوى رضاهم الوظيفي

تعتبر الإطارات النظرية من العناصر الأساسية التي تدعم الدراسات الأكاديمية، حيث توفر السياق والفهم الأعمق للمسائل المطروحة. في هذا البحث، يتم تطبيق

نظريات متعددة لفهم كيفية تأثير وسائل التواصل الاجتماعي على أداء الموظفين، مثل نظرية البيئة الرقمية التي تشير إلى كيفية تعديل سلوكيات الأفراد في بيئات العمل التفاعلية، توضح الدراسات السابقة أن الاستخدام الفعال لهذه الوسائل يمكن أن يعزز من التعاون والتواصل بين الموظفين، مما يسهم في تحسين الإنتاجية الفردية والجماعية (rD. dhaF nib liqaoM IA-IAi, 8102). وفي سياق الهيئات الحكومية، تُظهر نتائج الأبحاث أن استخدام وسائل التواصل الاجتماعي بشكل استراتيجي يمكن أن يؤدي إلى تعزيز التفاعل الإيجابي بين الإدارات المختلفة وزيادة مستويات الرضا الوظيفي (licnuoC ecnegilletnI lanoitaN, 1202-30). تثمر هذه النتائج في صياغة توصيات تتعلق بكيفية تبني هذه الوسائل ليصبح لها أثر ملموس على الأداء المؤسسي

تأثير وسائل التواصل الاجتماعي على السلوك

تتأسس تأثيرات وسائل التواصل الاجتماعي على السلوك الفردي والجماعي على مجموعة من النظريات النفسية والاجتماعية التي تفسر كيفية تفاعل الأفراد مع هذه الوسائل. من ضمن هذه النظريات، نظرية الأثر الاجتماعي التي تفترض أن الأفراد يتأثرون بالبيئة الاجتماعية المحيطة بهم، حيث تسهم وسائل التواصل في تشكيل القيم والمعايير السلوكية لديهم. بالإضافة إلى ذلك، تبرز نظرية السلوك المتعقب، التي تشير إلى أن تفاعل الأفراد مع محتوى وسائل التواصل يمكن أن يؤدي إلى تعديل سلوكياتهم بناءً على ردود الأفعال الاجتماعية والرمزية (licnuoC ecnegilletnI lanoitaN, 1202-30). كما تشير الدراسات إلى أن الاستخدام المفرط لوسائل التواصل قد يسهم في تدهور التركيز والأداء الوظيفي، كما أكدته نتائج دراسات سابقة حول تأثير هذه الوسائل على الإنتاجية (ayahS siraF demmahoM, 9102)(ibrahIA fialuhK danaS, 0202). في نهاية المطاف، فإن فهم هذه النظريات يمكن أن يسهم في تطوير استراتيجيات فعالة لتعزيز البيئة الوظيفية والتقليل من التأثيرات السلبية المحتملة لاستخدام وسائل التواصل في مكان العمل.

نتائج الأبحاث السابقة حول وسائل التواصل الاجتماعي وأداء الموظفين

تشير نتائج الدراسات السابقة إلى أن تأثير وسائل التواصل الاجتماعي على أداء الموظفين يعتبر موضوعًا متعدد الأبعاد. فقد أظهرت الأبحاث أن الاستخدام المنتظم لهذه الوسائل يمكن أن يعزز التواصل الفعال بين الموظفين ويزيد من التعاون في بيئة العمل، مما يؤدي إلى تحسين الأداء والفاعلية التنظيمية. ومع ذلك، لا يمكن تجاهل الجوانب السلبية، حيث أظهرت الدراسات أن الاستخدام المفرط لهذه المنصات قد يسفر عن تشتت الانتباه وتقليل الإنتاجية (ayahS siraF demmahoM, 9102). في السياق العربي، أظهرت الأبحاث الحديثة مثل تلك التي تناولت تأثير وسائل التواصل على أداء العاملين في المؤسسات الحكومية، أن التوازن بين الاستخدام الإيجابي والسلبي هو أمر حيوي للحفاظ على جودة الأداء المؤسسي (منصور، أيمن عبدالرحيم فرج، الفليت، خلود عطية أحمد, 2202)(lanoitaN ecnegilletnI licnuoC, 1202-30). بالتالي، من المهم وضع استراتيجيات فعالة لإدارة استخدام وسائل التواصل الاجتماعي لتعظيم فوائدها وتقليل مخاطرها.

تعريف قنوات التواصل الاجتماعي

قنوات التواصل الاجتماعي هي منصات رقمية تسمح للمستخدمين بإنشاء، مشاركة، وتبادل المحتوى بأشكاله المختلفة مثل النصوص، الصور، الفيديوهات، والروابط. هذه القنوات تشمل مواقع مثل فيسبوك، تويتر، إنستجرام، ولينكد إن. تهدف إلى تسهيل التفاعل والتواصل بين الأفراد والمجتمعات عبر الإنترنت. تلعب وسائل التواصل الاجتماعي دورًا محوريًا في نشر المعلومات وتشكيل الرأي العام، كما تعتبر أدوات هامة في التسويق الرقمي والتفاعل بين الشركات والعملاء (nielneaH & nalpaK, 0102)

الأداء الوظيفي

الأداء الوظيفي يشير إلى مدى تحقيق الموظف للمهام والواجبات التي تم تكليفه بها في إطار دوره داخل المؤسسة. يتضمن الأداء الوظيفي عدة جوانب تشمل الكفاءة،

الجودة، الإنتاجية، الالتزام بالمواعيد، والقدرة على حل المشكلات والتفاعل مع الزملاء والعملاء. يعتبر تقييم الأداء الوظيفي جزءًا أساسيًا من إدارة الموارد البشرية، حيث يساعد في تحديد نقاط القوة والضعف وتوجيه التدريب والتطوير المهني لتحسين الإنتاجية (3991 ,oldiwotoM & namroB ;0991 ,llebpmaC)

نظرية التبادل الاجتماعي

نظرية التبادل الاجتماعي تعتبر التفاعل الاجتماعي بمثابة عملية تبادل بين الأفراد يسعى كل طرف فيها لتحقيق مكاسب تفوق التكاليف. تقوم هذه النظرية على فرضية أن العلاقات الاجتماعية تستمر وتزدهر عندما يشعر الأطراف بالرضا الناتج عن التبادل المتبادل للفوائد والمكافآت. يمكن أن تشمل هذه الفوائد الدعم العاطفي، المعلومات، والموارد المادية. ينظر إلى التفاعلات الاجتماعية على أنها مشابهة للمعاملات الاقتصادية حيث يتم تقييم الربح والخسارة باستمرار (6791 ,nosremE ;4691 ,ualB)

نظرية الاستخدام والإشباع

نظرية الاستخدام والإشباع تركز على كيفية استخدام الأفراد لوسائل الإعلام لتحقيق حاجاتهم المختلفة وإشباعها. تفترض هذه النظرية أن الأفراد يكونون نشطين في اختيار وسائل الإعلام بناءً على قدراتها في تلبية احتياجاتهم النفسية والاجتماعية. ترتكز النظرية على أن الدوافع الفردية تلعب دورًا حاسمًا في تحديد كيفية استهلاك وسائل الإعلام. تشمل هذه الدوافع البحث عن المعلومات، الترفيه، التفاعل الاجتماعي، والابتعاد عن الضغوط اليومية (6891 ,nibuR ;3791 ,hctiveruG & ,relmulB ,ztaK)

المبحث الثاني

نتائج الدراسة وتحليل البيانات

المطلب الأول: وصف خصائص العينة

تحليل الاستبيان

المحور الأول: العمر

توزيع الفئات العمرية:

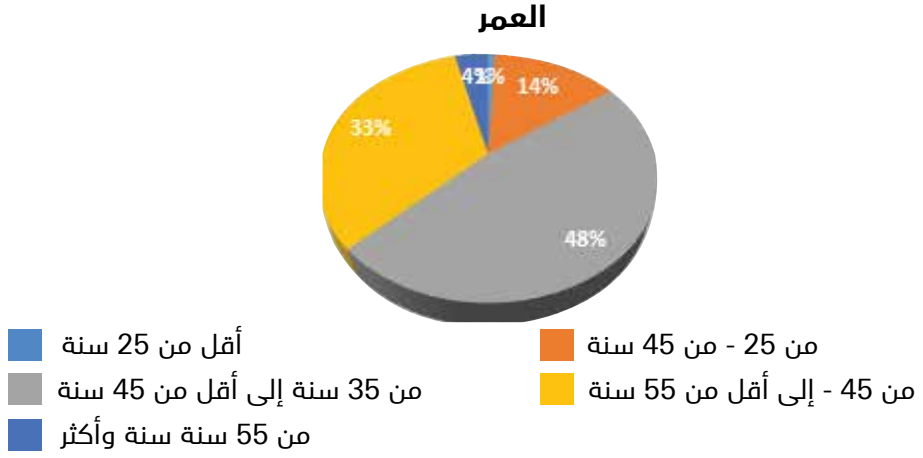
أقل من 52 سنة: 0. 67% (1 مستجيب)

من 52 إلى أقل من 53 سنة: 41. 93% (91 مستجيب)

من 53 إلى أقل من 54 سنة: 74. 37% (36 مستجيب)

من 54 إلى أقل من 55 سنة: 33. 33% (44 مستجيب)

55 سنة فأكثر: 3. 97% (5 مستجيبين)



التحليل:

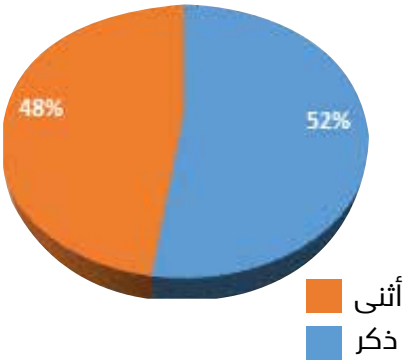
- **أكبر الفئات العمرية تمثيلاً:** الفئة من 53 إلى أقل من 54 سنة»، التي تشكل ما يقارب نصف العينة (74. 37%). هذا يشير إلى أن العينة مكونة بشكل رئيسي من الموظفين في منتصف العمر، والذين من المحتمل أن يكونوا في مرحلة مهنية متقدمة.

- **الفئات الأقل تمثيلاً:** الفئة «أقل من 52 سنة» و«55 سنة فأكثر» تشكلان أقلية، مما قد يعكس أن الموظفين في هذه الفئات العمرية إما أنهم أقل تمثيلاً في بيئة العمل أو أنهم أقل مشاركة في الاستبيان.

التأثيرات المحتملة

- من المتوقع أن تختلف تأثيرات وسائل التواصل الاجتماعي بناءً على الفئة العمرية. فقد تكون الفئات الأصغر سناً أكثر مرونة وتكيفًا مع التقنيات الحديثة، بينما قد تواجه الفئات الأكبر سناً تحديات في استخدامها بفعالية.
- يمكن استخدام تحليل الارتباط لفحص العلاقة بين العمر وتقييمات أثر التواصل الاجتماعي على الأداء الوظيفي.

النوع الاجتماعي (الجنس)



المحور الثاني: الجنس

توزيع النوع الاجتماعي:

- الذكور 25. 72%
- الإناث 74. 37%

التحليل:

- التوزيع المتوازن بين الجنسين يعزز من قوة العينة ويمكّن من تحليل الآراء المختلفة لكلا الجنسين.
- الفروق المحتملة بين الجنسين: يمكن أن يختلف استخدام وسائل التواصل الاجتماعي بين الذكور والإناث من حيث الأهداف والطرق، مما قد يؤثر على الأداء الوظيفي. على سبيل المثال، قد يكون لدى الإناث توجه نحو استخدام التواصل الاجتماعي للتواصل الاجتماعي وتعزيز العلاقات، بينما قد يستخدمه الذكور لأغراض مهنية.

المحور الثالث: سنوات الخبرة

توزيع سنوات الخبرة:

- من سنة إلى أقل من 5 سنوات: 7.58%
- من 5 سنوات إلى أقل من 10 سنوات: 11.36%
- 10 سنوات فأكثر: 81.06 %

التحليل:

- غالبية المستجيبين (81.06%) لديهم خبرة عمل تتجاوز 10 سنوات. هذا يشير إلى أن العينة مكونة في معظمها من الموظفين ذوي الخبرة العالية، مما قد يؤثر على كيفية استجابتهم للتغييرات في وسائل التواصل الاجتماعي داخل بيئة العمل.
- الفئات الأقل خبرة قد تكون أكثر تقبلاً لاستخدام أدوات التواصل الاجتماعي الجديدة، بينما قد يكون الموظفون ذوو الخبرة العالية أكثر تحفظًا في استخدامها.

المطلب الثاني

نتائج محاور الدراسة

أولاً: آراء حول تأثير وسائل التواصل الاجتماعي على الأداء الوظيفي

أبرز الآراء والمواقف:

1. استخدام وسائل التواصل الاجتماعي يسهم في الحصول على أفكار جديدة: 32. 86% من المستجيبين يعتقدون أن وسائل التواصل الاجتماعي تساعد في جلب حلول مبتكرة.
2. التفاعل المستمر على وسائل التواصل الاجتماعي قد يؤدي إلى الإجهاد: 51. 97% يرون أن التفاعل المستمر يمكن أن يسبب إرهاقاً نفسياً.
3. الإفراط في استخدام وسائل التواصل الاجتماعي يؤدي إلى انخفاض التركيز: 53. 69% من المستجيبين يعتقدون أن الاستخدام المفرط لوسائل التواصل الاجتماعي يمكن أن يقلل من مستوى التركيز.
4. وجهة نظر المبحوثين من استخدام وسائل التواصل الاجتماعي أثناء ساعات العمل تراوحت بين 3. 91 – 3. 33، وهو ما يشير إلى درجة استجابة متوسطة. حيث حصل البند (استخدام وسائل التواصل الاجتماعي أثناء ساعات العمل يساعد في إنجاز المهام بشكل أسرع)على أعلى متوسط حسابي بلغ3. 33 ، بينما كان أدنى متوسط حسابي للبند(الاعتماد على وسائل التواصل الاجتماعي يعزز من جودة القرارات الإدارية) بمتوسط 3. 91.
5. وجهة نظر المبحوثين من تأثير وسائل التواصل الاجتماعي على بيئة العمل، تراوحت المتوسطات الحسابية بين 3. 14 – 3. 67، وهو ما يعكس درجة استجابة مرتفعة نسبيًا. وقد جاء البند استخدام وسائل التواصل الاجتماعي يسهم في تحسين بيئة العمل التفاعلية) بالمرتبة الأولى بمتوسط حسابي3. 67، في حين كان أدنى متوسط للبند التفاعل المستمر على وسائل التواصل الاجتماعي يقلل من جودة الأداء بمتوسط 3. 14

التحليل:

- التنوع في الآراء يظهر أن هناك تبايناً في كيفية تأثير وسائل التواصل الاجتماعي على الأداء الوظيفي. بينما يرى البعض أن لها دوراً إيجابياً في تعزيز الأفكار والإبداع، يرى آخرون أن الإفراط في استخدامها يمكن أن يؤدي إلى تأثيرات سلبية مثل الإجهاد وقلة التركيز.

الاستنتاجات النهائية:

1. التوزيع الشامل للعينة يعكس تمثيلاً متوازناً للموظفين في مختلف الأعمار، الجنس، وسنوات الخبرة، مما يزيد من قوة النتائج ويجعلها قابلة للتعميم على بيئات عمل مشابهة.
2. الفروق المحتملة بين المتغيرات الديموغرافية تشير إلى أن تأثير وسائل التواصل الاجتماعي على الأداء قد يختلف بناءً على العمر، الجنس، والخبرة، مما يتطلب سياسات توجيهية خاصة لكل فئة.
3. التنوع في الآراء حول استخدام وسائل التواصل الاجتماعي يعكس الحاجة إلى تحقيق توازن في استخدام هذه الوسائل في بيئة العمل، بحيث يتم استغلال الفوائد وتقليل التأثيرات السلبية مثل الإجهاد وانخفاض التركيز.

المطلب الثالث

الفروق وفق المتغيرات

الفروق في استخدام وسائل التواصل الاجتماعي بين الذكور والإناث وتأثيرها على الأداء الوظيفي

1.الاختلافات في استخدام وسائل التواصل الاجتماعي حسب الأهداف:

- **الذكور:**

◊ يستخدم الذكور وسائل التواصل الاجتماعي في مكان العمل بشكل أكبر لأغراض مهنية بحتة مثل التواصل مع الزملاء لأداء المهام، أو البحث عن معلومات ومصادر جديدة يمكن أن تساعدهم في تحسين أداء العمل.

◊ يمكن أن يكون التركيز على استخدام وسائل التواصل كأداة لتعزيز الصورة المهنية وبناء شبكات مهنية أوسع، وخاصة على المنصات المهنية مثل nIdekniL.

◊ يُحتمل أن يتأثر الذكور أقل بالإجهاد النفسي الناتج عن التفاعل المستمر، حيث أنهم قد يستخدمون وسائل التواصل بشكل موجه وواضح نحو الهدف.

- **الإناث:**

◊ من المحتمل أن تُظهر الإناث ميلاً أكبر لاستخدام وسائل التواصل الاجتماعي لتعزيز العلاقات الاجتماعية داخل بيئة العمل، مما يساهم في تقوية الروح الجماعية والتعاون بين أعضاء الفريق.

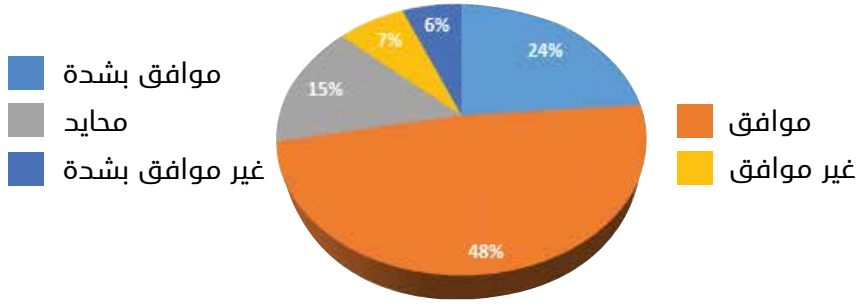
◊ قد تجد الإناث وسائل التواصل الاجتماعي مفيدة في إيجاد توازن بين الحياة الشخصية والعملية، حيث يمكن أن يستخدموها للبقاء على اتصال مع العائلة والأصدقاء إلى جانب زملاء العمل.

◊ من ناحية أخرى، يمكن أن تكون الإناث أكثر عرضة للإجهاد الناتج عن التفاعل المستمر على وسائل التواصل الاجتماعي، حيث قد يشعرن بالضغط للاستجابة السريعة للتواصل المستمر مع الآخرين.

تعتبر ديناميكية العمل الجماعي أحد العوامل الأساسية لتحقيق الأداء العالي في الهيئة، حيث تساهم وسائل التواصل الاجتماعي في تعزيز هذا التعاون من خلال توفير منصات تواصل فعالة. تعمل هذه المنصات على تسهيل تبادل المعلومات والأفكار بين الموظفين، مما يؤدي إلى زيادة الفهم المشترك وتعزيز الإبداع الجماعي. على سبيل المثال، يشير استخدام التطبيقات مثل واتساب وفيسبوك إلى أن التواصل الفوري بين الموظفين يسهم في بناء علاقات عمل متينة، مما يعزز من التفاعل الإيجابي ويقلل من حواجز التواصل. علاوة على ذلك، تظهر الأبحاث أن تحسين العلاقات الاجتماعية داخل بيئة العمل ينعكس بشكل إيجابي على أداء الموظفين ويساهم في تحقيق أهداف المؤسسة لذلك، يجب على الهيئة استثمار هذه التقنيات لتعزيز روح الفريق والعمل الجماعي، مما يسهم في تحسين الإنتاجية وزيادة رضا الموظفين

ومن ناحية أخرى أن الاستخدام المفرط لهذه الوسائل يمكن أن يؤدي إلى إجهاد الموظفين وفقدان التركيز، حيث تنصب المشكلات بشكل خاص على تأثر العلاقات الأسرية والاجتماعية سلبًا، مما يقلل من جودة الحياة. من جهة أخرى، إذا ما تم استخدام وسائل التواصل الاجتماعي بشكل حكيم، فإنها يمكن أن تساهم في تعزيز التواصل بين الموظفين، مما يسهم في تحسين الروح المعنوية والإنتاجية في بيئة العمل لذا، من المهم تطوير استراتيجيات تضمن الاستخدام الإيجابي لهذه الوسائل، مما يؤثر بشكل إيجابي على التوازن بين الحياة العملية والشخصية يتطلب تحقيق هذا التوازن إدراكًا شاملًا للأبعاد الاجتماعية والنفسية لاستخدام التكنولوجيا الحديثة في حياتنا.

استخدام وسائل التواصل الاجتماعي في العمل
يزيد من الرضا الوظيفي بين المواظفين.



2. الفروق في مدى التأثر السلبي أو الإيجابي:

- **الفروق في الرضا الوظيفي:**

◊ أظهرت بعض الدراسات أن الإناث قد يشعرن بزيادة الرضا الوظيفي عند استخدام وسائل التواصل الاجتماعي كوسيلة للتواصل مع زملائهن، لأنها تعزز من إحساسهن بالانتماء والاندماج في الفريق.

◊ في المقابل، قد يشعر الذكور بالرضا الوظيفي عند استخدام هذه الوسائل لتحسين الأداء الشخصي والمهني، مثل إيجاد حلول جديدة لمشاكل العمل أو تسهيل إنجاز المهام.

- **الفروق في تأثير الإجهاد:**

◊ الإناث قد يكن أكثر عرضة للتأثر بمستوى الإجهاد والإرهاق النفسي الناتج عن التواصل المستمر، مما قد يؤثر سلبًا على مستوى الأداء في بعض الأحيان، خاصة إذا شعرت بالتوقعات المرتفعة للاستجابة الفورية.

◊ الذكور قد يكونون أقل تأثرًا بالإجهاد الناتج عن التواصل المستمر، حيث يمكن أن يكون لديهم نظرة عملية أكثر لاستخدام وسائل التواصل الاجتماعي، ما يجعلهم يحددون أوقات استخدام هذه الوسائل بناءً على احتياجات العمل فقط.

3. الفروق في التأثير على مستوى التركيز:

- الإناث يشعرن بأن التفاعل الاجتماعي المستمر عبر وسائل التواصل يجعل بيئة العمل أكثر مرونة وسلاسة، لكن هذا قد يأتي على حساب التركيز أثناء أداء المهام.
- الذكور يرون أن الاستخدام المفرط لوسائل التواصل الاجتماعي يمكن أن يؤثر سلباً على مستوى التركيز أثناء أداء المهام، لكن قد يكونون أكثر قدرة على التحكم في استخدامهم لتقليل هذا التأثير السلبي.

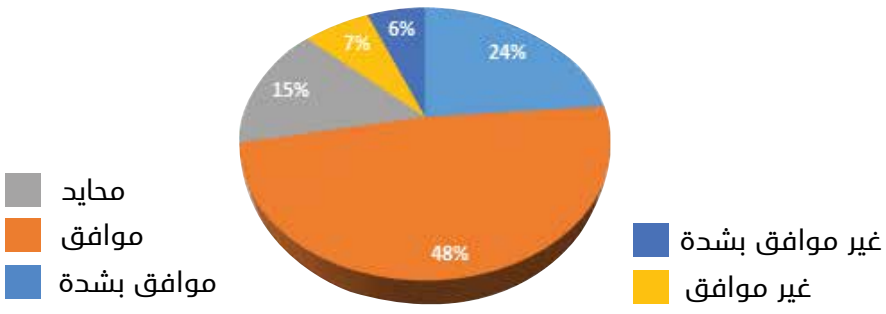
يعتبر الانشغال المستمر بمواقع التواصل الاجتماعي أحد العوامل الرئيسية التي تؤدي إلى تشتت انتباه الموظفين أثناء العمل، مما يعكس تأثيره السلبي على أدائهم.

العديد من الدراسات أظهرت أن هذا الانشغال المتواصل قد يُساهم في تقليل التركيز على المهام المحددة، بتسبب ما يُعرف حالياً بظاهرة الإلهاء الرقمي. تُشير نتائج البحث إلى أن الموظفين الذين يُستخدمون وسائل التواصل كمصدر مستمر للتواصل قد يجدون صعوبة في إعادة الانتباه إلى المهام الأساسية، مما يُسهم في تدهور جودة العمل المتحقق ورفع معدلات الأخطاء بالتالي، يُعتبر وضع استراتيجيات فعالة لتنظيم وتقييد استخدام هذه المواقع أثناء أوقات العمل ضرورة مُلحة لتعزيز التركيز والإنتاجية، مما يُساعد المؤسسات على تحقيق أهدافها بكفاءة عالية. إن فهم هذه الديناميكيات يُعد أساسياً لتطوير بيئات عمل صحية وفعّالة تتسم بالإنتاجية العالية

4. الفروق في تأثير وسائل التواصل الاجتماعي على الإبداع والابتكار:

- تُظهر الإناث تقديرًا أكبر لاستخدام وسائل التواصل الاجتماعي كوسيلة للحصول على أفكار جديدة وحلول مبتكرة للمشاكل، حيث يمكن أن يجدن في التفاعل الاجتماعي المتنوع مصدرًا للإلهام والتعلم.
- الذكور، من ناحية أخرى، قد يركزون على استخدام وسائل التواصل الاجتماعي للوصول إلى موارد ومعلومات متخصصة تسهم في تحسين أداء العمل مباشرة، مما يجعل استخدامهم أكثر تركيزًا على الجوانب التقنية والعملية.

استخدام وسائل التواصل الاجتماعي يسهم في الحصول على أفكار جديدة وحلول مبتكرة للمشكلات الوظيفية.



تعد بيئة العمل المبتكرة ضرورية لتعزيز الأداء والإنتاجية لدى الموظفين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ. تشير الدراسات إلى أن إدماج وسائل التواصل الاجتماعي يمكن أن يسهم بشكل كبير في تسهيل الابتكار والإبداع من خلال تعزيز التواصل بين الموظفين وفتح قنوات جديدة لتبادل الأفكار. من خلال هذه المنصات، يمكن للموظفين التواصل بحرية أكبر، مما يعزز روح التعاون بينهم ويحسن من جودة الحلول المقدمة للتحديات التي تواجههم علاوة على ذلك، تساعد هذه الأدوات على تيسير الوصول إلى المعرفة والموارد، مما يسهم في تعزيز قدرة الأفراد على التفكير الإبداعي وتطبيق أفكار جديدة في عملهم لذلك، يمثل الاستخدام الفعال لوسائل التواصل الاجتماعي ركيزة أساسية في تحسين مستوى الأداء وتحقيق أهداف الهيئة، مما يخلق بيئة عمل محفزة تعزز الابتكار والإبداع

5. العوامل التي تؤثر على استخدام وسائل التواصل الاجتماعي:

- **الضغوط الاجتماعية:** الإناث قد يشعرن بضغط أكبر للبقاء متصلات والتفاعل مع زملاء العمل عبر منصات التواصل الاجتماعي، مما قد يجعلهن أكثر تأثراً بالتوقعات الاجتماعية.
- **الفروقات الثقافية:** قد تؤثر الخلفية الثقافية بشكل مختلف على استخدام كل من الذكور والإناث لوسائل التواصل الاجتماعي في بيئة العمل، حيث قد يُنظر إلى استخدام وسائل التواصل بشكل مختلف بناءً على المعايير الثقافية المتعلقة بالتواصل المهني والاجتماعي.

التوصيات:

- تصميم استراتيجيات تواصل مرنة تراعي الفروق بين الجنسين في استخدام وسائل التواصل الاجتماعي، مما يساعد على تحسين الاستفادة منها دون التسبب في إجهاد أو انخفاض التركيز.
- تقديم برامج تدريبية تساعد الموظفين على كيفية إدارة وقتهم واستخدام وسائل التواصل الاجتماعي بشكل فعّال، بما يتناسب مع احتياجات كل جنس.

- تطوير سياسات استخدام وسائل التواصل الاجتماعي في العمل لضمان تحقيق توازن بين الفوائد والتحديات، وضمان بيئة عمل منتجة.

ما تأثير وسائل التواصل على إنتاجية الموظفين

تأثير وسائل التواصل الاجتماعي على إنتاجية الموظفين يمكن أن يكون معقداً ومتنوعاً، حيث يحتوي على جوانب إيجابية وسلبية تعتمد على كيفية استخدامها وطريقة دمجها في بيئة العمل. سأقوم بتحليل تأثير وسائل التواصل الاجتماعي على إنتاجية الموظفين من عدة جوانب، بناءً على النتائج التي تمت ملاحظتها من استبيانك والمعطيات العلمية المرتبطة

الجوانب الإيجابية لاستخدام وسائل التواصل الاجتماعي على الإنتاجية:

- **تحسين التواصل والتعاون بين الموظفين:**

◊ وسائل التواصل الاجتماعي يمكن أن تسهل التواصل بين الأعضاء في الفريق، خاصة إذا كانوا يعملون عن بعد أو في مواقع مختلفة. هذا يعزز التنسيق والتعاون، مما يمكن أن يؤدي إلى إنجاز المهام بشكل أسرع وأكثر كفاءة.

◊ المنصات مثل teem xebew أو smaeT تسمح بالتواصل السريع ومشاركة المعلومات، مما يقلل من زمن انتظار الردود أو التوضيحات، وبالتالي يساهم في تحسين الأداء العام للفريق.

- **مصدر للإبداع والأفكار الجديدة:**

◊ من خلال التفاعل على منصات مثل nIdekniL أو المنتديات المهنية، يمكن للموظفين استلهام أفكار جديدة أو الحصول على حلول مبتكرة للمشكلات التي يواجهونها في العمل. هذا يمكن أن يعزز من كفاءة العمل ويساعد في تحسين الأداء.

◊ بعض المستجيبين من الاستبيان أشاروا إلى أن التفاعل المستمر مع الأفكار الجديدة يمكن أن يكون دافعًا للإبداع والتجديد في العمل، مما ينعكس إيجابًا على الإنتاجية.

- **تعزيز الرضا الوظيفي:**

◊ وسائل التواصل الاجتماعي يمكن أن تساهم في تعزيز الرضا الوظيفي من خلال توفير فرص للتعبير عن الأفكار وتبادل الخبرات مع الزملاء. عندما يشعر الموظفون بأن لديهم منصة للتواصل والمشاركة، قد يكونون أكثر حماسًا للعمل وأكثر استعدادًا لبذل جهد إضافي، مما ينعكس على إنتاجيتهم.

1.التأثيرات الإيجابية لوسائل التواصل الاجتماعي على أداء الموظفين

تعتبر القدرة على الوصول إلى المعلومات الضرورية والموارد أحد العوامل الأساسية التي تؤثر على أداء الموظفين. يعد استخدام وسائل التواصل الاجتماعي من الأدوات الفعالة التي تسهم في تعزيز هذه القدرة، مما ينعكس إيجابًا على الأداء الوظيفي. وفقًا لدراسة، يمكن أن يؤدي زيادة التفاعل الإيجابي عبر المنصات الاجتماعية إلى تحسين معايير المسؤولية الاجتماعية في الهيئة، مما يدعم جهود الموظفين في تطوير استراتيجيات عمل فعالة. ووجود تحولًا في طرق تفاعل الموظفين مع المعلومات، حيث أصبحت منصات مثل فيسبوك وتويتر وسائل رئيسية للتواصل وتبادل المعرفة، مما يعزز التعاون بين الموظفين. من الضروري أن تتمكن الهيئة من استغلال هذه الأدوات بشكل جيد، مما يساهم في تحسين البيئة التنظيمية ويعزز من فاعلية الأداء بصفة عامة، خاصة في السياقات الحكومية التي تتطلب تبادل معلومات سريع ودقيق. لذا، يحتاج الأمر إلى وضع استراتيجيات تُمكن الموظفين من استخدام وسائل التواصل الاجتماعي بطريقة تعزز من قدراتهم على الوصول إلى المعلومات والموارد اللازمة لأداء مهامهم بكفاءة

كما أن استخدام وسائل التواصل الاجتماعي يمكن أن يعزز من أداء الموظفين من خلال تحسين التواصل وتعزيز التعاون بينهم، حيث أن الانخراط في وسائل التواصل الاجتماعي يعزز من الرفاه النفسي لدى الموظفين، مما يؤدي بدوره إلى تحسين أداء العمل فالإيجابيات المرتبطة بالوصول السريع إلى المعلومات وتبادل المعرفة تجعل من

وسائل التواصل الاجتماعي أداة فعالة لتحسين الإنتاجية وزيادة التفاعل بين الزملاء.

