



المعهد القضائي الأردني
JUDICIAL INSTITUTE OF JORDAN

الجرائم الإلكترونية (إشكاليات الإثبات – طرق مكافحتها)

دكتور/ جلال فضل محمد العودي
المعهد العالي للقضاء / وزارة العدل الجمهورية اليمنية

2026

مقدمة

تعتبر الجرائم الإلكترونية من بين الجرائم المستحدثة التي ظهرت في ظل التطور التكنولوجي الهائل الذي عرفه مجال الاعلام والاتصالات، فهي تختلف عن الجرائم التقليدية التي ترتكب في العالم المادي، وتتميز بخصائص وسمات جعلت منها ظاهرة إجرامية جديدة لم يألّفها العالم من قبل.

فالجرائم الإلكترونية في أغلب صورها تكون خفية ومستترة لا يلاحظها المجني عليه ولا يدري بوقوعها في كونها تقع في بيئة افتراضية غير محسوسة ولا يتطلب ارتكابها استعمال العنف أو بذل مجهوداً كبيراً كما في الجرائم التقليدية، فكل ما تحتاج هو القدرة على التعامل مع حاسوب مرتبط بشبكة المعلومات الدولية بمستوى تقني يوظف لارتكاب أفعال غير مشروعة، مما يجعلها في الغلب لا تترك أية آثار مادية⁽¹⁾.

وتتجلى خطورة الجريمة الإلكترونية في سهولة ارتكابها وتنفيذها الذي لا يستغرق إلا دقائق معدودة، وأحياناً في لمح البصر، حيث للمجرم المعلوماتي أن يلمس لوحة المفاتيح الحاسب الآلي والتي تقوم على الفور بعمليات الحساب واسقاط الحواجز، وأساليب الحماية الأكثر خدعاً، كما أن محو أثارها واتلاف أدلتها غالباً ما يلجأ إليه عقب ارتكابها، فعلاً مرتكبها يتسمون بالذكاء والدهاء⁽²⁾. ومن المشكلات الإجرائية التي يثيرها هذا النوع من الجرائم مدى حجية المخرجات الإلكترونية في الإثبات، نظراً لطبيعتها الخاصة بالمقارنة بوسائل الإثبات التقليدية. كذلك من المشكلات التي تطرحها الجرائم الإلكترونية ماهي الطرق أو الأساليب في مكافحتها؟

للإجابة عن التساؤلات يتطلب منا تقسيم هذا البحث إلى المباحث التالية:

- 1- المبحث الأول: الجريمة الإلكترونية.
- 2- المبحث الثاني: ماهية الدليل الإلكتروني.
- 3- المبحث الثالث: الإجراءات العملية والتشريعية لحل مشاكل الجرائم الإلكترونية.
- 4- المبحث الرابع: سلطات القاضي في تقييم الدليل الإلكتروني.
- 5- المبحث الخامس: دور الأمن السيبراني في مكافحة الجريمة السيبرانية.
- 6- المبحث السادس: الذكاء الاصطناعي وأثره على الأمن السيبراني.

(1) انظر: براهيم جمل ، التحقيق الجنائي في الجرائم الإلكترونية ، رسالة دكتوراه مقدمة إلى كلية الحقوق والعلوم السياسية – جامعة مولود معمري – الجزائر 2018م ، ص185.

(2) انظر: عائشة بن قارة مصطفى ، حجية الدليل الإلكتروني في الإثبات الجنائي في القانون الجزائري والقانون المقارن ، دار الجامعة الجديدة 2010م ، ص14 .

نقلاً عن: حياة البشير، دور الدليل الإلكتروني في الإثبات الجنائي ، المعهد العالي للقضاء وزارة العدل المغربية 2015 – 2017م ، ص1

7- المبحث السابع: الذكاء الاصطناعي واستخدامه في إجراءات التقاضي.

المبحث الأول

الجريمة الالكترونية

تتسم الجريمة الالكترونية بطبيعة خاصة تستعدي ضرورة إيجاد سلطات ينام بها الأمر أو التصريح أو مباشرة تنفيذ إجراءات جمع أو إنتاج عناصر الإثبات المرتبطة بالتحقيقات عن الأدلة في الجريمة الالكترونية، وتبعاً لذلك يتسم التحقيق في الجريمة الالكترونية بطبيعة خاصة شأنه شأن الجريمة ذاتها، لذا يتطلب فيمن يتولى التحقيق الابتدائي فيها أن يكون متخصصاً في التحقيق الجنائي ومعالجة البيانات، فضلاً عن ضرورة أن يتوافر لدى الحد الأدنى من المعرفة بالمهارات الفنية والتقنيات الالكترونية الحديثة.

وانتشرت الجرائم الإلكترونية مع انتشار المعاملات الإلكترونية، وتشمل المعاملات الإلكترونية: جميع المعاملات الإدارية الحكومية وخدمات المواطنين بشكل عام والتصاريف المختلفة التي تقدمها الجمارك والضرائب والسجل المدني والخدمات الاستثمارية، التي تتم عن طريق المحررات الإلكترونية التي تصدرها هذه الجهات، ويتم توقيعها من قبل الموظفين العموميين، مما يضيف على المحررات الصفة الرسمية؛ بسبب قيام الموظف العام بتوقيعها إلكترونياً⁽¹⁾.

لذا: سنقوم بتقسيم هذا المبحث إلى المطالب الآتية:

المطلب الأول: تعريف الجريمة الإلكترونية وخصائصها.

المطلب الثاني: تقسيم الجريمة الإلكترونية.

(1) أنظر : د/ خالد مصطفى فهمي ، الحماية القانونية لبرنامج الحاسب الآلي في ضوء قانون الحماية الفكرية ، دار الجامعة الجديدة للنشر ، الإسكندرية 2005
نقلاً عن : سوسن سعيد شندي ، دليل الإثبات الإلكتروني ، مجلة جامعة شندي بالسودان ، العدد يوليو 2011م ، ص 138 .

المطلب الأول

تعريف الجريمة الالكترونية وخصائصها

تتميز الجريمة الالكترونية بكونها لا تترك آثاراً مادية لها بعد ارتكابها، وصعوبة الاحتفاظ الفني بآثارها إن وجدت، إذ ليس هناك أموالاً أو مجوهرات مفقودة، فهي لا تعترف بحدود جغرافية أو سياسية، ولذا سنقوم بتقسيم هذا المطلب إلى الآتي:

الفرع الأول: تعريف الجريمة الالكترونية.

الفرع الثاني: خصائص الجريمة الإلكترونية.

الفرع الأول

تعريف الجريمة الالكترونية

لم يكن من اليسير على مشرعي وفقهاء القانون التوصل لتعريف جامع مانع متفق عليه لجرائم التقنية المعلوماتية، فهي جرائم من الصعوبة تعريفها أو كم قيل هي جرائم تقاوم التعريف نظراً لما يمر به العالم من تطور يومي على الصعيدين العلمي والتقني في مجال الاتصالات وتكنولوجيا المعلومات وما صاحبها من تطور في شبكة الإنترنت وظهور فئات من المجرمين والجرائم المتطورة بتطور تلك التكنولوجيا⁽¹⁾.

وهناك العديد من التعريفات للجريمة الالكترونية⁽²⁾ نختار منها الآتي:

1 - الجريمة الالكترونية: هو نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة الحاسب الآلي بطريقة مباشرة أو غير مباشرة لوسيلة أو هدف لتنفيذ الفعل الاجرامي⁽³⁾.

(1) أنظر: محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة 1994م، ص5 وما بعدها.

(2) لا يوجد تعريف محدد للجرائم الإلكترونية؛ نظراً لتطور الجريمة وتنوع أساليب ارتكابها؛ ولكن يمكن وضع أسس عامة وأركان عامة يمكن التعرف عليها، أو تحديد السلوك الاجرامي المستحدث المكون للجريمة، فإذا ما توافر هذا السلوك أو العناصر أو الأركان أصبح الفعل أو العمل المرتكب عملاً إجرامياً يستوجب العقاب.

(3) أنظر: د/ عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جريمة الكمبيوتر والانترنت، دار الكتل القانونية، القاهرة 2005، ص1.

2 - الجريمة الالكترونية: هو نشاط غير مشروع لنسخ أو الوصول إلى المعلومات المخزونة داخل الحاسوب أو تغييرها أو حذفها أو الذي تحول عن طريقه (1).

3- الجريمة الالكترونية: هو كل فعل أو امتناع عمدي ينشأ عن نشاط غير مشروع لنسخ أو تغييرات أو حذف أو الوصول إلى المعلومات المخزونة في الحاسب أو تلك التي تحول طريقه (2).

4- "هو نشاط اجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الاجرامي المقصود" (3)

5- خبراء المنظمة الاوربية للتعاون الاقتصادي عرفوا الجريمة الالكترونية بأنها: كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها".

6- أما مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين فقد عرف الجريمة الالكترونية بأنها: " أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي، أو شبكة حاسوبية، والجريمة تلك تتمثل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الالكترونية (4).

كما قد يطلق على الجريمة الكترونية مصطلح الجرائم السيبرانية والذي عرفها البعض بأنها " هي التي تتم بواسطة الكمبيوتر أو أحد وسائل التقنية الحديثة على كمبيوتر آخر أو أحد وسائل التقنية الحديثة مع ضرورة توفر شبكة اتصال فيما بينهما (5)".

فالجريمة السيبرانية هي: نشاط اجرامي تستخدم فيه تقنية الحاسب الالى بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الاجرامي المقصود(6).

(1) أنظر: د/ نهلا عبد القادر المومني، الجرائم المعلوماتية، ط: الأولى، دار الثقافة للنشر والتوزيع، عمان - الأردن 2008م، ص48.

(2) أنظر: د/ رامي القاض، مكافحة الجرائم المعلوماتية في التشريعات المقارنة في ضوء الاتفاقيات والمواثيق الدولية، دار النهضة العربية، ط: الأولى القاهرة 2011م، ص5

(3) أنظر: د/ عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والانترنت، بهجت للطباعة والتجليد، مصر 2009م، ص10.

(4) أنظر: شهر زاد حداد، الدليل الالكتروني في مجال الاثبات الجنائي، رسالة ماجستير قُدمت لكلية العلوم السياسية- جامعة العربي مهدي أم البواقي 2016م - 2017م، ص7.

(5) أنظر: عن اسمامة مهمل، الاجرام السيبراني، رسالة ماجستير، كلية الحقوق والعلوم السياسية - جامعة محمد بوضياف الجزائر 2017م - 2018م، ص9.

(6) أنظر: محمود أحمد القرعان، الجرائم الالكترونية، دار وائل للنشر والتوزيع، ط: الأولى، عان - الأردن 2017م، ص19.

من خلال ما التعاريف السابقة للجريمة الإلكترونية، يمكننا تعرفها بأنها الاستخدام الغير المشروع للأجهزة الإلكترونية مع ضرورة توفر شبكة اتصال فيما بينهما، مما نتج عنه الحاق الضرر لدى الآخرين سواء كانوا اشخاص، أو مؤسسات، أو دول.

فقد استعملنا مصطلح الأجهزة الإلكترونية؛ كون يدخل ضمن الأجهزة الكمبيوتر، والتلفون، الآيباد، أو أي جهاز إلكتروني، بخلاف بعض التعاريف الذي اقتصر استخدام الجريمة الإلكترونية عن طريق الكمبيوتر، كذلك استخدمنا مصطلح الحاق الضرر لدى الغير، يدخل ضمن الضرر اتلاف أو تدمير أو حذف أو سرقة البيانات من جهاز المستهدف وقد تحدث الجريمة الإلكترونية دون المساس في بيانات جهاز المجني عليه، كجريمة التشهير في الشخصيات الاجتماعية والسياسية عبر استخدام الشبكات العنكبوتية (النت).

الفرع الثاني

خصائص الجريمة الإلكترونية

تتميز الجريمة الإلكترونية بعدة خصائص تميزه عن الجرائم التقليدية، وأبرز تلك الخصائص ما يلي:

1- الجريمة الإلكترونية عابرة لحدود.

كشفت الجريمة الإلكترونية عالماً جديداً لا يعترف بالحدود الجغرافية والسياسية للدول ولا بسيادتها، حيث فقدت الحدود الجغرافية كل أثر لها في بيئة إلكترونية متشعبة العلاقات، الأمر الذي خلق صعوبات وإشكالات قانونية لا تقتصر على ضبط هذه الجرائم وإثباتها فحسب، وإنما أثارت أيضاً تحديات أكثر تعقيداً مرتبطة بتحديد جهة الاختصاص وبالتبعية القانون الواجب التطبيق على هذا الصنف من الجرائم⁽¹⁾.

(1) أنظر: عميد دكتور/ جلال فضل محمد العودي، مقالات في الجرائم السيبرانية، شبكة أجهزة إنفاذ القانون بشأن مكافحة الجريمة الإلكترونية، مكتب النائب العام عدن 2022م، ص50.

2- صعوبة اكتشافها وإثباتها.

تتميز الجريمة الإلكترونية بكونها لا تترك أثراً مادية لها بعد ارتكابها، وصعوبة الاحتفاظ الفني بأثارها إن وجدت، إذ ليس هناك أموال أو مجوهرات مفقودة، وإنما هي أرقام تتغير في السجلات لذا نجد أن معظم جرائم الأنترنت تكتشف بالمصادفة، أو بعد فترة طويلة من ارتكابها⁽¹⁾.

3- الجريمة الإلكترونية تتم عادة بتعاون أكثر من شخص.

تتميز الجريمة الإلكترونية أنها تتم عادة بتعاون أكثر من شخص على ارتكابها، فغالباً ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والأنترنت، يقوم بالجانب الفني من المشروع الإجرامي، وشخص آخر من المحيط أو خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه.

إذ أن الأشخاص الذين يقومون بارتكابها عادة يكونون من ذوي الاختصاص في تقنية المعلومات، والاشتراك في إخراج الجريمة المعلوماتية إلى حيز الوجود وقد يكون اشتراكاً سلبياً وهو الذي يتضح بالصمت من جانب من يعلم بالجريمة في محاولة منه لتسهيل إتمامها، وقد يكون اشتراكاً إيجابياً وهو الغالب في الكثير من الجرائم ويتمثل في المساعدة الفنية أو المادية⁽²⁾.

(1) أنظر: د/ سميرة معاشي، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني، العدد السابع، كلية الحقوق والعلوم السياسية – جامعة محمد خضير، سكرة 2010م، 284.

(2) أنظر: نهلا عبد القادر المومني، الجرائم المعلوماتية، مرجع سابق، ص 58.
نقلا عن: شهر زاد حداد، الدليل الإلكتروني في مجال الإثبات الجنائي، رسالة ماجستير مقدمة إلى كلية الحقوق والعلوم السياسية – جامعة العربي بن مهيدي أم البواقي 2016م – 2017م، ص 8، 9.

المطلب الثاني

تقسيم الجرائم الالكترونية

وتقسم الجرائم الإلكترونية من ناحية الاعتداء على النظام المعلوماتي، أو من ناحية القصد الجنائي للمجرم المعلوماتي لذا سنقوم بتقسيم هذا المطلب إلى:

الفرع الأول: تقسم الجرائم الالكترونية من ناحية الاعتداء على النظام المعلوماتي.

الفرع الثاني: تقسيم الجرائم الالكترونية من ناحية الدافع أو الباعث.

الفرع الأول

تقسيم الجرائم الالكترونية من ناحية الاعتداء على النظام المعلوماتي

- تقسم الجرائم الالكترونية من ناحية الاعتداء على النظام المعلوماتي إلى الآتي:
- 1- جريمة الدخول والبقاء غير المشروع في نظام المعلوماتية (جرائم الاختراق): وهي القدرة على الوصول لهدف معين عن طريق ثغرات في نظام الحماية الخاصة بالهدف، وهي سمة سيئة يتسم بها المخترق، لقدرته على دخول أنظمة الآخرين دون رغبة منهم ودون علمهم بغض النظر على الأضرار التي قد تحدثها، وتعد هذه الجريمة الأكثر انتشاراً⁽¹⁾.
 - 2- جريمة إتلاف وتعديل المعطيات: قد يعقب جريمة الدخول والبقاء غير المشروع، أفعال أخرى غير مشروعة تتمثل في جريمة إتلاف وتعديل المعطيات، حيث شملت

(1) أنظر: خالد عياد الحلبي، إجراءات التحري والتحقيق في جريمة الحاسوب والانترنت، ط: الأولى، دار الثقافة للنشر والتوزيع، عمان - الأردن، 2011م، ص 51 .

الحماية الجنائية التي تدخل في نظام المعالجة الآلية من كل إدخال أو تعديل أو إزالة بطريق الغش(2).

ويمكن القول إن مرتكبي جريمة الاحتيال الإلكتروني هم أشخاص لديهم السلطة في التعامل مع المعلومات التي يحتويها نظام الحاسب الآلي، سواء كان في مرحلة إدخال البيانات أو إخراجها والتعامل التعامل معها بعد تخزينها، ويستطيعون تحليل التلاعب ف هذه البيانات إلى ربح مادي غير مشروع وحتى أنه قد أطبق على الاحتيال الإلكتروني بأنه جريمة داخلية وإشارة إلى حدوثه داخل المؤسسة المجني عليها بواسطة المنتسبين اليها(1).

3- جرائم الاحتيال الالكتروني: وهي " كل فعل أو مجموعة من الأفعال غير المشروعة والمعتمدة التي ترتكب بهدف الخداع أو التحريف للحصول على شيء ذي قيمة ويكون نظام الحاسوب لازماً لارتكابها أو إخفائها" (2).

4- جرائم الاعتداء على بطائق الائتمان: تستخدم بطائق الائتمان من قبل حاملها كوسيلة وفاء للالتزاماتها بدل من الدفع الفوري بالنقد، وذلك وفقاً لشروط البنك مصدر البطاقة، وتختلف أنواع هذه البطاقات ونطاق استخدامها، فمنها ما هو محلي لا يتجاوز حدود الدولة التي صدر فيها ومنها ما يستخدم في كل دول العالم(3).

وجريمة إساءة استخدام بطاقة الائتمان قد ترتكب من طرف الغير، ويكون ذلك في حالة سرقة بيانات بطاقة الائتمان، أو في حالة استخدام بطاقة الائتمان مزورة، وقد ترتكب من قبل حاملها الشرعي لدفع ثمن السلع والخدمات من خلال شبكة الانترنت رغم علمه بعدم كفاية رصيده في البنك مصدر البطاقة، أو بعد انتهاء مدة صلاحيتها أو الغائها(4)، واستخدام بطاقة الائتمان بعد انتهاء صلاحيتها وعدم اعادتها إلى مصدرها تعد جريمة خيانة أمانة(5).

5- جريمة القذف والتشهير عبر الانترنت: تعتبر هذه الجريمة من أكثر الجرائم شيوعاً عبر شبكة الانترنت، فيعتقد العابثون أن لهم حرية التصرف في نشر وبث وسائل تحمل عبارات ذم وقذح وتحقير لأشخاص مستهدين بذاتهم، أو مجموعات من الأفراد، بصفة غيابية أو وجاهية عبر مختلف الوسائط الإلكترونية(6).

(2) أنظر: آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط: الثانية، دار هومة الجزائر 2007م، ص121.

(1) أنظر: سامر سليمان، جريمة الاحتيال الإلكتروني، رسالة ماجستير مقدمة إلى كلية الحقوق جامعة النهرين، ص 20، 21.

(2) أنظر: عبد الفتاح بيومي حجازي لحماية التجارة الإلكترونية - الكتاب الأول -، نظام التجارة الإلكترونية وحمايتها مدنياً، دار الفكر الجامعي، الإسكندرية 2002، ص108.

(3) نفس المرجع، نفس الصفحة.

(4) كل بطاقة ائتمان لها مدة صلاحية محددة، عادة ما تقدر نسبة يقوم العمل بعد انتهائها بإعادتها إلى البنك.

(5) أنظر: خالد عياد الحلبي، إجراءات التحري والتحقيق في جريمة الحاسوب والانترنت، مرجع سابق، ص125.

(6) أنظر: د/ نهلا عبد القادر المومني، الجرائم المعلوماتية، ص173- 174 .

6- جريمة التعدي على البيانات الشخصية: ومن صور جرائم التعدي على البيانات الشخصية، انتهاك السرية والخصوصية، وإفشاء البيانات بما يضر بصاحبها، وكذلك الاطلاع على المراسلات الإلكترونية، والإدلاء ببيانات كاذبة في إطار العمليات والمعاملات الإلكترونية⁽⁷⁾.

الفرع الثاني

تقسيم الجرائم الالكترونية من ناحية الدافع أو الباعث

يعبر فقهاء الشريعة الإسلامية عن القصد في الجرائم العمدية بلفظ (العمد) تمييزاً له عن الخطاء الذي تقوم به الجرائم غير العمدية.

ويتحقق العمد في الشريعة الإسلامية إذا اتجهت إرادة الشخص إلى تحقيق أثر محرم، بغض النظر عن الباعث الذي وجه، فسواء كان شريفاً أو وضيعاً⁽¹⁾

أما في التشريعات الوضعية فالقاعدة العامة هي أن الباعث لا يعد من عناصر القصد⁽²⁾، إلا أنه استثناء من القاعدة قد يعتد القانون بهذا الباعث ويجعل منه عذراً قانوناً، كحالة الزوج الذي يفاجئ متلبسه بالزنا فيقتلها هي ومن يزني بها (المادة 279 من قانون العقوبات الجزائري).

كما قد يكون للباعث أثره في تشديد العقوبات مثل ارتكاب جريمة قتل للتأهب لاقتراف جنحة أو تسهياً أو مساعدة لمرتكبيها أو شركاتهم على الهرب أو التخلص من العقوبة (المادة 263 من قانون العقوبات الجزائري). كذلك يمكن للقاضي أن يراعي عند تقدير العقوبة بين حديها الأدنى والأعلى نوع الباعث وما إذا كان شريفاً أو دنياً.

(7) أنظر: استاذنا الدكتور/ علي حسن الشرفي، النظرية العامة للجريمة - شرح قانون العقوبات اليمني (القسم العام - الجزء الأول)، مكتبة الوسيلة للنشر والتوزيع، صنعاء 2014، ص 260.

(1) المقصود بالقصد الجنائي النية، وعرف القرافي النية بأنها "قصد الانسان بقلبه ما يرد فعله" (أنظر: أبو العباس أحمد بن إدريس القرافي، الذخيرة - المجلد الأول -، الطبعة الأولى، دار الكتب العلمية، بيروت 1974م ص 234).

(2) أنظر: محمد أحمد لريد، نظرية ظروف الجريمة في الفقه الجنائي الإسلامي وقانون العقوبات الجزائري، رسالة دكتوراه مقدمه إلى كلية العلوم الإنسانية - جامعة وهران، الجزائر 2008م - 2009م، ص 107.

وبالنسبة للجرائم الالكترونية، فأخطر تلك الجرائم التي تكون لأغراض سياسية، كالإرهاب الإلكتروني، أو ما يعرف الإرهاب السيبراني.

ويعرف الإرهاب السيبراني : بأنه نشاط أو هجوم متعمد ذو دوافع سياسية بغرض التأثير على القرارات الحكومية أو الرأي العام باستخدام الفضاء الإلكتروني كعامل مساعد ووسيط في عملية التنفيذ للعمل الإرهابي أو الحربي من خلال هجمات مباشرة بالقوة المسلحة على مقدرات البنية التحتية للمعلومات ، أو من خلال ما يُعدُّ تأثيراً معنوياً ونفسياً، من خلال التحريض على بث الكراهية الدينية وحرب الأفكار، أو أن يتم في صورة رقمية من خلال استخدام آليات الأسلحة الإلكترونية الجديدة في معارك تدور رحاها في الفضاء الإلكتروني ، والتي قد يقتصر تأثيرها على بعدها الرقمي أو قد تتعدى لإصابة أهداف مادية تتعلق بالبنية التحتية الحيوية".

فالإرهاب السيبراني (الإلكتروني) يعتمد على استخدام الإمكانيات العلمية والتقنية ، واستغلال وسائل الاتصال والشبكات المعلوماتية ، من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم أو تهديدهم.

ونظراً لخطورته على الأمن والسلم الدوليين حذر مجلس الأمن التابع للأمم المتحدة، الخميس 15 ديسمبر 2022م، من أن تهديد الإرهاب قد ازداد وأصبح أكثر انتشاراً في مناطق مختلفة من العالم بمساعدة التكنولوجيا الجديدة.

وتم اعتماد البيان الرئاسي، الذي وافق عليه جميع أعضاء المجلس الخمسة عشر، في نهاية اجتماع مفتوح حول مكافحة الإرهاب برئاسة وزير الشؤون الخارجية الهندي سوبرامانيام جايشانكار، الذي وصف الإرهاب بأنه «تهديد وجودي للسلم والأمن الدوليين».

