رؤية الخبراء لتطبيقات الذكاء الاصطناعي في الكشف عن الأدلة الجنائية المصاحبة لجرائم شبكات التواصل الإجتماعى واتجاهاتهم نحو سيناريوهات تبنى توظيفها فى المؤسسات الأمنية العربية

د. مجدى الداغر*

الملخص:-

هدفت الدراسة التعرف على رؤية الخبراء نحو تطبيقات الذكاء الاصطناعي في الكشف عن الأدلة الجنائية المصاحبة لجرائم شبكات التواصل الإجتماعى بالتطبيق على وزارتا الداخلية فى مصر والسعودية، واعتمدت الدراسة على منهج المسح وأداة الاستبيان والمقابلة بالتطبيق على عينة قوامها (106) مفردة من العسكريين والمدنيين العاملين بالمؤسسات الأمنية العربية، وتوصلت الدراسة إلى ارتفاع معدل متابعة الخبراء فى المؤسسات الأمنية العربية لتطبيقات الذكاء الاصطناعى وأساليب توظيفها فى مكافحة الجرائم الالكترونية، كما كشفت النتائج جاهزية المؤسسات الأمنية العربية لاستخدام وتبنى تطبيقات الذكاء الاصطناعى عند أداء مهامها المهنية والوظيفية، وتنوع دوافع تبنى المؤسسات الأمنية العربية لتطبيقات الذكاء الاصطناعى فى قطاعاتها المختلفةحيث تصدرت دوافع التنافسية فى القطاعات الأمنية، وتحليل البيانات الضخمة والمعقدة، وزيادة كفاءة العامل البشرى بقطاع الأمن، وتصدرت جرائم الارهاب والاحتيال المالى واختراق الحسابات البنكية للعملاء وعمليات التجسس قائمة الجرائم الالكترونية التى من المتوقع أن يكون لتطبيقات الذكاء الاصطناعى دور فى الحد منها، كما تصدرت مجالات توظيف المؤسسات الأمنية العربية لتطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية فى" تتبع مسار مرتكب الجريمة، والكشف عن اختراقات الحسابات البنكية، والوصول للبصمة الوراثية بصور متعددة، والكشف عن الجثث مجهولة الهوية

الكلمات المفتاحية: الذكاء الاصطناعى ، الجرائم الالكترونية ، الأدلة الجنائية ، الأمن السيبرانى، المؤسسة الأمنية.

* الأستاذ المساعد بكلية الآداب - قسم الاعلام- جامعة المنصورة .

The applications of Artificial Intelligence in detecting forensic evidence associated with Cybercrime in Arab security institutions

Dr.Magdy Al-Dagher*

Abstract:-

study relied on the survey method and the questionnaire and interview tool by applying it to a sample of (106) individuals from the military and civilians working in security institutions. The study found a high rate of follow-up by experts in Arab security institutions on artificial intelligence applications and methods of employing them in combating cybercrimes.

The results also revealed the readiness of Arab security institutions to use and adopt artificial intelligence applications to a moderate degree when performing their professional and functional tasks, and the diversity of motives for Arab security institutions adopting artificial intelligence applications in their various sectors, as the motives of competitiveness in the security sectors, analysis of large and complex data, and increasing the efficiency of the human factor topped the list. In the security sector, crimes of terrorism, financial fraud, hacking into customers' bank accounts, and espionage operations topped the list of electronic crimes that artificial intelligence applications are expected to have a role in reducing. They also topped the areas in which Arab security institutions employ artificial intelligence applications in detecting electronic crimes in "tracking the path of the perpetrator." the crime, Detection of bank account hacks, access to genetic fingerprints in multiple forms, and detection of unidentified bodies.

Keywords: Artificial Intelligence, Cybercrime, forensic evidence, cybersecurity, security establishment.

* Assistant Professor at the Faculty of Arts - Department of Mass Communication - Mansoura University.

مقدمة:

شهدت السنوات العشرة الأخيرة (2014-2024) نمواً كبيراً في مجال تقنية المعلومات والاتصالات الحديثة، لا سيما في مجال تحليل البيانات الضخمة والنظم الخبيرة والتعليم العميق، حيث لم يعُد استخدام التقنية الحديثة محصوراً على العلوم التطبيقية فقط، وإنما إتسع ليشمل مجالات متعددة مثل توليد النصوص والبيانات، والصناعات الذكية، والروبوتات والألعاب الالكترونية، وغيرها من المجالات التي تتطلب مستويات عالية من التفكير والذكاء، كما شهدت تلك الفترة ظهور نمطاً جديداً للسلوك الإجرامي وهى الجرائم التى ترتبط بشبكات التواصل الإجتماعى والتي شكلت تحدياً جديداً في مواجهة أجهزة العدالة الجنائية، خاصة فيما يتعلق بإجراءات الضبط، وتكييف الجريمة، وإضفاء الوصف القانوني المناسب علي الوقائع التي تشكل هذه النوعية من الجرائم، ويرجع ذلك إلي الطبيعة الخاصة لهذه الجرائم، والتى تتم عادة في بيئة افتراضية تتميز بالتجدد والانتشار اللامحدود فى الأدوات والوسائل .

وتقوم الفكرة الأولية للذكاء الاصطناعي على محاكاة السلوك الإنساني من خلال فهمه وتحويله إلى برامج حاسوبية لديها القدرة على اتخاذ القرارات والبحث عن المشكلات وإيجاد الحلول المناسبة لها من خلال توصيفها والاستدلال عليها، وذلك باستخدام خوارزميات التصنيف والتنبؤ، وهى تقنية ذكية استطاعت أن تغير من نمط جمع المعلومات وتحليلها وأساليب كتابتها عن النمط التقليدى الذي كان سائدًا في الماضي، وهو ما يطرح اشكاليات عديدة حول مجالات توظيف الذكاء الاصطناعي والضوابط المهنية والأخلاقية التى يجب وضعها فى الاعتبار عند التطبيق فى العلوم الأمنية المختلفة .

وقد أوجد هذا التطور التقنى خدمات عديدة للحياة البشرية، يأتى أبرزها فى تنوع مجالات استخدام الروبوت وتقنية الذكاء الاصطناعي والتى تم توظيفها بداية في أداء مهام علمية محددة مثل تعديل الجينات، والكشف عن الفيروسات، وإتمام العمليات الجراحية ومتابعة نوعية الجرائم التى صاحبت وباء كورونا 2020م، إلا أن التوسع فى استخدام هذه التقنية وانتشارها صاحبه جوانب سلبية عديدة من بينها ما يعرف بالقرصنة وجرائم المعلومات والإنترنت، والتى يعتبرها أساتذة الاعلام نتيجة حتمية لكل تقدم تقنى مستحدث سواء كانت التقنية وأجهزتها أداة للجريمة أو هدفاً لها أو هى نفسها، الأمر الذى دفع عدداً من الباحثين في جامعة أوكسفورد (2022م) إلى إجراء استطلاع رأي حول مستقبل الذكاء الاصطناعي فى مكافحة الجرائم الالكترونية بالتطبيق على عينة قوامها (352) من الخبراء والمختصين فى تقنية الحاسوب وانتاج البرمجيات، وأظهرت النتائج وجود اتفاق بنسبه قدرها (92%) على أن الذكاء الاصطناعي سوف يتفوق على القدرات البشرية فى الكشف عن الأدلة الجنائية المصاحبة للجرائم بأنواعها ، بما فى ذلك تحليل سلوك "غير الأسوياء" قبل وبعد ارتكابهم للجريمة وقضاء مدة العقوبة. [1]

وأظهرت نتائج الاستطلاع أيضاً امكانية توظيف تقنيات الذكاء الاصطناعي فى رصد وتتبع مسارات الجريمة والتعرف على وجوه مرتكبيها، وسهولة الكشف عن الأدلة المتاحة والمخزنة رقمياً أو التى تم حذفها ، وتقديم مؤشرات حول طبيعة الجريمة، ومعدلات

انتشارها حسب المكان والزمان ودوافع ارتكابها، بالاضافة الى أهمية الدليل الرقمى الجنائى والذى يختلف تماماً عن الدليل التقليدى من حيث كم البيانات وكيفية اثباتها والاستدلال عليها لقد اصبح علم الأدلة الجنائية الرقمية من العلوم الأمنية المهمة فى الوقت الراهن، حيث تؤدى دوراً أساسياً فى اثبات أو نفى أى جريمة حديثة، ومن ثم فالدليل الجنائي هو "كل إجراء معترف به قانونًاً لإقناع القاضي بحقيقة الواقعة محل الاتهام، والذى يقود إلى الوصول للحقيقة المؤكدة، فيما يعتقد خبراء العلوم الأمنية أن توظيف تطبيقات الذكاء الاصطناعى فى الكشف عن الأدلة الرقمية سوف يحد من تنامى وتفاقم الظاهرة الاجرامية التي قد تلحق أضراراً بأمن الدول وانتهاك خصوصية الأفراد .

وفى اطار ذلك تحرص المؤسسات المعنية بالأمن على مواكبة التقنيات الحديثة ورصد استراتيجيات التحول الرقمي وتطبيقات الذكاء الاصطناعي للمحافظة على مستويات الأمن والأمان في كل قطاعاتها، حيث أعلنت وكالة الأبحاث التابعة لوزارة الدفاع الأمريكية عام 2018م، دعم وحدات الذكاء الاصطناعي لديها بقيمة ملياري دولار، كما قامت الصين أيضاً بضخ استثمارات تُقدر بنحو 5 مليار دولار في أبحاث الذكاء الاصطناعي لحماية مؤسساتها الحيوية من الاختراقات وأعمال القرصنة، كما يمكن استخدام التعرف على الأنماط لمراقبة نشاط وسائل التواصل الاجتماعي لتحديد الأفراد أو المنظمات التي تنشر معلومات كاذبة، أو للكشف عن أنماط غير عادية من المعاملات المالية التي قد تشير إلى نشاط احتيالي، واستخراج المعلومات تلقائيًا من الصور ومقاطع الفيديو التي قد يصعب الوصول إليها بالوسائل وسائل التقليدية الأخرى. [2]

كما اهتمت الدول الكبرى بتطوير تطبيقات الذكاء الاصطناعي واستخداماتها في المجالات الأمنية مثل: (جمع المعلومات وتحليلها، والخدمات اللوجستية، والمحاكاه الإلكترونية، والقيادة والسيطرة، والحرب الإلكترونية) وغيرها، وقد تطلب هذا التطوربعض القرارات المتعلقة بالميزانية والقوانين والتشريعات التي تدعم اتخاذ القرارات الأمنية، وتعزز من اعتماد ودعم استخدام تطبيقات الذكاء الاصطناعي في المجالات الأمنية المختلفة.

وعلى الرغم من اهتمام الحكومات وشركات التقنية الكبرى بتطوير الخوارزميات في مجال العلوم الأمنية للحدّ من انتشار الجريمة الالكترونية وأهمية الكشف المبكر عنها، الا أن المحاولات والنتائج المتوقعة لا تزال محدودة ونتائجها غير مؤكدة ، وجاءت المحاولة الأولى عندما أطلقت الصين خدمة التقاضي عبر الإنترنت، فيما استطاعت استونيا تطوير روبوت يقوم على اصدار احكام نهائية في القضايا الصغيرة، كما تمكنت الولايات المتحدة من استحداث تطبيق تقنى يقوم على التنبؤ بسلوك المجرم قبل الإفراج النهائى عنه وخروجه من السجن .[3]

وفى ظل التقدم السريع فى مجال الذكاء الاصطناعى أصبحت جرائم المستقبل تشكل تحدياً متزايد الأهمية للمؤسسات الأمنية والقضائية حول العالم، واتجهت حكومات الدول الكبرى مثل" الولايات المتحدة والصين" إلى الاستثمار الأمنى في تطبيقات الذكاء الاصطناعي للحد من تنامى الجرائم المنظمة بأنواعها، وهو ما أشار اليه تقرير"مؤسسة دبي للمستقبل"من أن حجم أضرار الجرائم الإلكترونية على الاقتصاد العالمي بلغت عام 2020م نحو 3 تريليون دولار، وأن معدل الجرائم الإلكترونية ارتفع بنسبة 33% مع تفشي وباء كورونا 2020م، [4]

وجاء قطاع الرعاية الصحية ومكافحة الأوبئة على قائمة القطاعات التي تعرضت للتهديد واعمال القرصنة من خلال برامج الفدية، خاصة وأن مرتكبي الهجمات الإلكترونية كانوا يعتقدون أن المؤسسات الصحية سوف تضطر إلى دفع "الفدية" لاستعادة أنظمتها التي تعتمد عليها في مواجهة انتشار الفيروس، ومتابعة نتائج اللقاحات التى تم التوصل اليها، وفى المقابل تمكنت إسرائيل من توظيف "فيروس"ستاكسنت" فى الهجوم على المنشآت النووية الإيرانية، ونجحت في اغتيال "فخري زاده" مدير البرنامج النووي الايرانى عبر رشاش روبوت يتم التحكم به عن بُعد، فيما نجحت إيران في تنفيذ هجوم سيبراني مضاد على مواقع إسرائيلية عطلت خلاله عمل القبة الحديدية لساعات طويلة ، أعقبه هجوم اسرائيلى جديد استهدف قطع الكهرباء عن مدن ايرانية كاملة عبر تطبيقات الذكاء الاصطناعى. (5)

وقد تزامن مع الاهتمام الدولى بالذكاء الاصطناعى اهتمامات مماثلة أخرى من قبل الشركات الكبرى مثل "أمازون وIBM ومايكروسوفت وشركة أبل وجوجل"،واستطاعت الأخيرة التوسع فى استخدام الخوارزميات فى جمع المعلومات وكتابة التقارير عن الجرائم بأنواعها ، بالإضافة الى تأمين البيانات السرية، وتحقيق مستوى أعلى من الأمان فى جمع وتداول المعلومات، حيث من المتوقع أن تسهم تطبيقات الذكاء الاصطناعي فى التنبؤ بالمخاطر والتهديدات المختلفة وتحصين أنظمة المؤسسات والشركات من السرقة أو الاختراق، وذلك اعتماداً على توظيف المعلومات المخزنة والبناء عليها في الاستدلال على الجرائم بأنواعها الالكترونية والتقليدية المعقدة. (6)

ويعتقد العديد من خبراء تقنية الحاسبات بتفوق وجدوى الاستثمار في مجال الذكاء الاصطناعي مقارنة بالاستثمارات فى قطاع النفط، حيث توقع الخبراء أن تختفي 47%من الوظائف الحالية عام (2027) بسبب التوسع فى تطبيقات الذكاء الاصطناعي، واستبدال نحو 83% من المهن التي لا تتجاوز 20 دولار في الساعة، وهو ما يزيد من نسب البطالة عالمياً. (7)

وفى المقابل سعت العديد من البلدان العربية مثل الامارات وقطر والسعودية والكويت ومصر نحو التحول الرقمي فى قطاعات الأمن بعد تزايد التهديدات الإلكترونية من قبل التنظيمات الإرهابية وقراصنة الانترنت باعتبارها قضايا تأتى ضمن موضوعات الأمن القومي العربي؛ ومن ثم كان من الضروري استخدام تطبيقات حديثة يمكن تطويعها للتصدي لتلك التهديدات التي تتم معظمها عبر مواقع الانترنت، وذلك لما يتميز به هذا النمط الجديد من قدرة فائقة على مراقبة البيانات والكشف عن الأخبار والمعلومات والصور المزيفة، مما يجعل تطبيقات الذكاء الاصطناعي تعمل جنباً إلى جنب مع برامج المؤسسات الأمنية والتنبؤ بالجرائم والوصول لمرتكبيها بسرعة تتجاوز عشرات المرات الأساليب التقليدية السابقة، حيث أثبتت نتائج دراسة عربية حديثة أن معظم منصات الانترنت عرضة للاختراق بما في ذلك أنظمة وتطبيقات الحماية ذاتها. (8)

ولما كان الاستعانة بتطبيقات الذكاء الاصطناعي في الكشف عن الجريمة والوصول الى الأدلة الرقمية المصاحبة لها وتحقيق العدالة يتطلب تدقيقاً صارماً لضمان الشفافية القانونية والحقوق الإجرائية، كان على التحليل الجنائي استعادة الأدلة الموضوعية للنشاط الإجرامي الرقمي، والذى يشمل كل ممارسات جمع الأدلة من الأجهزة الرقمية وتحديدها واستخراجها وتحليلها من قبل محققين ذوي مهارات عالية وتتبع الأثر الرقمي لمصدر الهجوم وأخذ

البيانات دون العبث بالأدلة المتاحة والتنبؤ بالتهديدات المحتملة للدول، وأن تنفيذ الذكاء الاصطناعى فى آلية رصد جرائم المستقبل يمكن أن يكون حلاً مبتكراً للتصدى لهذا التحدى المتنامى من صعوبة الحصول على الأدلة الجنائية التى ترتبط بشبكات التواصل وغيرها .(9)
ومن هنا تأتى أهمية الدراسة الحالية نتيجة المخاطر التي تشكلها الجرائم المتداولة على شبكة الإنترنت وصعوبة الوصول إلى الأدلة الجنائية الكافية بالطرق التقليدية، الأمر الذى يتطلب ضرورة توظيف تقنيات حديثة وأكثر دقة، منها تطبيقات الذكاء الاصطناعى فى عملية جمع الأدلة الجنائية الرقمية وطرق الاستدلال عليها من الناحية التشريعية والإجرائية، أو من الناحية الفنية بإعداد كوادر مؤهلة على استخدام التطبيقات الحديثة فى الكشف عن الجرائم بأنواعها.
ومن هذا المنطلق تأتى الدراسة للتعرف على رؤية خبراء الأمن فى دور تطبيقات الذكاء الاصطناعي في الكشف عن الأدلة الجنائية المصاحبة لجرائم شبكات التواصل الاجتماعى واتجاهاتهم نحو توظيفها فى المؤسسات الأمنية العربية بالتطبيق على القطاعات الأمنية بوزارتى الداخلية المصرية والسعودية .

مشكلة الدراسة:

اكتسب الذكاء الاصطناعي شعبية كبيرة مؤخراً فى مجال العلوم الأمنية، ويرجع ذلك إلى ثلاثة عوامل مهمة هي :الحجم المتزايد للبيانات الرقمية المتاحة، وزيادة سعة تخزين البيانات والمعالجة الحسابية وانخفاض تكلفتها، والتقدم في الخوارزميات المستخدمة، ومن ثم الاستفادة من قدرات الذكاء الاصطناعي، والذي ينمو استخدامه بشكل كبير في كل القطاعات والعلوم المختلفة منها" الاقتصاد والطب والعلوم بشكل عام"،بالاضافة إلى الذكاء الاصطناعي التوليدي، والثورة التي أطلقتها OpenAI بإطلاق Chat GPT، أعقبها شركات أخرى تعمل فى انتاج تطبيقات أكثر ذكاءاً.
وقد شهد عام 2022 ارتفاع حجم الاستثمارات في تطبيقات الذكاء الاصطناعي، حيث بلغت قيمة تلك الاستثمارات 2.65 مليار دولار بنسبة ارتفاع بلغت نحو 72% مُقارنة بعام 2021، والذي شهد استثمارات بقيمة 1.55 مليار دولار، بينما بلغت 0.27 مليار دولار في عام 2020، وبلغت في عام 2019 نحو 1.3 مليار دولار، بينما بلغت نحو0.2 مليار دولارعام 2018،حيث جذب هذا التطور الشركات الناشئة باستثمارات وصلت إلى نحو 17.1 مليار دولار، وبلغ حجم التمويل15.1 مليار دولار في الربع الأول 2023،فيما بلغت قيمة سوق الذكاء الاصطناعي في عام 2021 نحو 328 مليار دولار، ومن المتوقع أن تصل إلى 1.394 تريليون دولار عام 2029، وأن يعمل نحو 97 مليون شخص في قطاع الذكاء الاصطناعي.(10)
وبما أن تطبيقات الذكاء الاصطناعي تحاكي فى الأصل الذكاء البشري، وتدخل في مختلف المجالات التي تتعلق بالتفكير فائق القدرة، وتحليل البيانات، والمعلومات لأداء وظائف معقدة، أو تنفيذ عمليات صعبة، فإن ذلك سوف يشكل تحدياً أمام القانون في إثبات الجرائم التي تنشأ عن هذا النوع من التطبيقات، الأمر الذى يحتاج إلى قوانين وتشريعات تعزز هذا التقدم الجديد، وما يمكن أن يسهم به فى مواجهة التهديدات والمخاطر الأمنية، بالاضافة إلى

مستقبل حماية المؤسسات الأمنية من الهجمات الإلكترونية الخبيثة، وضمان أمن المعلومات والبيانات لفضاء إلكتروني أكثر أمناً.

ومع تنامى الجرائم الالكترونية وعدم فاعلية القوانين القائمة في مواجهتها، لاختلاف طبيعتها عن الجرائم التقليدية التي لها طبيعة محددة، كان لزاماً علي المؤسسات الأمنية البحث عن كيفية المواجهه، ولأهمية إثبات هذه الجرائم وعدم قدرة أدلة الإثبات التقليدية علي تحقيق ذلك، أصبحت الحاجة ملحة إلي إثباتها من خلال أدلة تنتمى إلي البيئة نفسها مثل تطبيقات الذكاء الاصطناعى، وهو ما فرضته الطبيعة الخاصة لتلك الجرائم، ولذا أصبح الإثبات بالأدلة الجنائية الرقمية من أبرز وسائل الإثبات، وهو ما يمكن تصنيفه علي أنه نوع جديد من الأدلة التي لها خصائصها وأساليب تتفق وطبيعة استخدامها.

وقد توصلت نتائج العديد من البحوث العلمية إلى أهمية الذكاء الاصطناعي في المؤسسات الأمنية في قدرته على تحليل كميات هائلة من البيانات في ثواني معدودة من خلال معالجة المعلومات والبيانات من مصادر متعددة منها "كاميرات المراقبة وقواعد البيانات الجنائية والبصمات وبصمة الوجة"،كما تستطيع تحديد الأنماط بسرعة وتوليد رؤية استباقية قابلة للتنفيذ، وهذا يساعد كثيراً المؤسسات الأمنية وقطاع إنفاذ القانون في الاستجابة بشكل استباقي للتهديدات المحتملة، ومنع تنامى الأنشطة الإجرامية في ظل التطور التقنى المدعوم بالذكاء الاصطناعى. (11)

وفى إطار ذلك يُصبح توظيف الذكاء الاصطناعي ضرورة حتمية فى مجال الكشف عن الجرائم بأنواعها، والتى أظهرت- حتى الآن- تفوق قدرات المحقق الآلى في بعض الجرائم مقارنة بالمحقق الطبيعى، وذلك في رصد الأدلة الجنائية بدقة من مسرح الجريمة، والتنبؤ بإمكانية وقوعها فى مكان أخر، بالاضافة إلى التعرف على الوجوه ورسم صورة للجاني من خلال التغريدات والتعليقات التي تظهر في كتاباته على شبكات التواصل، كما يمكن استخدام الذكاء الاصطناعى فى تحسين أنظمة الإنذار المبكر للجرائم المستقبلية من خلال رصد الأنشطة الاشتباهية على الإنترنت وابلاغ الجهات المعنية فى وقت مبكر.

وفى المقابل يساهم الذكاء الاصطناعي في تقديم أدلة دامغة إلى الجهات القضائية حول الجرائم المعقدة، إلى جانب توفير معلومات تم توليدها للأجهزة الأمنية عن الجرائم بأنواعها، بالإضافة إلى دورها فى مجال الأمن السيبراني والتحقيقات الرقمية الجنائية، والقدرة على التنبؤ بمعظم الجرائم حتى قبل حدوثها، وهو ما يعنى أن تطبيقات الذكاء الاصطناعي سوف تنقل مجال الأمن والعدالة ومكافحة الجريمة إلى عهد جديد عبر خوارزميات التصنيف والتنبؤ بالجرائم والتهديدات المحتملة، والتنبؤ بالكوارث الطبيعية وبعض الأحداث قبل حدوثها، بالإضافة إلى انظمة التعرف على الوجوه التي تتيح رصد لصوص المتاجر أو الزبائن المشبوهين في المطاعم ومصارف البنوك وغيرها، وهى معلومات وبيانات سوف تعتمد عليها تطبيقات الذكاء الاصطناعي فى اثبات الجريمة والكشف عن ملابساتها بدقة عالية، وفهم كيفية ترابط الحقائق المتعددة لتشكيل المعرفة وتمثيل تلك المعرفة في شكل يمكن فهمه آليًا، وعليه يمكن استخدام التقنيات الحديثة في مجال الذكاء الاصطناعي لتحسين أداء الشرطة وتعزيز الأمن العام.

وهذا التطور جعل استخدام التقنيات الذكية في المؤسسات الأمنية أمراً ملزماً على العاملين فى إداراتها المختلفة ومعياراً للحكم على إمكاناتهم المهنية وتطوير قدراتهم المعرفية، حيث ألزمت العديد من المؤسسات الأمنية فى دول العالم جميع العاملين لديها بضرورة اتقان التطورات الحديثة، ومن ثم أصبح الضباط وضباط الصف والجنود مطالبين بمراجعة مهاراتهم في ضوء التغيير التقنى داخل مؤسساتهم، وعلى الرغم من تعدد المزايا التى أضافتها تقنيات الذكاء الاصطناعى للعلوم الأمنية بشكل عام، إلا أن لدى العديد من الخبراء والقيادات الأمنية تخوفاً من التطبيق الكامل، وخاصة بالإدارات التى يتطلب عملها طابع السرية،فيما يرى أخرون ضرورة السرعة فى تبنى التطبيقات الذكية والتى سوف تساعدهم فى إنجاز العديد من مهام المؤسسة الأمنية وخاصة فى الجرائم المعقدة، دون الاستغناء عن الكوادر البشرية فى المهام والعمليات التى يصعب على الذكاء الاصطناعى اتمامها، **وفى ضوء ما سبق** تتحدد مشكلة الدراسة فى التعرف على مدى توظيف تطبيقات الذكاء الاصطناعي في الكشف عن الأدلة الجنائية المصاحبة لجرائم شبكات التواصل الاجتماعى، كما يراها الخبراء بالمؤسسات الأمنية العربية .

أهمية الدراسة:

أولاً : من الناحية النظرية : تكمن الأهمية النظرية للدراسة في فهم وتحليل ماهية الذكاء الاصطناعي ومكوناتها ومجالاتها ، هذا الفهم يعطي قيمة أكبر لأهمية تبني القطاعات الأمنية في الدولة لهذه التقنية، وهو ما أكده الباحث(Harry Surden) ، أن الذكاء الاصطناعى غالبًا ما يركز على أتمتة أنواع محددة من المهام، تلك التي يُعتقد أنها تنطوي على الذكاء عندما يؤديها الناس، ومن ثم يعطي فهماً واضحاً بأن مستويات الذكاء الاصطناعي تنطوي على مراحل عديدة منها محاكاة الذكاء البشري للآلات، ثم البيانات الضرورية، ثم العمليات المبرمجة وانتاج ما يسمى بالذكاء الاصطناعي.

ثانياً : من الناحية العلمية : تُعد هذه الدراسة من الدراسات العربية القليلة التى تتناول مستقبل توظيف تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية، والتى تأتي استجابة إلى حاجة المكتبة الإعلامية والأمنية لهذا النوع من الدراسات، ومحاولة الوصول إلى فهم حقيقى لأهمية توظيف الذكاء الاصطناعى فى العلوم الجنائية، حيث أثبتت العديد من الدراسات السابقة أن الذكاء الاصطناعي قد أسهم بشكل كبير في الكشف عن الجرائم المستحدثة ، ليس فى المساعدة فى معرفة ملابسات ودوافع الجريمة، وانما التنبؤ بالجريمة قبل حدوثها، كما تأتى أهمية الدراسة من واقع الاستخدامات الحديثة لتطبيقات الذكاء الاصطناعي في قطاع الأمن وقياس جدوى تطبيقات الذكاء الاصطناعي فى مكافحة الجريمة والقبض على المجرمين، حيث تحرص المؤسسات المعنية بالأمن فى المنطقة العربية على مواكبة التقنيات الحديثة واستراتيجيات التحول الرقمي للمحافظة على مستويات الأمن والأمان لديها، وبات التحدي اليوم أكبر مقارنة بالماضى، حيث تعددت أساليب الجريمة وتنوعت أدواتها ومن ثم أصبح لزاماً على مؤسسات الدولة الحيوية تطبيقها في مختلف قطاعاتها المختلفة.

ثالثاً : من الناحية التطبيقية : تهتم الدراسة بواقع تطبيقات الذكاء الاصطناعي في الكشف عن الأدلة الجنائية المصاحبة للجرائم الالكترونية وانعكاس ذلك على المؤسسات الأمنية العربية، بالاضافة إلى اتجاه عدد من المؤسسات الأمنية العربية نحو الاستفادة من تطبيقات الذكاء الاصطناعي في الكشف عن الجرائم الالكترونية، وهو ما يتطلب معرفة المزيد من التطبيقات الحديثة المستخدمة في الكشف عن الأدلة الجنائية الرقمية، واستحداث تشريعات جديدة تتواكب مع وظائف النمط الجديد، بالاضافة إلى التنافس بين شركات التقنية والحكومات في امتلاك تطبيقات الذكاء الاصطناعى، وهى منافسة لا تعتمد على الإمكانات المادية بقدر اعتمادها على قدرة امتلاك الأدوات التكنولوجية وعرضها للبيع لمن يستطيع دون تمييز، الأمر الذى قد يجعلها متاحة لتنظيمات ارهابية تهدد من خلالها دول العالم، ويؤمل أن يستفيد من هذه الدراسة صانعو السياسات من خلال تشريع وسياسات تُعزز دور واقع تفعيل برامج تطبيقات الذكاء الاصطناعي في آلية رصد جرائم المستقبل، تستفيد من توصيات هذه الدراسة القيادات للقيام بدورها في تشجيع العاملين في الأجهزة الأمنية على تقييم مستمر وتغذية راجعة عن التطبيقات الذكية.

أهداف الدراسة:

يأتى الهدف الرئيسى للدراسة فى التعرف على:"**رؤية الخبراء نحو تطبيقات الذكاء الاصطناعي في الكشف عن الأدلة الجنائية المصاحبة لجرائم شبكات التواصل الإجتماعى واتجاهاتهم نحو توظيفها فى المؤسسات الأمنية العربية**"، ومن خلال الهدف الرئيسى تأتى الأهداف الفرعية التالية .

1- معرفة مدى اهتمام المؤسسات الأمنية العربية بتطبيقات الذكاء الاصطناعى.

2- التعرف على دوافع استخدام وتبنى المؤسسات الأمنية العربية لتطبيقات الذكاء الاصطناعى فى قطاعاتها.

3- الكشف عن مدى جاهزية المؤسسات الأمنية العربية نحو توظيف الذكاء الاصطناعى لديها.

4- رصد أهم تطبيقات الذكاء الاصطناعى المستخدمة فى علوم الأدلة الجنائية بالمؤسسات الأمنية.

5- توضيح مجالات ومتطلبات توظيف تطبيقات الذكاء الاصطناعي فى الكشف عن الجرائم الالكترونية .

6- الكشف عن أشكال الجرائم الالكترونية المصاحبة لتطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية .

7- تحليل التأثيرات الايجابية والسلبية عند استخدام وتبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية.

8- الوقوف على المعوقات التى تواجه توظيف الذكاء الاصطناعى فى الجرائم الالكترونية.

9- التنبؤ بالسيناريوهات المستقبلية نحو توظيف الذكاء الاصطناعي فى المؤسسات الأمنية العربية .

10-مدى وجود فروق ذات دلالة احصائية فى اتجاهات خبراء الأمن حول استخدام وتبنى تطبيقات الذكاء الاصطناعى فى الحد من جرائم شبكات التواصل الاجتماعى وفق المتغيرات الشخصية والوظيفية .

تساؤلات الدراسة:

تسعى هذه الدراسة إلى الاجابة عن السؤال الرئيسى التالى: **"ما رؤية الخبراء نحو دور تطبيقات الذكاء الاصطناعي في الكشف عن الأدلة الجنائية المصاحبة لجرائم شبكات التواصل الإجتماعى واتجاهاتهم نحو توظيفها فى المؤسسات الأمنية العربية** ؟ وينبثق من هذا التساؤل تساؤلات فرعية على النحو التالي :

1. ما مدى متابعة خبراء الأمن لتطبيقات الذكاء الاصطناعى؟
2. ما مدى اهتمام المؤسسات الأمنية العربية بتطبيقات الذكاء الاصطناعى ؟
3. ما مدى جاهزية المؤسسات الأمنية العربية نحو توظيف الذكاء الاصطناعى بقطاعاتها المختلفة ؟
4. ما أهم تطبيقات الذكاء الاصطناعى المستخدمة فى قطاع الأدلة الجنائية بالمؤسسات الأمنية العربية؟
5. ما مجالات توظيف الذكاء الاصطناعي فى الكشف عن الجرائم الالكترونية ؟
6. ما متطلبات توظيف الذكاء الاصطناعى فى الكشف عن الأدلة المصاحبة للجرائم الالكترونية ؟
7. ما الأدوار المتوقعة عند تبنى المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى فى العلوم الأمنية ؟
8. ما أشكال الجرائم الالكترونية المصاحبة لتطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية؟
9. ما التأثيرات المترتبة عند توظيف وتبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية ؟
10. ما المعوقات التى تواجه توظيف تطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية ؟
11. ما سيناريوهات استخدام وتبنى تطبيقات الذكاء الاصطناعي فى القطاعات الأمنية العربية ؟
12. هل هناك فروق ذات دلالة احصائية فى اتجاهات خبراء الأمن حول استخدام وتبنى تطبيقات الذكاء الاصطناعى فى الحد من جرائم شبكات التواصل الاجتماعى وفق المتغيرات الشخصية والوظيفية ؟

مصطلحات ومفاهيم الدراسة:

- **الذكاء الاصطناعي:** يقصد به قدرة الكمبيوتر أو الروبوت على معالجة المعلومات والوصول إلى نتائج بطريقة مماثلة لعملية التفكير لدى البشر في التعلم واتخاذ القرارات، ويهدف إلى تطوير أنظمة قادرة على معالجة المشكلات المعقدة وإجراء العمليات الإنتاجية بطرق مشابهة للعمليات المنطقية والاستدلال عند البشر. (12)
- **الجريمة الالكترونية:** هي سلوك غير قانوني من خلال استخدام الأجهزة الالكترونية، ينتج منه حصول المجرم على فوائد مادية أو معنوية مع تحميل الضحية خسارة مقابلة، وغالبا ما يكون هدف هذه الجرائم هو القرصنة من أجل سرقة أو إتلاف المعلومات الموجودة في الأجهزة ومن ثم ابتزاز الضحايا باستخدام تلك المعلومات المسروقة. (13) ، واجرائياً يتم

تعرف الجريمة الالكترونية بأنها "الواقعة التي تبدأ وتنتهى في اطار العالم الافتراضي" وبذلك تشكل الواقعة الافتراضية الإجرامية البناء الحقيقي للجريمة الالكترونية .

- **التحقيق الجنائي :** هو عملية التحقيق في الجرائم المرتكبة باستخدام أي نوع من أجهزة الحوسبة مثل أجهزة الكمبيوتر والخوادم وأجهزة الكمبيوتر المحمولة والهواتف المحمولة والأجهزة اللوحية والكاميرا الرقمية وأجهزة الشبكات وأجهزة إنترنت الأشياء (IoT) أو أي نوع من أجهزة تخزين البيانات التى تحمل أدلة حول الجرائم المثارة . (14)

- **الأدلة الجنائية** : هى الوسائل التي تربط الوقائع بإدانة أو براءة الأفراد أثناء المحاكمات الجنائية، وهي مجموعة من القرائن التي من خلالها يمكن إثبات مجموعة من الحقائق التي تدور حول الجريمة، بالإضافة إلى القدرة على نسبتها إلى فاعل معين، أو هي مجموعة من البراهين مقبولة بحكم القانون، لا يمكن أن يتم إثبات وقائع الجريمة إلّا بواسطتها أمام الجهات القضائية، سواء أكانت المحاكم أم النيابة العامة، وهي تتنوع تبعًا لتنوع الجرائم، ومن ثم فالدليل الجنائي هو: "كل إجراء معترف به قانونًا لإقناع القاضي بحقيقة الواقعة محل الاتهام،(15) والأدلة الجنائية الرقمية : هى معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو شبكة الانترنت وما في حكمها، ويمكن تجميعها وتحليلها باستخدام برامج تكنولوجية خاصة.

- **الأمن السيبرانى :** يُقصد به الدفاع عن الأنظمة الإلكترونية والشبكات وأجهزة الكمبيوتر والمحمولة والبرامج والبيانات من الهجمات الرقمية الضارة. (16)

حدود الدراسة : تتمثل حدود الدراسة فى الأتى :

- **حدود موضوعية** :اقتصرت هذه الدراسة على تحديد رؤية خبراء الأمن نحو توظيف تطبيقات الذكاء الاصطناعي في الكشف عن الأدلة الجنائية المصاحبة للجرائم الالكترونية واتجاهاتهم نحو توظيفها فى المؤسسات الأمنية العربية.

- **حدود مكانية** : اقتصرت هذه الدراسة على المنسوبين للمؤسسات الأمنية العربية وتحديدا "وزارة الداخلية" فى كل من مصر والسعودية من فئة خبراء الأمن "عاملين ، ومتقاعدين".

- **حدود زمانية** : وهى الفترة التى اعقبت تحكيم الاستبيان وتوزيعه ثم تجميعه وفرزه، واستخلاص الصحيح منه للتحليل وهى الفترة من (1 - 30 مارس2024م) .

- **حدود بشرية:** اقتصرت الدراسة الحالية على عينة قوامها (106) مفردة من خبراء الأجهزة الأمنية، موزعين كالتالى :(53) من خبراء وقيادات وزارة الداخلية فى مصر، و(53) من خبراء وقيادات وزارة الداخلية فى المملكة العربية السعودية، ويرجع اختيار هذه الفئة (عينة للدراسة) كونها أكثر الفئات اهتماماً برصد ومتابعة الجرائم الكترونية والقضايا الأمنية المصاحبة وأنهم الفئة الأجدر علي تقديم رؤية مستقبلية حول أبعاد الدور المتوقع لتطبيقات الذكاء الاصطناعي في مجال الكشف عن الأدلة الجنائية المصاحبة للجرائم الالكترونية على شبكات التواصل الإجتماعى وغيرها .

الإطار النظري للدراسة :

أولاً: النظرية الموحدة لقبول واستخدام التكنولوجيا :

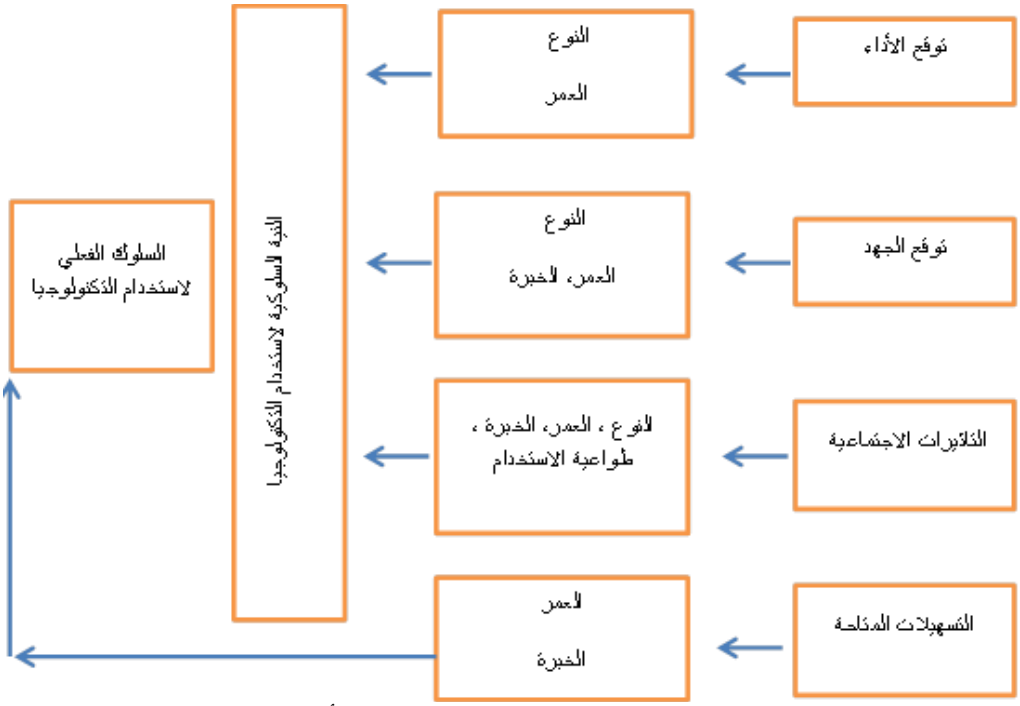
تُعد النظرية الموحدة هى إحدى نظريات علم النفس وتهدف إلى تفسير نية وسلوك الاستخدام للتقنية الحديثة، وترى النظرية أن الأداء المتوقع، والجهد المتوقع، والتأثير الاجتماعي والتسهيلات المتاحة تؤثر على نية الاستخدام للتقنية الحديثة

كما يُعد نموذج قبول واستخدام التكنولوجيا من النماذج الثقة عند تفسير قبول واستخدام التقنية الحديثة؛ حيث تم اختباره بشكل واسع ، واظهرت النتائج أن 86% من الدراسات والبحوث التي تناولت مجالات توظيف التقنية الحديثة اعتمدت فى اطارها النظرى على هذا النموذج، ويُعد العالم دافيد "Davis" هو المؤسس الحقيقي لنموذج قبول واستخدام التكنولوجيا وذلك عام 1989م حيث أشار إلى أن عدم قبول المستخدمين للعمل على التقنية والتكنولوجيا يعتبر عائقًا مهمًا أمام نجاح هذه النظم فى أداء مهامها، كما أثبت أن فهم قبول أو رفض أي تكنولوجيا يُعد من أكبر تحديات الباحثين في مجال التقنية الحديثة، وهو ما يفسر تنامى استخدامات نموذج قبول واستخدام التكنولوجيا فى العلوم التطبيقية. (17)

وهناك اتفاق بين الباحثين على أن نموذج النظرية الموحدة لقبول التكنولوجيا (UTAUT-2) يمتاز بأنه قام على تجميع بعض المتغيرات التي وجدت متفرقة في النظريات السابقة والتي تؤثر في سلوك الاستخدام ونية المستخدم ، ومن هنا كان تسميتها بالنظرية الموحدة، والتي تتضمن توحيد 8 نظريات مختلفة ، ويتكون النموذج من 4 عوامل أساسية هي : (18)

1. الأداء المتوقع: وهو مدي اعتقاد الفرد أن استخدامه للتقنية سوف يزيد من انتاجيته للعمل.
2. الجهد المتوقع : هو درجة السهولة المتعلقة باستخدام الفرد للتقنية .
3. التأثير الاجتماعي : هو مدي تأثير المجتمع علي الفرد لاستخدام التقنية .
4. تسهيل الظروف : هي مدي اعتقاد الفرد بتوفر التسهيلات والبني التحتية للتقنية .