علاوة على ذلك أن الموظفين الذين يستفيدون من المنصات في تحسين العلاقات الاجتماعية داخل العمل يتمتعون بمستوى عالٍ من الرضا الوظيفي، وبالتالي ينعكس ذلك بشكل إيجابي على أدائهم. من المهم أن تسعى الهيئة الى استغلال هذه الخصائص الإيجابية لتحقيق أهدافها وتعزيز بيئة العمل، حيث تعتبر منصات التواصل الاجتماعي فضاءات حيوية تتيح للموظفين فرصة للتواصل وبناء علاقات مهنية تسهم في التطوير المهني. من خلال هذه المنصات، يمكن للعاملين تبادل الأفكار والخبرات وتعزيز مهاراتهم عبر الانخراط في مناقشات مهنية متخصصة. فعلى سبيل المثال، تساهم الشبكات الاجتماعية في تعزيز التعاون بين الموظفين، مما يؤدي إلى زيادة الفعالية العامة في بيئة العمل. ومن خلال التفاعل المستمر مع زملاء العمل والاستفادة من التجارب الحياتية المختلفة، يمكن للعاملين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ أن يُبنوا شبكة دعم مهنية متينة، مما يساعدهم في تحقيق الأهداف المهنية والشخصية. لذا، ينبغي على الإدارات تعزيز استخدام هذه الأدوات بطرق منظمة، بالإضافة إلى تقديم التدريب اللازم تؤدي هذه المبادرات إلى توفير بيئة عمل محفزة تدعم التطور المستدام للأفراد داخل الهيئة.

2. الجوانب السلبية لاستخدام وسائل التواصل الاجتماعي على الإنتاجية:

- **الإفراط في الاستخدام وتأثيره على التركيز:**

◊ أشار حوالي 53. 69% من المستجيبين إلى أن الإفراط في استخدام وسائل التواصل الاجتماعي يمكن أن يؤدي إلى انخفاض التركيز أثناء أداء المهام. قد يؤدي ذلك إلى تشتت الانتباه، حيث يمكن أن يجد الموظفون أنفسهم ينشغلون بالمنشورات والتحديثات بدلاً من التركيز على العمل المطلوب.

◊ التنقل المستمر بين العمل والتفاعل على وسائل التواصل قد يؤدي إلى ضياع الوقت وزيادة الوقت اللازم لإنجاز المهام، مما يقلل من الكفاءة العامة.

- **الإجهاد والإرهاق النفسي:**

◊ التفاعل المستمر على وسائل التواصل الاجتماعي يمكن أن يؤدي إلى زيادة مستوى الإجهاد لبعض الموظفين، خاصة إذا كانوا يشعرون بأنهم مضطرون للبقاء متصلين طوال الوقت. هذا الإجهاد يمكن أن يؤثر سلبًا على مستوى الأداء والإنتاجية، حيث قد يحتاج الموظف إلى وقت أطول للتعافي والتركيز على المهام.

◊ بعض المستجيبين أشاروا إلى أن التفاعل المستمر يمكن أن يخلق بيئة عمل مرهقة، مما قد يؤدي إلى تقليل الحافز للعمل وتقليل الإنتاجية.

- **تأخير إنجاز المهام:**

◊ الانشغال بوسائل التواصل الاجتماعي خلال العمل قد يؤدي إلى تأخير في إنجاز المهام المطلوبة، حيث يمكن أن يجد الموظفون أنفسهم ينشغلون بالاطلاع على المستجدات والرسائل بدلاً من التركيز على المهام العاجلة. أشار حوالي 13. 85% من المستجيبين إلى أن هذا يمكن أن يكون عاملاً سلبياً في بيئة العمل.

◊ تُعتبر البيئة الرقمية، وخاصة وسائل التواصل الاجتماعي، سلاحًا ذا حدين، حيث يمكن أن تُعزّز من سرعة تبادل المعلومات وتفاعل الأفراد، لكنها في الوقت ذاته تخلق فرصًا لنشر المعلومات الخاطئة وسوء الفهم. إن التحليل الدقيق لطبيعة المعلومات المتداولة على هذه المنصات يكشف عن أن التوجه إلى نشر أخبار غير موثوقة يمكن أن يؤثر سلبًا على أداء الموظفين وأن انعدام المصداقية في المعلومات يمكن أن يؤدي إلى تضارب في الآراء وخلق توترات بين العاملين، مما يؤثر على الروح الجماعية والأداء العام علاوة على ذلك، تعني قلة الوعي حول كيفية التحقق من المعلومات أن الموظفين قد يتبنون رؤى خاطئة أو غير دقيقة، مما ينعكس سلبًا على اتخاذ القرارات الاستراتيجية أو تنفيذ المهام اليومية بكفاءة.

3. العوامل التي تؤثر على تأثير وسائل التواصل الاجتماعي على الإنتاجية:

- **الضوابط التنظيمية في بيئة العمل:**

◊ إذا كانت المؤسسة لديها سياسات واضحة لاستخدام وسائل التواصل الاجتماعي

في العمل، يمكن أن يتم التحكم في كيفية استخدام الموظفين لهذه الوسائل، مما يقلل من الآثار السلبية ويزيد من الآثار الإيجابية.

- ◊ تحديد أوقات معينة لاستخدام وسائل التواصل الاجتماعي أو استخدام المنصات المخصصة للعمل يمكن أن يساهم في تحسين إدارة الوقت، ويضمن بقاء الموظفين مركزين على مهامهم الرئيسية.
- ◊ تُعتبر بيئة العمل المحفزة ضرورة لتحقيق الأداء الفعال للموظفين، حيث يسهم التواصل الجيد بين الأفراد في تعزيز التعاون وزيادة الإنتاجية. يُظهر استخدام وسائل التواصل الاجتماعي في المؤسسات، مثل الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ، دورًا حيويًا في تحسين التواصل بين الموظفين، مما يؤدي إلى تقليل الفجوات المعلوماتية وزيادة الشعور بالانتماء لدى الأفراد. يتضح أن الاستخدام المنظم لهذه الوسائل يمكن أن يُعزز من جودة التفاعلات اليومية ويساهم في خلق ثقافة مؤسسية قائمة على التعاون والابتكار، حيث يتيح تبادل الأفكار والملاحظات بشكل فوري. علاوة على ذلك، تحتاج المؤسسات إلى إنشاء استراتيجيات واضحة لإدارة هذا التواصل، لتفادي تحديات مثل تشتت الانتباه وفقدان التركيز الناتج عن الاستخدام غير المنضبط. بالتالي، فإن تعزيز التواصل الفعال بين الموظفين يعدّ خطوة أساسية نحو تحسين الأداء المؤسسي وتحقيق الأهداف المشتركة.

- **الفروق بين الأفراد:**

◊ العمر، الجنس، وسنوات الخبرة يمكن أن تلعب دوراً في كيفية استجابة الموظفين لتأثيرات وسائل التواصل الاجتماعي. على سبيل المثال، الموظفون الأكبر سناً والأكثر خبرة قد يكونون أكثر قدرة على إدارة وقتهم بشكل فعال عند استخدام وسائل التواصل الاجتماعي مقارنة بالموظفين الأصغر سناً.

◊ الفروق الشخصية: بعض الأفراد قد يكونون أكثر ميلاً للتشتت عند استخدام وسائل التواصل الاجتماعي، بينما قد يكون آخرون قادرين على استخدام هذه الوسائل بشكل فعال لتعزيز عملهم.

4. التوصيات لتحسين تأثير وسائل التواصل الاجتماعي على الإنتاجية:

- تحديد سياسات استخدام واضحة: وضع إرشادات للاستخدام المسموح به لوسائل التواصل الاجتماعي خلال ساعات العمل، مثل تحديد أوقات الاستراحة لاستخدام المنصات الاجتماعية.
- تشجيع الاستخدام الفعّال: توفير التدريب على كيفية استخدام وسائل التواصل الاجتماعي كأداة لتطوير العمل والتعلم المهني بدلاً من كونها مصدرًا للتسلية فقط.
- تعزيز بيئة العمل المرنة: السماح بالتفاعل الاجتماعي بشكل معتدل يمكن أن يعزز من الروح الجماعية دون التأثير على الإنتاجية.

الاستنتاج النهائي:

وسائل التواصل الاجتماعي يمكن أن تكون أداة قوية لتحسين الإنتاجية إذا تم استخدامها بشكل صحيح، ولكنها قد تكون عائقًا إذا لم تكن هناك سياسات واضحة لضبط استخدامها. الأثر يعتمد بشكل كبير على عادات الاستخدام الفردية، والضوابط المؤسسية، والثقافة التنظيمية.

لذلك، من الضروري على الهيئة أن

- تضع استراتيجيات توازن بين فوائد التواصل الاجتماعي والتحديات التي يمكن أن تنتج عنه .
- تحليل أعمق للعوامل المؤثرة في الأداء الوظيفي المرتبط بوسائل التواصل الاجتماعي.
- دراسة تأثير استخدام وسائل التواصل الاجتماعي على جوانب أخرى من الأداء الوظيفي مثل الإبداع، التعاون، والروح الجماعية.
- اختبار استراتيجيات تدخلية لتحسين استخدام وسائل التواصل الاجتماعي في بيئة العمل لتعزيز الإنتاجية والرضا الوظيفي.

المبحث الثالث

مناقشة النتائج والتوصيات

المطلب الأول: مناقشة النتائج في ضوء الأدبيات

1. التأثيرات السلبية لوسائل التواصل الاجتماعي على أداء الموظفين

تعتبر وسائل التواصل الاجتماعي أداة قوية لتعزيز التواصل بين الموظفين، لكن استخدامها الزائد يمكن أن يؤدي إلى آثار سلبية تشمل تشتت الانتباه وانخفاض الإنتاجية. الأبحاث تظهر أن الكثير من الموظفين يواجهون صعوبة في إدارة الوقت بسبب الانغماس في هذه المنصات، مما ينعكس سلبًا على جودة الأداء وفعالية إنجاز المهام الوظيفية. علاوة على ذلك، تشير الدراسات إلى أن وسائل التواصل الاجتماعي قد تؤدي إلى تفشي الثقافة السلبية داخل بيئة العمل، حيث يتم تداول الشائعات والمعلومات غير الدقيقة، مما يؤثر على الحالة النفسية للموظفين ويزيد من شعورهم بالإحباط (ط. د. اليزيد مقدم la te., 1202). لتحقيق أقصى فائدة من وسائل التواصل الاجتماعي، يجب وضع استراتيجيات واضحة لتوجيه استخدامها، وتوفير برامج تدريبية تركز على كيفية إدارة الوقت وتقليل المخاطر المرتبطة بذلك (oM demmahoM siraF ayahS, 9102)(5591-40)

2. وجهات نظر العاملين حول استخدام وسائل التواصل الاجتماعي

تؤثر وسائل التواصل الاجتماعي بشكل ملحوظ على الأداء الوظيفي للعاملين داخل الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ، حيث تعكس وجهات نظر العمال تباينًا في الاستخدام والتأثير. تشير الدراسات إلى أن هذه الوسائط تعزز من التواصل بين الزملاء، مما يسهم في تحسين جودة العمل وزيادة الإنتاجية (dhaF .rD nib liqaoM iIA-IA, 8102). على الرغم من الفوائد المعروفة، هناك مخاوف من أن الاستخدام غير المنظم لهذه المنصات قد يؤدي إلى تشتت الانتباه وانخفاض مستويات الأداء. وفقًا لدراسة أجريت في سياقات مشابهة، أظهرت النتائج أن نسبة كبيرة من العمال يشعرون بأن استخدام وسائل التواصل الاجتماعي أثناء ساعات العمل يمكن أن

يسهل الوصول إلى المعلومات، ولكنه في نفس الوقت قد يحجب الفعالية (gnipuhS oahZ, 4202). لذا، يُنصح بضرورة تطوير استراتيجيات تنظيمية واضحة لاستغلال فوائد هذه الوسائط وتعزيز التفاعل الإيجابي بينها وبين الأداء الوظيفي

3.المواقف تجاه وسائل التواصل الاجتماعي في مكان العمل

تواجه المؤسسات تحديات كبيرة تتعلق بمواقف الموظفين تجاه استخدام وسائل التواصل الاجتماعي في بيئة العمل. تشير الدراسات إلى أن الاستخدام المناسب لهذه المنصات يمكن أن يسهم في تعزيز التفاعل بين الزملاء، مما يؤدي إلى تحسين الأداء الوظيفي بشكل عام (منصور، أيمن عبدالرحيم فرج، الفليت، خلود عطية أحمد, 2202). ومع ذلك، يمكن أن يسهم الاستخدام غير المنظم لهذه الوسائل في تقليل الالتزام الإداري، حيث أظهرت نتائج دراسة شملت موظفي وزارة الاتصالات وتكنولوجيا المعلومات في فلسطين ارتباطًا إيجابيًا بين استخدام وسائل التواصل الاجتماعي والرضا الوظيفي (ط. د. اليزيد مقدم la te., 1202). كما أظهرت الأبحاث أن الموظفين غالبًا ما يستفيدون من وسائل التواصل الاجتماعي لتبادل المعرفة والتعاون، مما يعزز من كفاءة العمل الجماعي (zehcnaS-oyapmaC odnanreF, 4202). ومع ذلك، فإن هذه الفوائد قد تأتي مع تحديات، مثل الانحراف عن المهام الأساسية وفقدان التركيز، وهو ما يتطلب تطوير استراتيجيات واضحة لإدارة استخدام وسائل التواصل الاجتماعي في مكان العمل (eH gnoiqnauY, 4202)

4.الفوائد المدركة لوسائل التواصل الاجتماعي من وجهة نظر الموظفين

تعتبر وسائل التواصل الاجتماعي من الأدوات المهمة التي تؤثر بشكل كبير على أداء الموظفين، حيث توفر منصات سهلة للتواصل وخلق بيئة عمل تفاعلية. يرى العديد من الموظفين أن استخدام هذه الوسائل يسهم في تعزيز تبادل المعلومات وزيادة سرعة التواصل بينهم، مما يسهل إنجاز المهام وتحقيق الأهداف المرسومة. بالطبع، لا تقتصر الفوائد على تحسين التواصل، بل تشمل أيضًا تعزيز التعاون بين الفرق المختلفة من

خلال مشاركة المعرفة والخبرات، كما توضح بعض الدراسات (منصور، أيمن عبدالرحيم فرج، الفليت، خلود عطية أحمد, 2202). ومع ذلك، يجب اعتبار تلك الفوائد في سياق الاستخدام المسؤول، حيث إن الاستخدام المفرط قد يؤدي إلى تشتت الانتباه وانخفاض الإنتاجية (ayahS siraF demmahoM, 9102). ولذلك، من الضروري أن تقوم المؤسسات بوضع استراتيجيات لتنظيم استخدام وسائل التواصل الاجتماعي بحيث تعزز الفوائد المدركة مع تقليل المخاطر المحتملة (5591-40)

5. المخاوف التي أثارها الموظفون بشأن استخدام وسائل التواصل الاجتماعي

تتباين مخاوف الموظفين بشأن استخدام وسائل التواصل الاجتماعي في بيئة العمل، حيث يعبر العديد منهم عن قلقهم تجاه تأثير هذه الوسائل على الأداء الوظيفي. يعد الانشغال الزائد عن العمل بمتابعة الأنشطة على منصات مثل فيسبوك وواتساب من أبرز العوامل التي تؤثر سلبًا على مستوى الإنتاجية، مما يؤدي إلى تراجع جودة العمل. كما يثير البعض مخاوف تتعلق بحماية المعلومات الشخصية والسرية، حيث يُعتبر مشاركة المحتوى على هذه الشبكات عرضة للتسريبات وانتهاك الخصوصية (danaS ibrahlA fialuhK, 0202). بالإضافة إلى ذلك، يشعر الموظفون بالقلق من المقارنات الاجتماعية والتأثير السلبي الذي قد يحدث على صحتهم النفسية نتيجة تلك المقارنات، حيث يساهم استخدام وسائل التواصل في تعزيز ضغوط العمل والتوتر (نصير صالح بوعلي, 0202). هذه المخاوف تدعو المؤسسات إلى وضع استراتيجيات واضحة تضبط استخدام هذه الوسائل وتُعزز من وعي الموظفين بمخاطرها، لضمان تحقيق توازن صحي بين العمل والحياة الشخصية (ayahS siraF demmahoM, 9102)(lanoitaN licnuoC ecnegilletnI, 1202-30)

6.اختلاف تأثير وسائل التواصل الاجتماعي عبر الأقسام المختلفة

تمثل وسائل التواصل الاجتماعي في الوقت الراهن عنصرًا حيويًا في بيئات العمل، حيث تختلف تأثيراتها من قسم إلى آخر. في بعض الأقسام، مثل قسم العلاقات

العامة، تُعتبر وسائل التواصل نافذة لتعزيز التواصل وبناء العلاقات مع العملاء، مما يساهم في رفع مستوى الأداء وزيادة الإبداع في استراتيجيات التسويق. في المقابل، تُشير الدراسات إلى أن تأثير وسائل التواصل الاجتماعي في الأقسام التقنية قد ينعكس سلبًا، حيث تزداد احتمالية تشتت تركيز الموظفين نتيجة التفاعل المستمر عبر هذه المنصات (ayahS siraF demmahoM, 9102). إن فهم هذه الاختلافات أمرٌ حيوي لتحسين الأداء العام في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ، مما يستدعي وضع استراتيجيات تستهدف تعزيز الجوانب الإيجابية وتقليل السلبيات حسب طبيعة كل قسم (iroL arooN, 9102-80-22). بالتالي، يتعين على إدارة الموارد البشرية العمل على خلق بيئة تدعم الاستخدام الفعّال لوسائل التواصل الاجتماعي مع الأخذ بعين الاعتبار خصائص كل قسم

7. تأثير العمر والفروق بين الأجيال على إدراك وسائل التواصل الاجتماعي

تتأثر وسائل التواصل الاجتماعي بشكل كبير بتغيرات العمر والفروق بين الأجيال، مما يعكس اختلافات واضحة في كيفية إدراك الأفراد لهذه المنصات. تشير الدراسات إلى أن الأجيال الشابة تتمتع بقدرة أكبر على استخدام التكنولوجيا ووسائل التواصل الاجتماعي بشكل متقن، مما يسهم في تعزيز أدائهم الوظيفي، كما هو موضح في (منصور، أيمن عبدالرحيم فرج، الفليت، خلود عطية أحمد, 2202)، حيث تلعب وسائل التواصل دوراً مهماً في تحسين الرضا الوظيفي. من ناحية أخرى، يواجه الجيل الأكبر سناً تحديات في التكيف مع هذه الأدوات الرقمية، مما قد يؤثر سلباً على تفاعلاتهم في بيئة العمل. كما يظهر أن الاختلافات بين الأجيال تؤثر على استخدام وسائل التواصل الاجتماعي في المؤسسات الحكومية، حيث تبين وجود قواسم مشتركة بين استعمال هذه الوسائل وتوجهات الأداء الوظيفي (hsiemO idnaF, 4202)(nemraC-led-aíraM, omA-led-nócralA, 4202). هذه الفروق تستوجب من القائمين على تطوير الموارد البشرية تبني استراتيجيات مصممة وفقاً لاحتياجات كل جيل لزيادة فعالية الأداء وتعزيز التفاعل بين الموظفين

8. قضايا التنمر الالكتروني

تشكل البيئة الرقمية اليوم فضاءً معقدًا يتداخل فيه التواصل بين الأفراد، مما يطرح تساؤلات حول السلامة النفسية وسلوكيات التنمر الالكتروني. في هذا السياق، يشير العديد من الدراسات إلى أن وسائل التواصل الاجتماعي قد ساهمت في زيادة حوادث التنمر الإلكتروني، حيث يصبح الفضاء الافتراضي ملاذًا لبعض الأفراد للتعبير عن سلوكيات عدوانية تجاه الآخرين، مما يترك آثارًا سلبية على صحة الأفراد النفسية ودرجة أدائهم في العمل. وقد أظهرت الأبحاث أن التنمر الإلكتروني يمكن أن يؤثر بشكل مباشر على معنويات الموظفين وإنتاجيتهم، حيث يؤدي الشعور بالتهديد أو الخوف من المضايقات إلى تدني الدافعية وانخفاض الأداء (la te laeNcM ,. 8102-40-60). لذلك، من الضروري أن تعمل المؤسسات على توفير بيئة عمل آمنة، تتضمن استراتيجيات واضحة للتوعية ومكافحة التنمر الإلكتروني، للحفاظ على رفاهية العاملين وأداءهم المتميز في إطار الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ.

9. مخاوف الخصوصية ومخاطر أمان البيانات

تُعد مخاوف الخصوصية ومخاطر أمان البيانات من القضايا الجوهرية التي تواجه الموظفين في إطار استخدام وسائل التواصل الاجتماعي داخل بيئات العمل. إذ يتسبب الاستخدام الواسع لهذه الوسائل في تعرض المعلومات الشخصية والمهنية لمخاطر تسرب البيانات وارتفاع مستويات الانتهاك. يُشير العديد من الباحثين إلى أن استخدام وسائل التواصل الاجتماعي يمكن أن يفضي إلى تقليل التركيز وتأثيرات سلبية على الأداء الوظيفي، فضلاً عن تفشي قلق الموظفين بشأن كيفية معالجة بياناتهم الشخصية من قبل المؤسسات. وعلاوة على ذلك، تشير الأبحاث إلى أن الموظفين في القطاع العام يمكن أن يشعروا بمزيد من الضغوط بسبب عدم وجود سياسات واضحة تحمي المعلومات الحساسة، مما يؤدي إلى ضعف الثقة في الإدارة (iroL arooN, 9102-80-22). لذلك، يتطلب الأمر تطوير استراتيجيات فعالة للتوجيه وإدارة هذه المخاطر من

أجل الحفاظ على سلامة البيانات وتعزيز أداء الموظفين بشكل يتماشى مع المعايير المطلوبة

10. التأثيرات السلبية على الصحة العقلية للموظفين

تعتبر الضغوط النفسية الناتجة عن استخدام وسائل التواصل الاجتماعي في بيئة العمل من العوامل الرئيسية المسببة للأثر السلبي على الصحة العقلية للموظفين. حيث يؤدي الاستخدام المفرط لهذه الوسائل إلى الشعور بالعزلة الاجتماعية، وفقدان التواصل المباشر مع الزملاء، مما يزيد من مستويات التوتر والقلق. تشير الدراسات إلى أن الانشغال بالتفاعلات الافتراضية يمكن أن يؤدي إلى تفاقم الاكتئاب ووهن العلاقات الشخصية (ط. د. اليزيد مقدم la te., 1202). بالإضافة إلى ذلك، فإن عدم وضوح الحدود بين الحياة المهنية والشخصية بسبب التسرب التكنولوجي قد يسهم في استنزاف الطاقة النفسية للموظفين، مما يعرقل قدرتهم على التركيز ورفع كفاءة أدائهم (ayahS siraF demmahoM, 9102)(1002). لذا، يعتبر من الضروري أن تقوم المؤسسات بتوفير بيئات عمل تعزز من التوازن النفسي وتحد من التأثيرات الضارة لوسائل التواصل الاجتماعي، مما يسهم في تحسين الصحة العقلية للموظفين وجودتهم في العمل.

11. انخفاض الإنتاجية بسبب الاستخدام المفرط لوسائل التواصل الاجتماعي

تُظهر الدراسات أن الاستخدام المفرط لوسائل التواصل الاجتماعي يمكن أن يؤدي إلى انخفاض ملحوظ في إنتاجية الموظفين، حيث يُعتبر التسرب الذهني الناتج عن التشتت والتفاعلات غير الرسمية واحدًا من أبرز المسببات لذلك. قد ينجذب الموظفون إلى تصفح المحتوى الترفيهي أو التفاعل مع أخبار شخصية بدلاً من التركيز على مهامهم الرسمية، مما يُعدّ هدرًا للوقت وتقليلًا للفعالية. تشير الأبحاث إلى أن شاشة الهاتف المحمولة قد تستهلك ما يصل إلى 2. 5 ساعة من وقت العمل كل يوم، مما يُعزز من السلبية في بيئة العمل (ibrahIA fialuhK danaS, 0202). إضافةً إلى ذلك، يفقد

الموظفون القدرة على تحقيق الأهداف المحددة نتيجة لتقلبات الانتباه، مما يجعل الحاجة إلى وضع استراتيجيات تنظيمية أكثر إلحاحًا من أي وقت مضى لضمان الاستخدام الفعّال للتكنولوجيا من دون التأثير سلبًا على الأداء (licnuoC ecnegilletnI lanoitaN, 1202-30)

المطلب الثالث: التوصيات والبحوث المستقبلية

تعد الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ من الجهات الحيوية التي تؤثر بشكل مباشر على الأمن الوطني وسلامة المجتمع. إذ أن تعزيز الأداء الوظيفي لموظفي هذه الهيئة يتطلب تكامل العمليات التكنولوجية مع استراتيجيات التواصل الاجتماعي، حيث يمكن لتلك الأدوات أن تسهم في تحسين التواصل بين الإدارات والفروع المختلفة بالإضافة إلى تحسين مستوى الخدمة المقدمة للجمهور. ومن خلال دمج وسائل التواصل الاجتماعي بفعالية، يمكن للموظفين الحصول على معلومات فورية وتحقيق تواصل مستمر مع الزملاء، مما يعزز من كفاءتهم وقدرتهم على الاستجابة السريعة للطلبات الطارئة، (hsayyA .N massI, 2202). ومن الضروري تطوير سياسات واضحة لاستخدام وسائل التواصل الاجتماعي لضمان تحقيق الأهداف المؤسسية مع تقليل التأثيرات السلبية المحتملة على الإنتاجية والتركيز في مهام العمل (fesuoY hemaS, 9102)، (iroL arooN, 9102-80-22).

1. اقتراحات الموظفين لوضع سياسات فعالة لوسائل التواصل الاجتماعي

تعد وسائل التواصل الاجتماعي أداة قوية تؤثر على بيئة العمل وتعزز من تواصل الموظفين، مما يتعين معه وضع سياسات فعالة تنظم استخدامها داخل الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ. يُمكن أن تسهم ممارسات الاستخدام المُنتظم لهذه الوسائل في زيادة الإبداع وتبادل المعرفة بين الموظفين، كما أشار إلى ذلك البحث الذي أظهر الارتباط الإيجابي بين التواصل الفعّال وزيادة الأداء الوظيفي (neM atiR naujniL, 4202). من الضروري أن تشمل السياسات المقترحة إرشادات واضحة تُحدد الأغراض المسموح بها لاستخدام هذه المنصات خلال ساعات

العمل، وتوفير تدريبات متعلقة بكيفية استخدامها بشكل إيجابي، بالإضافة إلى تشجيع الموظفين على المشاركة في محتوى يعزز من قيم العمل المشترك. كما يبدو أن بناء ثقافة تنظيمية تدعم الاستخدام البناء لوسائل التواصل الاجتماعي يُعتبر جزءاً أساسياً لتحقيق نتائج إيجابية، وهو ما أشارت إليه الدراسات السابقة التي تناولت تأثير هذه الممارسات على الأداء الوظيفي (gnahZ gnaixiY, 4202)

2. توصيات لتحسين استخدام وسائل التواصل الاجتماعي في مكان العمل

تُعتبر وسائل التواصل الاجتماعي أدوات فعّالة يمكن أن تُحدث تأثيرًا إيجابيًا في بيئات العمل إذا تم استخدامها بطرق مدروسة. يجب على المؤسسات تطوير استراتيجيات واضحة لاستخدام هذه الوسائل، مثل تحديد أهداف محددة للاستفادة منها، بما يسهم في تعزيز التواصل بين الموظفين وتحفيز الإبداع في العمل. علاوة على ذلك، من الضروري توفير تدريب شامل للموظفين يهدف إلى تحسين مهارات استخدام وسائل التواصل الاجتماعي، مما يدعم فهمهم للتحديات المحتملة ويعزز من قدرتهم على التعامل معها بفعالية (ayahS siraF demmahoM, 9102). ينبغي أيضًا إنشاء سياسات تُحدد أوقات وأساليب استخدام وسائل التواصل خلال ساعات العمل، لضمان تحقيق التوازن بين الاستفادة من هذه الأدوات والمحافظة على الإنتاجية (ط. د. اليزيد مقدم la te., 1202). وأخيرًا، يجب تشجيع بيئة مفتوحة ترتكز على التغذية الراجعة، مما يساعد في تقييم أداء استخدام وسائل التواصل بشكل دوري ويتيح تحسينات مستمرة في هذا الجانب (licnuoC ecnegilletnI lanoitaN, 1202-30)

3. أفكار نهائية حول التوازن بين وسائل التواصل الاجتماعي وأداء الموظفين

تتطلب البيئات المهنية الحديثة توازنًا فعّالًا بين استخدام وسائل التواصل الاجتماعي وأداء الموظفين، إذ إن الاستخدام المنضبط لهذه الوسائل يمكن أن يسهم بشكل إيجابي في تحسين الإنتاجية وتعزيز التواصل بين الأفراد داخل المنظمات. من المهم أن تدرك المؤسسات أن وسائل التواصل الاجتماعي ليست مجرد مصادر للتسلية بل أدوات استراتيجية يمكن أن تحسن من جودة العمل وتسرّع من إنجاز المهمات، كما ورد في

تجارب سابقة. ومع ذلك، فإن الاستخدام غير المنظم لها قد يؤدي إلى تشتت انتباه الموظفين وتقليل مستوى الأداء، مما يستدعي ضرورة وضع استراتيجيات محددة لتحسين استخدام هذه المنصات (ط. د. اليزيد مقدم la te., 1202). لذا، يتوجب على الإدارة توفير تدريبات للموظفين حول كيفية توظيف وسائل التواصل الاجتماعي لصالح أهداف المؤسسة، مما يعزز من ثقافة العمل الجماعي والابتكار، ويحقق نتائج إيجابية بشكل عام (9102 ,ayahS siraF demmahoM)(National Intelligence Council, 2021-03).

4. دعوة للعمل لقادة المنظمات وصانعي السياسات

في ظل التغيرات السريعة التي تشهدها بيئة العمل الحديثة بفعل انتشار وسائل التواصل الاجتماعي، تصبح الحاجة ماسة لقادة المنظمات وصانعي السياسات لإعادة التفكير في استراتيجياتهم الإدارية والتواصلية. ينبغي عليهم توظيف هذه الأدوات لتعزيز الأداء الوظيفي، وتيسير التواصل بين الموظفين، مما يعكس مدى تأثير هذه الوسائط على مستوى الانخراط والتحفيز. يتوجب على القادة أن يدركوا أن استخدام وسائل التواصل الاجتماعي ليس مجرد تسلية، بل يمكن أن يكون أداة فعالة لتعزيز الإنتاجية وتسهيل تبادل المعرفة بين الأفراد. من الضروري أيضًا وضع سياسات واضحة تنظم استخدام هذه الوسائل، بحيث تقلل من الآثار السلبية التي قد تؤثر على التركيز والإنتاجية. في النهاية، يتعين على الرواد وصناع القرار تحقيق توازن بين الفوائد المحتملة والمخاطر المرتبطة بالطبيعة الديناميكية لوسائل التواصل الاجتماعي، لضمان تحقيق أهداف مؤسساتهم بكفاءة وفاعلية

5. البحوث المستقبلية

تعتبر نتائج البحث الحالي عن تأثير وسائل التواصل الاجتماعي على أداء الموظفين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ بمثابة نقطة انطلاق للبحث المستقبلي. من المهم استكشاف كيفية تأثير مختلف منصات التواصل الاجتماعي على سلوكيات الموظفين، خصوصًا في سياق تعزيز الرضا الوظيفي وزيادة الإنتاجية. كما يمكن دراسة العلاقة بين مستوى استخدام وسائل التواصل الاجتماعي وبين مدى

الالتزام الوظيفي، وهو ما تشير إليه الأبحاث التي تسلط الضوء على العلاقة الإيجابية بين الاستخدام الفعال لوسائل التواصل وتحسين الأداء الوظيفي (ط. د. اليزيد مقدم te la., 1202). فمن خلال النظر في هذه الديناميكيات، يمكن تطوير استراتيجيات تساهم في إدارة استخدام وسائل التواصل الاجتماعي بشكل أكثر كفاءة، مما يساعد في تقليل تأثيراتها السلبية وزيادة فوائدها، كما تشير الدراسات إلى ضرورة دمج التوجهات التكنولوجية الحديثة في ممارسات العمل (uohZ gniJ, 4202)(snevetS knarF, 4202). بالنظر إلى ذلك، فإن البحث في تأثيرات وسائل التواصل الاجتماعي على أداء الموظفين يجب أن يتضمن تقييمات شاملة تتناول البيئات المختلفة والتوجهات الثقافية والتنظيمية في المستقبل

المراجع:

.1 boj no aidem laicos gnisu fo tcapmi ehT .(8102) .M .F ,ilA-lA .aibarA iduaS ni seicnega latnemnrevog ni ecnamrofrep

.2 gnitropxe fo scimanyd eht gnilievnU .(4202) .C-.M ,omA-led-nócralA .spihsnoitaler dna stsoc tropxe sepahs aidem laicos woH :smrif /ecneics/moc.tceridecneics.www//:sptth .weiveR ssenisuB lanoitanretnI 8370004213959690S/iip/elcitra

.3 lamrof gnirud aidem laicos gnisu fo tceffe ehT .(0202) .K .S ,ibrahlA fo lanruoJ .snoinipo 'seeyolpme morf ytivitcudorp nopu sruoh gnikrow .751–041 ,(1)4 ,secneicS lageL dna evitartsinimdA ,cimonocE

.4 .yeliW .efil laicos ni rewop dna egnahcxE .(4691) .M .P ,ualB

.5 بوعلي، ن. ص. (0202). أثر شبكات التواصل الاجتماعي على الأداء والتحصيل الدراسي للطلبة: دراسة ميدانية على عينة من طلبة جامعة الشارقة. المجلة العربية للإعلام والاتصال، 42، 36–29.