وأعرب مجلس الأمن في البيان الرئاسي، الذي يعد خطوة أقل من قرار، عن قلقه البالغ من قيام الإرهابيين بجمع الأموال وتحويلها بطرق عدة، بما في ذلك استغلال الأعمال التجارية المشروعة والمنظمات غير الهادفة للربح، والاختطاف من أجل الحصول على فدية، والاتجار في البشر والمواد الثقافية والمخدرات والأسلحة.

وأشار البيان إلى ضرورة «تعزيز التعاون في مواجهة استخدام التكنولوجيا الجديدة والناشئة لأغراض إرهابية»، مشيراً إلى زيادة استخدام الإنترنت ووسائل التواصل الاجتماعي وأصول الإنترنت والأدوات المالية الجديدة وتزايد إساءة استخدام الطائرات المسييرة في الهجمات الإرهابية»⁽¹⁾.

(1) لمزيد من المعرفة حول الإرهاب السيبراني، راجع مؤلفنا، أثر الإرهاب السيبراني على الأمن القومي، شبكة أجهزة إنفاذ القانون بشأن مكافحة الجرائم الجرمية الإلكترونية، مكتب النائب العام عدن.

الأسباب الدافعة إلى ارتكاب الجريمة الإلكترونية:

- من أهم الأسباب الدافعة إلى ارتكاب الجريمة الإلكترونية تكمن في الآتي:
- 1- الدوافع الذاتية: والتي تكون من الشخص الذي يقوم بارتكاب عدد من المخالفات نابعة من حب الاستطلاع والتحدي والرغبة في قهر النظام المعلوماتي واثبات الذات.
 - 2- الدوافع النفسية: وتكون من شخص لديه خلل نفسي أو أمراض نفسية تنعكس على السلوك.
 - 3- الدوافع الاجتماعية: وتتمثل في الاختراقات للأجهزة الشخصية والتعرف على نقاط الضعف لدى الآخرين.
 - 4- الدوافع المالية (الربح وكسب المال): وذلك بالرغبة في تحقيق مكاسب مادية تكون هائلة أحياناً بزمناً قياسي قد يكون من أكثر البواعث التي تؤدي إلى اقدام مجرمي المعلومات على اقتراف جرائمهم من أجل تحقيق المكاسب المالية.
 - 5- الدافع السياسي والعسكري: التطور العلمي والتقني أدّى إلى الاعتماد بشكل شبة كامل على أنظمة الحاسوب، وبذلك أصبح الاختراق من أجل الحصول على معلومات سياسية وعسكرية واقتصادية مسألة أكثر أهمية.
 - 6- الدافع القومي والوطني: وهو أن يقو الهاكرز بالهجوم على مواقع معادية تختلف مع قيم وعادات مجتمع ما بتدمير أو تغيير هذه المواقع؛ مما يؤدي إلى منعها من تهديد فكر وسلوك أفراد ذلك المجتمع⁽¹⁾

(1) أنظر: مولاي امحمد، صعوبات تطبيق الإدارة الإلكترونية بالجزائر، الجريمة الإلكترونية نموذجاً، المؤتمر العالمي الأول للإدارة الإلكترونية، مركز المدنية للوسائط المتعددة، طرابلس 2010م.

نقلاً عن: د/ عبد السلام محمد المايل، د/ عادل محمد الشريجي، د/ علي قابوسة، الجريمة الإلكترونية في الفضاء الإلكتروني، بحث منشور في مجلة أفاق للبحوث والدراسات سداسية، المركز الجامعي ايليزي – طرابلس، العدد (4) يونيو 2019م، ص 248 ، 249.

المبحث الثاني

ماهية الدليل الإلكتروني

الإثبات الجنائي في الجرائم الإلكترونية، تركز على الدليل الإلكتروني باعتباره الوسيلة الوحيدة والرئيسية لإثبات الجريمة، لذلك يمكننا معرفة ماهية الدليل الإلكتروني من خلال تقسيم هذا المبحث إلى الآتي:

المطلب الأول: تعريف الدليل الإلكتروني.

المطلب الثاني: خصائص الدليل الإلكتروني.

المطلب الثالث: أنواع الأدلة الإلكترونية.

المطلب الأول

تعريف الدليل الإلكتروني

1- الدليل في اللغة.

يقصد بالدليل في اللغة البرهان وما يستدل به⁽¹⁾.

كما يقصد بالدليل المرشد وما يتم به الارشاد⁽²⁾.

2- الدليل اصطلاحاً.

أما الدليل اصطلاحاً فهو الذي يلزم به علم بشيء آخر، وغايته أن يتوصل العقل إلى التصديق اليقيني بما كان يشك في صحته، أي التواصل إلى معرفة الحقيقة، وأيضاً يقصد بالدليل ما يمكن التواصل إلى معرفة الحقيقة⁽³⁾

3 - الدليل في القانون.

الدليل في الاصطلاح القانوني هو ما يلزم من العلم به العلم بشيء آخر. فإذا أعلم المدعي القاضي بحجته على دعواه لزم من علم القاضي بتلك الحجة مع اقتناعه بها علمه بصدق دعوى المدعي فيما أدعاه⁽⁴⁾.

(1) انظر: راتب أحمد قبيعة، القاموس العربي الوسيط، ط: الأولى، دار الراتب، بيروت 1670م ، ص310 .
(2) انظر: جميل صليبا، المعجم الفلسفي، ط: الأولى، دار الكتاب اللبناني، بيروت 1970م، ص23.
(3) انظر: محمد بن أبي بكر عبد القادر الرازي، مختار الصحاح، المطبعة الاميرية، القاهرة 2016م، ص564 ، 565.
(4) انظر: أحمد ابراهيم، طرق الاثبات الشرعية، مطبعة القاهرة الحديثة للطباعة، القاهرة، مصر، ص35.

وهناك من عرفه " هو ما يمكن التوصل به إلى معرفة الحقيقة" (5).

كما عرفه بعض فقهاء القانون " هو ما يثبت به الحق، أو هو الوسائل التي يستنتج منها القاضي صحة الدعوى" (6).

فالأثبات بمعناه القانوني هو إقامة الدليل امام القضاء بالطرق التي حددها القانون على وجود واقعة قانونية ترتبت آثارها (7).

فالدليل القانوني هو كل عمل يجري في الخصومة، أو يهدف إلى إعدادها أو له قيمة في الخصومة – أي كانت طبيعته أو معناه – نظمه القانون بقصد الوصول إلى تطبيق القانون الموضوعي فيها (1).

4- تعريف الدليل الالكتروني.

عرّف المشرع السوري في المادة الأولى من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية الدليل الرقمي بأنه: "البيانات الرقمية المخزنة في الأجهزة الحاسوبية أو المنظومات المعلوماتية، أو المنقولة بواسطتها، والتي يمكن استخدامها في إثبات جريمة معلوماتية أو نفيها".

في المقابل نجد أن العديد من القوانين الجزائية الخاصة بمكافحة الجرائم المعلوماتية أو الالكترونية، وإن لم تشر صراحة إلى الدليل الرقمي، إلا أنها عرّفت البيانات الإلكترونية أو البرامج المعلوماتية، منها القانون رقم (2) لسنة (2006م) بشأن مكافحة جرائم تقنية المعلومات الاتحادي بدولة الإمارات، الذي عرّف في المادة الأولى منه البرامج المعلوماتية بأنه: مجموعة من البيانات والتعليمات والأوامر، قابلة للتنفيذ بوسائل تقنية المعلومات ومعدة لإنجاز مهمة ما، وقانون مكافحة جرائم تقنية المعلومات العماني، والذي عرّف في الفقرة (د) من المادة الأولى البيانات الإلكترونية بأنها: كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات أياً كان شكله كالكتابة والصور والأصوات والرموز والاشارات"، وجاء في المادة الأولى من القرار بقانون رقم (16) لسنة (2017م) بشأن الجرائم الإلكترونية الفلسطيني أن البيانات الإلكترونية هي: كل ما يمكن تخزينه أو معالجته أو إنشاؤه أو نقله باستخدام تكنولوجيا المعلومات بوجه خاص الكتابة، أو الصور، أو الصوت أو الأرقام أو

(5) أنظر: أحمد أبو القاسم، الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص، الجزء الأول، دار النشر بالمركز العربي للدراسات الأمنية والتدريب، الرياض 1993م، ص 178.

(6) أنظر: احمد فتحي زغلول، شرح القانون المدني، المطبعة الاميرية، مصر، 1913، ص 385.

(7) أنظر: د/ عبد الرزاق السنهوري، الوسيط في نظرية الالتزام بوجه عام، دار احياء التراث العربي، بيروت 2007م، ص 52.

(4) أنظر: أحمد ضياء الدين، مشروعية الدليل في المواد الجنائية، رسالة دكتوراه قُدمت إلى كلية الحقوق جامعة عين شمس، القاهرة 1984م، ص 473.

الحروف، أو الرموز، أو الإشارات ، وغيرها"، أما المستند الإلكتروني فهو " السجل الإلكتروني الذي يصدر باستخدام إحدى وسائل تكنولوجيا المعلومات، يتم إنشاؤه أو تخزينها أو استخراجها أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة تكنولوجيا المعلومات عل وسيط مادي أو على أي وسيط إلكتروني آخر، ويكون، قابلاً للاسترجاع بشكل يمكن فهمه"(2).

وهناك تعريفات كثيرة للدليل الإلكتروني، فهناك من عرفه من منظور فني وهناك من عرفه منظور قانوني، وهناك من جمع بين القانوني والفني، ونحن بدورنا نميل إلى التعريف الآتي: أنه " الدليل الذي تم الحصول عليه بواسطة التقنية الفنية الالكترونية من معطيات الحاسوب وشبكة الانترنت، الأجهزة المتصل به وشبكات الاتصالات، من خلال إجراءات قانونية لتقديمها للقضاء كدليل الكتروني جنائي يصلح لإثبات الجريمة(1) .

أما البيئة الالكترونية فقد عرفت بأنها " المعلومات والبيانات ذات القيمة في التحقيقات الجارية والمخزونة، أو المنقولة، أو المعالجات بواسطة الأجهزة الإلكترونية"(2).

(2) أنظر: أحمد محمد العمر، الدليل الرقمي وحجبه في الإثبات الجزائي، مجلة المعهد العالي للقضاء، العدد الثالث، يناير 2020م، ص 133 ، 134.

(1) أنظر: خالد عباد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت ، ط : الأولى ، دار الثقافة للنشر والتوزيع ، عمان – الأردن 2011م ، ص 230 .

(2) أنظر : أحمد عبيد المجيد الحاج ، جرائم النشر الصحفي الإلكتروني وأحكام المسؤولية الجنائية (دراسة مقارنة) ، وزارة الاعلام الإماراتية العربية 2007م ، ص 44 .

المطلب الثاني

خصائص الدليل الإلكتروني

يتميز الدليل الإلكتروني عن الدليل التقليدي بعدة خصائص أبرزها:

1- الدليل الإلكتروني دليل علمي.

إن الطبيعة الخاصة للدليل الإلكتروني والوسط الذي يتواجد في بيئة افتراضية غير ملموسة، تجعل من الدليل غير مادي كذلك، فهو دليل غير ملموس يتكون من بيانات ومعلومات على هيئة الإلكترونيات، حيث إن العالم الافتراضي التقني هو عالم أعده متخصصون في التقنية، وبالتالي لا يمكن الحصول على البيانات والمعلومات في ذلك العالم التقني إلا بأساليب عملية وتقنية كذلك، وهو ما يميز الدليل الإلكتروني بهذه الخاصة بأنه دليل علمي⁽¹⁾

فاستخراج الدليل الإلكتروني يحتاج إلى بيئة مشابهة للبيئة التي نتج عنها، لذا يتطلب الاستعانة بأجهزة وأدوات التقنية واستخراج برامج حاسوبية ملائمة للاطلاع عليه أو استخراج برامج حاسوبية ملائمة، للاطلاع عليه واستخراجه في هيئة ملموسة أو مادية، وهي تعد أساليب علمية⁽²⁾.

2- الدليل الإلكتروني دليل تقني.

(1) أنظر: عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة، الإسكندرية، ص 61 – 62 .

نقلاً عن: د/ مسعود بن حميد المعمري، الدليل الإلكتروني لإثبات الجريمة الإلكترونية، مجلة القانون الكويتية، العدد (6)، 2018م، ص 197 – 198.

(2) أنظر: د/ مسعود بن حميد المعمري، الدليل الإلكتروني لإثبات الجريمة الإلكترونية، مرجع سابق، 198.

يتطلب في استخلاص الدليل الإلكتروني وتحليله طرقاً غير تقليدية، بحيث يتم إجراء تجارب عملية وتقنية على جهاز الحاسب الآلي الذي استخدم في جريمة معينة(3).

لذا يمكن استنتاج أن الدليل الإلكتروني يتميز بأنه دليل تقني، استناداً للمصدر الذي جاء منه وهو البيئة الرقمية أو التقنية، مثلما هو دليل علمي استناداً للبيئة التي يتواجد والتي تم انشاؤها من قبل مختصين فنيين على أساس علمي. إن الدليل الإلكتروني التقني ليس كالأدلة التقليدية الأخرى، فالتقنية لا تنتج أي أدلة مادية ملموسة كالسلاح أو البصمات أو الاعتراف المكتوب الذي تدل على مرتكب أدلة الجريمة، إنما تنتج التقنية نبضات رقمية ذات طبيعة ديناميكية فائقة السرعة تنتقل بين أجزاء وسائل التقنية وشبكات الاتصال متعددة حدود المكان والزمان الواحد(1).

3- الدليل الإلكتروني دليل متنوع ومتطور.

إن مصطلح الدليل الإلكتروني، يشمل جميع البيانات والمعلومات الرقمية التي يمكن تداولها بمختلف أشكالها وأنوعها، سواء كانت هذه الأدلة متعلقة بالحاسب الآلي أو غيرها من الأجهزة أو شبكة الانترنت، أو شبكات الاتصال السلكية واللاسلكية، ومنه فالآثار الرقمية المستخلصة من الحاسب الآلي أو شبكة الانترنت، تكون ثرية جداً ومتنوعة بما تحتويه من معلومات عن وقائع تشكل جريمة ما، وترتقي إلى أن تصبح دليل براءة أو إدانة، ومن بين هذه المعلومات صفحات التواصل والمواقع الإلكترونية المختلفة، البريد الإلكتروني، النصوص والصور والفيديوهات الرقمية، الملفات المخزنة في الكمبيوتر الشخصي والمعلومات المتعلقة بمستخدم شبكة الانترنت وغيرها(2).

4- الدليل الإلكتروني يصعب التخلص منه.

تعتبر هذه الخاصية من أهم الخصائص التي يتميز بها الدليل الإلكتروني عن الأدلة التقليدية الأخرى، حيث إنه يمكن التخلص بسهولة من الأدلة الأخرى كالأوراق والسلاح والأموال المزورة بإتلافها وحرقها لتخفي معالمها، وأيضاً بالنسبة لبصمات الإصبع، حيث يمكن مسحها بسهولة وإخفاؤها من موضعها، أما الدليل الإلكتروني

(3) أنظر: ناصر آل ثنيان، إثبات الجريمة الإلكترونية - دراسة تأصيلية تطبيقية -، (رسالة ماجستير)، جامعة نايف للعلوم الأمنية، كلية الدراسات العليا، الرياض 2012م، ص74.

(4) أنظر: د/عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية، ص 61-62.

نقلاً عن: د/ مسعود بن حميد المعمري، الدليل الإلكتروني لإثبات الجريمة الإلكترونية، مرجع سابق، ص 198.

(2) أنظر: ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر، دار الكتب القانونية، القاهرة 2009م، ص22.

بشكل خاص وكل ما يتعلق بتكنولوجيا المعلومات بشكل عام، فإنه كما حدث ارتباط أو اتصال أو وسيلة تقنية المعلومات وبمعنى إدخال لبيانات معينة، فإنه يصعب التخلص من ذلك ولو استخدمت أدوات الحذف والإلغاء. وكما أن التخلص من الدليل الإلكتروني باستخدام الأدوات المتوفرة في وسيلة التقنية، مثل خيارات الحذف أو الإلغاء أو الإزالة، لا تعتبر من العوائق التي تمنع من استرجاع الدليل، فهناك برامج متخصصة من ذوات طبيعة الدليل التقني تمكن جهات القضائية المختصة من الحصول على الدليل المحذوف واسترجاع البيانات الملغاة من الجهاز محل ارتكاب الجريمة⁽³⁾. إلا إن ذلك لا يمنع من القيام بسرعة الاحتفاظ بالأدلة الجنائية؛ كي لا يتم اتلاف الأدلة الإلكترونية⁽¹⁾.

5- الدليل الإلكتروني قابل للنسخ.

الأصل أنه عند إعداد نسخة من محتوى دليل معين فإن قوته لن تكون مثل قوة الأصل في حجية إثباته، سواء كان في المجال الجنائي أم المدني، كما أن الأدلة التقليدية الأخرى على خلاف الدليل الإلكتروني إذ لا يمكن الحصول على نسخ من تلك الأدلة لتقديمها كدليل بديل عن الأصل، فالمحرر المزور لا بد من مضاهاته مع الأصل عن طريق المستند المزور وليس على نسخه له، إلا أن ذلك يختلف في مجال الدليل الإلكتروني فهو دليل يمكن استخراج نسخ منه مطابق للأصل ويكون لتلك النسخة ذات القيمة العملية للأصل⁽²⁾.

(3) أنظر: د/ مسعود بن حميد المعمرى، الدليل الإلكتروني لإثبات الجريمة الإلكترونية، مرجع سابق، ص 199 – 200.

(1) أنظر: أسامة أحمد المناعسة وآخرون، جرائم الحاسب الآلي، دراسة تحليلية مقارنة، ط: الأولى، دار وائل للنشر، عمان 2001م، ص 290.

(2) أنظر: د/ عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، مرجع سابق، ص 64.

المطلب الثالث

أنواع الأدلة الإلكترونية وشروط قبولها

يجب الحصول على الدليل بصورة مشروعة غير مخالفة لأحكام التشريعات الوطنية والدولية، ويجب اخذ الأدلة بطريقة صحيحة يمنع إتلافها سواء الأدلة الإلكترونية التي تم ضبطها من أجهزة الحاسوب، أو غيرها، ولمزيد من التوضيح حول هذا سنقوم بتقسيم هذا المطلب إلى الآتي:

الفرع الأول: أنواع الأدلة محل الضبط في الجرائم الإلكترونية.

الفرع الثاني: شروط الدليل الإلكتروني المستمد من التفتيش.

الفرع الأول

أنواع الأدلة محل الضبط في الجرائم الإلكترونية

الأشياء التي يتم ضبطها والتحفظ عليها في الجرائم الإلكترونية، والتي لها قيمة في إثبات تلك الجرائم ونسبتها للمتهم هي:

1- ضبط جهاز الكمبيوتر وملحقاته: ذلك أن ضبطه أمر مهم جداً للقول بأن الجريمة الواقعة هي جريمة إلكترونية وأنها مرتبطة بالمكان والشخص الحائز على الجهاز، ولأجهزة الكمبيوتر أنواع مختلفة الأمر الذي يتطلب في ضابط الشرطة القضائية

المعرفة الكافية التي تؤهله للتعامل معه – الجهاز المضبوط - والتعرف على مواصفاته بسرعة.

2 – ضبط المعدات المستعملة في شبكة الأنترنت: كالمودم وهي الوسيلة التي تمكن أجهزة الكمبيوتر من الاتصال ببعضها البعض عبر خطوط الهاتف.

3- وسائط التخزين المتحركة: كالأقراص المدمجة، والأقراص المرنة، والاشربة المغناطسية.

4- ضبط البرمجيات: (Soft Ware): فإذا كان الدليل الإلكتروني ينشأ باستخدام برنامج خاص فإن ضبط الأقراص الخاصة بتنصيب وتنصيب هذا البرنامج أمر جد مهم عند فحص الدليل.

5- ضبط البريد الإلكتروني: والذي يحتوي على برامج متخصصة لكتابة وإرسال واستعراض وتخزين الرسائل الإلكترونية، وهذه الرسائل لا يختلف التعامل معها مع التعامل مع الرسائل الورقية، إذ بمقدور المستخدم أن يطرحها جانباً أو يرد عليها أو ينقلها إلى شخص آخر أو يحتفظ بها في ملف خاص، لذلك فالمحقق الذي يريد ضبط الرسائل الإلكترونية (Boite Email) الخاص به ثم يشغل برامج البريد الإلكتروني في جهاز حاسوبه ثم مراجعة قائمة الرسائل ليلتقط من بينها الرسائل المطلوبة⁽¹⁾

الفرع الثاني

شروط الدليل الإلكتروني المستمد من التفتيش

الدليل المتحصل من تفتيش نظم الأجهزة الإلكترونية لا يكون مشروعاً، ويعتبر باطلاً إذا تم الحصول عليه بغير الشروط الآتية -

-الشرط الأول: يجب الحصول على الدليل بصورة مشروعة غير مخالفة لأحكام الدستور أو القوانين النافذة، فأهم هدف للدستور هو صيانة كرامة الإنسان وحماية حقوقه لذلك تتضمن الدساتير الحديثة نصوصاً تنظم القواعد الأساسية في الاستجواب والتوقيف والحبس والتفتيش وغيرها ، بحيث يتقيد المشرع بها عند وضع قانون

(1) أنظر: سعيداني نعيم آلية البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير قدمت إلى كلية الحقوق والعلوم السياسية – جامعة الحاج لخضر، الجزائر 2013م، ص 160 – 161.

العقوبات، وقانون الإجراءات الجزائية ، فنص الدستور اليمني في المادة (53) على حرية وسرية المواصلات البريدية والهاتفية والبرقية وكافة وسائل الاتصال مكفولة ولا يجوز مراقبتها أو تفتيشها أو إفشاء سريتها أو تأخيرها أو مصادرتها إلا في الحالات التي يبينها القانون وبأمر قضائي .

فهذه النصوص الواردة في الدستور تفرض على المشرع عند وضع قواعد الإجراءات الجزائية الالتزام بها وعدم الخروج عنها ، وكذلك فإن إجراءات الحصول على الأدلة الجنائية يجب أن تكون ضمن الإطار العام الذي حدده الدستور وإلا فإن الدليل المستمد بطريق مخالف للأحكام الواردة في الدستور يكون باطلاً بطلاناً مطلقاً لتعلقه بالنظام العام ، ويجوز لكل ذي مصلحة التمسك به كما أن للمحكمة أن تقضي به من تلقاء نفسها، ونرى ضرورة أن يقوم المشرع اليمني بتشريع نصوص إجرائية تتكفل بحماية الحياة الخاصة المخزونة في الأجهزة الالكترونية، بحيث تمنع اقتحام الملفات الشخصية بدون سند قانوني ، حماية للحقوق والحريات الفردية التي كفلها الدستور اليمني بالإضافة إلى المواثيق الدولية.

أما جزاء مخالفة القانون في الحصول على الأدلة فيترتب عليه بطلان الدليل الإلكتروني؛ كونه متعلقاً بالنظام العام.

كما نصت المادة (48) دستور الجمهورية اليمنية المعدل لعام 2001م

أ- تكفل الدولة للمواطنين حريتهم الشخصية وتحافظ على كرامتهم وأمنهم ويحدد القانون الحالات التي تقيد فيها حرية المواطن ولا يجوز تقييد حرية أحد إلا بحكم من محكمة مختصة.

ب- لا يجوز القبض على أي شخص أو تفتيشه أو حجزه إلا في حالة التلبس أو بأمر توجبه ضرورة التحقيق وصيانة الأمن يصدره القاضي أو النيابة العامة وفقاً لأحكام القانون، كما لا يجوز مراقبة أي شخص أو التحري عنه إلا وفقاً للقانون.

كما لا يجوز مراقبة أي شخص أو التحري عنه إلا وفقاً للقانون وكل إنسان تقييد حريته بأي قيد يجب أن تصان كرامته ويحظر التعذيب جسدياً أو نفسياً أو معنوياً، ويحظر القسر على الاعتراف أثناء التحقيقات، وللإنسان الذي تقييد حريته الحق في الامتناع عن الإدلاء بأية أقوال إلا بحضور محاميه ويحظر حبس أو حجز أي إنسان في غير الأماكن الخاضعة لقانون تنظيم السجون ويحرم التعذيب والمعاملة غير الإنسانية عند القبض أو أثناء فترة الاحتجاز أو السجن.

ج- كل من يقبض عليه بصفة مؤقتة بسبب الاشتباه في ارتكابه جريمة يجب أن يقدم إلى القضاء خلال أربع وعشرين ساعة من تاريخ القبض عليه على الأكثر وعلى

القاضي أو النيابة العامة تبليغه بأسباب القبض واستجوابه وتمكينه من إبداء دفاعه واعتراضاته ويجب على الفور إصدار أمر مسبب باستمرار القبض أو الإفراج عنه. وفي كل الأحوال لا يجوز للنيابة العامة الاستمرار في الحجز لأكثر من سبعة أيام إلا بأمر قضائي، ويحدد القانون المدة القصوى للحبس الاحتياطي.