كما يخضع النموذج ذاته للتعديل من خلال 4 عوامل إضافية هي(العمر، النوع ، الخبرة، وطواعية الاستخدام).



ومن الشكل السابق يتضح وجود ثلاثة خصائص أساسية للنظرية وضعها (Venkatesh2010)، تتمثل فيما يلي: [19]

- ردود أفعال الأفراد تجاه استخدام التكنولوجيا (المتغيرات المستقلة)
- النية السلوكية والاستخدام الفعلي للتكنولوجيا(المتغيرات التابعة)
- الخصائص الفردية لمُستخدمي التكنولوجيا(المتغيرات الوسيطة)

مدى توظيف النظرية في الدراسة :

تمكن النظرية الموحدة لقبول واستخدام التكنولوجيا الباحث من تفسير اتجاهات خبراء الأمن نحو مدى توظيف تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية، وإمكانية التنبؤ بطبيعة ذلك الاستخدام مستقبلًا وتأثيره فى الكشف عن أبعاد الجريمة الالكترونية، وذلك بناء على عدد من المتغيرات التى اعتمدت عليها النظرية تتمثل فى التالى: [20]

1- **متغير الأداء المتوقع:** حيث أن استخدام الذكاء الاصطناعي سوف يساهم فى تحسين مهارات وقدرات رجال الأمن داخل المؤسسة الأمنية، وهو ما يعود بالنفع عليهم وعلى أدائهم ؛ وأن ذلك قد يؤدي إلى إيجاد نية سلوكية لاستخدام هذه التطبيقات، ومن ثم قيامهم بالفعل بتوظيفها في عملهم عند الكشف عن الجريمة وتعقب مرتكبيها عبر آليات الأدلة الرقمية المتاحة .

2- **متغير الجهد المتوقع**: ويعنى أنه بالمقارنة بين التكلفة والوقت والجهد المتوقع في الطرق التقليدية لتجميع الأدلة الجنائية والتكلفة والوقت والجهد المتوقع عند توظيف الذكاء الاصطناعي، قد يتبين مدى توفير هذه التطبيقات للتكلفة والوقت والجهد، إلى جانب سهولة

الاستخدام ، والدقة فى الكشف عن الأدلة الجنائية المصاحبة للجرائم الالكترونية، والسرعة في الأداء، وهى دوافع قد تساعدهم على أخذ نية التبنى الفعلي لتلك التقنيات فى مجال عملهم.

3- **متغير التأثيرات الاجتماعية**: ويمكن توضيح ذلك المتغير من خلال توقع الآخرين-مثل الدولة والعاملين بالمؤسسة الأمنية من زملائهم والإدارة على قدر كبير من الاستعداد لتوظيف مثل هذه التقنية؛ ربما يكون له تأثير على طبيعة استخدامهم لها.

4- **متغير التسهيلات المتاحة**: ويتوقف هذا المتغير على مدى توفير الإمكانات المختلفة اللازمة لاستخدام - رجال الأمن- لتقنيات الذكاء الاصطناعي في الكشف عن الأدلة الجنائية المصاحبة للجرائم الالكترونية، وتطوير المضامين الخاصة بالثراء المعلوماتي مثل توفير الإمكانات المادية من أنظمة حاسوبية متطورة، وعقد دورات تدريبية مستمرة، ووجود العقلية المستنيرة القائمة على إدارة مسرح الجريمة بمهارة وكفاءة عالية .

وتأتى الاستفادة من النظرية فى جمع البيانات، وتفسير وشرح أسباب استخدام أو عدم استخدام تطبيقات الذكاء الاصطناعي في المؤسسات الأمنية العربية، وذلك بناء على عدد من المتغيرات، منها: الأداء المتوقع، والجهد المتوقع، والتأثيرات الاجتماعية والتسهيلات المتاحة، ونية الاستخدام فى ضوء النوع والعمر والخبرة وطواعية الاستخدام .

ثانياً: الدراسات والبحوث السابقة :

قام الباحث بمراجعة الأدبيات والدراسات والبحوث السابقة حول موضوع الدراسة، وقد أسفر البحث عدم وجود بحوث ودراسات تناولت تطبيقات الذكاء الاصطناعي فى العلوم الأمنية، إلا أن هناك دراسات تناولت البعد الأمنى لجرائم الإنترنت من زوايا مختلفة يمكن رصدها فى التالى :

دراسة سعد مفلح (2023) [21] والتى هدفت إلى التعرف على دور أنظمة الذكاء الاصطناعى فى مكافحة الشائعات الالكترونية ، واعتمدت الدراسة على منهج المسح وأداة تحليل المضمون لعدد من التقارير المنشورة، وتوصلت إلى أن الشائعات والأكاذيب تمثل أدوات حروب الجيل الخامس عبر منصات التواصل الاجتماعى ولديها تأثير على الأمن القومى، وتوصى الدراسة بضرورة استخدام تطبيقات الذكاء الاصطناعى فى مكافحة نشر الشائعات باستخدام التعليم الآلى، والشبكات العصبية والخوارزميات وتحليل المعلومات ودعم استراتيجيات الوعى ضد المخاطر داخل المجتمع ، **وهدفت دراسة ليلى بن برغوث (2023)** [22] الكشف عن واقع الأمن السيبرانى وخصوصية البيانات الرقمية الموجودة فى المواقع الالكترونية الجزائرية، والتقنيات المستخدمه فى عمليات الاختراق والسرقة الالكترونية، واعتمدت الدراسة على المنهج الوصفى التحليلى وأداة الاستبيان، وتوصلت نتائج الدراسة الى امكانية توظيف تقنيات الذكاء الاصطناعى فى التصدى للهجمات السيبرانية ومكافحة الجرائم الالكترونية مستقبلاً.

أما دراسة عبدالمولى اشبيبة (2022) [23] فقد هدفت إلى التعرف على الدليل الإلكتروني في الإثبات الجنائي في القانون المغربي من حيث إثبات التهمة أو نفيها، واعتمدت الدراسة على المنهج الوصفى التحليلى وأداة الاستبيان بالتطبيق على عينة قوامها (120) مفردة من ضباط الشرطة فى المغرب، وأظهرت النتائج اتفاق عينة الدراسة على أن التقنية الحديثة كانت سبباً فى تنوع الجرائم الالكترونية ، وأن الاهتمام بالأدلة الإلكترونية ساهم في اكتشاف

هذا النوع من الجرائم وفي محاصرة مرتكبيها، **كما هدفت دراسة علياء عمر كامل (2022)** [24] الى التعرف على دواعي ثقافة الأمن السيبراني في ظل التحول الرقمي، واعتمدت الدراسة على المنهج الوصفي التحليلى، وأداة الاستبانة بالتطبيق على عينة قوامها (125) مفردة من أعضاء هيئة التدريس بجامعة الأمير سطام بن عبد العزيز بالسعودية، وتوصلت الدراسة إلى عدم وجود فروق ذات دلالة تبعا لمتغير الكلية، والرتبة العلمية، ووجود فروق تعزى لمتغير سنوات الخبرة.

وسعت دراسة تقي مباركية (2022) [25] نحو التعرف على دور الخبرة في إثبات المعاملات الإلكترونية والقواعد الفنية التى تحكمها في اكتشاف الدليل الرقمي، واعتمدت الدراسة على منهج المسح وأداة الاستبيان بالتطبيق على عينة قوامها (45) مفردة من اعضاء النيابة العامة،وتوصلت نتائج الدراسة إلى أن الأدلة الرقمية ساعدت في إثبات الجرائم المعلوماتية وكشف أنماطها لدى الخبراء المتخصصون في التحقيق الجنائى، فيما **كشفت دراسة ممدوح خليل (2022)** [26] عن مدى تأثير الإجراءات القانونية للتفتيش في الوسط الافتراضي على حرية القاضي، واعتمدت الدراسة على منهج المسح وأداة الاستبيان بالتطبيق على عينة قوامها (120) مفردة، وتوصلت نتائج الدراسة إلى دور التقنية الحديثة فى ارتكاب الجرائم، يقابلها ظهور مجموعة جديدة من الأدلة تتفق وطبيعة الوسط الذي ارتكبت فيه.

أما دراسة خليل سعيدى (2022) [27] والتى هدفت التعرف على أهمية الذكاء الاصطناعى فى تحقيق الأمن السيبرانى والحفاظ على البيانات والمعلومات المعرضة للإختراق، واعتمدت الدراسة على المنهج الوصفى التحليلى وأداة الاستبيان بالتطبيق على عينة قوامها (115) مفردة ، وتوصلت النتائج إلى ضرورة توظيف تقنيات الذكاء الاصطناعى فى حماية خصوصية الأفراد والمستخدمين عبر مختلف المنصات الرقمية، **واهتمت دراسة عدنان الحجار(2021)** [28] بالتعرف على ماهية الجرائم الالكترونية، والأدلة التي تثبتها، ومدى حضور هذه الأدلة أو غيابها في القوانين المحلية والعالمية، أظهرت نتائج الدراسة وجود فراغ تشريعي يعتري الدليل الرقمي، يعزى إلى نقص وضعف التعامل مع الواقع التقني الذي فرض نفسه في التحقيق الجنائى، وأوصت الدراسة بضرورة العمل على نشر التوعية الإلكترونية بين العاملين في القانون، وتدريب الكوادر الفنية على تقنيات البحث الجنائي الرقمي، وتعزيز عمل القضاء في إصدار أحكاماً تستند إلى الدليل الجنائى الرقمى.

أما دراسة يعقوب بلبشير (2021) [29] فقد هدفت التعرف على الاستراتيجيات الأمنية المستخدمة فى حماية الفضاء الالكترونى ، واعتمدت الدراسة على منهج المسح وأداة تحليل المضمون، وتوصلت إلى أن الأمن السيبرانى أصبح يشكل جزءاً أساسياً من السياسة الأمنية، وأن استغلال الشبكات الإلكترونية لأهداف إجرامية يؤثر سلباً على سلامة البنى التحتية للمعلومات الوطنية ،وتوصى الدراسة بضرورة وضع منظومة وطنية شاملة لأمن الفضاء السيبراني وحمايته، و**دراسة علاء الدين فرحات** (2021) [30] والتى تناولت اساليب تحقيق مبدأ الردع في الفضاء السيبراني، واعتمدت الدراسة على المنهج الوصفى التحليلى وأداة الاستبيان بالتطبيق على عينة قوامها (110) مفردة، وتوصلت الدراسة إلى صعوبة فى إسناد الهجمات السيبرانية إلى مرتكبيها، بالاضافة الى صعوبة تحديد الهجمات الإلكترونية ذات الاهتمام الجماهيرى.

وهدفت دراسة توفيق الخشاشنة (2021) [31] الى التعرف على الدليل الإلكتروني ومدى حجيته في الإثبات الجنائي، واعتمدت الدراسة على منهج المسح وأداة تحليل الوثائق، وتوصلت النتائج إلى أهمية الدليل الإلكتروني فى رصد النبضات الموجودة أو المستخلصة من أي جهاز رقمي، ومن ثم يتم تجميعها وتحليلها باستخدام برامج خاصة، والتى تظهر على شكل صور أو تسجيلات صوتية أو مرئية بهدف إثبات وقوع الجريمة ونسبتها إلى من ارتكبها، بينما سعت **دراسة على محمود ابراهيم (2021)** [32] الى التعرف على الأدلة الرقمية وحجيتها في إثبات الجرائم الإلكترونية، واعتمدت الدراسة على منهج المسح وأداة الاستبيان، وتوصلت النتائج إلى أن الأدلة الرقمية تكيف على أنها قرائن، ويجوز للقاضي الجنائي الاعتماد عليها في إثبات الجرائم الإلكترونيةإذا توافرت فيها الضوابط التي اشترطها القائلون بحجيتها.

واهتمت دراسة أحمد جابر صالح (2019) [33] بالتعرف على كيفية التعامل مع الأدلة الإلكترونية، واعتمدت الدراسة على المنهج الوصفي التحليلي، وتوصلت نتائج الدراسة إلى أن النصوص القانونية في التشريع الأردني ما زالت بعيدة عن الدليل الإلكتروني، وعليه توصي الدراسة بضرورة تعديل قانون أصول المحاكمات بما يتوافق مع طبيعة الدليل الإلكتروني في إثبات المسائل الجزائية، فيما سعت **دراسة محمد محمود عمرى** (2016) [34] نحو التعرف على عملية الإثبات الجنائي الإلكتروني ومدى صلاحيته في الكشف عن الجرائم الإلكترونية من خلال التعرف على ماهية الدليل الرقمي وتفتيش مكونات الحاسوب والشبكات التي تنتهي بطرفيات الحاسوب والخوادم المزودة للإنترنت وشبكات الاتصال واعتمدت الدراسة على منهج المسح وأداة الاستبيان، وتوصلت النتائج إلى أهمية توظيف التقنية الحديثة فى الكشف عن الأدلة الرقمية فى الجرائم المستحدثة.

أما دراسة محمد النمر (2013) [35] فقد هدفت التعرف على دور تقنية المعلومات فى مكافحة جرائم الابتزاز الالكترونى، واعتمدت الدراسة على منهج المسح واداة الاستبيان بالتطبيق على عينة قوامها(164) من ضباط الشرطة ، وأظهرت النتائج أن وظائف تقنية المعلومات فى مكافحة جرائم الابتزاز هى" تحديد موقع مرتكب الجريمة ، والتقاط الدليل الالكترونى لاثباتها "، واهتمت **دراسة محمد الحقبانى** (2013) [36] بالتعرف على مهارات البحث فى الجرائم المعلوماتية، واعتمدت الدراسة على منهج المسح وأداة الاستبيان بالتطبيق على عينة قوامها (146) مفردة من ضباط الشرطة بالرياض، وأظهرت النتائج ضعف المهارات لدى ضباط الشرطة فى مجال البحث والتحرى عن الجرائم الالكترونية، وهدفت **دراسة ناصر البقمى** (2012) [37] الى التعرف على أهمية الأدلة الرقمية فى الاثبات الجنائى، واعتمدت الدراسة على منهج المسح واداة الاستبيان بالتطبيق على عينة قوامها (150) مفردة من ضباط الشرطة ، وتوصلت النتائج إلى وجود صعوبات تواجه جهات التحقيق الجنائى فى جرائم المعلومات يتصدرها قله خبرة الضباط فى فهم التقنية الحديثة .

وهدفت دراسة سيدى محمد البشر (2010) [38] الى التعرف على دور الدليل الرقمى فى اثبات الجرائم المعلوماتية ، واعتمدت الدراسة على منهج المسح واداة الاستبيان بالتطبيق على عينة قوامها (75) مفردة من ضباط الشرطة ، وتوصلت الدراسة إلى أن مسرح الجريمة الالكترونية يتشكل من الحاسب والأفراد وخدمة شبكة الانترنت ، بينما سعت **دراسة سلمان**

العتيبى (2010) [39] الى الكشف عن مدى توافر الدليل الرقمى فى الجرائم المعلوماتية لدى ضباط الشرطة بمنطقة مكة المكرمة ، واعتمدت الدراسة على منهج المسح وأداة الاستبيان بالتطبيق على عينة قوامها (173) مفردة ، وتوصلت النتائج الى عدم توافر أدوات الكشف عن الدليل الرقمى فى الجرائم المعلوماتية لديهم .

أما دراسة تركى المويشير (2009) [40] فقد هدفت التعرف على أساليب مكافحة الجرائم المعلوماتية فى المملكة العربية السعودية ، واعتمدت الدراسة على منهج المسح وأداة الاستبيان بالتطبيق على عينة قوامها (210) مفردة من ضباط الشرطة بالرياض، وتوصلت الدراسة إلى أن قلة الخبرة وضعف أداء ضباط الشرطة تأتى على قائمة معوقات تحقيق العدالة الجنائية الرقمية، و**دراسة أحمد الشهرى** (2005) [41] والتى هدفت التعرف على ملامح الظاهرة الاجرامية فى عصر التقنية والتهديدات الأمنية المصاحبة لها ، واعتمدت الدراسة على منهج المسح وأداة الاستبيان بالتطبيق على عينة قوامها (75) مفردة من ضباط الشرطة بالمنطقة الشرقية السعودية، وأظهرت النتائج أهمية الاثبات والدليل الرقمى فى عصر التقنية، وأوصت الدراسة بضرورة التغلب على التحديات التى تواجه جرائم الابتزاز الالكترونى.

وسعت دراسة محمد السرحان (2004) [42] الى التعرف على المهارات الفنية لدى ضباط الشرطة السعودية، واعتمدت الدراسة على منهج المسح وأداة الاستبيان بالتطبيق على عينة قوامها (340) مفردة من ضباط الشرطة فى منطقة عسير، وتوصلت النتائج إلى ضعف مهارات الضباط فى التعرف على المكونات المادية للحاسبات وشبكات الانترنت، وهو ما ينعكس على عدم المعرفة بالأداوت المستخدمة فى ارتكاب الجريمة على شبكة الانترنت، فيما هدفت **دراسة خالد العنزى** (2003) [43] الى التعرف على أدوات التحقيق فى جرائم نظم المعلومات، واعتمدت الدراسة على منهج المسح وأداة الاستبيان بالتطبيق على عينة قوامها (410) مفردة من ضباط أقسام الشرطة بمدينة الرياض، وأظهرت النتائج قلة خبرة ضباط الشرطة فى التعامل مع التقنية الحديثة فى التحقيق الجنائى والكشف عن الجريمة

وسعت دراسة عبد الله الشهرى (2002) [44] الى التعرف على أهم المعوقات التى تواجه الحاسب الآلى أثناء التحقيق فى الجرائم الالكترونية، واعتمدت الدراسة على منهج المسح وأداة الاستبيان بالتطبيق على عينة قوامها (120) مفردة من ضباط الشرطة بالرياض، وتوصلت إلى أن نقص المعرفة بالحاسب وضعف مهارات التعامل مع الانترنت وعدم كفاية التدريب أهم الأسباب التى تعوق التعامل الأمنى مع جرائم الانترنت، و**دراسة محمد البشرى** (2001) [45] والتى هدفت التعرف على اتجاهات النخب الأمنية نحو التحقيقات الاستدلالية فى جرائم الالفية الثالثة، واعتمدت الدراسة على منهج المسح وأداة الاستبيان بالتطبيق على عينة قوامها (45) مفردة من خبراء العلوم الأمنية بالرياض، وتوصلت إلى أهمية الدليل الرقمى فى الاثبات والتعامل مع مسرح الجريمة .

التعليق على الدراسات السابقة

1. هدفت غالبية الدراسات السابقة إلى التعرف على أهمية تقنيات الذكاء الاصطناعي في مجتمعات مختلفة مثل الولايات المتحدة والصين وإيطاليا وكوريا الجنوبية وبعض الدول العربية مثل السعودية والامارات ومصر، كما هدفت أيضاً إلى التعرف على استخدامات الذكاء الاصطناعي فى التصدى لهجمات الأمن الالكترونى والأخبار المزيفة .

2. اعتمدت غالبية الدراسات السابقة على عدة مداخل نظرية لفهم تعامل الجمهور مع تقنيات الذكاء الاصطناعى ومدى تقبلهم لها، كان أبرزها النظرية الموحدة لقبول واستخدام التكنولوجيا وانتشار المبتكرات المستحدثة .

3. تظهر نتائج الدراسات السابقة وجود ندره في البحوث التي تناولت تطبيقات الذكاء الاصطناعي فى العلوم الأمنية على المستوى العربى والدولى، مقارنة ببعض الدراسات التى اهتمت بدور الذكاء الاصطناعى فى الحفاظ على الأمن السيبرانى.

أوجه الاستفادة من الدراسات السابقة:

وعليه يمكن رصد الاستفادة من الدراسات والبحوث السابقة فى الأتى :

1. **على المستوى المعرفي:** ساعدت الباحث على تحديد تساؤلات الدراسة وصياغة الفروض العلمية بشكل أفضل وضبط نوع وحجم العينة وإعطاء فكرة عن المعاملات والاختبارات الإحصائية التي يمكن استخدامها في الدراسة.

2. **على المستوى النظري**: ساعدت على تعميق الإطار النظري وتوسيع معلومات الباحث في تحديد الأهمية الخاصة بالذكاء الاصطناعي، حيث قدمت تلك الدراسات والبحوث إطارا معرفيا عن الذكاء الاصطناعي، وجانبا عن تأثيرات التقنيات الحديثة في مجالات مختلفة، مما ساعد على إيضاح جميع جوانب النظرية الموحدة وأهم المتغيرات التي يعتمد عليها الباحثون في اختباراتهم لفروض النظرية.

3. **على المستوى التطبيقي**:، فقد استفاد الباحث من طريقة تطبيق الدراسات على العينات البشرية مما أمكنها التوصل إلى نتائج مهمة يمكن الاسترشاد بها في الجانب التطبيقي للدراسة الحالية، وإجراء المقارنات الخاصة بالفروق بين نتائج ما توصلت إليه الدراسات السابقة وما ستتوصل إليه الدراسة الحالية من نتائج.

الإجراءات المنهجية للدراسة :

نوع الدراسة : تُعد هذه الدراسة من الدراسات الكشفية، حيث تستهدف توفير قدر من المعلومات عن مدى فاعلية توظيف تطبيقات الذكاء الاصطناعي في الكشف عن الأدلة الجنائية المصاحبة للجرائم الالكترونية في المؤسسات الأمنية العربية.

-**منهج الدراسة**: اعتمدت الدراسة على منهج المسح الاعلامى بالتطبيق على عينة من الخبراء بالمؤسسات الأمنية العربية، وفي إطار هذا المنهج ايضاً تم استخدم أسلوب المقارنة المنهجية، وهي أداة من أدوات الاستقراء في الدارسات الميدانية وتسهم فى الاستدلال على أوجه الاتفاق أو الاختلاف بين آراء المبحوثين .

أدوات جمع بيانات الدراسة :

اعتمد الباحث على صحيفة الاستبيان كأداة لجمع البيانات والتى تركز على عدة محاور ترجمت أهداف الدراسة، وتمثلت في قياس اتجاهات خبراء الأمن فى المؤسسات الأمنية العربية نحو مدى توظيف تطبيقات الذكاء الاصطناعي في الكشف عن الأدلة الجنائية المصاحبة للجرائم الالكترونية في المؤسسات الأمنية العربية.

- **أداة المقابلة:** وقد استخدم الباحث المقابلة غير المقننة للحصول على بعض المعلومات التى لم تتضمنها صحيفة الاستبيان، وتفسير بعض النتائج التي تتوصل إليها هذه الدارسة.

مجتمع وعينة الدراسة :

تم تطبيق الدراسة على عينة عمدية من العاملين بالمؤسسات الأمنية العربية وتحديداً "وزارتا الداخلية فى مصر والسعودية" ، حيث تم تطبيق الدراسة على عينة قوامها (106) من خبراء الأمن فى المؤسسات الأمنية الخاضعة للدراسة .

وقد وقع اختيار الباحث على أسلوب العينة العمدية فى دراسته لاعتبارات عديدة منها :

1. أن مجتمع الدراسة مجتمع متحرك، يتم إعادة تشكيل العاملين به بين فترة وأخرى.
2. أن مجتمع الدراسة مجتمع نوعي متخصص في العلوم الأمنية، وأن عينة الدراسة من الخبراء لديهم معرفة كاملة بمهددات ومخاطر التطبيقات الحديثة على أمن الأفراد والمجتمعات، ورغبة من الباحث الاستفادة من آراء أفراد مجتمع الدراسة، قام بتوزيع نحو (200) استبانة، عاد منها (106) فقط، وبناء عليه اعتبر الباحث هذا العدد مناسباً وكافياً للدراسة.

متغيرات الدراسة :

المتغير المستقل : ويتمثل فى تطبيقات الذكاء الاصطناعى فى العلوم الأمنية والجرائم الالكترونية.

المتغير التابع : ويتمثل فى المؤسسات الأمنية العربية (وزارة الداخلية فى مصر والسعودية)

المتغير الوسيط : يتمثل فى خبراء الأمن من حيث (النوع ، العمر، الخبرة ، الرتبة الوظيفية ، الدولة...)

اختبارات الصدق والثبات:

-**اختبار الصدق** : تم التأكد من صدق الاستبيان من خلال عرضه علي مجموعة من المحكمين في مجال الأمن والإعلام ومناهج البحث الإعلامي، [46] وفي ضوء آراء المحكمين تم إجراء بعض التعديلات عليه حتي أصبح بشكله النهائي بعد إضافة بعض الفئات والبدائل)، وقد تراوحت نسبة الاتفاق بين المحكمين نحو (95%) على صلاحية الاستبيان للتطبيق .

اختبار الثبات :تم إجراء اختبار الثبات عن طريق إعادة تطبيق الاستبيان Retest عقب فترة زمنية من إجاباتهم عليها، وذلك علي عينة قوامها 5 مفردات، وذلك بعد مرور عشرين يوما عقب الانتهاء من التطبيق الاول علي العينة الأساسية، وقد اعتمد الباحث في حساب ثبات نتائج الاستبيان علي حساب نسبة الاتفاق بين إجابات المبحوثين في التطبيق الأول والثاني وكانت قيمة معامل الثبات 90% ، وهو معامل ثبات مرتفع ،ويدلل علي عدم وجود اختلاف كبير في إجابات المبحوثين، ومن ثم صلاحية الاستبيان للتطبيق.

وقد تم توزيع الاستبانة على أفراد مجتمع الدراسة من قبل الباحث شخصياً، وجمعها بعد إعطائهم المدة الكافية، وتمكن من جمع (106) استبانة صالحة للتحليل، وبعد ذلك تم إدخال البيانات، ومعالجتها إحصائياً واستخراج نتائجها.

كما تم الاعتماد على مقاييس ليكارت الثلاثى والخماسى وذلك على النحو التالى :

القياس	المستوى	الفئة
(1- 2.49)	ضعيف	1
(2.50 - 3.49)	متوسط	2
(3.50 -5)	مرتفع	3

أما المقياس الخماسى فقد جاءت مستوياته على النحو التالى :

القياس	المستوى	الفئة
(1 - 1.80)	لا تستخدم / أبداً / موافق بدرجة قليلة جداً	1
(1.80 - 2.60)	تستخدم بدرجة قليلة / نادراً / موافق بدرجة قليلة	2
(2.60 - 3.40)	تستخدم بدرجة متوسطة / أحياناً / موافق بدرجة متوسطة	3
(3.40 - 4.20)	تستخدم بدرجة كبيرة / غالباً / موافق بدرجة كبيرة	4
(4.20 -5)	تستخدم بدرجة كبيرة جداً / نعم دائماً / موافق بدرجة كبيرة جداً	5

الأساليب الإحصائية بالدراسة :

استخدمت الدراسة العديد من الأساليب الإحصائية من خلال برنامج الحزم الإحصائية (SPSS)، وذلك بعد أن تم ترميز وإدخال البيانات إلى الحاسوب، ووضع المقاييس المناسبة للدراسة ، ومن هذه الأساليب التالي :

1. حساب التكرارات، والنسب المئوية: للتعرف على الخصائص الشخصية والوظيفية لأفراد مجتمع الدراسة.
2. حساب المتوسط الحسابي الموزون : لمعرفة مدى ارتفاع أو انخفاض استجابات العينة على كل عبارة .
3. المتوسط الحسابي: لمعرفة مدى ارتفاع أو انخفاض استجابات عينة الدراسة عن محاور الدراسة.
4. الانحراف المعياري : للتعرف على مدى انحراف استجابات عينة الدراسة لكل عبارة من عبارات متغيرات الدراسة.
5. تم استخدام اختبار كا^2: لتحديد مدى تجانس أو تباين وجهات نظر عينة الدراسة حول متوسطات إجاباتهم.
6. تم استخدام اختبار(T): للتعرف على ما إذا كانت هناك فروق ذات دلالة إحصائية في اتجاهات أفراد مجتمع الدراسة نحو محاور الدراسة باختلاف متغيراتهم الشخصية والوظيفية التي تنقسم إلى فئتين.
7. تم استخدام تحليل التباين الأحادي(Anova): للتعرف على ما إذا كانت هناك فروق ذات دلالة إحصائية في اتجاهات أفراد مجتمع الدراسة نحو محاور الدراسة باختلاف متغيراتهم الشخصية والوظيفية التي تنقسم إلى أكثر من فئتين.
8. تم استخدام اختبار (LSD): لتحديد صالح الفروق بين فئات المتغيرات الشخصية والوظيفية التي تنقسم إلى أكثر من فئتين، في حالة إذا ما أظهر اختبار تحليل التباين (F) وجود فروق بين فئات هذه المتغيرات.

المبحث الأول : الإطار المعرفى للدراسة :

اشكالية مفهوم الذكاء الاصطناعي فى دراسات العلوم الأمنية :

يُعتبر الذكاء الاصطناعي أحد فروع علم الحاسوب وأحد الركائز الرئيسية التي تستند إليها التكنولوجيا الحديثة ، ويمكن تعريف مصطلح الذكاء الاصطناعي، والذي يشار إليه باختصار (AI)بأنه قدرة الآله على أداء مهام معينة تحاكي أداء البشر، مثل القدرة على التفكير والتعلم، ومعالجة البيانات والمعلومات، كما يقوم الذكاء الاصطناعي على منح الآله القدرة

على أداء المهام الصعبة، والدخول في تحدي مع العقل البشري في القدرات والمهارات المختلفة.[47]

وبالنسبة لمراحل تطور الذكاء الاصطناعى فقد كانت البداية بفكرة الآله مطلع القرن العشرين، حيث بدأ العلماء باختراع آلات تعمل بدون تدخل من البشر، وخلال الفترة ما بين (1950 – 1990)، كان اختراع الإنسان الآلى، أعقبها التفكير فى إنشاء دماغ اصطناعي، وظهور ما يعرف بـ"الروبوتات" لأداء مهام أكبر وأسرع من البشر، ثم كان التقدم الأكبر من خلال الذكاء الاصطناعى حيث يملك النظام الألي القدرة على تنسيق وتنظيم التعلم، واكتشاف الأشكال، وتفسير وتحليل المشكلات واتخاذ القرارات، وخيارات الاستدلال لتحليل وإدراك العلاقات بين الأشياء وفهم الحقائق بأنواعها .[48]

وقد شهد عام 2023 ومطلع 2024م تطورات في تقنيات الذكاء الاصطناعى منها تطبيقات الدردشة وتوليد النصوص مثل تطبيق ChatGPT لشركة Open AI، وتطبيق Bard وهو من انتاج شركة جوجل، وتطبيقات أخرى مثل Character ، Janitor AI، Dall e.، وكذلك تطبيقات معالجة الصور ومقاطع الفيديو أبرزها تطبيق Midjourney ، وتطبيق Capcut وهو تطبيق متخصص في توليد الفيديو، وتطبيقات أخرى Civital ، Crayon، Stable diffusion وهى تطبيقات خاصة بمعالجة الصور، بالاضافة إلى تطبيقات الكتابة بالذكاء الاصطناعي ومنها تطبيق Quillbot ، وتطبيق Novel AI ، وتطبيقات معالجة البيانات ومنها تطبيق.Hugging Face .

ويتفق خبراء التقنية والبرمجة على أن تطبيقات الذكاء الاصطناعي هو "مجموعة الجهود المبذولة لتطوير نظم المعلومات بطريقة تستطيع أن تتصرف وتفكر بأسلوب مماثل لقدرات البشر، بجانب تخزن الخبرات والمعارف الإنسانية في عملية اتخاذ القرارات المعقدة، وقدرة الخوارزميات على تعليم وتحليل وتفسير البيانات الضخمة، وهو ما تحتاح اليه المؤسسات الأمنية عند الكشف عن الجرائم الجنائية المعقدة.

أهداف الذكاء الاصطناعي فى العلوم الأمنية :

تكمن أهداف الذكاء الاصطناعى فى العلوم الأمنية فى التالى : [49]

- تسهم تقنيات الذكاء الاصطناعى فى أداء الكثير من المهام الأمنية، خاصة تصنيف المجرمين وتحديد المناطق الأكثر خطورة فى نسب الجريمة ، وهو ما يساعد الشرطة فى التحقيق والإثبات الجنائي وتحقيق العدالة وغيرها
- تستطيع تقنيات الذكاء الاصطناعي مساعدة إدارة البحث الجنائى فى تحديد الجاني، حيث تستطيع الخوارزميات الذكية الكشف عن الجرائم المعقدة من مسرح الجريمة ، وذلك بصورة أكثر دقة وكفاءة مقارنة بالبشر.
- تساهم تقنيات الذكاء الاصطناعي فى تقييم المحبوسين في المؤسسات الاصلاحية، ودراسة كل حالة بمفردها من خلال التقارير التى يتم إدخالها للأنظمة الخبيرة، والتى تقوم التطبيقات بتحليلها والوصول بها إلى نتيجة من شأنها الإفراج عن المتهم من عدمه .
- تستطيع تقنيات الذكاء الاصطناعي تعقب المطلوبين جنائيًا، وتحديد هوية المجرم وتحليل شخصيته وطرق التعامل معه، بجانب قدرتها علي مراجعة السجل الإجرامي للمجرم فى ثوانى معدودة ، وامكانية القبض عليه.

- تساهم تقنيات الذكاء الاصطناعي فى تقليل حوادث السيارات باستخدام نظام مبنى على خوارزميات داخل السيارة نفسها، حيث يعطى النظام تنبيهات لقائد السيارة بمرور سيارة بجانبه أو تقترب منه، وهو ما يقلل وربما يمنع الحوادث وتجعل القيادة أكثر أمنًا .
- تستطيع تقنيات الذكاء الاصطناعي الكشف عن الجرائم المعقدة، والتنبؤ ببعض الجرائم المحتملة والأماكن التى تشكل بؤرًا إجرامية مستقبلًا ، وذلك عبر خوارزميات محددة تقوم بتحليل البيانات والخروج بنتائج تسهم في الوقاية من الجرائم المتوقع حدوثها.
- تساهم تقنيات الذكاء الاصطناعي فى دعم التعلم العميق فى مجال الأمن، وهى تقنية تركز على شبكات عصبية صناعية تحاكي عملها العقل البشرى، وهى قادرة على تطوير نفسها ذاتيًا دون تدخل من البشر، حيث استطاع برنامج لشركة IBM من هزيمة بطل العالم فى لعبة الشطرنج عام 1996[50]، مما يؤكد على أن تقنية التعليم العميق المدعومة بالذكاء الاصطناعى قد تصبح بديلاً عن الخبراء والمختصين في العلوم المختلفة .

أهمية الذكاء الاصطناعي في دعم المؤسسات الأمنية : يعتمد الذكاء الاصطناعي على ثلاثة مكونات أساسية تتمثل في الأتى : [51]

- **استكمال نقص المعلومات :**حيث تستطيع تطبيقات الذكاء الاصطناعي القيام بها في ظل ندرة المعلومات. [52]
- **القابلية على التعلم** :حيث القابلية على التعلم من الخبرات والممارسات السابقة، إضافة إلى قابلية تحسين الأداء والتعلم من الأخطاء السابقة، وهذه القابلية ترتبط بالقابلية على تعميم المعلومات واستنتاج حالات مماثلة وانتقائية وإهمال بعض المعلومات وغير المفيدة .
- **قابلية الاستدلال** :وهي القدرة على استنباط الحلول الممكنة من واقع الخبرات السابقة، لاسيما المشكلات التي لا يمكن معها استخدام الوسائل التقليدية المعروفة، وتتحقق هذه القابلية بواسطة الحاسوب وتخزين جميع الحلول الممكنة إضافة إلى استخدام قوانين واستراتيجيات الاستدلال وقوانين المنطق وغيرها. [53]

دوافع تبنى الذكاء الاصطناعي فى المؤسسات الأمنية:هناك عوامل عديدة دفعت المؤسسات الأمنية نحو تبنى تقنيات الذكاء الاصطناعي منها الأتى : [54]

- **توفر إمكانية الحوسبة :** حيث أن توافر الحوسبة في المؤسسة الأمنية قد يسهم فى أداء المهام الأمنية بكفاءة عالية ، وقبل هذا التطور كانت المهام غير قائمة على الحوسبة السحابية وتحتاج إلى تكاليف باهظة.
- **البيانات الضخمة :** وذلك من خلال التعلم العميق وظهور أدوات جديدة فى جمع البيانات المُصنفة، بالإضافة إلى تَمَكن المؤسسات الأمنية من تخزين هذه البيانات ومعالجتها بسهولة، واستخراجها وقت الحاجة اليها .
- **التنافس الأمنى :** حيث تدرك المؤسسات الأمنية بشكل متزايد الميزة التنافسية وجعلها أولوية على مستوى الاجراءات التى تقوم بها، حيث يمكن أن تساعد تقنية الذكاء الاصطناعي على اتخاذ قرارات أسرع، كما يمكن للعديد من ميزايا وقدرات الذكاء الاصطناعي أن تؤدي إلى خفض التكاليف وتقليل المخاطر وتسريع وقت الوصول إلى مسرح الجريمة .

خصائص الذكاء الاصطناعي فى المؤسسات الأمنية :

تقوم تقنيات الذكاء الاصطناعي على تحسين أداء المؤسسات الأمنية عن طريق أتمتة العمليات التي كانت تتطلب الذكاء البشري فيما مضى، حيث يمكن بالذكاء الاصطناعي فهم البيانات على نطاق أوسع، بالاضافة الى الخصائص التالية: (55)

1. المساهمة فى عملية التدريب وتطوير الذات من خلال التعلم والبرمجة الذاتية.
2. تقديم الاستشارات الأمنية وتحقيق التعليم التفاعلي بكفاءة عالية .
3. تقليل أعباء البحث الجنائى والدقة فى استخراج النتائج والاستدلال المنطقى عليها .
4. توفير فرص عمل جديدة فى المؤسسات الأمنية فى مجال علوم الأدلة الجنائية الرقمية .
5. دعم مكافحة الجرائم الالكترونية والكشف عن الادلة الجنائية المصاحبة لها.
6. توفر قاعدة ضخمة من البيانات والمعلومات لا تتوفر في الكتب أو المصادر المعرفية الأخرى.
7. القدرة على التفكير والإدراك واكتساب المعرفة وتطبيقها بسرعة وبكفاءة عالية ومتقنة .
8. القدرة على التعلم والفهم من التجارب والخبرات السابقة وتوظيفها في مواقف جديدة.
9. القدرة على الاستجابة السريعة للمواقف والظروف الجديدة والحالات الصعبة والمعقدة.
10. القدرة على التعامل مع المواقف الغامضة فى ظل غياب الحقائق وفهم الأمور المرئية وإدراكها.

مجالات توظيف الذكاء الاصطناعي في المؤسسات الأمنية :

يمكن حصر تطبيقات الذكاء الاصطناعي في ثلاث مجالات رئيسية هي: تطبيقات العلوم الإدراكية، وتطبيقات الواجهة ، تطبيقات الآلات الذكية ، حيث يعتقد أكثر من 60% من صانعي القرار في المؤسسات الكبرى أن الذكاء الاصطناعي يمكن أن يساهم في تقديم الحلول لأهم المشكلات التي تواجه المجتمعات المعاصرة،(56) بدءًا من استخدامات الطاقة النظيفة وصولًا الى القضايا التي ترتبط بالأمن الوطنى، ويمكن تحديد مجالات توظيف الذكاء الاصطناعى فى المؤسسات الأمنية فى التالى: (57)

1. يقلل من مخاطر الحوادث الارهابية ورصد المخالفات المرورية عن بُعد .
2. الكشف عن الشائعات، وتحليل البيانات وتفادى عمليات النصب والاحتيال بسهولة
3. فحص الأدلة الجنائية وصيانة الأسلحة والكشف عن عمليات التجسس وغيرها.
4. الكشف عن عمليات السرقات والاختراقات وسرعة التجاوب معها بسرعة فائقة .
5. الكشف عن البضائع غير المشروعة مثل المخدرات والانشطة الارهابية وغيرها.
6. تحديد العملاء الذين يشترون المواد الكيميائية التى تستخدم فى الانشطة الارهابية .
7. استخدام بيانات شركات الشحن لتحديد الحاويات التى يرجح استخدامها فى الاتجار بالبشر.
8. رصد عمليات غسيل الأموال والاستيلاء على الحسابات البنكية ووسائل الدفع الإلكتروني
9. تحقيق انفاذ القانون وذلك من خلال المستشعرات الرقمية والبيومترية فى تنفيذ الاحكام.
10. تحديد الأراضي الصحراوية التي تزرع الحشيش والأفيون ورصد تداول المواد المخدرة.
11. تحديد جرائم نقل البيانات والاستيلاء عليها من خلال برامج ضارة وذلك بهدف التهديد والابتزاز.

