المجلة العلمية لجامعة الملك فيصل
The Scientific Journal of King Faisal University
العلوم الإنسانية والإدارية
Humanities and Management Sciences

تأثير الذكاء الاصطناعي على الجريمة الإلكترونية

The Effect of Artificial Intelligence on Electronic Crime

رانا مصباح عبد المحسن عبد الرازق
قسم العلوم الإدارية والإنسانية، عمادة خدمة المجتمع والتعليم المستمر، جامعة الأميرة نورة بنت عبد الرحمن، الرياض، المملكة العربية السعودية

Rana Mosbah Abdel Mohsen Abdel Razek
Administrative and Human Sciences, Deanship of Community Service and Continuing Education, Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia

الكلمات المفتاحية: الذكاء الاصطناعي، الجريمة الإلكترونية، أمن المعلومات، مكافحة جرائم الحاسوب، تقنية المعلومات
KEYWORDS: Artificial intelligence, Cybercrime, Information Security, Combating computer crime

الاستقبال RECEIVED	القبول ACCEPTED	النشر PUBLISHED
15/08/2020	16/08/2020	01/03/2021

https://doi.org/10.37575/h/mng/2417

الملخص

تهدف الدراسة إلى التعرف على تأثير استخدام الذكاء الاصطناعي على ارتكاب الجرائم المعلوماتية، وذلك نظرًا لاستحداث عدد من الجرائم الفنية المستمدة من التقنية المعلوماتية. فبعض المجرمين اتجهوا لاستخدام الوسائل التقنية المستحدثة لتنفيذ جرائمهم، فكانت محل اهتمام رجال القانون والمختصين من أجل إيجاد الحلول المناسبة لقمعها ومكافحتها. لذلك سارعت الكثير من الدول المتقدمة والدول العربية، للتَّصدي لتلك الظاهرة، وذلك بتشريع وسن القوانين التي تمنع من ارتكاب مثل تلك الجرائم. واعتمدت الدراسة على المنهج الوصفي التحليلي بالإضافة إلى الاستعانة بالمنهج المقارن، واشتملت الدراسة على ثلاثة مباحث وبيَّنت ماهية الذكاء الاصطناعي والجريمة الإلكترونية، وطبيعتها القانونية، وخصائصها، والتعرف على صور الجرائم المعلوماتية وعلاقتها بمجال الذكاء الاصطناعي، والتعرف على موقف التشريع السعودي والمصري بشأن مكافحة جرائم تقنية المعلومات. ومن أبرز النتائج أن الذكاء الاصطناعي يلعب دورًا مهما في زيادة الجرائم الإلكترونية وانتشارها وهو ما يثبت صحة فرضية الدراسة.

ABSTRACT

This study aimed to identify the impact of artificial intelligence on rates of cybercrime. This is due to the development of a number of technical crimes derived from information technology. Some criminals have tended to use modern technical means to commit their crimes, which has attracted the attention of lawyers, professionals, and specialists, who are working to find appropriate solutions to prevent and suppress such crimes. Therefore, many developed and Arab countries have rushed to thwart this phenomenon by legislating and enacting laws that prevent such crimes from being committed. The study relied on a descriptive analytical approach, in addition to a comparative approach. The study included three investigations, and focused on artificial intelligence, cybercrime, its legal nature, and its characteristics. The aims of the study were to identify the different types of computer crime and their relationship to the field of artificial intelligence, and to identify the position of Saudi and Egyptian legislation regarding combating IT crimes. The most prominent result was that artificial intelligence plays an important role in increasing cybercrime, which proves the validity of the study hypothesis.

1. المقدمة

يُعّد الذكاء الاصطناعي من الميادين المهمة التي تستقطب اهتمام الباحثين، ومع التقدم السريع لتكنولوجيا الحاسبات في الوقت الراهن، وبفضل كون الحواسب مصممة خصيصًا لتحصيل المعلومات وتخزينها واستخدامها، فمن ثمة وجود علاقة ارتباط قوية بين استخدامات الحاسب الآلي وارتكاب بعض الجرائم المستحدثة، أي استخدام الحاسب الآلي كأداة لارتكاب الأفعال غير المشروعة. وسواء أكانت الحاسبات الآلية محلًا للجريمة المعلوماتية أو وسيلة لها، فإن الجوهري في الأمر أن انتشار الوسائل المعلوماتية نتيجة لثورة المعلومات، والتي تنتشر بسرعة هائلة وتغزو مختلف مجالات الحياة أصبح يزيد من فرص انتشار هذا النوع من الجرائم المستحدثة. فعندما يتم الاعتداء على خصوصية الأفراد، والمؤسسات، والدول، بتدمير مواقعهم الإلكترونية أو اختراقها، أو قرصنة المعلومات الخاصة بالمواقع الحكومية، فإن هذا الاعتداء يؤدي إلى نشوء مشاكل قانونية جديدة تعتمد بطبيعة الحال على الآليات الجديدة. وبمعنى آخر، فنحن أمام مجموعة من الجرائم المستحدثة ذو تكنيك متميز نظرًا لوجود الحاسب الآلي.

2. موضوع الدراسة

لقد شهد القرن الحادي والعشرون تطورًا هائلًا في مجال الاتصالات، وبالأخص الشبكة العنكبوتية، مما أدى إلى ظهور طائفة جديدة من الجرائم مختلفة عن باقي الجرائم التقليدية، وقد سميت بالجرائم المعلوماتية، أو الإلكترونية أو جرائم الإنترنت. وقد أدى تسارع إيقاع التقدم التكنولوجي والتقني الهائل، ووسائل الاتصالات الحديثة كالفاكس والإنترنت، وسائر صور الاتصال الإلكتروني عبر الأقمار الاصطناعية، إلى استغلاله من قبل مرتكبي الجرائم الإلكترونية في تنفيذ جرائمهم؛ إذ لم تعد تقتصر على إقليم واحد أو دولة واحدة، بل تجاوزت حدود الدول، وهي جرائم مبتكرة ومستحدثة تمثل ضربًا من ضروب الذكاء الإجرامي، وقد استعصى إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية.

3. مشكلة الدراسة

تكمن مشكلة الدراسة في مدى الخطورة التي تفرز عن إساءة استخدام الذكاء الاصطناعي، واستغلال الأنظمة المعلوماتية على نحو غير شرعي قصد الإضرار بمصالح الأفراد والمؤسسات والدول، فساهم التطور التقني في ظهور أنماط وصور مستحدثة من الجرائم سميت بالجرائم المعلوماتية. ونظرًا لحداثة الجرائم المعلوماتية واتصالها بالذكاء الاصطناعي، كانت محل اهتمام رجال القانون والمختصين من أجل إيجاد الحلول المناسبة لقمعها ومكافحتها.

وبناءً على ذلك تتمثل مشكلة الدراسة بصفة أساسية في التساؤل الرئيس الآتي: ما مدي تأثير استخدام الذكاء الاصطناعي على الجريمة الإلكترونية؟ وينبثق من هذا السؤال الرئيس الأسئلة الفرعية الآتية:

- ما المقصود بمفهوم الذكاء الاصطناعي؟
- ما المقصود بمفهوم الجريمة الإلكترونية، وطبيعتها القانونية، وخصائصها؟
- ما صور الجرائم الإلكترونية وعلاقتها بالذكاء الاصطناعي؟
- ما موقف التشريع السعودي من الجرائم الإلكترونية؟
- ما موقف التشريع المصري المقارن من الجرائم الإلكترونية؟

4. أهداف الدراسة

بناء على مشكلة الدراسة وتساؤلاتها تهدف الدراسة إلى الآتي:

- التعرف على مفهوم الذكاء الاصطناعي.
- التعرف على ماهية الجريمة الإلكترونية.
- التعرف على صور الجرائم الإلكترونية وعلاقتها بالذكاء الاصطناعي.
- التعرف على موقف التشريع السعودي من الجريمة الإلكترونية.
- التعرف على موقف التشريع المصري من الجريمة الإلكترونية.

5. أهمية موضوع الدراسة

تكمن أهمية دراسة هذا الموضوع من منطلق تأثير الذكاء الاصطناعي على ارتكاب الجرائم المعلوماتية، وهو نوع مستحدث من الإجرام، بسبب

المؤلف المراسل: رانا مصباح عبد المحسن عبد الرازق rmabdelmohsen@pnu.edu.sa, 00966509039953 Corresponding Author: Rana Mosbah Abdel Mohsen Abdel Razek

الطبيعة الخاصة للإجرام الإلكتروني، ولذلك تعمل الدول على ملاءمة قوانينها بما يتناسب مع هذا النوع من الإجرام، وسدًا للقصور الذي كان يعانيه القضاء في مكافحة الجريمة الإلكترونية بالنصوص القانونية التقليدية والذي كان يخالف مبدأ الشرعية، باعتباره مبدأ يحقق الحماية لحقوق المتهم من تجريمه على أفعال وعقابه بعقوبات لم ينص عليها القانون، كما يطرح جدوى هذا الموضوع في الاقتداء بتطور القوانين لدى التشريعات المقارنة في ملاحقتها للأنماط المستحدثة من الجريمة الإلكترونية والذي قد تأخر المنظم السعودي والمشرع الجنائي المصري في مواكبتها.