د- عند إلقاء القبض على أي شخص لأي سبب يجب أن يخطر فوراً من يخته المقبوض عليه كما يجب ذلك عند صدور كل أمر قضائي باستمرار الحجز، فإذا تعذر على المقبوض عليه الاختيار وجب إبلاغ أقاربه أو من يهه الأمر.

هـ- يحدد القانون عقاب من يخالف أحكام أي فقره من فقرات هذه المادة، كما يحدد التعويض المناسب عن الأضرار التي قد تلحق بالشخص من جراء المخالفة، ويعتبر التعذيب الجسدي أو النفسي عند القبض أو الاحتجاز أو السجن جريمة لا تسقط بالتقادم ويعاقب عليها كل من يمارسها أو يأمر بها أو يشارك فيها.

كما يجب الأخذ بالمواد الآتية من قرار جمهوري بالقانون رقم(13) لسنة 1994م بشأن الإجراءات الجزائية :-

مادة(131): للأشخاص و المساكن و المراسلات البريدية و المحادثات السلوكية و اللسلوكية و المحادثات الشخصية حرمة. وحرمة المسكن تشمل كل مكان مسوراً أو محاطاً بأي حاجز متى كان مستعملاً أو معداً للمأوى أو لحفظ الأشياء و حرمة المراسلات تمنع من الاطلاع عليها أثناء نقلها أو انتقالها من شخص إلى آخر بريدية كانت أم هاتفية.

مادة(132): لا يجوز تفتيش الأشخاص أو دخول المساكن أو الاطلاع على المراسلات البريدية أو تسجيل المحادثات السلوكية أو اللسلوكية أو الشخصية و كذا ضبط الأشياء إلا بأمر من النيابة العامة أثناء التحقيق و من القاضي أثناء المحاكمة.

مادة(133): تفتيش الشخص يكون بالبحث عما يكون في جسمه أو ملابسه أو أمتعته الموجودة معه.

مادة(134): يحصل التفتيش بحضور المتهم أو من ينيبه و بحضور شاهدين من أقاربه أو جيرانه إذا حصل التفتيش في منزل غير المتهم ، يدعى صاحبة الحضور بنفسه أو بواسطة من ينيبه و بحضور شاهدين من أقاربه أو جيرانه.

كما يعاقب من قام بذلك بناءً على نص المادة(253) من قانون الجرائم والعقوبات اليمني رقم (12) لسنة 1994م (يعاقب بالحبس مدة لا تزيد على سنة أو بالغرامة من دخل مكاناً مسكوناً أو معداً للسكن أو أحد ملحقاته أو أي محل معداً لحفظ المال أو عقاراً خلافاً لإرادة صاحب الشأن وفي غير الأحوال المبينة في القانون وكذلك من بقي فيه خلافاً لإرادة من له الحق في إخراجه .

وتكون العقوبة السجن مدة لا تزيد على خمس سنوات أو الغرامة إذا قعت الجريمة ليلاً أو بواسطة العنف على الأشخاص أو الأشياء أو باستعمال سلاح أو من شخصين فأكثر أو من موظف عام أم ممن ينتحل صفته).

-الشرط الثاني: يجب أن تكون الأدلة الإلكترونية يقينية غير قابلة للشك: يُشترط في الأدلة المستخرجة من الحاسوب والإنترنت أن تكون غير قابلة للشك حتى يمكن الحكم بالإدانة، ذلك أنه لا مجال لدحض قرينة البراءة وافترض عكسها إلا عندما يصل اقتناع القاضي إلى حد الجزم واليقين، وهكذا يستطيع القاضي من خلال ما يعرض عليه من مخرجات إلكترونية ، وما ينطبع في ذهنه من تصورات واحتمالات بالنسبة لها، أن يحدد قوتها الاستدلالية على صدق نسبة الجريمة المعلوماتية إلى شخص معين من عدمه. ويشترط قانون البوليس والإثبات في بريطانيا لسنة 1984م ، حتى تتحقق يقينية الأدلة الإلكترونية أن تكون البيانات دقيقة وناتجة عن الحاسوب بصورة سليمة ، أما في كندا ، فإن الرأي السائد في الفقه هو اعتبار مخرجات الحاسوب من أفضل الأدلة ، لذا فإنها تحقق اليقين المنشود في الأحكام الجنائية⁽¹⁾.

الشرط الثالث: إمكانية مناقشة الأدلة الإلكترونية المستخرجة من الأجهزة الإلكترونية سواء كمبيوتر أو تلفون جوال أو أي جهاز إلكتروني، حتى يتمكن القاضي من عرض الأدلة الإلكترونية على المتهم ومناقشته تفاصيل حول الجريمة المنسوب إليه ويعد هذا الاجراء أصول من أصول العدالة. ويجب على سطات التحقيق عند استجواب المتهم الأخذ بالمواد التالية من القرار جمهوري بالقانون رقم (13) لسنة 1994م بشأن الإجراءات الجزائية اليمني:-

مادة(177): يقصد بالاستجواب علاوة على توجيه التهمة إلى المتهم مواجهته بالدلائل و الأدلة القائمة على نسبة التهمة إليه و مناقشته فيها تفصيلاً.

مادة (180): يسمح للحامي بالإطلاع على التحقيق في اليوم السابق على الاستجواب أو المواجهة ما لم يقرر المحقق غير ذلك.

وفي جميع الأحوال لا يجوز الفصل بين المتهم ومحامية الحاضر معه أثناء التحقيق.

مادة (181): في غير حالة الجرائم المشهوددة وحالة السرعة بسبب الخوف من ضياع الأدلة لا يجوز للمحقق في الجرائم الجسيمة أن يستجوب المتهم أو يواجهه بغيره من

(1) انظر: عبد الإله أحمد الهلالي، حجية المخرجات الكمبيوترية في المواد الجنائية -دراسة مقارنة- ، دار النهضة العربية ، القاهرة 2008م ، ص 129

المتهمين أو الشهود إلا بعد دعوة محامية للحضور إن وجد وعليه أن يخطره أن من حقه ألا يجيب إلا بحضور محامية.

المبحث الثالث

الحلول العملية والقانونية لحل مشاكل الجرائم الإلكترونية

يتطلب في استخلاص الدليل الإلكتروني وتحليله طرقاً غير تقليدية، بحيث يتم إجراء تجارب عملية وتقنية على جهاز الحاسب الآلي الذي استخدم في جريمة معينة، فمضمون الدليل الإلكتروني يعتمد على استخدام أجهزة خاصة بتجميع وتحليل محتواه، ولذلك فكل ما لا يمكن تحديد محتواه بواسطة تلك الأجهزة لا يمكن اعتباره دليلاً إلكترونياً، وذلك لعدم إمكانية الاستدلال به على معلومة معينة، ما يعدل قيمته التدليلية في اثبات الجريمة الإلكترونية ونسبتها إلى الجاني(1).

فمثلاً يجب اخذ الأدلة الإلكترونية بطريقة صحيحة من الأجهزة الإلكترونية التي استخدم منها الجريمة، كذلك يجب الحصول على الدليل بصورة مشروعة غير مخالفة لأحكام التشريعات الوطنية والدولية.

وعليه سوف نقسم هذا المبحث إلى مطلبين على النحو الآتي:

(1) أنظر: الحسين الطيب عبد السلام الأسمر الحصري ، الاثبات الجنائي بالوسائل العلمية الحديثة ، رسالة ماجستير مقدمة إلى جامعة مولانا مالك إبراهيم الإسلامية ، السودان 2016م ، ص 56 ، 60).

المطلب الأول: الحلول العملية لحل مشاكل الجرائم الإلكترونية.
المطلب الثاني: الحلول التشريعية لحل مشاكل الجرائم الإلكترونية.

المطلب الأول

الحلول العلمية لحل مشاكل الجرائم الإلكترونية

هناك عدة معوقات تعوق إثبات الجريمة الإلكترونية كسهولة طمس الدليل الإلكتروني ومحوه كلياً، مما يسبب في عدم الكشف عن المجرم وملاحقته، والدور السلبي للمجني عليه، وعدم إبلاغه عن وقوع هذا الجرائم، فالكثير من الجهات التي تتعرض أنظمتها للانتهاك تعتمد إلى عدم الكشف عنها تجنباً لعدم الاضرار بسمعتها ومكانتها وتكتفي باتخاذ إجراءات إدارية، ونقص الخبرة الفنية والتقنية لدى سلطات الاستدلال والتحقيق والقضاء، يشكل عائقاً أساسياً أمام اثبات الجريمة الإلكترونية (1)، الأمر يتطلب من سلطات مأمور الضبط، وسلطات التحقيقات لإيجاد حلول عملية لتلك المشاكل حتى تتمكن من إثبات الجرائم الإلكترونية.

وعليه سنقوم بتقسيم هذا المطلب إلى فرعين على النحو الآتي:

الفرع الأول: المعوقات العملية التي تعوق إثبات الجرائم الإلكترونية.

الفرع الثاني: الحلول العملية لحل مشاكل الجرائم الإلكترونية.

(1) أنظر: د/ جلال فضل محمد العودي، الدليل الإلكتروني وسلطة القاضي الجنائي في تقديره، مجلة القانون ، العدد(26)، كلية الحقوق – جامعة عدن 2022م ص318.

الفرع الأول

المعوقات العملية التي تعوق إثبات الجرائم الإلكترونية

هناك عدة معوقات تعوق إثبات الجريمة الإلكترونية ابرزها:

- 1- سهولة طمس الدليل الإلكتروني ومحوه كلياً، مما يسبب في عدم الكشف عن المجرم وملاحقته⁽¹⁾.
- 2- الدور السلبي للمجني عليه، وعدم إبلاغه عن وقوع هذا الجرائم، فالكثير من الجهات التي تتعرض أنظمتها للانتهاك تعتمد إلى عدم الكشف عنها تجنباً لعدم الاضرار بسمعتها ومكانتها فتكتفي باتخاذ إجراءات إدارية.
- 3- نقص الخبرة الفنية والتقنية لدى سلطات الاستدلال والتحقيق والقضاء، يشكل عائقاً أساسياً أمام اثبات الجريمة الإلكترونية⁽²⁾.
- 4- ضعف التعاون الدولي في مكافحة الجرائم الإلكترونية، وعلى الرغم من أن هناك مناداة بضرورة التعاون الدولي في مكافحة الجرائم الإلكترونية إلا أن هناك عوائق تحول دون ذلك ذاك وتجعل هذا التعاون صعباً وأهما:

أ- وعدم وجود نموذج موحد للنشاط الإجرامي: فلأنظمة القانونية القائمة في الكثير من الدول لمواجهة الجرائم المعلوماتية لا يوجد فيها اتفاق عام مشترك حول نماذج إساءة استخدام نظم المعلومات وشبكة الانترنت الواجب تجريمها، فيما

(1) في الأونة الأخيرة وُجدت برامج متخصصة من ذوات طبيعة الدليل التقني تمكن جهات القضائية المختصة من الحصول على الدليل المحذوف واسترجاع البيانات المُلغاة من الجهاز محل ارتكاب الجريمة لمزيد من التفصيل راجع خصائص الدليل الإلكتروني في المبحث الثاني.

(2) أنظر: شهر زاد حداد، الدليل الإلكتروني في مجال الاثبات الجنائي، مرجع سابق، ص9.

- يكون مباحاً في بعض الأنظمة يكون محرماً في أنظمة أخرى، ويرجع ذلك إلى عدة عوامل كاختلاف العادات والتقاليد والثقافات من مجتمع لآخر.
- ب- بسبب تنوع واختلاف النظم القانونية الإجرائية نجد أن طرق التحري والتحقيق والمحاكمة التي تثبت فائدتها وفعاليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى.
- ت- عدم وجود معاهدات ثنائية أو جماعية بين الدول، وحتى في حالة وجودها فإنها تكون قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم وبرامج الحاسب وشبكة الانترنت.
- ث- مشكلة الاختصاص في جرائم الإنترنت: وتثار هذه المشكلة بالنسبة للاختصاص على المستوى الدولي وذلك لاختلاف التشريعات والنظم القانونية من دولة لأخرى حيث ينجم عنها تنازع بين هذه الدول بالنسبة للجرائم المتعلقة بالإنترنت التي تتميز بكونها عابرة للحدود، فيحدث أن ترتكب داخل إقليم دولة معينة إلا أنها تمتد إلى خارج إقليم دولة أخرى مما يعني خضوعها لأكثر من قانون جنائي.
- ج- عدم وجود قنوات اتصال: أن من أهم الأهداف المرجوة من التعاون الدولي في مجال الجريمة والمجرمين الحصول على المعلومات والبيانات المتعلقة بهم ولتحقيق هذه الهدف كان لازماً أن يكون هناك نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أمنية لجمع الأدلة والمعلومات العلمية التي غالباً ما تكون مفيدة في التحري لجرائم معينة ولمجرمين معينين وبالتالي تنعدم الفائدة من هذا التعاون(1).

الفرع الثاني

الحلول العملية لحل مشاكل الجرائم الإلكترونية

يطرح بعض الفقه حلولاً عملية لمواجهة تحديات ومشكلات الجرائم الإلكترونية وتتمثل في الآتي:

1- لا بد من اتخاذ وسائل الحيطة والحذر في تعامل البنوك مع الأنشطة المصرفية التي يتم عبر الانترنت نظراً لأن تركيز غاسلي الأموال يتم على هذا البنوك، وبهذه

(1) أنظر: جاسم خربيط خلف، الدليل الإلكتروني في الجريمة المعلوماتية، مجلة القانون للدراسات والبحوث القانونية، جامعة ذقار، ص25، 26.

نقلاً عن: الطيبي البركة، إشكالية الإثبات في الجريمة الإلكترونية، مجلة آفاق علمية، المجلد(11)، العدد (19) لسنة 2019م، ص279

الأساليب باعتبارها مرتعاً خصباً لتجارته خصوصاً إذا كانت الدول التي ترعى هذه البنوك أو التي في ضيافتها تعاني من عجز هذا النظام الرقابي العام للدولة.

2- إنشاء هيئة وطنية للأمن السيبراني⁽²⁾، كما نتمنى من رئيس مجلس القيادة الرئاسي الدكتور/ رشاد العليمي أن يصدر قراراً جمهورياً بإنشاء هيئة وطنية للأمن السيبراني، للتصدي العديد من الجرائم الإلكترونية، وخاصة جريمة الاحتراق الإلكتروني والتي قد تستهدف أبرز مؤسسات الدولة.

3- ضرورة قيام المصارف بتدابير عملية من شأنها تكشف محاولات غسل الأموال فيها، ومراقبة جميع التعامل الإلكترونية.

4- ضرورة قيام المصارف بإنشاء أجهزة أو إدارات تتولى مراقبة ومتابعة البلاغات التي تصلها عن أي عملية أو نشاط مشبوه، وبالتالي الإبلاغ عنها للجهات المختصة في الدولة خاصة إن كانت تلك العمليات المصرفية تتعلق بأنشطة تتم عبر الأنترنت.

5- ضرورة تدريب العاملين في المباحث الجنائية على تفحص الأدلة الإلكترونية.

6- ضرورة تدريب المحققين على القيام بالكشف عما تحتويه أجهزة الكمبيوتر من برامج مخزنة عند الضرورة مما ييسر عمليات التفتيش التي تتم على كمبيوتر المتهم.

7- ضرورة الاستعانة بخبراء في الكمبيوتر والشبكات أثناء عمليات التقصي والتحقيق في الجرائم المعلوماتية والأنترنت⁽¹⁾.

8- عدم مسح الرسائل المرسلة من الجاني، ومن ثم الإبلاغ عن الواقعة؛ وذلك لأن عملية مسح الرسائل يعد محو دليل إدانة «دليل إلكتروني» يعتد به أمام هيئة المحكمة حسب قانون 175 لمكافحة جرائم تقنية المعلومات⁽²⁾.

9- عدم استخدام بعض التطبيقات الخطيرة، أصدر الخبراء الأمنيون تحذيراً لمستخدمي «إنستجرام»، للاحتراس من تطبيقات Top Nine المستنسخة المشبوهة، والجزء الخطير هو أن هذه التطبيقات المستنسخة تطلب اسم المستخدم وكلمة مرور «إنستجرام» الخاصين بالمستخدم، على ما يبدو لإنشاء مجموعة من الصور التي

(2) المعرفة أهمية إنشاء هيئة وطنية للأمن السيبراني، أنظر: د/ جلال فضل محمد العودي، مقالات في الجرائم السيبرانية، شبكة أجهزة إنفاذ القانون بشأن الجريمة الإلكترونية، مكتب النائب العام، ص 6 وما بعدها.

(1) أنظر: د/ محمد الألفي، المسؤولية الجنائية عن الجرائم الأخلاقية عبر الأنترنت، المكتب المصري الحديث، القاهرة، ص 203، 204.

نقلاً عن: عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية، رسالة ماجستير مقدمة إلى جامعة الشرق الأوسط 2014م، ص 110 ، 111.

(2) أنظر: طلعت الصناديلي، كيف يُقع الجاني ضحيته للجريمة الإلكترونية، صحيفة الاهرم المصرية، الصادرة 2022/12/8م، على الموقع الإلكتروني:

<https://gate.ahram.org.eg/News/3871077.aspx>

حققت أكثر إعجاباً خلال العام، لكن هذا يؤدي في الواقع إلى اختراق حسابات أولئك الأشخاص(3).

كما أن هناك إجراءات ضرورية للحماية من جرائم الاختراقات الإلكترونية منها:

1- عدم الوثوق في أية رسائل الإلكترونية غير اعتيادية مثل تلك التي تطلب تحويل مبالغ مالية أو التي تُبشّر بالفوز بجائز معينة.

2- إنشاء كلمات سر قوية ومعقدة لا يسهل الوصول إليها، وعدم توحيد كلمة السر لأكثر من جهاز أو حساب، بحيث لو أخترق أحد أجهزتك، لا يستطيع الهاكر اختراق بقية أجهزتك الإلكترونية.

3- عدم الاتصال بشبكات الإنترنت المفتوحة في المطارات أو الأماكن العامة بدون وجود برنامج واقٍ ضدها، وكذلك ضرورة تفعيل التطبيقات المضادة للفيروسات، وإجراءات التحديثات الجديدة بشكل مستمر؛ لأنها في الغالب تكون لسدة ثغرة معينة قد يستغلها بعض المخترقين.

4- عدم التعامل مع مواقع غير مُعتمدة خاصة، في مسائل حجوزات الفنادق أو الطيران، وضرورة الاعتماد على المواقع الرسمية. للحجوزات.

5- لا تثق بأحد، حتى لو كان من لأشخاص التي تثق بهم، فعند إرسال معلومات مهمة على البريد الإلكتروني أو على الشبكات الاجتماعية لهذا الشخص لعملية اختراق وبالتالي الوصول لحسابك.

6- تغيير كلمة المرور من حين لآخر؛ كي تساعدك على إبقاء حسابك بحالة أمنية مستمرة دائماً.

7- عدم مشاركة البيانات البنكية مع أي شخص آخر، والتواصل مع البنك في حال حدوث أي تعامل على الحساب بدون علم صاحب الحساب.

8- قم بمسح بياناتك من على الأجهزة القديمة التي ستتخلص منها.

9- أحرص على استخدام خيار شبكة الضيوف، يرغب الأصدقاء والعائلة دائماً في استخدام شبكة الواي فاي Wi-Fi الخاصة بك عند زيارتك بدلاً من استخدام الشبكة الخاصة بك التي ترتبط بها جميع أجهزتك، يمكنك تخصيص شبكة خاصة لهم في جهاز التوجيه، والتي تعرف باسم الضيوف، تتيح لك هذه الميزة مشاركة اتصالك بالإنترنت مع ضيوفك في حين إبقائهم خارج شبكتك الأساسية، مما يمنعهم من رؤية

(3) لمزيد من التفصيل حول هذا الموضوع: راجع صحيفة الاتحاد الإماراتية الاثنين 12 ديسمبر 2022م على الموقع الإلكتروني: <https://alittihad.ae/news/%D8%AF%D9%86%D9%8A%D8%A7/4337393>

الملفات والخدمات المشتركة لذلك قم بإعداد شبكة الضيوف الخاصة بك باستخدام أسم شبكة مختلفة وكلمة المرور مختلفة وقوية.

10- حفظ إضافي للبيانات back up ؛ حتى يكون هناك نسخة إضافية لجميع الملفات الموجودة في الهاتف الذكي في حال التعرض لهجوم الإلكتروني، حتى لا يتعرض صاحب الجهاز للابتزاز من قبل المخترق لاستعادة البيانات(1).

نأمل أن نرى في المستقبل القريب إنشاء أكاديمية للأمن السيبراني تتبع الجامعة العربية، تختص في تدريب وتأهيل مأموري الضبط القضائي وأعضاء السلطة القضائية المختصين في مكافحة الجرائم الإلكترونية، كما يكون من ضمن مهام الأكاديمية عقد الندوات وورش العمل بين المختصين في تلك الجرائم في جميع أقطار الوطن العربي.

المطلب الثاني

الحلول التشريعية لحل مشاكل الجرائم الإلكترونية

كشفت الجريمة الإلكترونية عالماً جديداً لا يعترف بالحدود الجغرافية والسياسية للدول ولا بسيادتها، حيث فقدت الحدود الجغرافية كل أثر لها في بيئة إلكترونية متشعبة العلاقات، الأمر الذي خلق صعوبات وإشكالات قانونية لا تقتصر على ضبط هذه الجرائم وإثباتها فحسب، وإنما أثارت أيضاً تحديات أكثر تعقيداً مرتبطة بتحديد جهة الاختصاص وبالتبعية القانون الواجب التطبيق على هذا الصنف من الجرائم(1).

الأمر الذي يتطلب من المجتمع الدولي أن يتصدى لتلك الجرائم العابرة للحدود، عن طريق سن تشريعات وقوانين عقابية وإجرائية تتناسب مع خطورة هذه الجرائم ووضع المزيد من الضوابط اللازمة لمواجهتها والتصدي لها، وخلق آليات قانونية للحماية من أخطارها.

وعلى ضوء ذلك أصدرت العديد من الدول تشريعات للتصدي للجرائم الإلكترونية ولم تكف بذلك بل أبرمت الاتفاقيات الدولية حتى تتصدى لتلك الجرائم العابرة للحدود.

وعليه سوف نقسم هذا المطلب إلى الآتي:

الفرع الأول: الاتفاقية الدولية لمكافحة الجرائم الإلكترونية.

الفرع الثاني: التشريعات الوطنية في مكافحة الجرائم الإلكترونية.

(1) أنظر: د/ جلال فضل محمد العودي، مقالات في الجرائم السيبرانية، مرجع سابق، ص 43، 44.
(1) راجع خصائص الجريمة الإلكترونية الذي تناولنها في المبحث الأول من هذا البحث.

الفرع الأول

الاتفاقية الدولية لمكافحة الجرائم الإلكترونية

أبرمت العديد من الاتفاقيات الدولية لمكافحة الجرائم الإلكترونية ومن ضمن تلك الاتفاقيات:

1- في إطار التصدي أكثر لمكافحة الجريمة المعلوماتية عقد المجلس الأوروبي، في مؤتمراً لوزراء الدول الأعضاء لبحث مشكلة صياغة اتفاقية لمكافحة الجريمة المعلوماتية عُرفت باتفاقية بودابست في 23 نوفمبر 2001م، لقد تضمنت الاتفاقية أقساماً ثلاثة القسم الأول: تناولت مجموعة الجرائم التي تتعرض لها شبكة الإنترنت والحاسب الآلي، والقسم الثاني تناول الإجراءات الجنائية التي تتخذ في مواجهة هذه الجرائم، وتناول القسم الثالث التعاون الدولي في مكافحة هذه الجرائم بين الدول الأعضاء(1)

تجدر الإشارة أن المادة (16) من اتفاقية بودابست تنص على ضرورة كل طرف السماح لسلطاته المختصة أن تأمر مزود الخدمة التحفظ العاجل على البيانات المعلوماتية المخزنة بواسطة نظام معلوماتي وذلك عندما تكون هناك أسباب كافية عن تعرض هذه البيانات المعلوماتية المخزنة بواسطة نظام معلوماتي وذلك عندما تكون هناك أسباب كافية عن تعرض هذه البيانات للفقْد أو التغير، وهذا خلال 90 يوم كحد أقصى، وهذه المدة قابلة للتجديد(2).

2- أعتد مجلس وزراء العدل العرب في دورته التاسعة عشر القرار رقم 495 – د – 19 – 2003/10/8م، بشأن مشروع قانون استرشادي لمكافحة جريمة تقنية أنظمة المعلومات وما في حكمها، يتكون من 27 مادة وضع من خلالها القواعد الأساسية التي يتعين على التشريعات العربية الاستعانة له عند وضع قانون لمكافحة الجرائم الإلكترونية، كما تسعى الدول العربية إلى إنشاء منظمة عربية تهتم بالتنسيق في مجال مكافحة الجرائم الإلكترونية والتشجيع على قيام اتحاد عربية تهتم بالتصدي لتلك الجرائم، وتفعيل دور المنظمات والإدارات والحكومة العربية في موجهتها عن طريق نظام الأمن الوقائي(3).