12. الكشف عن الأدلة الرقمية والبصمة الوراثية والوجه والجثث مجهولة الهوية فى الحال .
13. توسيع نطاق المراقبة من خلال كاميرات عالية الدقة للتعرف على الوجوه ولوحات التراخيص على بُعد.

آليات توظيف تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية:

تعتمد المؤسسات الأمنية على تقنية التعلم عند أداء مهامها الوظيفية، وهو ما قد يساهم فى تحديد الأماكن والأوقات الأكثر احتمالاً لوقوع الحوادث والأنشطة الإجرامية ويمكن توضيح ذلك من خلال التالي : (58)

- **الشرطة الذكية :** حيث تتنوع مصادر المعلومات والبيانات التي يتم جمعها من مصادر عديدة مثل: كاميرات الجسم وقارئات لوحات السيارات وكاميرات الفيديو وأجهزة الاستشعار الذكية، ومن ثم يعتمد نجاح إستراتيجيات العمل الأمني في المستقبل على القدرة في تسخير هذه الكم الهائل من البيانات بسرعة لدعم التحقيقات وتنفيذ الإجراءات اللازمة، حيث يكون الذكاء الاصطناعي والتعلم الآلي عاملين أساسيين في التحقيقات الذكية، والتنبؤ بالجرائم، كما يمكن من خلال تحليل الأنماط وخلاصات أجهزة الاستشعار وقواعد البيانات والسجلات المخزنة، أن يساعد جهات التحقيق في تحديد الأماكن الارهابية، والعثور على الروابط الرئيسية بين المشتبه بهم، واستكشاف رؤى أخرى مخبأة في كم البيانات المتاحة .
- **الاستشعار عن بُعد :** وهو تقنية متطورة تستخدم الألياف الضوئية فى رصد واكتشاف المشكلات البيئية والصناعية، وقد توفر هذه التقنية قياسات مستمرة في الوقت الفعلي على طول كابل الألياف الضوئية، مقارنة بالمستشعرات التقليدية التي تعتمد على أجهزة استشعار منفصلة لقياس الأوضاع في نقاط محددة مسبقا. (59)

وتستخدم هذه التقنية فى رصد درجات الحرارة والضغط والأصوات ومراقبة واكتشاف الأعطال في الأعمال الصناعية الحساسة، يتم ربط المعلومات التي يبثها الاستشعار الموزع بالمعلومات المتصلة بقواعد بيانات المدينة الذكية، ومن ثم إرسال دورية إلى المكان المناسب ومعالجة المشكلات التي قد تحدث..

- **الأدلة الذكية :** كانت شرطة نيوزيلندا أول مؤسسة أمنية فى العالم تنشىء مركزًا للشرطة قائما على الأدلة، حيث تستعين الشرطة القائمة على الأدلة بالتحليل الإحصائي والبحث التجريبي للوصول إلى استنتاجات واقعية وتصحيح وتحسين سياسات وممارسات وقرارات جهاز الشرطة، اذ يلزم بجانب السلاح ومواد القانون، وسلامة الإجراءات،المعرفة بالإستراتيجيات التي ترفع مستوى عمليات مكافحة الجريمةإمكانية اتخاذ قرارات دقيقة أثناء التحقيق. (60)

التحديات التى تواجه تطبيقات الذكاء الاصطناعي فى المؤسسات الأمنية :

تعتبر تقنية الذكاء الاصطناعي أدوات قوية وفعالة في تحسين الحياة البشرية، لكنها تشكل أيضًا مخاطر على الأمن ومستقبل العمل البشرى، يقابلها إمكانيات هائلة وفرصًا مبتكرة في مجالات مختلفة، ويمكن رصد أبرز التحديات فى التالى: (61)

- **فقدان الوظائف:** تستطيع تطبيقات الذكاء الاصطناعي أتمتة العديد من المهام والوظائف التي يؤديها البشر، وقد يتسبب ذلك في فقدان بعض فرص العمل التقليدية وتعرض بعض الصناعات بأكملها للتهديد، خاصة الوظائف التي يمكن أتمتتها بسهولة وفعالية بتقنية الذكاء الاصطناعي، وهذا يمكن أن يؤدي إلى زيادة معدلات البطالة في بعض الصناعات الكبرى.

- **التهديدات الأمنية :** يشكل الذكاء الاصطناعي تحديًا أمنيًا بسبب إمكانية استخدامه في أعمال الاختراق والاحتيال والتجسس، ويمكن للقراصنة استخدام تقنيات الذكاء الاصطناعي فى اختراق أنظمة الأمان والحصول على معلومات سرية أو إلحاق الضرر بالأفراد والمؤسسات الحيوية المختلفة للدول .

- **العنصرية والتمييز :** قد يكون للذكاء الاصطناعي تأثيرات سلبية على المجتمع عندما يتم استخدامه بطرق تمييزية أو غير عادلة ، حيث يمكن للبيانات الضخمة أو التمييز الخوارزمي أن يؤدي إلى تعزيز التحيزات القائمة أو إظهار سلوك غير عادل تجاه فئات معينة من الأشخاص أو الموضوعات والرأي العام.

- **فقدان السيطرة :** في ظل تطور الذكاء الاصطناعي سوف يصبح ذات قدرات تفوق البشر، وقد يتسبب ذلك في فقدان السيطرة على النظم الذاتية واتخاذ القرارات، وقد يشكل هذا تحديًا كبيرًا فيما يتعلق بأخلاقيات الذكاء الاصطناعي وضمان أن يتم استخدامه بطرق تتوافق مع مصلحة البشرية.، والمعايير المهنية والأخلاقية المتعارف عليها .

- **التأثير الاقتصادي :** قد يتسبب الذكاء الاصطناعي في أزمات اقتصادية وفي سوق العمل، ويمكن أن ينشأ فجوة تقنية بين الأفراد والبلدان التي تستخدم الذكاء الاصطناعي والتي لا تستطيع ذلك . (62)

- **الاستخدام السيئ :** حيث يمكن استخدام الذكاء الاصطناعي لأغراض سيئة، مثل الهجمات السيبرانية والتجسس الصناعي والأنشطة الإجرامية الأخرى. (63)

- **انتهاك الخصوصية :** قد يؤدى الذكاء الاصطناعي إلى انتهاك خصوصية الأفراد، حيث يمكن لشركات الاتصالات ومزودى الخدمة جمع البيانات الشخصية وبيعها لشركات الاعلان والتسويق .

- **القرارات الخاطئة :** يمكن أن يؤدي الاعتماد الكامل على الذكاء الاصطناعي في اتخاذ قرارات خاطئة، خاصة إذا كانت الأدوات اللازمة للتحليل غير دقيقة أو تحتوي على معلومات غير كافية.

- **القضاء على الابداع :** قد يؤدي الاعتماد الزائد على الذكاء الاصطناعي إلى تراجع مهارات الإنسان وتقليل قدراته في الابداع واتخاذ القرارات وتحليل المعلومات بشكل مستقل.

- **التسلط السياسي :** يمكن استخدام الذكاء الاصطناعي كأداة للسيطرة وحشد الرأي العام نحو قضايا محددة .**مخاطر مخاطر تطبيقات الذكاء الاصطناعي فى المجال الأمنى:**

يمكن رصد أبرز المخاطر الأمنية المتوقعة عند توظيف الذكاء الاصطناعى في التالى : (64)

- **تهديد الأمن القومي :** حيث يتخوف خبراء الأمن من استخدام التقنية اثناء الانتخابات على نحو قد يُؤثر سلبًا على النتائج العامة، وكان الخداع العميق هو محور نقاش جلسة استماع بمجلس النواب الأمريكي، مما دفع عضو المجلس النواب الأمريكي "ماركو روبيو" اعتبار أن تلك التقنية تُعادل خطورة الأسلحة النووية.

- **الاحتيال والابتزاز :** لقد تسببت تسجيلاتٌ صوتيةٌ مفبركةٌ لبعض المديرين في ذيوع العمليات الاحتيالية لا سيما في الأعمال التجارية من خلال التصيد الاحتيالي، حيث تعرض الرئيس التنفيذي لإحدى شركات الطاقة البريطانية لسرقة 243 ألف دولار باستخدام مقطعٍ

صوتي مسجل لرئيس شركته الأم يَطلب منه إجراء تحويلٍ مالي طارئ، وقد كان التزييف مقنعًا إلى حدّ تصديقه، وحدث التحويل المالي بالفعل، وقد تم استخدام الخداع العميق في ابتزاز رؤساء الشركات عن طريق تهديدهم بنشر مقاطع فيديو قد تضر بسمعتهم ان لم يدفعوا أموالًا مقابل عدم النشر .

- **المقاطع المخلة بالاداب :** تم تداول بعض المقاطع الإباحية المنتجة بتقنية الخداع العميق لابتزاز الكتاب والصحفيين، كما حدث مع الصحفية "رنا أيوب"، ومن المتوقع زيادة استخدام الخداع العميق في المستقبل في عمليات الابتزاز والاحتيال مع تراجع تكلفتها المادية.

- **الهجمات السيبرانية :** حيث يمكن للمحتالين الدخول على الشبكات الافتراضية الخاصة عن طريق تزييف إحدى مكالمات الفيديو من مديري الشركات، ليخدع بها الموظفين لإفشاء كلمات السر، ما يُمكّن المحتالون والقراصنة من الحصول على بيانات الشركة ، وفي هذا السياق تتوقع شركة الأمن السيبراني "فورس بوينت (Forcepoint) "أن يستخدم مجرمو الإنترنت الخداع العميق لتوليد صور ومقاطع فيديو يُمكن توظيفها لطلب فدية، كما يُتوقع تزايد هجمات التصيد الاحتيالي من خلال نشر مقاطع فيديو تحتوي على البرامج الضارة أو تسجيل الرسائل المصممة لجذب المستخدمين إلى النقر على الروابط كجزءٍ من هجمات التصيد [65]

لقد واكب التوسع في استخدام تطبيقات الإنترنت تطورا كبيرا في ظهور وسائل حديثة لارتكاب الجرائم، فظهرت نوعية جديدة من الجرائم المستحدثة يتم ارتكابها من خلال استخدام التقنيات الحديثة ، أطلق عليها مسمى الجرائم الالكترونية، ولاشك أن هذه الجرائم تتمتع بالدقة وتهدد أمن المجتمع وسلامته ومع انتشار استخدام الإنترنت وتزايد المعلومات وأعمال التجارة الإلكترونية وغيرها .

ومع تنامى خطر هذه الجرائم وعدم فاعلية القوانين القائمة في مواجهتها، لاختلاف طبيعتها عن الجرائم التقليدية التي لها طبيعة محددة، كان لزاماً علي المؤسسات الأمنية البحث عن كيفية المواجهه ولأهمية إثبات هذه الجرائم وعدم قدرة أدلة الإثبات التقليدية علي تحقيق ذلك، أصبحت الحاجة ملحة إلي إثباتها من خلال أدلة تنتمى إلي البيئة نفسها، وهو ما فرضته الطبيعة الخاصة لتلك الجرائم، ولذا أصبح الإثبات بالأدلة الجنائية الرقمية من أبرز وسائل الإثبات، وهو ما يمكن تصنيفه علي أنه نوع جديد من الأدلة التي لها خصائصها وأساليب استخدامها.

مجالات توظيف تقنيات الذكاء الاصطناعى فى مكافحة الجرائم الالكترونية :تتعدد مجالات توظيف تقنيات الذكاء الاصطناعى فى مكافحة الجرائم وذلك من خلال التالى: [66]

– **فى مجال التحري والأدلة الجنائية** : وذلك في العديد من القضايا مثل العنف والإرهاب والمخدرات، وتجارة الأسلحة، والجثث المدفونة بعمق قد يصل الى 2.5 متر من سطح الأرض عبر الموجات الكهرومغناطيسية، والتى يتم توظيفها فى الكشف عن الأشياء المدفونة تحت الأرض مثل المخدرات والأسلحة والمفرقعات وكذلك جثث القتلى وأدوات الجرائم وغيرها، ويتسم هذا النظام بالذكاء ودقة البحث على الحاسوب، حيث يقلل من الوقت المستغرق فى كشف الأدلة، بالإضافة إلى تقليل الموارد البشرية المستخدمة فى التحرى

والكشف عن الجريمة، بالاضافة إلى قدرته على نقل الصور بسهولة إلى الحاسب الآلى ودمجها فى تقارير مصورة، ومن ثم يشيع استخدام هذا النظام فى الأماكن التى يصعب فيها عمليات الحفر والتنقيب، ومثال ذلك استخدام شرطة إحدى المقاطعات فى المملكة المتحدة تقنيات الذكاء الاصطناعى فى توقيف مئات المتهمين فى قضايا جنائية، وذلك حال وجودهم فى الأماكن التي تكثر فيها الحوادث الجنائية مثل الأسواق التجارية والبنوك والملاعب الرياضية وغيرها .

- وفى إطار ذلك أيضاً تم الاستعانة بتقنيات الذكاء الاصطناعى فى الكشف عن الحركة من خلال الجدران الصلبة بشكل سرى ومعرفة ما إذا كان هناك أشخاص في الداخل أم لا؟، وتعمل هذه التقنية من خلال موجات الراديو واكتشاف التنفس البشرى من مسافة أكثر من 50 قدماً، ويمكن تركيب هذه التقنية على الطائرات بدون طيار للاستعانة بها فى مراقبة أوكار الإرهابين فى المناطق الجبلية التى يصعب الوصول اليها، بالاضافة الى تقنية نقار الخشب وهى أحدث أجهزة التنصت اللاسلكية عن بُعد وتستخدم في حالات المراقبة والتنصت من خلال حوائط، وأسقف، وأبواب..)، وتستخدم هذه التقنية فى العمليات التكتيكية مع فرق التدخل السريع مثل إنقاذ الرهائن ومكافحة الإرهاب، وتتكون هذه التقنية إلى وحدتين الأولى تثبت بسهولة على الجدران أو الأسقف، أو فى أى أماكن غير مرئية، والوحدة الثانية هى وحدة استقبال الصوت عن بُعد من خلال موجات الراديو إلى وحدة الاستقبال ، وبالتالي سهولة تحديد موقع الشخص داخل الغرفة، ويمكن أن يعمل الجهاز 24 ساعة متواصلة في نقل الصوت وعلى مدى قد يصل إلى 50 مترًا داخل البنايات .[67]

2 - **فى مجال الدوريات الشرطية** : حيث يتم توظيف"الروبوت الأخطبوط" ، بدلًا عن الدوريات الشرطية : والذى يمكن أن يكون بديلا في المستقبل لضباط الشرطة أو حتى بديلًا عن سيارة دورية الشرطة التقليدية، واستطاع الروبوت أن يحدث ثورة في عمل الشرطة، حيث يجمع بين دور مركبة الشرطة وضباط الشرطة في تصميم واحد، من خلال استخدام مفاهيم الروبوتات المتقدمة وتقنية الذكاء الاصطناعي، والاعتماد عليها في حراسة المنشآت والشخصيات المهمة وكذلك في عملية نقل الأموال، ويمكن للشرطة الاستعانة بها أيضًا فى تنفيذ عمليات الضبط للمتهمين الخطرين، وبصفة خاصة العصابات الإجرامية المنظمة.

- وهناك ما يعرف بسيارة الشرطة الكهربائية للمطاردات "الخنفساء السوداء": وهذه السيارة ذاتية القيادة تهدف إلى الحد من عدد رجال الشرطة فى المطاردات ، ويمكن للمركبة أن تشارك في كل من المطاردات عالية السرعة وفى تنظيم الحركة المرورية والحفاظ على سلامة الضباط والأبرياء.

- وهناك ما يعرف بسيارة الشرطة المستقبلية من BMW لعام 2025: حيث تم تصميم السيارة استنادًا إلى مجموعة من المعايير من بينها السرعة وخفة الحركة وسلامة البيئة، وتم تصميم النموذج على هيكل وحدات مجمعة مبنية على تكنولوجيا الطائرات بدون طيار، ومن فوائد هذا النموذج إرسال نبضات إلى سيارة أخرى أثناء الهروب أو المطاردة وتعطلها. [68]

- وهناك ما يعرف بالمدرعة صغيرة الحجم متعددة المهام "تراك": وهذه السيارة متعددة الفوائد لرجال الشرطة، بالإضافة إلى حجمها الصغير حيث يمكن وضعها في الممرات

والمصاعد والمباني الشاهقة، وتتميز المدرعة بقدرتها العالية على المناورة فى المناطق الوعرة. (69)

3- **أنظمة الكاميرات الذكية:** تسعى الدولة إلى الاستعانة بكل ما تقدمة التكنولوجيا في مجال الجريمة، ومن هذه الآليات وضع كاميرات مراقبة بالشوارع والميادين العامة والمنشآت الحيوية، تقوم على رصد وتسجيل الأحداث على مدار الساعة ، كما تساهم فى منع وقوع الجريمة، بمجرد معرفة المجرم بوجود كاميرات تغطى المكان.

4 - **الاستعانة بكاميرات المراقبة:**

– **فى مجال المرور**: قامت وزارة الداخلية المصرية بالاستعانة بكاميرات المراقبة لتنظيم حركة المرور، والوقوف على أماكن الزحام المرورى والاختناقات المرورية وتحويلها إلى الشوارع البديلة، ورصد المخالفات المرورية ونقلها فورًا على أجهزة الكمبيوتر بإدارة المرور .

– **فى تأمين المنشآت**: تكمن أهمية كاميرات المراقبة فى تأمين المنشآت المهمة مثل الوزارات وأقسام الشرطة والبنوك والمدارس والنوادى الاجتماعية والمساجد والكنائس..، حيث تقوم على رصد المخالفات التى تقع فيها أو فى محيطها، فالاعلان عن وجود كاميرات مراقبة يجعل الجاني يفكر قبل تنفيذ سلوكه الإجرامي، وضبطه وتقديمه للعدالة. (70)

– **فى تعقب المجرمين**: وذلك عن طريق المراقبة الإلكترونية باستخدام Telemetric System وهى وسيلة لمراقبة الأشخاص، والحصول على معلومات تتعلق بحالتهم العصبية بواسطة موجات كهربائية، وفي هذه الحالة يمكن إبلاغ رجل الشرطة الذي يتابعه، بل يمكن أن يتم إرسال إشارة كهربائية للمجرم للعزوف عن الفعل الإجرامى . (71)

- وهناك نموذج حديث يستعين به رجل الأمن فى الدورية المترجلة حيث يتم تثبيت **كاميرا مراقبة** على نظارة الوجه أو على الجاكت الذي يرتديه، ومن خلالها يتم تصوير الأحداث المحيطة بفرد الأمن ، وفضلا عن تحديد الأماكن التى يتم المرور بها خاصة في الأماكن الصحراوية من خلال تقنية ما يعرف GPS.

- وهناك ما يعرف **بالخوذة الذكية،** وهى أشبه بغطاء الرأس، إلا أنها تمتلك نظامًا يساعد على زيادة الرؤية بأكثر من 65% ، وقد تم تصميمها لتحسين أوقات الاستجابة في حالات الطوارئ ، كما تضم الخوذة قناة راديو ومولف تردد آلى مما يسمح للضابط بالتحدث إلى قيادة الشرطة أو أقرب مستشفى أو المطافئ، ويمكن للخوذة الذكية أيضاً إرسال لقطات فيديو حية إلى مراكز الشرطة فى الحال بما يشبه البث المباشر. (72)

- وهناك ما يعرف **بالحزام الذكى لضباط الشرطة**: وهو يقوم بتسجيل عدد مرات خروج سلاح من حافظة الضابط ويرصد إحداثيات الضابط والسرعة في مرات مختلفة، وهذه التقنية يمكن أن تحمل رجل الشرطة مسئولية عدم استخدام السلاح إلا في حالات الضرورة القصوى، مما يساعد على إبقاء رجال الشرطة مسئولين أمام جهات التحقيق والتفتيش لديهم (73).

- وهناك **الكبسولة الذكية**: عند قيام الدورية الأمنية بمطاردة أحد اللصوص أو أحد المطلوبين أثناء قيامه بالفرار باستخدام السيارة، تقوم السيارة الأمنية بإرسال كبسولة لاصقة إلكترونية على السيارة المطلوب ضبطها، ومن خلال تلك الكبسولة يمكن تحديد مكان السيارة فى حالة

تمكن قائدها من الفرار من الدورية الأمنية، وإيقاف الدائرة الكهربائية للسيارة الهاربة فتتوقف في الحال ويتم ضبطها.

- وهناك ما يعرف **بالكاميرات الحرارية**: وهى تستخدم فى حالة الظلام الدامس، ولها القدرة على تحديد الأشخاص والسيارات والحيوانات من بُعد، وإصدار التنبيهات وقت الحاجة، ويتم تركيبها في دوريات الشرطة التى تعمل في المناطق النائية، وتعمل التقنية الذكية بنظام التصوير الحرارى عالى الدقة، ومتعدد الأطياف (MSX)، والكاميرا مدمجة وخفيفة الوزن ومقاومة للحرارة والماء، وتوفر رؤية واضحة عند حدوث الحرائق وتصاعد الدخان الكثيف وصعوبة الرؤية. (74)

5- **في مجال تحديد الهوية في المطارات** ، حيث تقوم التقنية الحديثة بطبع بصمة الشخص على جهاز يشبه الهاتف المحمول، ويتم التحقق من البيانات من خلال قاعدة البيانات المركزية للشرطة والمعمل الجنائى، ويمكن الاستفادة من تلك التقنية في ضبط المطلوبين فى أحكام قضائية أو هاربين من قضايا قتل وسرقة وغيرها. (75)

6- **في مجال مكافحة الشغب**: حيث تتم الاستعانة بتقنية الذكاء الاصطناعى فى التنبؤ بأعمال الشغب، حيث يمكن لخوارزميات التعلم الآلي، ومن خلال تحليل التغريدات على"تويتر"،أن تحدد أماكن الشغب قبل وصول الخبر مراكزالشرطة، ويمكنها التنبؤ بالأماكن التي ستنتقل إليها أعمال الشغب. (76)

7- **كشف الجرائم والتنبؤ بها**: وذلك عن طريق خوارزميات برمجية يتم إعطاؤها بيانات محددة، وتقوم بتحليل تلك البيانات والخروج بنتائج غاية فى الأهمية، تساعد في الاستعداد والوقاية من الجرائم المتوقع حدوثها.

- وهناك ما يعرف ببصمة المخ: وهى تقنية تقوم على مسح الموجات الدماغية من خلال تقنية خاصة بتحليل الإشارات التى يصدرها المخ، حيث تعتمد على المعلومات المخزونة في عقل المجرم وما تحويه من تفاصيل وأحداث ووقائع الجريمة التي ارتكبها .

- هناك ما يعرف بجهاز استشعار Bricks Tream 3D"، حيث يقوم بدمج البيانات التي يتم جمعها في الوقت الحقيقى، وتوفير منصة مشتركة لجمع مجموعة واسعة من البيانات التحليلية لسلوك المجرمين، ويوفر جهاز الاستشعار مزايا متعددة عن أجهزة جمع المعلومات التقليدية ومنصات الفيديو التحليلية، مما يتيح تحليلات السلوك المتطور التى تتجاوز قدرات العد الأساسية . (77)

8- **فى المؤسسات العقابية**: تستطيع تقنيات الذكاء الاصطناعي القيام بمهام تقييم سلوك المساجين في المؤسسات العقابية، ودراسة حالاتهم من خلال التقارير التي يتم إدخالها للأنظمة الأمنية، وتقوم بتحليلها والوصول إلى قرار بشأن الإفراج الشرطي عن المتهم أو إكمال العقوبة. (78)

9- **في مجال تنفيذ الأحكام** : وتقوم هذه التقنية على السماح للمحكوم عليه بالبقاء في منزله ، حيث تتم المراقبة بواسطة جهاز يشبه ساعة اليد أو سوار مثبت في معصمه أو أسفل قدمه، ومن هنا جاءت تسميه هذا الأسلوب بالسوار الإلكتروني.

10- **تقنية اللوحات الإلكترونية** : وفيها يتم تقدم معلومات لشرطة المرور عن لوحات السيارات بدقة ومراجعة بيانات السيارة المبلغ بسرقتها، حيث ابتكرت إحدى الشركات

العالمية Compliance Innovations شريحة إلكترونية تسمى R Plites، تحتوى الشريحة على معلومات حول رقم الهيكل الداخلى للسيارة، والتعريف بمالك السيارة والمخالفات السابقة ومعلومات الاتصال، ويمكن قراءتها على بعد 100 متر باستخدام قارئ خاص، ومن المزايا التي توفرها لوحات الترخيص الرقمية، حيث ترسل إشارة لمالكها فى حالة السرقة وإخطار الشرطة بذلك فورا. (79)

تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية :

ومن واقع توظيف وزارات الداخلية العرب لتطبيقات الذكاء الاصطناعي يمكن رصد التالى : (80)

- تكنولوجيا الواقع الافتراضي والمعزز: تُستخدم تقنية الواقع الافتراضي والواقع المعزز لمحاكاة الهجمات الإرهابية ، وهذه التقنية هي نتاج محاكاة تجربة المعارك القتالية باستخدام أجهزة الحاسوب لخلق بيئة ثلاثية الأبعاد، مما يسمح للمستخدم بتجربة عوالم افتراضية فريدة من نوعها، مثل أن يكون مقاتلاً في معركة مع البقاء ضمن حدود مجال التدريب الخاص به.

ويمكن للمستخدم أن يكون جزءًا من هذه التجربة، والتنقل داخلها، والتفاعل معها من خلال أجهزة خاصة، في المقام الأول نظارات الواقع الافتراضي، التي تساعده على الاندماج بشكل أعمق في التجربة.

أما بالنسبة للواقع المعزز، فهو تجربة تقوم بتكرار أجهزة الحاسوب، ولكنها تنقل مناظر ثنائية وثلاثية الأبعاد مع شاشة تتحد مع محيط المستخدم الحقيقي لإنتاج واقع عرض مركب.

وفي الواقع الافتراضي، يكون المستخدم في عالم آخر، بينما في الواقع المعزز، يكون المستخدم في بيئته الخاصة، ولكن مع تأثيرات إضافية في كل سيناريو .

وقد أدى التقدم التكنولوجي في البلدان العربية إلى تحسين عمل قوات الشرطة من خلال زيادة اعتمادها على التكنولوجيا واستخدامها، وفي العصر الحديث تطورت المجتمعات وأصبحت أكثر ترابطاً، مما أدى إلى وجود بيئة جديدة يجب أن تعمل فيها وكالات إنفاذ القانون، فيما ساهمت التقنيات الحديثة أيضًا فى التنسيق الدولي بين المؤسسات الأمنية على نطاق عالمي، والاستقلال المؤسسي ضروري للتعاون الدولي بين أجهزة الشرطة، بالإضافة إلى التطورات في أنظمة الاتصالات والنقل، تشمل هذه التقنيات أيضًا تطور العديد من إجراءات تحديد الهوية الجنائية.

- الدوريات الذكية : اهتمت المؤسسات الأمنية العربية بادراج سيارات شرطة ذكية مزودة بأجهزة تحكم عن بُعد وكاميرات رادار، وترتبط بغرفة عمليات الشرطة المركزية، حيث تساعد الدوريات الذكية أفراد الشرطة في التعامل مع زيادة عدد السيارات على الطرق ، وهو ما يعزيز من ثقافة السلامة المرورية وفرض سيادة القانون. (81)

- الكاميرات الملحقة بالزي العسكري : وهى تعنى امكانية توظيف الكاميرات الملحقة بملابس ضباط الشرطة ، حيث تساعد مراجعة تسجيلات الكاميرا من الفيديو الضباط على جمع الأدلة وتقليل الأخطاء، فضلاً عن زيادة ثقة المجتمع وتحسين المساءلة والشفافية.

أولاً: التجربة السعودية فى تطبيقات الذكاء الاصطناعى فى المجال الأمنى : (82)

تُعد الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA) هيئة حكومية سعودية أنشئت بأمر ملكي في 30 أغسطس 2019، وترتبط مباشرةً برئيس مجلس الوزراء "ولى العهد

الأمير محمد بن سلمان"، ويلحق بها المركز الوطني للذكاء الاصطناعي، ومكتب إدارة البيانات الوطنية اللذين تم انشاؤهما معها، ويرتبطان بها تنظيميًا، إضافةً إلى مركز المعلومات الوطني.

وفى اطار ذلك بدأت المؤسسة الأمنية السعودية فى تدشين"الهيئة الوطنية للأمن السيبراني" و"وزارة الاتصالات وتقنية المعلومات والأكاديمية السعودية الرقمية، والاتحاد السعودي للأمن السيبراني والبرمجة والدرونز، واتجهت الجامعات السعودية نحو تقديم خطط تطويرية متخصصة؛ تستهدف تأهيل الكوادر الوطنية في تخصص الذكاء الاصطناعى لتفادى عمليات التخريب التى تتعرض لها المنشآت الحيوية السعودية كل عام تقريباً .

وفي 26 مارس 2020 قامت الهيئة بتشغيل أول قمة افتراضية لمجموعة العشرين فى الرياض ، وكذلك قامت ببناء منظومة الاتصال المرئي الآمن لعدد من الجهات الحكومية واتاحة امكانية عقد اجتماعاتها عن بُعد، كما دمجت ووحدت أكثر من 80 هيئة حكومية تعمل فى مجال المعلومات والبيانات .

أما أكاديمية سدايا فهي إحدى مبادرات **الهيئة السعودية للبيانات والذكاء الإصطناعي** التي تستهدف دعم وتطوير الكفاءات الوطنية العاملة في القطاعين الحكومي والخاص عن طريق قيادة العديد من البرامج والأنشطة الواعدة والمتنوعة بالتعاون مع الجهات الرائدة في مجالي البيانات والذكاء الإصطناعي لبناء القدرات والكفاءات المناسبة لسوق العمل .[83]

وانعكست الإنجازات التي حققتها المملكة في مجال الذكاء الاصطناعي وتطبيقاته على رقمنة الخدمات الحكومية المقدمة للمواطنين والمقيمين عبر تطبيقات متقدمة مثل: تطبيق أبشر الذي تشرف عليه وزارة الداخلية، والذى سهّل على مستخدميه الحصول على الخدمات الحيوية التي يحتاجها الإنسان في حياته بمجرد الضغط عليه، كما قدمت سدايا تطبيق توكلنا خدمات وغيره من التطبيقات الخدمية التي استفاد منها المواطن والمقيم، وأسهمت هذه الأدوار الناجحة في تفعيل دور الشركات الصغيرة والمتوسطة ورواد الأعمال للمساهمة في بناء الوطن ورفعته وذلك في إطار عمل حكومي منظم بالتعاون مع القطاع الخاص بما يتوافق مع رؤية السعودية 2030م، كما أطلق المركز الوطني للذكاء الاصطناعي في سدايا نظام"صوتك" المتقدم لتحويل الكلام إلى نصوص اعتماداً على تقنيات التعرّف على الصوت بالتعاون مع الشركة السعودية للذكاء الاصطناعي (سكاي) المملوكة بالكامل لصندوق الاستثمارات العامة . [84]

كما اعلنت السعودية عن مدينة المستقبل "ذا لاين" التي تُعد اول مدينة رقمية في كيفية تخطيط المدن خلال الـ150 سنة القادمة، وكيفية تطويع المملكة لحلول الذكاء الاصطناعي والبيانات لبناء المجتمعات المستدامة، حيث الاستفادة من البيانات الجغرافية المكانية في إيقاف التصحر والزراعة العشوائية والمحافظة على البيئة، وفى المقابل تتصدر شركة "أرامكو" السعودية استخدام صناعي للبيانات والذكاء الاصطناعي حيث استخدمت حساسات الميثان وإنترنت الأشياء والبيانات والذكاء الاصطناعي لتقديم أفضل الأنشطة في قطاع التكرير والكيميائيات والتسويق للعالم.

وفي الجانب الأكاديمي برز دور جامعة الملك عبد الله للعلوم والتقنية (كاوست) حيث تم تأسيس مركز للتميز في علوم البيانات والذكاء الاصطناعي مع سدايا، إضافة إلى أدوار

علمية أخرى تقوم بها الجامعات الحكومية والخاصة في سبيل تطوير مناهجها الأكاديمية التي تدّريس علوم الذكاء الاصطناعي بمختلف مجالاته، وهو ما قد يسهم في بناء جيل سعودي قادر على التعامل مع هذه التقنيات بكل احترافية . (85)

وفى السياق استثمرت وزارة الصحة السعودية الذكاء الاصطناعي بالتعاون مع سدايا فى إنشاء مركز للتميز في الذكاء الاصطناعي يتم من خلاله تحديد الأمراض ذوات الأولوية (مثل سرطان الثدي، والسكري) وتطوير الحلول الذكية للمساهمة في التنبؤ المبكر بمثل هذه الأمراض.

كما أطلقت وزارة البيئة والمياه والزراعة بالشراكة مع سدايا أول مركز متخصص في المملكة والشرق الأوسط لحلول وتطبيقات الاستدامة "مركز الذكاء الاصطناعي في البيئة والمياه والزراعة"، وبرنامج "الكوكب الذكي"، وذلك ضمن الأولويات الوطنية لإيجاد حلول مبتكرة للمساعدة في الاستفادة من إمكانات الموارد غير المستغلة واستدامتها عبر تطبيق أحدث تقنيات الذكاء الاصطناعي.

كما اعتمدت الهيئة العامة للطيران المدني السعودية تكنولوجيا الفحص الأمني بالذكاء الاصطناعي (ICMOR) للاستخدام التشغيلي في مطارات المملكة، بعد عقد شراكة مع مجموعة عالمية متخصصة في ذلك المجال خلال أعمال القمة العالمية للذكاء الاصطناعي التي نظمتها الهيئة السعودية للبيانات والذكاء الاصطناعي "سدايا" بالرياض خلال الفترة من 13 إلى 15 سبتمبر 2022م .(86)

وفى إطار ذلك استضافت السعودية قمة عالمية تحت شعار"الذكاء الاصطناعي لخير البشرية" برعاية الأمير محمد بن سلمان ولى العهد فى أكتوبر2021، ضمت كبريات الشركات المتخصصة فى الذكاء الاصطناعى، وتناولت أساليب توظيف الذكاء الاصطناعى فى مجال أمن الأفراد والمؤسسات وقدرتها فى تحقيق رفاهية الشعوب والحد من الجرائم فى العالم، يقابل ذلك تدشين العديد من المدن الذكية تعتمد فى الأساس على تطبيقات الذكاء الاصطناعى والتحول الرقمى فى المؤسسات الحكومية.

وعلى المستوى الاجرائى تخضع مواقع التواصل الاجتماعي في المملكة لنظام مكافحة جرائم المعلومات بناء على القرار الصادر بالمرسوم الملكي عام 1428هـ الذي يعرف الموقع الإلكتروني بأنه "مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد"، حيث أوضح نظام مكافحة الجرائم المعلوماتية التي يتم من خلالها إثبات جرائم النشر عبر مواقع التواصل الاجتماعي، وذلك في المادة التي تنص على أن تقوم هيئة الاتصالات وتقنية المعلومات بتقديم الدعم والمساعدة الفنية للجهات الأمنية خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة، خاصة أن هيئة الاتصالات لديها من الوسائل والتقنيات ما يكفل إثبات أو نفي الجريمة عبر مواقع التواصل الاجتماعي . (87)

وعلى الرغم من وجود النظام الرادع لجرائم الانترنت فى المملكة، إلا أن المملكة تتصدر المراكز الأولى عالمياً في عدد الهجمات الالكترونية وخاصة على المنشأت النفطية والمؤسسات الحيوية، ففي عام 2010م تعرض الموقع الخاص ببنك الرياض السعودي لهجوم من جانب أحد قراصنة الإنترنت، كما وقع في 2011م هجوما الكترونيا أخر على وزارة الخارجية السعودية، والذي ترتب عليه تسريب عدد من الوثائق المهمة لعملاء

دبلوماسيين، كما تعرضت جامعة الملك سعود عام 2012 للقرصنة على يد مجهول وسرقة قاعدة بيانات الجامعة والتى تحوي 812 مستخدمًا، وقد تضمنت تلك البيانات أرقام الهواتف المحمولة، والعناوين، وكلمات المرور، أما أشد انوع الهجوم كان عام 2012 عندما تعرضت شركة أرامكو للبترول لتخريب أكثر من 30 ألف كمبيوتر في الشركة بفيروس دمّر بيانات ومسح أقراصًا صلبة في أجهزة الحاسب، ويعتقد أنه كان يهدف لوقف إنتاج البترول في مايو 2013 ، وفي نهاية مايو 2015 تمكن أحد قراصنة الإنترنت من الهجوم على شبكات الجامعات السعودية وقام بسرقة العديد من المعلومات منها، نتائج نحو 4000 طالب، وفي أغسطس 2015 قام فريق سايبر أوف إيموشن، بقرصنة أكثر من 24 موقعًا حكوميًّا سعوديًّا على الإنترنت، اعقبها هجوماً من تنظيم الدولة داعش على شبكة كمبيوتر حكومية تضم بيانات الموظفين العاملين بها، منها أسماؤهم وأرقام هواتفهم وعناوين البريد الإلكتروني خاصتهم . (88)

وأثبتت إحصائيات مجلس التعاون الخليجى تصدر المملكة المركز الأول على مستوى دول الخليج العربي في التعرض للجرائم الالكترونية وذلك وفقاً لما ذكرته شركة (تريند مايكرو) إلى وجود أكثر من 700 ألف حالة انهيار نظامي خلال تسعة شهور فقط في السعودية بنسبة 64% . (89)

ويعرف النظام السعودى بعضاً من أنواع تلك الجرائم منها الدخول غير المشروع إلى موقع إلكتروني أو الدخول إلى موقع إلكتروني بهدف تغيير تصاميم هذا الموقع أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه، إساءة استخدام الهواتف الذكية المزودة بكاميرا أو ما في حكمها للمساس بالحياة الخاصة للأفراد بقصد التشهير وإلحاق الضرر بهم عبر وسائل الاتصال المختلفة، كأدنى عقوبة تذكر في النظام. وفرض النظام عقوبة بالسجن مدة لا تزيد عن عشر سنوات وبغرامة مالية لا تزيد عن خمسة ملايين ريال أو بإحداهما، على كل شخص ينشئ موقعا للمنظمات الإرهابية على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات تلك المنظمات أو ترويج أفكارها أو نشر كيفية صنع المتفجرات وما يتم استخدامه في الأعمال الارهابية، كأقصى عقوبة تذكر في النظام. (90)

وتطبيقاً لذلك ظهر أول حكم قضائي لأول جريمة الكترونية في المملكة والذي صدر من المحكمة الجزئية في الإحساء، حيث تم الحكم على شاب سعودي بالسجن 21 شهرا والجلد 200 جلدة بالإضافة لغرامة مالية قدرها 50 ألف ريال جراء قيامه باختراق البريد الالكتروني لفتاة سعودية والاستيلاء على صورها الخاصة الموجودة به وتهديدها بنشر صورها إذا لم تستجب لمطالبه، وكان ذلك نتيجة قيام الفتاة برفع دعوى ضد الشاب انتهت بصدور هذا الحكم. (91)

ومع التزايد الكبير في حجم البيانات والمعلومات الكيميائية وربطها مع تقنية المعلومات والحوسبة الرقمية تم استحداث برامج علمية حديثة فى الجامعات السعودية سوف تُسهم في إجراء العمليات الحسابية لحل المعادلات والنظريات الكيميائية، وتسمح بالتوقع لنواتج التفاعلات، وكذلك تطوير الأساليب الإحصائية لتحليل البيانات الكيميائية، والمساعدة في تحليل المركبات والأطياف الكيميائية، ومثال على ذلك قدرة الطرق الإحصائية على التعرف

على عدد من أنماط من المركبات أو التعرف عليها من خلال المقارنة الطيفية بقواعد البيانات. (92)

الإستراتيجية الوطنية للتحول الرقمي في المملكة .

جاء التوجيه الملكي للحكومة بإعداد إستراتيجية للإعلام الوطني بمختلف أشكاله؛ المرئي، والمقروء، والمسموع، والإلكتروني، تقوم على قاعدتي الحريّة والمسؤولية، وتأخذ بعين الاعتبار متغيرات العصر من أدوات جديدة للاتصال، تأكيداً لدور الإعلام المتقدّم وتكريساً لشراكة كافة القطاعات المعنيّة والمتّصلة في صياغة ملامح الإعلام الوطني المطلوب، حيث دشنت المملكة العربية السعودية استراتيجية جديدة للتحول الرقمى تتضمن ثلاثة محاور هى : (93)

خطة العمل الأولى: 2006-2010: حيث سعت إلى أن يتمكن المواطن السعودى بنهاية عام 2010م، من أي مكان وفي أي وقت من الحصول على الخدمات الحكومية بشكل كامل من خلال الكثير من الوسائل الإلكترونية الآمنة.