.6 :lias ruoy tsujda ,swolb dniw eht fI .(4202) .F ,zehcnaS-oyapmaC fo slannA .ecnamrofrep dna ,ytilibisnopser laicos ,ygoloedi lacitiloP /moc.tceridecneics.www//:sptth .021–301 ,801 ,hcraeseR msiruoT 4190004238370610S/iip/elcitra/ecneics

.7 pihsdneirf fo tceffe ehT :lauqe detaerc era sdneirf lla toN .(4202) .Y ,eH fo lanruoJ .aidem laicos no sda evitan derahs fo ecnamrofrep no epyt /moc.tceridecneics.www//:sptth .522–012 ,381 ,hcraeseR ssenisuB X8230042369284l0S/iip/elcitra/ecneics

.8 ehT !etinu ,dlrow eht fo sresU .(0102) .M ,nielneaH & ,.M .A ,nalpaK ,(1)35 ,snoziroH ssenisuB .aidem laicos fo seitinutroppo dna segnellahc .86–95

.9 snoitacifitarg dna sesU .(3791) .M ,hctiveruG & ,.G .J ,relmulB ,.E ,ztaK .325–905 ,(4)73 ,ylretrauQ noinipO cilbuP ehT .hcraeser

10. Lori, N. (2019). Offshore citizens. Cambridge University Press.

11. Mansour, A. A. F., & Al-Faleet, K. A. A. (2022). The effect of using social media sites in the work environment on employee performance: Job satisfaction as a mediating variable (Master's thesis). Islamic University of Gaza, Gaza, Palestine.

12. Men, L. R. (2024). The impact of diversity communication on employee organizational identification and employee voice behaviors: A moderated mediation model. Public Relations Review, 50, 75–90. https://www.sciencedirect.com/science/article/pii/S0363811124000717

13. 13. مقدم، اليزيد، & سيدهم، خ. هـ. (2021). مواقع التواصل الاجتماعي والأداء الوظيفي: دلالات التأثير على العمل بالمكتبات الجامعية: دراسة ميدانية بمكتبات جامعة 20 أوت 1955 سكيكدة. مجلة العلوم الإنسانية، 8(1), 280–292.

14. 14. National Intelligence Council. (2021). Global trends 2040. Cosimo Reports.

15. 15. Rubin, A. M. (1986). Uses, gratifications, and media effects research. In J. Bryant & D. Zillmann (Eds.), Perspectives on media effects (pp. 281–301). Lawrence Erlbaum Associates.

16. 16. Shaya, M. F. (2019). Use of social media by employees during work hours: Case study of employees of the Saudi Telecom Company STC. Journal of Economic, Administrative and Legal Sciences, 3(4).

17. 17. Stevens, F. (2024). An integrated evaluation framework for environmental, social, and governance-driven social media performance through multi-criteria decision-analysis. Decision Analytics Journal, 12, 100–115. https://www.sciencedirect.com/science/article/pii/S2772662224001097

18. 18. Ayyash, I. N. (2022). The impact of social media on employee productivity at the workplace. International Journal of Business Ethics and Governance, 5(1).

19. 19. Yousef, S. (2022). أثر استخدام تويتر في وقت العمل على الأداء الوظيفي. مجلة البحوث الإدارية، 41(157), 180–197.

20. 20. Zhou, J. (2024). The role of social media in CSR performance: An

integrated institutional and resource dependence perspective. Journal of Business Research, 184, 104–116. https://www.sciencedirect.com/9483004236928410S/iip/elcitra/ecneics

بحث عنوان:

تعزيز الوعي بالأمن السيبراني لدى موظفي الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ بشأن التهديدات والهجمات السيبرانية وتأثيرها على الأصول والممتلكات الرقمية

إعداد:
المهندس / محمد أحمد سعيد الزعابي
محاضر أكاديمي ومدرب
أكاديمية الامارات للهوية والجنسية

الملخص

هدفت الدراسة إلى تحديد التهديدات السيبرانية التي تواجه المستخدِم في الهيئة الإتحادية للهوية والجمارك وأمن المنافذ، وتقييم المستوى الحالي للوعي الأمني لدى موظفي الهيئة فيما يتعلق بالتهديدات السيبرانية وتأثيرها المحتمل على الأصول والممتلكات، ووضع مقترحات لتطوير برامج التوعية السيبرانية للموظفين لمواجهة التحديات السيبرانية الحالية والمستقبلية، وقد تكون مجتمع الدراسة من موظفي الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ، وهو يشمل مجموعة متنوعة من المنتسبين سواء كانوا ضباطًا، أفرادًا، أو مدنيين، واشتملت عينة الدراسة على (226) مفردة، واستخدم الباحث المنهج الكمي كمنهج للدراسة، واستعان الباحث بالاستبيان كأداة للدراسة، وقد توصل الباحث للعديد من النتائج أهمها

1. تشمل التهديدات السيبرانية على خطر الكوارث الطبيعية، والحروب السيبرانية، والجرائم الإلكترونية، بكل أنواعها، ومِن ضمنها الاختراق، وتخريب البنية التحتية، والولوج غير المرخص إلى البيانات، والتصيد الاحتيالي، وانتحال الهوية، وغيره.
2. المستوى الحالي للوعي بالأمن السيبراني لدى موظفي الهيئة يظهر أن هناك درجة عالية من الوعي بأهمية الأمن السيبراني، حيث يظهر ذلك من خلال متوسط مؤشر الوعي السيبراني الذي وصل إلى 17.68 (على 20)، وحصول 71 % من الإجابات على مؤشر وعي سيبراني أعلى من 16.81 %.
3. تتمثل مقترحات لتطوير برامج التوعية السيبرانية للموظفين لمواجهة التحديات السيبرانية الحالية والمستقبلية في إقامة ورش عمل ودورات تدريبية مكثفة، والتعليم الإلكتروني والموارد الذاتية، وتحديث وتوسيع سياسات الأمن السيبراني.

وقد أوصت الدراسة بالعديد من التوصيات أهمها: تصميم وتنفيذ برامج توعوية شاملة للموظفين حول كافة أنواع التهديدات السيبرانية، وتوجيه برامج التوعية إلى جميع موظفي الهيئة، بغض النظر عن وظائفهم أو مستوياتهم

الكلمات المفتاحية: الامن السيبراني، التهديدات والهجمات السيبرانية، الأصول والممتلكات الرقمية، الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ.

الفصل الأول

الإطار التنظيمي:

- **المقدمة:**

أصبحت جميع المؤسسات والهيئات والشركات مع التحول الرقمي تقدم خدماتها ومنتجاتها عبر المواقع الإلكترونية، والمنصات الرقمية، والتطبيقات الذكية، حيث بلغ عدد مستخدمي الإنترنت أكثر من نصف سكان الكرة الأرضية، الأمر الذي أدى إلى زيادة ملحوظة في الهجمات الإلكترونية والتهديدات الأمنية، نتج عنها خسائر مالية تقدر بملايين الدولارات. ولا شك أن كل مستخدم في العالم الرقمي يمتلك بيانات ومعلومات شخصية وعلى الصعيد الحكومي والمؤسسي، كذلك تمتلك أصول وممتلكات رقمية حساسة للغاية، وأن الولوج إلى تلك الأصول من قبل المخترقين وضعاف النفوس باتت مستهدفة، وذلك لعدة أسباب أبرزها تسريب البيانات، وتعطيل خط الإنتاج، وتدمير البني التحتية ولغايات التجسس

إن تأمين المعلومات أصبح هاجس الجميع، بل تعد أولوية قصوى، للحفاظ على الممتلكات والأصول الرقمية من التعدي عليها، أو الدخول غير المصرح به؛ إذ أن المستخدمون يشكلون عنصرًا حيويًا في سلسلة الأمان، حيث يمكن لقراراتهم وسلوكهم أن يلعبا دورًا حاسمًا في سلامة المعلومات. تحديدًا إذا لم يكن المستخدمين على دراية بالمخاطر الأمنية، أو لم يتبعوا ممارسات أمنية جيدة، فقد يتعرض النظام للتهديدات والهجمات بشكل أكبر. وتؤكد التقارير والدراسات بأن نسبة كبيرة من نجاح تلك الاختراقات الأمنية ناتجة عن قلة وعي المستخدم عن الأساليب المستخدمة في الحصول على البيانات، كالهندسة الاجتماعية، والتصيد الإلكتروني، وهجمات برامج الفدية، واستغلالهم للثغرات الأمنية في الأنظمة والشبكات والبرامج. وأن مثل تلك

الهجمات تؤدي إلى انتهاك البيانات، وتعطل الخدمات وإضرار بسمعة الهيئة

ويتولي الأمن السيبراني حماية الأنظمة الإلكترونية من الهجمات الخبيثة، إذ يشمل أجهزة الكمبيوتر والشبكات والخوادم والأجهزة المحمولة واستعادة البيانات بعد الهجوم، وتتجلى أهمية الوعي بالأمن السيبراني في دوره في حماية المعلومات الشخصية، والحفاظ على إنتاجية الموظفين، وتعزيز ثقة العملاء بالشركات، ومواجهة تهديدات مختلفة، تُصنف إلى: أمن التطبيقات، وأمن الشبكات، وأمن السحابة، وأمن إنترنت الأشياء، ويُعد الأمن السيبراني ضروريًا ليس فقط لتأمين البيانات، بل أيضًا للحماية من سرقة ومحو أنواع مختلفة من البيانات، بما في ذلك المعلومات الحساسة، والمعلومات الشخصية القابلة للتعريف [PII]، والمعلومات الصحية المحمية [PHI]، والبيانات الشخصية، وانتهاكات الملكية الفكرية (Al-Fatlawi, 2024)

ولا تزال هناك فجوة بين مستخدمي الإنترنت والأمن السيبراني، والسبب الرئيسي هو قلة وعي المستخدم بالوعي السيبراني، مما يؤدي إلى استغلال المهاجم لنقاط ضعفه، وهناك حاجة لبرامج توعية نظرًا لأهميتها في رفع ثقافة المستخدمين الأذكياء، ويتمثل الوعي الأمني في التعلم المستمر والإدراك لأهمية قضايا أمن المعلومات والمستوى المطلوب لتحقيق وعي أمني جيد ومعرفة بواجبات الأفراد الأمنية، وتتجلى أهمية الوعي السيبراني في أنه يمكن للمستخدمين غير الواعيين إحداث أضرار جسيمة لبياناتهم وكذلك للنظام، لذلك، يجب نشر الوعي بالمخاطر المرتبطة بتقنيات الإنترنت بين الناس للحد من فرص وقوع الهجمات (Alberici & Sadaf, 2023)

ويؤثر وعي موظفين الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ بأمن المعلومات بشكل كبير على سلوكيات الأمن السيبراني في المؤسسات التي تتمتع ببيانات حسّاسة، كما تؤثر على امتثال الموظفين لسياسات الأمن، وجدير بالذكر أن نقص وعي الموظفين بأمن المعلومات يعد السبب الرئيسي لسوء التعامل مع المعلومات الحساسة، علاوة على ذلك، أصبح وعي الموظفين بأمن المعلومات أولوية قصوى

على كافة المستويات، ويرجع ذلك أساسًا إلى أنه تُعدّ الأخطاء البشرية هي السبب المباشر أو غير المباشر لغالبية حوادث الأمن، بما في ذلك سوء السلوك المتعمد وغير المتعمد، وقد ثبُت أن ما يقرب من 77 % من خروقات بيانات الشركات تنتج عن استغلال نقاط الضعف البشرية، كما وُجد سابقًا أن أكثر من نصف خروقات أمن المعلومات تحدث بسبب ضعف امتثال الموظفين لمعايير أمن المعلومات (Khando et al., 2021).

وتتمثل التهديدات والهجمات السيبرانية في مجموعة واسعة من الأنشطة غير القانونية على الإنترنت في السرقة الإلكترونية، والتخريب الإلكتروني، واختراق الويب، وسرقة معلومات البطاقات، والإرهاب الإلكتروني، والمواد الإباحية للأطفال، والتصيد الاحتيالي، وبرامج الفدية، ونشر شبكات الروبوتات (Safiyanu et al., 2024).

كما أن التهديدات والهجمات الإلكترونية تُشكل خطرًا متزايدًا على الأصول الرقمية والممتلكات الإلكترونية للمؤسسات والأفراد على حد سواء، ومع تزايد الاعتماد على التكنولوجيا الرقمية، تُصبح البيانات الشخصية والمالية عُرضةً للهجمات التي تهدف إلى سرقتها أو التلاعب بها، مما يُعرّض الأصول الرقمية لخسائر فادحة وتأثيرات طويلة الأمد، وقد أدركت الحكومات والهيئات التنظيمية هذه التحديات، ووضعت أطرًا قانونية صارمة، مثل اللائحة العامة لحماية البيانات (GDPR) للاتحاد الأوروبي، والتي تهدف إلى حماية الخصوصية الرقمية ومنح الأفراد سيطرة أكبر على معلوماتهم الشخصية (Bhu-shan, 2023).

وتعد الهجمات الإلكترونية أفعال ينفذها تقني خبير، حيث يتم الوصول إلى المعلومات وسرقتها بشكل غير قانوني، علاوة على ذلك، يؤدي الهجوم الإلكتروني إلى تدمير ملفات البيانات وإفسادها، مما يؤثر على الوضع المالي لكل من الفرد والمؤسسة، وتتأثر العديد من الدول بمعضلة الجرائم الإلكترونية أو الهجمات الإلكترونية، ومع النمو السريع للقطاع المالي في دولة الإمارات العربية المتحدة، أصبحت عرضة لخطر الهجمات

الإلكترونية، حيث ترتبط الهجمات الإلكترونية بالأنشطة غير القانونية التي تتمثل في الرغبة في تحقيق الربح من خلال الوصول إلى البيانات الخاصة والحساسة لتهديد الأفراد أو المؤسسات أو لتحقيق الربح من خلال بيع المعلومات المسروقة في السوق السوداء، علاوة على ذلك، أصبحت دولة الإمارات العربية المتحدة هدفًا رئيسيًا للجرائم الإلكترونية نتيجةً لازدهار اقتصادها وسياحتها(Al-Kumaim & Alshamsi, 2023)

لذا ينبغي على الدول والحكومات والهيئات التي لديها تعاملات رقمية أن تولي اهتمام كبير بتوعية وتدريب وتأهيل المستخدِم. ومن هذا المنطلق يأتي هذا البحث ليسلط الضوء على تعزيز الوعي الأمني لدى موظفي الهيئة عن تلك الهجمات، والتهديدات السيبرانية، ولتقليل من حدة المخاطر الأمنية، وتقليل الضرر الناتج عنه وللحفاظ على المكتسبات والأصول

- **أهمية البحث:**

أصبحت التهديدات السيبرانية مصدر قلق كبير في جميع أنحاء العالم، ودولة الإمارات العربية المتحدة ليست استثناءً من تلك التهديدات. لذا تُعد هذه الدراسة ضرورية لحماية المصالح الوطنية لدولة الإمارات العربية المتحدة، حيث تلعب الجهات الحكومية دورًا حيويًا في حماية البنية التحتية الحيوية والمعلومات الحساسة؛ فتعزيز الوعي الأمني لدى موظفي الهيئة لن يؤدي فقط إلى حماية الأصول والممتلكات الرقمية فحسب، بل سيعزز أيضًا الوضع العام للأمن السيبراني داخل الدولة وخارجها. وهو يوضح التزام الهيئة بحماية المصالح العامة، والحفاظ على السلامة التشغيلية في المشهد الرقمي المتطور، وامتثالها للمعايير الوطنية والمؤشرات الدولية المعمول بها في الدولة وخارجها

وبما أن الهيئة الإتحادية للهوية والجمارك وأمن المنافذ تحتوي على أكبر قاعدة بيانات للمعلومات الشخصية لكافة مواطني، ومقيمي، وزوار دولة الإمارات العربية المتحدة، فإن هذا يجعلها أكثر عرضة للاستهداف، مما يتطلب منها تعزيز إجراءات الأمن السيبراني بشكل عالي جدا

- **نطاق البحث:**

- **النطاق الجغرافي:** دولة الإمارات العربية المتحدة.

- **النطاق المكاني:** الهيئة الإتحادية للهوية والجنسية والجمارك وأمن المنافذ.

- **إشكالية البحث:**

تتزايد الجرائم الإلكترونية والاختراقات السيبرانية والتهديدات تجاه المؤسسات والهيئات الإتحادية لحكومة الإمارات، بما في ذلك الأساليب الحديثة الذي يستخدمها المخترقون تجاه الموظفين للحصول على المعلومات بطريقة غير مشروعة، وبهدف الاستيلاء على الأموال، وغيرها من المخاطر الأمنية والتهديدات السيبرانية؛ حيث أن المستخدِم هو حلقة ضعيفة في سلسلة أمن المعلومات، والذي يتم محاولة استغلاله من أجل اختراق أنظمة المعلومات

وتعد الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ بما تحتويه من معلومات حسّاسة، معارك المعلومات والأمن السيبراني على جبهتين؛ إذ يتعين عليها التعامل مع كل من التهديدات الخارجية والداخلية، وقد عززت هذه المؤسسات جهودها في استخدام برامج التوعية والتدريب الأمني لتزويد موظفيها بالقدرة على التخفيف من تهديدات الأمن السيبراني، وتنجم معظم الخروقات عن عدم امتثال الموظفين لسياسات الأمن الخاصة بالمؤسسة، وفي حين يتزايد الوعي بالأمن السيبراني بين كبار المديرين التنفيذيين، تبرز حاجة المؤسسات لإعادة النظر في استراتيجياتها للتوعية بالأمن السيبراني، مع تزايد تعقيد التهديدات السيبرانية، كما تتزايد حاجة المؤسسات لفهم أسباب تجاهل الموظفين لسياسات الأمن المؤسسية، لا سيما مع وجود برنامج توعية أمنية داخل تلك المؤسسات (Agbo-ola, 2022)

كما تشير التهديدات السيبرانية إلى هجمات متعمدة تتضمن الوصول غير المصرح به إلى شبكة أو بيانات حساسة، وغالبًا ما تؤدي إلى تدمير أو إتلاف أو سرقة أصول تكنولوجيا المعلومات، وتُنفذ هذه الهجمات، بواسطة أفراد أو مؤسسات، من خلال

استغلال نقاط الضعف في أنظمة الحاسوب والشبكات، وهي تغطي مجموعة واسعة من الجرائم، من البرمجيات الخبيثة إلى رفض الخدمة، وصولًا إلى السرقة والاحتيال، ومع تزايد اعتماد الحياة اليومية على التكنولوجيا، أصبحت الجرائم الإلكترونية مشكلة خطيرة للأفراد والمؤسسات، حيث تُشكل خطرًا جسيمًا على أمن البيانات والخصوصية، ويواصل التقدم التكنولوجي دفع الجرائم الإلكترونية إلى الأمام، مما يؤدي إلى هجمات جديدة ويجعل الوقاية منها أكثر صعوبة (Kulkarni et al., 2024).

وتؤثر الهجمات السيبرانية على الممتلكات الرقمية من خلال عمليات مثل سرقة الهوية والتي تحدث عندما يسرق شخص ما هوية الفرد للوصول إلى موارد مثل بطاقات الائتمان والحسابات المصرفية وغيرها من المزايا، وقد يستخدم المحتال الهوية أيضًا لارتكاب جرائم أخرى، ويعد الاحتيال على بطاقات الائتمان هو مصطلح واسع النطاق للجرائم التي تنطوي على سرقة الهوية حيث يستخدم المجرم بطاقة الائتمان الخاصة بالضحية لتمويل معاملاته، مما يعمل على تحويل ممتلكات الضحية لتصبح تحت سيطرة المنتحل (Goni, 2022).

وأخيرًا تُعدّ دولة الإمارات العربية المتحدة من الدول التي تشهد تصاعدًا في الهجمات السيبرانية، لا سيما في مجالي التصيد الاحتيالي وسرقة الهوية، مستفيدة من النمو السريع للقاعدة الرقمية في مختلف القطاعات، ويُعد قطاع الخدمات المالية من بين الأكثر عرضة لهذه الهجمات، حيث أبلغ أكثر من نصف المؤسسات (56 %) كما أبلغت العديد من المؤسسات المالية بنسبة بلغت (36 %) عن تعرّضها لهجمات تصيّد احتيالي، وقد ساهمت جائحة كوفيد-19 في تسريع الرقمنة، ما وفّر بيئة خصبة لتوسّع الجرائم الإلكترونية، ووفقًا لإحصاءات شرطة الإمارات العربية المتحدة، تم تسجيل 9046 شكوى إلكترونية عام 2019، من بينها 1277 شكوى تتعلق باختراقات بريد إلكتروني، ولا يزال ضعف الوعي بالأمن السيبراني يُمثل أحد التحديات الأساسية في قطاع الخدمات المصرفية، حيث تُسجل المؤسسات خسائر مالية نتيجة سرقة الهوية والمعلومات الحساسة (Alshamsi & AlKumaim, 2021)

وفي هذا السياق توجد حاجة ملحة لتطوير برامج وأساليب التوعية السيبرانية للموظفين بهدف تقليل المخاطر الأمنية التي تواجه الهيئة الإتحادية للهوية والجمارك وأمن المنافذ؛ وبما ينسجم مع الجهود التي تبذلها الدولة، والتي جعلت منها رائدة في مجال الأمن السيبراني إقليميا ودوليا

- **أسئلة البحث**

وينبثق عن تلك الإشكالية عدة تساؤلات فرعية تشكل في مجملها محور الدراسة وجوهرها وهي كالآتي:

- **السؤال الأول:** ما هي التهديدات السيبرانية التي تواجه المستخدِم في الهيئة الإتحادية للهوية والجمارك وأمن المنافذ؟
- **السؤال الثاني:** ما هو المستوى الحالي للوعي بالأمن السيبراني لدى موظفي الهيئة فيما يتعلق بالتهديدات السيبرانية وتأثيرها المحتمل على الأصول والممتلكات؟
- **السؤال الثالث:** كيف يمكن تطوير برامج التوعية السيبرانية للموظفين لمواجهة التحديات السيبرانية الحالية والمستقبلية؟

- **أهداف البحث**

يسعى هذا البحث أن يحقق الأهداف الأساسية التالية:

- **الهدف الأول:** تحديد التهديدات السيبرانية التي تواجه المستخدِم في الهيئة الإتحادية للهوية والجمارك وأمن المنافذ.
- **الهدف الثاني:** تقييم المستوى الحالي للوعي الأمني لدى موظفي الهيئة فيما يتعلق بالتهديدات السيبرانية وتأثيرها المحتمل على الأصول والممتلكات.
- **الهدف الثالث: وضع مقترحات لتطوير برامج التوعية السيبرانية للموظفين** لمواجهة التحديات السيبرانية الحالية والمستقبلية.

- **منهج البحث**

سوف تستخدم هذه الدراسة منهجا كميا، حيث سيتم:

- **أولا:** جمع البيانات عبر إجراء استطلاع أراء موظفي الهيئة لتقييم مستويات الوعي الأمني الحالية لديهم، وجمع الأفكار حول تجاربهم مع التهديدات السيبرانية.
- **ثانيا:** دراسة التقارير السابقة حول التهديدات السيبرانية السائدة التي تؤثر على الأصول والممتلكات داخل دولة الإمارات العربية المتحدة.

- **هيكل البحث**

- **الفصل الأول:** الإطار التنظيمي
- **الفصل الثاني:** (الدراسات السابقة)
- **الفصل الثالث:** (المنهجية وطرق البحث)
- **الفصل الرابع:** نتائج الدراسة

الفصل الثاني

الدراسات السابقة

- **مفهوم الأمن السيبراني:**

عـرَّف ياسـمين والحسـين (2021) الأمـن السـيبراني بأنـه: «إجـراءات وتدابيـر يتـم اتخاذهـا لحمايـة الشـبكات والأجهـزة والبرمجيـات والبيانـات مـن التهديـدات المحتملـة مثـل الهجمـات والسـرقة والاختـراق والتلـف». ويَعتبـر نفـس المصـدر بـأن الأمـن السـيبراني هـو مجموعـة مـن الوسـائل التقنيـة والتنظيميـة والإداريـة تهـدف إلـى منـع سـوء اسـتغلال النظـام. ويتـم تعريـف هـذه الجوانـب وتوجيهها بشـكل تنظيمـي لضمـان فعاليـة وشـمولية الحمايـة الرقميـة.

وعـرَّف المنتشـري وحريـري (2020) الأمـن السـيبراني بأنـه: «مجموعـة الإجـراءات التـي تهـدف إلـى حمايـة شـبكات المعلومـات مـن جميـع الأعمـال والتدابيـر التـي تسـتهدف العبـث بالمعلومـات وتسـبب الضـرر للمسـتخدمين. يهـدف هـذا النهـج أيضًـا إلـى الحمايـة ضـد الاختـراق، وانتشـار البرمجيـات الخبيثـة والفيروسـات

وعرفـت ابـن ابراهيـم (2021) الأمـن السـيبراني بأنـه: «التدابيـر الأمنيـة المتعلقـة بالإجـراءات المتخـذة لحمايـة جهـاز الكمبيوتـر أو الشـبكة مـن وصـول غيـر مُصَـرَّح لـه، بهـدف الحفـاظ علـى سلامـة المعلومـات وتأمينهـا». ويشـمل مجـال الأمـن السـيبراني التـدخلات التقنيـة التـي تهـدف إلـى حمايـة البيانـات، ومعلومـات الهويـة، والأجهـزة مـن وصـول غيـر مصـرح بـه، أو أي ضـرر محتمـل، ويتضمـن ذلـك تأميـن الفضـاء الإلكترونـي

ويمكننـا ممـا سـبق اسـتنتاج أن مفهـوم الأمـن السـيبراني يشـمل كل مجـالات حمايـة الأنظمـة مـن الاختراقـات والهجمـات الإلكترونيـة والتهديـدات والجرائـم السـيبرانية التـي قـد تؤثـر علـى سـرية وسلامـة المعلومـات، وحـق الولـوج إليهـا، سـواء الأفـراد أو المؤسسـات.

إضافـة إلـى ذلـك يُعتبـر الأمـن السـيبراني جزءًا لا يتجـزأ مـن الاسـتراتيجيات الأمنيـة الضروريـة للحكومـات والمؤسسـات حيـث يُنظـر إليـه كأحـد الأذرع الحديثـة للأمـن التـي ينبغـي توفيرهـا. وأحـد الركائـز الأساسـية فـي الاقتصـاد القائـم علـى التكنولوجيـا الذكيـة لتحقيـق التنميـة المسـتدامة

- **أهمية الأمن السيبراني:**

بيَّن محمد (2021) أن أهمية الأمن السيبراني تتمثل في الحماية الشاملة لكل العناصر، سواء الفعلية أو الافتراضية، في البنية التحتية للقطاعات الحيوية داخل الدولة. ويشمل هذا الأمن حماية الأفراد، وتقليل مخاطر الهجمات من الداخل

- **حماية البنية التحتية:** توجيه حماية البنية التحتية يرتبط بضمان أمن العناصر الحيوية التي تشكل أساساً للاقتصاد الوطني. يتضمن ذلك جهود حماية شبكات الاتصالات وتكنولوجيا المعلومات والخدمات المالية، بالإضافة إلى القطاعات الحيوية الأخرى مثل الكهرباء، وصناعة النفط، والغاز، ووسائل النقل والمواصلات ويهدف هذا التوجيه إلى تعزيز مستوى الأمن والاستقرار في البنية التحتية الوطنية، مما يحميها من التهديدات السيبرانية، ويضمن استمرارية الخدمات الحيوية.

- **الخدمات العامة:** حماية الخدمات العامة تركز على ضمان استمرارية وأمن الخدمات الأساسية التي تقدمها الدولة للمواطنين. يتضمن ذلك حماية الخدمات الطبية والصحية ونظم الإسعاف والتعليم. بالإضافة إلى الحفاظ على أمن وسلامة الثقافة ووسائل الإعلام والمواقع الرسمية للدولة. حيث يهدف هذا التوجيه إلى تقديم الخدمات العامة بشكل مستمر وآمن، مما يضمن حماية حقوق واحتياجات المواطنين ويسهم في استقرار المجتمع وتطوره.

- **الأمن المالي:** تعتبر حماية الأمن المالي أمرًا حيويًا، حيث يتم التركيز على حماية القطاع المالي والبنوك ويهدف ذلك إلى ضمان سلامة التعاملات المصرفية عبر الشبكة وتأمين القطاع المالي بشكل عام. مما يسهم في الحفاظ على الاستقرار الاقتصادي للدولة ويحمي النظام المالي من التهديدات السيبرانية المحتملة.

- **النظم الحكومية:** تعتبر حماية النظم الحكومية جزءًا حيويًا من الأمن السيبراني، حيث يركز هذا الجانب على حماية الأنظمة والمؤسسات الحكومية المختلفة. ويتضمن ذلك حماية الجوانب الإدارية والتشريعية للحكومة، بالإضافة إلى ضمان سلامة البيانات والمعلومات الحكومية. ويساهم في الحفاظ على سرية البيانات،

وضمان استقرار وكفاءة الأنظمة الحكومية.

- **القطاعات الحيوية:** تعد حماية القطاعات الحيوية جزءًا أساسيًا من أهمية الأمن السيبراني، حيث يتعلق الأمر بتأمين القطاعات التي تلعب دورًا حيويًا في استدامة الحياة اليومية. ويشمل ذلك حماية قطاعات مثل: الطاقة، والنقل، والمواصلات، والصحة. هذا يهدف إلى ضمان استمرارية وفعالية هذه القطاعات ومقاومتها للتهديدات السيبرانية، ويعزز استقرار وسلامة الحياة اليومية للمجتمع.

أما المنتشري وحريري (2020) فقد بينوا أن أهمية الأمن السيبراني تتمثل في حماية المعلومات الحساسة، مثل بيانات الموظفين والعملاء والمالية والحفاظ على سرية المعلومات من الوصول غير المصرح به، ومنع تعطل الأعمال، مما يؤدي إلى خسائر مالية وانخفاض الإنتاجية، وحماية سمعة المؤسسة، حيث أن الهجمات السيبرانية تؤدي إلى فقدان ثقة العملاء، وانخفاض الأرباح، وحتى الإفلاس.