6. فرضية الدراسة

تتمثل فرضية الدراسة في الفرضية التالية: "من الممكن أن يساهم الذكاء الاصطناعي في زيادة وانتشار الجريمة الإلكترونية؛ خاصة بسبب وجود علاقة ارتباط قوية بين استخدامات الحاسب الآلي وارتكاب الجرائم الإلكترونية، أي استخدام الحاسب الآلي كأداة لارتكاب الأفعال غير المشروعة".

7. منهج الدراسة

اعتمدت الدراسة على المنهج الوصفي التحليلي الذي يقوم على أساس تحديد ماهية الجريمة الإلكترونية، وطبيعتها، وخصائصها، وصور الجرائم المعلوماتية وعلاقتها بالذكاء الاصطناعي، وشرح نصوص القانون الجزائي السعودي، بالإضافة إلى الاستعانة بالمنهج المقارن الذي يقوم على شرح نصوص القانون الجنائي المصري.

8. خطة الدراسة

سيتم تقسيم خطة الدراسة إلى ثلاثة مباحث يسبقها مقدمة وتنتهي بخاتمة، على النحو التالي:

8.1. مفهوم الذكاء الاصطناعي وماهية الجريمة الإلكترونية:

إن الجريمة المعلوماتية هي ثمرة من ثمار التقدم السريع في شتى المجالات العلمية الذي يتميز به عصرنا الحاضر؛ فهناك علاقة ارتباط قوية بين الذكاء الاصطناعي وارتكاب بعض الجرائم المستحدثة، أي استخدام الحاسب الآلي كأداة لارتكاب الأفعال غير المشروعة. وسواء أكان الحاسب الآلي محلًا للجريمة المعلوماتية أو وسيلة لها، لذلك سنتناول في المطلب الأول مفهوم الذكاء الاصطناعي، وماهية الجريمة الإلكترونية في المطلب الثاني.

1.1.8. مفهوم الذكاء الاصطناعي

يمثل الذكاء الاصطناعي أهم مخرجات الثورة الصناعية الرابعة لتعدد استخداماته في المجالات العسكرية والصناعية والاقتصادية والتقنية والتطبيقات الطبية والتعليمية والخدمية...إلخ، ويتوقع له أن يفتح الباب لابتكارات لا حدود لها وأن يؤدي إلى مزيد من الثورات الصناعية بما يحدث تغييرًا جذريًا في حياة الإنسان، وسيكون محرك للتقدم والازدهار في السنوات القادمة. فكانت بداية الثورة الصناعية الرابعة في مطلع القرن الحادي والعشرين معتمدة على الثورة الرقمية والإنترنت المتحرك، وتطور أجهزة الاستشعار عن بعد، والذكاء الاصطناعي والتكنولوجيا الحيوية، والروبوتات الذكية، والتحول الآلي، والتقنيات الرقمية والأنظمة الذكية.

وقد ظهر مصطلح الذكاء الاصطناعي لأول مرة من خلال مؤتمر للكمبيوتر عُقد في الولايات المتحدة عام 1946، فتنوعت مجالات الذكاء الاصطناعي في العديد من الفروع المختلفة مثل التعلم الآلي والأنظمة الخبيرة وصناعة الروبوت...إلخ، وفي هذه الدراسة نركز الحديث على علاقة الذكاء الاصطناعي بالجريمة المعلوماتية.

ويتعين لمعرفة مفهوم الذكاء الاصطناعي تحديد أولًا المقصود بالذكاء الإنساني، فهو الذي يرتبط بالقدرات العقلية مثل القدرة على التكيف مع ظروف الحياة، والاستفادة من التجارب، والخبرات السابقة، والتفكير، والتخطيط. ويعرف الذكاء الاصطناعي بأنه: هو فرع من فروع الحاسوب يهتم بدراسة أنظمة حاسوبية وصناعتها يمكنها إنجاز أعمال تتطلب ذكاءً بشريًا، حيث تمتاز هذه الأنظمة بأنها تتعلم مفاهيم ومهام جديدة ويمكنها أن تفكر وتستنتج استنتاجات مفيدة حول العالم الذي نعيش فيه (السلمي، 2017).

2.1.8. ماهية الجريمة الالكترونية

1.2.1.8. مفهوم الجريمة الإلكترونية

تعددت تعريفات الجريمة الإلكترونية، فقد عرفها البعض بأنها "الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي"(الشوابكة، 2004؛ بيومي، 2007)، بالنظر إلى وسيلة ارتكابها وهو الحاسب الآلي. لذلك نجد أن مكتب تقييم التقنية في الولايات المتحدة الأمريكية عرفها من خلال تعريف الحاسب الآلي بأنها "الجرائم التي تقوم فيها بيانات الحاسب الآلي والبرامج المعلوماتية بدور رئيس"(الملا، 2018)، وترى منظمة التعاون الاقتصادي والتنمية (OCDE) "أنَّ الجريمة المعلوماتية هي كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجًا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية "(مراد، 2005؛ الملط،2006)، وعرفها البعض أيضًا بأنها "نشاط جنائي يمثل اعتداءً على برامج وبيانات الحاسب الإلكتروني"(يوسف، 2009)، وعرفها البعض الأخر بأنها "هي كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي والتي تحول طريقه"(عفيفي، 2003؛ سامي، 2016)، ويندرج هذا النوع تحت جرائم المعالجة الآلية للبيانات، بالنظر إلى موضوع الجريمة ونمطها، فهي لا تقع على ماديات، وإنما على برامج الكمبيوتر وما يحتويه من معلومات.

وتبنى مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين تعريفًا جامعًا لجرائم الحاسب الآلي وشبكاته حيث عرف الجريمة المعلوماتية بأنها: "أي جريمة يمكن ارتكابها بواسطة نظام أو شبكة حاسوبية أو داخل نظام حاسوب"(الشوابكة، 2004؛ سامي، 2016)، ويعد هذا التعريف من أفضل التعريفات التي تناولت ظاهرة الإجرام المعلوماتي. ومن جانبنا نرى أنه يمكن تعريف الجريمة المعلوماتية أو الإلكترونية بأنها:" كل اعتداء يقع على نظم الحاسب الآلي وشبكاته أو بواسطتها".

2.2.1.8. الطبيعة القانونية للجريمة الإلكترونية

تدخل الجرائم الإلكترونية في نطاق دراسة القسم الخاص بقانون العقوبات، وهو الفرع المختص بدراسة كل جريمة على حدة متناولًا عناصرها الأساسية والعقوبة المقررة لها، إلا أن الجرائم المعلوماتية تمثل ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي. فالطبيعة القانونية الخاصة لهذه الجرائم من خلال المجال الذي يمكن أن ترتكب فيه، أو الذي يقع عليه الاعتداء، فطبيعة التطور السريع في مجال المعلوماتية يتحتم ضمه إلى نطاق القانون الجنائي الخاص، بسبب عجز النصوص الجنائية عن مواكب التطور المعلوماتي أو لما يحتويه من فراغ تشريعي في هذا المجال؛ لذا كان من الضروري تحديث قوانين الجنائية للجريمة المعلوماتية (المقصودي،2017).

3.2.1.8. خصائص الجريمة الإلكترونية

تتميز الجريمة الإلكترونية بعدة خصائص لعل من أبرزها ما يلي (العريان، 2004؛ المقصودي، 2017؛ الملط، 2006):

- تعد الجرائم الإلكترونية أقل عنفًا من الجرائم التقليدية أي أنها لا تحتاج إلى أدنى مجهود عضلي؛ بل تعتمد على القدرة الذهنية والتفكير العلمي المدروس المستند إلى معرفة بتقنيات الحاسب الآلي.
- يختلف الباعث على ارتكاب الجرائم الإلكترونية عنه بالنسبة إلى الجرائم التقليدية، ففي الجرائم الأخيرة يتمثل الباعث بالرغبة في مخالفة النظام العام والخروج عن القوانين أكثر من استهداف الحصول على الربح، في حين نجد أن الباعث لدى مرتكبي الجرائم الإلكترونية هو الحصول على النفع المادي السريع، فإن المبالغ التي يمكن تحقيقها من وراء ذلك تكون طائلة.
- يرتكب الكثير من الجرائم الإلكترونية، ولكن نادرًا ما تقع جريمة معلوماتية ويقوم المجني عليه بالإبلاغ عنها؛ وذلك بسبب عدم اكتشافه للجريمة، أو لأنه اكتشفها ولكنه يخاف من الإساءة لسمعته وفقدان الثقة في التعامل معه؛ لذلك لا يتم في الغالب الإبلاغ عن جرائم الإنترنت إما لعدم اكتشاف الضحية لها وإما خشيته من التشهير. لذا نجد أن معظم الجرائم تم

اكتشافها بالمصادفة، بل وبعد وقت طويل من ارتكابها.