خطة العمل الثانية: 2012-2016: حيث سعت إلى تمكين المواطن السعودى من استخدام خدمات حكومية فعالة بطريقة آمنة ومتكاملة وسهلة من خلال قنوات إلكترونية متعددة بالمؤسسات الحكومية المختلفة .

خطة العمل الثالثة: 2020-2024: وهي خطة العمل الحالية والتي تسعى للوصول إلى مفهوم "الحكومة الذكية" فى كل قطاعات المملكة .

ثانياً: التجربة المصرية فى تطبيقات الذكاء الاصطناعى فى المجال الأمنى :

شهدت مصر خطوات متسارعة للنهوض والتنمية والتحديث فى قطاعاتها الحكومية مثل شبكة الطرق التي أنشأتها الدولة لرفع كفاءة النقل والمواصلات مما سيكون له آثار اقتصادية كبيرة على التجارة والصناعة وحركة السكان داخل البلاد، وفى خطوة مهمة للنهوض بالبلاد واللحاق بركب الدول المتقدمة أعقبها إنشاء العاصمة الإدارية لتكون أول عاصمة ذكية في العالم تحديث العمل في الهيئات والمصالح الحكومية التي ستنتقل للعاصمة الإدارية، للانتقال إلى عصر الرقمنة والذكاء الاصطناعي.

وتأتى مصر في المرتبة الثانية إفريقيا بعد موريشيوس وفقا لتقرير مؤشر جاهزية حكومات دول العالم لتطبيقات الذكاء الاصطناعي لعام 2022 ، مقارنة بتقرير عام 2019 الذى أدرج مصر في المركز الثامن على مستوى إفريقيا، وفي المركز 111 من بين 194 دولة، والذى كشف عن تقدّم مصر 55 مركزًا في مؤشر "جاهزية الحكومة للذكاء الاصطناعي"، كما ذكر تقرير مؤشر المعرفة العالمي تقدم مصر من المركز 72 عام 2020 إلى المركز 53 عام 2021، ويأتي اهتمام الدولة ممثلة في الحكومة بالتحول الرقمي في العديد من القرارات والصور التنفيذية وتطبيق قرار التعامل في كافة الجهات الحكومية من خلال الدفع الإلكتروني، لتستكمل الدولة مسيرتها نحو الرقى بالخدمات المقدمة للمواطنين بالعمل على الاستراتيجية الوطنية للذكاء الاصطناعي لتوظيفه في المجالات الحيوية للبلاد. (94)

وترتكز الاستراتيجية الوطنية للذكاء الاصطناعي في مصر على ثلاثة محاور أساسية هى التعليم والتدريب، ثم الاستفادة العملية من حجم البيانات المتاحة، وإتاحة تلك البيانات للقطاع الخاص، حيث يبرز دور الذكاء الاصطناعي في التحول الرقمي كعامل محفز لحل مشاكل

البيئة والتحول إلى بيئة نظيفة .(Green) وكذلك استخدام تقنيات الذكاء الاصطناعي فى بناء المدن الجديدة وتحويل المدن الحالية إلى ذكية طبقاً للمعايير الدولية.

وانطلاقا نحو التحول الرقمي والتوسع في استخدام تطبيقات الذكاء الاصطناعي فى مصر، تم انشاء مركز الدراسات الأمنية والاستراتيجية عام 2021، لرصد وتحليل الظواهر الاجرامية المستحدثة باستخدام أحدث التطبيقات الالكترونية، والتي تسهم في بناء قاعدة من البيانات، بما يخدم عملية اتخاذ القرار الأمني، كما يضم المركز محطة داخلية يمكن من خلالها متابعة 8 قنوات إخبارية في آن واحد، لرصد وتحليل ما يبث من أخبار تتعلق بالشأن الأمني والقضايا القومية ذات الصلة، ليضاهي بذلك المراكز البحثية المناظرة اقليما ودوليا، حيث بدأت إدارات الشرطة المصرية بشكل روتيني في مسح وجوه الأشخاص أو محاولة تحديد المشتبه بهم من خلال مطابقة بيانات الصور أو الفيديو مع قواعد البيانات التي تحتوي على صور للذين سبق القبض عليهم ومحاكمتهم، ويعاقب القانون المصرى الاختراق المجرد الذي لا يهدف مرتكبه سوى الدخول غير المشروع للنظام الآلي أو الاختراق الموصوف الذي يهدف مرتكبه لإحداث تغيير في البيانات والمعلومات سواء بالسرقة أو التغيير أو الحذف أو الإضافة، كما أن قواعد القانون المصري قابلة -جزئيا- لاستيعاب بعض الجرائم التي ترتكب من خلال هذه الأنظمة عبر اختراقها، منها روبوتات المركبات ذاتية القيادة من أجل تنفيذ عمليات قتل أو إصابات أو هجمات إرهابية أو خطف راكب أو انتحال صفة الغير أو جرائم التزوير والنصب بأنواعها.

المبحث الثانى :عرض وتحليل بيانات الدراسة ومناقشة نتائجها:

1- المتغيرات الديموجرافية لعينة الدراسة :

جدول رقم (1)

خصائص عينة الدراسة

المتغير	الفئات	العدد	النسبة المئوية
من حيث النوع	ذكر	84	79.30
	أنثى	22	20.70
من حيث العمر- السن	من 30 إلى أقل من40 عام	47	44.30
	من 40 إلى أقل 50 عام	29	27.40
	أقل من 30 عام	25	23.60
	من 50 عام فأكثر	5	4.70
من حيث الرتبة الوظيفة	موظفون مدنيون	47	44.3
	ضابط وجنود	35	33.0
	قيادة شرطية	24	22.6
من حيث جهه العمل	قطاع أمن المعلومات	35	33.0
	قطاع الجوازات	19	17.9
	قطاع الأمن العام	17	16.0
	قطاع مكافحة المخدرات	12	11.3
	قطاع الأمن الوطنى	7	6.6
	قطاع الدفاع المدني	7	6.6
	قطاع المرور	7	6.6
	قطاع السجون	2	1.9

المتغير	الفئات	العدد	النسبة المئوية
من حيث سنوات الخبرة	من 10 سنوات إلى أقل 20 سنة	36	34.0
	من 20 سنة فأكثر	32	30.20
	أقل من 5 سنوات	20	18.80
	من 5 سنوات إلى أقل من 10 سنوات	18	17.0
من حيث متغير الدولة	مصر	53	50.0
	السعودية	53	50.0
اجمالى العينة		**106**	

من حيث النوع : تظهر بيانات الجدول السابق أن (84) من عينة الدراسة جاءت من الذكور وذلك بنسبة (79.30)، بينما جاءت الإناث بنسبة (20.70) ، وهو ما يفسر طبيعة العمل فى المؤسسات الأمنية العربية التى تفضل الذكور عن الإناث فى غالبية قطاعاتها، ويرى الباحث أن الواقع الراهن يثبت استحداث وظائف مدنية وعسكرية فى قطاعات وزارة الداخلية تناسب قدرات ومهارات النساء مثل قطاعات السجون وأمن المطارات والموانىء وقطاع الجوازات وغيرها .

من حيث العمر : يتضح من الجدول السابق أن (47) من أفراد عينة الدراسة يمثلون ما نسبته (44.3) من إجمالي عينة الدراسة الذين تتراوح أعمارهم من (30 عام إلى أقل من 40) عاما ، وهم الفئة الأكثر من أفراد عينة الدراسة، في حين أن (29) منهم يمثلون ما نسبته(27.4) من إجمالي أفراد عينة الدراسة بلغت أعمارهم من (40 إلى أقل من 50)عاماً ، مقابل (25) منهم يمثلون ما نسبته(23.6) أعمارهم أقل من 30 عام، و(5) منهم يمثلون ما نسبته (4.7) من إجمالي أفراد عينة الدراسة أعمارهم من 50 عام فأكثر، وهو الأمر الذى يفسر اهتمام المؤسسات الأمنية العربية بالأعمار الأصغر باعتبارها تمتلك القدرة على فهم وتشغيل أدوات التقنية الحديثة بكفاءة عالية.

من حيث الرتبة الوظيفية : يتضح من الجدول السابق أن (47) من أفراد مجتمع الدراسة يمثلون ما نسبته (44.3) من إجمالي عينة الدراسة طبيعة وظيفتهم (أفراد، صف ضباط)، وهم الفئة الأكثر من أفراد مجتمع الدراسة، في حين أن (35) منهم يمثلون ما نسبته(33.0) من إجمالي أفراد مجتمع الدراسة طبيعة وظيفتهم ضباط، و(24) منهم يمثلون ما نسبته(22.6) من إجمالي أفراد مجتمع الدراسة طبيعة وظيفتهم موظفين مدنيين.

من حيث جهه العمل : يتضح من الجدول السابق أن (35) من أفراد مجتمع الدراسة يمثلون ما نسبته (33.0) من إجمالي عينة الدراسة جهة عملهم قطاع أمن المعلومات، وهم الفئة الأكثر من أفراد مجتمع الدراسة، في حين أن (19) منهم يمثلون ما نسبته (17.9) من إجمالي أفراد مجتمع الدراسة جهة عملهم قطاع الجوازات، مقابل (17) منهم يمثلون ما نسبته(16.0) من إجمالي أفرد مجتمع الدراسة جهة عملهم قطاع الأمن العام، و(12) منهم يمثلون ما نسبته (11.3) من إجمالي أفراد مجتمع الدراسة جهة عملهم قطاع مكافحة المخدرات، و(7) منهم يمثلون ما نسبته (6.6) من إجمالي أفراد مجتمع الدراسة جهة عملهم قطاع الأمن الوطنى، و(7) منهم يمثلون ما نسبته (6.6) من إجمالي أفراد مجتمع الدراسة جهة عملهم فى كل من قطاع الدفاع المدنى وقطاع الإدارة العامة للمرور، و(2) منهم يمثلان ما نسبته (1.9) من إجمالي مجتمع الدراسة جهة عملهم قطاع السجون .

من حيث سنوات الخبرة : يتضح من الجدول السابق أن (36) من أفراد مجتمع الدراسة يمثلون ما نسبته(34.0) من إجمالي عينة الدراسة سنوات خبراتهم من 10 سنوات إلى أقل من 20 سنة، وهم الفئة الأكثر، ويشكلون ما يقرب من (ثلثي) أفراد مجتمع الدراسة، في حين أن (32) منهم يمثلون ما نسبته (30.2) سنوات خبراتهم من 20 سنة فأكثر، مقابل (20) منهم يمثلون ما نسبته(18.9) من إجمالي أفراد مجتمع الدراسة سنوات خبراتهم أقل من 5 سنوات، و(18) منهم يمثلون ما نسبته (17.0) سنوات خبراتهم من 5 سنوات إلى أقل من 10 سنوات

من حيث الدولة : يتضح من الجدول السابق تساوى عينة الدراسة (50%) وفق متغير الدولة وجاء اجمالى حجم العينة (106) مفردة، موزعة على النحو التالى: (53) من خبراء الأمن فى مصر، ومثلهم (53) من خبراء الأمن بالمملكة العربية السعودية، وذلك وفق العينة العمدية التى اعتمد عليها الباحث فى اطار جمع المعلومات عبر صحيفة الاستبيان والمقابلات المقننة، وقد جاء اختيار مجتمع الدراسة لأسباب عديدة منها أسباب وظيفية حيث يعمل الباحث بإحدى الجامعات السعودية الأمنية، يقابلها أسباب مكانية تتعلق بمحل اقامة الباحث فى مصر، بالاضافة إلى سعى كل من دولتى الدراسة إلى توظيف تطبيقات الذكاء الاصطناعى فى المؤسسة الشرطية والعدلية .

2- مدى متابعة المبحوثين لتطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية :

جدول رقم (2)

مدى متابعة المبحوثين لتطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية

مدى متابعة المبحوثين	التكرار	النسبة
دائماً	88	83.0
أحيانا	10	9.5
نادرا	8	7.5
المجموع	**106**	**100**

يتضح من الجدول السابق أن (88) من أفراد مجتمع الدراسة يمثلون ما نسبته(83.0) من إجمالي عينة الدراسة يتابعون دائماً الجديد بتطبيقات الذكاء الاصطناعى فى القطاعات الأمنية، وهم الفئة الأكثر من أفراد مجتمع الدراسة، بينما (10) منهم يمثلون ما نسبته (9.5) من إجمالي أفراد مجتمع الدراسة يتابعون أحياناً ، وأخيراً (8) منهم يمثلون ما نسيته (7.5) يتابعون نادراً، وهو ما يعنى أن ارتفاع مؤشرات المتابعة دائماً وأحياناً بنسبة اجمالية (92.5) لا يعنى بالضرورة الاتجاه نحو استخدام وتبنى هذه التطبيقات، وإنما تأتى مصحوبة بدوافع تصب غالبيتها فى معرفة كل جديد عن التقنيات الذكية المثارة

3- مدى اهتمام المؤسسات الأمنية العربية بتطبيقات الذكاء الاصطناعى وانعكاس ذلك لدى العاملين لديها :

جدول رقم (3)

مدى اهتمام المؤسسات الأمنية بتوفير فرص تدريب للمنسوبين لديها فى تطبيقات الحاسب الآلى

الحرص على دورات فى الحاسب	العدد	النسبة
أحياناً	82	77.3
دائماً	14	13.3
نادراً	10	9.4
المجموع	**106**	**100**

يتضح من الجدول السابق أن (82) من أفراد مجتمع الدراسة يمثلون ما نسبته (77.3) من اجمالى عينة الدراسة يؤكدون حرص المؤسسات التى يعملون بها "احياناً" على توفير دورات مؤهلة لتنمية قدراتهم فى تطبيقات الحاسب الآلى، وهم الفئة الأكبر من أفراد مجتمع الدراسة ، بينما (14) منهم يمثلون ما نسبته (13.3) من اجمالى افراد مجتمع الدراسة قالوا تحرص"دائماً"، وأخيرا (10) منهم يمثلون ما نسبته (9.4) قالوا "نادرا" ما تعلن مؤسساتهم عن وجود دورات مؤهلة لتنمية قدراتهم فى تطبيقات الحاسب الالى ودعم عمليات التحول الرقمى لديها، وهى مؤشرات تؤكد على عدم توسع المؤسسات الأمنية فى اتاحة الدورات للمنسوبين لديها فى كل قطاعاتها، حيث ما تزال هناك قطاعات كاملة تؤدى دورها الوظيفى بالشكل التقليدى القديم، على الرغم من حصول عدد كبير من العاملين على دورات متقدمة فى الحاسب الآلى، وقد يعزو ذلك إلى طبيعة المعلومات وسريتها وخاصة التى ترتبط بأمن الدولة، وهو ما يراه الباحث منطقياً وخاصة فى القطاعات التى تملك ملفات أمنية غاية فى الأهمية.

جدول رقم (4)

مدى حصول المبحوثين بالمؤسسات الأمنية على دورات في تطبيقات الذكاء الاصطناعى

الحصول على دورات	التكرار	النسبة
لا	63	59.4
نعم	43	40.6
المجموع	**106**	**100**

يتضح من الجدول السابق أن (63) من أفراد مجتمع الدراسة يمثلون ما نسبته (59.4) من إجمالي عينة الدراسة قالوا" لا " لم يسبق لهم الالتحاق بدورات في تطبيقات الذكاء الاصطناعى وهم الفئة الأكثر من أفراد مجتمع الدراسة، بينما (43) منهم يمثلون ما نسبته (40.6) من إجمالي أفراد مجتمع الدراسة قالوا "نعم" سبق لهم الالتحاق بدورات في تطبيقات الذكاء الاصطناعى ، وهو ما يفسر وجود حالة من البطىء نحو استخدام وتبنى التطبيقات الذكية فى قطاعات المؤسسات الأمنية العربية، إلا أن ذلك لا ينفى أن نحو (40.6) من أفراد مجتمع الدراسة قد حصلوا على دورات فى تطبيقات الذكاء الاصطناعى، وهى فى الأغلب ترتبط بالأمن السيبرانى والجرائم الالكترونية .

جدول رقم (5)

مدى حصول المبحوثين فى المؤسسات الأمنية على دورات فى علوم الأدلة الجنائية

دورات فى علوم الأدلة	العدد	النسبة
لا	75	70.80
نعم	31	29.2
المجموع	**106**	**100**

يتضح من الجدول السابق أن (75) من أفراد مجتمع الدراسة يمثلون ما نسبته (70.8) من إجمالي عينة الدراسة لم يسبق لهم الالتحاق بدورات تأهيلية في العلوم الجنائية الرقمية، وهم الفئة الأكثر من أفراد مجتمع الدراسة، بينما (31) منهم يمثلون ما نسبته(29.2) من إجمالي أفراد مجتمع الدراسة سبق لهم الالتحاق بدورات تأهيلية في علوم الأدلة الجنائية الرقمية، وهى مؤشرات تؤكد محدودية العاملين فى الطب الشرعى بوزارة العدل، ويفسر حقيقة قلة الحاصلين على دورات فى الأدلة الجنائية بجهاز الشرطة وقطاعات وزارة الداخلية عموماً .

جدول رقم (6)

موضوعات الدورات التى حصل عليها المبحوثين بالمؤسسات الأمنية

موضوعات الدورات	العدد	النسبة
الأمن السيبرانى	33	31.1
الجرائم الالكترونية	32	30.2
التزييف العميق	26	24.5
الأدلة الرقمية	8	7.5
مهددات الأمن الوطنى	7	6.6
المجموع	**106**	**100**

يتضح من الجدول السابق أن (33) من أفراد مجتمع الدراسة يمثلون ما نسبته (29.2) من إجمالى عينة الدراسة قد حصلوا على دورات فى مجال الأمن السيبراني وهم الفئة الأكبر من أفراد مجتمع الدراسة، بينما (32) منهم يمثلون ما نسبته (30.2) حصلوا على دورات فى الجرائم الالكترونية، و(26) منهم يمثلون ما نسبته (24.51) من إجمالى أفراد المجتمع حصلوا على دورات فى التزييف العميق، وأن (8) من أفراد المجتمع يمثلون ما نسبته (7.5) حصلوا على دورات فى الأدلة الرقمية، وأخيرا (7) من أفراد المجتمع يمثلون (6.6) حصلوا على دورات فى مهددات الأمن الوطني، وهو ما يعني أن المؤسسات الأمنية العربية قد اتجهت منذ 2018م نحو توظيف التقنية الحديثة فى قطاعاتها المختلفة باعتبارها أدوات قد تسهل علي المنسوبين لديها بعض المهام الوظيفية المكلفين بها وخاصة فى قطاع أمن المعلومات وحماية الشبكات، وهو ما انعكس على تنوع موضوعات ومضامين الدورات التى حصل عليها المبحوثين والتى تتجه نحو الأتمتة الأمنية وتوظيف البيانات الضخمة فى حل المشكلات المعقدة ، خاصة فى جرائم الارهاب وغسيل الأموال وتجارة البشر وغيرها .

4- مدى جاهزية المؤسسات الأمنية العربية نحو استخدام وتبنى تطبيقات الذكاء الاصطناعى.

جدول رقم (7)

مدى جاهزية المؤسسات الأمنية نحو تبنى تطبيقات الذكاء الاصطناعى لديها :

مدى الجاهزية	العدد	النسبة
جاهزة	18	16.9
إلى حد ما	77	72.6
غير جاهزة	11	10.5
المجموع	**106**	**100**

يتضح من الجدول السابق أن (77) من أفراد عينة الدراسة يمثلون ما نسبته (72.6) يرون أن مؤسساتهم الأمنية جاهزة "إلى حد ما" نحو استخدام وتبني التطبيقات الذكية بقطاعاتها المختلفة، وهى الفئة الأكثر من أفراد عينة الدراسة، بينما أكد (18) منهم يمثلون ما نسبته (16.9) أن مؤسساتهم جاهزة للاستخدام والتبني، وأخيراً قال (11) من أفراد العينة ويمثلون ما نسبته (10.5) أن مؤسساتهم غير جاهزة فى الوقت الراهن، ويعزو هذا التباين فى أراء المبحوثين إلى أن قطاعات المؤسسات الأمنية العربية لديها أولويات فى استخدام وتبنى تطبيقات الذكاء الاصطناعي حيث يأتي حماية الأمن الوطنى (أفراد – مؤسسات) فى صدارة الاهتمام باعتباره الأقرب للتطبيق مقارنة بقطاعات مثل المرور والدفاع المدني والسجون

وغيرها، الأمر الذى يراه الباحث منطقياً حيث يأتى التبني المحدود لتطبيقات تحمل في طياتها جوانب إيجابية ومخاطر أمنية فى الوقت نفسه .

جدول رقم (8)

مستوى جاهزية المؤسسات الأمنية نحو تبنى توظيف تطبيقات الذكاء الاصطناعى

مستوى الجاهزية	العدد	النسبة
الى حد كبير	12	11.3
الى حد ما	84	79.3
نادرا	10	9.4
المجموع	**106**	**100**

توضح بيانات الجدول السابق أن (84) من أفراد عينة الدراسة يمثلون ما نسبته (79.3) من إجمالى العينة يرون أن مستوى جاهزية مؤسساتهم نحو استخدام وتبني تطبيقات الذكاء الاصطناعي يأتى تحت فئة (إلي حد ما) ، فيما يؤكد (12) من أفراد مجتمع الدراسة يمثلون ما نسبته (11.3) أن مؤسساتهم جاهزة للتبني (إلى حد كبير)، وأخيرا قال(10) من أفراد مجتمع الدراسة يمثلون ما نسبته (9.4) أن تبني مؤسساتهم لتطبيقات الذكاء الاصطناعي يقع ضمن فئة (ضعيف)، وهو ما يعنى تباين آراء المبحوثين نحو تبنى القطاعات الأمنية لتطبيقات الذكاء الاصطناعي، وأن الجاهزية تستلزم إعداد كوادر مؤهلة علمياً وفنياً، بالاضافة إلى مراجعة البنية التكنولوجية التى يجب تطويرها وتحديثها فى قطاعات المؤسسة الأمنية، وهي مؤشرات تؤكد على أن المؤسسات الأمنية العربية ما تزال تسعي نحو تبني تطبيقات الذكاء الاصطناعي فى مختلف قطاعاتها وفق أولويات وترتيب زمنى يراعي فيه المخاطر التى قد تصاحب تطبيقات الذكاء الاصطناعى فى النواحى المهنية والوظيفية والأخلاقية.

جدول رقم (9)

واقع تبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية

واقع التبنى	العدد	النسبة
لا زالت فى مراحلها الأولى	70	66.3
لم تصل إلى المستوى المطلوب	22	20.7
وصلت لمستوى متقدم	14	13.0
المجموع	**106**	**100**

يتضح من الجدول السابق أن (70) من أفراد عينة الدراسة يمثلون ما نسبته (66.3) وهم الفئة الأكثر من أفراد عينة الدراسة يرون أن مستويات تبني تطبيقات الذكاء الاصطناعي داخل مؤسساتهم الأمنية ما يزال في مراحله الأولي (فترة التجريب)، فيما يري (22) منهم يمثلون ما نسبته (20.7)، أن تبني تطبيقات الذكاء الاصطناعي لديهم لم يصل بعد إلى المستوى المطلوب، وأخيرا قال (14) منهم يمثلون ما نسبته (13.0) من إجمالى عينة الدراسة أن التوظيف فى مؤسساتهم وصل لمستوى متقدم، وهو ما يعني أن تبنى وتوظيف تطبيقات الذكاء الاصطناعي لن يكون سريعاً فى كل القطاعات الأمنية على الأقل، خاصة وأن هذه التطبيقات ماتزال تعانى من الاختراقات والثغرات الأمنية، وهو ما يستلزم ضرورة فهم المنظومة كاملة قبل المضى نحو التبني الفعلى، وهى مؤشرات لا تنفى المضي نحو التبنى، لكن بقطاعات معينة وبحذر شديد.

جدول رقم (10)
ما درجة التبنى المتوقعة عند توظيف تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية

درجة التبنى المتوقع	العدد	النسبة
بدرجة كبيرة	26	24.5
بدرجة متوسطة	65	61.3
بدرجة محدودة	15	14.2
المجموع	**106**	**100**

تظهر بيانات الجدول السابق أن (65) من أفراد عينة الدراسة يمثلون ما نسبته (61.3) وهى الفئة الأكثر من أفراد عينة الدراسة يرون أن درجات التبني المتوقعة لتطبيقات الذكاء الاصطناعي فى مؤسساتهم الأمنية يقع ضمن فئة (متوسطة)، بينما يرى (26) منهم يمثلون ما نسبته (24.5) أن المتوقع أن تصل درجات التبني إلى مستويات كبيرة، وأخيرا قال (15) منهم يمثلون ما نسبته (14.2) من إجمالى عينة الدراسة أن المتوقع أن يكون التبني محدود وفى قطاعات محددة أيضاً ، وهو ما يعني ارتفاع درجة توقع المبحوثين نحو تبني وتوظيف تطبيقات الذكاء الاصطناعي داخل مؤسساتهم الأمنية، حيث تأتي بدرجة متوسطة، يليها التوقع بدرجة كبيرة، وهى مؤشرات تؤكد على حتمية التبني مستقبلاً، باعتبارها تطبيقات ذكية سوف تسهم فى الكشف عن الجرائم بأنواعها من ناحية، وتمكن المؤسسات الأمنية من حل الكثير من المشكلات الأمنية المعقدة والمساعدة فى الحد من الأضرار وزيادة فرص القبض على المجرمين قبل ارتكاب الجرائم من ناحية أخرى.

جدول رقم (11)
ما نتائج التبنى المتوقعة عند توظيف تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية

نتائج التبنى المتوقع	العدد	النسبة
ايجابية جدا	17	16.0
ايجابية	55	51.9
متوسطة	20	18.8
سلبية جدا	8	7.6
سلبية	6	5.7
المجموع	**106**	**100**

تظهر بيانات الجدول السابق أن (55) من أفراد عينة الدراسة يمثلون ما نسبته (51.9) وهم الفئة الأكثر من أفراد عينة الدراسة يرون إيجابية عملية تبني توظيف الذكاء الاصطناعي فى مؤسساتهم الأمنية العربية، بينما يري (20) منهم يمثلون ما نسبته (18.8) أن التبني يقع ضمن الفئة (إيجابية جدا)، ثم (17) منهم يمثلون ما نسبته (16.0) يرون أن التبني يقع فى فئة (متوسطة)، فيما يري (8) منهم يمثلون ما نسبته (7.6) أن نتائج التبني والتوظيف ستكون (سلبية جدا)، فيما قال (6) منهم يمثلون ما نسبته (5.7) من إجمالى أفراد العينة أن المتوقع من نتائج التبني أن تأتى (سلبية)، وهو ما يدلل على أن المبحوثين لديهم تفاؤل كبير إزاء النتائج المتوقعة عند استخدام وتبني مؤسساتهم الأمنية لتطبيقات الذكاء الاصطناعي، وقد أكدوا على أنها إيجابية، وإيجابية جداً ، وهو ما يفتح المجال واسعاً أمام المؤسسات

الأمنية العربية نحو المضي فى إجراءات التبني وسرعة تهيئة البيئة التكنولوجية لديها لاستيعاب قدرات وإمكانات الذكاء الاصطناعى وخاصة فى التحليل الكمى للبيانات التى تم جمعها من قبل قطاعات الأمن العام لاستخراج الأنماط والتنبؤ بالأحداث المستقبلية كاستخدام البيانات لفحص بيانات الجريمة، وهو ما تتفق فيه النتائج مع دراسة (Damiani،Zhang 2022.) [95] والتى توصلت الى وجود اساليب يمكن اعتمادها لجعل أنظمة الذكاء الاصطناعي أكثر قابلية للتفسير والتنوع (XAT)، ويعكس هذا التنوع أهمية تحقيق توازن بين توفير شفافية لقرارات الذكاء الاصطناعي والحفاظ على مرونة النظام في التعامل مع مجموعة واسعة من السياقات الأخرى.

5- دوافع تبنى المؤسسات الأمنية العربية لتطبيقات الذكاء الاصطناعى :

جدول رقم (12)

دوافع تبنى المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى عند أداء مهامها الوظيفية

دوافع التبنى	مستوى التبنى			المتوسط الحسابي	الانحراف المعياري
	بدرجة كبيرة	إلى حد ما	لا توجد		
	%	%	%		
تحقيق المنافسة بين القطاعات الأمنية	47.8	32.6	19.6	3.87	.863
تحليل البيانات الضخمة والمعقدة	31.1	41.1	27.8	3.85	.768
زيادة كفاءة العامل البشرى بقطاع الأمن	32.5	47.9	19.6	3.82	.909
توافر البيانات بصور واشكال متعددة	28.2	47.8	24	3.80	.931
سهولة تبادل المعلومات مع جهات أخرى	33.5	45	21.5	3.78	.989
امكانية التحديث الفورى للمعلومات الأمنية	28.7	55.5	15.8	3.74	.942
يساعد على التنبؤ بالتهديدات المستقبلية	35.9	49.3	14.8	3.73	1.006
سهولة التحقق من المعلومات المتداولة	44.5	39.7	15.8	3.72	.984
يساعد فى تقليل التكاليف فى البحث والتحرى	33	48.8	18.2	3.65	.923
امكانية متابعة المستجدات بلغات عديدة	32.5	49.8	17.7	3.65	.981
تحديد الوجوه والهوية بأشكال متعددة	35.4	46.4	18.2	3.64	.907
تقليل وقت الاستجابة للاحداث المهمة	31.1	49.1	19.1	3.53	.915
دعم اجراءات الأمن السيبرانى	51.1	35	13.9	3.50	.972
المتوسط العام				**3.72**	**.669**

** دالة إحصائياً عند مستوى 0.01 فأقل * دالة إحصائيا عند مستوى 0.05 فأقل

توضح بيانات الجدول السابق أن المؤسسات الامنية لديها دوافع نحو تبني تطبيقات الذكاء الاصطناعي وإن كان ذلك بدرجات متفاوتة، حيث توضح النتائج أن نسبة كبيرة من أفراد

عينة الدراسة قد أكدوا على أن دوافع التبني وعددها (13) دافعاً كافياً فى تبنى المؤسسات الأمنية العربية لتطبيقات الذكاء الاصطناعى، وقد بلغ المتوسط الحسابي لدوافع التبنى (3.72) وبانحراف معياري قدرة (0.669) وهو متوسط يقع فى الفئة الثالثة من فئات المقياس الثلاثى (5-3.72) وهى الفئة التى تشير الى أن دوافع التبنى جاءت (مرتفعة) على أداة الدراسة، وهى مؤشرات تؤكد على أن دوافع تبني المؤسسات الأمنية لتطبيقات الذكاء الاصطناعي فى أداء مهامهم الوظيفية جاءت كبيرة، كما يلاحظ أيضاً أن (3.87) من عينة الدراسة قد أشاروا إلى تنوع دوافع تبني تطبيقات الذكاء الاصطناعي بدرجات متفاوتة، وهو ما يعني عدم وجود موانع لعملية التبني، حيث يتوقع غالبية المبحوثين أن تسهم تطبيقات الذكاء الاصطناعى فى دعم كفاءة العنصر البشرى فى سرعة الكشف عن التهديدات والمخاطر المحتملة مستقبلاً، وأن يقلل الذكاء الاصطناعى من الجهود البشرية المبذولة خاصة فى اجراءات التحرى وسرعة انفاذ القانون وتقديم الجانى للمحاكمة عبر التعرف على الوجوه بتقنية التعلم العميق، بالإضافة إلى امكانية التعرف على الوجوه فى الصور غير الواضحة والأنماط السلوكية للمجرمين، وهو ما تتفق فيه النتائج مع دراسة (Walker 2022.) [96] والتى توصلت الى أهمية تطبيقات الذكاء الاصطناعى فى الكشف عن عمليات غسل الأموال والجرائم المالية من احتيال ونصب وسرقة بطاقات الائتمان وغيرها .

6 ـ ما مدى استخدام وتبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية :

جدول رقم (13) يوضح

مدى استخدام وتبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية

استخدام وتبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية		استجابة أفراد المجتمع					المتوسط	الانحراف المعيارى
		تستخدم بدرجة كبيرة جداً	تستخدم بدرجة كبيرة	تستخدم بدرجة متوسطة	تستخدم بدرجة قليلة	لا تستخدم		
المساعدة فى انشاء قواعد بيانات ضخمة للجرائم بأنواعها	ت	36	37	20	5	8	3.83	1.175
	%	34.0	34.0	18.9	4.7	7.5		
ادارة منصات وحسابات المؤسسات الأمنية عن بُعد	ت	36	35	19	6	10	3.76	1.1246
	%	34.0	33.0	17.9	5.7	9.4		
تنظيم العمل داخل قطاعات المؤسسة الامنية بالكفاءة المطلوبة	ت	27	34	26	9	10	3.56	1.227
	%	25.5	32.1	24.5	8.5	9.4		
سهولة الوصول للأدلة الجنائية	ت	16	16	27	25	21	2.82	1.336
	%	15.2	15.2	25.7	23.8	20.0		
تنوع الأدلة فى الجريمة الواحدة	ت	13	21	25	24	23	2.78	1.324
	%	12.3	19.8	63.6	22.6	21.7		
خلق وظائف أمنية جديدة	ت	19	16	20	18	33	2.72	1.491
	%	17.90	15.1	18.9	17.0	31.1		
يؤثر على العاملين بشكل ايجابى	ت	10	14	27	29	25	2.57	1.255
	%	9.5	13.3	25.7	27.6	23.8		
يساهم فى التفكير السريع	ت	5	10	17	20	53	1.99	1.221
	%	4.8	9.5	16.2	19.0	50.5		

استخدام وتبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية		استجابة أفراد المجتمع					المتوسط	الانحراف المعيارى
		تستخدم بدرجة كبيرة جداً	تستخدم بدرجة كبيرة	تستخدم بدرجة متوسطة	تستخدم بدرجة قليلة	لا تستخدم		
تحقيق الأمن المعلوماتى	ت	4	7	16	21	58	1.85	1.136
	%	3.8	6.6	15.1	19.8	54.7		
المنافسة فى الأداء الوظيفى	ت	2	9	14	12	68	1.71	1.107
	%	1.9	8.6	12.3	11.4	64.8		
المتوسط العام							**2.76**	**0.817**

** دالة إحصائياً عند مستوى 0.01 فأقل * دالة إحصائياً عند مستوى 0.05 فأقل

يتضح من نتائج الجدول السابق ما يلي:

1. موافقة أفراد مجتمع الدراسة (بدرجة بسيطة) على استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية بمتوسط (2.76 من 5.00)، وهو متوسط يقع في الفئة الثالثة من فئات المقياس الخماسي (2.60 - 3.40)، وهي الفئة التي تشير إلى خيار تستخدم بدرجة (متوسطة) وفق أداة الدراسة .
2. أن غالبية قيم مربع كاي كانت دالة إحصائياً عند مستوى (0.01) فأقل، ما يبين تباين وجهات نظر المبحوثين على فقرات استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية، فيما عدا الفقرات رقم (6،9،10)، فقد كانت قيمها غير دالة إحصائياً عند مستوى (0.05) فأقل، وهو ما يعنى تجانس وجهات نظر المبحوثين على هذه الفقرات
3. أن غالبية قيم (ت) لمفردة واحدة كانت دالة إحصائياً عند مستوى (0.01) فأقل، مما يبين موافقة المبحوثين على فقرات استخدام تطبيقات الذكاء الاصطناعى بدرجة متوسطة .
4. هناك تفاوت في موافقة المبحوثين على مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية ، وقد تراوحت متوسطات موافقتهم على مدى استخدام التطبيقات ما بين (1.71 إلى 3.83) ، وهى متوسطات تقع في الفئتين الأولى والرابعة من فئات المقياس الخماسي، واللتان تشيران إلى (لا تستخدم / تستخدم بدرجة كبيرة)، وهو ما يوضح التفاوت في موافقة أفراد مجتمع الدراسة على استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية، كما يتضح من النتائج أن أفراد مجتمع الدراسة موافقون بدرجة كبيرة على ثلاثة من الاستخدامات فى المؤسسات الأمنية تتمثل في العبارات رقم (1، 2 ،3)، التي تم ترتيبها تنازلياً حسب موافقة العينة على استخدامها بدرجة (كبيرة) ، حيث جاءت عبارة " المساعدة فى انشاء قواعد بيانات ضخمة للجرائم بأنواعها" بالمرتبة الأولى من حيث موافقة أفراد مجتمع الدراسة على استخدامها بدرجة كبيرة بمتوسط (3.83 من 5)، كما جاءت عبارة "سهولة ادارة منصات المعلومات بالمؤسسات الأمنية عن بُعد" بالمرتبة الثانية من حيث موافقة المبحوثين على استخدامها بدرجة كبيرة بمتوسط (3.76 من 5)، وجاءت عبارة "تنظيم العمل داخل المؤسسة الأمنية بالكفاءة المطلوبة" بالمرتبة الثالثة من حيث موافقة المبحوثين على استخدام التطبيقات بدرجة (كبيرة) بمتوسط (3.56 من 5).

كما يتضح من النتائج أيضاً أن أفراد مجتمع الدراسة موافقون بدرجة (متوسطة) على ثلاثة من استخدامات تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية تتمثل في العبارات رقم

(4 ، 5 ، 6)، والتي تم ترتيبها تنازلياً حسب موافقة عينة الدراسة على استخدامها بدرجة متوسطة حيث جاءت عبارة"سهولة الوصول للأدلة الجنائية" بالمرتبة الرابعة من حيث موافقة المبحوثين على استخدامها بدرجة متوسطة بمتوسط (2.82 من 5)، وجاءت عبارة "تنوع الأدلة فى الجريمة الواحدة" بالمرتبة الخامسة من حيث موافقة المبحوثين على استخدامها بدرجة متوسطة بمتوسط (2.78 من 5)، وجاءت عبارة "خلق وظائف أمنية جديدة" بالمرتبة السادسة من حيث موافقة المبحوثين على استخدامها بدرجة متوسطة بمتوسط (2.72 من5).

كما يتضح من النتائج أن أفراد مجتمع الدراسة موافقون بدرجة (ضعيفة) على ثلاثة من استخدامات لتطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية تتمثل في العبارات رقم (7، 8، 9، 10)، التي تم ترتيبها تنازلياً حسب موافقة عينة الدراسة على استخدامها بدرجة ضعيفة حيث جاءت عبارة "يؤثر على العاملين بشكل ايجابى" بالمرتبة السابعة من حيث موافقة المبحوثين على استخدامها بدرجة ضعيفة بمتوسط (2.57 من5)، وجاءت عبارة "يساهم فى التفكير السريع "بالمرتبة الثامنة من حيث موافقة المبحوثين على استخدامها بدرجة ضعيفة بمتوسط (1.99 من5)، وجاءت عبارة "تحقيق الأمن المعلوماتى" بالمرتبة التاسعة من حيث موافقة المبحوثين على استخدامها بدرجة ضعيفة بمتوسط (1.85 من 5)، وجاءت عبارة "المنافسة فى الأداء الوظيفى" بالمرتبة العاشرة من حيث موافقة المبحوثين على استخدامها بدرجة ضعيفة بمتوسط (1.71 من5)، وهو ما يفسر أهمية استخدام وتوظيف تطبيقات الذكاء الاصطناعى فى القطاعات الأمنية، والتى قد تسهم في تحليل مقاطع الفيديو عند مكافحة الجريمة وتأمين السلامة العامة، ومساعدة متاجر البيع في رصد أي محاولة سطو بشكل آني عبر تقنية الكشف عن وجود أسلحة أو مهاجمين مقنعين، وإطلاق صفارات الانذار تلقائياً عند حدوث سرقة أو اشتعال حرائق أو غيرها من المخاطر، كما توفر هذه التقنية مراقبة أكثر فعالية للمخاطر بتكلفة أدنى من الحراسة البشرية، فى المقابل يتوقع خبراء التقنية الحديثة أن استخدام تطبيقات الذكاء الاصطناعي فى القطاعات الأمنية سوف يؤدى الى العديد من السلبيات مثل غيرها من المهن والتى تتمثل فى: تزايد البطالة والاستغناء عن العديد من الوظائف، حيث تقوم تطبيقات الذكاء الاصطناعى بنفس المهام البشرية بتكلفة أقل، وهو ما قد يدفع الكثير من الحكومات مستقبلاً إلى وضع سياسات جديدة نحو إعادة تأهيل المنسوبين اليها وإكسابهم مهارات مؤهلة للوظائف الجديدة، اذ أن غالبية الخدمات المتاحة عند التبنى سوف تفرض على المستخدمين الموافقة على السماح لتطبيقات الذكية الدخول على بيانات الهاتف الشخصى، ومن ثم امكانية سرقة المحتوى ومعرفة اهتمامات صاحبه وتوظيفها دعائياً أو بيعها للشركات المعلنة أو طلب الفدية. [97]

7- ما متطلبات تبنى وتوظيف تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية :

جدول رقم (14) يوضح

متطلبات تبنى وتوظيف تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية

متطلبات تبنى وتوظيف تطبيقات الذكاء الاصطناعى		استجابة أفراد مجتمع الدراسة						الانحراف المعياري
		تستخدم بدرجة كبيرة جداً	تستخدم بدرجة كبيرة	تستخدم بدرجة متوسطة	تستخدم بدرجة قليلة	لا تستخدم	المتوسط	
الاستعانة بنماذج دولية ناجحة قابلة للتنفيذ	ت	24	26	21	14	21	3.17	1.437
	%	22.6	24.5	19.8	13.2	19.8		
تقليل الفجوة بين العاملين فى قطاع الأمن	ت	10	26	23	17	30	2.71	1.359
	%	9.4	24.5	21.7	16.0	28.3		
اقناع العاملين بأهمية عملية التبنى	ت	13	19	14	20	40	2.48	1.456
	%	12.3	17.9	13.2	18.9	37.7		
اقرار لوائح جديدة تسهل عملية التبنى	ت	11	19	16	16	44	2.41	1.439
	%	10.4	17.9	15.1	15.1	41.5		
توفير برامج تدريب لدعم مهارات التبنى	ت	10	14	19	22	41	2.34	1.358
	%	9.4	13.2	17.9	20.8	38.7		
توفير الامكانات المادية والبشرية للتبنى	ت	7	9	13	21	56	1.96	1.264
	%	6.6	8.5	12.3	19.8	52.8		
توفير بيئة داخلية تدعم عملية التبنى	ت	2	11	15	18	59	1.85	1.133
	%	1.9	10.5	14.3	17.1	56.2		
توفير برامج تشفير خاصة بالأمن السيبرانى	ت	5	5	13	11	27	1.68	1.151
	%	4.7	4.7	12.3	10.4	67.9		
المتوسط العام							**2.32**	**1.058**

** دالة إحصائياً عند مستوى 0.01 فأقل * دالة إحصائياً عند مستوى 0.05 فأقل

تظهر بيانات الجدول السابق أن أفراد مجتمع الدراسة موافقون بدرجة (قليلة) على عبارات متطلبات تبنى وتوظيف تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية بمتوسط (2.32 من 5.00) وهو متوسط يقع في الفئة الثانية من فئات المقياس الخماسي (من 1.80 إلى أقل من 2.60)، وهي الفئة التي تشير إلى خيار بدرجة (قليلة) على أداة الدراسة.