وفي هذا السياق، يرى المنتشري وحريري (2020) أن أهداف الأمن السيبراني هي:

- التصدي للبرامج التي تحتوي على فيروسات، أو تهديدات للأجهزة.
- تعزيز الوعي بأمن البيانات، والتصدي للهجمات الإلكترونية.
- تطوير وتعزيز مهارات وسلوكيات المستخدمين لتحسين الأمان السيبراني.
- مكافحة الجرائم الإلكترونية، وتقديم التدريب لتحسين استعداد المؤسسة لمواجهة التحديات.
- حماية الأنظمة والشبكات من التهديدات السيبرانية المتقدمة.
- تعزيز التعاون والتنسيق بين الأقسام المختلفة لتعزيز الأمان الشامل

- **مجالات الأمن السيبراني:**

في عالم تتزايد فيه التهديدات الرقمية يومًا بعد يوم يبرز الأمن السيبراني كحصن دفاعي أساسي لحماية معلوماتنا وخصوصيتنا. حيث يقسم السواط وآخرون (2020) الأمن السيبراني إلى مجالين رئيسيين:

- **أولا:** حماية الأجهزة الشخصية المحمولة، ووسائط التخزين، وجميع أنواع الأجهزة والتكنولوجيا، من خطر الهجمات الإلكترونية والاختراقات، والتدمير الجزئي أو الكلي.
- **ثانيا:** التفاعل مع خدمات تصفح الإنترنت من خلال زيادة وعي الأفراد بخطورة الهجمات والجرائم الإلكترونية، بما في ذلك وسائل الاحتيال والاعتداء، وتدمير البيانات الشخصية، أو سرقتها.

على الرغم من أن السواط وآخرون (2020) قاموا بتقسيم مجالات الأمن السيبراني لقسمين فقط إلا أنهم جمعوا في القسم الأول الأجهزة المختلفة، وهذا ما جعل التقسيم يقتصر على قسمين، إلا أنه من وجهة نظري، أرى أنه كان من الأجدر بهم أن يقوموا بتقسيم فرعي واضح لمجالات الأمن السيبراني

ونستخلص مما سبق أن هنالك حاجه ملحة لبذل جهد مكثف لزيادة وعي الناس بالتهديدات السيبرانية، وإنشاء خطط عملية لحماية أنفسهم والمجتمع من عدة جوانب، بدءًا من تشجيع السلوكيات الآمنة على الإنترنت، إلى حماية الأجهزة الإلكترونية، من أجل خلق بيئة رقمية آمنة تحمي المستخدمين، وتحافظ على بياناتهم وخصوصيتهم في الفضاء السيبراني، ويلزم ذلك وجود استراتيجية شاملة تدمج الأمن الإلكتروني للأجهزة مع الوعي بالتهديدات السيبرانية

- **آثار ضعف الأمن السيبراني:**

وفقا للشريف وآخرون (2023) يعتبر ضعف الأمن السيبراني أمرًا خطيرًا يضر بالأفراد والمؤسسات على نطاق واسع. وتعد الآثار الرئيسية لهذا الواقع المُقلق تتمثل في النقاط التالية

- **اختراق وتخريب البنية التحتية للاتصالات وتكنولوجيا المعلومات:** تتسم الهجمات السيبرانية بالتنوع والتطور السريع، حيث يستهدف المهاجمون البنية التحتية للاتصالات، وأنظمة تكنولوجيا المعلومات. ويشمل ذلك نشر البرامج الضارة والفيروسات بهدف تعطيل الأنظمة، وتكنولوجيا التحكم، ويؤثر ذلك بشكل كبير

على المؤسسات وخدماتها، خاصة في المرافق الحيوية والخدمات الحكومية.

- **الإرهاب والحروب السيبرانية:** تمتلك الجرائم السيبرانية أبعادًا دولية، حيث تعتمد على تقنيات متقدمة للتجسس والاختراق. وتُستخدم هذه الهجمات في أغراض جنائية مثل التخريب والإرهاب. وتسعى أيضًا لتحقيق أهداف دولية من خلال الحروب السيبرانية، ويكمن التأثير الكبير في تعطيل البنية التحتية، وزعزعة الاستقرار الاقتصادي والسياسي.
- **سرقة الهوية الرقمية والبيانات الخاصة:** تشكل جرائم سرقة الهوية الرقمية والبيانات الشخصية خطرًا كبيرًا؛ فيمكن للمهاجمين الوصول إلى معلومات حساسة وسرقتها، أو استخدامها لأغراض احتيالية. ويكون المستخدمون على شبكة الإنترنت والمؤسسات المستهدفة عرضة للتلاعب والسرقة مما يهدد الأمن الشخصي والاقتصادي.

ووفقا للدليل الإرشادي لجوانب الأمن السيبراني في العمل عن بُعد (2021) الذي أصدره المركز الوطني الإرشادي للأمن السيبراني في السعودية، فإنه يمكن تقديم المخاطر الأمنية للعمل عن بُعد، والتحديات الأمنية للقطاعين الخاص والعام، والتي تهدد السلامة والخصوصية للمشاركين، على النحو الآتي

- **إزعاج:** يشمل هذا الجانب إرباك الاجتماعات وتشويشها، مما يؤدي إلى إضاعة وقت المشاركين وانحراف انتباههم. وكما يتسم بحوادث واقعية تشمل اقتحامات غير مصرح بها لغرف الاجتماعات مع عرض مواد غير لائقة.
- **السرية:** يشمل تسريب المعلومات الحساسة من خلال التنصت على الاجتماعات، وكشف أسرار العمل. ويتضمن حالات واقعية، ككشف تسجيلات اجتماعات حساسة لأفراد غير مخولين بالوصول إليها.
- **الخصوصية:** يرتبط بالتعامل غير القانوني مع معلومات الموظفين الشخصية ومتابعة اهتماماتهم. ويتضمن حالات واقعية، مثل: استغلال الشركات للبيانات

الشخصية لأغراض تجارية دون إذن.

- **الاختراق:** ينطوي على استغلال ثغرات في أجهزة الموظفين، نتيجة لاعتماد قنوات إلكترونية جديدة. ويتضمن حالات واقعية، كالتلاعب بروابط الاجتماعات الافتراضية، واستخدامها للحصول على صلاحيات إلكترونية لحسابات المشاركين.

وتشير هذه المخاطر إلى أهمية رفع مستوى الوعي والحذر كموظف، وكيف يمكن للتقنيات المستخدمة في العمل عن بُعد أن تكون آمنة، وذلك من خلال تبني استراتيجيات ذكية، وتوجيه اهتمام كبير لحماية معلومات المؤسسة، وخصوصية الموظفين

- **مفهوم التهديدات والجرائم السيبرانية:**

تُشير كلمة «التهديدات والجرائم السيبرانية الإلكترونية» إلى الهجمات التي تتم باستخدام التقنيات الحديثة، والتي تستهدف المعلومات والبيانات. وتُعَرف آمال (2022) الجرائم السيبرانية بأنها: «التهديدات التي تأتي من مصادر إلكترونية أو عبر الإنترنت إلى الأفراد والجماعات والدول التي تستخدم وسائل الإنترنت كوسيلة لتحقيق أهدافها». بينما يُعَرف ياسمين والحسين (2021) أنها: «استغلال الحسابات وتكنولوجيا المعلومات في تخريب البنية المعلوماتية للخصوم بما في ذلك تعطيل شبكات الدفاع السيبراني، واختراق أنظمة المعلومات الحساسة لرؤساء الدول، والتجسس عليهم، وذلك وفقًا لخطة منهجية مدروسة»

أما البحيري (2023) فتعرف التهديدات والجرائم السيبرانية على أنها: «تشمل جميع أشكال الاختراقات، أو الاستخدامات غير المشروعة، والتعديلات، أو التعطيلات، التي تستهدف الشبكات، وأنظمة تقنية المعلومات والاتصالات، بما في ذلك الأنظمة التشغيلية ومكوناتها من الأجهزة والبرمجيات والخدمات».

كما عرَّف بكراوي وبو بكر (2023) التهديدات السيبرانية بأنها: «الجرائم والهجمات الإلكترونية التي تحدث في الفضاء السيبراني، والتي تستهدف اختراق البنية المعلوماتية للأفراد، أو المؤسسات بهدف الاستيلاء على المعلومات أو تدميرها»

وبناء على كل التعريفات السابقة يمكننا استخلاص أن التهديدات السيبرانية هي كل التحديات والمخاطر التي تواجه الأنظمة الإلكترونية، والمعلومات عبر الإنترنت.

- **أنماط التهديدات السيبرانية:**

لقد وضح بكراوي وبو بكر (2023) عدة أنماط للتهديدات السيبرانية تتمثل في:

- **خطر الكوارث الطبيعية أو العرضية للكابلات البحرية:** تُعد الكوابل البحرية عنصرًا حيويًا لتوفير خدمات الاتصال بين دول العالم في شبكات الإنترنت والحوسبة وغيرها. ومع التقدم التكنولوجي أصبحت هذه الكوابل أكثر انتشارًا وتأثيرًا.
- **الجريمة السيبرانية (الجريمة الإلكترونية):** تشير إلى: «أي فعل يتنافى مع القانون، ويتسبب في إلحاق ضرر بالأفراد، أو انتهاك حقوقهم الشخصية، ويتم تنفيذه عبر شبكات الاتصال والمعلومات مثل: الإنترنت والبريد الإلكتروني: والهواتف الذكية».
- **الحروب السيبرانية:** تعتمد على فرق من الخبراء في المعارك الإلكترونية، حيث يختص كل فريق بالتخطيط والتنفيذ، والدفاع عن العمليات السيبرانية، وتشمل العمليات الهجومية والدفاعية.

ووفقا للشريف وآخرون (2023) فقد بينوا أن المخاطر الناتجة عن ضعف الأمن السيبراني تشمل أنواعًا متنوعة، وتقسم إلى فئات داخلية وخارجية

- **المخاطر الداخلية:**

◊ **أخطاء الأفراد (الأخطاء البشرية):** وتمثل هذه المخاطر التحديات الأكثر حدة، حيث يمكن أن تكون ناتجة عن أفعال مقصودة، أو غير مقصودة، من قبل الأفراد، والتي يتعين على الجهة الأمنية وضع سياسات وقوانين لتقليل هذه المخاطر الناجمة عنها.

◊ **ضعف التحكم في الوصول:** يشير إلى عدم وجود تحكم فعال في الوصول إلى المعلومات والأنظمة، مما يسمح للأشخاص غير المصرح لهم بالوصول إلى المعلومات.

◊ **البرامج الضارة:** تشمل الفيروسات والديدان والتروجانات، وتستهدف إلحاق الضرر

بالمعلومات أو الأنظمة الإلكترونية.

◊ **هجمات التصيد الاحتيالي:** تستهدف خداع المستخدمين للحصول على معلومات شخصية أو مصرفية.

◊ **هجمات الهندسة الاجتماعية:** تهدف إلى خداع المستخدمين للحصول على معلومات حساسة، أو تنفيذ إجراءات غير مرغوب فيها.

- **المخاطر الخارجية:**

◊ هجمات القرصنة: تستهدف القراصنة اختراق المعلومات، أو الأنظمة الإلكترونية من خارج النظام

◊ هجمات رفض الخدمة.

◊ تهدف إلى تعطيل الوصول إلى المعلومات، أو الأنظمة الإلكترونية

◊ هجمات انتزاع الفدية: تشمل تشفير المعلومات، أو الأنظمة مع المطالبة بفدية لفك التشفير.

- **أنواع التهديدات السيبرانية:**

يمكن حصر أنواع التهديدات السيبرانية التي ذكرها العنزي (2022) بالآتي:

- **الاحتيالي الإلكتروني:** هو نشاط غير قانوني يستند إلى استخدام وسائل الإعلام الإلكترونية وتكنولوجيا المعلومات بهدف الحصول على معلومات سرية، أو القيام بعمليات نصب واحتيال عبر الإنترنت. ويتضمن الاحتيال الإلكتروني مجموعة واسعة من الأنشطة الاحتيالية مثل: الغش، والخداع، والتي تهدف إلى خداع الأفراد أو الكيانات بهدف الحصول على مكاسب غير قانونية. ويمكن أن يشمل الاحتيال الإلكتروني أشكالًا متعددة، مثل الاحتيال البريدي الإلكتروني (Phishing)، والتصيُّد الإلكتروني (Spoofing). وبحسب تقرير حول خروقات البيانات لشركة Verizon الذي وثقه(Daengsi 2022)وآخرون في دراستهم فقد ذكر أن 30 % من رسائل البريد الإلكتروني التصيدية تمت قراءتها من قبل الضحايا والاحتيال النصي (Vish-

ing)، وغيرها من التقنيات الخبيثة التي تستهدف الأفراد والمؤسسات عبر الشبكة العنكبوتية واستنادًا إلى الانتهاكات التي تشمل الصناعات أعلنت شركة Verizon أن حوالي 10٪ من الانتهاكات كانت في الصناعة المالية مما تسبب في خسارة مالية كبيرة، ليس فقط للشركات المالية، ولكن أيضًا لعملائها وموظفيها. ويُعد مكافحة الاحتيال الإلكتروني تحديًا مستمرًا للسلطات والمؤسسات، وتتطلب تكاملًا بين الحماية التكنولوجية والتوعية لتعزيز الأمن الرقمي.

- **التنمر الإلكتروني:** المعروف أيضًا بالتنمر عبر الإنترنت أو التنمر الرقمي، وهو نوع من أنواع التنمر يحدث عبر وسائل الاتصال الإلكتروني مثل الرسائل الإلكترونية، ووسائل التواصل الاجتماعي، ومنتديات الإنترنت. ويشمل التنمر الإلكتروني أنشطة متعددة، مثل: الاستهزاء، ونشر المعلومات الكاذبة أو المسيئة، والتهديد، والتشهير، وسرقة الهوية الرقمية، والتسلل إلى حسابات الأفراد، وإرسال الرسائل التحريضية، أو العنيفة، ويتميز التنمر الإلكتروني بتوسع نطاقه، وسرعته في التواصل، حيث يمكن للرسائل والمحتوى الضار أن ينتشر بسرعة كبيرة عبر الإنترنت، مما يؤدي إلى تأثيرات سلبية على الضحايا، ويمكن أن يستهدف التنمر الإلكتروني الأفراد أو الجماعات، وكما يمكن أن يكون موجهًا نحو الأطفال والمراهقين والكبار على حد سواء. وقد عرَّف العمري وآخرون (2023) التنمر الإلكتروني بأنه: «قيام الجناة باستغلال التكنولوجيا ووسائل الاتصالات للقيام بأفعال إجرامية موجهة نحو الأفراد الصغار، والشباب، عبر وسائل وقنوات متعددة، مثل: تهديدات ورسائل عدائية، ونشر صور مسيئة، والكشف عن معلومات شخصية، أو حساسة، أو التحرش، أو إلحاق الإحراج، أو التسلية على حساب الآخرين. ويتم ذلك عبر منصات متنوعة على الإنترنت، مثل: فيسبوك، ومنتديات النقاش، والمدونات، والبريد الإلكتروني، ورسائل الدردشة الفورية، ووسائل التواصل المحمولة. ويمكن لهذه الأفعال أن تؤدي إلى شعور الأفراد بالإحباط، وفقدان الثقة بالنفس، واضطرابات في حس الترابط الاجتماعي.
- **الهجمات المستهدفة:** تشير إلى أنواع من الهجمات السيبرانية التي تستهدف

هدفًا معينًا، سواء كان هذا الهدف فردًا، أو منظمة، أو نظامًا محددًا. وتختلف هذه الهجمات عن هجمات الإنترنت العشوائية التي لا تستهدف هدفًا محددًا، حيث تكون موجهة بشكل مباشر نحو هدف محدد بغرض تحقيق أهداف معينة. وقد وضح (Abdullah.Mohamed 2019) أن الهجمات السيبرانية كانت عادة عشوائية دون هدف محدد. ومع ذلك فقد تحولت الهجمات السيبرانية الحالية إلى هجمات موجهة نحو أهداف محددة.

- **تسريب البيانات:** يشير إلى حدوث تسريب أو تسرب للمعلومات السرية، أو البيانات الحساسة من مصدرها المعتمد إلى أطراف غير مخولة، أو غير مصرح لها بالوصول إليها. يمكن أن يحدث هذا التسريب بسبب الهجمات السيبرانية، الاختراقات، أو الأخطاء البشرية، أو أي نقص في التدابير الأمنية.
- **الهندسة الاجتماعية:** تشير إلى استخدام التلاعب بالعواطف، والأمور الاجتماعية، للحصول على معلومات سرية، أو تنفيذ أنشطة غير قانونية. ويعتمد هذا النوع من الهجمات على إقناع الأفراد بالكشف عن معلومات حساسة أو تحميل برامج خبيثة، أو القيام بأفعال تفضي إلى تسريب البيانات.
- **الابتزاز الإلكتروني:** هو نوع من أنواع الهجمات الإلكترونية التي تستخدم التهديدات والضغوط للحصول على مكاسب غير قانونية، أو تهديد الأفراد، أو المؤسسات بكشف معلومات حساسة يشمل الابتزاز الإلكتروني عدة أساليب.
- **التغرير والاستدراج:** هو تقنية احتيالية تستخدم لخداع الأفراد، وإقناعهم بالكشف عن معلومات حساسة، مثل: كلمات المرور، والمعلومات المصرفية عبر التظاهر بأنها جهة موثوقة.
- **التجسس الإلكتروني:** يشير إلى استخدام التكنولوجيا الرقمية للتجسس على الأنظمة الإلكترونية والحصول على معلومات سرية أو حساسة.
- **الإرجاف الإلكتروني:** يقوم المجرم من خلالها ببث معلومات مغلوطة بهدف نشر الذعر.

أما بكراوي وبو بكر (2023) فقد قسم التهديدات السيبرانية إلى ستة أنواع:

- **التنصت:** يتمثل في التجسس على حوارات بين أفراد أو مستخدمين عبر الشبكة، باستخدام تقنيات مخصصة لذلك.
- **الانتحال:** يعني تنكير الشخص على أنه كيان صالح من خلال تزوير المعلومات للوصول إلى بيانات غير مسموح للشخص بالوصول إليها.
- **التلاعب:** إجراء تعديلات مضرة في المنتجات، مما قد يتسبب في تلف البيانات
- **تجاوز الصلاحيات:** يتعلق بمحاولة شخص ذو صلاحيات محددة للوصول إلى نظام بطرق غير مصرح بها.
- **التصيد الاحتيالي:** يستهدف العثور على بيانات سرية مثل: المعلومات الشخصية، وكلمات المرور بشكل مباشر.
- **الاحتيال المصرفي:** يستهدف نقاط الربط بين البنوك، ويستهدف التحويلات المالية، وحسابات المؤسسات المالية.

وبذلك يتضح لنا بأن طبيعة، وأنواع التهديدات السيبرانية تتطور بشكل مستمر، ومواكبة للتغيرات والتقدم التكنولوجي. وكما أن التنوع المتزايد في أساليب الهجمات السيبرانية يشير إلى حقيقة أننا نواجه عالما أصبحت فيها الحماية والخصوصية الرقمية أكثر تعقيدا عن سابق عهدها. وستظهر لنا تحديات جديدة وستصبح الهجمات السيبرانية أكثر ذكاء وخطورة، وهذا في حقيقة الأمر يتطلب استجابة متقدمة وسريعة باستمرار، ولابد من فهم تلك التهديدات السيبرانية لضمان الحماية الفعالة، والاستعداد الكافي لمواجهة المخاطر المستقبلية في الفضاء الرقمي

- **مفهوم الوعي بالأمن السيبراني:**

عرف(Zwilling,2022) وآخرون مفهوم الوعي بالأمن السيبراني بأنه: «درجة فهم

المستخدمين لأهمية أمن المعلومات ومسؤولياتهم والأفعال التي يقومون بها لممارسة مستويات كافية من الرقابة على أمن المعلومات لحماية بيانات المؤسسة وشبكاتها». وقد لاحظ نفس الكاتب وجود نقص واسع في الوعي بالمخاطر السيبرانية يمتد إلى استخدام التطبيقات، والإدلاء بالمعلومات الشخصية على شبكات التواصل الاجتماعي، وصفحات الويب بشكل مهم. وكما أشار نفس الكاتب بأن الهاكرز (فردين أو جماعات) يميلون إلى البحث عن أكثر المستخدمين ضعفًا، أي الذين يعانون من نقص في الوعي بأمن المعلومات والشبكات

وعرفت ابن ابراهيم (2021) الوعي السيبراني على أنه: «إدراك للمخاطر والهجمات الإلكترونية، ويتضمن ذلك فهمًا دقيقًا للأمن المعلوماتي، واتخاذ جميع الخطوات الضرورية للحفاظ على سلامة الأجهزة والبيانات»

وفي تقرير أصدره المركز الوطني الإرشادي للأمن السيبراني (2021) المعروف أيضا بـ Saudi CERT في المملكة العربية السعودية، ركَّز على تعزيز الوعي والمعرفة بالأمن السيبراني، ويشمل ذلك إصدار التنبيهات حول آخر وأخطر الثغرات الأمنية بالأمن السيبراني، وبرامج التوعية، والتعاون مع المراكز الإرشادية الأخرى ذات العلاقة، لتعزيز حماية الشبكات وأنظمة تكنولوجيا المعلومات، بما في ذلك أنظمة التشغيل ومكوناتها المتألفة من الأجهزة والبرمجيات. وكما يهدف إلى منع أي اختراق أو تعطيل، أو تعديل، أو دخول غير مصرح به، أو استخدام غير قانوني، أو استغلال غير مشروع للبيانات.

حيث يتبين أن تعزيز الوعي السيبراني لا يقتصر على فهم الأخطار فحسب، بل يشمل أيضًا تطوير القدرات الفردية والمؤسسية لمواجهة هذه التحديات بفعالية. يكمن الجوهر في تحويل هذا الوعي إلى تدابير عملية وسلوكيات يومية تضمن الحماية الأمنية الشاملة للأجهزة والبيانات، ومع التركيز على الحد من الثغرات التي قد يستغلها المهاجمون. وهكذا سيصبح التركيز على الوعي السيبراني جزءًا لا يتجزأ من استراتيجية الأمن الرقمي الشاملة، والتي تسعى للحفاظ على خصوصية وأمن المعلومات في عالم رقمي متسارع ومتطور.

- **أهمية الوعي بالأمن السيبراني:**

وفقا للشهراني (2020)، فإن أهمية التوعية بالأمن السيبراني تظهر كدرع وقاية لحماية الأفراد والمؤسسات من المخاطر السيبرانية، وتأمين المعلومات التي قد تكون عرضة للخطر، والاختراق والاستيلاء، خاصةً مع انتشار استخدام الإنترنت، ونقص الوعي الرقمي، خاصةً بين الأطفال والمراهقين. ويتعين تعزيز الممارسات الصحيحة، وفحص الوسائط الرقمية، والقدرات التي تقيس مدى سلامة المحتوى، ومختلف التفاعلات عبر الإنترنت. ويبرز هذا الأمر أهمية زيادة الوعي حول أهمية الأمن السيبراني بين الأفراد، وتوفير التدريب حول الأساليب والإجراءات الأمنية

ووفقا لجمال الدين (2023)من المتوقع أن تكلف الجرائم السيبرانية «أكثر من 6 تريليون دولار بحلول عام 2021، مقارنة بـ 3 تريليون دولار في عام 2015». لذلك، تكافح المؤسسات باستمرار للحفاظ على أمن أصول المعلومات الخاصة بها، مما يجبرها بدوره على القيام باستثمارات ضخمة في التدابير التكنولوجية المضادة. ومع ذلك فإن التركيز على الجوانب التقنية لأمن المعلومات لا يكفي، لأن أمن المعلومات هو بطبيعته متعدد التخصصات، ويلعب الجانب الإنساني دورًا رئيسيًا فيه؛ لذلك يرجع عدد كبير من حوادث أمن المعلومات التنظيمية إلى أخطاء بشرية كسبب غير مباشر لغالبية الحوادث الأمنية، بما في ذلك سوء السلوك المتعمد وغير المتعمد (Khando,2021 وآخرون)

وأشارت وكالة الإتحاد الأوروبي للأمن السيبراني إلى أن حوالي 77 % من خروقات بيانات الشركات تكون بسبب استغلال نقاط الضعف البشرية (ENISA,2019). كما تبين سابقًا أن أكثر من نصف جميع انتهاكات أمن المعلومات تتعلق بضعف امتثال الموظفين لأمن المعلومات

وقد بيَّن (Khando,2021)وآخرون أن المؤسسات تفشل في حملات تعزيز توعية الموظفين بمخاطر تهديدات الأمن السيبراني الخاصة بها، لأنها لا تعكس بشكل كافٍ العوامل التي تؤثر على مستويات الضرر الذي يطال لموظفين أثناء تطوير محتوى حملات التوعية، والأهم من ذلك أن الباحثين وجدوا هنالك نقصًا في الأساليب لإنشاء

«مواد جذابة ومناسبة» لتعزيز الوعي بتهديدات الأمن السيبراني. علاوة على ذلك لم يتم أخذ العديد من العوامل السلوكية في الاعتبار عند تطوير حملات أو برامج التوعية في الماضي، لتحسين مستويات الوعي ضد تهديدات الأمن السيبراني لدى الموظفين.

ونستخلص من هذه الدراسات السابقة حول أهمية الوعي بالأمن السيبراني بأن هذا الوعي يُعتبر خط الدفاع الأول ضد التهديدات الإلكترونية، وأنه مع تصاعد التحديات في مجال الأمن السيبراني، يبرز الدور الحيوي لنهج متكامل يربط بين التطورات التكنولوجية والوعي البشري

يشهد هذا المجال تطوير استراتيجيات تركز على تحسين الوعي السيبراني، من خلال تحديث المواد التعليمية، وإيلاء اهتمام خاص للسلوكيات الآمنة، والمسؤولية الشخصية. وتواجه المؤسسات تحدياً في بناء ثقافة أمنية تتخطى المعرفة التقنية لتشمل فهم العناصر البشرية والنفسية التي تؤثر على الأمن. ويتجلى ذلك في الحاجة إلى تعاون متزايد بين جميع المستويات داخل المؤسسة لضمان بيئة رقمية آمنة.

- **مستويات الوعي بمخاطر الأمن السيبراني:**

يعد العامل الرئيسي في تجنب مخاطر أمن المعلومات هو مستوى وعي الفرد بالأمن السيبراني، والذي يمكن وصفه بفعالية كمنخفض، أو متوسط، أو عال. وتشمل السلوكيات ذات المستوى المنخفض عدم الانتباه أو إهمال تنبيهات الأمن التي يتم توفيرها في معظم الحالات تلقائيًا من قبل التطبيقات، كالولوج إلى شبكات الواي فاي العامة والمجانية، باستخدام أجهزة الهواتف الذكية، والكمبيوترات الشخصية. ويمكن أن يتميز المستوى المتوسط بالإهمال الذي يظهر في تشغيل التكنولوجيا بطريقة غير صحيحة. وأخيرًا يتضمن المستوى العالي معرفة بالتهديدات السيبرانية، واتخاذ إجراءات فعالة للوقاية منها (Khando,2021 وآخرون).

ووفقا (Al-Alawi,2020 وآخرون فإن أهم أصول المنظمة وعواملها هم العاملون فيها. ويمكن أن يكون هذا أيضًا الحلقة الأضعف في حماية البيانات، خاصة عندما يلعب التنقل وإمكانية الوصول دورًا هائلاً في تحسين الكفاءة

لذلك، فإن مسألة الأمن السيبراني لا تشكل مصدر قلق للمنظمة فحسب، بل أيضًا للأفراد العاملين الذين يتعرضون أيضًا للتهديدات السيبرانية من خلال الوسائط الرقمية الإلكترونية الخاصة بهم مثل: هواتفهم الذكية، وأجهزة الكمبيوتر الشخصية، ونظام بروتوكول الإنترنت

ونظرًا لأن العامل البشري قد تم إظهاره بالفعل كسبب رئيسي للتهديدات السيبرانية، يتم تركيز برامج التدريب على الوعي بالتهديدات السيبرانية من قبل المؤسسات الأكاديمية والشركات الخاصة، بهدف زيادة وعي الأفراد بالجرائم السيبرانية (Zwilling,2022 وآخرون).

أما من حيث الموظفين فيمكننا القول بأن الإنترنت قد غيَّر طريقة إدارة المهام الحياتية، مما سمح بالتواصل مع أشخاص جدد من خلال شبكات التواصل الاجتماعي، وفتح آفاق اقتصادية جديدة للمعاملات عبر الأجهزة المحمولة سواء للأفراد أو المنظمات، بما في ذلك التغيير الجذري في نظام التعليم العالي وطرق التدريس. ومع ذلك لا يزال العديد من الأشخاص يواجهون مخاطر أمن المعلومات من مجموعة واسعة من التهديدات. وتتنوع هذه التهديدات بين هجمات بسيطة إلى هجمات كارثية، فقد تتكون الأولى من رسائل البريد الإلكتروني غير المرغوب فيها، وتشمل الثانية مجموعات منظمة للجريمة السيبرانية والتي تستخدم برامج خبيثة لسرقة وتلف وتدمير البيانات على نطاق واسع

- **العوامل المؤثرة في الوعي بالأمن السيبراني:**

يعد الوعي بالأمن السيبراني أمرًا هامًا، وهذا ما دفع المؤسسات إلى زيادة جهودها للتخفيف من هذه التهديدات أو منعها. إن نوعية التأثيرات المترابطة التي تحدث بين مكونات نظام العوامل البشرية قد تؤثر على أداء الإنسان وتصرفاته بشكل عام. ويمكن أن يكون للممارسات الإدارية السيئة والقواعد المكتوبة بشكل سيء والإجراءات غير الواضحة العديد من الآثار السلبية.

يمكن وصف تحديات الأمن السيبراني من منظور اجتماعي تقني مع الأخذ في

الاعتبار وجهات النظر المتعددة للعوامل التنظيمية، والعوامل الفردية، والعوامل التكنولوجية، والأبعاد الأخلاقية (Mohammed, (Basmasoud 2022. إما بالتركيز على دراسات التوعية السابقة بالأمن السيبراني لدى العمال أو الموظفين، وهناك العديد من الدراسات المثيرة للاهتمام التي وصفت نتائجها على النحو التالي

Nachin, N (2019) والتي قامت بدراسة زيادة الوعي بالأمن السيبراني مع أكثر من 4500 موظف من 20 منظمة، ثم وجدوا أن النهج القائم على المحاكاة يمكن أن يساعد في تحسين أو زيادة مستوى الوعي بالأمن السيبراني، وهو أكثر عملية من النهج الذي يقوم على التعليم. ومع ذلك ينبغي استخدام كلا النهجين والجمع بينهما.

كما أنا Ikhsan, & Ramli (2019) قاموا بقياس مستوى الوعي بأمن المعلومات لدى الموظفين الحكوميين من خلال دراسات حالة مع 736 مستجيبًا في إحدى المنظمات في إندونيسيا باستخدام نهج السلوك والمعرفة عبر نموذج استبيان في محاكاة التصيد الاحتيالي. ووجدوا أن مستوى الوعي بأمن المعلومات لدى الموظفين أو العاملين بلغ 3.79%تقريباً، وهذه النتيجة لن تصل إلى مستوى «جيد»

أما (Baillon, A 2019) فقد درَّس عددًا كبيرًا جدًا من الموظفين في هولندا، ووجد أن الفئة العمرية الأصغر من الموظفين (16-25 عامًا) كانت الأقل احتمالًا لزيارة روابط التصيد، في حين كان الموظفون في الفئة العمرية فوق (46) عامًا حوالي 15 عامًا % أكثر احتمالية للوصول إلى الرابط المزيف من المجموعة الأصغر سنا.

كما حدَّدَ(Daengsi, T (2022 العديد من العوامل التي تلعب دورًا في الوعي بالأمن السيبراني، وهي تشمل: العمر، والجنس، والتعليم، والمؤهلات الجامعية، والخبرة في مجال تكنولوجيا المعلومات. وأكد أن الجنس يلعب دورًا في الوعي بالأمن السيبراني، حيث كان لدى الموظفات في شركة الخدمات المالية في هذه الدراسة مستوى أعلى من الوعي بالأمن السيبراني مقارنة بالموظفين الذكور، وبالإضافة إلى ذلك، فقد أظهرت النتائج أن الجيل العمري للمستخدمين يؤثر على وعيهم بالأمن السيبراني.

- **إجراءات تعزيز الوعي بالأمن السيبراني:**

وفقا للمنتشري وحريري (2020) تتضح أن هناك العديد من الإجراءات التي يمكن للأفراد، ورواد الفضاء السيبراني اتخاذها لاستخدام الإنترنت بشكل آمن، وتجنب التهديدات والهجمات الإلكترونية ومن أمثلة ذلك

- التحكم في وضعيات الأمان مثل «أمان كلمة المرور» واختيار كلمات مرور قوية وتغييرها بشكل دوري.
- الحفاظ على تحديث برامج جدار الحماية وبرامج مكافحة الفيروسات وبرامج مكافحة التجسس باستمرار.
- التأكد من إعدادات الحاسوب وشبكة الإنترنت وتحديث نظام التشغيل بشكل دوري.
- عدم الاستجابة لأي رسائل غير مرغوب فيها تصل إلى البريد الإلكتروني.
- حماية المعلومات الشخصية وعدم نشر أي معلومات شخصية عبر البريد الإلكتروني أو مواقع التواصل الاجتماعي.