(1) أنظر: نورة طرشي، مكافحة الجرائم المعلوماتية، رسالة ماجستير مقدمة إلى كلية الحقوق – جامعة الجزائر 2011م – 2012م، ص 69، 70.

(2) أنظر: عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة 2010م ص 154.

(3) أنظر: عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية (دراسة مقارنة)، رسالة ماجستير مقدمة إلى جامعة الشرق الأوسط 2014م، ص 92.

3- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة في القاهرة بتاريخ 21 ديسمبر 2014م، وتعد هذه الاتفاقية العربية التي أبرمت في مجال الجريمة التقنية بهدف منعها والتحقيق فيها وملاحقة مرتكبيها، مثل الاعتداء على سلامة البيانات، وجريمة إساءة استخدام وسائل تقنية المعلومات، والتزوير والاحتيال والإباحية والاعتداء على حرمة الحياة الخاصة، والجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات مثل نشر أفكار جماعات إرهابية والدعوة لها، وتمويل العمليات الإرهابية ونشر وصناعة المتفجرات، وأيضًا ما يتعلق بالجريمة المنظمة مثل غسيل الأموال والترويج للمخدرات والأعضاء البشرية والأسلحة.

نتمنى من بقية الدول العربية التي وقعت على اتفاقية القاهرة، ولم تصادق على الاتفاقية، سرعة المصادقة على تلك الاتفاقية.

الفرع الثاني

التشريعات الوطنية في مكافحة الجرائم الإلكترونية

أدركت العديد من دول العالم بأن الجرائم الإلكترونية لم يمكن مكافحتها بالتشريعات التقليدية، فأصدرت تشريعات محلية لمكافحة تلك الجرائم الخطيرة، من ضمنها العديد من الدول العربية التي واكبت هذا التطور التقني الحاصل في مجال تكنولوجيا المعلومات وعملت على حلول تشريعية لمكافحة الجرائم الإلكترونية ومن تلك الدول:

1- التشريع التونسي كان له السبق بين الدول العربية في سن القانون رقم 83 لسنة 2000م الخاص بالتجارة الإلكترونية.

2- أصدرت المملكة الأردنية الهاشمية القانون رقم 85 لسنة 2001م بشأن المعاملات الإلكترونية(2)

3- أصدرت سلطنة عمان المرسوم السلطاني رقم 72 لسنة 2001م الصادر بشأن تعديل بعض أحكام قانون الجزاء العماني ليشمل معالجة جرائم الحاسب الآلي (الكمبيوتر).

(2) أنظر نفس المرجع: هامش ص 92، 93.

4- أصدر المشرع المغربي القانون رقم 070003 تاريخ 11 نوفمبر 2003م، بإدخاله بعض فصول التشريع التي تعاقب على الأفعال التي تشكل جرائم تحت عنوان (المس بنظام المعالجة الآلية للمعطيات).

5- أصدرت دولة الإمارات العربية المتحدة عام 2006م القانون رقم (2) لسنة 2006م الخاص بمكافحة جرائم تقنية المعلومات، ثم تلاه إصدار القانون رقم (3) لسنة 2012م الخاص بإنشاء الهيئة الوطنية للأمن الإلكتروني، وفي نفس العام (2012م) أصدر المرسوم الاتحادي رقم (5) رقم (5) لسنة 2012م المتعلقة بمكافحة جرائم تقنية المعلومات.

6- أصدرت المملكة العربية السعودية عام 2007م أول قوانينها في مجال مكافحة التشريعية لجرائم تقنية المعلومات تحت عنوان نظام مكافحة الجرائم المعلوماتية.

7- أصدرت دولة الكويت، مجموعة من التشريعات من بينها: القانون رقم 64 لسنة 1999م في شأن حقوق الملكية الفكرية، والقانون رقم 9 لسنة 2001م بشأن اساءة استعمال أجهزة الاتصالات الهاتفية، وأجهزة التصنت والقوانين المعلة له، القانون رقم 3 لسنة 2006م بشأن المطبوعات والنشر، القانون رقم 61 لسنة 2007م بشأن الإعلام المرئي والمسموع، والقانون رقم 20 لسنة 2014م في شأن المعاملات الإلكترونية، والقانون رقم 37 لسنة 2014م بإنشاء هيئة تنظيم الاتصالات وتقنية المعلومات، وقانون رقم 63 لسنة 2015م بشأن مكافحة جرائم تقنية المعلومات.

8- أصدرت جمهورية مصر العربية حزمة من التشريعات منها: القانون رقم 10 لسنة 2003م الخاص بتأمين ونقل وتبادل المعلومات، والقانون رقم 15 لسنة 2004م بشأن تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات لتأمين معاملات الأفراد عبر شبكة المعلومات الدولية والإنترنت⁽¹⁾

ندعو بقية الدول العربية وفي مقدمتها الجمهورية اليمنية بإصدار قانون مكافحة الجرائم المعلوماتية، فالقواعد التقليدية في التشريعات الجزائية غير كافية لمواجهة الإلكترونية وما تثيره من مشكلات.

(1) أنظر: د/ حاتم أحمد محمد بطيح، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات ص20 وما بعدها.

المبحث الرابع

سلطات القاضي في تقييم الدليل الالكتروني

القاعدة العامة في الأدلة القانونية في الدعوى المدنية، هي التي حددها المشرع وحدد قوة كل منها، أو لا يمكن الإثبات بغيرها، ولا يمكن للقاضي أن يمنح أي دليل منها قوة أكبر مما حدد لها المشرع.

أما في الدعوى الجنائية فإن للقاضي حرية تكون قناعته من أي دليل مطروح في الدعوى، فالأدلة غير محصورة، إلا أنه يرد على ذلك استثناءات معينة على حرية القاضي، حيث يحدد القانون أدلة معينة يجب أن تتوفر في الدعوى من أجل إدانة المتهم فيها، وتكون لهذه التفرقة في حرية القاضي أهمية للأدلة المادية والقولية، أما للأدلة القانونية فإنها تنحسر، ومثال ذلك أشترط المشرع وجوب تواجد أربعة شهود في جريمة الزنا⁽¹⁾.

وإن أعظم ما يقع على عاتق القاضي هو تقدير أدلة الإثبات والاقتناع بها، وذلك حتى لا يدان بريء ولا يفلت مجرم، فالقاضي قبل أن يصدر حكمه يقوم بالبحث عن

(1) أنظر: د/ أحمد يوسف الطحاوي، الأدلة الالكترونية ودرها في الإثبات الجنائي، دراسة مقارنة، دار النهضة العربية، القاهرة 2015م، ص14.

الحقيقة، وهو في سبيل ذلك يقوم بفحص الأدلة الجنائية ويطرحها في الجلسة ليتناولها الخصوم بالفحص سيعاً للوصول إلى الحقيقة التي ترضي ضميره، وتكون اقتناعه الشخصي لتحقيق العدالة، وتختلف سلطة القاضي الجنائي في تقدير أدلة الإثبات من دولة إلى أخرى حسب ما تعتقه كل دولة من أنظمة الإثبات⁽²⁾.

لذا سنقوم بتقسيم هذا المبحث إلى الآتي:

المطلب الأول: مبدأ قناعة القاضي والضوابط التي تحكمه.

المطلب: الثاني: الدور الإيجابي للقاضي الجنائي في تقييم الأدلة الإلكترونية.

المطلب الثالث: صلاحية القاضي في تقدير الأدلة في الاتجاهات المختلفة للدول.

المطلب الأول

مبدأ قناعة القاضي والضوابط التي تحكمه

القاضي الجنائي ليس حر في تقدير أي دليل إلكتروني وخاصة التقييم الفني للأدلة الإلكترونية بل فقط تقدير الدليل الإلكتروني المقبول في الدعوى، بمعنى النظر في الأدلة الإلكترونية التي تم الحصول عليها بطريقة مشروعة.

وعليه سنقوم بتقسيم هذا المطلب إلى الآتي:

الفرع الأول: مبدأ قناعة القاضي.

الفرع الثاني: الضوابط التي تحكم اقتناع القاضي الجنائي بالدليل الإلكتروني.

الفرع الأول

مبدأ قناعة القاضي

(2) أنظر: عبد المطلب طاهري، الإثبات الجنائي بالأدلة الرقمية، رسالة ماجستير مقدمة إلى كلية الحقوق والعلوم السياسية – جامعة المسيلة 2014م – 2015م، ص58.

فمبدأ القناعة الوجدانية يخول القاضي الجزائي حرية كاملة وسلطة واسعة في تقدير الأدلة التي تطرح أمامه في الدعوى، بما فيها الأدلة الرقمية، واستخلاص اقتناعه من هذا الدليل أو ذاك، وبأية وسيلة يراها موصلة إلى الحقيقة، شرط أن يصدر القاضي حكمه عن اقتناع يقيني بالأدلة، وبخاصة الأدلة المتحصلة من الحاسب الآلي ومخرجاته الإلكترونية، فسلطة القاضي الجزائي في تقدير الأدلة مقيدة بضرورة أن يؤسس قناعته على أدلة قاطعة وحاسمة؛ لأن الأحكام الجزائية لا تبنى على الشك أو التخمين بل على الجزم اليقيني، والوصول إلى يقينية الدليل الرقمي يتم عن طريق ما يستنتجه القاضي بمختلف وسائل إدراكه من خلال معاينته لهذا الدليل، وما ينطبع في ذهنه من تصورات ذات درجة عالية من التوكيد عن طريق التحليل والاستنتاج والربط بين الوقائع⁽¹⁾.

وإذا كانت سلطة القاضي الجزائي في تقدير الدليل تتسع لتشمل الأدلة العلمية؛ إلا أن تطور العلوم وتشعب فروعها، ومقتضيات المنطق والعقل والعدالة توجب على القاضي، - وهو ذو تكوين قانوني غير قادر على إدراك الحقيقة المتعلقة بأصل الدليل الرقمي - أن يؤسس اقتناعه بالدليل الرقمي على رأي الخبرة الفنية في هذا المجال، فيجعل من هذا الرأي سنداً له في تمتع الدليل الرقمي بقيمة اثباته قد تصل إلى حد اليقين، فتحدد القيمة العلمية للدليل أمر لا يملك القاضي أية سلطة في تقديرها؛ لأنها حقيقة ثابتة، وليس من اختصاصه مناقشة الأمور العلمية البحتة، وإنما من اختصاص ذوي الخبرة في هذا الشأن، وليس للمحكمة الجزائية أن تثبت من تلقاء ذاتها، كما أنها لا تستطيع أن تحل نفسها محل الخبير الفني في المسائل الفنية البحتة، وعليها الاستعانة بخبير تخضع خبرته ورأيه لتقديرها، أما بالنسبة إلى الظروف والملابسات التي وجد فيها الدليل إذا تبين له أن وجوده لا يتناسب منطقياً مع ظروف الواقعة؛ لأن القاضي يتمتع بسلطة تقدير الأدلة والتحقق من سلامة إجراءات الحصول عليها ومشروعيتها⁽¹⁾.

الفرع الثاني

الضوابط التي تحكم اقتناع القاضي الجنائي بالدليل الإلكتروني

(1) أنظر: د/ طارق أحمد ماهر زغلول، شرح قانون الإجراءات الجزائية العمانية - الجزء الثاني -، المحاكمة وطرق طعن في الأحكام، ط: الأولى، دار الكتاب الجامعي، 2016، ص222.

(2) أنظر: أحمد محمد العمر، الدليل الرقمي وحجبه في الإثبات الجزائي، مجلة المعهد العالي للقضاء، العدد الثالث، يناير 2020م، ص163 ، 164.

هناك ضوابط بمثابة صمام أمان إزاء انحراف القاضي عند ممارسته لها، فضوابط تتعلق بالدليل الإلكتروني، وأخرى تتعلق بالقاضي الجنائي لفصلها على النحو الآتي:

1- الضوابط المتعلقة بالدليل الإلكتروني.

فيما يتعلق بالدليل الإلكتروني فهناك ضابطان يتحكمان بقناعة القاضي بالأدلة الإلكترونية هما:

أ- شروط قبول الدليل الإلكتروني:

فالقاضي ليس حر في تقدير أي دليل إلكتروني؛ بل فقط تقدير الدليل الإلكتروني المقبول في الدعوى، بمعنى النظر في الأدلة الإلكترونية التي تم الحصول عليها بطريقة مشروعة، إعمالاً بمبدأ الشرعية الإجرائية، وبالتالي تستبعد في مقابل ذلك من المرافعة سائر الأدلة الإلكترونية غير المقبولة، لأنها لا تدخل ضمن عناصر تقديره⁽²⁾.

ب- شروط وضعية الدليل الإلكتروني:

من القواعد الأساسية في الإجراءات الجزائية أنه لا يجوز للقاضي أن يبني حكمه على أدلة لم تطرح لمناقشة الخصوم في الجلسة، وهو ما يعبر عنه بوضعية الخصوم في الجلسة، وهو ما يعبر عنه بوضعية الدليل، ومقتضى ذلك أن يكون للدليل أصل ثابت في أوراق الدعوى وأن تتاح للخصوم فرصة الاطلاع عليه ومناقشته وكلا الأمرين ينبغي توافرها، ويترتب على ذلك أنه لا يجوز للقاضي الجنائي اقتناعه على دليل قدمه أحد أطراف الدعوى إلا إذا تم عرضه في جلسة المحاكمة وخضع للمناقشة بحيث يكون معلوماً لكافة أطراف الدعوى.

2- الضوابط المتعلقة بالإقناع ذاته:

يتيح مبدأ الإثبات الجنائي حرية كبيرة للقاضي في تقدير عناصر الإثبات بما في ذلك الأدلة الرقمية، وعليه فإن تقدير كفاية أو عدم كفاية الدليل الإلكتروني في إثبات الجريمة الإلكترونية ونسبتها إلى مرتكبها أمر متروك لمحكمة الموضوع المعروض عليها الدليل، ولا تخضع في ذلك لرقابة محكمة النقض التي يقتصر دورها على

(2) أنظر: عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، مصر 2010م، ص 242 - 243.

نقلاً عن: بشرى عواطة، حجية الدليل الإلكتروني في الإثبات الجنائي، رسالة ماجستير مقدمة إلى كلية الحقوق والعلوم السياسية - جامعة 8 مايو 1945، الجزائر 2017م - 2018م، ص 69.

مراقبة المنطق القضائي لمحكمة الموضوع عن طريق رقابتها على صحة تسبيب الحكم⁽¹⁾.

وعليه لبلوغ القاضي درجة الاقتناع التام للفصل في القضية، لا بد له من شرطان هما:

أ- بلوغ الاقتناع القضائي درجة اليقين: تقتضي العدالة أن يصدر القاضي حكمه عن اقتناع يقني بصحة ما ينتهي إليه من وقائع لا مجرد الظن والاحتمال.

ب- توافق الاقتناع مع مقتضيات العقل والمنطق: ومعنى ذلك أن يكون استخلاص محكمة الموضوع لوقائع الدعوى استخلاصاً للمعقول، وأن معيار معقولية الاقتناع بما في ذلك الأدلة الالكترونية، هو أن تكون هذه الأدلة مؤدية إلى مرتبة الحكم عليها من غير تعسف في الاستنتاج ولا تعارض مع مقتضيات العقل والمنطق⁽²⁾.

المطلب الثاني

الدور الإيجابي القاضي الجزائية في تقييم الأدلة الإلكترونية

يؤدي القاضي الجنائي دوراً هاماً جداً في الدعوى الجنائية خاصة فيما يتعلق بالإثبات، ومنح القاضي هذا الدور هو نتيجة اعتناق المشرع لمبدأ حرية الإثبات⁽¹⁾.

لذا سنقوم تقسيم هذا المطلب إلى الآتي:

الفرع الأول: الدور الإيجابي للقاضي الجنائي في توفير الدليل الإلكتروني.

الفرع الثاني: دور القاضي الجنائي في تقييم القيمة العلمية للدليل الإلكتروني.

(1) أنظر: عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، مرجع سابق، ص 606.

(2) أنظر فوزي عمارة، اعتراض المرسلات وتسجيل الأصوات والنقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية - جامعة قسنطينة، الجزائر، العدد (33) يونيو 2010م، ص 78
نقلاً عن: بشرى عواطة، حجية الدليل الإلكتروني في الإثبات الجنائي، ص 70..

(1) أنظر: د/ أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الالكترونية، دار الجامعة الجديدة، الإسكندرية 2009م، ص 198.

الفرع الأول

الدور الإيجابي للقاضي الجنائي في توفير الدليل الإلكتروني

المقصود بالدور الإيجابي للقاضي الجنائي هو عدم التزام القاضي بما يقدمه أطراف الدعوى من أدلة، وإنما له سلطة فيها، ويجب عليه أن يبادر من تلقاء نفسه إلى اتخاذ الإجراءات المناسبة للتحقيق في الدعوى والكشف عن الحقيقة⁽²⁾.

فالقاضي غير ملزم بأن يقتنع بما يقدمه إليه أطراف الدعوى، وإنما عليه أن يبحث بنفسه عن الأدلة اللازمة لتكوين قناعة.

فالقاضي الجنائي من واجبه أن يتحرى عن الحقيقة بجميع الوسائل، سواء نص عليها القانون أم لم ينص، وهذا ما أكدته المادة (212) من القانون رقم (3) لسنة 2001م من قانون الإجراءات الجزائية الجزائري⁽³⁾.

بالإضافة إلى النظام الإجرائي السائد في الدولة هو الذي يحدد دور القاضي الجنائي، فإذا كان النظام المتبنى هو النظام الاتهامي فمن الطبيعي أن يكون دور القاضي الجنائي سلبياً؛ لأن هذا النظام ينظر إلى الدعوى الجزائية على أنها ملك الطرفين أحدهما هو الادعاء الذي يمثله المضرور من الجريمة والآخر هو مرتكب الجريمة، ولا شأن للسلطات العامة بجميع الأدلة وينحصر دور القاضي في فحص الأدلة المقدمة من قبل الأطراف، أما إذا كان النظام التنقيبي هو المهيمن على الإجراءات الجزائية كالقانون الجزائري عندها يكون للقاضي دور إيجابياً، على أساس أن الضرر الذي تحدثه الجريمة ليس ضرر فردياً فحسب، وإنما ضرر يهدد مصلحة المجتمع في أمنه واستقراره وسلامته⁽¹⁾.

ويظهر الدور الإيجابي للقاضي الجنائي في توفير الدليل الإلكتروني، من خلال مهمة البحث عن الأدلة وتقديمها في مرحلة المحاكمة تقع بصفة أساسية على عاتق الادعاء والدفاع كما أن القاضي يحتمل جانباً من هذه المسؤولية.

وفيما يتعلق بالجرائم الإلكترونية فإن القاضي الجنائي يستطيع من أجل الوصول إلى الحقيقة أن يوجه أمراً إلى مزود الخدمة الانترنت التي زارها ووقت الزيارة

(2) أنظر: د/ عادل مختاري، دور القاضي الجزائي في ظل مبدأ الاقتناع القضائي، مجلة المنتدى القانوني، العدد الخامس، مارس 2008م، كلية الحقوق والعلوم السياسية، بجامعة محمد خضير، بسكرة، ص182.

(3) المادة 212: يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعاً لاقتناعه الخاص.

ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضورياً أمامه.

(4) أنظر: عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة 2010م، ص 190، 190.

والصفحات التي أطلع عليها، والملفات التي جلبها والحوارات التي شارك فيها والرسائل الإلكترونية التي أرسلها واستقبلها، وغيرها من المعلومات المتعلقة بكل أفعال المستخدم عندما يتصل بالشبكة.

كما أن القاضي الجنائي يمكنه أن يأمر القائم بتشغيل النظام بتقديم المعلومات اللازمة لاختراق النظام، والولوج إلى داخله كالإفصاح عن كلمات المرور السرية والشفرات الخاصة بتشغيل البرامج المختلفة، أو تكليفه بحل رموز البيانات مشفرة داخل ذاكرة الحاسوب والقاضي الجنائي يملك سلطة الأمر بتفتيش نظم الحاسوب بمكوناته المادية والمعنوية وشبكات الاتصالات متى رأى ضرورة هذا الاجراء⁽²⁾.

الفرع الثاني

دور القاضي الجنائي في تقييم القيمة العلمية للدليل الإلكتروني

يتمتع الدليل الإلكتروني، بصفة عامة، بقيمة اثباتية قد تصل إلى حد اليقين، فتحديد القيمة العلمية للدليل الإلكتروني أمر لا يملك القاضي أية سلطة في تقديرها؛ لأنها حقيقة ثابتة، وليس من اختصاصه مناقشة الأمور العلمية البحتة، وإنما هي من اختصاص ذوي الخبرة في هذا الشأن، وليس للمحكمة الجزائية أن تثبت من تلقاء ذاتها، كما أنها لا تستطيع أن تحل نفسها محل الخبير الفني في المسائل الفنية البحتة، وعليها الاستعانة بخبير تخضع خبرته ورأيه لتقديرها.

أما بالنسبة إلى الظروف والملابسات التي وجد فيها الدليل الإلكتروني، فالقاضي الجزائي يستطيع أن يرفض هذا الدليل إذا تبين أن وجوده لا يتناسب منطقياً مع ظروف الواقعة؛ لأن القاضي يتمتع بسلطة تقدير الأدلة، والتحقيق من سلامة إجراءات الحصول عليها ومشروعيتها.

ويعد الرأي الغالب في الفقه المقارن أن الأدلة المستخرجة من الحاسوب تتمتع باليقين المنشود في الأحكام الجزائية، ومن ثم هي من أحسن وأفضل الأدلة، باعتبارها أحد أقسام الأدلة المادية العلمية، بل أكثر منها حجية في الإثبات؛ لأنها محكمة بقواعد علمية وحسابية قاطعة لا تقبل التأويل⁽¹⁾.

ويمكن وصول القاضي إلى اليقين في هذه الحالة من خلال ما يعرض عليه من مخرجات إلكترونية بمختلف أنواعها وأشكالها، وما ينطبع في ذهنه من تصورات

(2) انظر: شهر زاد حداد، الدليل الإلكتروني في مجال الإثبات الجنائي، مرجع سابق، ص 76 ، 77 .
(1) أنظر: محمد الأمين البشري، التحقيق في الجرائم المستحدثة، أكاديمية نايف العربية للعلوم الأمنية، الرياض 2004م، ص 250.
نقلاً : د/ أحمد محمد العمر، الدليل الرقمي وحجتيه في الإثبات الجزائي، مرجع سابق، ص 165.

واحتمالات بالنسبة إليها، وأن يحدد قواها الاستدلالية على صدق نسبة الجريمة إلى شخص معين من عدمه⁽²⁾.

والمعلومات المخزنة في الحاسوب من أفضل الأدلة المتاحة لإثبات هذه البيانات، ومن ثم تعد من أفضل الأدلة ويتحقق مبدأ اليقين فيها، واستلزام يقينية المخرجات الإلكترونية يعد ضماناً أساسية تحد من احتمال انحراف القاضي بممارسة سلطته في تقدير الأدلة، وتضفي عليها المصادقية واقتربها من الحقيقة، ومن قبولها كأدلة إثبات في المواد الجزائية فلا محل لدحض قرينة البراءة وافترض عكسها، إلا عندما يصل قناعة إلى حد الجزم واليقين، والذي يتم عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من مخرجات الحاسوب سواء أكانت مخرجات إلكترونية أم كانت مجرد عرض لهذه المخرجات على الشاشة الخاصة بالحاسوب.

كما اشترطت بعض التشريعات، كاليوناني والنمساوي والسويسري والنرويجي، في سبيل يقينية الدليل الجزائي أن يكون الدليل الرقمي مقروءاً، سواء أكان مطبوعات على ورق بعد خروجه من الحاسوب أم كان مقروءاً على شاشة الحاسوب ذاته.

وبناء على ما تقدم نستطيع القول إن القاضي الجزائي إذا قرر صحة الدليل الرقمي، وإن استخلاصه كان متسقاً مع الظروف الواقعة وملابساتها، فإنه يستطيع بناء على قناعته عليه، شرط أن تتوفر الضمانات التي يستلزمها القانون لكي يأتي الاقتناع القضائي سليماً، ولكن من الواجب أن يؤسس القاضي الجزائي قناعته على جزم ويقين، مستنداً إلى حجج ثابتة وقطعية، تجعل هذا اليقين ثابتاً لا يناقضه شك أو احتمال آخر، فالدليل الرقمي من حيث إثباته للوقائع الإجرامية، تتوفر فيه شروط اليقين، ويترتب على ثبوت التهمة بلوغ الاقتناع بالإدانة درجة اليقين من جانب القاضي الجزائي؛ لأن الاقتناع ثمرة اليقين، وبناء عليه يسمح الدليل الرقمي للقاضي بأن يستند إليه كدليل إثبات، ويكون الحكم الذي بني عليه حكماً سليماً وعادلاً⁽¹⁾.