ويتضح من النتائج الموضحة بالجدول السابق ما يلي:

1. أن غالبية قيم مربع كاي كانت دالة إحصائياً عند مستوى (0.01) أو (0.05) فأقل، مما يبين تباين وجهات نظر أفراد مجتمع الدراسة على فقرات متطلبات تبنى والتوظيف فيما عدا الفقرة رقم (2) وهى" تقليل الفجوة بين العاملين فى المؤسسات الأمنية"، فقد كانت قيمتها غير دالة إحصائياً عند مستوى (0.05) فأقل، مما يبين تجانس وجهات نظر المبحوثين "مجتمع الدراسة" على هذه الفقرة.

2. أن غالبية قيم (ت) لمفردة واحدة كانت دالة إحصائياً عند مستوى (0.01) أو (0.05) فأقل، ما يبين موافقة أفراد مجتمع الدراسة على فقرات متطلبات تبنى وتوظيف تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية بدرجة قليلة.

3. أن هناك تفاوت في موافقة أفراد مجتمع الدراسة على متطلبات تبنى وتوظيف تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية، وقد تراوحت متوسطات موافقتهم ما بين (1.68 إلى 3.17)، وهي متوسطات تقع في الفئتين الأولي والثالثة من فئات المقياس الخماسي اللتان تشيران إلى (لا تستخدم / تستخدم بدرجة متوسطة)، مما يوضح التفاوت في موافقة أفراد مجتمع الدراسة على متطلبات تبنى وتوظيف تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية ، ويتضح من النتائج أيضاً أن أفراد مجتمع الدراسة موافقون بدرجة (متوسطة) على اثنين من متطلبات تبنى وتوظيف تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية ، تتمثلان في العبارتين رقم (1، 2)، واللتين تم ترتيبهما تنازلياً حسب موافقة أفراد على استخدامهما بدرجة (متوسطة) كالآتي: جاءت عبارة "الاستعانة بنماذج دولية ناجحة "بالمرتبة الأولى من حيث موافقة المبحوثين على متطلبات التوظيف بدرجة متوسطة (3.17 من5)، كما جاءت عبارة "تقليل الفجوة بين العاملين فى المؤسسات الأمنية "بالمرتبة الثانية من حيث موافقة المبحوثين على متطلبات تبنى وتوظيف تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية بدرجة متوسطة بمتوسط (2.71 من5).

كما يتضح من النتائج أيضاً أن أفراد مجتمع الدراسة موافقون بدرجة (ضعيفة) على خمسة من تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية تتمثل في العبارات رقم (3، 4، 5، 6، 7)، التي تم ترتيبها تنازلياً حسب موافقة أفراد عينة الدراسة على استخدامها بدرجة ضعيفة ، وجاءت عبارة " اقناع العاملين بأهمية تبنى الذكاء الاصطناعى" بالمرتبة الثالثة من حيث موافقة المبحوثين على متطلبات تبنى وتوظيف تطبيقات الذكاء الاصطناعى بدرجة ضعيفة بمتوسط (2.48 من5)، وجاءت عبارة "اقرار لوائح جديدة تسهل عملية التبنى "بالمرتبة الرابعة من حيث موافقة المبحوثين على متطلبات توظيف تطبيقات الذكاء الاصطناعى بدرجة ضعيفة بمتوسط (2.41 من5)، وجاءت عبارة" توفير برامج التدريب تدعم مهارات التبنى "بالمرتبة الخامسة من حيث موافقة المبحوثين على متطلبات تبنى وتوظيف تطبيقات الذكاء الاصطناعى بدرجة ضعيفة بمتوسط (2.34 من5)، وجاءت عبارة " توفير امكانات مادية وبشرية للتبنى"بالمرتبة السادسة من حيث موافقة المبحوثين على متطلبات توظيف تطبيقات الذكاء الاصطناعى بدرجة ضعيفة بمتوسط (1.96)، وجاءت عبارة" توفير بيئة داخلية تدعم التبنى"بالمرتبة السابعة من حيث موافقة المبحوثين على متطلبات تبنى وتوظيف تطبيقات الذكاء الاصطناعى بدرجة ضعيفة بمتوسط (1.85من5).

كما يتضح من النتائج أيضاً أن أفراد مجتمع الدراسة موافقون بدرجة (ضعيفة جدا) على واحدة من متطلبات تبنى وتوظيف تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية تتمثل في العبارة رقم (8)" تحتاج إلى برمجيات متخصصة عالية الجودة "بالمرتبة الثامنة من حيث موافقة المبحوثين على متطلبات تبنى وتوظيف تطبيقات الذكاء الاصطناعى بدرجة ضعيفة جدا بمتوسط (1.68)، وهو ما يفسر أهمية تنوع متطلبات التبنى فى المؤسسات الأمنية العربية، حيث توفر أنظمة تحليل البيانات الضخمة كميات كبيرة من المعلومات لا يمكن للمحقق البشري ادراكها بشكل كامل، وبالتالي تساعد صانعي القرار فى المؤسسات الأمنية على اختيار مسارات عمل أفضل وأسرع لكشف غموض الجريمة، حيث يمكن استخدام تطبيقات الذكاء الاصطناعي فى تحليل البيانات النصية ورسائل الواتساب والبريد

الإلكتروني لتحديد التهديدات المحتملة وأنواع أخرى من الأنشطة الإجرامية ووجوه مرتكبيها، وهو ما تتفق فيه النتائج مع دراسة (Al-Marghilani ،2022) [98] والتى توصلت إلى أهمية التعلم العميق (Deep Learning) لتوليف رسم الوجوه (FSS) للمشتبه فيه، مع امكانية إضافة مزايا التنبؤ بالجريمة قصيرة الأجل، ونتائج دراسة (2022 Powelson،) [99] التى توصلت الى أن الذكاء الاصطناعي فى حال توافر المقومات والمتطلبات المناسبة يمكن أن يكون أداة فعّالة في تعزيز فاعلية الكشف المبكر عن الجريمة .

.8- اشكال الجرائم الالكترونية المصاحبة لتطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية .

جدول رقم (15)

الجرائم الالكترونية التى تصاحب استخدام وتبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية

أشكال الجرائم الالكترونية	مستوى الاستخدم والتبنى			المتوسط الحسابي	الانحراف المعياري
	بدرجة كبيرة	إلى حد ما	لا توجد		
	%	%	%		
تنامى الأنشطة الارهابية	34.6	43.9	21.5	4.17	.822
سهولة الاحتيال المالى	26.3	32.7	41.0	4.09	.882
اختراق الحسابات البنكية	19.4	52.9	27.7	4.00	.825
تزايد جرائم التجسس	34.6	43.9	21.5	3.98	.834
تهديد الأمن الوطنى	39.4	44.2	16.3	3.95	.867
نشر الشفرات الخبيثة	46.3	31.2	22.4	3.94	.857
ترويج التجارة المحرمة	23.8	49	27.2	3.93	.931
التسويق المضلل للمنتجات والسلع	32.2	38.0	29.8	3.92	.934
نشر الشائعات والأخبار المغلوطة	31.7	43.4	24.9	3.89	.942
تنامى جماعات الاجرام الرقمى	42.5	38.2	19.3	3.82	.943
التصيد بالفيروسات الخبيثة	27.9	48.6	23.6	3.79	.968
انتهاك خصوصية الأفراد	23.8	49	27.2	2.36	0.71
انتهاك حقوق الملكية الفكرية	32.2	38.0	29.8	2.31	0.73
المتوسط العام				**3.95**	**.676**

** دالة إحصائياً عند مستوى 0.01 فأقل * دالة إحصائيا عند مستوى 0.05 فأقل

توضح بيانات الجدول السابق تنوع استجابات المبحوثين نحو الجرائم الالكترونية التى تصاحب استخدام وتبنى تطبيقات الذكاء الاصطناعى فى القطاعات الأمنية، والتى جاءت بنسب ودرجات متفاوتة ايضاً، حيث تظهر النتائج أن المبحوثين فى المؤسسات الأمنية العربية موافقون بدرجة (مرتفعة) على فئات الجرائم الالكترونية المصاحبة لتطبيقات الذكاء الاصطناعى بمتوسط (3.95 من 5.00)، وهو متوسط يقع فى الفئة الثالثة من فئات المقياس الثلاثى من (3.50-5.00)، وبانحراف معياري قدره (0.676)، وهى الفئة التى تشير إلى خيار (مرتفع) بشأن اشكال الجرائم المتوقعة عند تبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية، حيث تظهر النتائج تعدد الجرائم المتوقعة عند تبنى تطبيقات

الذكاء الاصطناعى والتى تتمثل فى التالي" تنامى الأنشطة الارهابية" بمتوسط حسابى قدره (4.17)، و"سهولة الاحتيال المالى" بمتوسط حسابى قدره (4.09)، و"اختراق الحسابات البنكية" بمتوسط حسابى قدره (4.00)، و"تزايد جرائم التجسس" بمتوسط حسابى قدره (3.98)، و"تهديد الأمن الوطنى" بمتوسط حسابى قدره (3.95)، و"نشر الشفرات الخبيثة" بمتوسط حسابى قدره (3.94)"بينما تراجعت تهديدات" ترويج التجارة المحرمة" بمتوسط حسابى قدره (3.93)، و"التسويق المضلل للمنتجات والسلع" بمتوسط حسابى قدره (3.92)، و"نشر الشائعات والأخبار المغلوطة" بمتوسط حسابى قدره (3.89)، و"تنامى جماعات الاجرام الرقمى" بمتوسط حسابى قدره (3.82)، و"التصيد بالفيروسات الخبيثة" بمتوسط حسابى قدره (3.79)، و"انتهاك وخصوصية الأفراد" بمتوسط حسابى قدره (2.36)، و"انتهاك حقوق الملكية الفكرية" بمتوسط حسابى قدره (2.31)"، وهو ما يفسر حقيقة اجماع أفراد عينة الدراسة على وجود مخاطر للتبنى فى القطاعات الأمنية وخاصة فى مجال الأنشطة الارهابية، حيث يصبح من السهولة استخدام التنظيمات الارهابية مثل هذه التقنية وتوظيفها فى عمليات عنف وتخريب ضد أمن واستقرار مؤسسات الدولة، وهو ما تتفق فيه النتائج مع ما توصلت اليه دراسه جامعة لندن(2022)،أن غالبية الجرائم الالكترونية تستهدف اختراق الحسابات البنكية والابتزاز، وتشويه السمعة عبر تقنية الخداع العميق، حيث يظهر مقطع فيديو بتقنية الذكاء الاصطناعى يعترف فيه "فلاديمير بوتين" بالتدخل الروسي في الانتخابات الامريكية الأخيرة (2021) لصالح بايدن، ومقطع أخر لرئيس مجلس النواب الأمريكي "نانسي بيلوسي" وهي فى حاله غياب عن الوعى أثناء مؤتمرٍ صحفيٍ على غير الحقيقة بتقنية التزييف العميق والتى تعمل على أخذ البيانات واستخدام نظام معالجة تكراري وخوارزميات مختلفة للتعلم من الأنماط الموجودة في البيانات، ثم التفاعل معها بطرق مختلفة لتوليد محتوى لا يكاد يختلف عن الحقيقة.[100]

9- وظائف تطبيقات الذكاء الاصطناعى فى الحد من الجرائم الالكترونية .

جدول رقم (16)

وظائف تطبيقات الذكاء الاصطناعى فى الحد من الجرائم الالكترونية

م	وظائف تطبيقات الذكاء الاصطناعى فى الحد من الجرائم الالكترونية	مستوى التوظيف			المتوسط الحسابي	الانحراف المعياري
		بدرجة كبير	إلى حد ما	لا توجد		
		%	%	%		
في مراقبة الجرائم.	تطبيق ذكي لا يفرق بين الثقافات والجنسيات	24.5	51.9	23.6	2.58	0.62
	يقوم على توثيق المخالفات غير القانونية	21.2	51.9	26.9	2.49	0.68
	إتاحة البيانات الأساسية لمنع وقوع الجرائم	21.2	49.0	29.8	2.45	0.64
	تفعيل مراقبة ورصد الجرائم بكافة أشكالها	28.5	49.3	22.2	2.40	0.70
	استشعار الجرائم قبل حدوثها من خلال التدوينات	28.5	49.3	22.2	2.37	0.70
في الكشف عن الجرائم.	امكانية حظر أي جريمة يمكن أن تقع في المستقبل	32.2	46.3	21.5	2.35	0.70
	الكشف الدقيق عن ملابسات الجرائم الخطيرة	27.9	48.6	23.6	2.35	0.66

م	وظائف تطبيقات الذكاء الاصطناعى فى الحد من الجرائم الالكترونية	مستوى التوظيف			المتوسط الحسابي	الانحراف المعياري
		بدرجة كبير	إلى حد ما	لا توجد		
		%	%	%		
	جمع أكبر عدد من الأدلة الخاصة بمسرح الجريمة	25.5	57.2	17.3	2.35	0.69
	تعطيل خطابات الكراهية وإيقاف حساب مستخدمها	29.8	45.4	24.9	2.34	0.63
	القدرة على الكشف عن المتسبب بالجريمة فى الحال	25.5	50.5	24.0	2.34	0.62
في تنفيذ عقوبة الجرائم	امكانية المساعدة فى تنفيذ العقوبة على الجميع	30.0	44.4	25.6	2.32	0.70
	تتيح عملية إنفاذ القانون والعقوبة بشكل دقيق	28.4	51.4	20.2	2.31	0.69
	اتاحة فرص المساواة في تطبيق العقوبة على الجميع	42.5	38.2	19.3	2.30	0.62
	المصداقية وتنفيذ صارم للقوانين بدون مجاملة	22.2	47.3	30.4	2.29	0.73
	وضع قواعد وإجراءات لمحاسبه أي سلوك اجرامى	27.2	51.5	21.4	2.27	0.73
	المتوسط العام				**2.75**	**0.92**

** دالة إحصائياً عند مستوى 0.01 فأقل * دالة إحصائيا عند مستوى 0.05 فأقل

توضح بيانات الجدول السابق تنوع استجابات المبحوثين حول "وظائف تطبيقات الذكاء الاصطناعى فى الحد من الجرائم الالكترونية " والتى جاءت بنسب ودرجات متفاوتة، حيث تظهر النتائج أن المبحوثين فى المؤسسات الأمنية العربية موافقون بدرجة (متوسطة) على مجموعة فئات الوظائف االمتاحة بمتوسط (2.75 من 5.)، وهو متوسط يقع فى الفئة الثانية من فئات المقياس الثلاثى من (250-3.49)، وبانحراف معياري قدره(0.92)،وهى الفئة التى تشير إلى خيار (متوسط) بشأن وظائف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية، حيث تظهر النتائج تنوع وظائف تطبيقات الذكاء الاصطناعى فى الحد من الجرائم الالكترونية ، **فمن حيث المراقبة الوقائية من الجرائم** تصدر كونه " تطبيق ذكي لا يفرق بين الثقافات والجنسيات"بمتوسط حسابى قدره (2.58)، يليه "يقوم التطبيق الذكى على توثيق المخالفات غير القانونية "بمتوسط حسابى قدره (2.49)، و"إتاحة البيانات الأساسية من قاعدة البيانات الضخمة لمنع وقوع الجرائم "بمتوسط حسابى قدره (2.45)، و" تفعيل تطبيقات مراقبة ورصد الجرائم بكافة أشكالها" بمتوسط حسابى قدره (2.40)، و"امكانية استشعار الجرائم قبل حدوثها من خلال التدوينات التى يكتبها المدونون "بمتوسط حسابى قدره (2.37)، **وفى مجال الكشف عن الجرائم** تصدرت " امكانية التطبيقات الذكية حظر أي جريمة يمكن أن تقع في المستقبل" بمتوسط حسابى قدره (2.35)، و"الكشف الدقيق عن ملابسات الجرائم الخطيرة"بمتوسط حسابى قدره (2.35)، و"جمع أكبر عدد من الأدلة الخاصة بمسرح الجريمة"بمتوسط حسابى قدره (2.35)، و"تعطيل خطابات الكراهية وإيقاف حساب مستخدمها" بمتوسط حسابى قدره (2.34)"،و"القدرة على الكشف عن المتسبب بالجريمة فى الحال"بمتوسط حسابى قدره (2.34)، **وفى مجال تنفيذ عقوبة الجرائم**

تصدرت وظائف" امكانية المساعدة فى تنفيذ العقوبة على الجميع"بمتوسط حسابى قدره (2.32)، و"تتيح عملية إنفاذ القانون والعقوبة بشكل دقيق"بمتوسط حسابى قدره (2.31)، و"اتاحة فرص المساواة في تطبيق العقوبة على الجميع" بمتوسط حسابى قدره (2.30)، و"المصداقية وتنفيذ صارم للقوانين دون مجاملة "بمتوسط حسابى قدره (2.29)، و"وضع قواعد وإجراءات ضد أي سلوك اجرامى"بمتوسط حسابى قدره (2.27)، وهو ما يفسر حقيقة تنوع وظائف تطبيقات الذكاء الاصطناعى فى الحد من الجرائم الالكترونية فى مجالاتها الثلاثة (مراقبة الجرائم، الكشف عن الجرائم، ومتابعة تنفيذ الأحكام بشأن الجرائم)، ويعتقد الباحث أنه ورغم تعدد وظائف تطبيقات الذكاء الاصطناعى فى اطار الحد من الجرائم الالكترونية،الا أن القدرات البشرية ما تزال لديها من القدرات ما يضفى على بعض الأحكام البعد الإنساني والحالة النفسية لمرتكب الجريمة وتحليل وتفسير تدويناته ومحادثاته الصوتية المسجلة، حيث قضت محكمة نيويورك الأمريكية أن الكشف عن محتوى الحساب الخاص للجاني علي "توتير" لا يشكل انتهاكاً للحق في الحياة الخاصة ولم يتم الاعتداء مادياً علي حقوق الملكية ولا يوجد انتهاكاً للحياة الخاصة، فالمتهم أرسل تغريداته عبر منصة توتير للجميع وهى منصة يتوافر فيها ركن العلانية .

10- ما أهم تطبيقات الذكاء الاصطناعى المستخدمة فى الكشف عن الجرائم الالكترونية :

جدول رقم (17)

أهم تطبيقات الذكاء الاصطناعى المستخدمه فى الكشف عن الجرائم الالكترونية

تطبيقات الذكاء الاصطناعى	مستوى الاستخدام			المتوسط الحسابي	الانحراف المعياري
	بدرجة كبيرة	إلى حد ما	لا توجد		
	%	%	%		
تقنية التحليل Seo- crime	34.0	48.5	17.5	2.55	0.65
تقنية الواقع المعززVr	34.6	44.7	20.7	2.52	0.63
تقنية الصورReverse image search	37.5	44.7	17.8	2.50	0.59
تقنيةالذكاء الاصطناعى Chat Gpt	42.3	45.7	12.0	2.49	0.63
تقنية التصوير الآلى photo Robot	26.6	45.4	28.0	2.48	0.62
تقنية التعلم E-narrative	35.3	42.5	22.2	2.47	0.60
تقنية التجسيم Hologram	37.7	44.0	17.9	2.46	0.71
تقنية الفيديو بدرجة 360	28.2	55.8	16.0	2.37	0.73
تقنية التزييف العميقDeep Facte	29.0	46.4	24.6	2.35	0.73
تقنية الطباعة ثلاثية الابعاد 3D	33.3	43.5	23.2	2.23	0.76
تقنية تحليل البياناتData analysis	37.5	44.7	17.8	2.22	0.76
المتوسط العام				**2.58**	**0.75**

** دالة إحصائياً عند مستوى 0.01 فأقل * دالة إحصائيا عند مستوى 0.05 فأقل

توضح بيانات الجدول السابق تنوع استجابات المبحوثين حول تطبيقات الذكاء الاصطناعى فى قطاعات المؤسسات الأمنية العربية، والتى جاءت بنسب ودرجات متفاوتة، حيث تظهر النتائج أن المبحوثين موافقون بدرجة (متوسطة) على مجموعة فئات التطبيقات المتاحة بمتوسط (2.58 من 5.00) وهو متوسط يقع فى الفئة الثانية من فئات المقياس الثلاثى من (3.49-250) ، وبانحراف معياري قدره (0.75)، وهى الفئة التى تشير إلى خيار(متوسط)

بشأن تقنيات الذكاء الاصطناعى المتاحة للتطبيق بقطاعات المؤسسات الأمنية العربية، حيث تظهر النتائج تنوع استخدام وتوظيف تطبيقات الذكاء الاصطناعى فى مجال العلوم الجنائية والتى جاءت على النحو التالى" تقنية التحليل Seo- crime بمتوسط حسابى قدره (2.55)، يليها تقنية الواقع المعززVr بمتوسط حسابى قدره (2.52)، وتقنية بحث الصور Reverse image search بمتوسط حسابى قدره (2.50) ، وتقنية الدردشة وتوليد النصوص Chat Gpt بمتوسط حسابى قدره (2.49)، وتقنية التصوير الالى photo Robot بمتوسط حسابى قدره (2.48)" بينما تراجعت تطبيقات مثل" تقنية التعلم E-narrative بمتوسط حسابى قدره (2.47)، وتقنية التجسيم Hologram بمتوسط حسابى قدره (2.46)، وتقنية الفيديو360 بمتوسط حسابى قدره (2.37)، والتزييف العميق Deep Facte بمتوسط حسابى قدره (2.35)، والطباعة ثلاثية الابعاد3D بمتوسط حسابى قدره (2.23)، وتحليل البيانات Data analysis بمتوسط حسابى قدره (2.22)"، وهو ما يعنى أهمية تطبيقات الذكاء الاصطناعى فى القطاعات الأمنية العربية، حيث أكدت نسبة كبيرة من المبحوثين استخدام القطاعات الأمنية عددا من تطبيقات الذكاء الاصطناعى تصدرتها تطبيقات الدردشة وتوليد النصوص مثل (ChatGPT، Bard ، Character، Janitor AI ، Dall.e)، وكذلك تطبيقات معالجة الصور ومقاطع الفيديو مثل، (Midjourney ، Capcut ، Civital، Crayon، stable diffusion)، وتطبيقات الكتابة بالذكاء الاصطناعي مثل ،(Quillbot، Novel AI)،[101] وتطبيقات معالجة البيانات الضخمة مثل، (Hugging Face)، وهى تطبيقات أثبتت فعالية فى العلوم الأمنية والكشف عن الأدلة الجنائية الرقمية التى صاحبت عدد من الجرائم الالكترونية المعقدة مثل الابتزاز والنصب والاحتيال وسرقة الحسابات البنكية وحقوق الملكية الفكرية وغيرها، وهو ما تتفق فيه النتائج جزئياً مع دراسة (Umair. 2022) [102] والتى توصلت الى امكانية استخدام تقنيات التعلم الآلي والتعلم العميق في التنبؤ بالجرائم باستخدام ذاكرة ثنائية الاتجاه طويلة المدى (Bi-LSTM)، وهي نوع من الشبكات العصبية التكرارية (RNN) تُستخدم في وضع إطار قانوني وأخلاقي يضمن استخدام الذكاء الاصطناعي بشكل آمن فى المراقبة وتعقب مسار القائم بالجريمة .

11- ما مجالات توظيف تطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية ؟

جدول رقم (18)

مجالات توظيف المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية

مجالات توظيف المؤسسات الأمنية		استجابة أفراد مجتمع الدراسة					المتوسط	الانحراف المعيارى
		دائماً نعم	غالباً	أحياناً	نادراً	أبدا		
تتبع مسار القائم بالفعل الاجرامى	ت	44	24	19	14	5	3.83	1.238
	%	41.5	22.6	17.9	13.2	4.7		
كشف اختراقات الحسابات البنكية	ت	41	22	28	9	6	3.78	1.211
	%	38.7	20.8	26.4	8.5	5.7		
سرعة الوصول للبصمة الوراثية	ت	34	32	22	13	5	3.73	1.175
	%	32.1	30.2	20.8	12.3	4.7		

مجالات توظيف المؤسسات الأمنية		استجابة أفراد مجتمع الدراسة					المتوسط	الانحراف المعيارى
		دائماً نعم	غالباً	أحياناً	نادراً	أبدا		
الكشف عن الجثث مجهولة الهوية	ت	36	29	22	13	6	3.72	1.217
	%	34.0	27.4	20.8	12.3	5.7		
تتبع تجارة وزراعة المخدرات	ت	34	24	28	14	6	3.62	1.222
	%	32.1	22.6	26.4	13.2	5.7		
سرعة انفاذ القانون فى الجرائم	ت	30	31	16	20	8	3.52	1.294
	%	28.6	29.5	15.2	19.0	7.6		
تحديد مكان النشاط الاجرامى	ت	29	26	28	14	9	3.49	1.259
	%	27.4	24.5	26.4	13.2	8.5		
الكشف عن الأدلة الرقمية	ت	13	43	29	18	3	3.42	1.004
	%	12.30	40.6	27.4	17.0	2.8		
سرعة تحديد بصمه الوجه والعين	ت	13	28	26	18	12	3.11	1.174
	%	12.3	26.4	33.0	17.0	11.3		
رصد حركة البضائع المشبوهة	ت	18	24	29	21	14	3.10	1.279
	%	17.0	22.60	27.4	19.8	13.2		
سهولة الكشف المبكر عن الجريمة	ت	14	24	24	29	23	3.09	1.250
	%	13.50	23.1	23.1	27.9	12.5		
المتوسط العام							3.48	0.865

** دالة إحصائياً عند مستوى 0.01 فأقل * دالة إحصائيا عند مستوى 0.05 فأقل

يتضح من نتائج الجدول السابق ما يلي:

1. موافقة أفراد مجتمع الدراسة بدرجة كبيرة (غالباً) على مجالات تطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية ، والتى جاءت بمتوسط (3.48 من 5)، وهو متوسط يقع في الفئة الرابعة من فئات المقياس الخماسي (من 3.40 إلى أقل من 4.20)، وهي الفئة التي تشير إلى خيار (غالباً) على أداة الدراسة.
2. أن غالبية قيم مربع كاي كانت دالة إحصائياً عند مستوى (0.01)، أو (0.05) فأقل، ما يبين تباين وجهات نظر المبحوثين على فقرات مجالات التطبيق فيما عدا الفقرتين رقم (3، 4)، المتمثلة بـ "سرعة الوصول للبصمة الوراثية "و"الكشف عن الجثث مجهولة الهوية"، وجاءا غير دالة إحصائياً عند مستوى (0.05) فأقل، وهو ما يعنى تجانس وجهات نظر المبحوثين على فقرات مجالات التوظيف فى المؤسسات الأمنية العربية .
3. أن غالبية قيم (ت) جاءت لمفردة واحدة كانت دالة إحصائياً عند مستوى (0.01) أو (0.05) فأقل، ما يبين موافقة أفراد مجتمع الدراسة على فقرات مجالات التوظيف بدرجة غالباً.
4. أن هناك تفاوتاً في موافقة أفراد مجتمع الدراسة على مجالات توظيف تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية ، وتراوحت متوسطات موافقتهم ما بين (3.09 إلى 3.83)، وهي متوسطات تقع في الفئتين الثالثة والرابعة من فئات المقياس الخماسي، واللتان تشيران إلى (أحياناً / غالباً) ، مما يوضح التفاوت في موافقة أفراد مجتمع الدراسة على مجالات التوظيف فى القطاعات الأمنية ، وأن أفراد مجتمع الدراسة موافقون (غالباً)

على ثمانية مجالات توظيف تتمثل في العبارات رقم(1، 2، 5، 6، 7، 8، 9، 10، 11) والتي تم ترتيبها تنازلياً حسب موافقة أفراد عينة الدراسة عليها (غالباً) كالآتي :
جاءت عبارة " تتبع مسار القائم بالفعل الاجرامى" بالمرتبة الأولى من حيث موافقة المبحوثين على مجالات توظيف تطبيقات الذكاء الاصطناعى غالباً بمتوسط (3.83 من 5)، وجاءت عبارة " كشف الاحتيال واختراقات الحسابات البنكية "بالمرتبة الثانية من حيث موافقة المبحوثين على مجالات توظيف تطبيقات الذكاء الاصطناعى غالباً بمتوسط (3.78 من5) ، وجاءت عبارة " تتبع تجار وزراعة المخدرات "بالمرتبة الخامسة من حيث موافقة المبحوثين على مجالات توظيف تطبيقات الذكاء الاصطناعى غالبا بمتوسط (3.62 من 5)، وجاءت عبارة "سرعة انفاذ القانون فى الجرائم المعقدة "بالمرتبة السادسة من حيث موافقة المبحوثين على مجالات توظيف تطبيقات الذكاء الاصطناعى غالباً بمتوسط (3.52 من5)، وجاءت عبارة" تحديد مكان النشاط الاجرامى"بالمرتبة السابعة من حيث موافقة المبحوثين على مجالات توظيف تطبيقات الذكاء الاصطناعى غالباً بمتوسط (3.49 من5)، وجاءت العبارة "الكشف عن الأدلة الرقمية "بالمرتبة الثامنة من حيث موافقة المبحوثين على مجالات توظيف تطبيقات الذكاء الاصطناعى غالباً بمتوسط (3.42 من5)، وجاءت عبارة "سرعة تحديد بصمه الوجه والعيون "بالمرتبة التاسعة من حيث موافقة المبحوثين على مجالات توظيف تطبيقات الذكاء الاصطناعى غالبا بمتوسط (3.11 من5)، وجاءت عبارة "رصد حركة البضائع المشبوهة "بالمرتبة العاشرة من حيث موافقة المبحوثين على مجالات توظيف تطبيقات الذكاء الاصطناعى غالباً بمتوسط (3.10 من 5)، وجاءت عبارة "سهولة الكشف المبكر عن الجريمة وعمليات غسيل الأموال" بالمرتبة الحادية عشرمن حيث موافقة المبحوثين على مجالات توظيف تطبيقات الذكاء الاصطناعى غالباً بمتوسط (3.09 من5).
ويتضح من النتائج السابقة حقيقة تنوع مجالات توظيف تطبيقات الذكاء الاصطناعى فى العلوم الأمنية، حيث أثبتت تطبيقات الذكاء الاصطناعي جدارتها في مجال تتبع مسارات القائم بالفعل الإجرامى عبر الكاميرات الذكية ، بالاضافة الى تطوير نظام آلي لتحديد عملية اختراق الحسابات البنكية والهوية الجنائية باستخدام التعرف على الوجوه لمساعدة الشرطة في التعرف على المجرمين والقبض عليهم، من خلال التسجيل الجنائي، حيث تتم إضافة الصور الإجرامية إلى النظام في قاعدة البيانات الضخمة عبر دوائر تلفزيونية مغلقة، كما يمكن لتطبيقات الذكاء الاصطناعي تحليل كميات كبيرة من البيانات فى ثوانى معدودة، بما في ذلك إحصاءات الجريمة وغيرها من المعلومات ذات الصلة، والتنبؤ بالمكان والوقت المحتمل لوقوع جريمة محددة، ومن ثم منعها قبل حدوثها، وهو ما تتفق فيه النتائج مع دراسة أنس عدنان، هبة توفيق (2023) [103]، والتى توصلت الى أن استخدام تطبيقات الذكاء الاصطناعي فى مكافحة الجرائم جاء فى ثلاثة مجالات هي: المُراقبة والوقائية من الجرائم، والكشف عن الجرائم، وسلامة وشفافية العقوبة.

12- ما التأثيرات المترتبة على توظيف المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية

جدول رقم (19)

تأثير توظيف تطبيقات الذكاء الاصطناعى المتوقعة على أداء المؤسسات الأمنية العربية

التأثير المتوقع لتطبيقات الذكاء الاصطناعى	مستوى التوظيف			المتوسط الحسابي	الانحراف المعياري
	بدرجة كبيرة	إلى حد ما	لا توجد		
	%	%	%		
تحليل البيانات الضخمة والمعقدة	24.5	51.9	23.6	2.58	0.62
التنبؤ بالهجمات والتهديدات المتوقعة	21.2	51.9	26.9	2.49	0.68
اثراء التحقيقات بالمعلومات المتنوعة	21.2	49.0	29.8	2.45	0.64
التحقق من مصداقية الصور المتداولة	28.5	49.3	22.2	2.40	0.70
تعزيز الحماية الشخصية والفكرية	28.5	49.3	22.2	2.37	0.70
دعم المؤسسات الحيوية بالأمن السيبرانى	32.2	46.3	21.5	2.35	0.70
اعادة تشكيل مسرح الجريمة 3D	27.9	48.6	23.6	2.35	0.66
سهولة الوصول للأحكام المتشابهة	25.5	57.2	17.3	2.35	0.69
امكانية تصنيف البيانات الضخمة وحفظها	29.8	45.4	24.9	2.34	0.63
تنوع تقنيات الوسائط المرئية	25.5	50.5	24.0	2.34	0.62
يوفر آلية الترجمة الفورية بجودة عالية	30.0	44.4	25.6	2.32	0.70
تحقيق الابهار فى عرض المعلومات	28.4	51.4	20.2	2.31	0.69
تحليل كلمات ومشاعر المتهمين	42.5	38.2	19.3	2.30	0.62
رصد تفاعل الجمهورعلى الجرائم	22.2	47.3	30.4	2.29	0.73
مزج الواقع والافتراضى فى الجرائم المعقدة	27.2	51.5	21.4	2.27	0.73
تساعد على التنبؤ بالجرائم المحتملة	24.3	50.5	25.2	2.23	0.71
تساعد على تصحيح أخطاء التحرى	22.7	60.4	16.9	2.18	0.71
ادارة العمل بسهولة وكفاءة عالية	21.2	57.7	21.1	2.12	0.63
المتوسط العام			**2.50**		**0.92**

** دالة إحصائياً عند مستوى 0.01 فأقل * دالة إحصائيا عند مستوى 0.05 فأقل

توضح بيانات الجدول السابق تنوع استجابات المبحوثين حول التأثيرات المتوقعة لتطبيقات الذكاء الاصطناعى على أداء المؤسسات الأمنية العربية، والتى جاءت بنسب ودرجات متفاوتة، حيث تظهر النتائج أن المبحوثين فى المؤسسات الأمنية العربية موافقون بدرجة (متوسطة) على مجموعة فئات التأثيرات المتوقعة بمتوسط (2.50 من 5.00)، وهو متوسط يقع فى الفئة الثانية من فئات المقياس الثلاثى من (250-3.49)، وبانحراف معياري قدره(0.92)، وهى الفئة التى تشير إلى خيار (متوسط) بشأن تأثيرات التوظيف المتوقع على أداء المؤسسات الأمنية العربية، حيث تظهر النتائج تأثيرات التوظيف المتوقع على أداء المؤسسات الأمنية العربية فى الجوانب التالية" تحليل البيانات المعقدة" بمتوسط حسابى قدره (2.58)، يليها "التنبؤ بالهجمات والتهديدات المتوقعة" بمتوسط حسابى قدره (2.49)، و"اثراء التحقيقات بالمعلومات المتنوعة"بمتوسط حسابى قدره (2.45)، و"التحقق من مصداقية الصور"بمتوسط حسابى قدره (2.40)، و"تعزيز الحماية الشخصية والفكرية"

بمتوسط حسابى قدره (2.37)، و"دعم الأمن السيبرانى بالمؤسسات الحيوية" بمتوسط حسابى قدره (2.35)، و"اعادة تشكيل مسرح الجريمة" بمتوسط حسابى قدره (2.35)، و"سهولة الوصول للأحكام المتشابهة" بمتوسط حسابى قدره (2.35)، و"امكانية تصنيف البيانات الضخمة وحفظها" بمتوسط حسابى قدره (2.34)"، بينما تراجعت مجالات التوظيف فى"تنوع تقنيات الوسائط المرئية "بمتوسط حسابى قدره (2.34)، و"يوفر آلية الترجمة الفورية بجودة عالية" بمتوسط حسابى قدره (2.32)، و"تحقيق الابهار فى عرض المعلومات" بمتوسط حسابى قدره (2.31)، و"تحليل كلمات ومشاعر المتهمين" بمتوسط حسابى قدره (2.30)، و"تنوع أدوات التفاعل على الجرائم "بمتوسط حسابى قدره (2.29)، و"المزج بين الواقعى والافتراضى فى الكشف عن الجرائم المعقدة "بمتوسط حسابى قدره (2.27)، و"تساعد على التنبؤ بالجرائم المحتملة" بمتوسط حسابى قدره (2.23)، و"تساعد على تصحيح أخطاء التحريات البشرية" بمتوسط حسابى قدره (2.18)، و"ادارة العمل بسهولة وكفاءة عالية" بمتوسط حسابى قدره (2.12)، وهو ما يفسر حقيقة تنوع تأثيرات تطبيقات الذكاء الاصطناعى على أداء المؤسسات الأمنية العربية وأنه على الرغم من محدوديتها الا أنها تؤثر بشكل أكبر على مجمل المهام الوظيفية لديها، ويعتقد الباحث أنه ورغم تعدد التطبيقات الأمنية وأتمتة العديد من القطاعات الأمنية، فإن القدرات البشرية ما تزال عامل مهم فى التنبؤ بالجرائم وحل العديد من القضايا المعقدة .

جدول رقم (20)

فوائد توظيف تطبيقات الذكاء الاصطناعى فى الكشف عن الأدلة الجنائية المصاحبة للجرائم الالكترونية

فوائد توظيف الذكاء الاصطناعى		استجابة أفراد مجتمع الدراسة					المتوسط	الانحراف المعيارى
		دائماً نعم	غالباً	أحياناً	نادراً	أبدا		
السرعة فى عملية البحث والتحرى	ت	29	32	30	7	8	3.63	1.174
	%	27.4	30.2	28.3	6.6	7.5		
توفر بيئة عمل مريحة لرجال الأمن	ت	25	32	34	12	2	3.60	1.031
	%	23.8	30.5	32.4	11.4	1.9		
التخلص من الروتين اليومى	ت	22	35	31	12	6	3.52	1.115
	%	20.8	33.0	29.2	11.3	5.7		
السهولة فى انفاذ القانون	ت	25	24	26	26	5	3.36	1.220
	%	23.6	22.6	24.5	24.5	4.7		
امكانية تحليل البيانات بسهولة	ت	29	23	24	17	13	3.36	1.361
	%	27.4	21.7	22.6	16.0	12.3		
الاستغناء عن الكوادر غير المؤهلة	ت	26	24	23	19	14	3.27	1.363
	%	24.5	22.6	21.7	17.9	13.2		
ضياع حقوق التأليف والملكية الفكرية	ت	25	19	31	20	11	3.25	1.295
	%	23.6	17.9	29.2	18.9	10.4		
وجود فئات رافضة للذكاء الاصطناعى	ت	20	23	24	24	15	3.08	1.332
	%	18.9	21.7	22.6	22.6	14.2		
تراجع مستوى التقارير الأمنية عن الجرائم	ت	19	21	27	25	14	3.06	1.301
	%	17.9	19.8	25.5	23.6	13.2		

فوائد توظيف الذكاء الاصطناعى		استجابة أفراد مجتمع الدراسة					المتوسط	الانحراف المعيارى
		دائماً نعم	غالباً	أحياناً	نادراً	أبدا		
فقدان الجوانب الانسانية فى انفاذ القانون	ت	17	24	24	25	16	3.01	1.313
	%	16.0	22.6	22.6	23.6	15.1		
المتوسط العام							3.31	0.980

** دالة إحصائياً عند مستوى 0.01 فأقل * دالة إحصائيا عند مستوى 0.05 فأقل

يتضح من نتائج الجدول السابق ما يلي:

1. موافقة أفراد مجتمع الدراسة (أحيانا) على فوائد توظيف تطبيقات الذكاء الاصطناعى فى الكشف عن الأدلة الجنائية المصاحبة للجرائم الالكترونية جاءت بمتوسط (3.31 من 5.00)، وهو متوسط يقع في الفئة الثالثة من فئات المقياس الخماسي (2.60 - 3.40)، وهي الفئة التي تشير إلى خيار (أحياناً) .