- يصعب في كثير من الأحيان العثور على أثر مادي للجريمة الإلكترونية، والسبب في ذلك يعود إلى استخدام الجاني وسائل فنية وتقنية معقدة في كثير من الأحيان، كما يتمثل السلوك المكوّن للركن المادي فيها بعمل سريع قد لا يستغرق أكثر من بضع ثوانٍ، فمن السهل إخفاء معالم الجريمة وصعوبة تتبع مرتكبيها، وسهولة محو الدليل والتلاعب به في الوقت الذي تفتقر فيه هذه الجرائم إلى الدليل المادي التقليدي؛ لذا فهذه الجرائم لا تترك أثرًا لها بعد ارتكابها.
- تعتمد الجرائم الإلكترونية على قمة الذكاء في ارتكابها؛ ويصعب على المحقق التقليدي التعامل مع هذه الجرائم، إذ يصعب عليه متابعة جرائم الإنترنت والكشف عنها وإقامة الدليل عليها، فهي جرائم تتسم بالغموض؛ وإثباتها والتحقيق فيها يختلف عن التحقيق في الجرائم التقليدية، والوصول للحقيقة بشأنها يستوجب الاستعانة بخبرة فنية عالية المستوى.
- يؤدي عولمة الجرائم الإلكترونية إلى تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم، فتعتبر هذه الجرائم هي صورة صادقة من صور العولمة؛ فمن حيث المكان يمكن ارتكاب هذه الجرائم عن بعد، وقد يتعدد هذا المكان بين أكثر من دولة.

4.2.1.8. صفات الجناة في الجريمة المعلوماتية

يتسم المجرم في الجريمة المعلوماتية بسمات خاصة، ومهارات تقنية في نظام الحاسبات الآلية، وجمعت عدة صفات شخصية بين من يرتكبون الجرائم المعلوماتية، فمنها: أنهم يتمتعون بقدر عالٍ من الذكاء، كما أنهم يعلمون جيدًا بالتقنية العالية، ومكتسبوا معارف علمية وعملية، وهذه الصفات تتشابه مع أصحاب الجرائم الذين يُرتكبون جرائم غير عنيفة، وترتكب من ذوي الطبقات الاجتماعية العليا، وهم من يسمون بمجرمي ذوي الياقات البيضاء، لأنهم ينتمون إلى طبقة اجتماعية تتصف بالثقافة والتعليم. فيعد الإجرام المعلوماتي إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف. وقد صنف المجرمون المعلوماتيون: إلى المهووسين أو المخترقين أو الهاكرز المتطفلين الذين يتحدّون إجراءات أمن النظم والشبكات، لكن لا تتوافر لديهم في الغالب دوافع حاقدة أو تخريبية، وإنما ينطلقون من دوافع التحدي وإثبات المقدرة، فهؤلاء الذين يرتكبون جرائم معلوماتية تبين أنهم في غياب تام عن الشعور بعدم مشروعية الطبيعة الإجرامية، كما أنهم يبررون أفعالهم الإجرامية، ولا يعتقدون بعدم مشروعيتها؛ ولذلك يدَّعون أنهم لا يستحقون عقابًا على أفعالهم. والمتطرفون: وهم كل طائفة لها أفكار سياسية أو دينية، ولكن هذه الأفكار لا تتسم بالاعتدال، بل إنها تكون بعيدة عن التوسط، فهؤلاء يستخدمون الشبكات المعلوماتية لسهولة التواصل بها مع الآخرين حتى ينشروا أفكارهم (العريان،2004؛ الملط، 2006؛ الملا، 2018).

5.2.1.8. دوافع ارتكاب الجرائم المعلوماتية

- **السعي وراء الكسب المادي(الربح):** نجد أن الكسب المادي الناتج عن الجرائم المعلوماتية قد يفوق لما ينتج عن الجرائم التقليدية، فذلك أول وأهم الدوافع لارتكاب تلك الجرائم.
- **الأخذ بالثأر من رب العمل:** يرتكب بعض عاملين في مؤسسات أو شركات، بسبب ضغط العمل وضغط نفسي عليهم، ينشأ بداخلهم الانتقام من رب العمل، ثم ينتج عن ذلك ارتكاب الجريمة.
- **التحدي الذهني:** تتسم الأجهزة التابعة للنظام المعلوماتي وكذلك الأنظمة الأمنية بالتعقيد وصعوبة اختراقها، وتحاط بهالة من القدرات التي تبين صعوبة أو استحالة التجسس عليها، وهذه الأمور تكون بمثابة استفزاز لمهارات وإمكانيات بعض الأشخاص المصابين بخلل في التفكير، وتثير فيهم رغبة التحدي، حينئذ بفهم خاطئ منه يسلك طريق الإجرام فيرتكب الجريمة (قارة، 2002؛ المقصودي، 2017).

6.2.1.8. الفرق بين الجريمة المعلوماتية، والجريمة التقليدية

تتفق الجرائم المعلوماتية كغيرها من الجرائم التقليدية في الأركان العامة للجريمة، إلا أن الجرائم المعلوماتية تختلف في طبيعتها عن الجرائم التقليدية فيما يلي (عفيفي، 2003؛ الملا، 2018):

- تقع الجريمة المعلوماتية في بيئة المعالجة الآلية للمعلومات والبيانات؛ حيث إنه يلزم لوقوعها أن يكون التعامل مع بيانات تم تجميعها وتجهيزها بغرض الدخول إلى نظام معلوماتي لمعالجتها إلكترونيًا.
- إثبات وقوع الجرائم التقليدية أسهل من إثبات وقوع الجرائم المعلوماتية؛ وذلك لأن الجرائم التقليدية تترك أثرًا خارجيًا؛ أما الجرائم المعلوماتية لا تترك وراءها أثرًا، وقد تقع دون اكتشافها، وإذا اكتُشفت قد يكون ذلك مصادفة.
- تكون الأدلة للجريمة المعلوماتية غير كافية، بسبب عدم وجود دليل مكتوب، كما أن المجرم يتمكن من إزالة دليل إدانته في وقت يسير قد يستغرق ثانية.
- الجرائم التقليدية لابد لمرتكبها أن يوجد في مكان الجريمة، أو يكون قريباً منها بمسافة تمكنه من ارتكاب الجريمة، أما الجرائم المعلوماتية فتختلف عن ذلك؛ فمثلًا قد يستطيع المجرم وهو في بلدته وفي منزله أن يخترق نظامًا معلوماتيًا في دولة أخرى، ويحول مبلغًا من المال لشخص ما في أي دولة، إذن فهذه الجرائم لا تعرف حدودًا بين الدول أو القارات.

7.2.1.8. تأثير دور الذكاء الاصطناعي على موضوع الجريمة المعلوماتية

أن محل الجريمة المعلوماتية هو الحاسب الآلي؛ فيقع الاعتداء على أجزائه ومكوناته المادية، وإما أن يتم الاعتداء على ما يحتويه من معلومات مثبتة ومخزنة في ذاكرة الحاسب، مثل: أن يقوم شخص بالاعتداء على الحاسب فيسرق ما به من معلومات، أو برامج مستخدمة فيه، أو يفشي ما به من معلومات وبيانات، أو يعطل عمله، أو يتلف طريقة استخدامه، أو يعبث بما مسجل عليه من معلومات فيزورها أو ينسخها، وإما أن تقع الجريمة باستخدام الحاسب، فيكون هو الأداة المستخدمة في ارتكاب الجريمة، فقد يستخدم الحاسب في جرائم اعتداء على الأموال؛ كالتزوير وخيانة الأمانة والنصب والسرقة، وانتهاك حرمة الحياة الخاصة، وأشد خطورة من ذلك أن يستخدم في جرائم القتل؛ كبرمجة جهاز يتم التحكم فيه آليًا عن بعد لتفجير أماكن بما فيها من أشخاص، فكل هذه الجرائم وأمثالها تستخدم بواسطة الحاسب، فهو حينئذ أداة لارتكاب الجريمة، ومحل الجريمة يختلف حسب ما يقع عليه فعل المجرم، والذي يعد محل الحق أو المصلحة المحمية (الملط،2006؛ الملا، 2018).