واقتراع القاضي بالدليل الإلكتروني يكون مرهون بالشروط الآتية:

1- الإحاطة بكل الأدلة المدرجة في ملف الدعوى، ومناقشتها جميعاً طبقاً للقانون وعدم الاكتفاء بمناقشة بعضها.

(2) أنظر: عبد المطلب طاهري، الإثبات الجنائي بالأدلة الرقمية، مرجع سابق، ص52.

(1) أنظر: أحمد محمد العمر، الدليل الرقمي وحججه في الإثبات الجزائي، مرجع سابق، ص164 وما بعدها.

- 2- أن يكون الدليل ضمن أوراق الدعوى ويطرح في جلسة المحكمة.
- 3- أن يكون وليد إجراء مشروع.
- 4- أن تكون الأدلة متساندة ومتماسكة، ولا يشوبها خطأ في الاستدلال أو تناقض.
- 5- أن يكون الحكم مبنياً على الجزم واليقين، لا على الفرض أو الظن أو الترجيح لأن الشك يفسر لصالح المتهم.
- 6- أن لا يحكم القاضي دون دليل اعتماداً على ما يدور في نفسه، بل من خلال الأدلة المقدمة إليه.
- 7- يجب أن يكون القاضي حرفي في قناعته في تقييم الأدلة المقدمة إليه وهذا ما يعرف بالافتناع الشخصي للقاضي⁽²⁾.

المطلب الثالث

صلاحية القاضي في تقدير الأدلة في الاتجاهات المختلفة للدول

في مجال الإثبات الجنائي في الجرائم الإلكترونية، انقسمت الدول إلى اتجاهات مختلفة، حيث تبنت كل دولة الاخذ بنظام إثبات معين، فبعض الدول أخذت بنظام الإثبات الحر، وبعض الدول أخذت بنظام الإثبات المقيد، وبعض الدول أخذت بنظام الإثبات المقيد.

لذا سنقوم بتقسيم هذا المطلب إلى الآتي:

الفرع الأول: نظام الإثبات الحر (النظام اللاتيني).

الفرع الثاني: نظام الإثبات المقيد (الأنجلوسكسوني).

الفرع الثالث: نظام الإثبات المختلط.

(2) أنظر: دنيزاد ثابت، مطبوعات محاضرات مقياس الإثبات الجنائي، كلية الحقوق والعلوم السياسية- جامعة العربي النبسي، الجزائر 2020م - 2021م، ص 102 - 103.

الفرع الأول

نظام الإثبات الحر (النظام اللاتيني)

وقد اخذ بهذا النظام العديد من الدول مثل: (فرنسا، الأردن، مصر، سوريا، لبنان) ويعتمد هذا النظام على منح القاضي الحرية في تقدير الدليل سواء كانت الأدلة تقليدية أو عملية حديثة كالأدلة الرقمية، وقد أكد على ذلك المشرع الفرنسي عندما نصّ في المادة (427) من قانون الإجراءات الجنائية الفرنسية على ما يلي: " مالم يرد نص مخالف، يجوز إثبات الجرائم بجميع الطرق ، ويحكم القاضي بناءً على اقتناعه الشخصي"، وتأكيداً على ذلك قضت محكمة النقض الفرنسية في أحد قراراتها بصلاحية القضاء بالأخذ بأشرطة التسجيل الممغنطة والمدمجة، واعتبارها صالحة للتقديم أمامها.

والسؤال الذي يطرح نفسه هو: هل التسجيلات الصوتية الممغنطة والمسجلة إلكترونياً حجية في مسائل الإثبات الجنائي أم لا؟

يرى جانب من الفقه أنه من الصعوبات التلاعب بهذه التسجيلات، ويمكن لخبراء الأدلة الرقمية اكتشاف التلاعب فيها إن وجد وبكفاءة فنية وتقنية عالية، وبالتالي فإن التسجيلات الممغنطة له الحجية الكاملة في الإثبات الجزائي باعتباره من الأدلة التي تحمل الخطأ والتلاعب فيه⁽¹⁾.

وقد سارت على الأخذ بهذا الاتجاه معظم الدول الأوروبية (كألمانيا، واليونان، وكذلك أمريكا اللاتينية كالبرازيل)، وقد اعتمدت هذه الدول على الأخذ بنظام الإثبات الحر من حيث خضوع الأدلة الرقمية لسلطان القاضي وقناعته الوجدانية، فله قبول الدليل أو رفضه، سيما إذا وجد أن هذه الأدلة لا تتسجم مع العقل والمنطق ووقائع الدعوى المطروحة عليه⁽¹⁾.

الفرع الثاني

نظام الإثبات المقيد (الأنجلوسكسوني)

ويستند هذا الاتجاه على عدم منح القاضي السلطة التقديرية للدليل مهما كان نوع الدليل تقليدياً أم رقمياً، بمعنى أن القاضي لا يملك تقدير حجية الدليل بالمطلق، فالقانون هو الذي يحدد للقاضي ماهية الدليل ونوعه، وقيّمته القانونية وحجيته في الإثبات الجزائي، وخلاصة ذلك أن الدليل لا يكون له القيمة القانونية إلا إذا نص القانون عليه

(1) أنظر: د/ محمد عبد الحميد عرفة، مدى حُجِّيَّة الأدلة الإلكترونية الرقمية في الإثبات الجنائي – دراسة مُقارنة -، مجلة الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية العدد 1، سنة 2018م، ص493 وما بعدها.

(2) أنظر: د/ لورنس سعيد الحوامدة، حجية الأدلة الرقمية في الإثبات الجنائي – دراسة تحليلية مقارنة -، مجلة البحوث الفقيه والقانونية، العدد السادس والثلاثون، أكتوبر 2021م، جامعة طيبة، ص926.

واعتبره ضمن القائمة، فعدم وجود النص يعني لا قيمة للدليل، وليس له الحجية في الإثبات الجزائي.

ومن الدول التي أخذت بهذا النظام بريطانيا حيث حدد المشرع البريطاني أدلة الإثبات في قانون الشرطة والإثبات الجنائي الصادر عام 1984م متناولاً المشرع البريطاني في هذا القانون أدلة الإثبات في القضايا الجنائية بصورة دقيقة، سيما أن المشرع لم يمنح القاضي صلاحية تقدير الدليل من حيث قبوله أو رفضه. وقد سارت على نهج الأخذ بنظام الإثبات المقيدة العديد من الدول كالولايات المتحدة الأمريكية، وكندا وفي أمريكا صدر قانون الحاسب الآلي عام 1984م متمخضاً عنه اعتبار مخرجات الحاسوب الإلكتروني أدلة لها قيمة وحُجتها القانونية⁽²⁾.

الفرع الثالث

نظام الإثبات المختلط

أخذ هذا النظام بالجمع بين النظام اللاتيني والنظام الأنجلوسكسوني، بمعنى أن نظام الإثبات المختلط منح القاضي السلطة التقديرية لقبول الدليل في بعض أدلة الإثبات كأدلة الرقمية⁽¹⁾.

وفي أدلة أخرى القاضي لم يكن له إلا التزام بالنص القانوني والذي يحدد القيمة والحجية للدليل هو القانون وليس القاضي، ففي بعض الدول كاليابان التي أخذت بنظام الإثبات المختلط اعتبرت أن الأدلة الجنائية التقليدية (كالشهادة، وأقوال المتهم والقرائن، والخبرة) هي أدلة قانونية، وليس للقاضي سلطة تقديرية فيها، لأن القانون هو الذي يمنح هذه الأدلة القيمة والحجة القانونية، بينما أستاذ الفقه الجنائي الياباني

(2) أنظر: د/ محمد عبد الحميد عرفة، مدى حُجَّة الأدلة الإلكترونية الرقمية في الإثبات الجنائي – دراسة مُقارنة -، مرجع سابق، ص490.

نقلاً عن: د/ لورنس سعيد الحوامدة، حجية الأدلة الرقمية في الإثبات الجنائي – دراسة تحليلية مقارنة -، مرجع سابق، ص 927.

(1) أنظر: خالد مصطفى الجسمي، الإثبات الجنائي بالأدلة الرقمية، مجلة القانون المغربي، دار السلام للطباعة والنشر، العدد (34) 2007م، ص7.

على أن الأدلة الإلكترونية تخضع للسلطة التقديرية للقاضي فمثلاً: المجالات الإلكترونية مغناطيسية إذا كانت غير ملموسة أو مرئية لا تعد دليلاً يستند عليه القاضي المختص، أما إذا تحولت المجالات الإلكترونية مغناطيسية إلى أدلة مقروءة ومرئية فيمكن اعتبارها دليلاً في الإثبات الجنائي، وهذه تخضع للسلطة التقديرية للقاضي بحكم طبيعة الدليل ووقائع الدعوى⁽²⁾.

المبحث الخامس

دور الأمن السيبراني في مكافحة الجريمة السيبرانية

التطور التكنولوجي وإن أرسى قواعد جديدة (الفضاء السيبراني) استطاعت من خلالها الدول، والهيئات والشعوب والأمم للتواصل والتخاطب مباشرة وفي جميع الميادين، إلا أن هذا المضافة خلقت في مستويات معينة من التوظيف بعض التجاوزات حولت هذا الفضاء إلى مخبر للجرائم السيبرانية التي حالت دون حماية حقوق المؤسسات والأفراد للاستفادة من هذا الفضاء بكل حرية وفي إطار قانوني فالاستخدام المفرط لتكنولوجيا الاتصالات والتدفق السريع والمذهل للمعلومات (ثورة المعلومات)، ضاعفت من نسبة الاختراقات ووسائل التجسس، لتمس في بداية الأمر أمن الأشخاص مما جعل حياة البشر وخصوصياتهم ملاذ للابتزاز بشكل لا يصدق، وكثرت عمليات المساومة، فلم يعد يسلم فرد من هذه العمليات القذرة، سواء كان

(2) أنظر: عبد الفتاح بيومي حجازي، الإثبات في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، القاهرة 2007م، ص46.
نقلًا عن: د/ لورنس سعيد الحوامدة، حجية الأدلة الرقمية في الإثبات الجنائي – دراسة تحليلية مقارنة -، مرجع سابق، ص928.

مسئولا أو مواطننا ثم انتقلت الاختراقات بهدف التجسس والتخريب لتتال من الأجهزة ووزارة الدفاع والمؤسسات الحكومية والشركات والبنوك في أكبر دول العالم.

أمام هذا الخطر الذي أصبح لا يعرف حدود وتنوع في تطبيقاته (جرائم الإلكترونية، إرهابي إلكتروني، الحروب الإلكترونية)، توجه صناع القرار على المستوى الدولي إلى إطلاق صفارات الإنذار لإعادة بناء حواجز وجدران تقنية لمنع الهجمات (الأمن السيبراني) وخاصة وعملية الابتزاز قد بلغت مستويات من شأنها المساس بالأمن الوطني، القومي العالمي⁽¹⁾.

لذا سنقوم بتقسيم هذا المبحث إلى المطالب التالية:

المطلب الأول: مفهوم الأمن السيبراني.

المطلب الثاني: أهمية الأمن السيبراني وأهدافه.

المطلب الثالث: أبعاد الأمن السيبراني والمخاطر والتهديدات المرتبطة به.

المطلب الرابع: استراتيجيات مواجهة تهديدات الأمن السيبراني

المطلب الأول

مفهوم الأمن السيبراني

قضية أمن وحماية المعلومات تعتبر من أهم قضايا العصر حيث أصبح نجاح أي مؤسسة يعتمد بشكل كبير على ما تمتلكه من معلومات، لكن العديد من المعلومات والأنظمة والبنى التحتية المتصلة بالشبكات عرضة للخطر بين حين وآخر، حيث تواجه بأنواع شتى من الخروقات للمعلومات، كما تتعرض لأنشطة إجرامية (هاكرز) تعطل خدماتها وتدمر ممتلكاتها، وتختلف هجمات الهاكرز من جهة لأخرى ومن مكان لآخر ومن زمن إلى زمن مستخدمة أدوات وآليات اختراق متجددة ومتطورة طوال الوقت⁽¹⁾

(1) أنظر: د. جمال بوازدية، الإستراتيجية الجزائرية في مواجهة الجرائم السيبرانية " التحديات والافاق المستقبلية، مجلة العلوم القانونية والسياسية، المجلد (10)، العدد (1)، جامعة الجزائر 2019م، ص1264.

(1) أنظر: د. مني عبد الله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية - جامعة المنصورة، العدد 111 - يونيو 2020م، ص3.

فمصطلح (الأمن السيبراني) مكون من كلمتي (الأمن) و (السيبراني)، وقد اختلف الباحثين فتعريف معنى الأمن والسيبراني وتعريفهما معاً الأمر نقسم هذا المطلب إلى الفروع التالية:

الفرع الأول: تعريف الأمن.

الفرع الثاني: تعريف السيبرانية.

الفرع الثالث: تعريف الأمن السيبراني.

الفرع الرابع: الفرق بين أمن المعلومات والأمن السيبراني.

الفرع الأول

تعريف الأمن

الأمن هو نقيض الخوف، وهو شعور الفرد بالاطمئنان والأمان، وانعدام الإحساس بالخطر، وهو يتحقق من خلال أمن الدولة ككل حيث يمثل الأمن مفهوماً مركزياً في حياة كل المجتمعات المتقدمة والمختلفة، كما يؤثر مفهوم الأمن في الأذهان، معاني البقاء والتكامل داخل الدولة الواحدة وبينها وبين الدول المجاورة لها، والتماسك الاجتماعي، أي التماسك بين طبقات الشعب، وحماية المصالح سواء كانت مصلحة الأفراد أو مصلحة المجتمع والدولة ككل، ثم حماية قيم المجتمع ضد التهديد⁽²⁾.

ومن البديهي أن تكون نظرية الأمن مرتبطة أساساً بالمخاطر التي تهدد مجتمعاً معيناً ، الأمر الذي أضفى عليها طابعاً عسكرياً واستراتيجياً بحتاً باعتبار أن القوة العسكرية هي الدرع الواقي الوحيد ضد المخاطر كافة "خارجية أم داخلية" لكن هذا المفهوم الضيق لنظرية الأمن بدءاً من طبيعة القوى الاجتماعية وعلاقتها وانتهاء بدور الدولة على صعيد العلاقات الاقتصادية والاجتماعية، وكذلك تغير المعطيات الخارجية التي قلبت مقاييس علاقات السلم والحرب في العالم ، بدءاً من التنظيمات العالمية الجديدة وانتهاء بالتطور التكنولوجي الكبير. ومن هنا بدأت نظرية الأمن تتخذ أبعاداً جديدة لتشمل سائر جوانب الحياة الوطنية في عملية نكوص داخلية أفرزتها طبيعة العلاقات الدولية والاجتماعية المعاصرة، الأمر الذي أدى إلى تجاوز المفهوم العسكري الاستراتيجي المحض نحو مفهوم واسع قادر على الاستجابة لمقتضيات العصر وتحدياته⁽¹⁾.

(2) أنظر: د/ محمد رضا فودة، "الاستراتيجية والأمن القومي، المكتب العربي للمعارف"، القاهرة 1995م، ص3.

(1) أنظر: د/ جلال فضل محمد العودي، القرصنة البحرية وحرية أعالي البحار، الطبعة: الأولى، دار النشر المصرية للنشر والتوزيع، القاهرة 2020م، ص313.

الفرع الثاني

تعريف السيبرانية

مصطلح (سيبار) Cyber هو لفظ يوناني الأصل مشتق من كلمة (Kybernetes)، بمعناها الشخص الذي يدير دفة السفينة، حيث تستخدم مجازاً للمتحكم (governor)، وتم استخدامها من طرف افلاطون للتعبير عن الحكم. وتجدر الإشارة أن العديد من المؤرخين يرجعون أصلها إلى عالم الرياضيات الأمريكي (Norbert Wiener 1894-1964)، وذلك للتعبير عن التحكم الآلي⁽²⁾.

فتعريف السيبرانية مأخوذة من كلمة (سيبر) Cyber، وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي، فالسيبرانية، تعني (فضاء الإنترنت)⁽³⁾.

فإضافة كلمة سايبير إلى أي شيء آخر تضيفي عليه معنى الإلكترونية مثل Cyber-Security الأمن الإلكتروني و Cyber-Attack تعني الهجمات الإلكترونية، فكلمة سايبير تستخدم بمعنى الفضاء الإلكتروني⁽⁴⁾.

الفرع الثالث

تعريف الأمن السيبراني

أما الأمن السيبراني اصطلاحاً فهناك العديد من التعاريف التي قدمت لمفهوم الأمن السيبراني، حيث يُعرف بأنه (مجموعة من الإجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل التدابير المضادة المطلوبة).

وهذا ما ذهب إليه الكاتبان Neittaanmaki Pekka, Leht0 Martti في كتابهما Security: Analytics, Technology and Automation Cyber ، حيث عرفا الأمن السيبراني أنه: " عبارة عن مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قرصنة الكمبيوتر وعواقبهما، ويتضمن تنفيذ التدابير المضادة المطلوبة".

(2) راجع: خالد ساسوي، محمد بن حسين، الحروب السيبرانية والأمن العالمي التحديات والمواجهة، رسالة ماجستير مقدمة إلى كلية الحقوق والعلوم السياسية – جامعة زيان عاشور 2019م – 2020م، ص23.

(3) أنظر: صالح بن علي عبد الرحمن الربيع، الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت. نقلاً عن: د. أمانة على البشير محمد، الأمن السيبراني في فضاء مقاصد الشريعة، مجلة كلية الدراسات الإسلامية والعربية للبنات بالإسكندرية، العدد (37)، الجد الأول، ص459.

(4) نقلاً عن: خلية وريدة، إشكالية المواطنة في ظل قيم التكنولوجيا الحديثة بين حرية المواطن والأمن السيبراني، حوليات جامعة الجزائر، المجلد (35) العدد (2)، كلية الإعلام والاتصال – جامعة الجزائر 2021م، ص811، 812.

بينما عرفه (إدوار أمورسو AmOrOso Edward) بأنه " وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة"(1).

كما عرفت وزارة الدفاع الأمريكية الأمن السيبراني بأنه " مجموعة الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها (الإلكترونية والمادية)، من مختلف الجرائم، الهجمات التخريب، التجسس والحوادث.

كما عرفته وكالة الأمن الرقمي الأوروبية – أول من أصدرت تشريع في هذا المجال – بأنه قدرة النظام المعلوماتي على مقاومة الاختراق أو الحوادث غير المتوقعة، التي تستهدف البيانات المتداولة أو المخزونة وفق إطار توافقي (أول اتفاقية في الموضوع صدرت في بودابست 2001).

كما جاء تعريفه من قبل الاتحاد الدولي للاتصالات الصادرة في تقريره حول – اتجاهات الإصلاح في الاتصالات للعام 2010م – 2011م، والذي يعتبر بمثابة أرضية إجماع لمختلف التوجهات الفكرية والمهنية – الأمن السيبراني " هو مجموعة من المهمات، مثل تجميع وسائل وسياسات، وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين(2).

الفرع الرابع

الفرق بين أمن المعلومات والأمن السيبراني

أمن المعلومات يهدف إلى حماية الأنظمة الحاسوبية من الوصول غير الشرعي لها، أو العبث بالمعلومات أثناء التخزين أو المعالجات أو النقل، كما يهدف إلى الحماية ضد تعطيل خدمة المستخدمين الشرعيين.

كما أنه يعني أمن المعلومات بالوسائل الضرورية لاكتشاف وتوثيق وصد كل هذه التهديدات، وأمن المعلومات يشمل كل ما شأنه حماية (المعلومة) التي قد تكون في نظام حاسوبي، أو قد لا تكون فهو المضلة الكبرى التي تغطي كل الأفرع الأخرى المرتبطة بحماية البيانات والمعلومات وتأمينها، ويهتم بمجالات ضخمة، كالتشفير، والتخزين، والتأمين الفيزيائي، والمعايير الأمنية، وإدارة من المعلومات والمخاطر.

(1) نقلاً عن: د. مني عبد الله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية – جامعة المنصورة، العدد (111)، يوليو 2020م، ص10.

(2) أنظر: د. جمال بوازدية، الإستراتيجية الجزائرية في مواجهة الجرائم السيبرانية " التحديات والأفاق المستقبلية"، مجلة العلوم القانونية والسياسية، المجلد (1)، العدد (1)، جامعة الجزائر 2019، صص1266، 1267.

فالمعلومات والأمن السيبراني هما مصطلحان متشابهان، لكنهما ليسا متطابقين أن الحرب السيبرانية أصبحت جزءاً لا يتجزأ من الأساليب الحديثة للحروب والهجمات بين الدول⁽¹⁾.

وعلى الرغم من التشابه بين المجالين إلا أن هناك نقاط اختلاف جوهرية بين أمن المعلومات والأمن السيبراني من أبرزها:

1- الأمن: في حين أن الأمن السيبراني يدور حول حماية الفضاء الإلكتروني الخاص بك من الوصول الرقمي غير المصرح به، لذلك فالأمر كله يتعلق بحماية البيانات الموجودة في شكل إلكتروني، أمن المعلومات هو كل شيء عن حماية أصول المعلومات الخاصة بك من الوصول غير المصرح به.

2- البيانات: وقد يشمل ذلك المعلومات غير الإلكترونية أيضاً، فأمن المعلومات يهتم بأمن المعلومات الفيزيائية (الورقية)، بينما لا يهتم الأمن السيبراني بذلك، فالعلاقة بين أمن المعلومات والأمن السيبراني تتقاطع من حيث الاهتمام بأمن المعلومات الموجودة بالسايبير، ويختلفان فيما تبقى من الاهتمامات.

3- وظيفة الأمن السيبراني مقابل أمن المعلومات: يتعامل أمن الإنترنت مع التهديدات التي قد تكون موجودة في عالم الإنترنت مثل حماية حسابات الوسائط الاجتماعية الخاصة بك، والمعلومات الشخصية، وما إلى ذلك، بينما يتعامل أمن المعلومات بشكل أساسي مع أصول المعلومات ونزاهتها وسريتها وتوافرها، وهذه هي الأهداف الأمنية الثلاثة لأمن المعلومات⁽²⁾.

المطلب الثاني

أهمية الأمن السيبراني وأهدافه

بعد التقدم الكبير الذي حدث في عالم التكنولوجيا وأيضاً مع تطور المعاملات الرقمية المختلفة، أصبح الاعتماد على الأمن السيبراني من أهم الأمور في وقتنا هذا، فإنه يعمل على حماية الشركات والمؤسسات الخاصة والعامة من الهجمات السيبرانية التي قد يشنها القراصنة - عبر الانترنت - على كافة الأجهزة الإلكترونية (أجهزة الكمبيوتر - الأجهزة الرقمية - الهواتف الذكية - الأجهزة اللوحية) التي تستخدم بشكل يومي

وعليه سنقوم بتقسيم هذا المطلب إلى الفروع التالية:

(1) أنظر: صالح بن علي بن عبد الرحمن الربيع، الأمن القومي وحماية المستخدم من مخاطر الانترنت، هيئة الاتصالات وتقنية المعلومات، المملكة العربية السعودية 2020م، ص 10 - 11.

(2) أنظر: آمنه على البشير محمد، الأمن السيبراني في ضوء مقاصد الشريعة، مجلة كلية الدراسات الإسلامية للنبات بالإسكندرية، المجلد الأول العدد (37)، ص 463، 464.

الفرع الأول: أهمية الأمن السيبراني.

الفرع الثاني: أهداف الأمن السيبراني.

الفرع الأول

أهمية الأمن السيبراني

في عالم المترابط بواسطة الشبكات، ويستفيد الجميع من برامج الدفاع السيبراني وتتمثل أهمية الأمن السيبراني فيما يلي⁽¹⁾:

1- الحفاظ على المعلومات وسلامتها وتجانسها، وذلك بكف الأيدي من العبث بها، وتحقيق وفرة البيانات وجاهزيتها عند الحاجة إليها.

2- حماية الأجهزة والشبكات ككل من الاختراقات لتكون درعاً واقياً للبيانات والمعلومات.

3- استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.

4- استخدام الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيق مبادئ الأمن السيبراني.

5- توفير بيئة آمنة جداً خلال العمل عبر الشبكة العنكبوتية.

فالأمن السيبراني أصبح قضية رئيسية للشركات الحديثة والحكومات والأفراد. مع التحول الرقمي للشركات، والاستخدام الواسع النطاق لأدوات تكنولوجيا المعلومات والاتصالات عبر الإنترنت، أصبحت حماية أنظمة المعلومات والبيانات المتداولة ضد مجرمي الإنترنت أمراً ضرورياً. يمكن أن تتسبب الهجمات الإلكترونية في خسائر مالية كبيرة للشركات، فضلاً عن الإضرار بسمعتها وصورة علامتها التجارية.