2. أن غالبية قيم مربع كاي كانت دالة إحصائياً عند مستوى (0.01) أو(0.05) فأقل، ما يبين تباين وجهات نظر المبحوثين على فقرات التأثيرات فيما عدا الفقرات رقم (4 ،5 ، 6 ، 7، 9)، فقد كانت قيمتها غير دالة إحصائياً عند مستوى (0.05) فأقل، ما يبين تجانس وجهات نظر مجتمع الدراسة على فقرات فوائد تطبيقات الذكاء الاصطناعى فى الكشف عن الأدلة الجنائية المصاحبة للجرائم الالكترونية

3. أن غالبية قيم (ت) لمفردة واحدة كانت دالة إحصائياً عند مستوى (0.01) أو (0.05) فأقل، ما يبين أن أفراد الدراسة موافقون على فقرات فوائد توظيف تطبيقات الذكاء الاصطناعى فى الكشف عن الأدلة الجنائية المصاحبة للجرائم الالكترونية بدرجة متوسطة (أحياناً) .

4. أن هناك تفاوتاً في موافقة أفراد مجتمع الدراسة على فوائد توظيف تطبيقات الذكاء الاصطناعى فى الكشف عن الأدلة الجنائية المصاحبة للجرائم الالكترونية، وتراوحت متوسطات موافقتهم ما بين (3.01 إلى3.63)، وهي متوسطات تقع في الفئتين الثالثة والرابعة من فئات المقياس الخماسي واللتان تشيران إلى (أحياناً / غالباً)، مما يوضح التفاوت في موافقة أفراد مجتمع الدراسة على فوائد توظيف تطبيقات الذكاء الاصطناعى فى الكشف عن الادلة الجنائية المصاحبة للجرائم الالكترونية، وأن أفراد مجتمع الدراسة موافقون (غالباً) على ثلاثة من فوائد التوظيف تتمثل في العبارات رقم (3، 2، 1) ، والتي تم ترتيبها تنازلياً حسب موافقة أفراد مجتمع الدراسة عليها غالباً، حيث جاءت عبارة "السرعة فى عملية البحث والتحرى "بالمرتبة الأولى من حيث موافقة المبحوثين على فوائد توظيف تطبيقات الذكاء الاصطناعى فى العلوم الجنائية غالباً بمتوسط (3.63 من5)، كما جاءت عبارة " توفر بيئة عمل مريحة لرجال الأمن "بالمرتبة الثانية من حيث موافقة المبحوثين على فوائد توظيف تطبيقات الذكاء الاصطناعى فى العلوم الجنائية غالباً بمتوسط (3.60 من5)، وجاءت عبارة" التخلص من الروتين اليومى" بالمرتبة الثالثة من حيث موافقة المبحوثين على فوائد توظيف تطبيقات الذكاء الاصطناعى فى العلوم الجنائية غالبا بمتوسط (3.52 من5).

كما يتضح من النتائج أيضاً أن أفراد مجتمع الدراسة موافقون (أحيانا) على ثلاثة من فوائد توظيف تطبيقات الذكاء الاصطناعى فى العلوم الجنائية، تتمثل في العبارات رقم (4، 5، 6، 7، 8، 9، 10)، التي تم ترتيبها تنازلياً حسب موافقة أفراد مجتمع الدراسة عليها غالباً ، حيث جاءت عبارة "سهولة الأداء المهنى للقائمين على انفاذ القانون" بالمرتبة الرابعة من حيث موافقة المبحوثين على فوائد توظيف تطبيقات الذكاء الاصطناعى فى العلوم الجنائية غالباً بمتوسط (3.36 من 5)، وجاءت عبارة" امكانية تحليل البيانات بسهولة "بالمرتبة الخامسة من حيث موافقة المبحوثين على فوائد توظيف تطبيقات الذكاء الاصطناعى فى العلوم الجنائية غالباً بمتوسط (3.36 من5)، وجاءت عبارة" الاستغناء عن الكوادر الأمنية" بالمرتبة السادسة من حيث موافقة المبحوثين على فوائد توظيف تطبيقات الذكاء الاصطناعى فى العلوم الجنائية غالباً بمتوسط (3.27 من5)، وجاءت عبارة "ضياع حقوق التأليف والملكية الفكرية" بالمرتبة السابعة من حيث موافقة المبحوثين على فوائد توظيف تطبيقات الذكاء الاصطناعى فى العلوم الجنائية غالباً بمتوسط (3.25 من 5)، وجاءت عبارة " وجود فئات رافضة للذكاء الاصطناعى" بالمرتبة الثامنة من حيث موافقة المبحوثين على فوائد توظيف تطبيقات الذكاء الاصطناعى فى العلوم الجنائية غالباً بمتوسط (3.08 من5)، وجاءت عبارة "تراجع مستوى التقارير الأمنية التى يتم انتاجها" بالمرتبة التاسعة من حيث موافقة المبحوثين على فوائد توظيف تطبيقات الذكاء الاصطناعى فى العلوم الجنائية غالباً بمتوسط (3.06 من5)، وجاءت عبارة "اهمال الجوانب الانسانية فى الاحكام القضائية "بالمرتبة العاشرة من حيث موافقة المبحوثين على فوائد توظيف تطبيقات الذكاء الاصطناعى فى العلوم الجنائية غالباً بمتوسط (3.01 من5).

ويتضح من النتائج السابقة تعدد فوائد تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية، حيث يمكن استخدام الذكاء الاصطناعي فى سرعة الوصول للأدلة الجنائية ، والتنبؤ ببعض الجرائم المحتملة والأماكن التى تشكل بؤرًا إجرامية مستقبلًا، وذلك عبر استخدام خوارزميات يتم إعطاؤها بيانات محددة، ومن ثم تقوم بتحليل تلك البيانات والخروج بنتائج تسهم في الوقاية من الجرائم المتوقع حدوثها، حيث تستطيع التطبيقات الذكية كشف الغموض فى أى واقعة عن طريق المعطيات التى تحصل عليها من خلال تصويرها لمسرح الجريمة بتقنية الـ 3D ودراسة الحالة الصحية للمتهم وقت ارتكاب الجريمة ، وإثبات مدى قدرته على ارتكاب السلوك المكون للجريمة من عدمه، ويرى الباحث أن هذه النظرة والتخوف من مستقبل الأدلة الجنائية جعل العديد من الحكومات مواجهة هذا التحدى من خلال وضع سياسات تقوم على إعادة تأهيل المنسوبين لدى المؤسسة الأمنية، وكانت البداية 2020 عندما قامت شرطة مدينة نيويورك بإنشاء مركزاً لإدارة الجريمة وتحليل البيانات والتنبؤ بسلوك الجانى، وتحسين زمن الاستجابة من خلال تكثيف وتوزيع الدوريات فى الأماكن الأكثر عرضة لحدوث الجرائم، وبالرغم من اهتمام الحكومة الأمريكية بإصدار القوانين الرادعة، إلا أنَّ التطبيق العملي لهذه القوانين يصطدم بتحديات إجرائية تعود إلي طبيعة ومسرح الجريمة، وهو ما يزيد من صعوبة تطبيق بعض الإجراءات مثل"التفتيش، المعاينة، والضبط.."مما يشكل عائقاً كبيراً أمام الاستفادة من الذكاء الاصطناعى التي تثبت الواقعة أو تنفيها.

جدول رقم (21)
التأثيرات السلبية المتوقعة عند استخدام وتبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية

التاثيرات المتوقعة من التبنى	مستوى التهديد			المتوسط الحسابي	الانحراف المعياري
	بدرجة كبيرة	إلى حد ما	لا توجد		
	%	%	%		
التعدى على حقوق الملكية الفكرية	24.5	51.9	23.6	2.47	0.62
كثرة الشائعات والاخبار الكاذبة	29.8	45.4	24.9	2.34	0.73
تسريب البيانات والمعلومات المهمة	30.0	44.4	25.6	2.25	0.75
تجاوز المعايير المهنية والاخلاقية	24.3	50.5	25.2	2.15	0.72
سرقة المواقع والمنصات الرقابية	27.2	51.5	21.4	2.08	0.71
المتوسط العام				**2.30**	**0.72**

** دالة إحصائياً عند مستوى 0.01 فأقل * دالة إحصائيا عند مستوى 0.05 فأقل

توضح بيانات الجدول السابق تنوع استجابات المبحوثين حول التأثيرات السلبية المتوقعة عند استخدام وتبنى المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى، حيث تظهر النتائج أن المبحوثين فى المؤسسات الأمنية موافقون بدرجة (ضعيفة) على مجموعة فئات مخاطر التبنى بمتوسط (2.30 من5)، وهو متوسط يقع فى الفئة الأولى من فئات المقياس الثلاثى من (1-2.49)، وهى الفئة التى تشير إلى خيار (ضعيف) بشأن التأثيرات السلبية المتوقعة عند استخدام وتبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية، حيث تصدرت التأثيرات السلبية المتوقعة عبارة "التعدى على حقوق الملكية الفكرية" بمتوسط حسابى قدره (2.47)، يليها "كثرة الشائعات والاخبار الكاذبة" بمتوسط حسابى قدره (2.34)، و"تسريب البيانات والمعلومات المهمة" بمتوسط حسابى قدره (2.25)، و"تجاوز المعايير المهنية والاخلاقية" بمتوسط حسابى قدره (2.15)، و"سرقة المواقع والمنصات الرقابية"بمتوسط حسابى قدره (2.08)، وهو ما يفسر أهمية تطبيقات الذكاء الاصطناعى فى الكشف عن الاختراقات والسرقات العلمية والأدبية بما فى ذلك حقوق الملكية الفكرية عبر تصميم أنظمة استباقية لإدارة الثغرات التى تصاحب نقاط الضعف فى الأنظمة الذكية، حيث تسهم تطبيقات الذكاء الاصطناعى فى رفع فاعلية التقنيات الحيوية وزيادة دقتها فى تحديد وتتبع عمليات التعدى على حقوق الملكية الفكرية وخصوصية الغير، يقابل ذلك الفراغ التشريعي القائم في مواجهة كافة صور الانتهاكات التي تقع عبر تقنيات الذكاء الاصطناعى، فالقوانين الجنائية الحالية تصبح عاجزة عن مواجهة تطورات تكنولوجية متلاحقة لا يمكن التصدي لها جنائيا إلا من خلال نصوص جنائية قائمة تطبيقًا لمبدأ الشرعيّة الجنائيّة "لا جريمة ولا عقوبة إلا بنص"،حيث ينظر إلى تقنيات الذكاء الاصطناعى بأنها ستنقل العالم إلى آفاق مختلفة وغير تقليدية ستثير بلا شك مشكلات غير محدودة من منظور القانون الجنائي.

13- الأدوار المتوقعه عند تبنى تطبيقات الذكاء الاصطناعى بالمؤسسات الأمنية :

جدول رقم (22)

الدور الوظيفى المتوقع عند تبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية

الدور الوظيفى	مستوى الدور الوظيفى			المتوسط الحسابي	الانحراف المعياري
	بدرجة كبيرة	إلى حد ما	لا توجد		
	%	%	%		
تحقق الادارة الذكية فى البحث الجنائى	31.1	49.1	19.1	3.57	1.014
استشراف النتائج فى الجرائم بدقة عالية	35.5	44.8	19.7	3.38	1.096
توفير الوقت والمجهود البشرى	34.3	39.7	26.0	3.33	1.208
تنوع مصادر الأدلة الجنائية ومصداقيتها	30.1	43.2	26.7	3.22	1.149
سرعة انفاذ القانون وصدور الأحكام	25.6	36.0	38.4	3.18	1.165
المتوسط العام				**3.34**	**1.150**

** دالة إحصائياً عند مستوى 0.01 فأقل * دالة إحصائيا عند مستوى 0.05 فأقل

توضح بيانات الجدول السابق تنوع الأدوار الوظيفية التى قد تؤديها تطبيقات الذكاء الاصطناعي عند تبنى المؤسسات الأمنية العربية لها، حيث توضح النتائج أن نسبة كبيرة من أفراد عينة الدراسة قد أكدوا على قدرة تطبيقات الذكاء الاصطناعى فى دعم البحث الجنائي، واستخراج نتائج التحقيقات الجنائية بدقة عالية، وقد بلغ المتوسط الحسابي للدور الوظيفى المتوقع (3.34) وبانحراف معياري (1.150) وهو متوسط يقع فى الفئة الثانية من فئات المقياس الثلاثى (2.50- 3.49) وهى الفئة التى تشير إلى أن الأدوار الوظيفية لتطبيقات الذكاء الاصطناعي فى المؤسسات الأمنية العربية قد تأتى (متوسطة) على أداة الدراسة، حيث ما تزال المؤسسات الأمنية العربية تقوم على مراجعة البنية الحيوية لقطاعاتها المختلفة بحيث تكون أكثر أمناً عند التبنى الفعلى والسعى نحو تحقيق الادارة الذكية فى البحث الجنائى، ونتيجةً لذلك تُنفق قطاعات الشرطة قدرًا كبيرًا من الوقت والموارد في اكتشاف اتجاهات الجريمة الرقمية والتنبؤ بها، حيث ان محاولة التنبؤ بالجريمة يدويًا يصبح من الصعوبة، فيما اصبح بالامكان استخدام تقنيات التعلم الآلي على نطاق واسع للمساعدة في الوقاية من الجريمة والتنبؤ بها تقليديا باستخدام تقنية "تحليل النقاط الساخنة" لمنع الجرائم المستقبلية، وهو ما يفسر حقيقة تصدر البحث الجنائى واستشراف نتائج التحقيقات فى الجرائم المعقدة أدوار التطبيقات الذكية حيث تحتاج الأدلة الجنائية الرقمية في عملية استخلاصها وفحصها إلى مهارات وخبرات خاصة، بالإضافة إلى فهم أساسيات وأصول التحقيق الجنائي المطبقة في الجرائم التقليدية، لذا فإن نقص خبرة لدى المحققين في مجال التقنية، وعدم معرفتهم بالتطبيقات المستعملة في ارتكاب الجريمة قد يشكل عائقاً كبيراً في جمع الأدلة الجنائية وتحليلها .

جدول رقم (23)

الدور المهنى المتوقع عند تبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية

الدور المهنى	مستوى الدور المهنى			المتوسط الحسابي	الانحراف المعياري
	بدرجة كبيرة	إلى حد ما	لا توجد		
	%	%	%		
الدقة العالية فى نتائج التحقيقات	27.9	51.0	21.1	3.52	1.051
الموضوعية والشفافية فى الأحكام	31.9	41.0	27.1	3.44	1.074
حرية تداول المعلومات وسريتها	25.6	47.3	27.1	3.42	1.102
أهمية المعلومات وتنوع مصادرها	25.4	50.7	23.9	3.42	1.098
التفاعل والمشاركة الآنية	24.9	45.9	29.2	3.35	1.146
تصحيح المعلومات الخاطئة بسرعة	30.0	48.3	21.7	3.29	1.185
المتوسط العام				**3.37**	**.883**

** دالة إحصائياً عند مستوى 0.01 فأقل * دالة إحصائيا عند مستوى 0.05 فأقل

توضح بيانات الجدول السابق تنوع الأدوار المهنية التى قد تؤديها تطبيقات الذكاء الاصطناعي عند تبنى المؤسسات الأمنية العربية لها، كما توضح النتائج أن المبحوثين موافقون بدرجة (متوسطة) على الأدوار الوظيفية التى قد تؤديها تطبيقات الذكاء الاصطناعي فى المؤسسات الأمنية بمتوسط (3.37 من 5)، وهو متوسط يقع فى الفئة الثانية من فئات المقياس الثلاثي من (2.50- 3.49) وهى الفئة التى تشير إلى خيار (بدرجة متوسطة) على مقياس أداة الدراسة، وهو ما يؤكد على تباين وجهات نظر المبحوثين فى الأدوار المهنية التى سوف تؤديها تطبيقات الذكاء الاصطناعي فى بالمؤسسات الأمنية بقطاعاتها المختلفة، والتى تتصدرها فئات الدقة والموضوعية والشفافية فى البحث واستخراج النتائج المصاحبة للجرائم بأنواعها مقارنة بالكوادر البشرية ، ويفسر حرص المؤسسات المعنية بقطاع الأمن على مواكبة التقنيات الحديثة واستراتيجيات التحول الرقمي للمحافظة على مستويات الأمن والأمان لديها، حيث بات التحدي أكبر مقارنة بالماضى، وأن تعدد أساليب الجريمة وتنوع أدواتها أصبح لزاماً على القطاعات الأمنية تطبيقها في مراحل إجراءات البحث والتحرى وتعقب الجناه وغيرها .

جدول رقم (24)

الدور الاخلاقي المتوقع عند تبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية

الأدوار الاخلاقية	مستوى المعايير			المتوسط الحسابي	الانحراف المعياري
	بدرجة كبيرة	إلى حد ما	لا توجد		
	%	%	%		
احترام قيم المجتمع والحفاظ عليها	33.8	40.6	25.6	3.51	1.092
احترام ثقافة وخصوصية الغير	27.9	49.5	22.6	3.48	1.009
الحفاظ على سرية المعلومات الأمنية	43.5	44.0	12.6	3.43	1.011
توعية الجمهور بالمخاطر المحتملة	35.5	44.8	19.7	3.38	1.020
تقديم المعلومات كاملة دون تزييف	29.5	44.0	26.6	3.36	1.024
المتوسط العام				**3.40**	**1.022**

** دالة إحصائياً عند مستوى 0.01 فأقل * دالة إحصائيا عند مستوى 0.05 فأقل

توضح بيانات الجدول السابق تنوع الأدوار الأخلاقية التى قد تؤديها تطبيقات الذكاء الاصطناعي عند تبنى المؤسسات الأمنية العربية لها، حيث تظهر النتائج أن المبحوثين موافقون بدرجة (متوسطة) على مجموعة الأدوار الاخلاقية لتطبيقات الذكاء الاصطناعي فى المؤسسات الأمنية بمتوسط (3.40 من 5.00) ، وهو متوسط يقع فى الفئة الثانية من المقياس الثلاثي من (2.50- 3.49) وهى الفئة التى تشير إلى (خيار متوسط) بشأن المعايير الاخلاقية المتوقعة عند تبنى تطبيقات الذكاء الاصطناعي فى المؤسسات الأمنية العربية، وهو ما يفسر أهمية المعايير الأخلاقية عند استخدام تطبيقات الذكاء الاصطناعي فى تحليل البيانات وإعادة إنشاء الجرائم بشكل ثلاثي الأبعاد، وتوظيف تقنيات الواقع الافتراضي فى تحليل المشاهد المسجلة، مثل لقطات الكاميرات أو مشاهد الجرائم، والبحث عن أدلة إضافية أو فهم الأحداث بشكل أفضل، إلا أن ذلك لا ينفى وجود بعض المخاطر المحتملة مثل انتهاك خصوصية الأفراد والتعدى على حقوق الملكية الفكرية لدي البعض منهم وعدم احترام ثقافة الغير، وهو ما يتطلب أهمية استخدام وتبنى التطبيقات الذكية بشكل مسؤول وفقًا للقوانين والأنظمة المنصوص عليها، وأن الرقابة البشرية ضرورية لضمان أن تكون القرارات التي تتخذها الأنظمة الذكية عادلة وغير متحيزة.

14- المنافع المتوقعة عند تبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية فى ضوء النظرية الموحدة

جدول رقم (25)

المنافع المتوقعة عند تبنى تطبيقات الذكاء الاصطناعى فى ضوء النظرية الموحدة :

المنافع المتوقعة عند التبنى	مستوى التبنى			المتوسط الحسابي	الانحراف المعياري
	بدرجة كبيرة	إلى حد ما	لا توجد		
	%	%	%		
دقة توثيق المعلومات عن مختلف الجرائم	31.7	43.4	24.9	2.39	0.63
انسيابية المعلومات بين القطاعات الأمنية	19.4	52.9	27.7	2.34	0.63
امكانية تطوير مهارة العاملين بقطاعات الأمن	42.5	38.2	19.3	2.32	0.70
ثراء المعلومات عن الجرائم المعقدة	32.2	38.0	29.8	2.31	0.67
استشراف الجرائم المحتملة والتصدى لها	23.8	49	27.2	2.27	0.73
الأداء الآلى فى البحث الجنائى والتحرى	27.9	48.6	23.6	2.23	0.71
المتوسط العام				**2.24**	**0.66**

** دالة إحصائياً عند مستوى 0.01 فأقل * دالة إحصائيا عند مستوى 0.05 فأقل

توضح بيانات الجدول السابق تنوع استجابات المبحوثين حول المنافع المتوقعة عند تبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية، حيث تظهر النتائج أن المبحوثين موافقون بدرجة (متوسطة) على مجموعة المنافع المتوقعة نتيجة التبنى بمتوسط (2.24 من 5.00) وهو متوسط يقع فى الفئة الثانية من فئات المقياس الثلاثى من (2.50- 3.49)، وهى الفئة التى تشير إلى خيار (متوسط) بشأن المنافع المتوقعة عند التبنى، حيث تظهر النتائج تصدر المنافع المرتبطة بتوثيق المعلومات عن مختلف الجرائم بمتوسط حسابى قدره (2.39)، يليها سهولة انسابية المعلومات بين القطاعات الأمنية بمتوسط حسابى قدره (2.34) ، وتطوير مهارة العاملين بقطاعات الأمن بمتوسط حسابى قدره (2.32)، وثراء المعلومات عن الجرائم المعقدة بمتوسط حسابى قدره (2.31)، واستشراف الجرائم المحتملة والتصدى

لها بمتوسط حسابى قدره (2.27)، والأداء الآلى فى البحث الجنائى والتحرى بمتوسط حسابى قدره (2.23)، ويمكن تفسيرذلك فى ضوء المنافع المتوقع تحقيقها عند تبنى واستخدام تطبيقات الذكاء الاصطناعى ، حيث ترى النسبة الأكبر من المبحوثين أن دقة وتوثيق المعلومات وانسيابها داخل المؤسسة الأمنية من شأنه أن يعزز من القدرات البشرية فى قطاع الأمن من ناحية، وتطبيق الحوكمة والتنبؤ بالتهديدات والمخاطر المحتملة والتصدى لها من ناحية أخرى.

جدول رقم (26)

سهولة استخدام وتبنى تطبيقات الذكاء الاصطناعى فى ضوء النظرية الموحدة :

سهولة الاستخدام والتبنى	مستوى الاستخدام			المتوسط الحسابي	الانحراف المعياري
	بدرجة كبيرة	إلى حد ما	لا توجد		
	%	%	%		
تنوع اليات البحث الجنائى	28.5	49.3	22.2	2.44	0.66
اختصار الوقت فى البحث والتحرى	46.3	31.2	22.4	2.43	0.62
سهولة البحث فى الأدلة الرقمية	26.3	32.7	41.0	2.41	0.59
سهولة اجراءات البحث الجنائى	28.4	51.4	20.2	2.35	0.60
استخدام طائرات الدارون فى انفاذ القانون	34.6	43.9	21.5	2.34	0.66
المتوسط العام				**2.40**	**0.62**

** دالة إحصائياً عند مستوى 0.01 فأقل* دالة إحصائيا عند مستوى 0.05 فأقل

توضح بيانات الجدول السابق تنوع استجابات المبحوثين حول سهولة استخدام وتبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية، حيث تظهر النتائج أن المبحوثين موافقون بدرجة (ضعيفة) على مجموعة فئات سهولة استخدام وتبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية بمتوسط (2.40 من 5.00)، وهو متوسط يقع فى الفئة الأولى من فئات المقياس الثلاثى من (2.49 – 1) وهى الفئة التى تشير إلى خيار (ضعيف) بشأن سهولة استخدام وتبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية، حيث تظهر النتائج بشأن استخدام وتبنى تطبيقات الذكاء الاصطناعى تصدر تنوع آليات البحث الجنائى بمتوسط حسابى قدره (2.44)، يليها اختصار الوقت فى البحث والتحرى بمتوسط حسابى قدره (2.43)، ثم سهولة البحث فى الأدلة الرقمية بمتوسط حسابى قدره (2.41)، وسهولة اجراءات البحث الجنائى وتفسير الأنماط السلوكية للخارجين عن القانون بمتوسط حسابى قدره (2.35)، وسهولة تغطية ومتابعة الأحداث من خلال طائرات الدارون وانفاذ القانون بمتوسط حسابى قدره (2.34)، وهو ما يعنى وجود اجماع من غالبية المبحوثين على أهمية استخدام وتبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية، والذى سوف يكون أكثر فعالية عندما يصبح أمام جهات الضبط والتحقيق خيارات عديدة من الأدلة الجنائية تتمثل فى كمية البيانات الضخمة المتاحة أثناء اجراء التحقيق، بالاضافة إلى امكانية التعرف على بصمة الصوت والصورة والعين بسهولة، وهو ما يقلل من وقت الوصول للجناه وسرعة اصدار الأحكام وانفاذ القانون عليهم .

جدول رقم (27)
التسهيلات المتاحة عند استخدام وتبنى تطبيقات الذكاء الاصطناعى فى ضوء النظرية الموحدة :

التسهيلات المتاحة عند التبنى	مستوى التسيهلات			المتوسط الحسابي	الانحراف المعياري
	بدرجة كبيرة	إلى حد ما	لا توجد		
	%	%	%		
توفير بيئة الكترونية قوية تستوعب كل جديد فى آليات مكافحة الجرائم العابرة للحدود	22.2	47.3	30.4	2.49	0.64
تدريب الضباط وتأهيلهم للتعامل مع هذه التقنيات والاستفادة منها فى اجراءات الضبط وانفاذ القانون	21.2	51.9	26.9	2.47	0.63
توفير الامكانات اللازمة القادرة على مواكبة التطورفى نوعية الجرائم ومنع التهديدات المحتملة	21.2	49.0	29.8	2.41	0.65
دراسة التجارب العالمية الناجحة والاستفادة منها فى تتبع الجرائم الالكترونية بما يدعم الشراكة الدولية	24.5	45.6	29.9	2.33	0.66
تطوير اللوائح التى تدعم الذكاء الاصطناعى فى مكافحة الجرائم الالكترونية والحد من مخاطرها	32.2	46.3	21.5	2.28	0.65
صياغة مبادىء أخلاقية وتشريعية منظمة لعمل الذكاء الاصطناعى فى المؤسسات الأمنية	22.7	60.4	16.9	2.27	0.67
تطوير آليات التعاون بين المؤسسات الأمنية وشركات التقنية فى دعم الأمن السيبرانى دولياً	25.5	57.2	17.3	2.25	0.75
دعم الشركات التكنولوجية العربية للمحتوى الآلى بما يسمح لقطاع الأمن أداء عمله الوظيفى	21.2	57.7	21.1	2.23	0.68
ادراج مقرر تطبيقات الذكاء الاصطناعى بالجامعات العربية بكليات الحقوق والاعلام والحاسبات والعلوم العسكرية والشرطية	25.5	50.5	24.0	2.22	0.70
المتوسط العام				**2.34**	**0.71**

** دالة إحصائياً عند مستوى 0.01 فأقل * دالة إحصائيا عند مستوى 0.05 فأقل

توضح بيانات الجدول السابق تنوع استجابات المبحوثين حول التسهيلات المتاحة عند استخدام وتبنى المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى ، حيث تظهر النتائج أن المبحوثين موافقون بدرجة (ضعيفة) على مجموعة فئات تسهيلات عملية الاستخدام والتبنى بمتوسط (2.34 من 5.00)، وهو متوسط يقع فى الفئة الأولى من فئات المقياس الثلاثى من (1-2.49)، وهى الفئة التى تشير إلى خيار (ضعيف) بشأن التسهيلات المتاحة عند استخدام وتبنى المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى، حيث تصدرت التسهيلات المتاحة عبارة" توفير بيئة الكترونية قوية تستوعب كل جديد فى آليات مكافحة الجرائم العابرة للحدود"بمتوسط حسابى قدره (2.49)، يليها تدريب الضباط وتأهيلهم للتعامل مع التقنية الحديثة والاستفادة منها فى عمليات الضبط وانفاذ القانون بمتوسط حسابى قدره (2.47)، وتوفير الامكانات اللازمة القادرة على مواكبة التطور فى أساليب ارتكاب الجرائم والقبض على مرتكبيها بمتوسط حسابى قدره (2.41)، ودراسة التجارب العالمية الناجحة والاستفادة منها فى تتبع الجرائم الالكترونية بمتوسط حسابى قدره (2.33)، وتطوير اللوائح التى تدعم

تطبيق الذكاء الاصطناعى فى مكافحة الجرائم والحد من مخاطرها بمتوسط حسابى قدره (2.28)، وصياغة مبادىء أخلاقية وتشريعية منظمة لعمل الذكاء الاصطناعى بمتوسط حسابى قدره (2.27)، وتطوير آليات التعاون بين المؤسسات الأمنية وشركات التقنية فى دعم الأمن السيبرانى بمتوسط حسابى قدره (2.25)، ودعم شركات التكنولوجيا العربية لدعم المحتوى الآلى بما يسمح لمؤسسة الشرطة من أداء عملها الوظيفى بمتوسط حسابى قدره (2.23)، وادراج مقرر تطبيقات الذكاء الاصطناعى بالجامعات العربية فى كليات الحقوق وتخصص الاعلام والحاسبات والعلوم العسكرية والشرطية بمتوسط حسابى قدره (2.22)، ويمكن تفسير ما سبق فى ضوء التسهيلات التى تمنحها تطبيقات الذكاء الاصطناعى للمؤسسات الأمنية فى تحليل البيانات وتسريع وتيرة الاستجابة والتصدى للتهديدات ذات البعد الدولى، حيث يمكن لتطبيقات الذكاء الاصطناعى مراقبة البيانات والمعلومات والكشف عن الرسائل المتداولة بين العناصر الخطرة على أمن الدول، وكذلك الجماعات والتنظيمات المتطرفة، والتى تشير إلى احتمال وجود اختراقات أمنية أو أعمال عنف وتخريب، تستوجب تفعيل الأمن السيبرانى عبر التطبيقات الذكية التى تستخدمها المؤسسات الأمنية العربية.

15- ما المعوقات التي تواجه المؤسسات الأمنية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية ؟

جدول رقم (28)

المعوقات التي تواجه المؤسسات الأمنية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية

المعوقات التى تواجه تطبيقات الذكاء الاصطناعى		استجابة أفراد مجتمع الدراسة					المتوسط	الانحراف المعيارى
		موافق بدرجة كبيرة جداً	موافق بدرجة كبيرة	موافق بدرجة متوسطة	موافق بدرجة قليلة	موافق بدرجة قليلة جداً		
قلة العناصر المؤهلة فنياً في مجال الذكاء الاصطناعى بالمؤسسة الأمنية	ت	43	25	19	10	8	3.81	1.279
	%	41.0	23.8	18.1	9.5	7.6		
الافتقار إلى البرامج التدريبية المناسبة فى الكشف عن الأدلة الجنائية الرقمية فى قطاعات الأمن	ت	33	32	26	8	7	3.72	1.177
	%	31.1	30.2	24.5	7.5	6.6		
عدم توفر التجهيزات الكافية لمسايرة التطورات السريعة في مجال تطبيقات الذكاء الاصطناعى	ت	35	30	26	6	9	3.72	1.225
	%	33.0	28.3	24.5	5.7	8.5		
تعثر الإجراءات الإدارية عند تنفيذ البرامج التوعوية الأمنية عبر تطبيقات الذكاء الاصطناعى	ت	36	31	18	14	7	3.71	1.250
	%	34.0	29.2	17.0	13.2	6.6		
ضعف مستوى التأهيل الأمنى لدى بعض العاملين في مجال تطبيقات الذكاء الاصطناعى	ت	32	32	24	14	4	3.70	1.148
	%	30.2	30.2	22.6	13.2	3.8		
عدم توفر الاعتمادات المالية الكافية نحو تبنى تطبيقات الذكاء الاصطناعى	ت	34	30	20	15	7	3.65	1.250
	%	32.1	28.3	18.9	14.2	6.6		

المعوقات التى تواجه تطبيقات الذكاء الاصطناعى		استجابة أفراد مجتمع الدراسة					المتوسط	الانحراف المعيارى
		موافق بدرجة كبيرة جداً	موافق بدرجة كبيرة	موافق بدرجة متوسطة	موافق بدرجة قليلة	موافق بدرجة قليلة جداً		
قلة عدد العناصر المؤهلة في مجال تطبيقات الذكاء الاصطناعى بالمؤسسات الأمنية	ت	35	28	18	16	8	3.63	1.295
	%	33.3	26.7	17.1	15.2	7.6		
عدم وجود إستراتجية محددة لاخلاقيات تطبيق الذكاء الاصطناعي فى المؤسسات الأمنية	ت	34	27	23	14	8	3.61	1.269
	%	32.1	25.5	21.7	13.2	7.5		
عدم وجود أساليب لقياس وتقويم جهود المؤسسات الأمنية في مجالات التوعية الأمنية	ت	25	34	29	15	3	3.59	1.085
	%	23.6	32.1	27.4	14.2	2.8		
ضعف مستوى التأهيل التقني لدى بعض العاملين بالمؤسسات الأمنية في مجال الذكاء الاصطناعى	ت	27	27	29	14	9	3.46	1.243
	%	25.5	25.5	27.4	13.2	8.5		
عدم وجود قناعة لدى بعض المسؤولين بقطاع الأمن من جدوى تطبيقات الذكاء الاصطناعى	ت	27	21	24	23	10	3.30	1.324
	%	25.7	20.0	22.9	21.9	9.5		
المتوسط العام							**3.62**	**0.912**

** دالة إحصائياً عند مستوى 0.01 فأقل * دالة إحصائيا عند مستوى 0.05 فأقل

يتضح من نتائج الجدول السابق ما يلي:

1. موافقة أفراد مجتمع الدراسة (بدرجة كبيرة) على المعوقات التي يمكن أن تواجه المؤسسات الأمنية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية بمتوسط (3.62 من5) ، وهو متوسط يقع في الفئة الرابعة من فئات المقياس الخماسي (من 3.40 إلى أقل من 4.20)، وهي الفئة التي تشير إلى خيار تستخدم بدرجة (كبيرة) .
2. أن غالبية قيم مربع كاي كانت دالة إحصائياً عند مستوى (0.01)، أو (0.05) فأقل، ما يبين تباين وجهات نظر المبحوثين على فقرات المعوقات فيما عدا الفقرة رقم (6)، التي كانت قيمتها غير دالة إحصائياً عند مستوى 0.05 فأقل، ما يبين تجانس وجهات نظر أفراد مجتمع الدراسة على هذه الفقرة .
3. أن غالبية قيم (ت) جاءت لمفردة واحدة كانت دالة إحصائية عند مستوى (0.01) أو (0.05) فأقل، ما يبين أن أفراد الدراسة موافقون على فقرات المعوقات التي يمكن أن تواجه المؤسسات الأمنية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية بدرجة كبيرة .
4. أن هناك تفاوتاً في موافقة أفراد مجتمع الدراسة على المعوقات التي يمكن أن تواجه المؤسسات الأمنية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية، إذ تراوحت متوسطات موافقتهم ما بين (3.30 إلى 3.81)، وهي متوسطات تقع في الفئتين الثالثة والرابعة من فئات المقياس الخماسي، واللتان تشيران إلى (بدرجة متوسطة / بدرجة كبيرة) مما يوضح التفاوت في موافقة أفراد الدراسة على المعوقات التي يمكن أن تواجه

المؤسسات الأمنية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية، إذ يتضح من النتائج أيضاً أن أفراد الدراسة موافقون بدرجة (كبيرة) على عشرة من المعوقات تتمثل في العبارات رقم (1 ، 2 ،3 ، 4 ، 5 ، 7، 8، 9، 10، 11)، والتي تم ترتيبها تنازلياً حسب موافقة أفراد مجتمع الدراسة عليها بدرجة كبيرة، حيث جاءت عبارة "قلة عدة العناصر المؤهلة فنياً في مجال تطبيقات الذكاء الاصطناعى"بالمرتبة الأولى من حيث موافقة المبحوثين على المعوقات التي يمكن أن تواجه المؤسسات الأمنية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية بدرجة كبيرة بمتوسط (3.81 من5)، كما جاءت عبارة" الافتقار إلى البرامج التدريبية المناسبة فى مجال الذكاء الاصطناعى" بالمرتبة الثانية من حيث موافقة المبحوثين على المعوقات التي يمكن أن تواجه المؤسسات الأمنية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية بدرجة كبيرة بمتوسط (3.72 من5)، وجاءت عبارة"عدم توفر التجهيزات التقنية الكافية لمسايرة التطورات السريعة في مجال تطبيقات الذكاء الاصطناعى "بالمرتبة الثالثة من حيث موافقة المبحوثين على المعوقات التي يمكن أن تواجه المؤسسات الأمنية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية بدرجة كبيرة بمتوسط (3.72 من5)، وجاءت عبارة"تعثر الإجراءات الإدارية عند تنفيذ البرامج التوعوية عبر تطبيقات الذكاء الاصطناعى"بالمرتبة الرابعة من حيث موافقة المبحوثين على المعوقات التي يمكن أن تواجه المؤسسات الأمنية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية بدرجة كبيرة بمتوسط (3.71 من 5)، وجاءت عبارة "ضعف مستوى التأهيل الأمنى لدى بعض العاملين في مجال تطبيقات الذكاء الاصطناعى" بالمرتبة الخامسة من حيث موافقة المبحوثين على المعوقات التي يمكن أن تواجه المؤسسات الأمنية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية بدرجة كبيرة بمتوسط (3.70 من5)، وجاءت عبارة" قلة عدد العناصر المؤهلة في مجال تطبيقات الذكاء الاصطناعى "بالمرتبة السابعة من حيث موافقة المبحوثين على المعوقات التي يمكن أن تواجه المؤسسات الأمنية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية بدرجة كبيرة بمتوسط (3.63 من5)، وجاءت عبارة " عدم وجود إستراتجية محددة المؤسسات الأمنية " بالمرتبة الثامنة من حيث موافقة المبحوثين على المعوقات التي يمكن أن تواجه المؤسسات الأمنية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية بدرجة كبيرة بمتوسط (3.61 من5)، وجاءت عبارة "عدم وجود أساليب لقياس وتقويم جهود المؤسسات الأمنية في مجالات التوعية الأمنية "بالمرتبة التاسعة من حيث موافقة المبحوثين على المعوقات التي يمكن أن تواجه المؤسسات الأمنية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية بدرجة كبيرة بمتوسط (3.59 من5)، وجاءت عبارة" ضعف مستوى التأهيل التقني لدى بعض العاملين في مجال الذكاء الاصطناعى "بالمرتبة العاشرة من حيث موافقة المبحوثين على المعوقات التي يمكن أن تواجه المؤسسات الأمنية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية بدرجة كبيرة بمتوسط (3.46 من5)، وجاءت عبارة"عدم وجود قناعة لدى بعض المسؤولين من جدوى توظيف تطبيقات الذكاء الاصطناعى" بالمرتبة الحادية عشرمن حيث موافقة المبحوثين على المعوقات التي يمكن أن

تواجه المؤسسات الأمنية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية بدرجة كبيرة بمتوسط (3.30 من5)..

ويتضح من خلال النتائج السابقة أهمية الذكاء الاصطناعى فى القطاعات الأمنية العربية على الرغم من الصعوبات التى تواجه عمليات التطبيق والتبنى، حيث لم تعُد القدرات البشرية كافية للتعامل مع الجرائم المعقدة، ومن ثم فقد تم الاعتماد على تقنيات الواقع الافتراضي والواقع المعزز عند محاكاة الهجمات الإرهابية وخلق بيئة ثلاثية الأبعاد، وقد طبقت شرطة ويلز فى بريطانيا استخدام تقنيات الذكاء الاصطناعى فى توقيف المتهمين فى القضايا الجنائية، والكشف عن ماضى أصحاب السوابق حال وجودهم فى الأماكن العامة، في المقابل طرحت الامارات فكرة توظيف الذكاء الاصطناعي في مجال الأدلة الجنائية، وكيفية الاستفادة من "الممر الذكي بمطار دبى" فى الكشف عن مرتكبى الجرائم، حيث يتم فحص الركاب القادمين للامارات بمجرد المرور داخل البوابة الإلكترونية، والتى تظهر سلامة الراكب الصحية وخلوه من الأمراض المعدية ووباء كورونا، والمواد الممنوعة مثل المخدرات والمفرقعات والأسلحة بأنواعها .