8.2. صور الجريمة المعلوماتية وعلاقتها بالذكاء الاصطناعي:

تنوعت جرائم الحاسوب إلى جرائم ترتكب على نظم الحاسوب، وأخرى ترتكب بواسطته، فهي جرائم تنصَّب على معطيات الحاسوب (بيانات ومعلومات وبرامج) وتطال الحق في المعلومات، ويستخدم لاقترانها وسائل تقنية تقتضي باستخدام الحاسوب. وأن الجرائم التي تنصَّب على الكيانات المادية تدخل في نطاق الجرائم التقليدية ولا يندرج ضمن الظاهرة المستجدة لجرائم الحاسوب، لذلك سنقوم بسرد أفعال الاعتداء في مجال الأنظمة المعلوماتية في خلال المطالب الآتية، بدءًا من محاولة الاعتداء على المعدات المادية لأنظمة المعلوماتية، ومرورًا بالاعتداء على المعلومات المختزنة آليًا، ثم الاعتداء على برامج الحاسب الآلي، وجرائم اعتداء على أشخاص وهناك جرائم تقع على المال، وأخيرًا ضد الحكومة والجرائم الإلكترونية الأخرى.

1.2.8. الجرائم الماسة بالاعتداء على سلامة البيانات والمعلومات

تم تصنيف الجريمة الإلكترونية إلى جرائم تستهدف نظام المعلومات كالاستيلاء على المعلومة لتعديلها أو إتلافها، أو محوها، أو تخريب الأنظمة المعلوماتية المادية. ويمكن ارتكاب بعض الجرائم المعلوماتية في هذه المرحلة لا سيما بالنسبة للمعلومات المختزنة داخل الحاسب الآلي، وتتمثل هذه الجرائم في الاطلاع غير المصرح به للمعلومات المختزنة آليًا، والتدخل المعلوماتي غير المشروع، وذلك على النحو التالي:

1.1.2.8. التلاعب في المعلومات

يكون التلاعب بالنظام المعلوماتي له صورتان، تلاعب مباشر، وغير مباشر، وذلك كالآتي: التلاعب المباشر: يكون من خلال إدخال معلومات لا تطابق الحقيقة المطابقة للواقع، مثال ذلك: تدوين أسماء عاملين لا وجود لهم في شركة، ويكون لكل عامل ملف، ويتقاضى كل واحد منهم مبلغًا شهريًا، ثم يقوم الجاني بتحويل الأموال لحسابه، أو الإبقاء على أسماء عاملين تركوا العمل، فيقوم المسؤول عن الإدارة المالية المعلوماتية بالإبقاء على هذه الملفات، وكأنهم ما زالوا يعملون، فيتحصل على مرتبات شهرية لهؤلاء العاملين، مع أنهم تركوا أعمالهم. وهذه الجرائم يصعب وقوعها إلا بواسطة الحاسب الآلي (الشوا،1994؛ العريان،2004؛ سامي، 2016).

التلاعب غير المباشر: لا يتم بتدخل مباشر في المعلومات المسجلة بالنظام المعلوماتي، وإنما يتم عن بعد؛ وذلك بأن يعرف المعتدي مثلًا الشفرات الخاصة بالحسابات، أو استخدام إحدى وسائط التخزين، أو التلاعب في الشرائط الممغنطة، أن تقوم شركة بإرسال شرائط ممغنطة لجهات أخرى،

وتحتوي هذه الشرائط على تعاملات مالية كأذون الدفع مثلًا، فيقوم المعتدي بعملية احتيال بطريق غير مباشر بالتلاعب فيها، أو التلاعب في البيانات عن بعد؛ فالجاني يمكنه أن يتسلل إلى أي نظام معلوماتي، ويصل إلى المعلومات المخزنة بذاكرة الحاسب فيجري عليها تعديلات، وذلك كله يحدث إذا كان المعتدي على علم بكلمة السر(الشوا،1994؛ العريان،2004؛ سامي، 2016).

2.1.2.8. إتلاف المعلومات

يحاول الجاني أن يصل إلى المعلومات المخزنة بالنظام المعلوماتي؛ لأنها هدفه الأساسي، وهذه المعلومات قد تتلف نتيجة ارتكاب الجريمة، ويكون إتلاف المعلومات له صورتان، استبدال المعلومات، محو المعلومات، وذلك على النحو التالي:

- **استبدال المعلومات:** يتم أسلوب تزوير المعلومات عن طريق استبدالها حيث ترتكب الجريمة بمجرد الاستبدال، مثال على ذلك: أن يقوم الجاني باستبدال المعلومات فيتقاضى أضعاف مرتبه، ولا يكون ذلك مرة واحدة، بل قد تستمر آثار ارتكاب الجريمة لعدة سنوات حتى يكتشف هذا التزوير، ولم يتم اكتشاف الجريمة إلا مصادفة.
- **محو المعلومات:** يكون بالدخول إلى النظام المعلوماتي، وحذف المعلومات جزئيًا أو كليًا، وهذا النوع من الجريمة أسهل من النوع السابق؛ حيث إنه لا تحتاج إلى دراية كبيرة بالحاسب وتقنياته؛ فأي مستخدم عادي يستطيع ارتكابها بسهولة، وكذلك إزالة آثار الجريمة (الشوا، 1994؛ سامي، 2016؛ الملا، 2018).

2.2.8. الجرائم الواقعة على البرامج:

تكون جريمة الاعتداء على المكونات المادية للنظام المعلوماتي، محل الجريمة هو الاعتداء على البرامج؛ حيث إن هذه البرامج تحتوي على معلومات وبيانات، ولا يستطيع ارتكاب تلك الجريمة إلا من كانت له معرفة فائقة في مجال البرمجة.

1.2.2.8. جريمة الاعتداء على البرامج التطبيقية

يقوم الجاني بالاعتداء على البرامج من خلال تعديلها، والهدف الرئيس من هذا التعديل هو الاختلاس، وأكثر هذه الجرائم تقع في مجال الحسابات، مثال على ذلك: أن يقوم مبرمج بأحد البنوك بزرع برنامج فرعي بإدارة الحسابات، فنتج عن ذلك تجاهل كل عمليات السحب – بطاقات أو شيكات حسابية - التي تتم بمعرفة المبرمج، وبهذا جعل هذا الجاني البنك يتحمل هذه المسحوبات في باب ميزانية الإدارة، ولم تتم اكتشاف الجريمة إلا عندما أصيب الحاسب بفيروس فسبب عطلًا بأحد النظم المعلوماتية، مما جعل العاملين بالبنك مضطرين للمعالجة اليدوية لكل الحسابات، وحينئذ تظهر الجريمة (الملط، 2006؛ الملا، 2018).

2.2.2.8. جريمة الاعتداء على برامج الحاسب الآلي

يمكن الاعتداء على برامج الحاسب الآلي في أية مرحلة من مراحل صنع برامج التشغيل أو برامج التطبيق أو في لحظة صيانتها أو تحديثها، فلابد أن من يرتكب هذه الجرائم يكون من قِبل المتخصصين الذين لديهم معرفة تقنية في برامج الحاسب الآلي وبصفة خاصة في مجال البرمجة، وبالتالي قد يتمكن الجاني من إحداث تعديل في برامج التشغيل أو في برامج التطبيق. فبرامج التشغيل هي البرامج التي لا يعمل النظام المعلوماتي بدونها، وهي التي تقوم بتنظيم التعليمات الخاصة بالنظام، ويتحقق الاعتداء عليها عندما يتدخل شخص فيضيف للبرامج عدة تعليمات يستطيع من خلالها أن يحصل على معلومات أو جميع البيانات المثبتة على النظام المعلوماتي (حمشاشي، 2009؛ رمضان، 2009).

3.2.8. الجرائم المعلوماتية بالاعتداء على الأشخاص

هي الجرائم التي تنال بالاعتداء أو تهدد بالخطر على الحقوق ذات الطابع الشخصي، ومن هذه الجرائم جرائم القتل، وجرائم الجرح والضرب، والإجهاض، والاعتداء على العرض... إلخ. ومن الجرائم الاعتداء على النفس التي تقع بواسطة الحاسوب ما يلي (حمشاشي، 2009؛ رمضان، 2009).