أما الشريف وآخرون (2023) فقد وضح اجراءات تعزيز الأمن السيبراني بأنها تتمثل في عدة نقاط:

- التأكد من سلامة وصحة البنية التحتية والحفاظ على تحديث جدران الحماية ومتابعتها بشكل منتظم.
- إعداد كلمات مرور قوية، وأن تكون غير معتادة، ولابد من تحتوي على حروف وأرقام وإشارات.
- القيام بتأهيل وتدريب المستخدمين على التعامل، واستخدام نظم المعلومات التي تتميز بقوتها وسريتها، وأيضا لابد من التوجيهات التي تعمل على توعيتهم وإدراكهم لضمان الأمن والسرية.
- توعية المستخدمين بالحذر من تحميل أي برامج مجهولة المصدر أو غير موثوقة

وفحص البرمجيات قبل استخدمها بشكل فعلي.

- الإمكانية من تحديد الدخول وتأمين الوصول إلى النظام، وهنا لابد من وضع بعض الأسس والتعليمات للأشخاص المخولين لهم بدخول، والتعامل مع النظام بكل موثوقية.
- عمل نسخ احتياطية للبيانات والملفات من أجل ضمان الحصول عليها عند حدوث مشكلة ما، وهي تكون محددة مسبقا من أجل ضمان التوحيد في معايير الحفظ والحماية.

إن تأمين الأجهزة الشخصية يظل أمرًا ذا أهمية بالغة في عصرنا الرقمي المتقدم، حيث يعتبر هذا التدابير الأمنية ضروريًا لضمان سلامة المعلومات الحساسة والبيانات الشخصية. ويكمن الخطر في أن الأجهزة الشخصية يمكن استخدامها بشكل مباشر أو غير مباشر في مجموعة واسعة من الأنشطة بدءًا من العمل اليومي إلى التفاعلات الشخصية. من خلال تأمين هذه الأجهزة سيتم الحفاظ على الخصوصية والأمان، وأيضا سيمنع التجاوزات غير المصرح بها

وأن تحقيق الأمان للأجهزة الشخصية يحمي البيانات المخزنة عليها من التسريب غير المصرح به والوصول غير المرغوب فيه. بالإضافة إلى ذلك سيُعزز تأمين الأجهزة الشخصية استعداد الأفراد للتعامل مع التحديات السيبرانية المتزايدة، ويمكن استخدام هذه الأجهزة كوسيلة للهجمات الإلكترونية

بشكل عام يعد تأمين الأجهزة الشخصية خطوة ضرورية للمحافظة على الاستقرار والأمان في بيئة العمل والحياة الشخصية في عصر تكنولوجيا المعلومات

ووفقا للدليل الإرشادي لجوانب الأمن السيبراني للعمل عن بعد (2021) أضاف بعض الممارسات لتحصين أجهزة الموظفين من التهديدات السيبرانية، وذلك على النحو الآتي:

- **استخدام أنظمة وبرامج أصلية:** تجنب استخدام أنظمة تشغيل أو برامج غير أصلية، حيث قد تحتوي على مكونات غير آمنة، وتشكل مخاطر لا يمكن إصلاحها بسهولة.

يفضل استخدام نسخ أصلية من نظام التشغيل لتعزيز أمان جهازك.

- **تحديث البرامج ونظام التشغيل:** بمجرد التأكد من أن جميع برامجك أصلية، قم بتنزيل جميع التحديثات الدورية لنظام التشغيل والبرامج الأخرى لسد الثغرات الأمنية الجديدة. ويفضل السماح بتحديثات النظام بشكل تلقائي إذا كان جهازك جزءًا من بيئة عمل.
- **تفعيل مكافحة الفيروسات والحماية:** قم بتفعيل برامج مكافحة الفيروسات والحماية إذا كانت متوفرة. في حال عدم توفرها، احصل على برنامج حماية شامل يتضمن جدارًا ناريًا ومكافحة فيروسات قوية، وتأكد من تحديثه بانتظام لمواكبة أحدث التهديدات.
- **إيقاف خاصية المشاركة الشبكية:** قم بإيقاف خاصية «المشاركة الشبكية» إذا لم تكن ضرورية، لتقليل فرص دخول الآخرين إلى جهازك.
- **إدارة الاتصالات غير الضرورية:** أطفئ خدمات الاتصالات الغير ضرورية مثل Wi-Fi، وNFC، وBluetooth، وHotspot، لتوفير طاقة البطارية، وتقليل فرص استغلال الثغرات الأمنية.
- **تشفير الأقراص الداخلية:** قم بتشفير أقراص الجهاز لحماية بياناتك في حالة سرقته، باستخدام برامج مثل BitLocker أو Vera Crypt.
- **مراقبة التحديثات خارج الشبكة:** تحقق من عمليات التحديث لنظام التشغيل، وبرنامج مكافحة الفيروسات أثناء خروجك من شبكة العمل للتأكد من استمرار عملها بشكل صحيح، وإبلاغ الدعم الفني في حالة وجود أي مشكلة.

طرق تدريب الموظفين على الوعي بالأمن السيبراني:

وفقا(Al-Alawi,2020) وآخرون يعد تدريب الموظفين أمرًا ضروريًا لرفع مستوى الوعي بين الموظفين وتحفيزهم على الاهتمام بالتهديدات السيبرانية وخطوات التصدي

لها، حتى لو لم تكن جزءًا من دورهم

ووفقًا لمعيار أمن البيانات، يعتبر توفير التوجيهات والمواد المناسبة للأشخاص المناسبين بطريقة سريعة وفعالة هو المفتاح لرفع الوعي بأمن المعلومات بشكل فعّال. ومن الناحية النظرية والعملية يمكن تحديد العديد من الأساليب لبناء وعي أمن المعلومات، سواء كانت تقليدية، أو تعتمد على تكنولوجيا المعلومات والاتصالات. وتشمل أكثر الأساليب استخدامًا وفقا لـ Stefanik, T (2020

التدريب في الفصل (في مكان العمل أو في مركز خارجي): الغرض الرئيسي هو توفير مجموعة من المعلومات للموظفين المتعلقة بأمان المعلومات (السياسات والإجراءات المعمول بها في المنظمة، والتغييرات إلخ) بطريقة سريعة وفعّالة

- **المناقشة الجماعية:** اجتماع لمجموعة من 15-20 شخصًا يستفيد المشاركون فيه بشكل كامل من تبادل المعرفة والخبرة، حيث لا تكون هناك اتصالات أحادية الاتجاه. ويتم اختيار قضايا تتعلق بأمن المعلومات ومناقشتها، ويتاح لجميع المشاركين فرص متساوية لشرح وجهات نظره.
- **النشرات:** تهدف إلى تعزيز برامج أمن المعلومات، ويمكن أن تكون على ورق أو إلكترونية، وتوفر فرصة إرسال العديد من الرسائل في نفس الوقت.
- **ألعاب الفيديو:** تحفز معرفة أمن المعلومات، وتجمع بين المتعة والتدريب، ولها تأثير كبير على تغيير مواقف المستخدم. ومع ذلك ليست أفضل مصدر لتوفير معلومات مفصلة حول سياسة أمن المعلومات.
- **مقاطع الفيديو:** تمكين المشاركين من التعلم في أي وقت، أو لمدة يرغبون فيها دون فرض قيود زمنية، ومع ذلك فإنها لا تسمح بالتفاعل بين المدرب والمشارك.
- **حملات الملصقات:** وضع الملصقات في المناطق المشتركة يهدف إلى جذب انتباه أكبر بطريقة شعاريه إلى الخطوات (السلوكيات) التي يجب اتخاذها لتحسين الأمان.

- **التدريب القائم على الحاسوب (CBT):**

كما أظهرت دراسة Bada,& Nurse (2019) أهمية إجراء فعاليات، وندوات، وورش عمل، من أجل التوعية السيبرانية

ووفقا لـ (Mohammed, & Basmasoud 2022) فإن عوامل تعزيز الوعي بالأمن السيبراني تشمل

- **أولاً:** إعداد الوعي الأمني وتنظيمه بشكل احترافي للعمل.
- **ثانياً:** إن إثارة الخوف لدى الناس ليس أسلوباً فعّالاً جاهزاً للاستخدام، لأنه قد يخيف الناس الأقل قدرة على خوض المخاطر
- **ثالثًا:** يجب أن يكون التعليم الأمني أكثر من مجرد توفير المعلومات للمستخدمين ، بل يجب أن يكون مستهدفًا وقابلاً للتنفيذ ويقدم تعليقات.
- **رابعًا:** بمجرد أن يصبح الأشخاص مستعدين للتغيير، ويعد التدريب والتغذية الراجعة المستمرة أمرًا ضروريًا لإبقائهم خلال فترة التغيير.
- **خامسًا:** من الضروري التركيز على السياقات والخصائص الثقافية المختلفة عند إنشاء حملات التوعية بالأمن السيبراني.

أظهرت الدراسة أهمية التفكير النقدي في التحديات المتعلقة بتحسين سلوكيات أمن المعلومات لدى الموظفين والمواطنين والمستهلكين. يُعتبر فهم كيفية إدراك الأفراد للمخاطر السيبرانية أمرًا حيويًا لتصميم حملات توعية فعّالة. أكد الباحثون أنهم استعرضوا مفهوم تمارين الدفاع السيبراني (CDX)، التي تسهم في تعزيز الوعي بسلامة الفضاء السيبراني وتجميع الخبرات التجريبية. كما تساهم هذه التمارين في اختبار قدرة المنظمة على مقاومة الأحداث السيبرانية والتعامل معها، بهدف إيجاد بيئة آمنة.

ويمكن تعريف برامج التوعية الأمنية وفقًا للمعهد الوطني للمعايير والتكنولوجيا في الولايات المتحدة الأمريكية على أنها حملات تستخدم جميع الوسائل الممكنة لجذب

انتباه الجمهور المستهدف وتوجيه انتباههم نحو مجال الأمان السيبراني وأهميته. يهدف هذا التوجيه إلى جعلهم على دراية بالتحديات والمخاطر والتهديدات الأمنية، وتحقيق التوعية للوقاية منها، وتعزيز التعامل السليم معها هوساوي، ياسر (2020)

يجب أن يشمل برنامج توعية الأمن السيبراني بشكل جيد تدريبًا فعّالًا يتناسب مع أهداف المنظمة، مع التركيز على زيادة الوعي بالأمن السيبراني أثناء أداء الموظفين لواجباتهم وتحقيق التواصل التفاعلي بين جميع الفاعلين حيال أي قضية تتعلق بالأمن السيبراني. وقد تفشل برامج التوعية إذا لم تكن مصممة لتغيير سلوك الأفراد وكذلك إذا لم يمكن تحقيق تأثير إيجابي على المنظمة. ويُعَدُّ برنامج توعية الأمن السيبراني استثمارًا مؤسسيًا طويل المدى يُسهم في بناء ثقافة للأمن السيبراني في حال تقديم التدريب بشكل مستمر. هوساوي، ياسر (2020)

وقد اقترح Sabillon,R (2019) وآخرون نموذجا للتدريب على التوعية بالأمن السيبراني (catram) للتوعية بثقافة الأمن السيبراني لدعم تدريب مختلف الموظفين التنظيميين.

ويقوم نموذج التدريب على التوعية بالأمن السيبراني (CATRAM) بكسر أنماط التدريب التقليدية، من خلال استهداف جماهير معينة ومجموعات مختلفة من الأهداف في أي منظمة. وقد يرتبط تقديم التوعية بالأمن السيبراني لأعضاء مجلس الإدارة والتنفيذيين بالاستراتيجية والحوكمة، بينما يستهدف المديرون على المستوى التكتيكي محتوى واسع للأمن السيبراني للمستخدمين النهائيين على المستوى التشغيلي، وأخيرًا ولكن ليس آخراً، التدريب المتخصص لموظفي تكنولوجيا المعلومات.

كما اقترح(2022) Hijji,& Alam هيكل إطار CAT، والذي يتضمن ثلاثة مستويات رئيسية: المبتدئ (الوعي)، المتوسط (التدريب)، والمتقدم (العملي والتقييم). وبالمثل فقد حدد مجموعة مكونة من 25 ممارسة من أهم الممارسات لتحقيق المستويات المتقدمة.

وتم إنشاء دراسة حالة وإجراؤها لتقييم إطار عمل CAT المقترح داخل منظمات

الأمن السيبراني للتحقق من صحتها، ولأغراض التحسين الإضافية. وتم تنفيذ دراسات الحالة في منظمتين فقط في المرحلة الأولية، وتم تحقيق النتائج.

ووفقا لـ (هوساوي، ياسر 2020)، فإنه يمكن تنفيذ برامج التوعية بالأمن السيبراني باستخدام عدة أساليب وسياسات، وتعتمد هذه الاستراتيجيات على الوضع الأمني للمنظمة، والبيئة المحيطة بها. والتي يمكن تلخيصها في تقديم التوعية من خلال التعليم والتدريب، واستخدام تقنيات الترغيب والتشجيع، وتبني نهج العقوبات أو الإجبار. وفي النهاية يُشدد الكاتب نفسه على أن أفضل برامج التوعية بالأمن السيبراني تكون شاملة وتجمع بين جميع هذه الأساليب بشكل متدرج ومتكامل

- **فجوات الدراسات السابقة:**

بناءً على الدراسات المشار إليها خلال هذا الفصل، يمكن حصر فجوات الأبحاث الحالية حول وعي الموظفين بالأمن السيبراني في النقاط التالية

- لم تدرس جميع الدراسات كامل العوامل الديموغرافية المُهمّة بخلاف العمر، مثل: الجنس والمستوى التعليمي، والخبرة، ونوع المهنة. فمن الضروري دراسة تأثير هذه العوامل على الوعي بالأمن السيبراني.
- تركز معظم الدراسات السابقة على قطاع واحد، وهو القطاع الحكومي، لذا فإنه من المهم إجراء دراسات مماثلة في قطاعات أخرى مثل: الصناعة، والأعمال، والتعليم، والرعاية الصحية.
- تقتصر الدراسات الراهنة في مجال الأمن السيبراني إلى التركيز على الدراسات التي تجمع البيانات في وقت واحد (الدراسات المستعرضة) بدلاً من النظر في كيفية تطور الأمور على مر الزمن. حيث أن هذه الدراسات تلتقط صورة لحالة الوعي بالأمن السيبراني في لحظة معينة، لكنها لا تشرح كيف يمكن تحسين هذا الوعي، أو ما هي النتائج الفعلية لأي تدخلات تمت لزيادة الوعي. وهناك نقص في الدراسات

التي تطبق تدخلات معينة (مثل برامج التدريب أو الحملات التوعوية)، والتي تقيس مدى فعاليتها في تحسين الوعي بالأمن السيبراني على المدى الطويل.

- هنالك قصور في الدراسات السابقة بمجال الأمن السيبراني، حيث أنها لم توفر طريقة لمقارنة فعالية طرق التدريس المختلفة مثل: الدروس التقليدية مقابل استخدام المحاكاة. ولم تقم بإجراء دراسات تجريبية جديدة مباشرة وواضحة بين هذه الأساليب المختلفة لتحديد أيها أكثر فعالية في تعزيز الوعي بالأمن السيبراني.
- على الرغم من وجود دراسات لا حصر لها حول قضايا الأمن السيبراني في الوطن العربي وفي العالم، إلا أنه هناك نقص في الدراسات التي تركز على الوعي بالأمن السيبراني بين الإدارة العليا والموظفين ومواقفهم.
- من الشائع أن تركز الأبحاث السابقة على النتائج الفورية مقللة من أهمية وضرورة النظر في العواقب والنتائج طويلة المدى. حيث أن هذه الفجوة تدل على وجود فراغ كبير بالمعرفة في هذا المجال، وهذا يتطلب من الأبحاث المستقبلية إيلاء المزيد من الاهتمام للتأثيرات طويلة الأمد.
- لم يتم التطرق حول تأثير التقنيات الحديثة أو الناشئة على المستخدمين، وهذا النقص يبرز الحاجة لفهم أعمق حول كيفية تأثيرها على مختلف المجالات.
- لاحظنا أنه لم يتم مراعاة الجانب الأخلاقي والاجتماعي في بعض الدراسات السابقة، وهذا قد ينتج عنه عدم تحديد المشكلة الرئيسية والدوافع وكيفية التغلب عليها.
- بالرغم من وجودة دراسات سابقة في مجال الأمن السيبراني، إلا أنه لوحظ بقلة الدراسات التي تقوم بتحليل الهجمات السيبرانية لفهم الثغرات الأمنية وكيفية مواجهتها، بما في ذلك الأساليب التي قد يستخدمها المهاجمون وتقييم الإستراتيجيات الدفاعية المعمول بها، والآثار المترتبة على الأمن السيبراني، والتوصيات المستقبلية لتحسين الاستجابة والوقاية، وزيادة الوعي والإدراك الأمني

الرقمـي لـدى المسـتخدمين.

- بالرغـم مـن وجـود دراسـات سـابقة فـي مجـال الأمـن السـيبراني، إلا أننـا لـم نجـد دراسـات تقـوم بدراسـة التأثيـر النفسـي للتهديـدات السـيبرانية ودورهـا فـي التأثيـر علـى الصحـة النفسـية للمسـتخدمين الأفـراد، وكيفيـة تطويـر لوائـح أو اسـتراتيجيات للتعامـل مـع تلـك الآثار.

الفصل الثالث

منهجية البحث:

- **مقدمة:**

هذا البحث يهدف إلى استكشاف وقياس الوعي السيبراني بين موظفي الهيئة، لتحديد كيفية تأثير هذا الوعي على حماية الأصول والممتلكات الرقمية. من خلال بحث ميداني يستخدم استبيان وتحليلات إحصائية دقيقة. ويقدم هذا الفصل منهجية البحث الكمية، مع التركيز على المقاربة الاستقرائية لفهم أعمق للتحديات والفرص المتعلقة بالأمن السيبراني. إن التزامنا بأخلاقيات البحث وحرصنا على سرية وخصوصية المشاركين يعزز من قيمة هذه الدراسة.

- **تصميم البحث:**

نذكر أولا بأهداف هذا البحث:

- **أولًا:** يسعى البحث إلى تحديد الثغرات المعرفية في فهم الأمن السيبراني، من خلال تحديد نقاط القوة ومجالات التحسين، يمكن تطوير استراتيجيات مستهدفة تساهم في تعزيز الأمن الرقمي على مستوى الهيئة.
- **ثانيًا:** يهدف البحث إلى استكشاف العلاقة بين مستويات الوعي السيبراني ومدى التزام الموظفين بالسياسات والإجراءات الأمنية. يشكل هذا الفهم أساسًا لتقديم توصيات ملموسة لتحسين البنية التحتية للأمن السيبراني وتطوير برامج تدريبية أكثر فعالية تلبي الاحتياجات الفعلية للموظفين.
- **ثالثا:** يسعى البحث إلى تقييم التأثير المتوقع لتحسين الوعي السيبراني على الحد من الحوادث الأمنية، وتعزيز قدرة الهيئة على الاستجابة للتهديدات السيبرانية بكفاءة. من خلال تحليل شامل للبيانات المجمعة من الاستبيانات والمقابلات، يهدف البحث إلى توفير رؤى قيمة تسهم في بناء بيئة عمل رقمية أكثر أمانًا واستدامة.

واستنادًا إلى الأهداف الموضحة أعلاه، صُمم هذا البحث ليستفيد من الدراسات السابقة في الإجابة على أسئلته الرئيسية، مع التركيز على استخدام الاستبيان كأداة أساسية لجمع البيانات. هذا النهج يضمن تغطية شاملة ودقيقة لموضوع الأمن السيبراني، مما يسهم في تعزيز الوعي، وتحسين استراتيجيات الحماية ضد التهديدات السيبرانية في بيئة العمل

- **مجتمع البحث:**

مجتمع البحث في هذه الدراسة يتألف من موظفي الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ، وهو يشمل مجموعة متنوعة من المنتسبين سواء كانوا ضباطًا، أفرادًا، أو مدنيين.

الموظفون في الهيئة ينتمون إلى تخصصات وأقسام متعددة تشمل الإدارة العامة للهوية وجوازات السفر، الإدارة العامة للإقامة وشؤون الأجانب، الإدارة العامة للخدمات المساندة، الإدارة العامة لأمن المنافذ، الإدارة العامة للجمارك، بالإضافة إلى الوحدات التنظيمية التابعة لمدير عام الهيئة. هذا التنوع يسمح بإجراء تحليل متعمق لمستويات الوعي السيبراني عبر مختلف الوظائف والمسؤوليات

سيتم استخدام مجموعة من الأسئلة الاختيارية لقياس وعي الموظفين بالأمن السيبراني، مع التركيز على التهديدات والهجمات السيبرانية وتأثيرها على الأصول والممتلكات الرقمية

تُعتبر المشاركة في البحث اختيارية، وقد تم تصميم الاستبيان لضمان السرية والخصوصية. هذه الخطوة تهدف إلى تشجيع الموظفين على المشاركة بصدق وشفافية، مما يعزز من دقة وفعالية النتائج المتوقعة من البحث

- **منهجية البحث:**

في هذا البحث، نعتمد منهجًا كميًا يهدف إلى قياس مستوى الوعي السيبراني لدى موظفي الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ. وقد تم استخدام

الاستبيان كأداة لجمع البيانات، حيث صُمم لتغطية مجموعة واسعة من الأسئلة التي تتناول مختلف جوانب الأمن السيبراني. الأسئلة مبنية بطريقة تسمح بتقييم مفصل للمعرفة والممارسات، والاتجاهات المتعلقة بالأمن السيبراني بين الموظفين

ولحرص الدراسة على ضمان مصداقية ودقة البيانات المجمعة والسرية والخصوصية في جمع وتحليل البيانات، تم اعتماد تدابير صارمة تضمن سرية معلومات، وذلك من استخدام منصة Survey Monkey، المعتمدة من الهيئة المختصة، كأداة لإنشاء استطلاعات الرأي وتوزيعها وتحليل نتائجها.

كما يشمل ذلك الحفاظ على الإجابات مجهولة الهوية ومعالجتها بطريقة تجميعية لتحليل النتائج. وتسعى الدراسة لتقديم فهم معمق لواقع الوعي السيبراني لدى موظفي الهيئة، من خلال هذا النهج الكمي، مما يسهم في صياغة استراتيجيات فعالة لتعزيز الأمن السيبراني ضمن الهيئة

- **تحليل البيانات:**

تحليل البيانات في هذه الدراسة يتبع منهجية كمية، معتمدًا على استخدام برنامج إحصائي لتحليل البيانات المتحصلة من الاستبيان.

يتم استخدام برنامج SPSS لتنظيم وتحليل البيانات. هذا يشمل حساب الإحصائيات الوصفية مثل: المتوسطات، والانحرافات المعيارية، بالإضافة إلى تطبيق تحليلات أكثر تعقيدًا كتحليل العوامل واختبارات الفروق لاستكشاف العلاقات والأنماط ضمن البيانات. الهدف من هذا التحليل هو تحديد مستويات الوعي السيبراني، وتحديد أي فجوات معرفية قد تحتاج إلى معالجة

نتائج التحليل ستُستخدم لصياغة توصيات محددة تهدف إلى تعزيز الوعي والإجراءات الأمنية السيبرانية ضمن الهيئة. هذه التوصيات ستكون مدعومة بالأدلة وموجهة نحو تحسين السياسات والبرامج التدريبية الحالية، لضمان تحقيق بيئة عمل أكثر أمانًا ووعيًا بالمخاطر السيبرانية.

- **الاعتبارات الأخلاقية:**

تعتبر الاعتبارات الأخلاقية جزءًا لا يتجزأ من تصميم وتنفيذ هذه الدراسة، حيث تم تبني مجموعة من المبادئ الأخلاقية لضمان احترام حقوق وخصوصية جميع المشاركين.

1. **أولًا:** تم إبلاغ المشاركين بشكل كامل عن طبيعة البحث، أهدافه، وكيفية استخدام البيانات المجمعة قبل موافقتهم على المشاركة. كما تم ضمان الحق في الانسحاب من الدراسة في أي وقت دون أي تبعات.
2. **ثانيًا،** تم التأكيد على مجهولية البيانات وسريتها. تم تصميم الاستبيانات بطريقة تضمن عدم الكشف عن هوية المشاركين، وتم التعامل مع جميع البيانات المجمعة بسرية تامة، حيث يتم تخزينها في قواعد بيانات مؤمنة والوصول إليها مقصور فقط على الباحثين المسؤولين عن الدراسة. إضافة إلى ذلك، أخلاقيات البحث تلعب دورًا مهمًا في عملية تحليل البيانات، حيث يتم التعامل مع جميع المعلومات المجمعة بسرية وخصوصية تامة. يتم ضمان أن تظل هويات المشاركين مجهولة، وأن يتم استخدام البيانات لأغراض البحث هذا فقط.
3. **ثالثًا:** تم التركيز على العدالة والإنصاف في اختيار عينة البحث، لضمان تمثيل جميع فئات الموظفين في الهيئة بشكل عادل ومتوازن، مما يساهم في الحصول على نتائج دقيقة وشاملة.
4. **رابعًا:** تم التأكيد على أهمية حماية خصوصية المشاركين وسرية بياناتهم. تم توضيح طبيعة البحث وأهدافه للمشاركين.

أخيرًا: تم الالتزام بالشفافية في كل مراحل البحث، بدءًا من جمع البيانات، وصولًا إلى نشر النتائج، وذلك من خلال نقل بيانات ونتائج الاستبيان كما هي دون تغيير أو تحريف أو إنقاص. هذا الالتزام يؤكد على الهدف الأساسي من الدراسة، وهو تعزيز الوعي بالأمن السيبراني، وتحسين السياسات والإجراءات الأمنية لحماية الأصول والمعلومات الحيوية للهيئة

الفصل الرابع

تحليل بيانات الدراسة:

- **مقدمة:**

تسعى هذه الدراسة إلى تحقيق أهداف أساسية حول الوعي بالأمن السيبراني لدى موظفي الهيئة الاتحادية للهوية والجمارك وأمن المنافذ، وهي تحديد التهديدات السيبرانية التي تواجه موظفي الهيئة، وتقييم المستوى الحالي للوعي الأمني لديهم، واقتراح برامج لتطوير الوعي بالأمن السيبراني.

ولتنفيذ هذه الأهداف، تم تنفيذ استبيان تم توزيعه، وشارك فيه 226 مجيبا من موظفي الهيئة. وتمت معالجة نتائج الاستبيان باستخدام التحليل الإحصائي الوصفي ويعرض هذا الفصل الرابع نتائج الاستبيان.

- **تحليل البيانات:**

تعكس الإجابات الكبيرة والتي تمثلت في 226 إجابة على أسئلة البحث اهتماماً وتفاعلاً واضحاً من قبل الموظفين مع موضوع الأمن السيبراني. هذا العدد من الإجابات يوفر نظرة شاملة على مدى الوعي بالأمن السيبراني داخل الهيئة، مشيراً إلى وجود مستوى معين من الاهتمام بالمسائل الأمنية. التجاوب الواسع مع الاستبيان يسلط الضوء أيضاً على التزام الموظفين بالمشاركة في الجهود الرامية لفهم ومعالجة قضايا الأمن السيبراني.

تنوع الإجابات والنسب المئوية المختلفة تساعد في رسم صورة عن مستويات الفهم والإدراك لدى الموظفين بخصوص التهديدات السيبرانية والإجراءات الوقائية.

وبالإجمال، تشير البيانات المجمعة من هذا العدد الكبير من الإجابات إلى وعي ملموس بالمخاطر الأمنية ويعكس تفاعل الموظفين مع المواضيع المتعلقة بالأمن السيبراني داخل الهيئة.

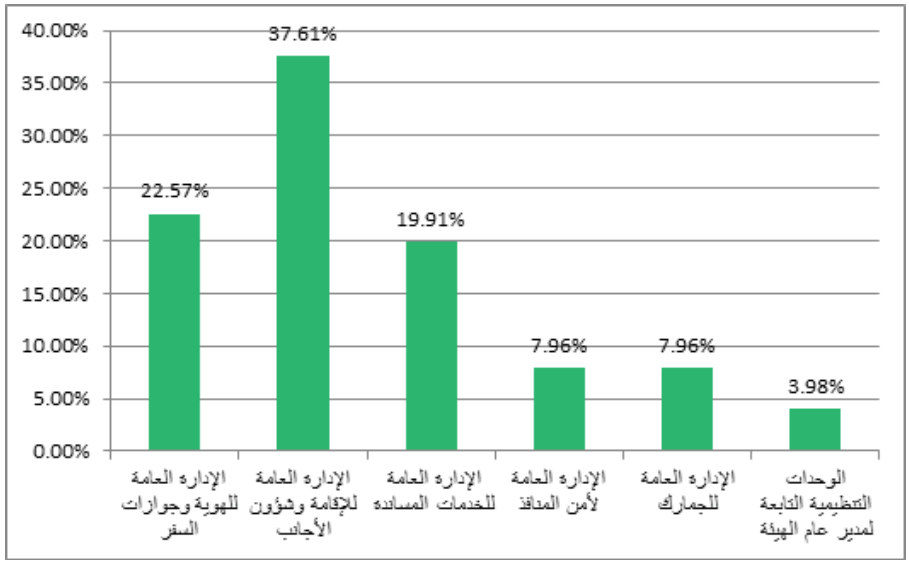
- **توزيع الإجابات حسب القطاعات**

توزعت قطاعات الموظفين الذين أجابوا على الاستبيان كالتالي:

النتائج:

- الإدارة العامة للإقامة وشؤون الأجانب: **37.61 % (85 صوت)**
- الإدارة العامة للهوية وجوازات السفر: **22.57 % (51 صوت)**
- الإدارة العامة للخدمات المساندة: **19.91 % (45 صوت)**
- الإدارة العامة لأمن المنافذ: **7.96 % (18 صوت)**
- الإدارة العامة للجمارك: **7.96 % (18 صوت)**
- الوحدات التنظيمية التابعة لمدير عام الهيئة: **3.98 % (9 أصوات)**

الرسم البياني:



- **التحليل:**

تُظهر نتائج استبيان الوعي بالأمن السيبراني أن موظفي الإدارة العامة للإقامة وشؤون الأجانب هم الأكثر إجابة على الاستبيان بنسبة (37.61 %)، تليها الإدارة العامة للهوية وجوازات السفر (22.57 %) والإدارة العامة للخدمات المساندة (19.91 %). بينما كانت الإدارة العامة لأمن المنافذ والإدارة العامة للجمارك متساويتين في (7.96 %). أما الوحدات التنظيمية التابعة لمدير عام الهيئة، فجاءت بأدنى نسبة (3.98 %).

ويرى الباحث أن تباين النسب المئوية تختلف من قطاع إلى أخر قد تكون للعوامل التالية :

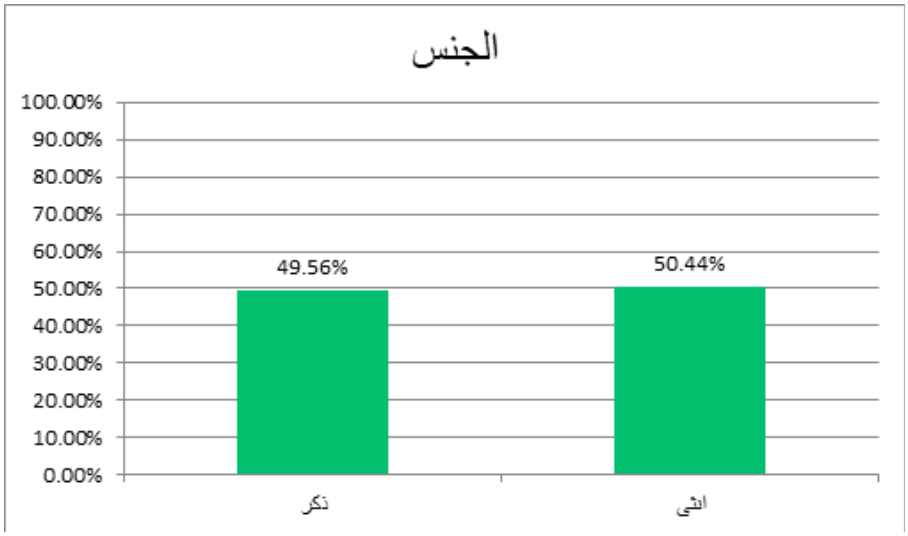
- **حجم القطاع وتوفر الوقت:** قد يؤثر حجم القطاع ومدى انشغال الموظفين بمهامهم اليومية على قدرتهم على المشاركة في الاستبيان. موظفي القطاعات التي تواجه ضغوطًا زمنية أقل قد تظهر نسب مشاركة أعلى.
- **الإدراك والقيمة الملموسة:** ربما يرى الموظفون في القطاعات ذات النسب المشاركة الأعلى قيمة أكبر ملموسة في المشاركة بالاستبيان، سواء بسبب تجارب سابقة مع التهديدات السيبرانية أو التأكيد من الإدارة على أهمية الأمن السيبراني لعملهم.
- **التعرض للتدريب:** قد تتلقى بعض القطاعات تدريبًا أكثر شمولاً وتخصصًا حول الأمن السيبراني، مما يزيد من اهتمام الموظفين ومشاركتهم في استبيانات ذات صلة بالموضوع.