16- السيناريوهات المقترحة عند استخدام وتبنى المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى:

جدول رقم (29)

اتجاهات المبحوثين نحو سيناريو الثبات فى عملية استخدام وتبنى تطبيقات الذكاء الاصطناعى

اتجاهات سيناريو الثبات	مستوى الاتجاه			المتوسط الحسابي	الانحراف المعياري
	ايجابى	متوسط	سلبى		
	%	%	%		
الاستمرار فى دعم الاجراءات الحالية	35.3	44.0	20.8	2.41	0.85
عدم توافر الامكانات البشرية والمادية	39.9	50.5	9.6	2.27	0.87
عدم اهتمام القيادات الأمنية بعملية التبنى	61.4	30.0	8.7	2.24	0.83
عدم تطوير البنية التكنولوجية لاستيعاب التبنى	45.7	0.5	14.4	2.19	1.00
عدم قناعة العاملين بالمؤسسات الأمنية بالتبنى	30.0	48.3	21.7	2.16	0.94
استمرار العمل باللوائح التقليدية المقيدة للتبنى	31.6	50.0	18.4	2.16	0.92
عدم الاتفاق على ضوابط استخدام التقنية الحديثة	26.6	45.4	28.0	2.12	1.09
اغفال تطوير مهارات العاملين بالمؤسسات الأمنية	33.3	53.6	13.0	2.03	0.96
تضارب حول الفوائد المادية والمعنوية من عملية التبنى	28.2	55.8	16.0	1.96	0.83
المتوسط العام				**2.20**	**0.99**

** دالة إحصائياً عند مستوى 0.01 فأقل * دالة إحصائيا عند مستوى 0.05 فأقل

توضح بيانات الجدول تباين وجهات نظر المبحوثين نحو سيناريوهات تبني تطبيقات الذكاء الاصطناعي فى المؤسسات الأمنية العربية، حيث تظهر النتائج وفق سيناريو الثبات أن المبحوثين موافقون بدرجة (ضعيفة) على فئات سيناريو الثبات بمتوسط (2.20 من5)، وهو متوسط يقع فى الفئة الأولي من فئات المقياس الثلاثي (أقل من 2.49)، وهى الفئة التى تشير إلى خيار (ضعيف) بشأن السيناريو الأول لعملية تبني وتوظيف تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية، وهو ما يعنى أن المؤسسات الأمنية العربية ما تزال مستمرة فى دعم اجراءات التبنى المحدود، يقابل ذلك سرعة نحو تدريب وتأهيل رجال الأمن لديها،

واكسابهم المعرفة والمهارات اللازمة لفهم الأنظمة الذكية عند أداء المهام الوظيفية بشكل فعال.

جدول رقم (30)

اتجاهات المبحوثين نحو سيناريو التفاؤل فى عملية استخدام وتبنى تطبيقات الذكاء الاصطناعى

اتجاهات سيناريو التفاؤل	مستوى الاتجاه			المتوسط الحسابي	الانحراف المعياري
	ايجابى	متوسط	سلبى		
	%	%	%		
ايجاد بيئة داخلية مؤسسية تدعم التبنى	34.0	48.5	17.5	2.59	0.71
تنافس المؤسسات الأمنية فى عملية التبنى	37.5	44.7	17.8	2.25	0.64
تطوير البنية التكنولوجية اللازمة للتبنى	35.3	42.5	22.2	2.12	0.76
تطوير القوانين اللازمة لعملية التبنى	37.7	44.0	17.9	2.10	0.77
مراعاه السياسات الأمنية لجهود التبنى	29.0	46.4	24.6	1.80	0.82
ايجاد صيغة للحوافز لدعم عملية التبنى	34.6	44.7	20.7	1.55	0.82
توفير الامكانات البشرية والمادية اللازمة للتبنى	42.3	45.7	12.0	1.51	1.04
تقوية مهارات العاملين نحو عملية التبنى	33.3	43.5	23.2	1.39	1.20
توفير دعم كاف من الجهات الرسمية نحو التبنى	35.7	50.2	14.0	1.17	0.93
حتمية تبنى الاستخدام فى المؤسسات الأمنية	30.4	48.3	21.3	1.13	0.98
المتوسط العام				2.07	1.12

** دالة إحصائياً عند مستوى 0.01 فأقل * دالة إحصائيا عند مستوى 0.05 فأقل

توضح بيانات الجدول السابق تباين وجهات نظر المبحوثين نحو سيناريوهات تبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية وفق سيناريو التفاؤل، حيث تشير النتائج أن المبحوثين موافقون بدرجة (ضعيفة) على فئات سيناريو التفاؤل بمتوسط (2.07 من5) وهو متوسط يقع فى الفئة الأولى من فئات المقياس الثلاثى (أقل من 2.49)، وهى الفئة التى تشير الى خيار(ضعيف) بشأن السيناريو الثانى لعملية تبنى وتوظيف تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية، وهو ما يفسر حقيقة وجود حالة من التفاؤل الحذر نتيجة التبنى الكامل فى القطاعات الأمنية مستقبلاً، يقابل ذلك تأكيد عدد من المبحوثين على الدورالذى تقوم به تقنيات التعلم الآلي في تقديم حلول مؤكدة فى مجال الأدلة الجنائية والجرائم المعقدة والتعرف على بصمات الأصابع تلقائياً ومقارنة الأقواس والحلقات والدوامات والتي يمكن التحقق منها بشكل آلى .

جدول رقم (31)

اتجاهات المبحوثين نحو سيناريو التشاؤم فى عملية استخدام وتبنى تطبيقات الذكاء الاصطناعى

اتجاهات سيناريو التشاؤم	مستوى الاتجاه			المتوسط الحسابي	الانحراف المعياري
	ايجابى	متوسط	سلبى		
	%	%	%		
تدهور البنية الداخلية التى تدعم التبنى	33.8	35.3	30.9	2.43	0.76
انعدام الخبرة لدى العاملين بالمؤسسة الأمنية	26.1	59.9	14.0	2.42	0.91
تناقص الامكانات المادية المخصصة للتبنى	29.3	46.8	23.9	2.36	0.85
تراجع الاستعانة بخبرات كافية فى عملية التبنى	40.1	36.7	23.2	2.24	0.85
تدنى مستوى برامج التدريب فى التقنية	33.5	53.1	13.4	2.22	0.83

اتجاهات سيناريو التشاؤم	مستوى الاتجاه			المتوسط الحسابي	الانحراف المعياري
	ايجابى	متوسط	سلبى		
	%	%	%		
تنوع التشريعات المقيدة لعملية التبنى	51.1	35	13.9	2.18	0.91
ازدياد القناعات بعدم جدوى عملية التبنى	31.1	49.1	19.1	2.10	0.85
تراجع الامكانات التكنولوجية اللازمة للتبنى	35.4	46.4	18.2	2.06	0.91
غياب المحاسبة القانونية وتبنى الآلة	28.2	47.8	24	1.93	0.86
اخطاء التحريات البشرية المتكررة	33.5	45	21.5	1.92	0.99
المتوسط العام				**2.45**	**0.88**

** دالة إحصائياً عند مستوى 0.01 فأقل * دالة إحصائيا عند مستوى 0.05 فأقل

يتضح من الجدول السابق تباين آراء المبحوثين نحو سيناريوهات تبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية وفق سيناريو التشاؤم ، حيث تظهر النتائج أن المبحوثين موافقون بدرجة (ضعيفة) على فئات سيناريو التشاؤم بمتوسط (2.45 من 5) ، وهو متوسط يقع فى الفئة الأولى من فئات المقياس الثلاثى (أقل من 2.49)، وهى الفئة التى تشير الى خيار (ضعيف) بشأن السيناريو الثالث لعملية تبنى وتوظيف تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية، وهو ما يعنى أن القطاعات الأمنية العربية ومن خلال واقعها الحالى ليست جاهزة لتبنى التطبيقات الأمنية المدعومة بالذكاء الاصطناعى، حيث أكد عدد من المبحوثين أن تحديد الأشخاص المطلوبين يحتاج إلى تطوير وتصميم نظام التعرف على الوجوه، وتعزيز الاجراءات الأمنية باستخدام الكاميرات الذكية CCTV فى رصد الأشخاص المطلوبين أثناء تواجدهم فى الشوارع والأماكن العامة، وهو ما يتطلب تدشين نظام ذكي بقطاعات الأمن المختلفة للتعرف على الجناه من خلال استخدام خوارزميات التعلم العميق وتقنية التعرف على وجوه الأشخاص المطلوبين أمنياً، ومن ناحية التطبيق أخذت الولايات المتحدة بالأدلة الرقمية، وقد نصت علي ذلك في عدة قوانين منها قانون الحاسب الآلي عام 1984م، والذي اعتبر أن الأدلة الناتجة عن الحاسب الآلي مقبولة، كما تضمن ذلك قانون الإثبات لسنة 1983م الصادر بولاية كاليفورنيا والذي نص علي أن النسخ المستخرجة من جهاز الحاسب تكون مقبولة بوصفها أفضل الأدلة المتاحة للإثبات، وقد اشترط المشرع الأمريكي لقبول الأدلة الرقمية أمام المحاكم أن يكون جهاز الحاسب الآلي يؤدى وظائفه بصورة سليمة وان يكون الدليل الرقمي له صلة بالقضية المعروضة والأشخاص المشتبه بهم [104]، وهى مؤشرات توكد على دعم المبحوثين من النخبة الأمنية للسيناريو التفاؤلى فى أهمية واستخدام وتبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية .

17- هل هناك فروق ذات دلالة إحصائية في اتجاهات خبراء الأمن حول مدى استخدام وتوظيف تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية وفقاً للمتغيرات الشخصية والوظيفية ؟

- الفروق باختلاف متغير العمر:

للتعرف على ما إذا كانت هناك فروق ذات دلالة إحصائية في إجابات عينة الدراسة طبقاً إلى اختلاف متغير العمر، استخدم الباحث " تحليل التباين الأحادي" (One Way Anova) لتوضيح دلالة الفروق في إجابات المبحوثين .

الجدول رقم (32)
تحليل التباين الأحادي للفروق في إجابات عينة الدراسة طبقاً لاختلاف متغير العمر

فئات المحور	مصدر التباين	مجموع مربعات	درجات الحرية	متوسط المربعات	قيمة ف	الدلالة الإحصائية
مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية	بين المجموعات	1.593	3	0.531	0.789	0.503
	داخل المجموعات	68.611	102	0.673		
	المجموع	70.204	105			
متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية	بين المجموعات	3.974	3	1.325	1.188	0.318
	داخل المجموعات	113.765	102	1.115		
	المجموع	117.739	105			
مجالات توظيف تطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية	بين المجموعات	0.470	3	0.157	0.205	0.893
	داخل المجموعات	78.109	102	0.766		
	المجموع	78.579	105			
التأثيرات المترتبة على توظيف تطبيقات الذكاء الاصطناعى فى العلوم الجنائية	بين المجموعات	3.014	3	1.005	1.047	0.375
	داخل المجموعات	97.841	102	0.959		
	المجموع	100.854	105			
المعوقات التي يمكن أن تواجه توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية	بين المجموعات	3.543	3	1.181	1.437	0.236
	داخل المجموعات	83.842	102	0.822		
	المجموع	87.385	105			

يتضح من نتائج الجدول السابق عدم وجود فروق ذات دلالة إحصائية عند مستوى (0.05)، فأقل في اتجاهات أفراد مجتمع الدراسة من المبحوثين حول (مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية، متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية، مجالات توظيف المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية، التأثيرات المترتبة على توظيف المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى فى العلوم الجنائية،والمعوقات التي يمكن أن تواجه المؤسسات الأمنية العربية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية) باختلاف متغير العمر.

- الفروق باختلاف متغير الرتبة الوظيفية :

وللتعرف على ما إذا كانت هناك فروق ذات دلالة إحصائية في إجابات أفراد مجتمع الدراسة طبقاً لاختلاف متغير الرتبة الوظيفية استخدم الباحث تحليل التباين الأحادي One Way (Anova) لتوضيح دلالة الفروق في إجابات المبحوثين طبقاً لاختلاف متغير الرتبة الوظيفية، وجاءت النتائج كما يوضحها الجدول الآتي:

الجدول رقم (33)
تحليل التباين الأحادي للفروق في إجابات عينة الدراسة طبقاً لاختلاف متغير الرتبة الوظيفية

فئات المحور	مصدر التباين	مجموع مربعات	درجات الحرية	متوسط المربعات	قيمة ف	الدلالة الإحصائية
مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية	بين المجموعات	1.305	2	0.653	0.976	0.380
	داخل المجموعات	68.899	103	0.669		
	المجموع	70.204	105			
متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية	بين المجموعات	7.633	2	3.817	3.570	×0.032
	داخل المجموعات	110.106	103	1.069		
	المجموع	117.739	105			
مجالات توظيف تطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية	بين المجموعات	3.641	2	1.820	2.502	0.087
	داخل المجموعات	74.939	103	0.728		
	المجموع	78.579	105			
التأثيرات المترتبة على توظيف تطبيقات الذكاء الاصطناعى فى العلوم الجنائية	بين المجموعات	5.049	2	2.524	2.714	0.071
	داخل المجموعات	95.805	103	0.930		
	المجموع	100.854	105			
المعوقات التي يمكن أن تواجه توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية	بين المجموعات	0.755	2	0.377	0.449	0.640
	داخل المجموعات	86.630	103	0.841		
	المجموع	87.385	105			

* دالة عند مستوى 0.05 فأقل

يتضح من نتائج الجدول السابق عدم وجود فروق ذات دلالة إحصائية عند مستوى(0.05) فأقل في اتجاهات أفراد مجتمع الدراسة حول (مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية، متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية، مجالات توظيف المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية، التأثيرات المترتبة على توظيف المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى فى العلوم الجنائية، المعوقات التي يمكن أن تواجه المؤسسات الأمنية العربية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية) باختلاف متغير الرتبة أو المرتبة، في حين يوجد فروق ذات دلالة إحصائية عند مستوى (0.05) فأقل في اتجاهات أفراد مجتمع الدراسة حول (مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية) باختلاف متغير الرتبة الوظيفية، ولتحديد صالح الفروق بين كل رتبة على حدة ؛ تم استخدام اختبار LSD الذي جاءت نتائجه كالآتي:

جدول رقم (34)

نتائج اختبار LSD للتحقق من الفروق بين كل رتبة وظيفية على حدة

المحور	الرتبة الوظيفية	العدد	المتوسط الحسابي	موظف مدني	ضابط	أفراد ، صف ضباط
مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية	موظف مدني	24	1.8802		**	
	ضابط	35	2.6117			
	أفراد ، صف ضباط	47	2.3378			

** دالة عند مستوى 0.01 فأقل

يتضح من نتائج الجدول السابق وجود فروق ذات دلالة إحصائية عند مستوى (0.01) فأقل بين الموظفين المدنيين والضباط حول (مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية) لصاح الضباط، وهذا يعني أن فئة الضباط يرون أن استخدامات تطبيقات الذكاء الاصطناعى ضعيفة مقارنة بالفئات الأخرى.

- الفروق باختلاف متغير جهه العمل:

وللتعرف على ما إذا كانت هناك فروق ذات دلالة إحصائية في إجابات أفراد مجتمع الدراسة طبقاً لاختلاف متغير جهة العمل استخدم الباحث " تحليل التباين الأحادي" One Way) Anova) لتوضيح دلالة الفروق في إجابات أفراد مجتمع الدراسة طبقاً لاختلاف متغير جهة العمل، وجاءت النتائج كما يوضحها الجدول الآتي:

الجدول رقم (35)

تحليل التباين الأحادي للفروق في إجابات عينة الدراسة طبقاً لاختلاف متغير جهة العمل

فئات المحور	مصدر التباين	مجموع مربعات	درجات الحرية	متوسط المربعات	قيمة ف	الدلالة الإحصائية
مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية	بين المجموعات	12.843	6	2.140	3.650	**0.003
	داخل المجموعات	56.890	97	0.586		
	المجموع	69.733	103			
متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية	بين المجموعات	20.989	6	3.498	3.525	**0.003
	داخل المجموعات	96.252	97	0.992		
	المجموع	117.241	103			
مجالات توظيف تطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية	بين المجموعات	8.610	6	1.435	2.025	0.070
	داخل المجموعات	68.735	97	0.709		
	المجموع	77.345	103			
التأثيرات المترتبة على توظيف تطبيقات الذكاء الاصطناعى فى العلوم الجنائية	بين المجموعات	15.769	6	2.628	3.011	**0.010
	داخل المجموعات	84.653	97	0.873		
	المجموع	100.422	103			
المعوقات التي يمكن أن تواجه توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية	بين المجموعات	6.101	6	1.017	1.244	0.291
	داخل المجموعات	79.256	97	0.817		
	المجموع	85.357	103			

** دالة عند مستوى 0.01 فأقل

يتضح من خلال نتائج الجدول السابق عدم وجود فروق ذات دلالة إحصائية عند مستوى(0.05) فأقل في اتجاهات أفراد مجتمع الدراسة حول (مجالات توظيف المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية، والمعوقات التي يمكن أن تواجه المؤسسات الأمنية العربية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية) باختلاف متغير جهة العمل.

في حين يوجد فروق ذات دلالة إحصائية عند مستوى (0.01) فأقل في اتجاهات أفراد مجتمع الدراسة حول (مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية، متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية) باختلاف متغير جهة العمل، ولتحديد صالح الفروق بين كل جهة عمل على حدة تم استخدام اختبار LSD، الذي جاءت نتائجه كالآتي:

جدول رقم (36)

نتائج اختبار LSD للتحقق من الفروق بين كل جهة عمل على حدة

المحور	جهة العمل	العدد	المتوسط الحسابي	الأمن الوطني	مكافحة المخدرات	الجوازات	الدفاع المدني	الأمن العام	أمن المعلومات	المرور
مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية	الأمن الوطنى	7	2.2571	-		*		**		
	مكافحة المخدرات	12	2.1704		-	**	*	**	*	
	الجوازات	19	2.9737			-				*
	الدفاع المدني	35	2.8293				-			*
	الأمن العام	17	3.1647					-		**
	امن المعلومات	7	2.9143						-	
	المرور	7	2.1143							-
متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية	الأمن الوطنى	7	1.2857	-		**	**	**		
	مكافحة المخدرات	12	2.2083		-					
	الجوازات	19	2.5855			-			*	*
	الدفاع المدني	35	2.6439				-		*	**
	الأمن العام	17	2.4779					-		*
	امن المعلومات	7	1.6429						-	
	المرور	7	1.5000							-
مجالات توظيف تطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية	الأمن الوطنى	7	2.2429	-	*	*	**	**		
	مكافحة المخدرات	12	3.2167		--					
	الجوازات	19	3.2789			-				
	الدفاع المدني	35	3.5914				-		*	
	الأمن العام	17	3.6882					-	*	
	امن المعلومات	7	2.7841						-	
	المرور	7	3.0286							-

** دالة عند مستوى 0.01 فأقل * دالة عند مستوى 0.05 فأقل

يتضح من نتائج الجدول السابق ما يلي:

1. وجود فروق ذات دلالة إحصائية عند مستوى (0.01)، فأقل بين اتجاهات أفراد مجتمع الدراسة الذين يعملون في الأمن العام، وأفراد مجتمع الدراسة الذين يعملون في قطاع الأمن

الوطنى حول (مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية، متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية، مجالات توظيف المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية)، لصالح أفراد مجتمع الدراسة الذين يعملون في الأمن العام.

2. وجود فروق ذات دلالة إحصائية عند مستوى (0.01) فأقل بين اتجاهات أفراد الدراسة الذين يعملون في المديرية للدفاع المدني، وأفراد مجتمع الدراسة الذين يعملون قطاع الأمن الوطنى حول (متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية، مجالات توظيف المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية) لصالح أفراد مجتمع الدراسة الذين يعملون في المديرية العامة للدفاع المدني.

3. وجود فروق ذات دلالة إحصائية عند مستوى (0.01) فأقل بين اتجاهات أفراد مجتمع الدراسة الذين يعملون في المديرية العامة للجوازات، وأفرد مجتمع الدراسة الذين يعملون في الأمن الوطنى حول (متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية)، لصالح أفراد مجتمع الدراسة الذين يعملون في المديرية العامة للجوازات

4. وجود فروق ذات دلالة إحصائية عند مستوى (0.01) فأقل بين اتجاهات أفراد مجتمع الدراسة الذين يعملون في المديرية العامة للجوازات، وأفراد مجتمع الدراسة الذين يعملون في المديرية العامة لمكافحة المخدرات حول (مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية)، لصالح أفراد مجتمع الدراسة الذين يعملون في المديرية العامة للجوازات

5. وجود فروق ذات دلالة إحصائية عند مستوى (0.01) فأقل بين اتجاهات أفراد مجتمع الدراسة الذين يعملون في الأمن العام، وأفراد مجتمع الدراسة الذين يعملون في المديرية العامة لمكافحة المخدرات حول (متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية)، لصالح أفراد مجتمع الدراسة الذين يعملون في الأمن العام.

6. وجود فروق ذات دلالة إحصائية عند مستوى (0.01) فأقل بين اتجاهات أفراد مجتمع الدراسة الذين يعملون في الإدارة العامة للمرور، وأفراد مجتمع الدراسة الذين يعملون في المديرية العامة لمكافحة المخدرات حول (متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية) لصالح أفراد مجتمع الدراسة الذين يعملون في الأمن العام .

7. وجود فروق ذات دلالة إحصائية عند مستوى (0.01) فأقل بين اتجاهات أفراد مجتمع الدراسة الذين يعملون في المديرية العامة للدفاع المدني، وأفرد مجتمع الدراسة الذين يعملون في المديرية العامة لمكافحة المخدرات حول (متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية) لصالح أفراد مجتمع الدراسة الذين يعملون في الأمن العام.

8. وجود فروق ذات دلالة إحصائية عند مستوى (0.05) فأقل بين اتجاهات أفراد مجتمع الدراسة الذين يعملون في المديرية العامة لمكافحة المخدرات، وأفراد مجتمع الدراسة الذين يعملون في الأمن الوطنى حول (مجالات توظيف المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية) لصالح أفراد مجتمع الدراسة الذين يعملون في المديرية العامة لمكافحة المخدرات.

9. وجود فروق ذات دلالة إحصائية عند مستوى (0.05) فأقل بين اتجاهات أفراد مجتمع الدراسة الذين يعملون في المديرية العامة للجوازات، وأفراد مجتمع الدراسة الذين يعملون في الأمن الوطنى حول (متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية، مجالات توظيف المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية) لصالح أفراد مجتمع الدراسة الذين يعملون في المديرية العامة للجوازات.

10. وجود فروق ذات دلالة إحصائية عند مستوى (0.05) فأقل بين اتجاهات أفراد مجتمع الدراسة الذين يعملون في المديرية العامة للدفاع المدني، وأفراد مجتمع الدراسة الذين يعملون في المديرية العامة لمكافحة المخدرات حول (مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية)، لصالح أفراد مجتمع الدراسة الذين يعملون في المديرية العامة للدفاع المدني.

11. وجود فروق ذات دلالة إحصائية عند مستوى (0.05) فأقل بين اتجاهات أفراد مجتمع الدراسة الذين يعملون في قطاع الأمن الوطنى وأفراد مجتمع الدراسة الذين يعملون في المديرية العامة لمكافحة المخدرات حول (مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية) لصالح أفراد مجتمع الدراسة الذين يعملون في قطاع الأمن الوطنى.

12. وجود فروق ذات دلالة إحصائية عند مستوى (0.05) فأقل بين اتجاهات أفراد مجتمع الدراسة الذين يعملون في المديرية العامة للجوازات، وأفراد مجتمع الدراسة الذين يعملون في قطاع الأمن الوطنى والإدارة العامة للمرور حول (متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية)، لصالح أفراد مجتمع الدراسة الذين يعملون في المديرية العامة للجوازات.

13. وجود فروق ذات دلالة إحصائية عند مستوى (0.05) فأقل بين اتجاهات أفراد مجتمع الدراسة الذين يعملون في المديرية العامة للدفاع المدني، وأفراد مجتمع الدراسة الذين يعملون في قطاع الأمن الوطنى حول (متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية، مجالات توظيف المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية) لصالح أفراد مجتمع الدراسة الذين يعملون في المديرية العامة للدفاع المدني .

14. وجود فروق ذات دلالة إحصائية عند مستوى (0.05) فأقل بين اتجاهات أفراد مجتمع الدراسة الذين يعملون في الأمن العام، وأفراد مجتمع الدراسة الذين يعملون في قطاع الأمن الوطنى حول (مجالات توظيف المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية)، لصالح أفراد مجتمع الدراسة الذين يعملون في الأمن العام.

15. وجود فروق ذات دلالة إحصائية عند مستوى (0.05) فأقل بين اتجاهات أفراد مجتمع الدراسة الذين يعملون في المديرية العامة للجوازات، وأفراد مجتمع الدراسة الذين يعملون في الإدارة العامة للمرور حول (مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية) لصالح أفراد مجتمع الدراسة الذين يعملون في المديرية العامة للجوازات.

16. وجود فروق ذات دلالة إحصائية عند مستوى (0.05) فأقل بين اتجاهات أفراد مجتمع الدراسة الذين يعملون في المديرية العامة للدفاع المدني، وأفراد مجتمع الدراسة الذين يعملون

في الإدارة العامة للمرور حول (مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية) لصالح أفراد مجتمع الدراسة الذين يعملون في المديرية العامة للدفاع المدني.

17. وجود فروق ذات دلالة إحصائية عند مستوى (0.05) فأقل، بين اتجاهات أفراد مجتمع الدراسة الذين يعملون في الأمن العام، وأفراد مجتمع الدراسة الذين يعملون في الإدارة العامة للمرور حول (متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية) لصالح أفراد مجتمع الدراسة الذين يعملون في الأمن العام .

- الفروق باختلاف متغير عدد سنوات الخبرة :

وللتعرف على ما إذا كانت هناك فروق ذات دلالة إحصائية في إجابات أفرد مجتمع الدراسة طبقاً لاختلاف متغير سنوات الخبرة استخدم الباحث " تحليل التباين الأحادي" One Way) (Anova، لتوضيح دلالة الفروق في إجابات المبحوثين:

الجدول رقم (37)

نتائج " تحليل التباين الأحادي للفروق في إجابات عينة الدراسة طبقاً لاختلاف سنوات الخبرة

فئات المحور	مصدر التباين	مجموع مربعات	درجات الحرية	متوسط المربعات	قيمة ف	الدلالة الإحصائية
مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية	بين المجموعات	1.284	3	0.428	0.633	0.595
	داخل المجموعات	68.921	102	0.676		
	المجموع	70.204	105			
متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية	بين المجموعات	1.380	3	0.460	0.403	0.751
	داخل المجموعات	116.359	102	1.141		
	المجموع	117.739	105			
مجالات توظيف تطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية	بين المجموعات	0.710	3	0.237	0.310	0.818
	داخل المجموعات	77.869	102	0.763		
	المجموع	78.579	105			
التأثيرات المترتبة على توظيف تطبيقات الذكاء الاصطناعى فى العلوم الجنائية	بين المجموعات	3.677	3	1.226	1.286	0.283
	داخل المجموعات	97.178	102	0.953		
	المجموع	97.178	105			
المعوقات التي يمكن أن تواجه توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية	بين المجموعات	6.767	3	2.256	2.854	*0.041
	داخل المجموعات	80.617	102	0.790		
	المجموع	87.385	105			

* دالة عند مستوى 0.05 فأقل

يتضح من نتائج الجدول السابق عدم وجود فروق ذات دلالة إحصائية عند مستوى (0.05) فأقل، في اتجاهات أفراد مجتمع الدراسة حول (مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية، متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية، مجالات توظيف المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى فى الكشف عن

الجرائم الالكترونية، التأثيرات المترتبة على توظيف المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى فى العلوم الجنائية، المعوقات التي يمكن أن تواجه المؤسسات الأمنية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية) باختلاف متغير عدد سنوات الخبرة، في حين يوجد فروق ذات دلالة إحصائية عند مستوى (0.05) فأقل في اتجاهات أفراد مجتمع الدراسة حول(المعوقات التي يمكن أن تواجه المؤسسات الأمنية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية) باختلاف متغير سنوات الخبرة، ولتحديد صالح الفروق تم استخدام اختبار LSD ، الذي جاءت نتائج كالآتي:

جدول رقم (38)

نتائج اختبار LSD للتحقق من الفروق باختلاف متغير عدد سنوات الخبرة

المحور	سنوات الخبرة	العدد	المتوسط الحسابي	أقل من 5 سنوات	من 5 سنوات إلى أقل من 10سنوات	من 10 سنوات إلى أقل من 20 سنة	من 20 سنة فأكثر
المعوقات التي يمكن أن تواجه توظيف الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية	أقل من 5 سنوات	20	3.4095				
	من 5 سنوات إلى أقل من 10 سنوات	18	3.2172				**
	من 10 سنوات إلى أقل من 20 سنة	36	3.7035				
	من 20سنة فأكثر	32	3.9114				

** دالة عند مستوى 0.01 فأقل

يتضح من نتائج الجدول السابق : وجود فروق ذات دلالة إحصائية عند مستوى (0.01) فأقل بين اتجاهات أفراد الدراسة، الذين تتراوح سنوات خبرتهم من 5 سنوات إلى أقل من 10 سنوات، وأفراد مجتمع الدراسة الذين سنوات خبرتهم من 20 سنة فأكثر حول (المعوقات التي يمكن أن تواجه المؤسسات الأمنية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية) لصالح أفراد مجتمع الدراسة الذين تتراوح سنوات خبرتهم من 5 سنوات إلى أقل من 10 سنوات، وهذا يبين أن هذه الفئة لا ترى أن المعوقات مؤثرة مقارنة بالفئات الأخرى.

- الفروق باختلاف متغير الالتحاق بدورات في تطبيقات الحاسب الآلى :

للتعرف على ما إذا كان هنالك فروق ذات دلالة إحصائية في إجابات أفراد مجتمع الدراسة طبقا لاختلاف متغير الالتحاق بدورة في تطبيقات الحاسب الآلى استخدم الباحث اختبار " ت" T-test ، لتوضيح دلالة الفروق بين إجابات أفراد مجتمع الدراسة، وجاءت النتائج كما يوضحها الجدول الآتي:

الجدول رقم (39)

نتائج اختبار " ت: T-test " للفروق بين إجابات عينة الدراسة طبقاً لاختلاف متغير الالتحاق بدورة في مجال تطبيقات الحاسب الآلى

المحور	الالتحاق	العدد	المتوسط	الانحراف	قيمة ت	الدلالة
مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية	لا	18	2.4957	0.69963	-1.526	0.130
	نعم	88	2.8164	0.83284		
متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية	لا	18	2.3403	0.83281	0.068	0.946
	نعم	88	2.3214	109674		
مجالات توظيف تطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية	لا	18	3.5439	0.80618	0.319	0.750
	نعم	88	3.4722	0.88053		
التأثيرات المترتبة على توظيف تطبيقات الذكاء الاصطناعى فى العلوم الجنائية	لا	18	3.3327	0.85171	0.079	0.937
	نعم	88	3.3125	1.00868		
المعوقات التي يمكن أن تواجه توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية	لا	18	3.4035	0.80891	-1.149	0.253
	نعم	88	3.6742	0.92951		

يتضح من نتائج الجدول السابق عدم وجود فروق ذات دلالة إحصائية عند مستوى (0.05) فأقل في اتجاهات أفراد مجتمع الدراسة حول (مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية، متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية، مجالات توظيف المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية، التأثيرات المترتبة على توظيف المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى فى العلوم الجنائية، المعوقات التي يمكن أن تواجه المؤسسات الأمنية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية) باختلاف متغير الالتحاق بدورة تأهيلية في مجال الحاسب الآلى.

- الفروق باختلاف متغير الالتحاق بدورات في الأدلة الجنائية الرقمية:

للتعرف على ما إذا كانت هناك فروق ذات دلالة إحصائية في إجابات أفراد مجتمع الدراسة طبقاً لاختلاف متغير الالتحاق بدورات في مجال الأدلة الجنائية الرقمية استخدم الباحث اختبار "ت" T-test "، لتوضيح دلالة الفروق بين إجابات أفراد مجتمع الدراسة، وجاءت النتائج كما يوضحها الجدول الآتي:

الجدول رقم (40)

نتائج اختبار " ت" T-test للفروق بين إجابات عينة الدراسة طبقاً لاختلاف متغير الالتحاق بدورات في مجال الأدلة الجنائية الرقمية

فئات المحور	الالتحاق	العدد	المتوسط	الانحراف	قيمة ت	الدلالة
مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية	لا	63	2.6852	0.77862	-1.172	0.244
	نعم	43	2.8744	0.86880		
متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية	لا	63	2.2446	0.98309	-0.941	0.349
	نعم	43	2.446	0.98309		

فئات المحور	الالتحاق	العدد	المتوسط	الانحراف	قيمة ت	الدلالة
مجالات توظيف تطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية	لا	63	3.4635	0.90884	-0.300	0.765
	نعم	43	3.5150	0.80622		
التأثيرات المترتبة على توظيف تطبيقات الذكاء الاصطناعى فى العلوم الجنائية	لا	63	3.3236	0.98592	0.097	0.923
	نعم	43	3.3047	0.95525		
المعوقات التي يمكن أن تواجه توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية	لا	63	3.5014	0.95525	-1.749	0.083
	نعم	43	3.8140	0.82105		

يتضح من نتائج الجدول السابق عدم وجود فروق ذات دلالة إحصائية عند مستوى (0.05) فأقل في اتجاهات أفراد مجتمع الدراسة حول (مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية، متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية، مجالات توظيف المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية، التأثيرات المترتبة على توظيف المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى فى العلوم الجنائية، المعوقات التي يمكن أن تواجه المؤسسات الأمنية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية) باختلاف متغير الالتحاق بدورة تأهيلية في مجال الأدلة الجنائية الرقمية.

الفروق باختلاف متغير الالتحاق بدورات تأهيلية في تطبيقات الذكاء الاصطناعى.

للتعرف على ما إذا كانت هناك فروق ذات دلالة إحصائية في إجابات أفراد الدراسة طبقاً لاختلاف متغير الالتحاق بدورات تأهيلية في تطبيقات الذكاء الاصطناعى استخدم الباحث اختبار"ت" لتوضيح دلالة الفروق بين إجابات أفراد مجتمع الدراسة، وجاءت النتائج كما يوضحها الجدول الآتي:

الجدول رقم (41)

نتائج اختبار " ت" T-test " للفروق بين إجابات عينة الدراسة طبقاً لاختلاف متغير الالتحاق بدورات تأهيلية في تطبيقات الذكاء الاصطناعى

المحور	الالتحاق	العدد	المتوسط	الانحراف	قيمة ت	الدلالة
مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية	لا	75	2.6676	0.79111	-1.870	0.064
	نعم	31	2.9903	0.84867		
متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية	لا	75	2.2905	1.11313	0.515	0.608
	نعم	31	2.2905	0.92644		
مجالات توظيف تطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية	لا	75	3.4785	0.90412	-0.108	0.914
	نعم	31	3.4985	0.77633		
التأثيرات المترتبة على توظيف تطبيقات الذكاء الاصطناعى فى العلوم الجنائية	لا	75	3.2865	1.03648	-0.0523	0.603
	نعم	31	3.3871	0.83934		
المعوقات التي يمكن أن تواجه توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية	لا	75	3.5618	0.93632	-1.168	0.246
	نعم	31	3.7889	0.84416		

يتضح من نتائج الجدول السابق عدم وجود فروق ذات دلالة إحصائية عند مستوى(0.05) فأقل في اتجاهات أفراد مجتمع الدراسة حول (مدى استخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية، متطلبات توظيف تطبيقات الذكاء الاصطناعى فى علوم الأدلة الجنائية، مجالات توظيف المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية، التأثيرات المترتبة على توظيف المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى فى العلوم الجنائية، المعوقات التي يمكن أن تواجه المؤسسات الأمنية عند توظيف تطبيقات الذكاء الاصطناعى فى الجرائم الالكترونية) باختلاف متغير الالتحاق بدورة تأهيلية في تطبيقات الذكاء الاصطناعى.

مناقشة النتائج العامة للدراسة :

1- تظهر نتائج الدراسة ارتفاع معدل متابعة الخبراء فى المؤسسات الأمنية العربية لتطبيقات الذكاء الاصطناعى ورصد أساليب توظيفها فى مكافحة الجرائم الالكترونية، وهو ما انعكس بدرجة كبيرة على اهتمام مماثل من جانب المؤسسة الأمنية العربية ودعم العاملين لديها من خلال دورات متخصصة فى الحاسب الآلى والأدلة الجنائية والذكاء الاصطناعى والأمن السيبرانى والتزييف العميق والسلوكيات المهددة للأمن الوطنى .

2- كشفت نتائج الدراسة جاهزية المؤسسات الأمنية العربية نحو استخدام وتبنى تطبيقات الذكاء الاصطناعى بدرجة متوسطة بنسبة (72.6)، وجاهزة بشكل كامل بنسبة (16.9)، وغير جاهزة بنسبة (10.5)، وهى مؤشرات تؤكد على أن مستوى الجاهزية نحو التبنى فى قطاعات الأمن جاء متوسطاً ، حيث ما تزال عملية التتبنى تتسم بالبطىء والتوظيف المحدود فى قطاعات أمنية بعينها منها، قطاعات المرور والجوازات والأحوال المدنية وأمن المطارات والموانىء، ورغم الاستخدام المحدود لتطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية ما تزال عمليات الاستخدام والتبنى فى مراحلها الأولى، وأن نتائج التبنى المتوقعة مستقبلاً كما يرى الخبراء سوف تكون ايجابية بنسبة بلغت (51.9) .

3- أوضحت نتائج الدراسة تنوع وتعدد دوافع تبنى المؤسسات الأمنية العربية لتطبيقات الذكاء الاصطناعى فى قطاعاتها المختلفة، والتى جاءت بمستويات مرتفعة، حيث تأتى دوافع مثل "التنافس بين القطاعات الأمنية، وتحليل البيانات الضخمة والمعقدة، وزيادة كفاءة العامل البشرى بقطاع الأمن، وعرض البيانات بصور متعددة، وسهولة وسرعة تبادل المعلومات الأمنية على المستوى المحلى والدولى"، وهى مؤشرات تدلل على امكانية الاستخدام والتبنى وخاصة بعد نجاح التجربة فى العديد من البلدان، حيث تم تطبيقها بشكل آمن فى قطاعات انتاجية مختلفة .

4- أظهرت نتائج الدراسة تنوع استخدام وتبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية، حيث تصدر استخدامها فى "انشاء قواعد بيانات ضخمة للجرائم بأنواعها، بالاضافة إلى إدارة منصات وحسابات المؤسسات الأمنية عن بُعد، وتنظيم العمل داخل قطاعات المؤسسة الأمنية بكفاءة عالية، وسهولة الوصول إلى الأدلة الجنائية المصاحبة للجرائم الالكترونية"، وهو ما يفسر مزايا تطبيقات الذكاء الاصطناعي في عمل الشرطة والتى تتمثل في قدرتها على تحليل كميات هائلة من البيانات في غضون ثواني معدودة، ومعالجة المعلومات من مصادر متعددة عبر كاميرات المراقبة وقواعد البيانات الجنائية

والبصمات وبصمة الوجهة، وتحديد الأنماط بسرعة وتوليد رؤية استباقية قابلة للتنفيذ. وهذا يساعد الشرطة وقطاع إنفاذ القانون في الاستجابة بشكل استباقي للتهديدات المحتملة .

5- أوضحت نتائج الدراسة تنوع متطلبات تبنى وتوظيف تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية ، حيث تصدر أهمية "الاستعانة بنماذج دولية ناجحة قابلة للتطبيق فى البيئة العربية، بالاضافة إلى ضرورة تقليل الفجوة بين العاملين فى القطاع الأمنى، ومساعدة المحققين في تحليل الأدلة وإيجاد الصلات بين الحالات التي تبدو غير ذات صلة، وإعادة إنشاء الجرائم بشكل ثلاثي الأبعاد فى الواقع الافتراضي، وتحليل المشاهد المسجلة عبر الكاميرات الذكية، والبحث عن أدلة إضافية أو فهم الأحداث بشكل أفضل.

6- كشفت نتائج الدراسة أهمية تطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم بأنواعها التقليدية والمستحدثة، حيث تصدرت "جرائم الارهاب والاحتيال المالى واختراق الحسابات البنكية للعملاء وعمليات التجسس قائمة الجرائم الالكترونية،حيث يمكن للجماعات الإجرامية غسل الأموال غير المشروعة والقيام بعمليات شراء وبيع للأصول الافتراضية عن طريق تحميل محتويات افتراضية إلى سوق الميتافيرس ثم الشراء من خلال شركات وهمية أو شركات مشبوهة الملكية بالعملة المستخدمة فقط داخل Metaverse Coin التي من المتوقع إساءة استخدامها في عمليات غسل الأموال غير المشروعة مستقبلًا؛ وذلك لكون المستخدم يبتكر الصور الرمزية بشكل مجهول، ومن ثم يمكن شراء عملة الميتافيرس بأموال حقيقية وتستبدل بها أموال حقيقية، ورغم ذلك هناك اتفاق بين خبراء الأمن على امكانية استخدام وتبنى تطبيقات الذكاء الاصطناعى للحد الجرائم وخاصة التى ترتبط بالأموال والحسابات البنكية.