- القتل بالحاسب والتسبب في الوفاة.
- التحريض على قتل الغير.
- التحريض على قتل الإنسان لنفسه (الانتحار) عبر الإنترنت.
- الترويج للمواد المخدرة بواسطة الحاسوب.
- بث معلومات مزيفة، ونشر معلومات بغرض التضليل، أو إرسال بريد إلكتروني غير مرغوب فيه.
- نشر المواقع الإباحية عبر الإنترنت بقصد نشر الفحشاء والمساس بالحياء عبر الإنترنت، واستخدامه من أجل الترويج للدعارة.
- الاطلاع على البيانات الشخصية غير المصرح بدخولها لغير أصحابها؛ مما يعد انتهاكًا شخصيًا للحرمات.
- الدخول على المواقع الشخصية بطريقة غير مشروعة لسرقة الصور والهويات بطريقة غير مشروعة لاستغلالها في أنشطة جنسية غير المشروعة.

4.2.8. الجرائم المعلوماتية ضد الأموال

هي الجرائم التي تنال بالاعتداء أو تهدد بالخطر على الحقوق ذات القيمة المالية، ومن أهم تطبيقات هذه الجرائم في نطاق الجرائم المعلوماتية (سامي، 2016؛ الملا، 2018):

- التعدي على بيانات ومعلومات الحاسب وسرقتها.
- قرصنة البرامج وسرقة خدمات الحاسب.
- اقتحام الأنظمة المعلوماتية للأفراد أو المؤسسات على الحاسوب لتخريبها.
- استخدام الحاسب للحصول على البطاقات المالية أو استخدامها للغير دون ترخيص أو تدميرها.
- جرائم الاحتيال بالتلاعب بالمعطيات والنظم.
- استخدام علامات تجارية للغير موجودة مسبقًا من غير ترخيص.

5.2.8. الجرائم المعلوماتية ضد الحكومة:

يقصد بالجرائم ضد الحكومة أو ضد المصلحة العامة، هي تلك الجرائم التي تنال بالاعتداء أو تهدد الخطر على الحقوق ذات الطابع العام، لعل من أبرزها (حمشاشي، 2009؛ البشرى، 2014):-

- تزييف وتقليد العملة المالية – تزوير المستندات الرسمية – الاعتداء على أمن الدولة داخليًا وخارجيًا، والعبث بالأدلة القضائية، والتأثير فيها.
- تهديد السلامة العامة.
- بث البيانات من مصادر مجهولة.
- جرائم تعطيل الأعمال الحكومية.
- جرائم تعطيل تنفيذ القانون.
- جرائم الإخفاق في الإبلاغ عن جرائم الحاسب.
- الإرهاب الإلكتروني.
- التجسس للوصول إلى معلومات سرية لا ينبغي إذاعتها.

6.2.8. الجرائم الإلكترونية الأخرى

وتشتمل على جرائم مزادات الإنترنت متعددة الصور، ومن أبرزها ما يلي (البشرى، 2014؛ سامي، 2016؛ الملا، 2018):-

1.6.2.8. الاحتيال وعدم التسليم أو التوصيل

هو أن يعرض المحتال في المزاد صنفًا وهميًا لا وجود له بالفعل؛ بحيث إن المشتري بعد حصول الدفع وانتهاء المزاد لا يتسلم الصنف الذي اتفق على شرائه، أما إذا كان الدفع عن طريق البطاقة الائتمانية فإن هذا المحتال يسيء استخدامها بعد أن حصل على رقمها واسم المشتري.

2.6.2.8. الاحتيال وخداع المشتري حول القيمة الحقيقية لصنف المعروض للبيع

وهو أن يعرض معلومات غير صحيحة عن المبيع، مثل استخدام صور غير حقيقية للمبيع، أو تصوير المبيع وتعديل الصورة بمدخلات توهم المشتري بأن المبيع بحالة جيدة.

3.6.2.8. الاحتيال بطريقة المثلث

أن يقوم المحتال أولًا بشراء المبيع من إحدى الشركات عن طريق بطاقة ائتمانية مزورة أو مسروقة، ثم يقوم بيع ما اشتراه في مزاد عبر الإنترنت، فيقوم المشتري بتحويل ثمن المبيع إلى المحتال، ثم يرسل المبيع للمشتري. وإذا اكتشف أن البطاقة الائتمانية مسروقة أو مزورة فإن ضحية هذا الاحتيال هما المشتري والشركة؛ أما المحتال فإنه يكون خرج من هذا المثلث.

4.6.2.8. تجارة بضائع السوق السوداء

هي عرض المبيع في مزاد عبر الإنترنت، ويسلم المبيع بدون تعليمات الاستخدام وبغير تغليف.

5.6.2.8. جرائم مزودي الخدمات

هي كافة الأفعال التي يقوم بها المورد أو المتعهد المستضيف لخدمات الإنترنت، مثال ذلك: شركات توفير الخدمة، والتي يفترض أن تقوم بتوفير وتأمين الخدمة وبتنظيم وتخزين المضمون الذي يسمح للموردين المستخدمين بالوصول إلى الجمهور، وذلك من خلال توريد الخدمات إلى مواقع خارجية.

6.6.2.8. جرائم أسماء نطاقات الإنترنت

تلك الجرائم تدور حول التنازع على هوية أي موقع على الإنترنت تريد أن تصل إليه، والذي يعتبر هو العنوان الفعلي للموقع؛ فهناك طريقة كسبهم للأموال هو أنهم يحجزون أسماء النطاقات التي يشيع استعمالها حتى يبيعوها فيما بعد لمن يرغب فيها.

8.3. موقف التشريع السعودي والمصري من الجريمة المعلوماتية:

تعتبر أغلبية التشريعات العربية المقارنة المتعلقة بمكافحة الإجرام المعلوماتي حديثة نسبيًا، لقد تأخر المشرعون في إصدار قوانين منظمة للمجال المعلوماتي، خاصّة منها المتعلقة بمكافحة الجريمة الإلكترونية، ورغم أن بعض الدول المتقدمة كانت سباقة لسن قوانين للوقاية من مخاطر الجريمة الإلكترونية، لذلك أصبحت الحاجة ملحة بسن قوانين لحماية الأنظمة المعلوماتية، ليواكب التشريع الجنائي ما تفرزه ثورة تكنولوجيا المعلومات.

تعد دولة الإمارات من أوائل الدول العربية التي شرعت قانونًا من أجل الحماية القانونية للمعلومات، حيث صدر القانون الاتحادي رقم (40) لسنة 1992 الخاص بحقوق المؤلف والمصنفات الفكرية. وأصدرت قانون خاص بشأن مكافحة جرائم تقنية المعلومات رقم (2) لسنة 2006. وفي دولة قطر صدر القانون رقم (25) لسنة 1995 بشأن المصنفات الفكرية حقوق المؤلف، ورد هذا القانون نص لحماية برامج الحاسب الآلي. وصدر في دولة الكويت قانون لحماية المصنفات والحاسب الآلي والبرنامج وقواعد البيانات، بالمرسوم رقم (5) لسنة 1999.

لذلك سنتناول في هذا المبحث في المطلب الأول موقف التشريع السعودي، أما في المطلب الثاني موقف التشريع المصري المقارن.

1.3.8. موقف التشريع السعودي

أدركت المملكة السعودية العربية أهمية تنظيم التعاملات الإلكترونية، لذلك وافق مجلس الوزراء في المملكة على نظام مكافحة جرائم المعلوماتية بموجب المرسوم الملكي رقم (17) لعام 1428 H(2007)، وتعد المملكة العربية السعودية من الدول العربية التي أصدرت نظامًا خاصًا لمكافحة الجرائم المعلوماتية. ويلاحظ على النظام السعودي أنه حدد معظم الأفعال التي تشكل خطرًا على المعلومات وجعلها من الجرائم المعلوماتية، ووضح متى تشدد العقوبة، وعقوبة الشروع في تلك الجرائم، ومتى يعفى من العقاب، وتطرق إلى العقوبة التكميلية.

1.1.3.8. الإطار التجريمي والعقابي للجرائم المعلوماتية

عرف النظام السعودي في الفقرة الثامنة من المادة الأولى من نظام مكافحة الجرائم المعلوماتية نص على أن المقصود بالجريمة المعلوماتية هي: أي فعل يرتكب متضمنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام.

نصت المادة الثالثة من هذا النظام على عقوبة السجن مدة لا تزيد عن سنة وبغرامة لا تزيد على خمس مئة ألف **ريال**، أو بإحدى هاتين العقوبتين؛ على كل شخص يرتكب أيةً من الجرائم المعلوماتية الآتية:

- التنصت على ما هو مرسل عن طريق شبكة المعلوماتية أو أحد أجهزة الحاسب الآلي-دون مسوغ نظامي صحيح -أو التقاطه أو اعتراضه.
- الدخول غير المشروع لتهديد شخص أو ابتزازه؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعًا.
- الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.
- المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها.
- التشهير بالآخرين، وإلحاق الضرر بهم، عبر وسائل تقنيات المعلومات المختلفة.