وبحسب احصائيات لشركة اي بي ام الأميركية، قدرت الخسائر المالية الناجمة عن الهجمات الإلكترونية في الولايات المتحدة بنحو 3.5 مليار دولار فقط في العام 2019م⁽¹⁾

(1) أنظر: مني عبد الله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مرجع سابق، ص12.

(1) سهام عثمانى، الأمن السيبراني في قلب تحديات الأعمال الحديثة، مقالة في ملف عن الامن السيبراني بالفرنسية على الرابط /

لا تكمن الخسارات في طابعها المادي بل أن يمكن أن تكون لها آثار مدمرة حقيقية، أخذًا بالاعتبار الاعتماد المتزايد والكامل على الحلول التقنية في تسيير أعمال المؤسسات والشركات. شبكات الطاقة والنقل والرعاية الصحية وغيرها من القطاعات، تكون عرضة للهجمات السيبرانية. ويمكن أن تسبب هذه الأنواع من الهجمات أضرارًا كبيرة لهذه الأنظمة الحيوية الضرورية للحفاظ على نوعية الحياة في بلد ما. على سبيل المثال، يمكن أن يؤدي الهجوم الإلكتروني على نظام الطاقة إلى انقطاع هائل يؤثر على البلد بأكمله. وبالمثل فإن الهجوم على نظام الرعاية الصحية قد يجعل من الصعب على المرضى الوصول إلى الرعاية الطبية بسبب انقطاع الأداء الطبيعي للنظام. باختصار، من المهم حماية هذه البنى التحتية الحيوية ضد التهديدات السيبرانية حتى تتمكن من الاستمرار في تقديم خدماتها الحيوية دون انقطاع أو تأثير كبير.

وحتى على مستوى الأفراد يعد الأمن السيبراني مهمًا جدًا لنا جميعًا نظرًا للتحول الرقمي للشركات والمؤسسات. ويستخدم هذا التحول تكنولوجيا المعلومات وأدوات الاتصال عبر الإنترنت، بالإضافة إلى حماية أنظمة المعلومات والبيانات المتبادلة ضد المجرمين على الإنترنت. بمعنى آخر، يتعلق الأمر بحماية معلوماتنا الشخصية والتجارية من المتسللين الذين يسعون إلى سرقة هذه المعلومات الحساسة أو إتلافها. إذا أجريت مثلًا معاملة مصرفية عبر الإنترنت أو شاركت بياناتك مع أخرى عبر الإنترنت فإن الأمن السيبراني يضمن لك بقاء معلوماتك سرية وعدم تعرضها للخطر من قبل طرف ثالث ضار.

مهارات الكمبيوتر التي يكتسبها الأشخاص الخبيثون هي مخاطر لا ينبغي الاستخفاف بها. بالإضافة إلى الهجمات السيبرانية، يسمح الأمن السيبراني بتنفيذ العمليات بين الموظفين لإنشاء ممارسات عملية وتقنية جيدة. وفي الواقع، تؤخذ الأخطاء البشرية أيضًا بعين الاعتبار في مجال الأمن السيبراني⁽¹⁾.

الفرع الثاني

أهداف الأمن السيبراني

<https://www.village-justice.com/articles/cybersecurite-coeur-des-enjeux-entreprise-moderne,39117.html>

(1) الأمن السيبراني / تعريف مقالة على مدونة بالفرنسية على الرابط :

<https://www.sage.com/fr-fr/blog/glossaire/cybersecurite-definition-de-la-cybersecurite>

من أهم أهداف الأمن السيبراني هي⁽²⁾:

- 1- تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات وما تحويه من بيانات.
- 2- التصدي لهجمات وحوادث امن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص.
- 3- توفير بيئة آمنة موثوقة للتعاملات في مجتمع المعلومات.
- 4- صمود البنى التحتية الحساسة للهجمات الإلكترونية.
- 5- توفير المتطلبات اللازمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين.
- 6- التخلص من نقاط الضعف في أنظمة الحاسب الآلي والأجهزة المحمولة باختلاف أنواعها.
- 7- سد الثغرات في أنظمة أمن المعلومات.
- 8- مقاومة البرمجيات الخبيثة، ما تستهدفه من أحداث أضرار بالغة للمستخدمين.
- 9- حد من التجسس والتخريب الإلكتروني على مستوى الحكومة والأفراد.
- 10- اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الإنترنت.
- 11- تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزةهم التقنية بقصد الضرر بمعلوماتهم الشخصية سواء بالإتلاف أو بقصد السرقة.

أما فيما يختص أهداف الأمن السيبراني في المملكة العربية السعودية فهو على النحو التالي:

- 1- ضمان توافر استمرارية عمل نظم المعلومات.
- 2- حماية الأنظمة التشغيلية من أي محاولات للولوج بشكل غير مباشر غير مسموح به لأهداف غير سلمية.
- 3- حماية مصالح المملكة الحيوية وأمنها الوطني، والبنى التحتية الحساسة فيها.

(2) أنظر: د. مني عبد الله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مرجع سابق، ص12.

- 4- اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة.
- 5- تعزيز حماية الشبكة وأنظمة المعلومات.
- 6- تعزيز حماية وسرية وخصوصية البيانات الشخصية.
- 7- تعزيز حماية أنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحتويه من بيانات.
- 8- التأسيس لصناعة وطنية في مجال الأمن السيبراني تحقق للمملكة الريادة في هذا المجال⁽¹⁾.

المطلب الثالث

أبعاد الأمن السيبراني والمخاطر والتهديدات المرتبطة به

الأمن السيبراني هو المجال الذي يتعامل مع حماية الأنظمة الإلكترونية والشبكات والبرامج والأجهزة من الهجمات الإلكترونية والاختراقات السيبرانية والتهديدات الأمنية الأخرى، وبما أن الأمن السيبراني يتعلق بالحماية من التهديدات الإلكترونية، يعتبر مجالاً متطوراً ومتغيراً باستمرار، ويتطلب متابعة دائمة للتطورات التقنية

(1) أنظر: فاطمة يوسف المنتشري، دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات، المجلة العربية للعلوم التربوية والنفسية، المجلد الرابع، العدد (17) يوليو 2020م، ص463، 464.

والتهديدات الأمنية الجديدة، وتحديث الإجراءات والأدوات الأمنية بشكل دوري لتلبية التحديات الجديدة.

لذا سنقوم بتقسيم هذا المطلب إلى الفروع التالية:

الفرع الأول: أبعاد الأمن السيبراني.

الفرع الثاني: المخاطر والتهديدات المرتبطة بالأمن السيبراني.

الفرع الأول

أبعاد الأمن السيبراني

يعتبر متغير الأمن السيبراني مفهوم ذات أبعاد نسبية أهمها:

1- البعد العسكري: كانت البدايات الأولى للأنترنت في البيئة العسكرية، وبعد ذلك انتقلت إلى الأوساط العلمية والأكاديمية وأبحاث تخدم القدرات العسكرية، وتشمل الميزة النسبية للأمن السيبراني في بعد عسكري، عن طريق قدرة القوة السيبرانية على ربط الوحدات العسكرية ببعضها البعض عبر العالم الافتراضي، وهذا ما يسهل عملية تبادل المعلومات، والذي ينعكس إيجاباً على تحقيق الأهداف العليا للمؤسسة العسكرية. كما توجد في هذا المجال عدة أمثلة توضح البعد العسكري للأمن السيبراني ومدى خطورة الهجمات السيبرانية، وهو ما حصل في جورجيا، وأستونيا، وكوريا الجنوبية، وإيران على بعض الهجمات والاختراقات، والتي أشارت إلى اندلاع صراع مسلح لاحق كذلك الذي وقع بين جورجيا وروسيا، أو بانقطاع الاتصال بالأنترنت في أستونيا بين الدولة والمواطنين والتشويش على الإدارات الحكومية.

كذلك اختراقات أنظمة المنشآت النووية الإيرانية، والتلاعب بها أدى إلى تهديد الأمن القومي للدولة المعنية. فسيناريوهات الهجمات السيبرانية نتائجها كارثية، الأمر الذي يجعل العمل بجدية في تحقيق الأمن السيبراني دون التقاعس أو انتظار وقوع كارثة تكون نتائجها أكثر دراماتيكية.

2- البعد السياسي: تتمثل الأبعاد السياسية للأمن السيبراني بشكل أساسي في حق الدولة في حماية النظام السياسي وكيانها ومصالحها الاقتصادية والسعي إلى تحقيق رفاه شعبها. في حين تؤثر التقنيات في موازين القوى داخل المجتمع نفسه، بحيث أصبح المواطن بإمكانه التحول إلى لاعب سياسي في اللعبة السياسية، وأصبح بإمكانه الاطلاع على خلفيات القرارات السياسية التي تتخذها الحكومة عبر الكم الهائل من المعلومات التي يمكن الوصول إليه أو تم نشرها على الإنترنت.

بالمقابل هناك تأثير – بغض النظر – عن صحة السياسيات والمبادئ والمواقف والتي يروج إليها. فقد استخدم باراك أوباما مثلاً: الشبكات الاجتماعية بشكل كثيف خلال حملته الانتخابية، كما تركت التسريبات الوثائقية الدبلوماسية السرية عبر (ويكيليكس) أثراً سلبياً على العلاقات بين الدول ومصادقيتها.

3- البعد الاجتماعي: تعتبر الشبكة الدولية للمعلومات مجاًلاً مفتوحاً لجميع الأفراد، حيث يمكن لجميع المتعلمين السيبرانيين أن يستفيدوا من البنى التحتية والخدمات المتاحة لهم دون تحمل مخاطر أمنية، وهنا يجب التنويه إلى ضرورة التحسيس بأخلاقيات الأمن السيبراني. بالمقابل ساهم جميع المجتمع في تطور الفضاء السيبراني، وذلك بتبادل الأفكار والمعلومات المختلفة، وافتتاح المجتمع على الآخر، ويؤسس لتبادل الخبرات والأفكار وتكون حاجات جديدة وآفاق تعاون وتكامل. يضاف إلى ذلك ما يقدمه الأنترنت من إمكانات وقدرات، للمجالات العلمية والثقافية والخدمية. فالمحتويات غير المشروعة غير مرغوب بها؛ كونها ذات تأثير سلبي على أخلاقيات مجتمع معين، وارتفاع نسبة الممارسات الجرمية، ومن أمثلة ذلك: الإباحية والترويج للاتجار بالممنوعات، والإرهاب والتجنيد لقضايا تمس الأمن والسلام الدوليين، وعليه لا بد من بناء مجتمع مسؤول ومدرك لمخاطر الفضاء السيبراني، والتعامل معه بحد أدنى من قواعد السلامة مع إدراك العواقب القانونية⁽¹⁾.

4- البعد القانوني: يترتب على النشاطات الفردية والمؤسسية والحكومية في الفضاء السيبراني، نتائج قانونية تتمثل في إيجاد القواعد القانونية التي تنظم العلاقات في الفضاء السيبراني، وحل النزاعات التي تنشأ عنها، وقد نشأت أساليب وممارسات عديدة في استخدام تقنية المعلومات، كإنشاء المدونات والمجتمعات على الأنترنت. والحق في حماية ملكية البرامج المعلوماتية، والإبلاغ عن المخالفات والجرائم السيبرانية، وهذا ما أدى إلى ضرورة وجود ترسانة قانونية مع المتغيرات الحاصلة، كذلك بروز تحويلات جديدة على مستوى جميع المجالات، وتساعد القضايا التي رفعت أمام المحاكم، مما يستدعي إعداد بيئة تنظيمية تشريعية، وبناء ميثاق لمكافحة الجرائم السيبرانية والحكم⁽¹⁾.

5- البعد الاقتصادي: يرتبط الأمن السيبراني ارتباطاً وثيقاً بالاقتصاد، فقد توسع استخدام تقنيات المعلومات والاتصالات ما أتاح وعزز التنمية الاقتصادية لعدد من البلدان وزادت فرص الاستخدام التي تقدمها الشركات الدولية الكبرى، ولا ننسى حلول

(1) أنظر: منى الأشقر حبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت 2017م، ص 28.
نقلًا عن: خالد ساسوي، محمد بن حسين، الحروب السيبرانية والأمن العالمي التحديات والمواجهة، رسالة ماجستير مقدمة إلى جامعة زيان عاشور – الجلفة- كلية الحقوق والعلوم السياسية 2019م – 2020م، ص 25.
(2) أنظر: بارة سمير، الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر، جامعة قاصدي مرياح ورقلة – كلية الحقوق والعلوم السياسية 2001م، ص 229 وما بعدها.
نقلًا عن: خالد ساسوي، محمد بن حسين، الحروب السيبرانية والأمن العالمي التحديات والمواجهة، مرجع سابق، ص 26

عصر المال الإلكتروني ضمن بيئة تقنية متحركة كوجود المحفظة الإلكترونية. وإصدار البطاقات التي تسمح بالدفع الإلكتروني⁽²⁾.

الفرع الثاني

المخاطر والتهديدات المرتبطة بالأمن السيبراني

مخاطر الأمن السيبراني عديدة ويمكن أن يكون لها عواقب وخيمة على كل فئات وقطاعات المجتمع ومؤسساته. ومن أهم التهديدات السيبرانية يمكن أن نشير هنا إلى:

1-الهجمات على أجهزة الحواسيب المختلفة

تشكل تهديدات الأمن السيبراني الناتجة عن التخريب أو الأخطاء البشرية خطرًا كبيرًا على الشركات والأفراد. وفقًا لأبحاث شركة أي بي أم الأميركية هذه الأخطاء تساهم في 95% من خروقات الأمن⁽³⁾.

وهذه المخاطر ذات الطابع البشري قد تكون أخطاء غير مقصودة أو عمليات تخريب متعمدة.

أ. من أمثلة هذه الأخطاء البشرية:

- قد يكشف الموظفون عن غير قصد عن معلومات حساسة أو يفتحون مرفقات ضارة⁽⁴⁾.

- كلمات المرور الضعيفة أيضا من هذه الأخطاء حيث يمكن للمستخدمين اختيار كلمات مرور ضعيفة أو إعادة استخدامها عبر حسابات متعددة، مما يسهل على مجرمي الإنترنت الوصول إلى معلوماتهم الشخصية.

-الإهمال: قد يهمل المستخدمون التحديثات الأمنية أو التحذيرات الأمنية، مما قد يجعل أنظمتهم عرضة للهجمات الإلكترونية.

2-أما من ناحية التخريب والتهديدات الداخلية فقد تأخذ هذه الأخطاء المتعمدة شكل:

(2) أنظر: منى الأشقر حبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، ص28.
نقلًا عن: نقلًا عن: خالد ساسوي، محمد بن حسين، الحروب السيبرانية والأمن العالمي التحديات والمواجهة، مرجع سابق، ص26
(3) تهديدات للأمن السيبراني للشركات لعام 2023م، مقالة على موقع شركة Ester رابط المقالة :

<https://www.exter.fr/cybersecurite-en-entreprise>

(4) نفس المرجع السابق:

<https://www.exter.fr/cybersecurite-en-entreprise>

سرقة البيانات وتسريبها: يمكن للموظفين سرقة البيانات الحساسة أو التسبب في تلف أنظمة تكنولوجيا المعلومات الخاصة بالشركة⁽¹⁾.

التجسس: يمكن أن تقوم به دول أو شركات منافسة لسرقة معلومات حساسة.

التخريب: يمكن تنفيذه لتعطيل العمليات التجارية أو التسبب في أضرار مادية.

يضاف إلى ذلك أيضا استخدام برامج الفدية، والفيروسات، والبرامج الضارة عبر البرامج الفيروسية والخبثية. تمكن هذه البرامج الخبيثة مجرمي الإنترنت من استخدام هذه الهجمات لسرقة البيانات الحساسة، أو تعطيل العمليات التجارية، أو ابتزاز الأموال، أو الإضرار بسمعة الشركات.

3- التهديدات الهجينة:

التهديدات الهجينة هي هجمات تجمع بين عناصر من أشكال مختلفة من الحرب، مثل الحرب التقليدية، والحرب الاقتصادية، وحرب المعلومات وتمثل هذه التهديدات الهجينة تحديًا متزايدًا للشركات والحكومات.

تشمل أهم تهديدات الأمن السيبراني الهجين ما يلي:

هجمات التضليل: يمكن لمجرمي الإنترنت استخدام حملات التضليل للتأثير على الرأي العام وتعطيل العمليات الديمقراطية، الاتهامات الأميركية لروسيا في التدخل في الانتخابات الأميركية الماضية مثالا بارزا على قدرات هذه الهجمات على تضليل الرأي العام.

الهجمات التخريبية: عبر استخدام الهجمات التخريبية لتعطيل العمليات التجارية أو التسبب في أضرار مادية.

هجمات التصيد الاحتيالي: يمكن لمجرمي الإنترنت استخدام هجمات التصيد الاحتيالي لسرقة معلومات حساسة أو تثبيت برامج ضارة على أجهزة كمبيوتر المستخدمين.

2- التحديات الراهنة في مجال الأمن السيبراني:

(1) ثغرات الأمن السيبراني: ضرورة الاعتراف بالعامل البشري، مقالة على موقع شركة اورانج الفرنسية.

<https://www.orange cyberdefense.com/fr/insights/blog/cyberdefense/failles-de-cybersecurite-la-necessite-de-reconnaitre-le-facteur-humain>

لا تقتصر التهديدات السيبرانية على ماهي عليه اليوم، بل إن التحديات الحالية والمستقبلية في مجال الأمن السيبراني عديدة ومتنوعة وأكثر خطورة. مما يجعل الأمن السيبراني أكثر أهمية من أي وقت مضى.

ومع استمرار تحول العالم نحو أجيال جديدة من التقنيات والحلول الرقمية تزداد أهمية الأمن السيبراني، من أهم هذه التطورات المستقبلية التي يمكن أن تشكل فرصا وخطورة متزايدة نذكر:

أ. إنترنت الأشياء أو: (IoT)

إنترنت الأشياء هو شبكة من الأشياء المتصلة بالإنترنت والتي يمكنها جمع ونقل البيانات. يمكن أن تكون هذه الأشياء أي شيء من الأجهزة المنزلية إلى السيارات إلى المعدات الصناعية.

يمكن أن تستخدم إنترنت الأشياء لتحسين الكفاءة والإنتاجية والأمان والخدمات. على سبيل المثال، يمكن استخدامها لمراقبة العمليات الصناعية وتحسينها، أو لتوفير معلومات حول حالة الآلات والأجهزة، أو لتوفير خدمات جديدة للعملاء.

من الأمثلة على إنترنت الأشياء:

المنازل الذكية: يمكن استخدام إنترنت الأشياء لتشغيل الأجهزة المنزلية عن بعد، ومراقبة الطاقة، وتوفير الأمان.

المدن الذكية: يمكن استخدام إنترنت الأشياء لمراقبة حركة المرور، وإدارة النفايات، وتوفير الخدمات العامة.

الرعاية الصحية: يمكن استخدام إنترنت الأشياء لجمع البيانات الصحية عن المريض، ومراقبة حالة المريض، وتوفير العلاج عن بعد.

التصنيع: يمكن استخدام إنترنت الأشياء لمراقبة الإنتاج، وتحسين جودة المنتجات، وتوفير الخدمات اللوجستية.

ينمو إنترنت الأشياء بسرعة كبيرة، ويتوقع أن يبدأ استخدامه على نطاق واسع خلال سنوات قليلة مع استمرار التنافس التكنولوجي وتقنيات الجيل الخامس والسادس من الانترنت.

فيما يلي فوائد إنترنت الأشياء:

الكفاءة: يمكن أن يساعد إنترنت الأشياء في تحسين الكفاءة التشغيلية من خلال أتمتة المهام وتوفير معلومات غنية بالبيانات. ويساعد أيضا في تحسين الإنتاجية من خلال تحسين مراقبة العمليات واتخاذ القرارات.

الخدمات: يمكن أن تساعد إنترنت الأشياء في توفير خدمات جديدة للعملاء من خلال جمع وتحليل البيانات.

ومع ذلك، هناك أيضًا بعض التحديات التي تواجه إنترنت الأشياء، مثل:

الخصوصية: يمكن أن تؤدي إنترنت الأشياء إلى جمع كميات كبيرة من البيانات الشخصية، مما يثير مخاوف بشأن الخصوصية.

التكلفة: يمكن أن تكون تكلفة نشر وصيانة أنظمة إنترنت الأشياء باهظة.

على الرغم من هذه التحديات، فإن إنترنت الأشياء لديها القدرة على إحداث ثورة في العديد من الصناعات وتحسين حياتنا بشكل كبير.

إنترنت الأشياء يشكل أيضًا تحديًا كبيرًا في مجال الأمن السيبراني لأنه يتضمن توسعًا هائلًا في الأجهزة المتصلة بالإنترنت. يمكن أن يكون لنقاط الضعف في إنترنت الأشياء عواقب وخيمة للغاية، خاصة فيما يتعلق بأمن وسرية البيانات الشخصية. في كثير من الأحيان، يتم تصميم أجهزة إنترنت الأشياء بروتوكولات أمان غير كافية، مما يجعلها عرضة للهجمات الإلكترونية⁽¹⁾.

ج. التهديدات المتعلقة بالشبكات الاجتماعية والخصوصية على الإنترنت

تعد الشبكات الاجتماعية والخصوصية عبر الإنترنت من القضايا المهمة في مجال الأمن السيبراني.

حيث قد يتعرض مستخدمو وسائل التواصل الاجتماعي لمخاطر مثل سرقة الهوية والابتزاز وسرقة المعلومات والمطاردة عبر الإنترنت. يمكن لمجرمي الإنترنت أيضًا استخدام وسائل التواصل الاجتماعي لارتكاب عمليات الاحتيال وسرقة المعلومات الشخصية أو التجارية.

هذه التحديات تتطلب من المستخدمين اتخاذ خطوات لحماية خصوصيتهم عبر الإنترنت، مثل حماية الوصول إلى حساباتهم، والتحقق من إعدادات الخصوصية، والحذر من الرسائل المشبوهة وطلبات الصداقة. وهو ما انتبهت إليه الحكومات والمؤسسات الدولية مؤخرًا مثل الاتحاد الأوروبي الذي بدأ عملية تشريع واسعة تفرض عمالقة التكنولوجيا اتخاذ خطوات لحماية البيانات الشخصية لعملائها وموظفيها، من خلال تنفيذ سياسات أمنية صارمة وتدريب موظفيها على الأمن

(1) ادوارد ماير، الذكاء الصناعي في خدمة الأمن السيبراني، مقالة على الرابط :

<https://maltem.com/en/blog/ia-service-cyber-securite>

السيبراني وتعزيز حماية الخصوصية عبر الإنترنت، بما في ذلك إدخال قوانين ولوائح لحماية البيانات الشخصية وحقوق المستخدمين عبر الإنترنت⁽¹⁾.

د. الأمن السيبراني الصناعي والبنية التحتية الحيوية:

أن البنية التحتية الحيوية، مثل شبكات الطاقة وأنظمة النقل وأنظمة الرعاية الصحية، معرضة أيضًا للهجمات الإلكترونية. وبالتالي فإن تحديات الأمن السيبراني للشركات والمؤسسات كبيرة جداً، حيث يمكن أن تكون الخسائر المالية والخسائر المتعلقة بالسمعة كبيرة. والشركات التي تتمتع بثقافة قوية في مجال الأمن السيبراني تتمكن من رؤية أفضل للتهديدات المحتملة⁽²⁾.

المطلب الرابع

استراتيجيات مواجهة تهديدات الأمن السيبراني

(1) أمن مواقع الشبكات الاجتماعية، مقالة على الموقع الحكومي الفرنسي حول البرمجيات الخبيثة، على الرابط <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/reseaux-sociaux>

(2) الأمن السيبراني، تحدي أساسي للشركات في العام 2023م، مقالة على الرابط: <https://www.fibre-pro.fr/cybersecurite>

أصبح الأمن السيبراني قضية حاسمة لأمن واستقرار مجتمعنا الحديث.

وإدارة المخاطر السيبرانية ضرورية للشركات والأفراد ومؤسسات الدولة الحيوية، من أجل حماية بياناتهم وأنظمة المعلومات الخاصة بهم⁽¹⁾، وتتطلب مواجهة هذا النوع الجديد من التهديدات اتخاذ استراتيجية متزامنة ومتنوعة، محلية ودولية للتخفيف من أثارها المتزايدة على المجتمع والدولة. وهذه الاستراتيجية تتوزع على عدة محاور:

أولاً: المحور التقني

التقنيات وتدابير الحماية هي خط الدفاع الأول في مواجهة تحديات الامن الالكتروني والسيبراني وذلك عبر سلسلة من التقنيات مثل التشفير وجدران الحماية وأنظمة كشف/منع التسلل بالإضافة إلى أمن الشبكات اللاسلكية وتعزيز دور المصادقة متعددة العوامل وإدارة الهوية والبيانات الشخصية.