7- تبين نتائج الدراسة تنوع وظائف تطبيقات الذكاء الاصطناعى وامكانية الحد من الجرائم بأنوعها ، حيث جاءت وظيفة كونها" تطبيق ذكى لا يفرق بين الثقافات والجنسيات عند التعامل من الجرائم، والقدرة على توثيق المخالفات غير القانونية، وامكانية اتاحة البيانات الضخمة لمنع حدوث الجرائم المتشابهة، وتفعيل مراقبة ورصد الجرائم بكافة أشكالها، وهى وظائف يرى خبراء الأمن امكانية تطبيقاتها عبر تطبيقات الذكاء الاصطناعى ، والتى سوف تسهم فى الحد من ارتكاب الجريمة بمختلف أشكالها، حيث تصدرت مراقبة السلوك الاجرامى، والكشف عن الجريمة عند حدوثها ، ومتابعة انفاذ القانون بعد ثبوتها، وتوافر الأدلة الجنائية الكافية مجموعة الوظائف التى من الممكن أن تقوم بها تطبيقات الذكاء الاصطناعى، حيث يمكن من خلال الدليل الرقمي رصد المعلومات عن الجاني وتحليلها في الوقت ذاته، كما يمكن للدليل الرقمى تسجيل تحركات الفرد وسلوكياته وبعض الأمور الشخصية عنه.

8- تظهر نتائج الدراسة تنوع تطبيقات الذكاء الاصطناعى فى مكافحة الجرائم الالكترونية ، حيث تصدرت تطبيقات "تقنية التحليل Seo Crime، وتقنية الواقع المعزز VR، وتقنية البحث فى الصور Image Search، وتقنية Chat Gpt، وتقنية التصوير الآلى Photo Robot، وهى تطبيقات ذكية يرى خبراء الأمن استخدامها فى المراقبة والكشف عن الجرائم ، وقد أثبتت قدرتها فى تقديم الجناة إلى محاكمات عادلة، وبالرغم من الإمكانات الهائلة التي يوفرها الذكاء الاصطناعي ودوره المركزي في جمع الأدلة الجنائية، وتعامله مع كميات

ضخمة من البيانات بكفاءة تفوق قدرات البشر، إلا أنه لا يزال يفتقد بشكل تام القدرة على التمييز بين ما هو حقيقي وما هو خيال، وبالتالي فإن الحديث عن استخدام تطبيق الذكاء الاصطناعي مثل Chat GPT في الكشف عن الجرائم المعقدة قد لا يكون السبيل الأمثل فى ذلك بالرغم من قدرته الهائلة في جلب البيانات حسب الطلب، وهو ما يفسر قيام أحد المستخدمين باعطاء تطبيق مثل (Auto GPT) أمرًا نصيًّا يطلب منه القيام بأية مهمة تكسبه (100) دولار؛ فقام التطبيق برحلة أتمتة، وقام ببناء هوية وموقع إلكتروني لمشروع تسوق، ثم حدد منتجاً مناسباً يمكن تسويقه ، وخلال يوم واحد فقط حصل المستخدم على (25) ألف دولار عبر تقنية الذكاء الاصطناعى (Auto GPT) والتى تم توظيفها فى التسويق المضلل لمنتج غير موجود.

9- أظهرت نتائج الدراسة تعدد صور الجرائم الالكترونية والتي كشفت عن أنماط جديدة من السلوك الإجرامي، منها ما يتصل بالاعتداء على أمن الدولة من جهة الخارج أو الداخل، كالإرهاب الإلكتروني أو التحريض على ارتكاب بعض أفعال التعدي على أجهزة الدولة ومؤسساتها، ومنها ما يتصل بالاعتداء على الأشخاص أو الأموال، كجرائم الاتجار بالبشر أو ترويج المخدرات أو الاحتيال والنصب أو غيرها من الجرائم التي ترتكب عبر تطبيقات الانترنت، ومن المتوقع ازدياد أهمية الدليل الرقمي في الحقل الجنائي، وهو ما سيتطلب من جهات إنفاذ القانون إجراء تغييرات جذرية في طرق جمع الأدلة وآليات التعاون الدولي بالشكل الذي يتناسب وطبيعة هذه النوعية المستحدثة من الأدلة الجنائية.

10- . توصلت نتائج الدراسة إلى تعدد مجالات توظيف المؤسسات الأمنية العربية لتطبيقات الذكاء الاصطناعى فى الكشف عن الجرائم الالكترونية، حيث تصدرت مجالات التوظيف فى" تتبع مسار مرتكب الجريمة، والكشف عن اختراقات الحسابات البنكية، والوصول للبصمة الوراثية بصور متعددة، والكشف عن الجثث مجهولة الهوية والمدفونة فى تحت سطح الأرض، وتتبع أماكن زراعة المخدرات وأوكار تجارتها، وفى المقابل يرى الباحث أن السلوك البشرى هو الحرك الأساسى للجرائم على اختلاف بيئتها ، وأن الذكاء الاصطناعي ليس سوى "خوارزميات بحث" في البيانات الضخمة Big Data ، متى عثر على ما يطابق المطلوب قدمه على أنه المعلومة والرأى الصواب، وربما تكون عكس ذلك تماماً.

11- أشارت نتائج الدراسة الى تنوع التأثيرات المترتبة على توظيف المؤسسات الأمنية لتطبيقات الذكاء الاصطناعى، حيث جاءت التأثيرات بصورة كبيرة فى "تحليل البيانات الضخمة والمعقدة، والتنبؤ بالهجمات والتهديدات المتوقعة، واثراء التحقيقات بالمعلومات المتنوعة، والتحقق من مصداقية الصور المتداولة، وتعزيز الحماية الشخصية والفكرية، ودعم المؤسسات الحيوية بالأمن السيبرانى، وهى مؤشرات تؤكد على ايجابية التأثيرات المتوقعة عند توظيف تطبيقات الذكاء الاصطناعى فى مكافحة الجرائم الالكترونية وأن تحليل البيانات الضخمة والمعقدة فى اثبات الجرائم من شأنها أن تسهم فى سرعة رصد الجريمة والكشف عنها بدقة وشفافية، فالإثبات في المواد الجنائية ما هو إلا كافة الأدلة التي تؤكد وقوع الجريمة، وتحقق حالة اليقين لدى القاضي للفصل في الدعوى فإما يقضى بالإدانة، أو ترجح حالة الشك لديه فيقضى بالبراءة.

12- أجمع خبراء الأمن على مجموعة من الفوائد عند توظيف تطبيقات الذكاء الاصطناعى فى الكشف عن الأدلة الجنائية المصاحبة للجرائم الالكترونية، حيث أكدوا على فائدة "عامل السرعة فى عملية البحث والتحرى عن الجريمة محل التحقيق والاثبات، بالاضافة إلى كونها توفر بيئة عمل مريحة لرجال الأمن من وقت وجهد كبيرين، والتخلص من الروتين، وسهولة انفاذ القانون، وهى مؤشرات تثبت أهمية عنصر السرعة فى الحصول على الأدلة الجنائية فى الجرائم الالكترونية عند تطبيق تقنيات الذكاء الاصطناعى.

13- يرى غالبية خبراء الأمن وجود تأثيرات سلبية من الممكن أن تنتج عن استخدام وتبنى تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية، حيث تصدرت جملة من السلبيات أبرزها " التعدى على حقوق الملكية الفكرية، وكثرة الشائعات، وتسريب المعلومات، والتلاعب بالصور، وتجاوز المعايير المهنية والأخلاقية، وسرقة المواقع والمنصات الرقابية، وهو ما يفسر حقيقة أن التقنية الذكية بقدر ما لها من مزايا وفوائد، بقدر ما يقابلها من سلبيات والتى تمثل تحدياً أمام المؤسسات الأمنية فى مجال مكافحة الجرائم ، فالقوانين الأمريكية على سبيل المثال نصت صراحة علي أنه يجب علي الخصم عند تقديمه دليلاً رقمياً أن يثبت صحة ما يدعيه.

14- أظهرت نتائج الدراسة أهمية الدور الوظيفى لتطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية، حيث تصدر " قدرتها فى تحقيق الادارة الذكية فى البحث الجنائى والاستدلال القانونى، واستشراف النتائج فى الجرائم الالكترونية بدقة عالية، بالاضافة الى كونها استطاعت توفير الوقت والجهد البشرى فى مجال البحث والتحرى وانفاذ القانون ، وكذلك تنوع مصادر الأدلة الجنائية وارتفاع مستوى مصداقيتها، وهو ما قد يسهم فى سرعة صدور الاحكام فى الجرائم المعقدة، حيث أعطى القانون المصري على سبيل المثال الحق لجهة التحقيق المختصة في اصدار أمر بضبط أو سحب أو جمع أو التحفظ علي البيانات والمعلومات أو أنظمة المعلومات أو تتبعها في أي مكان أو نظام أو دعامة الكترونية أو حاسب تكون موجودة فيه، وأن يتم تسليم أدلتها الرقمية الي الجهة مصدرة الأمر من قضاء أو نيابة عامة.

15- توصلت نتائج الدراسة الى أهمية الدور المهنى المتوقع نتيجة تبنى تطبيقات الذكاء الاصطناعى، حيث تصدرت أدوار "الدقة فى نتائج التحقيقات، وموضوعية وشفافية الأحكام، وحرية تبادل المعلومات وسريتها بالاضافة إلى أهمية المعلومات وتنوع مصادرها، وامكانية التفاعل والمشاركة الآنية فى المؤسسات ذات الاختصاص، وتصحيح المعلومات وتدارك الخطأ بسرعة وسهولة، وهو ما يفسر أهمية الدور المهنى فى حال تبنى التطبيقات الذكية فى الكشف عن الجرائم الالكترونية وتقديم الجناه لجهات انفاذ القانون، ورغم ذلك لا زالت تتوجس المؤسسات الأمنية من الآثار السلبية التي قد يخلفها الذكاء الاصطناعي مثل: الشفافية والمصداقية والموضوعية وأصالة البيانات والمعلومات؛ وذلك كون الذكاء الاصطناعي يتعامل مع بيانات مبنية على مدخلات البشر الذين يحملون- بالضرورة- مواقفهم الفكرية، وانتماءاتهم الأيديولوجية، وتحيزاتهم المعرفية، ومن ثم فقد تأتى المخرجات بنتائج معروفة سلفاً .

16- أكدت نتائج الدراسة أهمية الدور الأخلاقى عند استخدام وتبنى تطبيقات الذكاء الاصطناعى فى رصد الجرائم الالكترونية والكشف عنها، حيث تصدر : أهمية احترام قيم المجتمع والحفاظ عليها، واحترام ثقافة وخصوصية الغير ، والحفاظ على سرية المعلومات بالمؤسسات الأمنية، بالاضافة إلى أهمية التوعية من المخاطر المحتملة فى أوقات الأزمات، وأهمية تقديم المعلومات بشفافية، وهو ما يفسر حقيقة اهتمام المجتمع الدولى بالدور الأخلاقى الذى قد يصاحب تبنى واستخدام تطبيقات الذكاء الاصطناعى باعتبارها قطاعات تعتمد فى أداءها الوظيفى والمهنى على سرية المعلومات والبيانات، ويعتقد الباحث أنه ورغم كل المواثيق التى حاولت وضع أخلاقيات للتعامل مع التقنية الذكية إلا أن القواعد القانونية والأخلاقية المنظمة لها لا تزال غير واضحة، وقد يواجه المحققون صعوبات في الحصول على بعض البيانات التي تتصل بإدارة بيانات المستخدم؛ مثل الخدمات المالية وخدمات الدفع، إذا كانت الخدمة المتضمنة في الحادث تستخدم مواردها الخاصة؛ حيث يتم تخزين البيانات في البنية التحتية للمزود ، ولهذا السبب كان على المحققين طلب البيانات ذات الصلة بالحادثة، وقد يكون إجراء جمع البيانات مستحيلًا، حينما لا يكون هناك التزام قانوني على مزود الخدمة بتوفير البيانات، والسؤال المطروح من يضع تلك القواعد، ومن يفرضها ، وما هى الآليات التى تكفل تطبيق تلك القواعد بفاعلية ؟

17- توصلت نتائج الدراسة الى مجموعة من الفوائد المتوقعة عند استخدام وتبنى تطبيقات الذكاء الاصطناعى فى ضوء النظرية الموحدة، حيث جاءت الفوائد ممثلة فى "دقة توثيق المعلومات عن مختلف الجرائم ، وانسابية المعلومات التى سوف تصبح متاحة بكل سهولة ويسر، بالاضافة الى امكانية تطوير مهارة العاملين بقطاع الجريمة والأمن السيبرانى، وثراء وتنوع الأدلة الجنائية التى سوف تصاحب الجرائم التى تخضع للتطبيقات الذكية، وهى مؤشرات تؤكد على امكانية تحقيق فوائد عديدة عند استخدام وتبنى تطبيقات الذكاء الاصطناعى، فادارة الشرطة في ولاية نيويورك بالولايات المتحدة على سبيل المثال تملك وحدة خاصة لمواقع التواصل الاجتماعي مهمتها البحث في فيسبوك وتوتير واليوتيوب من أجل البحث عن أدلة أو ضبط أي نشاط إجرامي يتم من خلالها، أما بالنسبة للإجراءات المستخدمة فى جمع البيانات من هذه المنصات فهي مماثلة لتلك المستخدمة مع إنترنت الأشياء والأجهزة المحمولة، إلا أنه بالنظر إلى التطورات المتلاحقة في تطبيقات الذكاء الاصطناعى، فإنه يجب أن يراعى في الاعتبار الأجهزة الطرفية التى يتم ربطها بهذه التطبيقات فى العالم الحقيقي؛ حيث يتم نقل البيانات الخاصة بتلك التطبيقات على الأجهزة الأخرى.

18- .أظهرت نتائج الدراسة أن سهولة تبنى واستخدام تطبيقات الذكاء الاصطناعى قد يسهم فى تطوير أداء القطاعات الأمنية العربية وذلك من خلال "تنوع آليات البحث الجنائى فى مختلف الجرائم، واختصار الوقت والجهد فى عملية التحرى ، والكشف عن الأدلة الجنائية، بالاضافة الى سهولة اجراءات البحث الجنائى، واستخدام طائرات الدارون فى انفاذ القانون ، وهى مؤشرات تدلل على أن تبنى واستخدام تطبيقات الذكاء الاصطناعى من شأنه أن يمنح القائمين على التحقيقات فى الجرائم المختلفة تنوعاً فى الأدلة التى تم التوصل اليها، وهو ما

يعطى سهولة فى البحث الجنائى الرقمي وسرعة اجراءات التحرى وسهولة انفاذ القانون بحق مرتكبى الجرائم بأنواعها .

19- توضح نتائج الدراسة أن تطبيقات الذكاء الاصطناعى سوف تمنح المؤسسات الأمنية العربية مجموعة من التسهيلات عند التطبيق فى القطاعات الأمنية يتصدرها" توفير بيئة الكترونية تستوعب كل جديد من آليات مكافحة الجرائم العابرة للحدود، وتدريب وتأهيل الضباط ومعاونيهم للتعامل مع التطبيقات الذكية والاستفادة منها فى اجراءات الضبط وانفاذ القانون، بالاضافة الى توفير الامكانات اللازمة لمواكبة التطور فى نوعية الجرائم ، ومنع التهديدات المحتملة ، وأهمية التجارب الدولية الناجحة فى تتبع مسارات الجريمة بما يدعم الشراكة الدولية فى القطاعات الأمنية، وهو ما يفسر حقيقة أن التسهيلات سوف تكون اضافة فى مجالات مراقبة الجناه ومعتادى الإجرام، وامكانية مراقبتهم عن باستخدام System Telemetric كوسيلة لمراقبة الأشخاص، والحصول على معلومات تتعلق بوظائف أعضائهم وحالتهم العصبية عن بُعد بواسطة موجات كهربائية، وخاصة ما يتعلق منها بالتنفس، والضغط العصبي ونسبة الأدرينالين في الدم، والتى إذا اجتمعت مع معرفة مكان وُجُود الشخص كانت ذات دلالة على أن هناك شيئًا غير مشروع سوف يحدث، وفي هذه الحالة يُمكن إبلاغ رجل الشرطة أو ضابط الاختبار الذي يتابعه.

20- كشفت النتائج وجود عدد من المعوقات تحول دون اتمام عملية تبنى واستخدام تطبيقات الذكاء الاصطناعى تصدرها " قلة العناصر المؤهلة فى تقنيات الذكاء الاصطناعى، والافتقار الى البرامج التدريبية المناسبة فى مجال الكشف عن الأدلة الرقمية فى القطاعات الأمنية، بالاضافة إلى عدم توافر التجهيزات الفنية الكافية لمسايرة التطورات السريعة فى مجال الذكاء الاصطناعى ، ووجود إجراءات إدارية معقدة فى تنفيذ البرامج التوعية بالتقنية الذكية، وضعف مستوى التأهيل الأمنى لدى العاملين بالقطاعات الأمنية المختلفة مع قلة المخصصات المالية الكافية فى تبنى واستخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية، وهى مؤشرات تدلل على وجود حالة من التبنى فى عدد من القطاعات الأمنية العربية عند مكافحة الجرائم الالكترونية، وأن قلة العناصر المؤهلة والافتقار الى البرامج التدريبية المناسبة معوقات قد تختفى بمجرد تكثيف الدورات التى قد تسهم فى اكساب العاملين بالمؤسسات الأمنية بالمهارات والخبرات المناسبة لعملية التبنى .

21- توضح نتائج الدراسة تنوع سيناريوهات تبنى واستخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية، وجاءت الاتجاهات نحو السيناريو الأول (الثبات) ممثلاً فى"الاستمرار فى دعم الاجراءات الحالية نظراً لعدم توافر الامكانات البشرية والمادية، وعدم اهتمام القيادات الأمنية بعملية التبنى، وعدم قناعة العاملين بالمؤسسة الأمنية بجدوى عملية التبنى، وفى السيناريو الثانى (التفاؤل) أجمع خبراء الأمن على أن تبنى واستخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية يرتبط "بايجاد بيئة داخلية مؤسسية تدعم عملية التبنى ، وتنافس المؤسسات الأمنية فى عملية التبنى، وتطوير البنية التكنولوجية اللازمة للتبنى، مع تطوير القوانين الداعمة لعملية التبنى، وفى السيناريو الثالث (التشاؤم) اتفقت غالبية خبراء الأمن على أن صعوبة التبنى تأتى نتيجة " تدهور البنية الداخلية التى تدعم عملية التبنى، وانعدام الخبرة لدى العاملين بقطاع المعلومات بالمؤسسة

الأمنية، مع قلة الميزانية المخصصة لعملية التبنى ،وعدم الاستعانة بخبرات كافية لعملية التبنى، فضلاً عن توقعات زيادة الهجمات السيبرانية الإجرامية والإرهابية؛ الأمر الذي يرتفع معه نسبة المخاطر المتوقع حدوثها على الأمن السيبراني بسبب غياب الرقابة ؛ إذ ان مراقبة عدد كبير جدًا من المستخدمين في وقت واحد لن تكون بالمهمة السهلة، وتكاد أن تكون مستحيلة، خاصةً أن تلك التطبيقات الذكية لم يتم وضع ضوابط منظمة لتشغيلها حتى الآن.

22- أثبتت نتائج الدراسة عدم وجود فروق ذات دلالة احصائية فى اتجاهات خبراء الأمن نحو تبنى واستخدام تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية العربية وفق متغيرات "النوع ، العمر ، سنوات الخبرة ، الرتبة الوظيفية، جهة العمل، والالتحاق بدورات فى الحاسب والأدلة الجنائية والذكاء الاصطناعى.

مقترحات الدراسة :

1. ضرورة تأهيل رجال الضبط على كيفية استخدام الوسائل الفنية الحديثة، حيث إن اكتساب المعرفة والمهارات اللازمة لفهم واستخدام الأدوات والأنظمة المبنية على الذكاء الاصطناعي يؤدي إلى إنجاز بالمهام بشكل فعال.
2. الاطلاع على تجارب الدول المتقدمة في مواجهة الأدلة الجنائية والإثبات عبر مواقع التواصل الاجتماعي وملاحقة مرتكبها وجمع الأدلة، كون هذا النوع من الأدلة يتمثل في شكل معلومات رقمية مسجلة إلكترونيا.
3. تأسيس بنية تحتية ذكية تواكب متغيرات العصر الرقمي، وتحسين أوضاع مكافحة الجرائم المستقبلية من خلال زيادة الميزانية والمخصصات للتوسع في البنى التحتية للحكومة الإلكترونية والاستفادة من الخطط الإستراتيجية للدول التي خاضت التجربة من قبل .
4. تدشين حملات توعية تقوم على تثقيف أفراد المجتمع بإمكانية تطبيق الاعلام الأمني المدعوم بالذكاء الاصطناعي في مكافحة الجرائم الالكترونية، وهو ما يتطلب تضافر جهود مؤسسات الاعلام والأمن فى المجتمع، وأن وعي أفراد المجتمع واستشعارهم المسؤولية يعدان عاملين رئيسيين في تحقيق الأمن والحد من الجرائم بأنواعها.
5. تكثيف البرامج التوعوية الموجهة لأفراد المجتمع، ورفع الوعي بالمخاطر والتهديدات الأمنية، والتعريف بأفضل الممارسات الكفيلة بجعل الذكاء الاصطناعي بيئة آمنة الاستخدام لا سيما في مجال مكافحة الجرائم وتعزيز الأمن.
6. التأكد من أن الذكاء الاصطناعي يعمل لصالح الناس، وأنه قوة من أجل التنمية في المجتمع، من خلال اتخاذ الإجراءات اللازمة لضمان أن يكون تطوير هذا القطاع وطرحه في السوق مرتكزاً على الإنسان، ومستداماً، وآمناً، وشاملاً، ويمكن الوصول إليه، وجديراً بالثقة.
7. التوسع في إعداد الكادر البشري الوطنية وتطوير البُنى التحتية بشكل يتيح تطوير هذه التقنيات وتطبيقاتها، وصياغة السياسات الاقتصادية التي تجذِّب الشركات الكُبرى العاملة في هذا المجال.
8. اجراء دراسة مستقبلية حول سبل توظيف تطبيقات الذكاء الاصطناعى فى مكافحة الارهاب الالكترونى.
9. ضرورة وضع اساليب لقياس وتقويم الجهود العربية فى مجال تطبيقات الذكاء الاصطناعى فى المؤسسات الأمنية .

مصادر ومراجع الدراسة :

1. Dunham، R. S. (2022) Artificial Intelligence، Virtual Reality and Computer-Driven Storytelling. In Multimedia Reporting (pp. 355-367). Springer

2. Sherif Darwish Al-Labban (2022) New approaches to developing the press content industry
http://www.acrseg.org/41440

3. Guzman، A. L.، & Lewis، S. C. (2020). Artificial intelligence and communication: A Human-Machine Communication research agenda. New Media & Society، 22(1)، 70-86

4. Mohamed Abdel-Zaher (2020) Artificial Intelligence Journalism، Badael House for Publishing and Distribution، Cairo. P 23

5.Dalal Al-Agaili (2019) Artificial intelligence and the future of journalism
https://m.annabaa.org/arabic/informatics/18987

6. Biswal، S. K.، & Gouda، N. K. (2020). Artificial Intelligence in Journalism: A Boon or Bane?. In Optimization in Machine Learning and Applications >pp. 155-167

7. Waltzman، Rand، (2022) The Weaponization of Information .The Need for Cognitive Security، Santa Monica، Calif.: RAND Corporation، CT-473، 2022. As of September 12، 2022

8. عبدالرحمن سعيد (2021) **مطالبات بتشريعات تواكب** "الذكاء الاصطناعي".. متاح على الرابط التالى
https://www.alroeya.com/author/3543

9. أحمد ضياء الدين (2010) **مشروعية الدليل في المواد الجنائية**، دار النهضة العربية، القاهرة 2010م ، ص382

10. مركز المعلومات واتخاذ القرار ، **مجلس الوزراء** ، على الرابط التالى
https://www.idsc.gov.eg/Article/details/8980

11. حسين أبو منصور. (2020). الذكاء الاصطناعي وأبعاده الأمنية .**أوراق السياسات الأمنية**،(1)2 ، 01-18.، جامعة نايف للعلوم الأمنية ، بالرياض ، على الرابط التالى :
https://doi.org/10.26735/SKHN3682

12. دور الذكاء الاصطناعي(2020). في تطوير محتوى إدارة الأزمات الإعلامية، **مركز القرار للدراسات** ، الرياض ، 2020

13. ناصر البقمي (2008) مكافحة جرائم المعلوماتية وتطبيقاتها ، **مركز الامارات للبحوث** ، دبى، ص 6

14. محمد عنب (2015) **تكنولوجيا الاثبات الجنائي**، جامعة نايف العربية للعلوم الامنية، الرياض، ص 108

15. الهام شهر زاد (2016) الدليل الرقمى، **مجلة الدراسات القانونية**، جامعة بليدة، العدد 10 الجزائر، ص 196

16. أحمد ماجد،(2018) الذكاء الاصطناعي بدولة الإمارات، وزارة الاقتصاد، **إدارة الدراسات والبحوث**، دبى، ص 34.

17. Venkatesh،V.،Morries،M.G.،Davies،G.B.،&Davies،F.D.(2003) User acceptance of information technology: Toward a unified view" MIS Quarterly، Vol.27، No.(3)،P. 425

18. Williams، Michael D.، Nripendra P. Rana، and Yogesh K. Dwivedi. "The unified theory of acceptance and use of technology (UTAUT): a literature review." Journal of enterprise information management، Vol. 28 No. 3، (2015): p.2.

19. VenkateshV. and zhang X،(2010)، "Unified Theory of acceptance of information technology U.S Vs.China"،Journal of Global Information Technology Management، Vol.13، No.(1)، P.8
20. Fathema، N.، Shannon، D.، & Ross، M.، (2015). "Expanding the Technology Acceptance Model (TAM) to examine faculty use of Learning Management Systems (LMS)". Journal of Online Learning and Teaching.Vol.11، No.(2)،P.p.210-233
21. سعد مفلح حمود (2023) دور أنظمة الذكاء الاصطناعى فى مكافحة الشائعات الالكترونية ، **المجلة العربية للدراسات الأمنية** ، العدد 39 ، الرياض
22. ليلى بن برغوث (2023) الأمن السيبرانى وخصوصية البيانات الرقمية الموجودة فى المواقع الالكترونية الجزائرية فى عصر التحول الرقمى والذكاء الاصطناعى، **المجلة الدولية للإتصال الإجتماعى** ، الجزائر ، المجلد 1، العدد 10
23. عبدالمولى بن اشبيبة (2022) الدليل الإلكتروني في الإثبات الجنائي في القانون المغربي، **مجلة الباحث للدراسات القانونية والقضائية**، عدد 41 ، المغرب ، ص 112
24. علياء عمر كامل ، (2022) دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي، **المجلة التربوية** ، كلية التربية ، جامعة سوهاج ، العدد الثالث ، ص 10.
25. تقي مباركية، (2022) دور الخبرة في إثبات المعاملات الإلكترونية والقواعد الفنية التى تحكمها في اكتشاف الدليل الرقمي، **مجلة العلوم الإنسانية**، جامعة منتوري قسنطينة، مجلد 33، عدد 2 ، الجزائر
26. ممدوح خليل البحر (2022) مدى تأثير الإجراءات القانونية للتفتيش في الوسط الافتراضي على حرية القاضي في تقدير الدليل الإلكتروني والاقتناع به، **مجلة العلوم القانونية** ،جامعة عجمان، مجلد 8، عدد 15
27. خليل سعيدى (2022) الذكاء الاصطناعى والأمن السيبرانى ، **مجلة السلام للعلوم الإنسانية والاجتماعية**، الجزائر، العدد 1 ، المجلد 6
28. عدنان إبراهيم الحجار(2021) الأدلة الرقمية وإثبات الجرائم السيبرانية: ما بين التأصيل والتأويل، **مجلة جامعة الاستقلال**، الرباط ، المجلد 6، العدد 1
29. يعقوب بلبشير (2021) رهانات الأمن السيبراني الوطني في ظل التحول الرقمي: قراءة في التأصيل المعرفي واستراتيجية المواجهة التشريعية، **مجلة كلية القانون الكويتية العالمية** ، كلية القانون الكويتية العالمية مجلد 10، عدد 37
30. علاء الدين فرحات (2021) من الردع النووي إلى الردع السيبراني: دراسة لمدى تحقيق مبدأ الردع في الفضاء السيبراني، **مجلة المفكر، جامعة محمد خيضر بسكرة** ، الجزائر ، مجلد 16، عدد 1
31. توفيق عبدالله الخشاشنة (2021) الدليل الإلكتروني ومدى حجيته في الإثبات الجنائي، **المجلة الأردنية للعلوم التطبيقية** ، سلسلة العلوم الانسانية، الاردن ، مجلد 27، عدد 1
32. على محمود ابراهيم (2021) الأدلة الرقمية وحجيتها في إثبات الجرائم الإلكترونية ، **مجلة كلية الشريعة والقانون**، جامعة الأزهر ، أسيوط، عدد 32، جزء 4
33. أحمد جابر (2019) قيمة الدليل الإلكتروني في الإثبات الجنائي، **ماجستير غير منشورة** ، جامعة عمان الأهلية، الاردن
34. محمد محمود عمرى (2016) الإثبات الجزائي الإلكتروني في الجرائم المعلوماتية: دراسة مقارنة، **مجلة العلوم القانونية والسياسية** ، الجمعية العلمية للبحوث والدراسات الاستراتيجية مجلد6، عدد 2
35. محمد منصور النمر (2013) دور تقنية المعلومات فى مكافحة جرائم الابتزاز ، **ماجستير غير منشورة** ، جامعة نايف العربية للعلوم الامنية ، الرياض.
36. محمد عبد الله الحقبانى (2013) مهارات البحث والتحقيق فى الجرائم المعلوماتية، **دكتوراة غير منشورة** ، جامعة نايف العربية للعلوم الامنية ، الرياض.
37. ناصر البقمى (2012) أهمية الأدلة الرقمية فى الاثبات الجنائى ، مجلة الفكر الشرطى ، دبى ، الامارات.

38. سيدى محمد البشر (2010) دور الدليل الرقمى فى اثبات الجرائم المعلوماتية ، **ماجستير غير منشورة،** جامعة نايف العربية للعلوم الأمنية ، الرياض .
39. سلمان غازى العتيبى (2010) درجة توافر كفايات البحث عن الدليل الرقمى فى الجرائم المعلوماتية لدى ضباط شرطة العاصمة المقدسة ، **ماجستير غير منشورة** ، جامعة نايف العربية للعلوم الأمنية ، الرياض .
40. تركى بن عبد الله المويشير (2009) بناء نموذج امنى لمكافحة الجرائم المعلوماتية وقياس فعاليته، **دكتوراه غير منشورة** ، جامعة نايف للعلوم الأمنية ، الرياض .
41. أحمد بن حسن الشهرى (2005) قانون دولى موحد لمكافحة الجرائم الالكترونية، **مجلة العلوم الأمنية** ،العدد 53، جامعة نايف العربية للعلوم الأمنية ، الرياض .
42. محمد السرحانى (2004) مهارات التحقيق الجنائى الفنى فى جرائم الانترنت، **ماجستير غير منشورة،** جامعة نايف العربية للعلوم الأمنية ، الرياض
43. خالد عسكر العنزى (2003) الابتزاز انواعه واسبابه، المعهد العالى للامر بالمعروف والنهى عن المنكر، **ماجستير غير منشورة** ، جامعة أم القرى ، السعودية .
44. عبد الله محمد الشهرى (2002) المعوقات الادارية فى التعامل الأمنى مع جرائم الحاسب، **ماجستير غير منشورة ، كلية الآداب** ، جامعة الملك سعود ، الرياض .
45. محمد الامين البشرى (2001) التحقيق فى جرائم الحاسب والانترنت، **المجلة العربية للدراسات الأمنية،** العدد 30 ، جامعة نايف العربية للعلوم الأمنية ، الرياض.
46. **المحكمون من الأساتذة :** د. مصطفى الفقى ، د. على الدين هلال ، د.نيفين مسعد، د. شريف درويش اللبان ، د. على عجوة ، د. ضياء رشوان.
47. John Villasenor، "Artificial intelligence، geopolitics، and information integrity"، in: Fabio Rugge، ed.، The Global Race for Technological Superiority: Discover the Security Implications، (Milano: ISPI and Brookings، November 2019)، PP. 131-142
48. Tableau، Producer (2023). What is the history of artificial intelligence (AI)? Retrieved May 2023، from https://www.tableau.com/ : https://www.tableau.com/data-insights/ai/history#history
49. Akerkar R، Artificial Intelligence for Business Springer Briefs in Business. Springer، Cham.2019،p.11
50. Dorla jelonek Agata، et-al.، The Artificial Intelligence Application in the Managarment of Contemporary Organization; Theoretical Assumptions، Current practices and Review، Springer، cham، 2019،p. 24
51. Erkan Akar، (2015) The Impact of Social Influence on the Decision-Making Process of Sports Consumers on Facebook، Journal of Internet، Vol. 6، No. 2، P. 8.
52. https://www.alarabiya.net/ar/saudi-today/2018/11/24
53. Harry Surden، Artificial Intelligence and Law: An Overview، 35 Ga. St. U. L. Rev. (2019). Available at: https://readingroom.law.gsu.edu/gsulr/vol35/iss4/8
54. Cherry، M. A.، "Beyond Misclassification: The Digital Transformation of Work،" Comparative Labor Law Journal & Policy Journal، Vol. 37، 2015، p. 577.
55. Aristea Papadimitriou، The Future of Communication Artificial Intelligence and Social Networks، Media & Communication Studies ،Malmö University، Summer 2016.
56. شريف درويش اللبان،(2019) مداخل جديدة لتطوير صناعة المحتوى، القاهرة، **المركز العربي للبحوث** ، ص 34

57. Aristea Papadimitriou، (2016)The Future of Communication Artificial Intelligence and Social Networks، Media & Communication Studies ،Malmö University، Summer.p 34.
58. Deniz، Y. (2023، April 20). How Artificial Intelligence (AI) Is Used In Biometrics. (aratek، Producer) Retrieved June 2023،
59. Vasylchenko، O. (2022، April 24). AI Biometric Authentication for Enterprise Security. Retrieved June 2023، from mobidev.biz: https://mobidev.biz/blog/ai-biometrics-technology-authentication-verification-security
60. What is the history of artificial intelligence (AI)? (Tableau، Producer) Retrieved May 2023، from https://www.tableau.com/ : https://www.tableau.com/data-insights/ai/history#history
61. P. A. K. Nagnath B، Deep Chokshi، Criminal identification system using facial recognition، International Conference on Innovative Computing Communication (ICICC) 2021 (2021).
62. Manning، P. (2020). Artificial Intelligence Definitions. Stanford University.Müller، Vincent C.، "Ethics of Artificial Intelligence and Robotics"، The Stanford Encyclopedia of Philosophy (Summer 2021 Edition)،
63. استشراف مستقبل المعرفة (2020) **مؤسسة محمد بن راشد آل مكتوم للمعرفة** ، الغرير للطباعة ، دبي، ص 3
64. K. M. Manik Sharma، J Anuradha، G. S. C. Kashyap، Facial detection using deep learning، IOP Conference Series: Materials Science and Engineering (2017).
65. Gasteiger، "Chemistry in Times of Artificial Intelligence،" ChemPhysChem، vol. 21، no. 20، pp. 2233–2242، 2020، doi: 10.1002/cphc.202000518.
66. سعد خلفان الظاهرى (2020) الذكاء الاصطناعى والقوة التنافسية الجديدة ، **مركز استشراف المستقبل** ، دبى ، الامارات العربية ، عدد 299
67. عدى عيد الاسدى (2020) الذكاء الاصطناعى والنظم الخبيرة ، **ماجستير غير منشورة** ، جامعة الملك سعود ، الرياض
68. https://www.albayan.ae/across-the-uae/news-and-reports/2019-03-19-1. 2020/1/13- 351542
69. http://www.Businessinsider.com/Stephen-hawking-elon-musk-backed-asimolar- ai-principles-for-artificial-intelligence25/12/2019
70. عبد الناصر فرغلى (2022) **الاثبات الجنائى بالأدلة الرقمية**، جامعة نايف للعلوم الأمنية، الرياض ، ص 5
71. بشير عرنوس (2020) **الذكاء الاصطناعى** ، القاهرة ، دار السحاب ، ص 9
72. على الشريف (2022) **تطبيقات الذكاء الاصطناعى**، مطبوعات جامعة تشرين، دمشق، ص 34
73. محمد سعد الدين (2017) المستحدثات الشرطية ، **تقرير استشراف المستقبل**، دبى، العدد 5 ، مارس 2017م
74. سعد رزق على (2023) استخدام الذكاء الاصطناعى فى الكشف عن الجرائم ،**مجلة الدراسات القانونية** ، ص 22
75. Kristijian، how will Technology Impact the Future of Private Number Plates? the Future of Things، 2019
76. https://www.albayan.ae/across-the-uae-and-reports/2019/3/19-1.3515428.
77. محمد سعد الدين (2017) المستحدثات الشرطية ، **تقرير استشراف المستقبل**، مرجع سابق ، ص 11

78. فايق عوضين (2017) الوسائل الحديثة فى مكافحة الجريمة، **أكاديمية العلوم الشرطية** ، جامعة الشارقة ، ص 4
79. يحيى الدهشان (2020) **المسؤولية الجنائية فى جرائم الذكاء الاصطناعى**، مرجع سابق ، ص 45
80. Vasylchenko، O. (2022). AI Biometric Authentication for Enterprise Security. Retrieved June 2023، from mobidev.biz: https://mobidev.biz/blog/ai-biometrics-technology-authentication-verification-security
81. Chen، L.، Zaharia، M. and Zou، J. (2023) How is CHATGPT's behavior changing over time?، arXiv.org. Available at: https://arxiv.org/abs/2307.09009
82. Alkhunaizi، S. (2023). Saudi Arabia should look into investing in AI to control English narrative: Saudi Media Forum panelists، https://www.newscientist.com/article/2383218
83. https://sdaia.gov.sa/ar/MediaCenter/KnowledgeCenter/Pages/SDAIAPublications.aspx
84. Global Digital Report (2018) ،http://digitalreport.wearesocial.com.
85. L. Wang، M. A knowledge-based reasoning model for crime reconstruction and investigation،" Expert Syst. Appl.، vol. 159، p. 113611، 2020، doi: 10.1016/j.eswa.2020.113611
86. Kabir، S. et al. (2023) Who answers it better? an in-depth analysis of chat gpt and stack overflow answers to software engineering questions، arXiv.org. Available at: https://doi.org/10.48550/arXiv.2308.02312 (Accessed: 22 August 2023
87. Artificial Intelligence and National Security، Congressional Research Service (CRS)، 2020، available on https://crsreports.congress.gov/product/pdf/R/R45178/10
88. Global Digital Report (2018) ،http://digitalreport.wearesocial.com.
89. بهاء المرى (2022) **جرائم السوشيال ميديا** ، مؤسسة الأهرام للنشر، القاهرة ، ص 5
90. Lehto Martti ، Neittaanmäk Pekka .Cyber Security: Analytics، Technology and Automation. Switzerland: Springer International Publishing، 2015
91. Intelligence and National Security Congressional Research Service. Congressional Research Service، November، 2020. Available at: https://fas.org/sgp/crs/natsec/R45178.pdf
92. Lewis، J. A، Cybersecurity and Critical Infrastructure Protection، Center for Strategic and International Studies، . Washington، DC، 2006
93. خالد ابراهيم (2020) **الاثبات الالكترونى** ، دار الفكر الجامعى ، الاسكندرية ، ص 23
94. S. K. Chinnikatti، "Artificial Intelligence in Forensic Science،" Forensic Sci. Addict. Res.، vol. 2، no. 5، pp. 182–183، 2018.
95. M. A. Marciano and J. D. Adelman، "PACE: Probabilistic Assessment for Contributor Estimation—A machine learning-based assessment of the number of contributors in DNA mixtures،" Forensic Sci. Int. Genet.، vol. 27، pp. 82–91، 2017.
96. Haenlein، Siri، (2022) in my Hand، who's the Fairest in the Land? On the Interpretations، Illustrations and Implications of Artificial Intelligence، Business Horizons، 62(1)، p.15

97. Peter stone ،Rodney Brooks ،Erik Brynjolfsson et al، Artificial I intelligence and Life in 2030 "One Hundred Year Study on Artificial Intelligence :Report of the 2015-3016 Study Panel .Stanford .University Stanford.CA.، September
98. Zhang, Z., Hamadi, H. A., Damiani, E., (2022). Explainable artificial intelligence applications in cyber security: State- of-the-art research. Ithaca: Cornell University Library, arxiv.org
99. Walker,Munro, B.,)2022(. The guilty silicon (mind: Blameworthiness and liability in human, machine teaming. Ithaca: Cornell University Library, arXiv.org
100. Al-Marghilani, A. (2022). Target detection algorithm in crime recognition using artificial intelligence. Computers, Materials, & Continua, 71(1), 809
101. Powelson, K. (2022). The impact of artificial intelligence on anti-money laundering programs to detect and prevent financial crime (Order No. 30241947). Avail- able from ProQuest Dissertations &Theses Global
102. Umair, M. B., Contributed equally to this work with: Umair,Muneer Butt, Letchmunan, S., Sukumar Letchmunan Fadratul, H. H., & Tieng, W. K. (2022). Hybrid of deep learning and exponential smooth- ing for enhancing crime forecasting accuracy. PLOS One, 17(9
103. أنس عدنان ،(2023) تطبيقات الذكاء الاصطناعي في رصد الجرائم، **أكاديمية الشرطة الملكية**، الأردن، ص4.
104. Peter Sommer, Digital Evidence, Digital Investigation and E-Disclosure (A Guide to Forensic Readiness for Organizations, Security Advisers and Lawyers), Third Edition, Information Assurance Advisory Council (L,A,A,C), United Kingdom, 2011, p..30