كما نصت المادة الرابعة من هذا النظام على عقوبة السجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني **ريال**، أو بإحدى هاتين العقوبتين؛ على كل شخص يرتكب أيةً من الجرائم المعلوماتية الآتية:-

- الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة.
- الوصول-دون مسوغ نظامي صحيح-إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات.

ويعاقب المنظم السعودي بعقوبة السجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين **ريال**، أو بإحدى هاتين العقوبتين على الجرائم المعلوماتية الآتية:

- الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها.
- إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها.
- إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت.

كما نصت المادة السادسة من هذا النظام على أنه يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين **ريال**، أو بإحدى هاتين العقوبتين، على الجرائم المعلوماتية الآتية:

- إنتاج ما من شأنه المساس بالنظام العام، أو القيم الدينية، أو الآداب العامة، أو حرمة الحياة الخاصة، أو إعداده، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي.
- إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره للإتجار في الجنس البشري، أو تسهيل التعامل به.
- إنشاء المواد والبيانات المتعلقة بالشبكات الإباحية، أو أنشطة الميسر المخلة بالآداب العامة أو نشرها أو ترويجها.
- إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للإتجار بالمخدرات، أو المؤثرات العقلية، أو ترويجها، أو طرق تعاطيها، أو تسهيل التعامل بها.

ونصت المادة السابعة من هذا النظام على أخطر أنواع الجرائم المعلوماتية وهي إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره؛ لتسهيل الاتصال بقيادات الأجهزة الحارقة، أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية. أو الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني. عقوبة السجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين.

كما عاقبت المادة التاسعة من هذا القانون على الاشتراك في الجريمة، حيث نصت على أنه" يعاقب كل من حرض غيره، أو ساعده، أو اتفق معه على ارتكاب أي من الجرائم المنصوص عليها في هذا النظام؛ إذا وقعت الجريمة بناءً على هذا التحريض، أو المساعدة، أو الاتفاق، بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها، ويعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية".

وكما نصت المادة العاشرة من هذا النظام على أنه "يعاقب كل من شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة".

2.3.8. موقف التشريع المصري

نص المشرع المصري على مكافحة جرائم تقنية المعلومات في القانون رقم 175 لسنة 2018، فحصر المشرع المصري الجرائم التي يتوقع ارتكابها بواسطة تقنية المعلومات مع عدم الإخلال بأي عقوبة أشد، وبيان تلك الجرائم هو على النحو التالي:

1.2.3.8. جريمة الانتفاع بدون حق بخدمات الاتصالات والمعلومات وتقنيتها

نصت المادة (13) من هذا القانون على أنه كل من انتفع بدون وجه حق عن طريق شبكة النظام المعلوماتي أو إحدى وسائل تقنية المعلومات بخدمة اتصالات أو خدمة من خدمات قنوات البث المسموع أو المرئي. يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين.

جريمة الدخول غير المشروع: نصت المادة (14) من هذا القانون على أنه كل من دخل عمدًا، أو دخل بخطأ غير عمدي وبدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه، يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدًا، أو دخل بخطأ غير عمدي وبدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه. فإذا نتج عن ذلك الدخول إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي، يعاقب بالحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين.

جريمة تجاوز حدود الحق في الدخول: نصت المادة (15) على أنه كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتي مستخدما حقًا مخولًا له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول. يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين.

جريمة الاعتراض غير المشروع: نصت المادة (16) على أنه كل من اعترض بدون وجه حق أي معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي. يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتين وخمسين ألف جنيه، أو بإحدى هاتين العقوبتين.

2.2.3.8 . جريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية

نصت المادة (17) على أنه كل من أتلف أو عطل أو عدل مسار أو ألغى كليًا أو جزئيًا، متعمدًا وبدون وجه حق البرامج والبيانات أو المعلومات المخزنة أو المعالجة على أي نظام معلوماتي وما في حكمه، يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين.

3.2.3.8. جريمة الاعتداء على البريد الإلكتروني أو المواقع أو الحسابات الخاصة

نصت المادة (18) على أنه كل من أتلف أو عطل أو أبطأ أو اخترق بريدًا إلكترونيًا أو موقعًا أو حسابًا خاصًا بأحد الناس. يعاقب بالحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين.

فإذا وقعت الجريمة على بريد إلكتروني أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة، تكون العقوبة الحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين.

جريمة الاعتداء على تصميم موقع: نصت المادة (19) على أنه كل من أتلف أو عطل أو أبطأ أو أخفى أو غير تصاميم موقع خاص بشركة أو مؤسسة أو منشأة أو شخص طبيعي بغير وجه حق". يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين.

4.2.3.8. جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة

نصت المادة (20) على أنه كل من دخل عمدًا، أو بخطأ غير عمدي وبدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو اخترق موقعًا أو بريدًا إلكترونيًا أو حسابًا خاصًا أو نظامًا معلوماتيًا يدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكا لها، أو يخصها. يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين.

فإذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية، فتكون العقوبة السجن، والغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه. وفي جميع الأحوال، إذا ترتب على أي من الأفعال السابقة إتلاف تلك البيانات أو المعلومات أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي أو البريد الإلكتروني، أو تدميرها أو تغييرها أو تغيير تصاميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها، أو إلغائها كليا أو جزئيا، تكون العقوبة السجن، والغرامة التي لا تقل عن مليون جنيه ولا تجاوز خمسة ملايين جنيه".

5.2.3.8. جريمة الاعتداء على سلامة الشبكة المعلوماتية

نصت المادة (21) على أنه كل من تسبب متعمدًا في إيقاف شبكة معلوماتية عن العمل أو تعطيلها أو الحد من كفاءة عملها أو التشويش عليها أو اعتراض عملها أو أجرى بدون وجه حق معالجة إلكترونية للبيانات الخاصة بها. يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين.

ويعاقب كل من تسبب بخطئه في ذلك بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين.

فإذا وقعت الجريمة على شبكة معلوماتية تخص الدولة أو إحدى الشخصيات الاعتبارية العامة أو تمتلكها أو تدار بمعرفتها تكون العقوبة السجن المشدد، وبغرامة لا تقل عن خمس مئة ألف جنيه ولا تجاوز مليون جنيه.

6.2.3.8. البرامج والأجهزة والمعدات المستخدمة في ارتكاب جرائم تقنية المعلومات

نصت المادة (22) على أنه كل من حاز أو أحرز أو جلب أو باع أو أتاح أو صنع أو أنتج أو استورد أو صدَّر أو تداول، أي أجهزة أو معدات أو أدوات أو برامج مصممة أو أكواد مرور أو شفرات أو رموز أو أية بيانات مماثلة، وثبت أن ذلك السلوك كان بغرض استخدام أي منها في ارتكاب أو تسهيل ارتكاب أية جريمة من الجرائم المنصوص عليها في هذا القانون، أو إخفاء آثارها أو أدلتها أو ثبت ذلك الاستخدام أو التسهيل أو الإخفاء. يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن ثلاث مئة ألف جنيه ولا تجاوز خمس مئة ألف جنيه، أو بإحدى هاتين العقوبتين.

7.2.3.8. الجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات

جرائم الاحتيال والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الإلكتروني: نصت المادة (23) على أنه كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أو بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الإلكترونية. يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه، ولا تجاوز خمسين ألف جنيه أو بإحدى هاتين العقوبتين.

فإن قصد من ذلك استخدامها في الحصول على أموال الغير أو ما تتيحه من خدمات يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين. وتكون العقوبة الحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو إحدى هاتين العقوبتين، إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على تلك الخدمات أو مال الغير.

الجرائم المتعلقة باصطناع المواقع والحسابات الخاصة والبريد الإلكتروني: نصت المادة (24) على أنه كل من اصطنع بريدًا إلكترونيًا أو موقعًا أو حسًابا خاصًا ونسبه زورًا إلى شخص طبيعي أو اعتباري. يعاقب بالحبس مدة لا تقل

عن ثلاثة أشهر، وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز ثلاثين ألف جنيه أو بإحدى هاتين العقوبتين.

فإذا استخدم الجاني البريد أو الموقع أو الحساب الخاص المصطنع في أمر يسئ إلى ما نسب إليه، تكون العقوبة الحبس الذي لا تقل مدته عن سنة، والغرامة التي لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين.