ثانياً. تشريعات ولوائح الأمن السيبراني

أ. القوانين واللوائح الوطنية عبر تعزيز مبدأ المسؤولية الفردية والجنائية وتعزيز المنظومات العقابية بعقوبات محدثة وصارمة تجاه أي تهديدات تتعلق بالفضاء السيبراني.

ب. هناك أيضاً دور للبرلمان والجهات الحكومية والهيئات الرقابية في تعزيز الأمن السيبراني، بما في ذلك إدخال القوانين واللوائح التنظيمية لحماية البيانات الشخصية والبنية التحتية الحيوية⁽²⁾.

ج. التشريعات والاتفاقيات على المستويات الإقليمية والدولية باعتبار أن مخاطر الإنترنت وتهديدات الأمن السيبراني تتجاوز الحدود الوطنية والمحلية.

ثالثاً: دور الشركات

يتعين على الشركات إعادة التفكير في نهجها تجاه الأمن السيبراني وتوقع التهديدات المحتملة. وذلك عبر تنفيذ تدابير فعالة للأمن السيبراني لحماية أنشطتها من هذه

(1) تركيز على ادارة مخاطر الاعمال - مقالة بالفرنسية منشورة في موقع ادارة المخاطر، على الرابط:

<https://www.c-risk.com/fr/blog/gestion-des-risques>

(2) تهديدات رئيسية، مقالة على الموقع الرسمي للوكالة الوطنية الفرنسية لأمن وحماية أنظمة المعلومات، على الرابط:

<https://www.ssi.gouv.fr/entreprise/principales-menaces>

التهديدات. ويشمل ذلك جدران الحماية ومكافحة الفيروسات وأنظمة كشف التسلل وسياسات الأمان الصارمة. يجب على هذه الشركات أيضاً تدريب موظفيها على الأمن السيبراني ووضع العمليات اللازمة لاكتشاف الحوادث الأمنية والاستجابة لها.

رابعاً: دور المجتمع المدني والأفراد:

وهذا الدور يتنوع، من ضرورة نشر الثقافة الرقمية وسبل الوقاية إلى التوعية والتعليم في مجال الأمن السيبراني للأفراد إلى برامج التدريب والتعليم للموظفين في مجال الأمن السيبراني.

ويدرك الأفراد أيضاً بشكل متزايد أهمية الأمن السيبراني لحماية خصوصيتهم وبياناتهم الشخصية⁽¹⁾.

خامساً: جذب الاستثمارات التقنية والرقمية:

لن تكون هناك فعالية في مواجهة التحديات السيبرانية والرقمية الحديثة ما لم تكن هناك بنية تحتية رقمية جاهزة للدولة والمجتمع والمؤسسات. وفي هذا الصدد يأتي دور الدولة في ضخ استثمارات كبيرة في تطوير البنية المعلوماتية التحتية لمؤسساتها وأيضاً في سن تشريعات تقدم إعفاءات ضريبية على كل الاستثمارات في المجال الرقمي من أجل جذبها للاستثمار في البنية التحتية للبلد وتعزيز قدراتها الرقمية في الابداع والوقاية من التهديدات⁽²⁾.

وبصفة عامة هناك خطوات بسيطة تساعد في الحفاظ على مستوى جيد في مستوى جيد من الأمان والسلامة السيبرانية وهي:

1- الموثوقية: وتعني استخدام المواقع الموثوق بها عند تقديم معلومات شخصية والقاعدة الأساسية هي التحقق من عنوان URL ، وإذا كان الموقع يتضمن https في بدايته، فهذا يعني أنه موقع آمن، أما إذا كان عنوان URL يحتوي على http بدون

(1) الأمن السيبراني، تحدي أساسي للشركات في العام 2023م، مقالة على الرابط:

<https://www.fibre-pro.fr/cybersecurite>

(2) أنظر: الأمن السيبراني، مجلة الأمن السياسي، مجلة صادرة عن الجهاز المركزي للأمن السياسي بالجمهورية اليمنية العدد(11)، أكتوبر 2023م ص11

s؛ فيجب الحذر من إدخال أي معلومة حساسة مثل بيانات بطاقات الائتمان، أو رقم التأمين الاجتماعي الخ.

2- البريد الاحتيالي: ويعني عدم مرفقات البريد الإلكتروني أو النقر فوق رابط الرسائل من المصادر غير معروفة، إذ إن إحدى الطرق الأكثر شيوعاً التي يتعرض فيها الأشخاص للسرقة أو الاختراق هي عبر رسائل البريد الإلكتروني المتخفية على أنها رسالة من شخص موثوق به.

3- التحديثات (Always up-to-date) وتعني الحرص دائماً على تحديثات الأجهزة، فغالباً ما تحتوي تحديثات البرامج على تصحيحات مهمة لإصلاح مشكلات الأمان، وإن هجمات المخترقين الناجحة تتركز في الأجهزة القديمة بنسبة كبرى، والتي لا تمتلك برامج الأمان.

4- النسخ الاحتياطي: ويتطلب هذا عمل نسخة احتياطية من الملفات بانتظام لمنع هجمات الأمان على الإنترنت⁽¹⁾.

المبحث السادس

(1) أنظر: منى عبد الله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مرجع سابق، ص16.

الذكاء الاصطناعي وأثره على الأمن السيبراني

يشهد الأمن السيبراني تحولاً كبيراً بفضل الذكاء الاصطناعي (AI)، فقد يؤثر الذكاء الاصطناعي على الأمن السيبراني آثار إيجابية أو سلبية، فمن الناحية الإيجابية يعمل الذكاء الاصطناعي على تحسين التدابير الأمنية من خلال السماح بتحديد التهديدات في الوقت الحقيقي والتخفيف من آثارها، وأنظمة الاستجابة الآلية، والتحليلات التنبؤية. أما من الناحية السلبية، فيمكن للمهاجمين استغلال الذكاء الاصطناعي لتطوير أساليب هجمات أكثر تطوراً وتعقيداً، كما يمكن أن يتيح لهم استخدام تقنيات التعلم الآلي لتحليل البيانات واكتشاف الثغرات والأنماط غير المألوفة في الأنظمة السيبرانية، وهذا يجعل من الصعب اكتشاف هذه الهجمات بسبب تعقيد الأساليب المستخدمة، وهناك العديد من الآثار الإيجابية والسلبيات الذي يحدثها الذكاء الاصطناعي في الأمن السيبراني، وعليه سنقوم بتقسيم هذا المبحث إلى المطالب التالية:

- 1- المطلب الأول: الذكاء الاصطناعي ومشروعيته الدولية.
- 2- المطلب الثاني: الآثار الإيجابية والسلبيات الذي يحدثها الذكاء الاصطناعي في الأمن السيبراني.

المطلب الأول

الذكاء الاصطناعي ومشروعيته الدولية

من أهم مآثر التقدم التقني -في المجال الرقمي- ما قدمته البشرية من نوع مستحدث متطور من الذكاء يقوم إلى جانب الذكاء البشري المعتاد، ألا وهو (الذكاء الاصطناعي) الذي يمثل في تقنيات إلكترونية رقمية متقدمة تهدف إلى إكساب الآلات والأجهزة ذكاءً تقنيًا اصطناعيًا وليس طبيعيًا، يمكنها من محاكاة الإنسان في الكثير من مجالات الحياة، وأنشطتها المختلفة، ومن ضمنها الأنشطة والأعمال القانونية⁽¹⁾.

وعليه سوف نقسم هذا المطلب إلى الفرعين التاليين:

1- الفرع الأول: مفهوم الذكاء الاصطناعي.

2- الفرع الثاني: موقف القانون الدولي من الذكاء الاصطناعي.

الفرع الأول

مفهوم الذكاء الاصطناعي

فالذكاء الاصطناعي هو: قدرة الكمبيوتر الرقمي، أو الروبوت على أداء معظم المهام المختلفة التي تستطيع الكائنات الذكية القيام بها مثل: القدرة على التفكير، أو تحليل المعاني واكتشافها، أو التعلم من التجارب السابقة، فمنذ تطوير جهاز الحاسوب في أربعينيات القرن الماضي ثبت أنه يمكن برمجة أجهزة الحاسوب للقيام بمهام معقدة، وسوف نستعرض في هذا المطلب أهم مجالات الذكاء الاصطناعي.

الذكاء الاصطناعي هو مجال واسع من علوم الكمبيوتر ونظم المعلومات، يتعامل مع إنشاء آلات قادرة على أداء المهام التي تتطلب عادةً الذكاء البشري. مثل: التعلم، والتفكير، وحل كثير من للمشاكل⁽²⁾.

والذكاء الاصطناعي (AI) ARTIFICIAL INTELLIGENCE: يمثل فرعًا من فروع علم الحاسب الآلي، يقوم على قدرات التعلم العميق، والمعرفة، والتفكير المنطقي،

(1) أنظر د. إبراهيم الدستوقي أبو الليل، العقود الذكية والذكاء الاصطناعي ودورها في أتمتة العقود والتصرفات القانونية، مجلة الحقوق، جامعة الكويت 2020م، ص21.

(2) أنظر الموقع الإلكتروني:

<https://maltem.com/en/blog/ia-service-cyber-secureite>

والتخطيط، والإدراك، ليصل به الإنسان إلى جعل الآلة الجامدة الصماء قادرة على تقليد فكرة، ومحاكاة مهاراته المختلفة، فالذكاء الاصطناعي، غير الذكاء البشري أو الإنساني، مواز له ويعتمد عليه، ويُعبّر عن قدرة الآلات والأجهزة بما يلحقها من برامج إلكترونية متقدمة، على القيام بأعمال وتصرفات وإجراءات مختلفة لتحقيق تصرفات معينة، والوصول إلى بعض الاستنتاجات، واتخاذ قرارات بطريقة آلية وذاتية، ومستقلة عن التدخل البشري⁽¹⁾.

ويتم التركيز في برمجة الذكاء الاصطناعي على أربع مهارات، هي: (التعلم)، و(الإدراك) و(التصحيح الذاتي)، و(الابتكار).

1-يركز جانب التعلم على الحصول على البيانات وإيجاد القوانين والروابط بينها وتحويلها إلى بيانات مفيدة، ويتم تقديم قوانين مختلفة على شكل خوارزميات Algorithm كثيرة (الخوارزمية هي: نهج عمل برنامج ما لتحقيق الهدف المرغوب) حول كيفية إكمال مهمة محددة، مثل: التعرف على وجود إنسان في صورة (يجب تحديد ما يصف شكل معظم البشر: العينان والفم والأنف والحاجبان والرقبة، وهكذا).

2-وبالنسبة إلى مهارة الإدراك، فإنها تركز على اختيار الخوارزمية الصحيحة بقوانينها المرتبطة لتحقيق الهدف المرغوب.

3-أما التصحيح الذاتي، فتركز هذه المهارة على تعديل الخوارزميات وقوانينها بناءً على صحة المخرجات لإيجاد قوانين أكثر دقة من السابق، الأمر الذي ستنجم عنه نتائج صحيحة بنسبة أعلى في المرات المقبلة التي يعمل فيها ذلك النظام.

وتبقى المهارة الرابعة وهي: الابتكار، التي تستخدم الشبكات العصبونية Neural Networks الرقمية، والنظم المبنية على القوانين والبيانات الإحصائية، وتقنيات أخرى بهدف إيجاد صور ونصوص، وموسيقى، وأفكار جديدة.

ولعلكم قد سمعتم عن بعض المفردات التقنية المتقاربة، مثل: الذكاء الاصطناعي Artificial Intelligence، وتعلم الآلة Machine Learning، والتعلم العميق Deep Learning.

تحتاج هذه النظم إلى تحليل كميات كبيرة جداً من بيانات التدريب، وإيجاد روابط بين تلك البيانات واستخدامها لتوقع أمور مقبلة، مثل: تحليل ملايين الصور لفهم ما الذي يُميّز الإنسان عن النبات، عن الحيوان، عن الجماد، وما الطبيعة؟ وما العائلة؟ وكيف يمكن تمييز الليل عن النهار، والخيال عن الحقيقة؟

(1) أنظر د. إبراهيم الدستوقي أبو الليل، العقود الذكية والذكاء الاصطناعي ودورها في أتمتة العقود والتصرفات القانونية، مرجع سابق، ص21.

وبينما يُعرّف الذكاء الاصطناعي بأنه: "محاكاة الآلات للذكاء البشري لتحقيق هدف ما"

فإن تعلم الآلة يُعرّف بأنه: "رفع دقة البرامج والتطبيقات في توقع النتائج بناءً على البيانات السابقة من دون برمجتها بشكل مباشر على كيفية القيام بذلك، حيث تتم هذه العملية من دون تدخل المبرمجين"، ذلك أن النظام سيتعرف على الروابط بين البيانات ويستخدمها في التوقع.

أما التعلم العميق، فهو "جزء متخصص من تعلم الآلة مبني على فهمنا لتركيبية الدماغ البشري". وبسبب استخدام التعلم العميق لبنية الشبكات العصبونية الرقمية أخيراً، تم إيجاد تقنيات حديثة مفيدة جداً للبشر، مثل: القيادة الذاتية للسيارات ChatGPT⁽¹⁾. كم يجب التنويه بأن الذكاء الاصطناعي يقوم على أساساً افتراضي مبدئي مبناه: أن ملكة الذكاء لدى الإنسان يمكن وصفها بدرجة تمكن الآلة من محاكاته، ومن ثم اقتحام النشاط الإنساني بما يتضمنه من ذكاء وحنكة ظلاً إلى وقت قريب مقصورين عليه، ومن ثم القيام بما يقوم به السلوك البشري، وبذلك أصبحت الآلة قادرة ذاتياً واستقلالاً، على التعلم والقيام بالكثير من القدرات الذهنية البشرية وأنماط عملها. وبذلك، وبفضل الذكاء الاصطناعي، أمكن الاستعاضة بذكاء وتفكير البشر – في العديد من المجالات – ذكاء الآلة – بعد أن كانت مجرد متفوقة عليهم أحياناً.

وإذا كانت الثورتان الصناعيتان (الأولى) و(الثانية) قد تمكنتا من استبدال الآلات بعضلاتنا، فإن الثورة الرقمية الحالية استعاضت بالذكاء الإنساني الطبيعي "الذكاء الآلي الاصطناعي" في الكثير من أوجه الحياة⁽²⁾

وبسبب غموض مفهوم الذكاء الاصطناعي، لم يوضع – حتى الآن – تعريف محدد له، لكن يمكننا تعريفه من خلال ما سبق بأنه: "أحد علوم الحاسوب الحديثة التي تبحث عن أساليب متطورة البرمجة للقيام بأعمال واستنتاجات تشابه ولو في حدود ضيقة تلك الأساليب التي تسبب لذكاء الإنسان، فهو: علم يبحث في تعريف الذكاء الإنساني وتحديد أبعاده، ومن ثم محاكاة بعض خواصه، كالتعلم...

ومن خلال هذه التعريفات نصل إلى أن الذكاء الاصطناعي ما هو إلا محاولة لجعل الحواسيب تحاكي الذكاء الإنساني إلى حد ما، دون أن نغفل أن الحاسوب يتعامل مع

(1) أنظر صحيفة الشرق الأوسط السعودية على الموقع الإلكتروني:

<https://aawsat.com/%D9%81%D9%8A-%D8%A7%D9%84%D8%B9%D9%85%D9%82/%D8%AA%D8%AD%D9%82%D9%8A%D9%82%D8%A7%D8%AA-%D9%88%D9%82%D8%B6%D8%A7%D9%8A%D8%A7/4368481-%D9%85%D8%A7-%D9%87%D9%88-%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1-%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A-%D9%88%D9%83%D9%8A%D9%81-%D9%8A%D8%B9%D9%85%D9%84%D8%9F>

(2) أنظر د. إبراهيم الدسوقي أبو الليل: "العقود الذكية والذكاء الاصطناعي ودورها في أتمتة العقود والتصرفات القانونية"، مرجع سابق، ص 21، 22.

ارقام فهو لا يفكر ولا يدرك، ولذلك نجد الحاسوب رغم قدراته الفائقة في القيام ببعض العمليات الرياضية المعقدة، إلا أنه يعجز أحياناً على القيام ببعض العمليات البسيطة التي يقوم بها الطفل، لذلك فمحاكاة الذكاء الإنساني والاستنباط واتخاذ القرارات⁽¹⁾ الكلية لن تكون، وإنما في بعض خصائصه، لهذا أهتم الباحثون بهذا المجال بالتركيز على هدفين رئيسيين هما:

(محاولة كيف يعالج العقل المعلومات المكتسبة)، و(محاولة فهم الأسس العامة للذكاء)⁽²⁾.

الفرع الثاني

موقف القانون الدولي من الذكاء الاصطناعي

اعتمد "المجلس الأوروبي" أول اتفاقية دولية ملزمة قانوناً على الإطلاق تهدف إلى ضمان احترام حقوق الإنسان وسيادة القانون والمعايير القانونية للديمقراطية عند استخدام أنظمة الذكاء الاصطناعي. وتتضمن المعاهدة، التي تتيح انضمام الدول غير الأوروبية أيضاً، إطاراً قانونياً يشمل دورة حياة أنظمة هذا الذكاء بأكملها، ويعالج المخاطر التي قد تشكلها، مع تعزيز الابتكار المسؤول.

وتتبنى الاتفاقية نهجاً قائماً على المخاطر لتصميم وتطوير واستخدام وإيقاف تشغيل أنظمة الذكاء الاصطناعي، والذي يتطلب النظر بعناية في أي عواقب سلبية محتملة لاستخدام أنظمتها.

وتم اعتماد «اتفاقية إطار مجلس أوروبا بشأن الذكاء الاصطناعي وحقوق الإنسان والديمقراطية وسيادة القانون» في ستراسبورغ خلال الاجتماع الوزاري السنوي للجنة الوزارية لمجلس أوروبا في 71 مايو 2024م، والذي يجمع وزراء خارجية الدول الأعضاء الـ 46 في المجلس.

وصرحت الأمانة العامة لمجلس أوروبا، ماريا بيجسينوفيتش، قائلة: «اتفاقية إطار الذكاء الاصطناعي هي معاهدة عالمية الأولى من نوعها تضمن التزام الذكاء الاصطناعي بحقوق الإنسان. إنها استجابة للحاجة إلى معيار قانوني دولي تدعمه دول في قارات مختلفة تشارك القيم نفسها للاستفادة من مزاياه مع تخفيف المخاطر. من

(1) أنظر: سناء منعم: "اللسانيات الحاسوبية والترجمة الآلية"، عالم الكتاب الحديث، ط1، ص84.

(2) أنظر: عادل عبد النور، مدخل إلى عالم الذكاء الاصطناعي، دار النشر مدينة الملك عبد العزيز للعلوم والتقنية، السعودية، ص7.

خلال هذه المعاهدة الجديدة، نهدف إلى ضمان استخدام مسؤول للذكاء الاصطناعي يحترم حقوق الإنسان، وسيادة القانون، والديمقراطية».

وتعد الاتفاقية نتاج عمل لمدة عامين من قبل هيئة حكومية دولية، هي "لجنة الذكاء الاصطناعي"، والتي أجمعت لصياغة المعاهدة الدول الأعضاء الـ 46 في مجلس أوروبا والاتحاد الأوروبي و11 دولة غير عضو، بالإضافة إلى ممثلين عن القطاع الخاص والمجتمع المدني والأوساط الأكاديمية الذين شاركوا كمراقبين⁽¹⁾.

وذكر المجلس في بيان له، أن "الاتفاقية الإطارية لمجلس أوروبا بشأن الذكاء الاصطناعي وحقوق الإنسان والديمقراطية وسيادة القانون"، التي تم اعتمادها في ستراسبورغ خلال الاجتماع الوزاري السنوي للجنة وزراء المجلس، وتجمع وزراء خارجية الدول الـ 46 الأعضاء في مجلس أوروبا، تضع إطاراً قانونياً ينطبق طوال دورة حياة أنظمة الذكاء الاصطناعي.

وأضاف البيان: أن الاتفاقية المفتوحة أيضاً للتوقيع من قبل الدول غير الأوروبية، تتناول المخاطر التي يمكن أن تمثلها هذه الأنظمة، وتشجع الابتكار المسؤول، مشيراً إلى أن الاتفاقية تتبع نهجاً قائماً على المخاطر في تصميم أنظمة الذكاء الاصطناعي، وتطويرها، واستخدامها، وإيقاف تشغيلها، ما يتطلب "دراسة متأنية لأي عواقب سلبية محتملة مرتبطة باستخدام هذه الأنظمة".

وينطبق النص على: استخدام أنظمة الذكاء الاصطناعي من قبل السلطات العامة، بما في ذلك الشركات التي تعمل بالنيابة عنها، ومن قبل الجهات الخاصة، كما يحدد متطلبات الشفافية والرقابة المصممة خصيصاً لسياقات ومخاطر محددة، بما في ذلك: تحديد المحتوى الناتج عن الذكاء الاصطناعي.

وستحتاج الأطراف في الاتفاقية إلى تحديد المسؤوليات، وإنشاء المساءلة عن التأثيرات السلبية، والتأكد من احترام أنظمة الذكاء الاصطناعي للمساواة، وضمان حظر التمييز، وحماية الحياة الخاصة، علاوة على توفير سبل الانتصاف، والضمانات الإجرائية لضحايا انتهاكات حقوق الإنسان في استخدام أنظمة الذكاء الاصطناعي.

وتلزم المعاهدة أيضاً الأطراف: بتبني تدابير لضمان عدم استخدام الذكاء الاصطناعي لتقويض المؤسسات والعمليات الديمقراطية، بما في ذلك: مبادئ الفصل بين السلطات، واستقلال القضاء والولوج إلى العدالة⁽¹⁾.

(1) أنظر صحيفة الشرق الأوسط السعودية على الرابط الإلكتروني:

<https://aawsat.com/%D8%A7%D9%84%D8%A7%D9%82%D8%AA%D8%B5%D8%A7%D8%AF/5021709-%D8%A3%D9%88%D8%B1%D9%88%D8%A8%D8%A7-%D8%AA%D8%B9%D8%AA%D9%85%D8%AF>

(1) أنظر وكالة الأنباء العمانية على الموقع الإلكتروني:

<https://omannews.gov.om/topics/ar/86/show/433504/ona#:~:text=%D9%88%D8%B0%D9%83%D8%B1%20%D8%A7%D9%84%D9%85%D8%AC%D9%84%D8%B3%20%D9%81%D9%8A%20%D8%A8%D9%8A>

وفيما يتعلق بالمخاطر التي تهدد الديمقراطية، تطلبُ المعاهدةُ من الأطراف: اعتماد تدابير لضمان عدم استخدام أنظمة الذكاء الاصطناعي لتقويض المؤسسات والعمليات الديمقراطية، بما في ذلك مبدأ الفصل بين السلطات واحترام استقلال القضاء والوصول إلى العدالة.

ولن يُطلب من الأطراف في الاتفاقية: تطبيق أحكام المعاهدة على الأنشطة المتعلقة بحماية مصالح الأمن القومي، ولكنها ستكون ملزمة بضمان احترام هذه الأنشطة للقانون الدولي والمؤسسات والعمليات الديمقراطية.

ولن تنطبق الاتفاقية على: شؤون الدفاع الوطني، ولا على أنشطة البحث والتطوير، إلا عندما يكون لاختبار أنظمة الذكاء الاصطناعي القدرة على التدخل في حقوق الإنسان أو الديمقراطية أو سيادة القانون.

ومن أجل ضمان تنفيذها الفعال، تنشئ الاتفاقية آلية للمتابعة في شكل (مؤتمر للأطراف).

وأخيراً، تشترط الاتفاقية: أن يقوم كل طرف بإنشاء آلية رقابة مستقلة للإشراف على الامتثال للاتفاقية، ورفع مستوى الوعي، وتحفيز النقاش العام المستنير، وإجراء مشاورات بين أصحاب المصلحة المتعددين حول كيفية استخدام تكنولوجيا الذكاء الاصطناعي.

وتم فتح الاتفاقية الإطارية للتوقيع في فيلنيوس (ليتوانيا) في 5 سبتمبر (أيلول) بمناسبة انعقاد مؤتمر وزراء العدل⁽²⁾.

المطلب الثاني

الآثار الإيجابية والسلبية التي يحدثها الذكاء الاصطناعي في الأمن السيبراني

اعتادت الدول على مدار التاريخ أن تعتمد على العنصر البشري في تحقيق الأمن السيبراني، عبر جمع المعلومات، وتشديد الرقابة، ومطاردة التهديدات، وسد الثغرات،

(2) أنظر: د/ جلال فضل محمد العودي، الذكاء الاصطناعي واستخدامه في الجرائم الإلكترونية، بحث مقدم للأمانة العامة لوزراء الداخلية العرب، تونس 2024م، ص14 وما بعدها.