- **توزيع الإجابات حسب الجنس:**

في تحليل توزيع الأجوبة حسب الجنس، تبين تقارب كبير بين النسب الإجمالية لإجابات الذكور والإناث، حيث شكلت أجوبة الإناث نسبة 50.44%، في حين بلغت نسبة أجوبة الذكور 49.56 %. هذا التوزيع المتقارب يعكس تنوع العينة، ويساهم في الحصول على رؤية شاملة حول الوعي الأمن السيبراني بين الجنسين

- إناث: **50.44 % (114 صوت)**
- ذكور: **49.56 % (112 صوت)**

الرسم البياني:



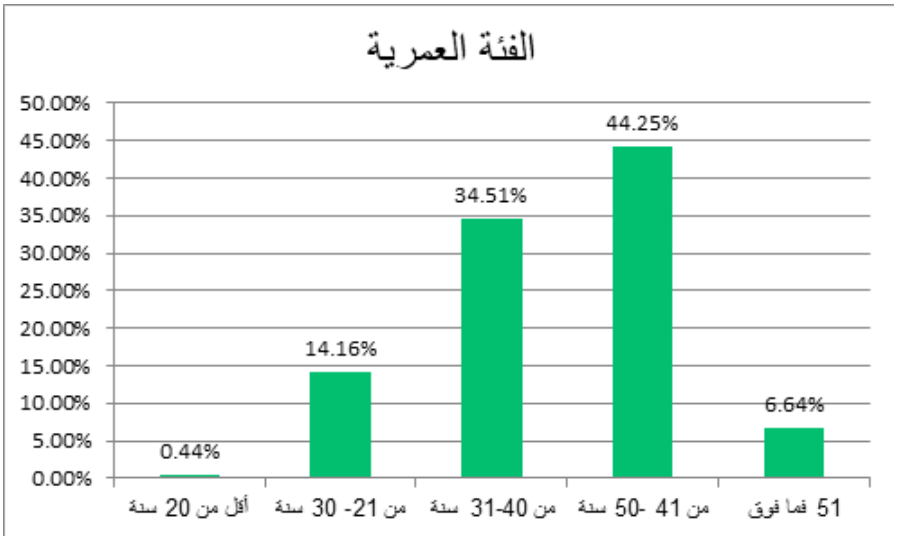
- **التحليل:**
- لا يوجد تقريبا بين الإناث والذكور بين المجيبين، مما يشير إلى توزيع متوازن بين الجنسين للمشاركين في الاستبيان.
- **توزيع الإجابات حسب الفئة العمرية:**

النتائج:

- أقل من 20 سنة 0.44 % (1 صوت)
- من 21- 30 سنة 14.16 % (32 صوت)
- من 31-40 سنة 34.51 % (78 صوت)
- من 41 -50 سنة 44.25 % (100 صوت)

- 51 فما فوق 6.64 % (15 صوت)

الرسم البياني:



- **التحليل:**

النتائج تُظهر أن الغالبية العظمى من المشاركين في الاستبيان تتركز في الفئات العمرية الوسطى، خصوصاً بين 41-50 سنة و31-40 سنة، مع نسب تبلغ 44.25 % و34.51 % على التوالي. هذا يشير إلى أن الاستبيان كان له صدى أكبر بين الأشخاص في منتصف العمر

الفئات العمرية الأصغر (أقل من 20 سنة) والأكبر سناً (51 فما فوق) ممثلة بنسب أقل بكثير، حيث تبلغ 0.44 % و6.64 % على التوالي. هذا يمكن أن يعكس التوزيع العمري العادي للموظفين، أو اهتماما محدودا بالاستبيان بين هذه الفئات.

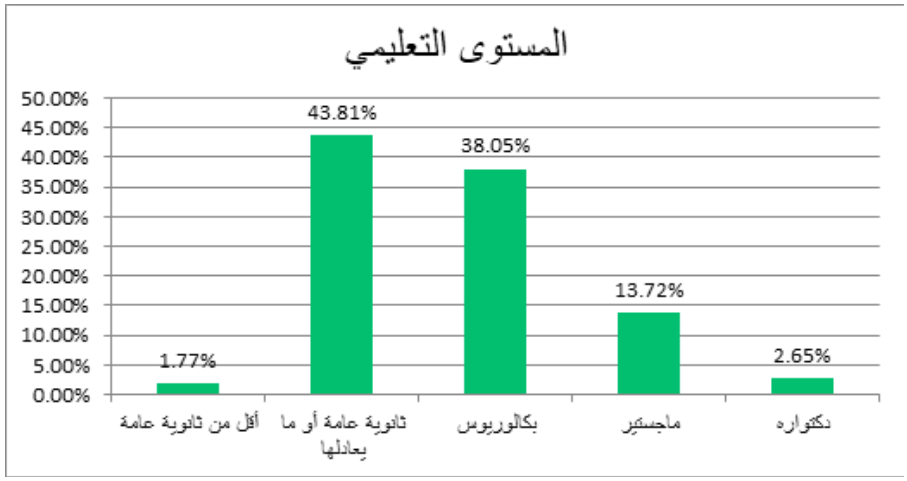
- **توزيع الإجابات حسب المستوى التعليمي:**

النتائج:

- أقل من ثانوية عامة 1.77 % (4 أصوات)

- ثانوية عامة أو ما يعادلها 43.81% (99 صوت)
- بكالوريوس 38.05 % (86 أصوت)
- ماجستير 13.72 % (31 صوت)
- دكتوراة 2.65 % (6 أصوات)

الرسم البياني:



- **التحليل:**

نتائج الاستبيان تكشف أن الغالبية العظمى من المشاركين هم من مستوى تعليمي يتراوح بشكل أساسي بين حملة شهادة الثانوية العامة والبكالوريوس. وهذه البيانات تشير إلى أن المشاركين يمتلكون نضجًا نسبيًا وتعليمًا جيدًا مع قاعدة معرفية متينة لتقديم إجابات مدروسة

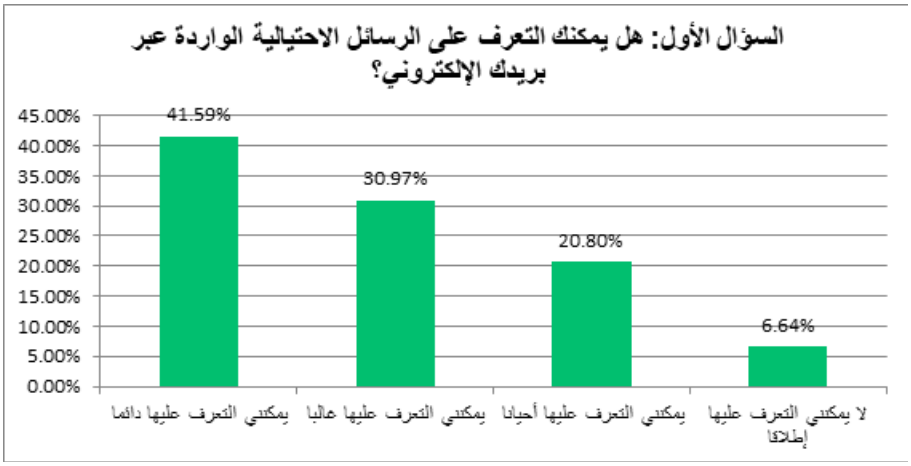
السؤال الأول: هل يمكنك التعرف على الرسائل الاحتيالية الواردة عبر بريدك الإلكتروني؟

النتائج:

- يمكنني التعرف عليها دائما 41.59 % (94 صوت)
- يمكنني التعرف عليها غالبا 30.97 % (70 صوت)

- يمكنني التعرف عليها أحيانا 20.80 % (47 صوت)
- لا يمكنني التعرف عليها إطلاقا 6.64 % (15 صوت)

الرسم البياني لنتائج السؤال الأول:



- **التحليل:**

المستجيبين (41.59 %) واثقون من قدرتهم على التعرف دائمًا على الرسائل الاحتيالية، مما يدل على ثقة عالٍ بقدراتهم في هذا المجال. نسبة كبيرة أخرى (30.97 %) تعتقد بقدرتهم على التعرف عليها غالبًا، بينما يمكن لـ20.80% التعرف عليها أحيانًا، مما يعكس وجود-نسبة من الثقة. أما 6.64 % من المجيبين يشيرون إلى عدم قدرتهم على التعرف على الرسائل الاحتيالية إطلاقًا

السؤال الثاني: تلقيتَ رسالة بريد إلكتروني من شخص لا تعرفه تتضمن ملفا مرفقا. ما هو الإجراء الصحيح؟

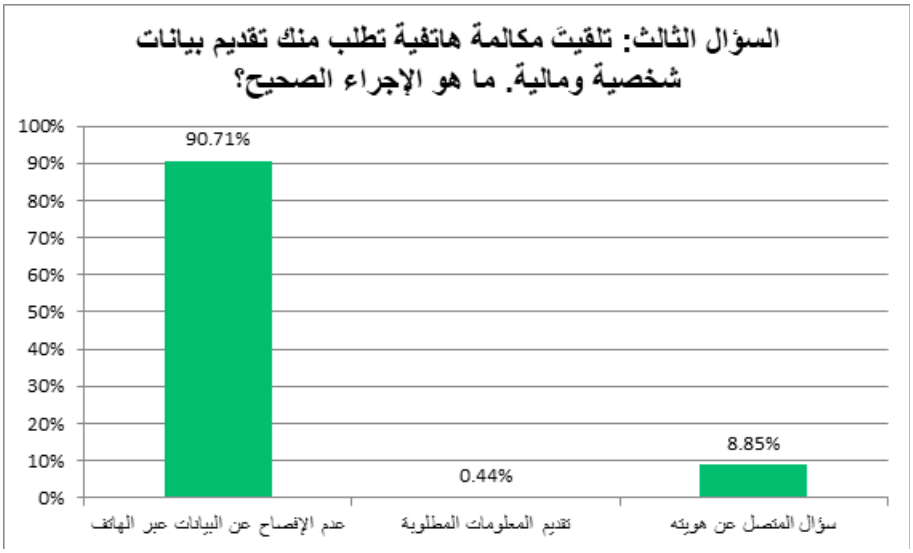
نظرا لوقوع خطأ فني في النسخة الالكترونية للاستبيان التي تم توزيعها، قام الباحث بإلغاء إجابات السؤال الثاني من الاستبيان.

السؤال الثالث: تلقيتَ مكالمة هاتفية تطلب منك تقديم بيانات شخصية ومالية. ما هو الإجراء الصحيح؟

النتائج:

- رفض تقديم البيانات عبر الهاتف: 90.71 % (205 صوت)
- تقديم المعلومات المطلوبة: 0.44 % (1 صوت)
- سؤال المتصل عن هويته: 8.85 % (20 صوت)

الرسم البياني لنتائج السؤال الثالث:



- **التحليل**

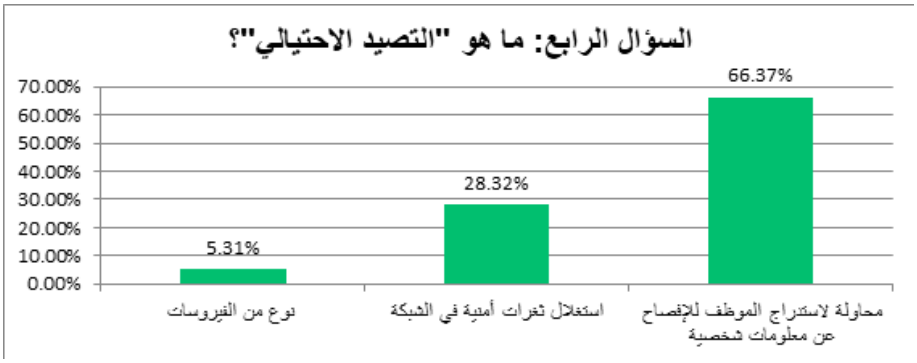
الإجابة للسؤال حول الإجراء الصحيح عند طلب تقديم بيانات شخصية ومالية عبر مكالمة هاتفية تظهر وعيًا كبيرًا بمخاطر الاحتيال والتصيد الاحتيالي، حيث أن غالبية المشاركين (90.71 %) اختاروا رفض تقديم البيانات عبر الهاتف، مما يدل على مستوى عالٍ من الحذر والوعي بأهمية حماية المعلومات الشخصية والمالية. استجابة ضئيلة (8.85 %) للتحقق من هوية المتصل تعكس نهجًا استقصائيًا، بينما أجاب شخص واحد بشكل خاطئ تماما.

السؤال الرابع: ما هو «التصيد الاحتيالي»؟

النتائج:

- نوع من الفيروسات5.31 % (12 صوت)
- استغلال ثغرات أمنية في الشبكة28.32 % (64 صوت)
- محاولة لاستدراج الموظف للإفصاح عن معلومات شخصية 66.37 % (150 صوت)

الرسم البياني لنتائج السؤال الرابع:



- **التحليل:**

النتائج تعكس فهم الغالبية العظمى من المجيبين (66.37 %) للتصيد الاحتيالي كمحاولة لاستدراج الموظف للإفصاح عن معلومات شخصية، ما يدل على إدراك صحيح لطبيعته، كتهديد سيبراني يستخدم الهندسة الاجتماعية. بينما يُظهِر الاعتقاد بأن التصيد الاحتيالي هو استغلال ثغرات أمنية (28.32 %) أو أنه نوع من الفيروسات (5.31%) بعض الالتباس لدى موظفي الهيئة حول مفاهيم الأمن السيبراني.

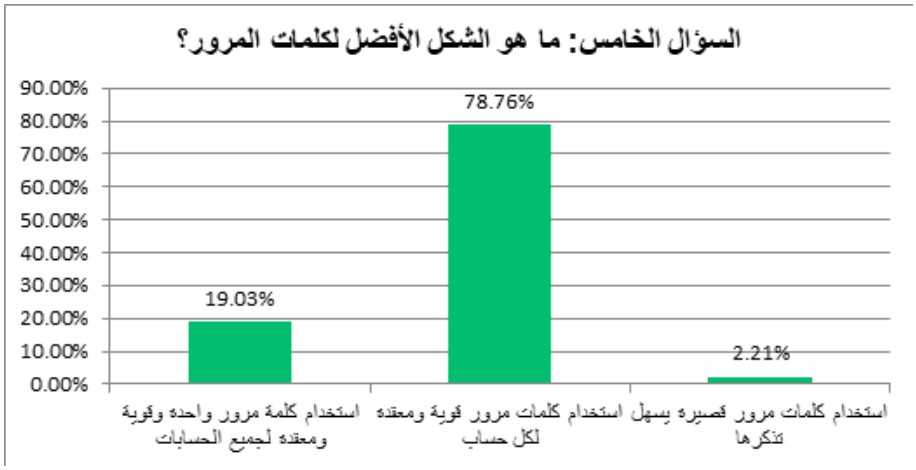
السؤال الخامس: ما هو الشكل الأفضل لكلمات المرور؟

النتائج:

- استخدام كلمة مرور واحدة وقوية ومعقدة لجميع الحسابات 19.03 % (43 صوت)
- استخدام كلمات مرور قوية ومعقدة لكل حساب 78.76 % (178 صوت)

- استخدام كلمات مرور قصيرة يسهل تذكرها 2.21 % (5 أصوات)

الرسم البياني لنتائج السؤال الخامس:



- **التحليل:**

من خلال الإجابات المقدمة في السؤال التاسع حول الشكل الأفضل لكلمات المرور، يُظهر المشاركون مستوى وعي متقدم بأهمية استخدام كلمات مرور قوية، حيث أن أغلبهم (78.76 %) يعتقدون أن استخدام كلمات مرور قوية ومعقدة ومختلفة لكل حساب هو الأسلوب الأمثل للحفاظ على الأمن الإلكتروني، ما يدل على تبنيهم لممارسات الأمان الموصي بها.

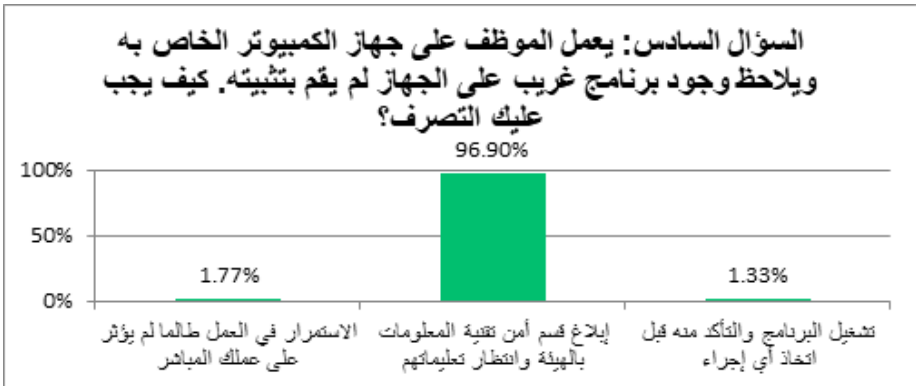
نسبة أقل (19.03 %) تفضل استخدام كلمة مرور واحدة قوية لجميع الحسابات، في حين أن النسبة البسيطة (2.21%) التي تفضل كلمات مرور قصيرة، مما يشير إلى وجود قصور في الفهم الأمني لديهم.

السؤال السادس: يعمل الموظف على جهاز الكمبيوتر الخاص به ويلاحظ وجود برنامج غريب على الجهاز لم يقم بتثبيته. كيف يجب عليك التصرف؟

النتائج:

- الاستمرار في العمل طالما لم يؤثر على عملك المباشر 1.77 % (4 أصوات)
- إبلاغ قسم أمن تقنية المعلومات بالهيئة وانتظار تعليماتهم 96.90 % (219 صوت)
- تشغيل البرنامج والتأكد منه قبل اتخاذ أي إجراء 1.33 % (3 أصوات)

الرسم البياني لنتائج السؤال السادس:



- **التحليل:**

الإجابات للسؤال العاشر تعكس درجة عالية من الوعي الأمني لدى الموظفين فيما يخص التعامل مع برامج غير متوقعة على أجهزة الكمبيوتر. فبنسبة غالبة (96.90 %)، اختار المستجيبون الإبلاغ عن البرنامج غير المعروف إلى قسم أمن تقنية المعلومات، مما يدل على اتباعهم للإجراءات القياسية والتقدير الجيد للإجراءات الاحترازية اللازمة في حالة الاشتباه بوجود برمجيات ضارة.

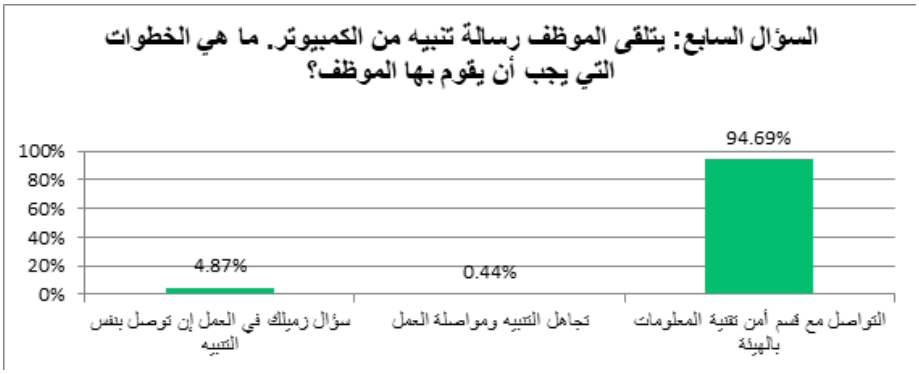
السؤال السابع: يتلقى الموظف رسالة تنبيه من الكمبيوتر. ما هي الخطوات التي يجب أن يقوم بها الموظف؟

النتائج:

- سؤال زميلك في العمل إن توصل بنفس التنبيه 4.87 % (11 صوت)

- تجاهل التنبيه ومواصلة العمل 0.44 % (1 صوت)
- التواصل مع قسم أمن تقنية المعلومات بالهيئة 94.69 % (214 صوت)

الرسم البياني لنتائج السؤال السابع:



- **التحليل:**

تشير النتائج المتعلقة بالسؤال السابع حول الخطوات التي يجب أن يتخذها الموظف عند تلقي رسالة تنبيه من الكمبيوتر إلى وجود وعي مرتفع بأهمية الأجوبة الفورية والمناسبة للتنبيهات الأمنية ضمن بيئة العمل. نسبة كبيرة من المجيبين (94.69 %) اختارت التواصل مع قسم أمن تقنية المعلومات بالهيئة، مما يدل على فهم جيد لأفضل الممارسات في التعامل مع الإشارات الأمنية. بالمقابل، نسبة ضئيلة اختارت سؤال زميل في العمل (4.87 %)، ما يعكس رغبة محدودة في التحقق المشترك من الإشارات الأمنية قبل اتخاذ الإجراءات. إجابة واحدة فقط اختارت تجاهل التنبيه ومواصلة العمل

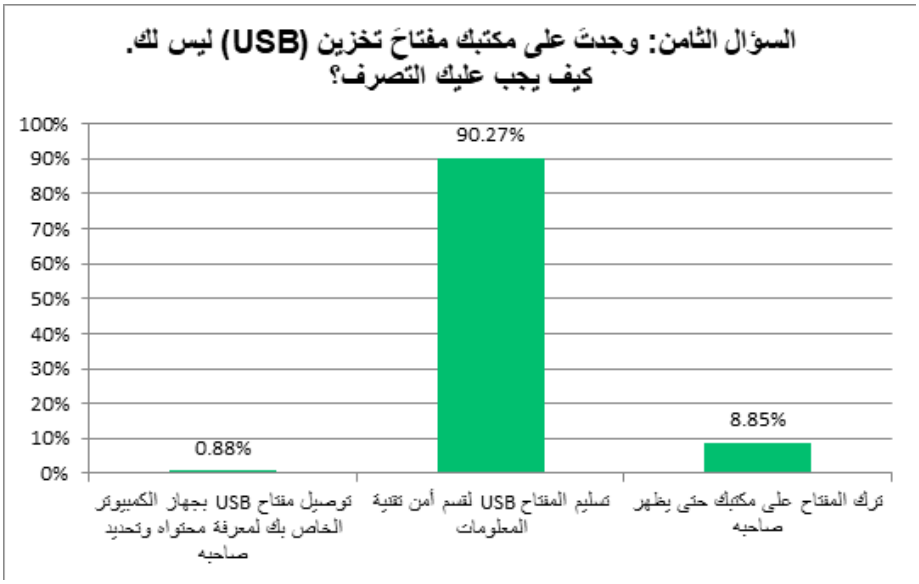
وتشير هذه النتائج إلى وعي شبه عام من طرق الموظفين حول خطورة تجاهل التنبيهات الأمنية، وحول الدور الذي يجب أن يلعبونه للتبليغ عن الأشياء المريبة إلى الجهات المعنية في الهيئة

السؤال الثامن: وجدتَ على مكتبك مفتاحَ تخزين (USB) ليس لك. كيف يجب عليك التصرف؟

النتائج:

- توصيل مفتاح USB بجهاز الكمبيوتر الخاص بك لمعرفة محتواه وتحديد صاحبه (0.88 %)2 صوتين
- تسليم المفتاح USB لقسم أمن تقنية المعلومات % 90.27) 204 صوتين)
- ترك المفتاح على مكتبك حتى يظهر صاحبه 8.85%)20 صوت)

الرسم البياني لنتائج السؤال الثامن:



- **التحليل:**

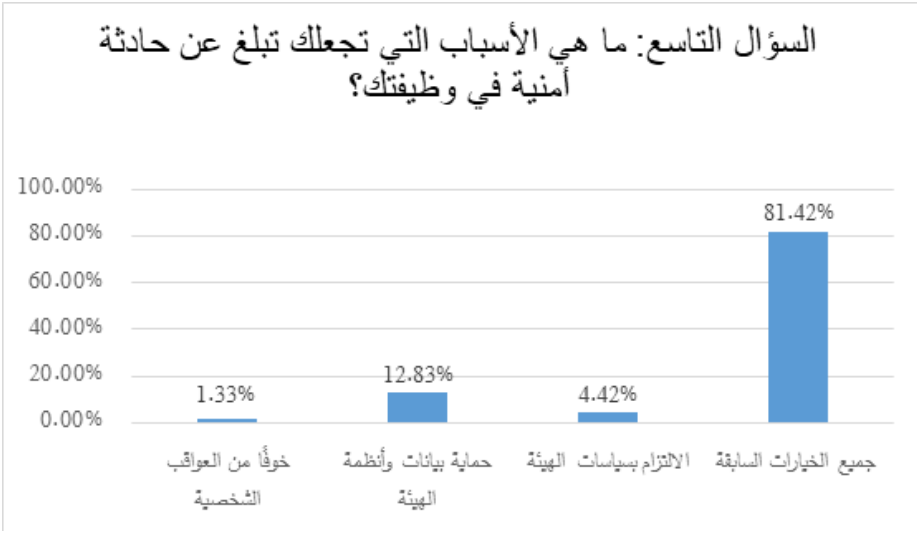
وفقًا للإجابات المقدمة للسؤال الثاني عشر، فإن الأغلبية العظمى من الموظفين (90.27 %) لديهم وعي أمني مرتفع ويتبعون أفضل الممارسات بتسليم مفتاح USB مجهول إلى قسم أمن تقنية المعلومات، مما يدل على تقديرهم للمخاطر الأمنية المحتملة من استخدام أجهزة غير معروفة. من ناحية أخرى، هناك نسبة صغيرة ممن يفضلون ترك المفتاح على المكتب، أو حتى توصيله بجهاز الكمبيوتر، ما يدل على فجوة معرفية

السؤال التاسع: ما هي الأسباب التي تجعلك تبلغ عن حادثة أمنية في وظيفتك؟

النتائج:

- خوفًا من العواقب الشخصية (1.33 %) 3 أصوات
- حماية بيانات وأنظمة الهيئة (12.83 %) 29 صوت
- الالتزام بسياسات الهيئة(4.42 %) 10 أصوات
- جميع الخيارات السابقة (81.42 %) 184 صوت

الرسم البياني لنتائج السؤال التاسع:



- **التحليل:**

النتائج المعروضة تدل على أن الدافع الرئيسي وراء الإبلاغ عن حوادث أمنية لدى الغالبية العظمى من الموظفين (81.42 %) هو مزيج من الالتزام بسياسات الهيئة، الخوف من العواقب الشخصية، وحماية بيانات وأنظمة الهيئة، وهي الإجابة الصحيحة. هذا يشير إلى وعي الموظفين بالمسؤولية المهنية والشخصية تجاه الأمن السيبراني. النسب الأقل للموظفين الذين اختاروا أسبابًا محددة يُظهرون تقديرًا لجوانب معينة من

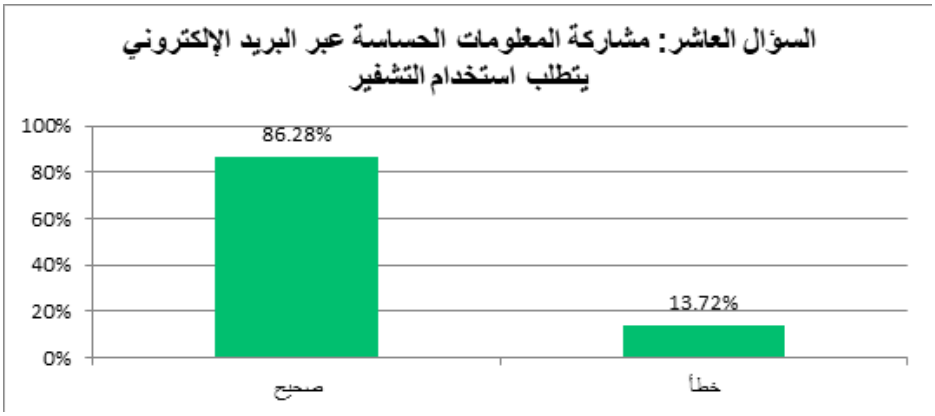
الأمن السيبراني.

السؤال العاشر: مشاركة المعلومات الحساسة عبر البريد الإلكتروني يتطلب استخدام التشفير

النتائج:

- صحيح 86.28 % (195 صوت)
- خطأ 13.72 % (31 صوت)

الرسم البياني لنتائج السؤال العاشر:



- **التحليل:**

البيانات المقدمة تظهر أن غالبية المشاركين (86.28 %) يتفقون على أن مشاركة المعلومات الحساسة عبر البريد الإلكتروني يجب أن تتم باستخدام التشفير، مما يعكس فهمًا قويًا لمبادئ أمن المعلومات. ومع ذلك، هناك نسبة (13.72 %) تعتقد خلاف ذلك، وذلك خطأ.