واذا وقعت الجريمة على إحدى الشخصيات الاعتبارية العامة، فتكون العقوبة السجن، والغرامة التي لا تقل عن مائة ألف جنيه، ولا تزيد على ثلاث مئة ألف جنيه".

الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتي غير المشروع: نصت المادة (25) على أنه كل من اعتدى على أي من المبادئ أو القيم الأسرية في المجتمع المصري أو انتهك حرمة الحياة الخاصة، أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقته، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخبارًا أو صورًا وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواءً كانت المعلومات المنشورة صحيحة أو غير صحيحة. يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين.

كما نصت المادة (26) على أنه كل من تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها بمحتوى منافٍ للآداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه. يعاقب بالحبس مدة لا تقل عن سنتين ولا تجاوز خمس سنوات، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز ثلاث مئة ألف جنيه، أو بإحدى هاتين العقوبتين.

الجرائم المرتكبة من مدير الموقع: نصت المادة (27) على أنه كل من أنشا أو أدار أو استخدم موقع أو حساب خاص على شبكة معلوماتية يهدف إلى ارتكاب أو تسهيل ارتكاب جريمة معاقب عليها قانونًا، في غير الأحوال المنصوص عليها في هذا القانون، يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن مائة ألف جنيه، ولا تزيد عن ثلاث مئة ألف جنيه، أو بإحدى هاتين العقوبتين.

كما نصت المادة (28) على أنه كل مسئول عن إدارة موقع أو حساب خاص أو بريد إلكتروني أو نظام معلوماتي، إذا أخفى أو عبث بالأدلة الرقمية لإحدى الجرائم المنصوص عليها في هذا القانون والتي وقعت على موقع أو حساب أو بريد إلكتروني بقصد إعاقة عمل الجهات الرسمية المختصة". يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين.

كما نصت المادة (29) على أنه كل مسئول عن إدارة الموقع أو الحساب الخاص أو البريد الإلكتروني أو النظام المعلوماتي عرض أي منها لإحدى الجرائم المنصوص عليها في هذا القانون. يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين.

ويعاقب كل مسئول عن إدارة الموقع أو الحساب الخاص أو البريد الإلكتروني أو النظام المعلوماتي تسبب بإهماله في تعرض أي منها لإحدى الجرائم المنصوص عليها في هذا القانون، بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مئة ألف جنيه، أو بإحدى هاتين العقوبتين.

9. تطبيقات قضائية

- قضت المحكمة الجزائية بمحافظة القطيف في دعوى رقم 3599201 بتاريخ 1435 H (2013)، توجيه الاتهام من قبل المدعي العام على المدعى عليه؛ طالبًا إثبات إدانته بإرسال رسائل إلكترونية عن طريق بريده الإلكتروني إلى البريد الإلكتروني للمدعي ولأشخاص آخرين تتضمن قذفًا وسبًا وشتمًا له وتشهيرا به. فحكمت المحكمة بعد ثبوت إدانة المدعى عليه بما نسب إليه، ومعاقبته لحق المدعي بالحق الخاص بجلده ثمانين جلدة حد القذف. ومعاقبته للحق العام بسجنه مدة شهرين وتغريمه خمسة آلاف ريال. وصدّق الحكم من محكمة الاستئناف بالمنطقة الشرقية بالقرار رقم 35239597 بتاريخ 1435 H (2013).
- قضت المحكمة الجزائية بمحافظة الاحساء في دعوى رقم 3426314 بتاريخ H1434 (2012)، توجيه الاتهام من قبل المدعي العام على المدعى عليهما؛ بالدخول غير المشروع على موقع صحيفة الالكترونية بغرض تخريب وتغيير التصميم إلى صور نسائية فاضحه واتلاف الموقع. فحكمت المحكمة على المدعى الأول بسجنه ستة أشهر والمدعى عليه الثاني بأربعة أشهر. وصدّق الحكم من محكمة الاستئناف بالمنطقة الشرقية بالقرار رقم 35110953 بتاريخ 1435 H (2013).
- قضت المحكمة الجزائية بمحافظة جدة في دعوى رقم 43271516 بتاريخ 1434 H (2012)، توجيه الاتهام من قبل المدعي العام على المدعى عليه؛ طالبًا إثبات إدانته بالشذوذ الجنسي وعرض نفسه على الآخرين لفعل الفاحشة به من خلال وسائل التواصل الاجتماعي وقيامه بوضع صور له بجواله وهو عارٍ. فحكمت المحكمة بعد ثبوت إدانة المدعى عليه بما نسب إليه، بمعاقبته بالسجن لمدة تسعة أشهر، وبجلده تسعين جلدة دفعة واحدة، وبمصادرة الجوال المستعمل في الجريمة. وصدّق الحكم من محكمة الاستئناف بمنطقة مكة المكرمة بالقرار رقم 35232371 بتاريخ 1435 H (2013).
- قضت المحكمة الجزائية بمحافظة سكاكا في دعوى رقم 345429119 بتاريخ 1434 H (2012)، توجيه الاتهام من قبل المدعي العام على المدعى عليه؛ طالبًا إثبات إدانته بحيازة وبيع الأفلام الإباحية وتخزينها واعداد ما من شأنه المساس بالقيم الدينية والآداب العامة عن طريق الشبكة المعلوماتية. فحكمت المحكمة بعد ثبوت إدانة المدعى عليه بما نسب إليه، بمعاقبته بالسجن لمدة سنة كاملة، وبجلده ثلاثمائة جلدة مفرقة، وتغريمه خمسة آلاف ريال، وبأخذ التعهد عليه بعدم العودة لمثل ذلك، وبإتلاف المضبوطات، مع التوصية بإبعاده إلى بلاده بعد إنهاء فترة محكوميته، وصدّق الحكم من محكمة الاستئناف بمنطقة الجوف بالقرار رقم 35228826 بتاريخ 1435 H (2013).

10. الخاتمة

استهدفت الدراسة مدى التعرف على تأثير الذكاء الاصطناعي على الجريمة الإلكترونية، فالجرائم المعلوماتية هي ظاهرة إجرامية مستجدة نسبيًا، وجاء هذا النوع من الجرائم بالتزامن مع التطورات التي تطرأ على التقنيات والتكنولوجيا الحديثة وثورة المعلوماتية، إلا أنها جرائم قابلة للتطور المستمر لارتباطها الوثيق بالتطور التقني الهائل في مجال الحاسب الآلي واستخدام شبكة الإنترنت في ظل انفتاح العالم وثورة المعلوماتية، وبقدر انتشار التكنولوجيا بقدر ما تكثر الجرائم المعلوماتية، لهذا كان لابد أن تواكب التشريعات الوطنية هذا التطور الملحوظ في جرائم المعلوماتية، لذلك تم مكافحتها من خلال سن قوانين خاصة بالجرائم المعلوماتية.

10.1. النتائج:

- يلعب الذكاء الاصطناعي دورًا مهما في زيادة الجرائم الإلكترونية وانتشارها وهو ما يثبت صحة فرضية الدراسة.
- لم يتفق فقهاء القانون على تعريفًا جامعًا للجريمة الإلكترونية.
- تتمتع الجريمة الإلكترونية بطبيعة قانونية مغايرة تمامًا للجريمة التقليدية.
- تعتبر الجرائم المعلوماتية أقل عنفًا من الجرائم التقليدية، حيث أنها لا تحتاج إلى أدنى مجهود عضلي؛ بل تعتمد على الدراسة الذهنية والتفكير العلمي القائم على معرفة بتقنيات الحاسوب.
- إن الباعث على ارتكاب الجرائم المعلوماتية هو الحصول على النفع المادي السريع.
- لا يتم في الغالب الإبلاغ عن جرائم الإنترنت إما لعدم اكتشاف الضحية لها وإما خشيته من التشهير.
- يسهل ارتكاب الجرائم المعلوماتية، على الرغم أنها تعتبر جرائم صعبة الإثبات، حيث يصعب في كثير من الأحيان العثور على أثر مادي للجريمة المعلوماتية.
- تؤدي عولمة الجرائم الإلكترونية إلى تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم، فتعتبر هذه الجرائم هي صورة صادقة من صور العولمة.
- تجريم النظام السعودي والقانون المصري للجريمة الإلكترونية في نصوص مستقلة عن النصوص القانونية للجرائم التقليدية.
- مواكبة النظام السعودي والقانون المصري للتشريعات المقارنة في ملاحقتها للأنماط المستحدثة من الجريمة الإلكترونية.

10.2. التوصيات:

بناءً على نتائج الدراسة السابقة، توصي الدراسة بما يلي:

- تطبيق أنظمة حماية المعلومات ومراجعتها بصورة دورية لتطويرها بما يتناسب مع سرعة التقدم التقني.
- ضرورة تأهيل مأموري الضبط القضائي والنيابة العامة وتدريبهم على كيفية التعامل مع الجرائم الإلكترونية وبالتعاون مع التقنيين من أصحاب الخبرة.
- يتعين تخصيص قضاة وتأهيلهم للنظر في هذا النوع من الجرائم.
- ضرورة التعاون الدولي لمكافحة الجرائم الإلكترونية من خلال الاتفاقيات الدولية والإقليمية.
- يجب نشر الوعي بين المواطنين وخاصَّة الشباب بمخاطر التعامل مع المواقع السيئة والمشبوهة على الشبكات، وذلك بتفعيل دور المجتمع المدني والمؤسسات للقيام بدوره التوعوي والوقائي من الوقوع في الرذيلة والممارسات الخاطئة للسلوكيات والممارسات الضارة أخلاقيًا عبر شبكة الإنترنت.

نبذة عن المؤلفة

رانا مصباح عبد المحسن عبد الرازق

قسم العلوم الإدارية والإنسانية، عمادة خدمة المجتمع والتعليم المستمر، جامعة الأميرة نورة بنت عبد الرحمن، الرياض، المملكة العربية السعودية، rmabdelmohsen@pnu.edu.sa, 00966509039953

د. عبد الرازق، دكتوراه في العلوم الجنائية من جامعة المنصورة -مصر، أستاذ القانون الجنائي المساعد، مديرة برنامج دبلوم القانون، عضو هيئة تحكيم بمجلة العلوم القانونية والسياسية بجامعة الشهيد حمه لخضر – الوادي بالجزائر، شاركت بعدة مؤتمرات في القانون الجنائي، ونشرت ستة أبحاث في مجلات محكمة مختلفة، أربعة أبحاث نشر بمجلات إلكترونية، نشرت كتابًا واحدًا.

المراجع

البشرى، محمد. (2014). التحقيق في جرائم الحاسب الآلي. في: مؤتمر *القانون والكمبيوتر والإنترنت*. الإمارات، كلية الشريعة والقانون، جامعة الإمام عبدالرحمن بن فيصل، الدمام، السعودية، 01-03/05/2014.

السلمي، عفاف. (2017). تطبيقات الذكاء الاصطناعي. *مجلة دراسة المعلومات لجمعية المكتبات والمعلومات السعودية*، **بدون رقم مجلد**(19)، 103-124.

الشوا، محمد. (1994). *ثورة المعلومات وانعكاساتها على قانون العقوبات*. القاهرة: دار النهضة العربية.

الشوابكة، محمد. (2004). *جرائم الحاسوب والإنترنت*. عمان: دار الثقافة للنشر والتوزيع.

العريان، محمد. (2004). *الجرائم المعلوماتية*. الإسكندرية: دار الجامعة الجديدة للنشر والتوزيع.

المقصودي، محمد. (2017). الجرائم المعلوماتية. *مجلة العربية للدراسات الأمنية*، **33**(7)، 101-131.

الملا، إبراهيم. (2018). الذكاء الاصطناعي والجريمة الإلكترونية. *مجلة الأمن والقانون: أكاديمية شرطة دبي*، **26**(1)، 114-177.

الملط، أحمد. (2006). *الجرائم المعلوماتية*. الإسكندرية: دار الفكر الجامعي.

بيومي، عبد الفتاح. (2007). *مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت*. الإسكندرية: دار الكتب القانونية.

حمشاشي، أمينة. (2009). *ماهية الجريمة المعلوماتية*. رسالة ماجستير، كلية الحقوق، الجزائر.

رمضان، مدحت. (2009). *جرائم الاعتداء على الأشخاص والإنترنت*. القاهرة: دار النهضة العربية.

سامي، خالد. (2016). الجهود الدولية لمكافحة الجرائم الإلكترونية. *مجلة الدراسات العليا لكلية الدراسات العليا: جامعة النيلين*، السودان، **14**(1)، 1-30.

عفيفي، كامل. (2003). *جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون*. بيروت: منشورات الحلبي الحقوقية.

قارة، آمال. (2002). *الجريمة المعلوماتية*. رسالة ماجستير، كلية الحقوق، جامعة الجزائر، الجزائر، الجزائر.

مراد، عبد الفتاح. (2005). *شرح جرائم الكمبيوتر والإنترنت*. القاهرة: دار الكتب الوثائق المصرية.

يوسف، أمير. (2009). *الجرائم المعلوماتية على شبكة الإنترنت*. الإسكندرية: دار المطبوعات الجامعية.

Adeniran, A.I. (2008). The Internet and Emergence of Yahoo boys Subculture. *International Journal of Cyber Criminology*, **2**(2), 381–68.

Al Badayneh, D. (2013). Human behaviour: when and where virtual society meets physical society. *European Journal of Science and Theology*, **9**(1), 105–10.

Al Bushra, M. (2014). Altahqiq fi jarayim alhasib alalay. 'Computer crime investigation'. *In: Law, Computer and Internet Conference Held*. College of Sharia and Law, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia, 01-03/05/2014.[in Arabic]

Al Arian, M. (2004). *Aljarayim Almaelumatiatu*. 'Informational Crimes'. Alexandria: The New University House for Publishing and Distribution. [in Arabic]

Al Malaa, I. (2018). *Aldhika alaistinaeiu w aljarimat* al'iiliktruniat. 'Artificial Intelligence and Cyber Crime'. *Security and Law Magazine: Dubai Police Academy*, **26**(1), 114–77. [in Arabic]

Al Maqsudiu, M. (2017). Aljarayim almaelumatiatu.'Informational crimes'. *The Arab Journal for Security Studies*, **33**(7), 101–31. [in Arabic]

Al Multu, A. (2006). *Aljarayim Almaelumatiatu*. 'Informational Crimes'. Alexandria: University Thought House. [in Arabic]

Al Shawa, M. (1994). *Thawrat Almaelumat Waineikasatiha Ealaa Qanun Aleuqubati* 'The Information Revolution and its Implications for the Penal Code'. Cairo: The Arab Renaissance House. [in Arabic]

Al Shawabkeh, M. (2004). *Jarayim Alhasub Walaintarnat*. 'Computer and Internet Crime'. Amman: House of Culture for Publishing and Distribution. [in Arabic]

Al Silami, A. (2017). Tatbiqat aldhika' alaistinaeii'. 'Artificial Intelligence Applications'. *Journal of the Study of Information of the Saudi Library and Information Association*, **n/a**(19), 103–24. [in Arabic]

Bayoumi, A. (2007). *Mabadi Al'iijra'at Aljinayiyat Fi Jarayim Alkimbiutur Walaintirnat*. 'Principles of Criminal Procedure in Computer and Internet Crime'. Alexandria: House of Legal Books. [in Arabic]

Afifi, k. (2003). *Jarayim Alkimbiutr Wahuquq Almualaf Walmusanifat Alfaniyat Wadawr Alshurtat Walqanuni* 'Computer Crime, Copyright, Artistic Works, The Role of the Police and the Law'. Beirut: Alhalabi Human Rights Publications. [in Arabic]

Qarat, A. (2002). *Aljarimat Almaelumatiatu*. 'Informational Crime'. Master's Dissertation, Faculty of Law, University of Algeria, Algeria, Algeria.[in Arabic]

Hmishashi, A. (2009). *Mahiat Aljarimat Almaelumatiati* 'What is Information Crime'. Master's Dissertation, Faculty of Law, University of Algeria, Algeria, Algeria. [in Arabic]

Murad, A. (2005). *Sharah Jarayim Alkimbiutur Walaintarnat*. 'Explain Computer and Internet Crimes'. Cairo: The Egyptian Library and Archives. [in Arabic]

Ramadan, M. (2009). *Jarayim Alaietida' Ealaa Al'ashkhas Wal'iintarnat*. 'Crimes of Assaults on Persons and the Internet'. Cairo: Arab Renaissance House. [in Arabic]

Sami, k. (2016). *Aljuhud alduwaliat limukafahat aljarayim al'iiliktruniati*. 'International efforts to combat cybercrime'. *Graduate Studies Journal of the Faculty of Graduate Studies: El-Neelain University,* Sudan, **14**(1), 1–30. [in Arabic]

Yousuf, A. (2009). *Aljarayim Almaelumatiat Ealaa Shabakat Alaintirnat*. 'Information Crimes on the Internet'. Alexandria: University Press. [in Arabic]