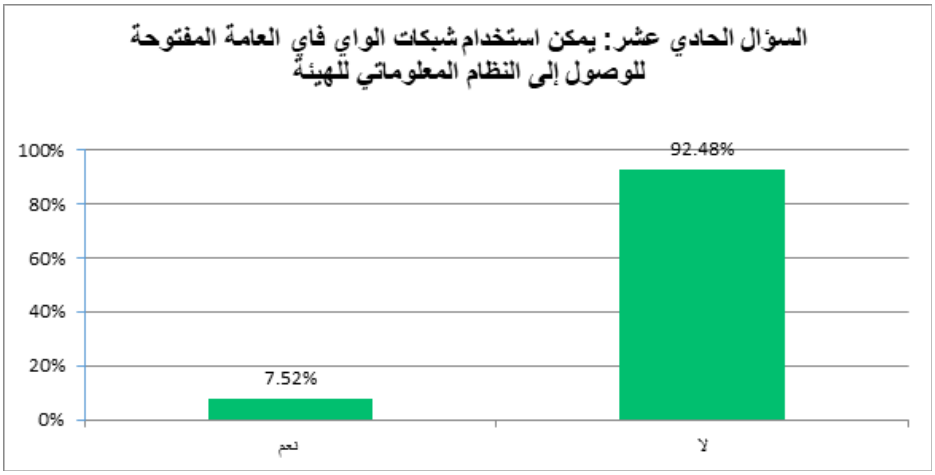
السؤال الحادي عشر: يمكن استخدام شبكات الواي فاي العامة المفتوحة للوصول إلى النظام المعلوماتي للهيئة

النتائج:

- نعم: 7.52 % (17 صوت)

- لا: 92.48 % (209 صوت)

الرسم البياني لنتائج السؤال الحادي عشر:



- **التحليل:**

الواضح من الأجوبة بأن الغالبية العظمى من المشاركين (92.48%) يؤيدون أن استخدام شبكات الواي فاي العامة المفتوحة للوصول إلى نظام معلومات الهيئة يشكل خطرًا أمنيًا ولا يجب أن يُمارس. هذا يعكس مستوى عالي من الوعي بالمخاطر الأمنية المرتبطة بشبكات الواي فاي العامة. من ناحية أخرى، هناك نسبة صغيرة (7.52 %) تعتقد أنه من المقبول استخدام هذه الشبكات، وهذا خطأ

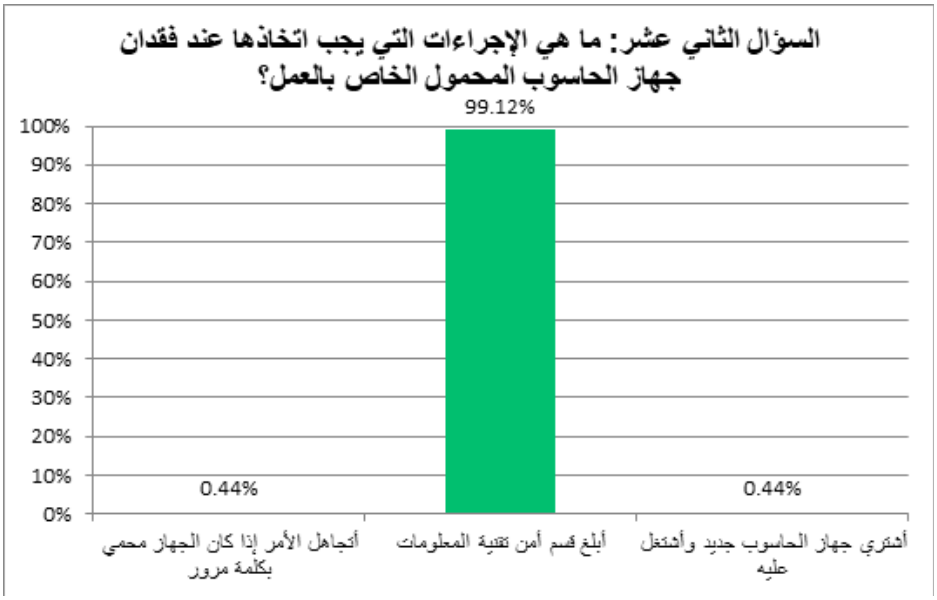
السؤال الثاني عشر: ما هي الإجراءات التي يجب اتخاذها عند فقدان جهاز الحاسوب المحمول الخاص بالعمل؟

النتائج:

- أتجاهل الأمر إذا كان الجهاز محمي بكلمة مرور:(1%0.44) صوت
- أبلغ قسم أمن تقنية المعلومات: (99.12 %) 224 صوت

- أشتري جهاز الحاسوب جديد وأشتغل عليه: (0.44 %)1 صوت

الرسم البياني لنتائج السؤال الثاني عشر:



- **التحليل:**

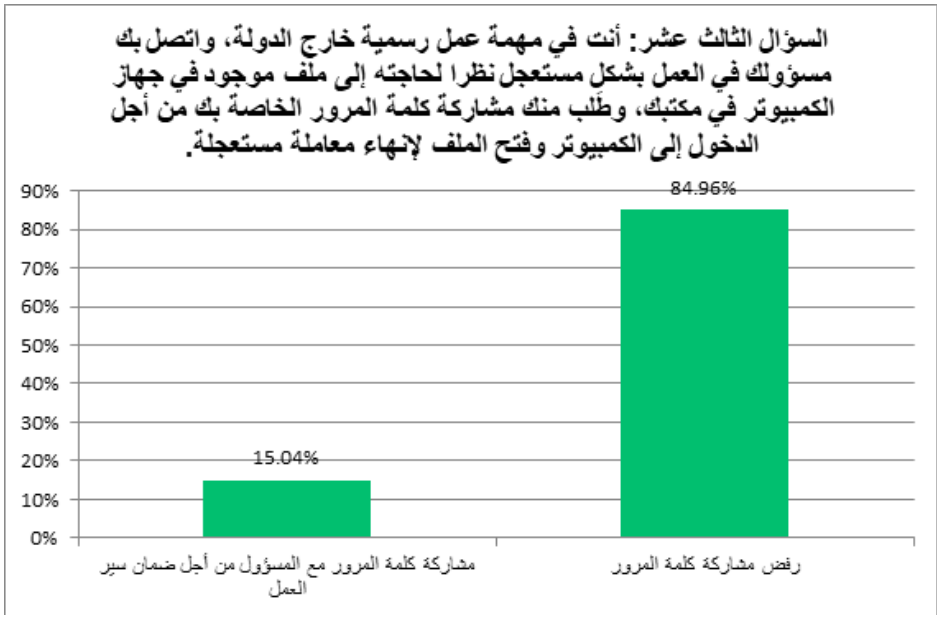
النتائج المقدمة توضح بوضوح أن الأغلبية الساحقة من المشاركين (99.12 %) تدرك الإجراء الصحيح عند فقدان جهاز الحاسوب المحمول الخاص بالعمل، وهو الإبلاغ الفوري لقسم أمن تقنية المعلومات. هذا يعكس وعيًا أمنيًا ممتازًا وفهمًا جيدًا للبروتوكولات الأمنية الخاصة بالأصول التقنية للهيئة.

السؤال الثالث عشر: أنت في مهمة عمل رسمية خارج الدولة، واتصل بك رئيسك في العمل بصفة عاجلة، نظرا لحاجته إلى ملف موجود في جهاز الكمبيوتر في مكتبك، وطَلب منك مشاركة كلمة المرور الخاصة بك للدخول على الكمبيوتر، وفتح الملف لإنهاء معاملة مستعجلة. ما هو التصرف الصحيح؟

النتائج:

- مشاركة كلمة المرور مع المسؤول من أجل ضمان سير العمل: 15.04 % (34 صوت)
- رفض مشاركة كلمة المرور: 84.96 % (192 صوت)

الرسم البياني لنتائج السؤال الثالث عشر:



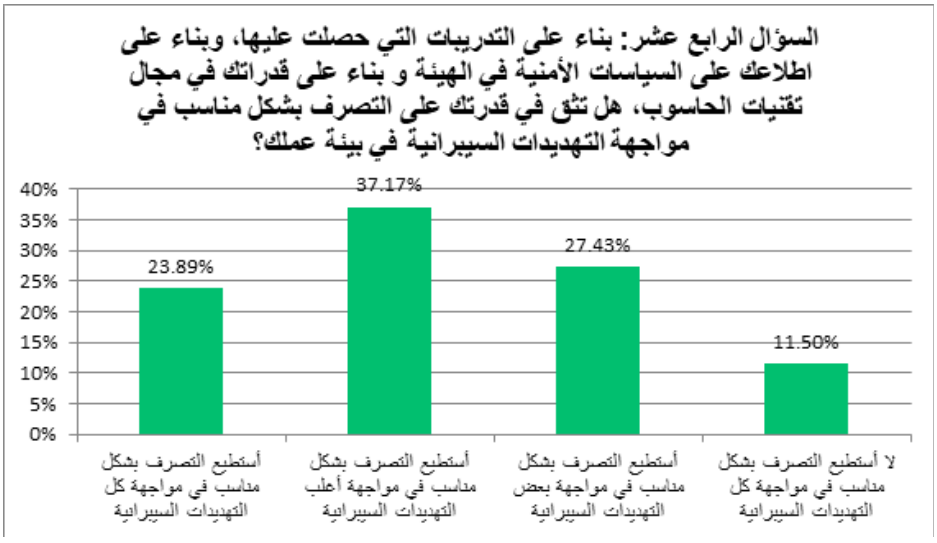
- **التحليل:**

تُظهر الإجابات للسؤال الثالث عشر تفضيلًا واضحًا لخيار رفض مشاركة كلمة المرور من قِبل الأغلبية (84.96 %) حتى في ظل الظروف المستعجلة. هذا يدل على وعي أمني قوي، وتقدير للسياسات التي تحظر مشاركة البيانات الحساسة، مثل: كلمات المرور. ومع ذلك، هناك نسبة، لا يُستهان بها (15.04%)، مستعدة لمشاركة كلمة المرور الخاصة بالموظف لضمان استمرارية العمل

السؤال الرابع عشر: بناء على التدريبات التي حصلت عليها، وبناء على اطلاعك على السياسات الأمنية في الهيئة وبناء على قدراتك في مجال تقنيات الحاسوب، هل تثق في قدرتك على التصرف بشكل مناسب في مواجهة التهديدات السيبرانية في بيئة عملك؟

النتائج:

- أستطيع التصرف بشكل مناسب في مواجهة كل التهديدات السيبرانية 23.89 % (54صوت)
- أستطيع التصرف بشكل مناسب في مواجهة أغلب التهديدات السيبرانية 37.17 % (84 صوت)
- أستطيع التصرف بشكل مناسب في مواجهة بعض التهديدات السيبرانية (27.43 % 62 صوت
- لا أستطيع التصرف بشكل مناسب في مواجهة كل التهديدات السيبرانية (11.50 % 26 صوت
- **الرسم البياني لنتائج السؤال الرابع عشر:**



- **التحليل:**

الاستطلاع يشير إلى أن ثقة العاملين في قدرتهم على التصرف بشكل مناسب ضد التهديدات السيبرانية متفاوتة. نسبة معتبرة (23.89 %) واثقة من القدرة على التعامل مع كل التهديدات، بينما يشعر (37.17 %) بالقدرة على التعامل مع أغلب التهديدات، و(27.43 %) يشعرون بالقدرة على التعامل مع بعضها. بينما ترى فئة نسبتها (11.50 %)

بأنها غير قادرة على مواجهة التهديدات السيبرانية بشكل كافٍ

ويعتقد الباحث أن هذا السؤال ونتائجه مهمة لفهم المستوى الحالي لوعي موظفي الهيئة بالأمن السيبراني. فوجود نسبة عالية من الموظفين (38.93 %) لا تثق في قدرتها على التصرف بشكل مناسب في مواجهة التهديدات السيبرانية، أو أنها تثق في قدرتها في التصرف في بعض الحالات فقط، هي مؤشر مهم. وقد تعكس هذه الأرقام نقصا في التدريب أو الوعي في مجال الأمن السيبراني، أو هما معًا، بين موظفي الهيئة.

وتتفق هذه النتيجة مع ما توصل إليه الشهراني (2020)، فأكد على أهمية التوعية بالأمن السيبراني تظهر كدرع وقاية لحماية الأفراد والمؤسسات من المخاطر السيبرانية، وتأمين المعلومات التي قد تكون عرضة للخطر، والاختراق والاستيلاء، خاصةً مع انتشار استخدام الإنترنت، ونقص الوعي الرقمي، خاصةً بين الأطفال والمراهقين. ويتعين تعزيز الممارسات الصحيحة، وفحص الوسائط الرقمية، والقدرات التي تقيس مدى سلامة المحتوى، ومختلف التفاعلات عبر الإنترنت. ويبرز هذا الأمر أهمية زيادة الوعي حول أهمية الأمن السيبراني بين الأفراد، وتوفير التدريب حول الأساليب والإجراءات الأمنية.

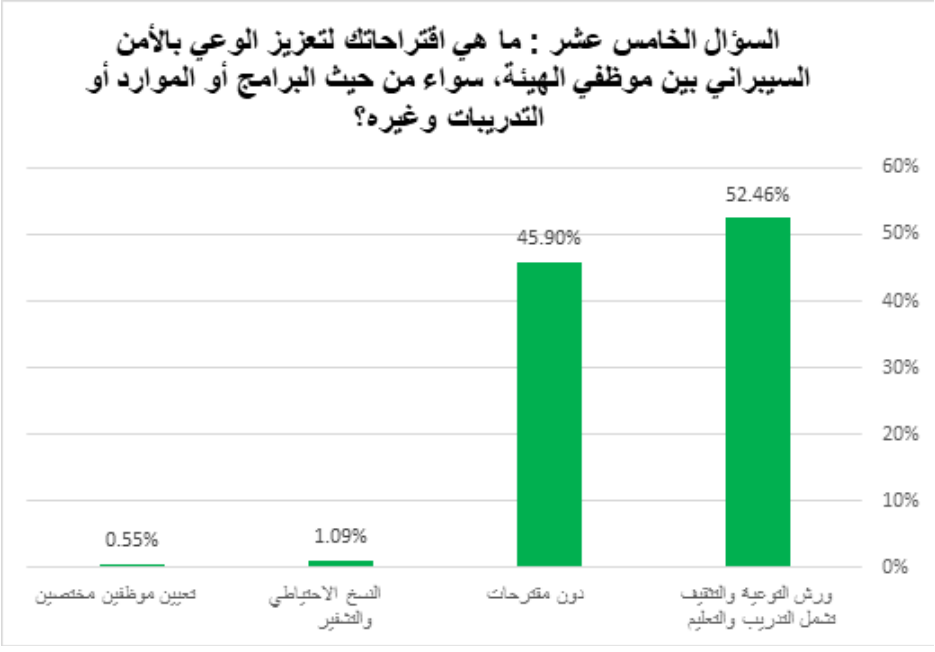
كما تتفق مع ما أشارت إليه وكالة الإتحاد الأوروبي للأمن السيبراني إلى أن حوالي 77 % من خروقات بيانات الشركات تكون بسبب استغلال نقاط الضعف البشرية (ENISA,2019). كما تبين سابقًا أن أكثر من نصف جميع انتهاكات أمن المعلومات تتعلق بضعف امتثال الموظفين لأمن المعلومات، وهو ما يؤكد على أهمية تعزيز قدرة الموظفين على التصرف بشكل مناسب في مواجهة التهديدات السيبرانية في بيئة عملهم.

السؤال الخامس عشر: ما هي اقتراحاتك لتعزيز الوعي بالأمن السيبراني بين موظفي الهيئة، سواء من حيث البرامج أو الموارد أو التدريبات وغيره؟

النتائج:

- ورش التوعية والتثقيف تشمل التدريب والتعليم: 52.46 %
- بدون مقترحات: 45.9 %
- النسخ الاحتياطي والتشفير: 1.09 %
- تعيين موظفين مختصين: 0.55 %

الرسم البياني لنتائج السؤال الخامس عشر:



- **التحليل:**

تحليل الإجابات المقدمة للسؤال الأخير، والذي استهدف جمع اقتراحات الموظفين حول تحسين الوعي بالأمن السيبراني، يكشف عن توزيع ملحوظ للاهتمامات بين المشاركين. وتظهر النتائج أن فئة «ورش التوعية والتثقيف تشمل التدريب والتعليم» قد حصلت على أكبر نسبة من الاهتمام بـ 52.46 %، مما يدل على إدراك كبير بين الموظفين لأهمية هذه الأنشطة في تعزيز الوعي الأمني.

ومن خلال ما سبق فقد أشارت الإجابات إلى أهمية ورش التوعية والتثقيف تشمل التدريب والتعليم، وتتفق هذه النتيجة مع ما توصل إليه(Khando,2021) وآخرون، فالعامل الرئيسي في تجنب مخاطر أمن المعلومات هو مستوى وعي الفرد بالأمن السيبراني، والذي يمكن وصفه بفعالية كمنخفض، أو متوسط، أو عال، وتشمل السلوكيات ذات المستوى المنخفض عدم الانتباه أو إهمال تنبيهات الأمن التي يتم توفيرها في معظم الحالات تلقائيًا من قبل التطبيقات، كالولوج إلى شبكات الواي فاي العامة والمجانية، باستخدام أجهزة الهواتف الذكية، والكمبيوترات الشخصية. ويمكن أن يتميز المستوى المتوسط بالإهمال الذي يظهر في تشغيل التكنولوجيا بطريقة غير صحيحة. وأخيرًا يتضمن المستوى العالي معرفة بالتهديدات السيبرانية، واتخاذ إجراءات فعالة للوقاية منها

كما تتفق مع (Al-Alawi,2020) وآخرون اللذين أشاروا إلى إن فإن أصول المنظمة وعواملها هم العاملون فيها. ويمكن أن يكون هذا أيضًا الحلقة الأضعف في حماية البيانات، خاصة عندما يلعب التنقل وإمكانية الوصول دورًا هائلاً في تحسين الكفاءة.

كما تختلف هذه النتيجة مع(Nachin, N (2019 والتي قامت بدراسة زيادة الوعي بالأمن السيبراني مع أكثر من 4500 موظف من 20 منظمة، ثم وجدوا أن النهج القائم على المحاكاة يمكن أن يساعد في تحسين أو زيادة مستوى الوعي بالأمن السيبراني، وهو أكثر عملية من النهج الذي يقوم على التعليم. ومع ذلك ينبغي استخدام كلا النهجين والجمع بينهما، فهذه الدراسة تؤكد أن المحاكاة أفضل من التعليم

على الجانب الآخر، الفئة التي لم تساهم بأي اقتراحات تشكل 45.9 % من الإجابات، مما يلقي الضوء على وجود نسبة لا يستهان بها من المشاركين الذين إما يشعرون بالرضا عن الإجراءات القائمة، أو لم يتمكنوا من تحديد مقترحات يرون أنها تستحق الاهتمام لتحسين الوعي الأمني

الاهتمام بـ ‹النسخ الاحتياطي والتشفير› و‹تعيين موظفين مختصين› كان أقل نسبيًا،

بـ 1.09 % و0.55 % على التوالي، مما يشير إلى أن هذه الجوانب ربما تُعتبر أقل أولوية أو فهمًا بين المشاركين في سياق التوعية الأمنية

وتتفق هذه النتيجة مع ما أشار إليه الدليل الإرشادي لجوانب الأمن السيبراني للعمل عن بعد (2021) أضاف بعض الممارسات لتحصين أجهزة الموظفين من التهديدات السيبرانية، وذلك على النحو الآتي

- **استخدام أنظمة وبرامج أصلية:** تجنب استخدام أنظمة تشغيل أو برامج غير أصلية، حيث قد تحتوي على مكونات غير آمنة، وتشكل مخاطر لا يمكن إصلاحها بسهولة. يفضل استخدام نسخ أصلية من نظام التشغيل لتعزيز أمان جهازك.
- **تحديث البرامج ونظام التشغيل:** بمجرد التأكد من أن جميع برامجك أصلية، قم بتنزيل جميع التحديثات الدورية لنظام التشغيل والبرامج الأخرى لسد الثغرات الأمنية الجديدة. ويفضل السماح بتحديثات النظام بشكل تلقائي إذا كان جهازك جزءًا من بيئة عمل.
- **تفعيل مكافحة الفيروسات والحماية:** قم بتفعيل برامج مكافحة الفيروسات والحماية إذا كانت متوفرة. في حال عدم توفرها، احصل على برنامج حماية شامل يتضمن جدارًا ناريًا ومكافحة فيروسات قوية، وتأكد من تحديثه بانتظام لمواكبة أحدث التهديدات.

بالمجمل، تعكس النتائج تقدير الموظفين للأنشطة التي تركز على التوعية والتعليم كعناصر حيوية في تعزيز الوعي الأمني، مع وجود تباين في الاهتمام بالجوانب الفنية والإدارية المحددة. بشكل عام، تسلط هذه النتائج الضوء على الاعتراف بأهمية التوعية والتدريب في مجال الأمن السيبراني بين موظفي الهيئة، وتؤكد على الدور الحيوي الذي يمكن أن تلعبه هذه الأنشطة في تعزيز الوعي الأمني وبناء ثقافة أمنية قوية داخل الهيئة.

- **مؤشر وعي الموظفين بالأمن السيبراني**

مقدمة

في ظل التطورات التكنولوجية المتسارعة والاعتماد المتزايد على الأنظمة الرقمية، يبرز الأمن السيبراني كأحد أهم الركائز لحماية المعلومات والبيانات الحساسة. إدراكاً لهذه الأهمية، تم خلال هذا البحث، تطوير مؤشر وعي الموظفين بالأمن السيبراني وذلك لقياس مستوى الوعي بشكل عددي باستخدام سُلم موحد

أسباب وضع مؤشر وعي الموظفين بالأمن السيبراني:

إن وضع المؤشر جاء استجابةً للحاجة إلى فهم دقيق وموضوعي لمستوى الوعي الأمني لدى الموظفين. حيث أن المؤشر العددي يعطي صورة واضحة ومباشرة لمستوى الوعي بالأمن السيبراني، مما يساعد على فهم واضح للوضع، خاصة على مستوى صناعة القرارات في الهيئة. كما أن وجود مؤشر عددي شامل يُمَكن من مقارنة تغيرات الوعي بالأمن السيبراني زمنيا (القياس والمقارنة بين فترتين) ومكانيا (القياس والمقارنة بين جهتين).

سلم الدرجات الذي تم اختياره لكل سؤال من الاستبيان:

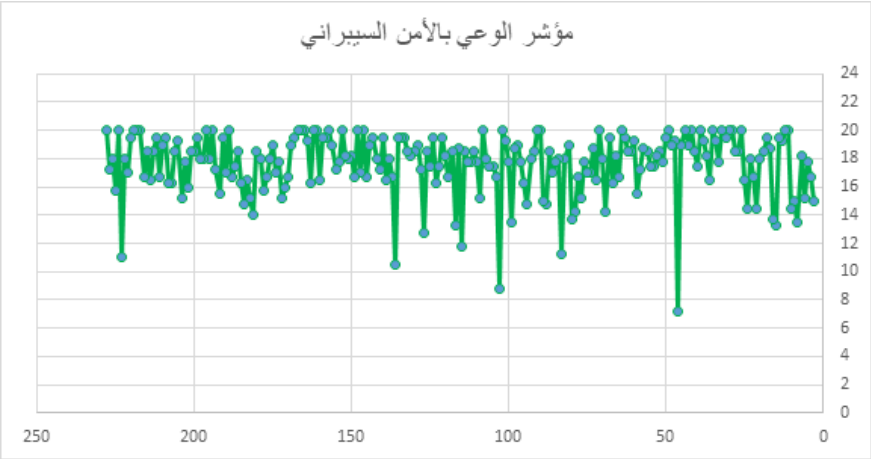
بناءً على أسئلة الاستبيان، تم اعتماد سُلَّم معياري مجموعه 20 نقطة يراعي أهمية وحساسية كل سؤال، وذلك بغية قياس مدى وعي الموظفين بكل أبعاد الأمن السيبراني بطريقة موضوعية. وبالتالي، تحمل بعض الأسئلة وزناً أكبر في قيمة المؤشر بناءً على مدى تأثيرها المحتمل على حماية أصول وممتلكات الهيئة الرقمية. لذلك، تم منح درجات أعلى للإجابات التي تعبر عن مستويات عالية من الوعي والفهم للتهديدات الأكثر حساسية وأهمية. ومن خلال هذه الطريقة، يأخذ مؤشر الوعي بالأمن السيبراني في الاعتبار التفاوت في الأهمية النسبية لكل سؤال، مما يعزز من قوة المؤشر. للمزيد من التفاصيل حول توزيع الدرجات وتصنيف الأسئلة بحسب أهميتها، يرجى الرجوع إلى سلم المؤشر الموجود في الملحق

نتائج مؤشر الوعي بالأمن السيبراني

التحليل الإحصائي الوصفي:

الوسط الحسابي	**17.68**
الخطأ المعياري	**0.14**
الوسيط	**18**
المنوال	**20**
الانحراف المعياري	**2.13**
القيمة الأدنى	**7.25**
القيمة الأقصى	**20**
عدد الإجابات	**226**

أما قيم مؤشر الوعي بالأمن السيبراني، فجاءت موزعة كالتالي:



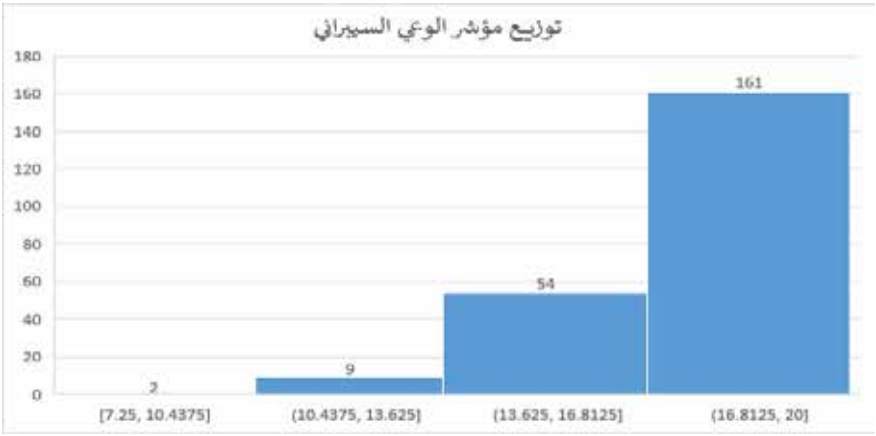
تحليل النتائج

تُظهر البيانات المُقدَّمة أن هناك 226 إجابة في مجموع البيانات. يبلغ متوسط مؤشر الوعي السيبراني حوالي 17.68، مع انحراف معياري يبلغ حوالي 2.13. الحد الأدنى للمؤشر هو 7.25 والحد الأقصى هو 20. قيمة الوسيط هي 18.0، مما يشير إلى أن

نصف درجات المؤشر أقل من 18، والنصف الآخر أعلى من 18، في حين أن المنوال عند القيمة 20 يُظهر القيمة الأكثر تكرارًا في البيانات

ويدل متوسط المؤشر (17.68)، على قيمة عالية للوعي بالأمن السيبراني بين موظفي الهيئة. ومن ناحية أخرى، تعطي القيمتان المئويتان 25 و75 (16.75 و19.25 على التوالي) فكرة عن انتشار البيانات، حيث تقع 50 % من الدرجات بين 16.75 و19.25.

وتتفق هذه النتيجة جزئيًا مع ما توصلت إليه(2019) Ikhsan, & Ramli قاموا بقياس مستوى الوعي بأمن المعلومات لدى الموظفين الحكوميين من خلال دراسات حالة مع 736 مستجيبًا في إحدى المنظمات في إندونيسيا باستخدام نهج السلوك والمعرفة عبر نموذج استبيان في محاكاة التصيد الاحتيالي. ووجدوا أن مستوى الوعي بأمن المعلومات لدى الموظفين أو العاملين بلغ3.79% تقريباً، وهذه النتيجة لن تصل إلى مستوى «جيد»



يوضح هذا الرسم البياني توزيع درجات المؤشر على أربع فئات رئيسية متساوية (من 7 إلى 10، من 10إلى 13، من 13 إلى 16، ومن 16 إلى 20). ويظهر أن التوزيع منحرف قليلاً نحو اليسار، مما يشير إلى أن معظم الدرجات تتركز في القيم الأعلى من 13. ومن الظاهر من الرسم البياني حصول (65 أو 28.67 %) من الإجابات على مؤشر وعي بالأمن السيبراني أقل من 16.8، وهو ما يعكس الحاجة إلى تطوير مستوى الوعي السيبراني لدى تلك الفئات من الموظفين.

الفصل الخامس

خلاصة البحث التداعيات والتوصيات:

- **مقدمة:**

في هذا الفصل الختامي من الدراسة، نعرض خلاصة النتائج التي توصلنا إليها، والتداعيات المترتبة لهذه النتائج على الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ، والتحديات التي واجهت البحث، ثم نختم بتقديم توصيات لتحسين الوعي السيبراني، وتعزيز الحماية ضد التهديدات السيبرانية في الهيئة والحكومة الاتحادية.

- **خلاصة النتائج:**

في هذه الفقرة، نقدم ملخصا شاملا لأبرز النقاط والاكتشافات التي تم التوصل إليها في كل من فصل الدراسات السابقة والدراسة الميدانية. سنركز بشكل خاص على تقديم الإجابات النهائية على الأسئلة البحثية الرئيسية، مستندين إلى ما توصلنا إليه من خلال تحليل البيانات المجمعة ومقارنتها بالأدبيات السابقة في هذا المجال. هذا التلخيص سيعكس جهودنا في فهم عميق لمستوى الوعي السيبراني بين موظفي الهيئة، وللأساليب الفعالة لتعزيز هذا الوعي، ولأفضل الطرق لتطوير برامج التوعية السيبرانية

وقد قام فصل الدراسات السابقة من هذه الدراسة بتحليل مفاهيم وأهمية الأمن السيبراني، مؤكدة على تعدد تعريفاته لكنها تتفق جميعاً على كونه يشمل إجراءات لحماية الأنظمة والشبكات والبرامج من الهجمات الرقمية. وسلطت الدراسة الضوء على أهمية الوعي بالأمن السيبراني في تقليل مخاطر الهجمات السيبرانية، وكيف أن نقص الوعي يمكن أن يؤدي إلى ضعف الحماية، وتعرض المعلومات للخطر. وقام فصل الدراسة السابقة بتحديد أنواع التهديدات السيبرانية، والتي تتنوع من الكوارث الطبيعية إلى الجرائم الإلكترونية والحروب السيبرانية، مع التأكيد على خطورة سرقة الهوية الرقمية والبيانات الخاصة. وتم التطرق إلى مفهوم الوعي بالأمن السيبراني، وأهميته

ومستويات الوعي المختلفة، وكيف أن العوامل مثل: العمر، الجنس، والخبرة يمكن أن تؤثر في هذا الوعي

بشكل عام، أكدت الدراسات السابقة على الحاجة الماسة لزيادة الوعي بالأمن السيبراني لتعزيز الحماية ضد التهديدات الرقمية المتزايدة، مشددةً على أهمية تطوير استراتيجيات شاملة تدمج بين التكنولوجيا والوعي البشري لضمان بيئة رقمية آمنة.

أما الدراسة الميدانية داخل الهيئة الاتحادية للهوية والجمارك وأمن المنافذ، فقد تم تنفيذها عبر استبيان وُزع على موظفي الهيئة، وتمكن من جمع 226 إجابة. وقد كشفت الدراسة الميدانية عن وعي متفاوت بالأمن السيبراني بين الموظفين، وأبرزت قدرة نسبة مهمة الموظفين على التعامل مع التهديدات السيبرانية بفعالية، وتمتعهم بثقة عالية في قدراتهم الأمنية السيبرانية، خصوصاً في التعرف على الإجراءات الاحتيالية والتصرف بمسؤولية عند مواجهة برمجيات أو أجهزة مجهولة. مع ذلك، أظهرت بعض الإجابات فجوات في الوعي قد تحتاج إلى تعزيز من خلال التدريب وورش العمل.

وتوصلت الدراسة إلى أن هناك حاجة ملحة لتعزيز الوعي بالأمن السيبراني عبر تطوير برامج توعية مستمرة ومتجددة تتناسب مع التحديات الأمنية المتطورة، وذلك لضمان بيئة عمل آمنة ومحمية من التهديدات السيبرانية

من خلال تحليل البيانات المجمعة ومقارنتها بالأدبيات السابقة، يظهر أن هناك قدراً معتبراً من الوعي بالأمن السيبراني بين موظفي الهيئة، وأن هناك فجوات تستدعي تعزيزاً من خلال برامج توعية سيبرانية مستمرة ومتجددة

بناءً على ذلك، يمكن لتطبيق الاستراتيجيات المقترحة في هذه الدراسة، والتي تشمل ورش العمل التثقيفية، والتدريبات الإلكترونية، وتحديث سياسات الأمن السيبراني، وتشجيع ثقافة الأمن السيبراني، أن يساعد في تعزيز الوعي بالأمن السيبراني وحماية الهيئة وموظفيها من التهديدات السيبرانية المتزايدة بفعالية أكبر

أما بالنسبة لأسئلة البحث، فقد تم التوصل إلى الأجوبة النهائية التالية:

السؤال الأول: ما هي التهديدات السيبرانية التي تواجه المستخدِم في الهيئة الاتحادية للهوية والجمارك وأمن المنافذ؟

الإجابة:

تتنوع التهديدات السيبرانية، وهي تشمل خطر الكوارث الطبيعية، والحروب السيبرانية، والجرائم الإلكترونية، بكل أنواعها، ومِن ضمنها الاختراق، وتخريب البنية التحتية، والولوج غير المرخص إلى البيانات، والتصيد الاحتيالي، وانتحال الهوية، وغيره

وتتفق هذه النتيجة مع ما توصل إليه بكراوي وبو بكر (2023) فقد قسم التهديدات السيبرانية إلى ستة أنواع:

- **التنصت:** يتمثل في التجسس على حوارات بين أفراد أو مستخدمين عبر الشبكة، باستخدام تقنيات مخصصة لذلك.
- **الانتحال:** يعني تنكير الشخص على أنه كيان صالح من خلال تزوير المعلومات للوصول إلى بيانات غير مسموح للشخص بالوصول إليها.
- **التلاعب:** إجراء تعديلات مضرة في المنتجات، مما قد يتسبب في تلف البيانات
- **تجاوز الصلاحيات:** يتعلق بمحاولة شخص ذو صلاحيات محددة للوصول إلى نظام بطرق غير مصرح بها.
- **التصيد الاحتيالي:** يستهدف العثور على بيانات سرية مثل: المعلومات الشخصية، وكلمات المرور بشكل مباشر.
- **الاحتيال المصرفي:** يستهدف نقاط الربط بين البنوك، ويستهدف التحويلات المالية، وحسابات المؤسسات المالية.

السؤال الثاني: ما هو المستوى الحالي للوعي بالأمن السيبراني لدى موظفي الهيئة

فيما يتعلق بالتهديدات السيبرانية، وتأثيرها المحتمل على الأصول والممتلكات؟

الإجابة:

المستوى الحالي للوعي بالأمن السيبراني لدى موظفي الهيئة يظهر أن هناك درجة عالية من الوعي بأهمية الأمن السيبراني، حيث يظهر ذلك من خلال متوسط مؤشر الوعي السيبراني الذي وصل إلى 17.68 (على 20)، وحصول 71 % من الإجابات على مؤشر وعي سيبراني أعلى من 16.81 %.

وتتفق هذه النتيجة جزئيًا مع ما توصلت إليه(Ikhsan, & Ramli (2019 قاموا بقياس مستوى الوعي بأمن المعلومات لدى الموظفين الحكوميين من خلال دراسات حالة مع 736 مستجيبًا في إحدى المنظمات في إندونيسيا باستخدام نهج السلوك والمعرفة عبر نموذج استبيان في محاكاة التصيد الاحتيالي. ووجدوا أن مستوى الوعي بأمن المعلومات لدى الموظفين أو العاملين بلغ 3.79%تقريباً، وهذه النتيجة لن تصل إلى مستوى «جيد».

السؤال الثالث: كيف يمكن تطوير برامج التوعية السيبرانية للموظفين لمواجهة التحديات السيبرانية الحالية والمستقبلية؟

الإجابة:

اقتراح تطوير برامج التوعية السيبرانية يجب أن يركز على عدة جوانب مهمة بناءً على التحليل الوصفي لنتائج الاستبيان

- **ورش عمل ودورات تدريبية مكثفة:** تشير النتائج إلى أهمية ورش العمل والتدريبات في رفع مستوى الوعي السيبراني، حيث أظهر 52.46% من المشاركين تفضيلهم لتعزيز الوعي بالأمن السيبراني من خلال ورش العمل التثقيفية والتدريبية. يجب تصميم هذه الورش لتغطية الجوانب الأساسية للأمن السيبراني وتحديثها بانتظام لتعكس التهديدات الجديدة.
- **التعليم الإلكتروني والموارد الذاتية:** إنشاء منصات تعليمية إلكترونية يمكن

للموظفين الوصول إليها في أي وقت لتعلم المزيد عن الأمن السيبراني وكيفية حماية أنفسهم والهيئة من التهديدات.

- **تحديث وتوسيع سياسات الأمن السيبراني:** يجب تحديث السياسات بشكل دوري لتعكس التطورات الأخيرة في مجال الأمن السيبراني، وتوزيعها بشكل واسع بين الموظفين، مع تدريبهم على هذه السياسات.
- **تشجيع ثقافة الأمن السيبراني:** من خلال تعزيز بيئة عمل تقدر الأمن السيبراني، وتشجع الموظفين على الإبلاغ عن أي أنشطة مشبوهة أو حوادث أمنية دون خوف من العواقب.
- **الاستجابة للحوادث وإدارة الأزمات:** تطوير برامج تدريبية تركز على كيفية الاستجابة للحوادث الأمنية وإدارة الأزمات بشكل فعال لضمان استعادة النظم بأسرع وقت ممكن.
- **التقييم المستمر والتحسين:** يجب تقييم فعالية برامج التوعية بشكل دوري، وتعديلها بناءً على التغذية الراجعة من الموظفين، وتطورات الأمن السيبراني.

من خلال تنفيذ هذه الاستراتيجيات والتركيز على التدريب المستمر والتوعية، يمكن للهيئة تحسين قدرتها على مواجهة التهديدات السيبرانية الحالية والمستقبلية بشكل أكثر فعالية

وتتفق هذه النتيجة مع ما توصل إليه هوساوي، ياسر (2020.) يجب أن يشمل برنامج توعية الأمن السيبراني بشكل جيد تدريبًا فعّالًا يتناسب مع أهداف المنظمة، مع التركيز على زيادة الوعي بالأمن السيبراني أثناء أداء الموظفين لواجباتهم وتحقيق التواصل التفاعلي بين جميع الفاعلين حيال أي قضية تتعلق بالأمن السيبراني. وقد تفشل برامج التوعية إذا لم تكن مصممة لتغيير سلوك الأفراد وكذلك إذا لم يمكن تحقيق تأثير إيجابي على المنظمة. ويُعَدُّ برنامج توعية الأمن السيبراني استثمارًا مؤسسيًا طويل المدى يُسهم في بناء ثقافة للأمن السيبراني في حال تقديم التدريب بشكل مستمر.

كما تتفق مع ما توصل إليه أما الشريف وآخرون (2023) فقد وضح اجراءات تعزيز الأمن السيبراني بأنها تتمثل في عدة نقاط:

- التأكد من سلامة وصحة البنية التحتية والحفاظ على تحديث جدران الحماية ومتابعتها بشكل منتظم.
- إعداد كلمات مرور قوية، وأن تكون غير معتادة، ولابد من تحتوي على حروف وأرقام وإشارات.
- القيام بتأهيل وتدريب المستخدمين على التعامل، واستخدام نظم المعلومات التي تتميز بقوتها وسريتها، وأيضا لابد من التوجيهات التي تعمل على توعيتهم وإدراكهم لضمان الأمن والسرية.
- توعية المستخدمين بالحذر من تحميل أي برامج مجهولة المصدر أو غير موثوقة وفحص البرمجيات قبل استخدمها بشكل فعلي.
- الإمكانية من تحديد الدخول وتأمين الوصول إلى النظام، وهنا لابد من وضع بعض الأسس والتعليمات للأشخاص المخولين لهم بدخول، والتعامل مع النظام بكل موثوقية.
- عمل نسخ احتياطية للبيانات والملفات من أجل ضمان الحصول عليها عند حدوث مشكلة ما، وهي تكون محددة مسبقا من أجل ضمان التوحيد في معايير الحفظ والحماية.

- **تداعيات البحث**

- سلطت الدراسة الضوء على أهمية الوعي بالأمن السيبراني وتحفيز الهيئة على تطوير استراتيجيات فعالة لتطوير هذا الوعي بين الموظفين.
- أظهرت الدراسة انكشاف الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ على بعض التهديدات السيبرانية بسبب نقص الوعي ببعض جوانب الأمن السيبراني لدى بعض الموظفين.

- حددت الدراسة احتياجات دقيقة للتدريب، وتطوير الوعي بالأمن السيبراني، لفائدة موظفي الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ.

- **حدود البحث**

واجهت الدراسة تحديات متعددة شملت محدودية الوصول إلى الموظفين لجمع البيانات، والتحديات التقنية في إدارة الاستبيان، وعدم كفاية وقت الباحث لإجراء التحليل الإحصائي الاستدلالي، حيث تم الاقتصار على التحليل الإحصائي الوصفي

- **توصيات البحث**

تبعا لنتائج هذا البحث، يمكن للباحث أن يُصدِر التوصيات التالية:

1. تصميم وتنفيذ برامج توعوية شاملة للموظفين حول كافة أنواع التهديدات السيبرانية.
2. توجيه برامج التوعية إلى جميع موظفي الهيئة، بغض النظر عن وظائفهم أو مستوياتهم.
3. استخدام مختلف الوسائط لتقديم محتوى التوعية، بما في ذلك: الدورات التدريبية، والندوات، وورش العمل، والمواد المطبوعة، والمواد الإلكترونية.
4. إشراك الإدارة العليا للهيئة في دعم وتعزيز ثقافة الأمن السيبراني.
5. تشجيع الموظفين على الإبلاغ عن أي حوادث أمنية مشبوهة.
6. تقديم مكافآت للموظفين الذين يُظهرون سلوكيات إيجابية في مجال الأمن السيبراني.
7. مشاركة نتائج هذه الدراسة مع الجهات ذات العلاقة، مثل مجلس الأمن السيبراني.
8. تطوير وتعميم تجربة قياس مؤشر الوعي بالأمن السيبراني بين الموظفين، سواء داخل الهيئة أو في الحكومة الاتحادية لدولة الإمارات العربية المتحدة.

- **خاتمة:**

إن تعزيز الوعي بالأمن السيبراني بين موظفي الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ مطلب ضروري في سياق التحديات السيبرانية اليومية. ومن خلال التوصيات المقترحة، يرجو أن يكون هذا البحث قد ساهم في تحسين قدرة الهيئة على مواجهة التهديدات السيبرانية، وحماية معلوماتها وأصولها الرقمية بكفاءة أعلى.

- **المراجع:**

1. بالعسل، ياسمين. عمروش، الحسين. (2021). التهديدات الإلكترونية والأمن السيبراني في الوطن العربي. مجلة نوميروس الأكاديمية. (2) . 161 – 180.
2. المنتشري، فاطمة، حريري، رندة. (2020). درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات. المجلة العربية للتربية النوعية، 4(14)، 95-140
3. الشهراني، بيان. فلمبان، فدوى. (2020). أثر برنامج تدريبي قائم على تصميم ألعاب تعليمية إلكترونية باستخدام برنامج (Game Maker) لإكساب مفاهيم الأمن السيبراني لدى طالبات المرحلة المتوسطة. مجلة البحث العلمي في التربية. م21. (9).
4. السواط، حميد. الصانع، نورة. أبو عيشة، زاهدة. سليمان، إيناس. عسران، عواطف. (2020) . العلاقة بين الوعي بالأمن السيبراني والقيم الوطنية والأخلاقية والدينية لدى تلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف. مجلة البحث العلمي في التربية. م 21. (4) . 278-306
5. البحيري، شيرين. (2023). دور الإعلام الرقمي في تعزيز الامن السيبراني ومكافحة التهديدات والجرائم السيبرانية. المجلة العلمية لبحوث العلاقات العامة والإعلان.
6. بزير، ريموش & سفيان/مشرف. (2022). الإستجابة الدولية للتهديدات السيبرانية. (رسالة ماجستير غير منشورة). جامعة محمد الصديق بن يحيى –قطب تاسوست– جيجل.
7. العنزي. تركي. (2022). الفروق في الوعي بالأمن السيبراني لدى الشباب الكويتي في ضوء بعض المتغيرات الديموغرافية والعوامل الخمسة الكبرى للشخصية.

حوليات أداب عين شمس. م 5. (2). 160-181

8. ابن ابراهيم منال (2021). الوعي بجوانب الأمن السيبراني في التعليم عن بعد. المجلة العلمية لجامعة الملك فيصل – العلوم الإنسانية والإدارية. م 22. (2) . 299- 337 .
9. المركز الوطني الإرشادي للأمن السيبراني (2021). الدليل الإرشادي لجوانب الأمن السيبراني في العمل عن بعد. متاح من خلال الرابط: https://cert .gov .Sa/ documents/13/online_working_guide.pdf
10. محمد & آمنة على البشير محمد. (2021). الأمن السيبراني في ضوء مقاصد الشريعة. مجلة كلية الدراسات الإسلامية والعربية للبنات بالإسكندرية، 37(1)، 449-505.
11. بكراوي، رانيا. بوبكر، زينب. (2023). دور الإعلام الأمني في مكافحة التهديدات السيبرانية (Doctoral dissertation, جامعة احمد دراية-ادرار).
12. وعد، إبراهيم، العمري، واخرون. (2023). تعزيز السلامة السيبرانية أثناء استخدام الاشخاص ذوي الإعاقة للإنترنت، وأثره على تحسين جودة الحياة الرقمية لديهم. العلوم التربوية, 31(1) , 466-496.
13. هوساوي. ياسر. (2020). دور التوعية بالأمن السيبراني في الحد من أثر تعقيد وسائل التحقق الرقمي من الهوية على سلوك المستخدم الطرفي. مجلة جامعة أم القرى للهندسة والعمارة. م 11 (1). 39 – 51.
14. الشريف، مرام. الحربي، ليان. الحربي، العنود. السليماني، أمل. (2023). فعالية برنامج تدريبي مقترح لتنمية الوعي بالأمن السيبراني لدى طالبات كلية الآداب والعلوم الانسانية: دراسة تجريبية. المجلة العربية الدولية لتكنولوجيا المعلومات والبيانات، 3(4)، 97-140.
15. جمال الدين. (2023). الأمن السيبراني والتحول في النظام الدولي. مجلة كلية الاقتصاد والعلوم السياسية، 24 (1)، 189-230.

- **المراجع الأجنبية:**

1. Abdullah, A. S., & Mohd, M. (2019). Spear Phishing Simulation in Critical Sector: Telecommunication and Defense Sub-sector. 2019 International Conference on Cybersecurity, ICoCSec 2019, 26–31. https://doi .org/10 .1109/ICoCSec47621 .2019 .8970803.
2. Agbo-ola, A. (2022). Motivating Cybersecurity Awareness within an Organization: An explorative study from an awareness practitioner's perspective. Unpublished Master Thesis, Luleå University of Technology, Sweden.
3. Al-Alawi, A . I ., & Al-Bassam, S . A. (2021). Assessing The Factors of Cybersecurity Awareness in the Banking Sector. Arab Gulf Journal of Scientific Research, 37(4), 2019.
4. Albediwi, M. R., & Sadaf, K. (2023). A Framework for Cybersecurity Awareness in Saudi Arabia. Journal of Engineering and Applied Sciences, 10(1)35-53.
5. Al-Fatlawi, H. H. M. (2024). Awareness of cyber security aspects in distance education. Journal of Pedagogical Sociology and Psychology, 6(1), 77-88.
6. Al-Kumaim, N. H., & Alshamsi, S. K. (2023). Determinants of cyberattack prevention in UAE financial organizations: assessing the mediating role of cybersecurity leadership. Applied Sciences, 13(10), 1-34.
7. Alshamsi, S. K. H. K., & Al Kumaim, N. H. S. (2021). A conceptual model

for prevention of e financial crimes in UAE: A review paper. Academy of Strategic Management Journal, 20(6), 1-10.

8. Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). Information & Computer Security, 27(3), 393-410.

9. Bâillon, A., De Bruin, J., Emirmahmutoglu, A., Van De Veer, E., & Van Dijk, B. (2019). Informing, simulating experience, or both: A field experiment on phishing risks. PLoS ONE, 14(12), 1–15.

10. Bhushan, B. (2023). The Growing Importance of Cyber Security in the Digital Age. international journal for innovative research in multidisciplinary field, 9(5), 234-239

11. Daengsi, T., Pornpongtechavanich, P. & Wuttidittachotti, P. (2021). Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. Educ Inf Technol 27, 4729–4752

12. ENISA. (2019). ENISA threat landscape report 2018: 15 Top Cyber-Threats and Trends. Heraklion: European Network and Information Security Agency (ENISA).

13. Goni, O. (2022). Cybercrime and its classification. Int. J. of Electronics Engineering and Applications, 10(1), 1-17

14. Hijji, M., & Alam, G. (2022). Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. Sensors (Basel,

Switzerland), 22(22), 8663

15. Ikhsan, M. G., & Ramli, K. (2019). Measuring the Information Security Awareness Level of Government Employees Through Phishing Assessment. 34th International Technical Conference on Circuits/Systems, Computers and Communications, ITC-CSCC 2019, 4–7.

16. Khando, K., Gao, S., Islam, S . M., & Salman, A. (2021). Enhancing employee's information security awareness in private and public organizations: A systematic literature review. Computers & security, 106, 102267.

17. Kulkarni, S., Kumbhare, D., More, A., & Purandare, R. (2024). Cyber Security: Types of Attacks. International Journal of Engineering Research in Computer Science and Engineering, 11(6), 252-257.

18. Mohammed, M . A . R . A . M., & Bamasoud, D. M. (2022). The Impact of Enhancing Awareness of Cybersecurity on Universities Students: A Survey Paper. J. Theor. Appl. Inf. Technol, 100.

19. Moti Zwilling, Galit Klien, Dušan Lesjak, Łukasz Wiechetek, Fatih Cetin & Hamdullah Nejat Basim (2020): Cyber Security Awareness, Knowledge and Behavior: A Comparative Study, Journal of Computer Information Systems

20. Nachin, N., Tangmanee, C., & Piromsopa, K. (2019). How to increase cybersecurity awareness. ISACA Journal, 2, 45–50.

21. Sabillon, R., Serra-Ruiz J., Cavaller V. An effective cybersecurity training

model to support an organizational awareness program : The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. J. Cases Inf. Technol. JCIT. 2019; 21:26–39

22. Safiyanu, A. M., Suleiman, A. & Yakubu, A. J. (2024). Cybersecurity: A Study on Attacks, Threats, And Vulnerabilities. International Journal of Creative Research Thoughts, 12(8), 892-896.

23. Stefanik, T. (2020). Training in shaping employee information security awareness. Entrepreneurship and Sustainability Issues, 7(3), 1832.

24. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 62(1), 82-97.

- **الملاحق**

الزملاء الأعزاء في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ:

مع التقدم المستمر في التكنولوجيا الرقمية، أصبح الوعي بالأمن السيبراني جزءًا مهما من ثقافتنا المؤسسية. نحن نعتمد على التكنولوجيا ليس فقط لتسهيل مهامنا اليومية، ولكن أيضًا لحماية معلوماتنا وأصولنا الحيوية

في هذا الإطار، يدعوكم الباحث / م. محمد أحمد سعيد الزعابي، من أكاديمية الإمارات للهوية والجنسية، للمشاركة في استبيان يهدف إلى قياس مستوى الوعي بالأمن السيبراني لدى موظفي الهيئة، وذلك ضمن دراسة « تعزيز الوعي بالأمن السيبراني لدى موظفي الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ بشأن التهديدات والهجمات السيبرانية وتأثيرها على الأصول والممتلكات الرقمية »

هذا الاستبيان مجهول الاسم حيث لا يتطلب إدخال اسم الموظف. وسيتم التعامل

مع جميع الإجابات بسرية تامة مع ضمان الخصوصية

إن مشاركتكم في هذا الاستبيان بالغة الأهمية، لأنها ستمكن من إنجاح هذه الدراسة والمساهمة في دعم ثقافة الأمن السيبراني وتعزيز الحفاظ على أصول وممتلكات الهيئة الرقمية

نقدر وقتكم ومشاركتكم الفعالة

وشكرًا لكم على حرصكم وتعاونكم.

في حال رغبتكم للتواصل مع الباحث:

اسم الباحث: محمد أحمد سعيد الزعابي

عنوان البريد الإلكتروني: ea.vog.pci@ibaazla.demmahom

الهاتف: 050 661 2255

أكاديمية الإمارات للهوية والجنسية

- **الإدارة:**
- الإدارة العامة للهوية وجوازات السفر
- الإدارة العامة للإقامة وشؤون الأجانب
- الإدارة العامة للخدمات المساندة
- الإدارة العامة لأمن المنافذ
- الإدارة العامة للجمارك
- الوحدات التنظيمية التابعة لمدير عام الهيئة

- **الجنس**:
- ذكر
- أنثى

- **الفئة العمرية:**
- أقل من 02 سنة
- من 12- 03 سنة
- من 13-04 سنة
- من 14 -05 سنة
- 15 فما فوق
- **المستوى التعليمي:**
- أقل من ثانوية عامة
- ثانوية عامة أو ما يعادلها
- بكالوريوس
- ماجستير
- دكتوراة

السؤال الأول: هل يمكنك التعرف على الرسائل الاحتيالية الواردة عبر بريدك الإلكتروني؟

- يمكنني التعرف عليها دائما 1
- يمكنني التعرف عليها غالبا 5.0
- يمكنني التعرف عليها أحيانا 52.0
- لا يمكنني التعرف عليها إطلاقا 0

السؤال الثاني: تلقيتَ رسالة بريد إلكتروني من شخص لا تعرفه تتضمن ملفا مرفقا. ما هو الإجراء الصحيح؟

- حذف البريد الإلكتروني فورًا 52.0

- فتح الملف المرفق للتأكد من سلامته 0
- التأكد مِنَ الجهة المرسِلة 2

السؤال الثالث: تلقيتَ مكالمة هاتفية تطلب منك تقديم بيانات شخصية ومالية. ما هو الإجراء الصحيح؟

- عدم الإفصاح عن البيانات عبر الهاتف 2
- تقديم المعلومات المطلوبة 0
- سؤال المتصل عن هويته 5.0

السؤال الرابع: ما هو «التصيد الاحتيالي»؟

- نوع من الفيروسات 0
- استغلال ثغرات أمنية في الشبكة 0
- محاولة لاستدراج الموظف للإفصاح عن معلومات شخصية 1+5.0

السؤال الخامس: ما هو الشكل الأفضل لكلمات المرور؟

- استخدام كلمة مرور واحدة وقوية ومعقدة لجميع الحسابات 52.0
- استخدام كلمات مرور قوية ومعقدة لكل حساب 5.1
- استخدام كلمات مرور قصيرة يسهل تذكرها 0

السؤال السادس: يعمل الموظف على جهاز الكمبيوتر الخاص به ويلاحظ وجود برنامج غريب على الجهاز لم يقم بتثبيته. كيف يجب عليك التصرف؟

- الاستمرار في العمل طالما لم يؤثر على عملك المباشر 0
- إبلاغ قسم أمن تقنية المعلومات بالهيئة وانتظار تعليماتهم. 5.1+5.0
- تشغيل البرنامج والتأكد منه قبل اتخاذ أي إجراء 0

السـؤال السـابع: يتلقـى الموظـف رسـالة تنبيـه مـن الكمبيوتـر. مـا هـي الخطـوات التـي يجـب أن يقـوم بهـا الموظـف؟

- سؤال زميلك في العمل إن توصل بنفس التنبيه 52.0
- تجاهل التنبيه ومواصلة العمل 0
- التواصل مع قسم أمن تقنية المعلومات بالهيئة 5.1

السـؤال الثامـن: وجدتَ علـى مكتبـك مفتـاحَ تخزيـن (BSU) ليـس لـك. كيـف يجـب عليـك التصـرف؟

- توصيل مفتاح BSU بجهاز الكمبيوتر الخاص بك لمعرفة محتواه وتحديد صاحبه 0
- تسليم المفتاح BSU لقسم أمن تقنية المعلومات 1
- ترك المفتاح على مكتبك حتى يظهر صاحبه 52.0

السؤال التاسع: ما هي الأسباب التي تجعلك تبلغ عن حادثة أمنية في وظيفتك؟

- خوفًا من العواقب الشخصية 5.0
- حماية بيانات وأنظمة الهيئة 1
- الالتزام بسياسات الهيئة 1
- جميع الخيارات السابقة 2

السـؤال العاشـر: مشـاركة المعلومـات الحساسـة عبـر البريـد الإلكترونـي يتطلـب اسـتخدام التشـفير

- صحيح 1
- خطأ 0

السـؤال الحـادي عشـر: يمكـن اسـتخدام شـبكات الـواي فـاي العامـة المفتوحـة للوصـول إلـى النظـام المعلوماتـي للهيئـة

- نعم 0
- لا 1+5.0

السؤال الثاني عشر: ما هي الإجراءات التي يجب اتخاذها عند فقدان جهاز الحاسوب المحمول الخاص بالعمل؟

- أتجاهل الأمر إذا كان الجهاز محمي بكلمة مرور 0
- أبلغ قسم أمن تقنية المعلومات. 5.2
- أشتري جهاز الحاسوب جديد وأشتغل عليه 0

السؤال الثالث عشر: أنت في مهمة عمل رسمية خارج الدولة، واتصل بك مسؤولك في العمل بشكل مستعجل نظرا لحاجته إلى ملف موجود في جهاز الكمبيوتر في مكتبك، وطَلب منك مشاركة كلمة المرور الخاصة بك من أجل الدخول إلى الكمبيوتر وفتح الملف لإنهاء معاملة مستعجلة. ما هو التصرف الصحيح؟

- مشاركة كلمة المرور مع المسؤول من أجل ضمان سير العمل 0
- رفض مشاركة كلمة المرور 2 + 5.0

السؤال الرابع عشر: بناء على التدريبات التي حصلت عليها، وبناء على اطلاعك على السياسات الأمنية في الهيئة وبناء على قدراتك في مجال تقنيات الحاسوب، هل تثق في قدرتك على التصرف بشكل مناسب في مواجهة التهديدات السيبرانية في بيئة عملك؟

◊ أستطيع التصرف بشكل مناسب في مواجهة كل التهديدات السيبرانية

◊ أستطيع التصرف بشكل مناسب في مواجهة أغلب التهديدات السيبرانية

◊ أستطيع التصرف بشكل مناسب في مواجهة بعض التهديدات السيبرانية

◊ لا أستطيع التصرف بشكل مناسب في مواجهة كل التهديدات السيبرانية

السؤال الخامس عشر: ما هي اقتراحاتك لتعزيز الوعي بالأمن السيبراني بين موظفي الهيئة، سواء من حيث البرامج أو الموارد أو التدريبات وغيره؟

.....

.....

.....

.....

.....

الملاحق:

الزملاء الأعزاء في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ:

مع التقدم المستمر في التكنولوجيا الرقمية، أصبح الوعي بالأمن السيبراني جزءًا مهما من ثقافتنا المؤسسية. نحن نعتمد على التكنولوجيا ليس فقط لتسهيل مهامنا اليومية، ولكن أيضًا لحماية معلوماتنا وأصولنا الحيوية

في هذا الإطار، يدعوكم الباحث / م. محمد أحمد سعيد الزعابي، من أكاديمية الإمارات للهوية والجنسية، للمشاركة في استبيان يهدف إلى قياس مستوى الوعي بالأمن السيبراني لدى موظفي الهيئة، وذلك ضمن دراسة « تعزيز الوعي بالأمن السيبراني لدى موظفي الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ بشأن التهديدات والهجمات السيبرانية وتأثيرها على الأصول والممتلكات الرقمية »

هذا الاستبيان مجهول الاسم حيث لا يتطلب إدخال اسم الموظف. وسيتم التعامل مع جميع الإجابات بسرية تامة مع ضمان الخصوصية

إن مشاركتكم في هذا الاستبيان بالغة الأهمية، لأنها ستمكن من إنجاح هذه الدراسة والمساهمة في دعم ثقافة الأمن السيبراني وتعزيز الحفاظ على أصول وممتلكات الهيئة الرقمية

نقدر وقتكم ومشاركتكم الفعالة

وشكرًا لكم على حرصكم وتعاونكم.

في حال رغبتكم للتواصل مع الباحث:

اسم الباحث: محمد أحمد سعيد الزعابي

عنوان البريد الإلكتروني: mohammed.alzaabi@icp.gov.ae

الهاتف: 0506612255

أكاديمية الإمارات للهوية والجنسية

الإدارة:

- الإدارة العامة للهوية وجوازات السفر
- الإدارة العامة للإقامة وشؤون الأجانب
- الإدارة العامة للخدمات المساندة
- الإدارة العامة لأمن المنافذ
- الإدارة العامة للجمارك
- الوحدات التنظيمية التابعة لمدير عام الهيئة

الجنس:

- ذكر
- أنثى

الفئة العمرية:

- أقل من 20 سنة
- من 21- 30 سنة
- من 31-40 سنة
- من 41 50- سنة
- 51 فما فوق

المستوى التعليمي:

- أقل من ثانوية عامة
- ثانوية عامة أو ما يعادلها
- بكالوريوس

- ماجستير
- دكتوراة

السؤال الأول: هل يمكنك التعرف على الرسائل الاحتيالية الواردة عبر بريدك الإلكتروني؟

- يمكنني التعرف عليها دائما 1
- يمكنني التعرف عليها غالبا 0.5
- يمكنني التعرف عليها أحيانا 0.25
- لا يمكنني التعرف عليها إطلاقا 0

السؤال الثاني: تلقيتَ رسالة بريد إلكتروني من شخص لا تعرفه تتضمن ملفا مرفقا. ما هو الإجراء الصحيح؟

- حذف البريد الإلكتروني فورًا 0.25
- فتح الملف المرفق للتأكد من سلامته 0
- التأكد مِنَ الجهة المرسِلة 2

السؤال الثالث: تلقيتَ مكالمة هاتفية تطلب منك تقديم بيانات شخصية ومالية. ما هو الإجراء الصحيح؟

- عدم الإفصاح عن البيانات عبر الهاتف 2
- تقديم المعلومات المطلوبة 0
- سؤال المتصل عن هويته 0.5

السؤال الرابع: ما هو «التصيد الاحتيالي»؟

- نوع من الفيروسات 0
- استغلال ثغرات أمنية في الشبكة 0

- محاولة لاستدراج الموظف للإفصاح عن معلومات شخصية 1+0.5

السؤال الخامس: ما هو الشكل الأفضل لكلمات المرور؟

- استخدام كلمة مرور واحدة وقوية ومعقدة لجميع الحسابات 0.25
- استخدام كلمات مرور قوية ومعقدة لكل حساب 1.5
- استخدام كلمات مرور قصيرة يسهل تذكرها 0

السؤال السادس: يعمل الموظف على جهاز الكمبيوتر الخاص به ويلاحظ وجود برنامج غريب على الجهاز لم يقم بتثبيته. كيف يجب عليك التصرف؟

- الاستمرار في العمل طالما لم يؤثر على عملك المباشر 0
- إبلاغ قسم أمن تقنية المعلومات بالهيئة وانتظار تعليماتهم. 1.5+0.5
- تشغيل البرنامج والتأكد منه قبل اتخاذ أي إجراء 0

السؤال السابع: يتلقى الموظف رسالة تنبيه من الكمبيوتر. ما هي الخطوات التي يجب أن يقوم بها الموظف؟

- سؤال زميلك في العمل إن توصل بنفس التنبيه 0.25
- تجاهل التنبيه ومواصلة العمل 0
- التواصل مع قسم أمن تقنية المعلومات بالهيئة 1.5

السؤال الثامن: وجدتَ على مكتبك مفتاحَ تخزين (USB) ليس لك. كيف يجب عليك التصرف؟

- توصيل مفتاح USB بجهاز الكمبيوتر الخاص بك لمعرفة محتواه وتحديد صاحبه 0
- تسليم المفتاح USB لقسم أمن تقنية المعلومات 1
- ترك المفتاح على مكتبك حتى يظهر صاحبه 0.25

السؤال التاسع: ما هي الأسباب التي تجعلك تبلغ عن حادثة أمنية في وظيفتك؟

- خوفًا من العواقب الشخصية 0.5
- حماية بيانات وأنظمة الهيئة 1
- الالتزام بسياسات الهيئة 1
- جميع الخيارات السابقة 2

السؤال العاشر: مشاركة المعلومات الحساسة عبر البريد الإلكتروني يتطلب استخدام التشفير

- صحيح 1
- خطأ 0

السؤال الحادي عشر: يمكن استخدام شبكات الواي فاي العامة المفتوحة للوصول إلى النظام المعلوماتي للهيئة

- نعم 0
- لا 1+0.5

السؤال الثاني عشر: ما هي الإجراءات التي يجب اتخاذها عند فقدان جهاز الحاسوب المحمول الخاص بالعمل؟

- أتجاهل الأمر إذا كان الجهاز محمي بكلمة مرور 0
- أبلغ قسم أمن تقنية المعلومات. 2.5
- أشتري جهاز الحاسوب جديد وأشتغل عليه 0

السؤال الثالث عشر: أنت في مهمة عمل رسمية خارج الدولة، واتصل بك مسؤولك في العمل بشكل مستعجل نظرا لحاجته إلى ملف موجود في جهاز الكمبيوتر في

مكتبك، وطَلب منك مشاركة كلمة المرور الخاصة بك من أجل الدخول إلى الكمبيوتر وفتح الملف لإنهاء معاملة مستعجلة. ما هو التصرف الصحيح؟

- مشاركة كلمة المرور مع المسؤول من أجل ضمان سير العمل 0
- رفض مشاركة كلمة المرور 2 + 0.5

السؤال الرابع عشر: بناء على التدريبات التي حصلت عليها، وبناء على اطلاعك على السياسات الأمنية في الهيئة وبناء على قدراتك في مجال تقنيات الحاسوب، هل تثق في قدرتك على التصرف بشكل مناسب في مواجهة التهديدات السيبرانية في بيئة عملك؟

- أستطيع التصرف بشكل مناسب في مواجهة كل التهديدات السيبرانية
- أستطيع التصرف بشكل مناسب في مواجهة أغلب التهديدات السيبرانية
- أستطيع التصرف بشكل مناسب في مواجهة بعض التهديدات السيبرانية
- لا أستطيع التصرف بشكل مناسب في مواجهة كل التهديدات السيبرانية

السؤال الخامس عشر: ما هي اقتراحاتك لتعزيز الوعي بالأمن السيبراني بين موظفي الهيئة، سواء من حيث البرامج أو الموارد أو التدريبات وغيره؟

.....

.....

.....

.....

.....


تم بحمد الله