والاستجابة لأي احتمالات بشأن وقوع حوادث سيبرانية، ولكن في العقد الأخير، تطوّر الذكاء الاصطناعي بشكل كبير بفضل تقنية تسمى بالتعلم العميق Deep Learning، تعطي الذكاء الاصطناعي القدرة على الاستنباط والتفكير بشكل مستقل، وتعليم نفسه بنفسه، وتحرره من أكلال "الذكاء الاصطناعي الضيق"، والذي يعني مجرد برمجة آلة لتقوم بوظيفة معينة دون تفكير.

وكان للذكاء الاصطناعي دور إيجابي، وسلبى على الأمن السيبراني نوضحها من خلال تقسيم هذا المطلب إلى الفروع التالية:

الفرع الأول: إيجابيات الذكاء الاصطناعي على الأمن السيبراني.

الفرع الثاني: سلبيات الذكاء الاصطناعي على الأمن السيبراني.

الفرع الثالث: فوائد الذكاء الاصطناعي (AI) في إدارة مخاطر الأمن السيبراني

الفرع الأول

إيجابيات الذكاء الاصطناعي على الأمن السيبراني

للذكاء الاصطناعي دور مهم في الأمن السيبراني تبرز من خلال:

1- الكشف المبكر عن التهديدات

يساهم الذكاء الاصطناعي في اكتشاف الهجمات الإلكترونية بسرعة فائقة، حيث يمكنه مسح كميات هائلة من البيانات في وقت قصير، والتعرف على الأنماط غير الطبيعية التي قد تدل على محاولات اختراق وتتفوق أنظمة الذكاء الاصطناعي على الأنظمة التقليدية بفضل قدرتها على التعلم الآلي، والذي يتيح لها تحديد التهديدات الجديدة بناءً على الأنماط دون الحاجة لتدخل بشري مستمر⁽¹⁾.

2- تعزيز أمن المؤسسات: يضع الذكاء الاصطناعي نهجاً ديناميكياً بحماية كلمة المرور وأمن حساب المستخدم عبر اللجوء إلى بصمات الوجه والأصابع، خاصة في ظل توسع العمل عن بعد وتزايد مخاطر الهجمات الإلكترونية، ووقوع الحلول التقليدية في خطأ الاكتفاء بالكشف عن الاختراقات التقليدية والشبكات الافتراضية الخاصة "VPN"، وترك أمان نقاط النهاية عرضة للخطر (الكشف عن برامج الفدية، وتشفيرها قبل الوصول للمستخدم).

(1) أنظر:

Kumar, R. (2020). Machine Learning for Early Threat Detection. Cyber Threat Analysis, 6(1), 23-37

3- تخفيف حدة التهديدات: يعمل الذكاء الاصطناعي على إنشاء استجابات مبكرة للتهديدات السببرانية المتوافقة، مع حركة مرور شبكة الإنترنت واتصالات البريد الإلكتروني، لذا يتم إطلاق تدابير استجابة استباقية تلقائياً، وحظر حركة المرور الضارة، وعزل الملفات المهددة لأمن المؤسسات والأفراد.

4- تقييم الثغرات الأمنية: الذكاء الاصطناعي لديه قدرة على تحديد أولويات التهديدات، ومدى خطورة كل ثغرة وتأثيرها، الأمر الذي يسهل على فريق الأمان من تركيز جهوده لمعالجة المخاطر الأشد والأكثر ضرراً.

5- تبسيط العمليات الأمنية: رغم ارتكاز الذكاء الاصطناعي على خوارزميات التعلم الآلي المتقدمة لأتمتة العمليات الأمنية، إلا أن معالجتها تتم بشكل مبسط لتحديد التهديدات عالية الخطورة عبر التحليل، لتعزيز القدرات الأمنية للدول والمؤسسات بشأن مواجهة أي أنشطة احتيالية(1).

6- التحليلات التنبؤية: واحدة من أبرز ميزات الذكاء الاصطناعي هي قدرته على التعلم من التجارب السابقة، مما يجعله أكثر كفاءة في مواجهة التهديدات المستقبلية. يمكن للذكاء الاصطناعي تطوير نماذج الدفاعية تلقائياً، بناءً على تحليل الهجمات السابقة، مما يزيد من فعاليته في التصدي للتهديدات الجديدة(2).

7- الاستجابة التلقائية والفورية

يمكن للأنظمة المعتمدة على الذكاء الاصطناعي اتخاذ قرارات فورية عند اكتشاف تهديد محتمل، مثل: عزل الجهاز المصاب أو حظر عنوان IP مشبوه، مما يقلل من الوقت المتاح للمهاجم لتنفيذ الهجوم هذه السرعة في الاستجابة تقلل من الأضرار المحتملة، وتساهم في حماية البيانات بشكل أفضل(3)

الفرع الثاني

(1) انظر: بون - المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات ECCI - على الموقع الإلكتروني:

<https://www.europarabct.com/%D8%A3%D9%85%D9%86-%D9%82%D9%88%D9%85%D9%8A-%D9%80-%D8%AF%D9%88%D8%B1-%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1-%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A-%D9%81%D9%8A-%D8%A7%D9%84>

(2) أنظر:

Chen, L., Wang, T., & Yang, Z. (2022). Learning from Previous Attacks: AI's Role in Proactive Cybersecurity. Journal of Cyber Intelligence, 8(1), 73-89

(3) أنظر:

Johnson, D., & Smith, A. (2019). The Automated Response of AI in Cybersecurity. IT Security Research, 11(3), 99-114

سلبات الذكاء الاصطناعي على الأمن السيبراني

تتزايد تحديات الأمن السيبراني مع تقدم التكنولوجيا، خاصة مع تطور الذكاء الاصطناعي.

ويعزى ذلك إلى أن الذكاء الاصطناعي (AI) قد يسهم في تعزيز قدرات الهجمات السيبرانية وجعلها أكثر تطوراً وتعقيداً، في الوقت الذي يُمكن أن يُستخدم أيضاً في رفع إمكانيات مواجهة تلك التهديدات من ناحية أخرى، كسلاح ذو حدين.

فيمكن للمهاجمين استغلال الذكاء الاصطناعي لتطوير أساليب هجمات أكثر تطوراً وتعقيداً، كما يمكن أن يتيح لهم استخدام تقنيات التعلم الآلي لتحليل البيانات واكتشاف الثغرات والأنماط غير المألوفة في الأنظمة السيبرانية، وهذا يجعل من الصعب اكتشاف هذه الهجمات بسبب تعقيد الأساليب المستخدمة⁽¹⁾.

وقد يستخدم تطبيق الذكاء الاصطناعي في مجال المراقبة أو الأمن الإلكتروني للأمن القومي وجهة هجوم إلكتروني جديدة قائمة على هذا الضعف في ماهية البيانات المغذية.

وقد يتعلم الخصوم كيفية تغذية نظم المراقبة العاملة بالذكاء الاصطناعي بمعلومات مضللة بشكل سري وعن غير قصد. وسبق أن بدأت الأعمال الحديثة تبين قابلية تنفيذ مثل هذه الهجمات السامة المستندة إلى التدريب لاستهداف نظم كشف البرامج الضارة القائمة على تعلم الآلة. ويقدم فساد خدمة الدردشة الذكية (تشات بوت) القائمة على الذكاء الاصطناعي من مايكروسوفت برهاناً واسع النطاق لهذا النوع من الهجمات على نظام ذكاء اصطناعي تجاري، ويمكن أن يفسح ذلك فرصة لعمليات مكافحة التجسس في الشبكات، فقد أفادت وكالات الاستخبارات الأمريكية أنها تعتقد أن دورة الانتخابات الأمريكية التي انعقدت عام 2016م تعرّضت لتدخل اجنبي تجاوز حده من خلال هجمات إلكترونية خارجية. وتتمثل هذه الهجمات بشكل إصدارات عامة انتقائية لبيانات خاصة مسربة في محاولة للتأثير على آراء الناخبين الأمريكيين⁽²⁾.

وبصفة عامة يمكننا أن نقول: أن مخاطر الذكاء الاصطناعي على الأمن السيبراني تتمثل على بالآتي:

1- التحيز وإمكانية الوقوع في الخطأ

(1) أنظر:

<https://www.skynewsarabia.com/business/1646519-%D8%A7%D9%94%D8%A8%D8%B1%D8%B2-%D8>

(2) أنظر: أ. أوسوبا أوسوندي، وبلسر الرابع وويليام، مخاطر الذكاء الاصطناعي على الأمن ومسقبل العمل، راند، ص 5، 6.

تعتمد أنظمة الذكاء الاصطناعي على البيانات المقدمة لها، وقد تؤدي الأخطاء أو التحيزات في البيانات إلى اتخاذ قرارات غير دقيقة، مما قد يؤدي إلى الكشف عن تهديدات وهمية أو تجاهل تهديدات حقيقية. يمكن للأنظمة أن تكون عرضة للتحيز في حالة الاعتماد على بيانات غير كافية أو غير دقيقة، وهذا قد يؤثر على فعالية النظام في مكافحة الهجمات⁽¹⁾.

2- سباق التسلح بالذكاء الاصطناعي

عندما يتعلق الأمر بالذكاء الاصطناعي والأمن القومي، فإن السرعة هي النقطة المهمة، لكنها أيضا المشكلة. ولأن أنظمة الذكاء الاصطناعي تمنح مستخدميها مزايا سرعة أكبر فإن الدول التي تطور أولا تطبيقات عسكرية تكتسب ميزة إستراتيجية، لكن في المقابل قد يكون بهذا الأمر خطورة بالغة قد يتسبب بها أصغر عيب في النظام، والذي يمكن للمخترقين استغلاله، وقد تؤدي الحاجة الملحة للفوز بسباق التسلح بالذكاء الاصطناعي إلى عدم كفاية تدابير السلامة، مما يزيد من احتمالية إنشاء أنظمة ذكاء اصطناعي ذات عواقب غير مقصودة وربما كارثية.

3- قد يؤدي إلى حرب نووية.

قد يميل قادة الأمن القومي إلى تفويض قرارات القيادة والتحكم للذكاء الاصطناعي ويلغون الإشراف البشري على نماذج التعلم الآلي التي لا نفهمها تماما، من أجل الحصول على ميزة السرعة. وفي مثل هذا السيناريو، حتى الإطلاق الآلي لأنظمة الدفاع الصاروخي التي تبدأ دون إذن بشري يمكن أن يؤدي إلى تصعيد غير مقصود، وربما يؤدي إلى حرب نووية⁽²⁾.

4- شن هجمات إلكترونية.

مع تزايد تطور التكنولوجيا، يمكن للقراصنة استخدام الذكاء الاصطناعي لأغراض هجومية، مثل تطوير برمجيات خبيثة قادرة على تجاوز الأنظمة الأمنية التقليدية.

(1) أنظر:

Evans, M., & Lee, S. (2021). Bias and Errors in AI-based Cyber Defense Systems. Journal of Cyber Ethics, 3(4), 15-29

(2) أنظر: الموقع الإلكتروني لقناة الجزيرة على الرابط الإلكتروني:

<https://www.aljazeera.net/tech/2023/6/11/%d9%85%d8%b3%d8%aa%d9%82%d8%a8%d9%84-%d8%a7%d9%84%d8%b0%d9%83%d8%a7%d8%a1-%d8%a7%d9%84%d8%a7%d8%b5%d8%b7%d9%86%d8%a7%d8%b9%d9%8a-%d9%85%d8%a7-%d9%87%d9%8a-%d8%a3%d8%b3%d9%88%d8%a3>

فعلى سبيل المثال، يمكن للذكاء الاصطناعي مساعدة المهاجمين في إنتاج هجمات تصيد إلكتروني دقيقة وموجهة، تعتمد على البيانات الشخصية للضحايا⁽¹⁾.

فخطر الهجمات السيبرانية المدعومة بالذكاء الاصطناعي يتزايد بشكل كبير. لا يتم استخدام الذكاء الاصطناعي والتعلم الآلي من قبل متخصصي أمن تكنولوجيا المعلومات فحسب، بل يتم نشرهما من قبل الجهات الفاعلة التي ترعاها الدولة والمنظمات السيبرانية الإجرامية⁽²⁾.

5- نهاية الخصوصية والإرادة الحرة

مع كل إجراء رقمي نتخذه فإننا ننتج بيانات جديدة: رسائل البريد الإلكتروني، النصوص، ما نُحَمِّله من الإنترنت، المشتريات، المنشورات، صور السلفي، مواقع "جي بي إس". ومن خلال السماح للشركات والحكومات بالوصول غير المقيد إلى هذه البيانات، فإننا نسلمها أدوات المراقبة والتحكم.

ومع إضافة التعرف على الوجه، القياسات الحيوية، البيانات الجينية، التحليل التنبئي المدعوم بالذكاء الاصطناعي، فإننا ندخل منطقة خطرة ومجهولة مع تنامي المراقبة والتتبع من خلال البيانات دون أي فهم تقريبا للآثار المحتملة.

وتمتد قوة البيانات، بمجرد جمعها وتحليلها، إلى ما هو أبعد من وظائف المراقبة. فاليوم، تتنبأ الأنظمة التي تدعم الذكاء الاصطناعي بالمنتجات التي سنشتريها، الترفيه الذي سنشاهده، الروابط التي سننقر عليها. فعندما تعرفنا هذه المنصات بشكل أفضل مما نعرف أنفسنا، فقد لا نلاحظ الزحف البطيء الذي يسلبنا إرادتنا الحرة ويخضعنا لسيطرة القوى الخارجية⁽³⁾.

6 - الاعتماد المفرط على الذكاء الاصطناعي

يمكن أن يؤدي الاعتماد المفرط على أنظمة الذكاء الاصطناعي إلى تقليل دور الكوادر البشرية في الأمن السيبراني، مما يجعل الشركات عرضة للتهديدات في حال حدوث

(1) أنظر:

Miller, K. (2020). AI-driven Cyber Attacks: A New Wave of Threats. Hacker's Quarterly, 14(2), 40-52
(2) أنظر: د. جلال فضل محمد العودي، مخاطر الذكاء الاصطناعي على الأمن السيبراني، بحث مقدم للندوة العلمية (التعاون الدولي في قضايا الأمن السيبراني المنعقدة في معهد القضاء الأردني تاريخ 16 ديسمبر 2024م، ص19، 20.

(3) أنظر: الموقع الإلكتروني لقناة الجزيرة على الرابط الإلكتروني:

<https://www.aljazeera.net/tech/2023/6/11/%d9%85%d8%b3%d8%aa%d9%82%d8%a8%d9%84-%d8%a7%d9%84%d8%b0%d9%83%d8%a7%d8%a1-%d8%a7%d9%84%d8%a7%d8%b5%d8%b7%d9%86%d8%a7%d8%b9%d9%8a-%d9%85%d8%a7-%d9%87%d9%8a-%d8%a3%d8%b3%d9%88%d8%a3>

خلل في هذه الأنظمة كما قد يفقد خبراء الأمن السيبراني القدرة على التصدي للتهديدات بأنفسهم، بسبب الاعتماد الزائد على الأنظمة التلقائية⁽¹⁾.

7- الأسلحة الفتاكة ذاتية التشغيل

يمكن استخدام الذكاء الاصطناعي لتشغيل أسلحة فتاكة ذاتية التشغيل مثل الطائرات بدون طيار، أو إنشاء أسلحة مستقلة يمكنها اتخاذ قرارات بشأن من يُقتل دون تدخل بشري، وقد يؤدي هذا إلى سيناريوهات خطيرة حيث تخرج هذه الأسلحة عن السيطرة أو يتم اختراقها للاستخدام الضار.

فمثل هذه النوعية من الأسلحة قد تكون عرضة للحوادث أو اختراق القرصنة أو أي شكل آخر من الهجمات الإلكترونية، وفي حال تمكن المهاجمون من السيطرة على هذه الأنظمة، فيمكنهم، على سبيل المثال، استخدامها لإحداث ضرر واسع النطاق.

8- سوء الاستخدام من قبل الأنظمة الاستبدادية

بات معروفا حاليا أنه يمكن استخدام الذكاء الاصطناعي للمراقبة الجماعية (أنظمة التعرف على الوجوه على سبيل المثال) وتمكين الحكومات أو الكيانات الأخرى من مراقبة مواطنيها والسيطرة عليهم على نطاق غير مسبوق. وقد يؤدي ذلك إلى فقدان الخصوصية، فضلا عن إساءة استخدام السلطة من قبل أولئك الذين يتحكمون في تقنيات المراقبة هذه، وربما استخدامها لانتهاك حقوق الإنسان وغيرها من أشكال القمع.

وخير مثال على ذلك: ما تتبعه سلطات الاحتلال الإسرائيلي مع الفلسطينيين في مدينة الخليل حيث تنشر كاميرات ترصد حركة ووجوه الفلسطينيين، وتحفظ بياناتهم وتتعرف عليهم، فيتخذ الذكاء الاصطناعي قرارا بالسماح بمرورهم أو رفضه عند نقاط التفتيش المختلفة، أو حتى تصفية المشتبه فيهم، من دون تدخل بشري.

9- الإحلال الوظيفي (فقدان الوظائف واضطراب العمل)

يتمتع الذكاء الاصطناعي بالقدرة على أتمتة العديد من الوظائف، مما قد يؤدي إلى اضطراب أسواق العمل وطبيعة العديد من الوظائف بشكل كبير.

(1) أنظر:

Williams, P. (2019). Reliance on AI in Cyber Defense: Risks and Realities. IT Management Review, 12(4), 56-64.

فعلى الرغم من أن الذكاء الاصطناعي قد يخلف أنواعا وفرصا جديدة من الوظائف على المدى الطويل، إلا أن الفترة الانتقالية قد تكون صعبة، حيث تؤثر على ملايين الأشخاص الذين قد يجدون صعوبة في العثور على وظائف جديدة، والتكيف مع الاقتصاد الجديد.

ونظرا لأن أنظمة الذكاء الاصطناعي تصبح أكثر تقدما وقدرة، فهناك خطر من أنها قد تحل محل العاملين البشريين في مجموعة واسعة من الوظائف، مما قد يؤدي إلى انتشار البطالة والاضطراب الاقتصادي⁽¹⁾.

الفرع الثالث

فوائد الذكاء الاصطناعي (AI) في إدارة مخاطر الأمن السيبراني

تشمل فوائد الذكاء الاصطناعي (AI) في إدارة مخاطر الأمن السيبراني: قدرته على تحليل مجموعات بيانات شاسعة أثناء عملية التدريب لاكتشاف الأنماط، والانحرافات التي يمكن أن تشير إلى وجود تهديدات، حيث يمكن لنماذج الذكاء الاصطناعي وخاصة خوارزميات تعلم الآلة، الاكتشاف والاستجابة للتهديد المحتملة بشكل أسرع بكثير من الأنظمة القائمة على القواعد التقليدية، فقد ظهر للذكاء الاصطناعي تطبيقات في مجال الأمن السيبراني المتنوعة، بما في ذلك اكتشاف الاختراق، وتحديد البرامج الضارة، وتحليل حركة الشبكة، واكتشاف الأنشطة الاحتيالية، بالإضافة إلى ذلك: يمكن استخدام الذكاء الاصطناعي: لتعزيز الأمن السيبراني من خلال توفير استجابات ورصد وقائية وتنبؤية أكثر فعالية، وبالتالي التخفيف من المخاطر المرتبطة بالأمن السيبراني.

ويمكن لأنظمة الأمن السيبراني التي تعمل بالذكاء الاصطناعي: أتمتة عمليات الاستجابة للحوادث، مما يقلل الوقت المستغرق لتحديد التهديدات واحتوائها والتخفيف منها، كما يمكن لخوارزميات الذكاء الاصطناعي: تحليل طبيعة الحادث، وتقييم تأثيره والتوصية بالإجراءات المناسبة، من خلال التعلم الآلي تعمل أنظمة الذكاء الاصطناعي باستمرار على تحسين قدراتها على الاستجابة من خلال التعلم من الحوادث السابقة، والتكيف مع التهديدات الجديدة.

(1) أنظر: الموقع الإلكتروني لقناة الجزيرة على الرابط الإلكتروني:

<https://www.aljazeera.net/tech/2023/6/11/%d9%85%d8%b3%d8%aa%d9%82%d8%a8%d9%84-%d8%a7%d9%84%d8%b0%d9%83%d8%a7%d8%a1-%d8%a7%d9%84%d8%a7%d8%b5%d8%b7%d9%86%d8%a7%d8%b9%d9%8a-%d9%85%d8%a7-%d9%87%d9%8a-%d8%a3%d8%b3%d9%88%d8%a3>

كما يمكن لأنظمة الذكاء الاصطناعي الاستفادة من الكميات الهائلة من البيانات من مصادر مختلفة بما في ذلك موجز معلومات التهديدات، ومدونات الأمان وبيانات الهجوم التاريخية للبقاء على الاطلاع بأحدث تهديدات الأمن السيبراني، من خلال الجمع بين هذا الذكاء الخارجي والبيانات الداخلية التي جمعها من خلال العناصر البشرية يمكن لخوارزميات الذكاء الاصطناعي تحديد الأنماط والاتجاهات الناشئة التي تشير إلى الهجمات المحتملة، وتسمح هذه المعلومات الاستخبارية للمؤسسات بتحسين دفاعاتها بشكل استباقي، وتصحيح نقاط الضعف، وتنفيذ التدابير الأمنية اللازمة للتخفيف من المخاطر بشكل فعال.

ويتمثل أحد التحديات المهمة في الأمن السيبراني في: التمييز بين أنشطة المستخدم المشروعة والسلوك الضار، ويمكن لتحليلات سلوك المستخدم المدعومة بالذكاء الاصطناعي إنشاء أنماط أساسية لأنشطة المستخدم العادية داخل شبكة المؤسسة، حيث يمكن أن تؤدي أي انحرافات عن هذه الأنماط إلى إطلاق تنبيهات مما يُمكن فِرَق الأمان من التحقيق والاستجابة الفورية للتهديدات الداخلية المحتملة أو الحسابات المخترقة، كما يمكن لأنظمة الذكاء الاصطناعي أيضاً تحديد إساءة استخدام المستخدمين مثل: الوصول غير المصرح به أو تسريب البيانات غير المعتاد، من خلال تحليل سلوك المستخدم عبر أنظمة متعددة⁽¹⁾.

كيفية الحد أو درء مخاطر الذكاء الاصطناعي

للتخفيف من هذه المخاطر، يعمل الباحثون وصناع السياسات على تطوير طرق آمنة وموثوقة لتصميم ونشر أنظمة الذكاء الاصطناعي. ويشمل ذلك: وضع مبادئ توجيهية أخلاقية لتطوير الذكاء الاصطناعي، وضمان الشفافية والمساءلة في صنع القرار الخاص بالذكاء الاصطناعي، وبناء الضمانات لمنع العواقب غير المقصودة. على النحو التالي

1- تطوير أنظمة ذكاء اصطناعي شفافة وقابلة للتفسير.

ويشير الذكاء الاصطناعي القابل للتفسير إلى قدرة أنظمة الذكاء الاصطناعي على تقديم تفسيرات واضحة ومفهومة لعمليات صنع القرار لديها. ويمكن أن يُساعد ذلك في زيادة الشفافية والمساءلة، وتقديم رؤى حول كيفية وصول نظام الذكاء الاصطناعي إلى قراراته.

(1) أنظر: عبد الرحمن حسن، ورقة عمل بحثية مقدمة لمؤتمر تمكين الأول للذكاء الاصطناعي والابتكار وريادة الأعمال، بريطانيا 2024ن، ص15 وما بعدها.

2- تطوير أنظمة ذكاء اصطناعي تتماشى مع القيم الإنسانية

ويتضمن ذلك تصميم أنظمة ذكاء اصطناعي تمت برمجتها بشكل صريح لإعطاء الأولوية لسلامة الإنسان ورفاهيته، ولتجنب الإجراءات التي من شأنها الإضرار بالبشر. ويمكن تحقيق ذلك من خلال دمج الاعتبارات الأخلاقية في تصميم وتطوير أنظمة الذكاء الاصطناعي.

3- تطوير طرق للتحكم في أنظمة الذكاء الاصطناعي وإدارتها

على سبيل المثال، يستكشف الباحثون طرقاً لبناء آليات تسمح للبشر بالتدخل في عمليات صنع القرار بالذكاء الاصطناعي، أو لإغلاق أنظمة الذكاء الاصطناعي إذا بدأت في التصرف بشكل غير متوقع أو بطريقة ضارة.

4- التعاون متعدد التخصصات بمعالجة مخاطر الذكاء الاصطناعي

يتضمن ذلك: الجمع بين الخبراء من كل المجالات مثل: علوم الحاسوب والهندسة والأخلاق والقانون والعلوم الاجتماعية، للعمل معاً لتطوير حلول تعالج التحديات المعقدة التي يطرحها الذكاء الاصطناعي. ومن خلال العمل معاً، يمكن للباحثين وصانعي السياسات فهم المخاطر المرتبطة بالذكاء الاصطناعي بشكل أفضل، ووضع إستراتيجيات فعالة لإدارة هذه المخاطر⁽¹⁾.

(1) أنظر الموقع الإلكتروني لقناة الجزيرة على الرابط:

<https://www.aljazeera.net/tech/2023/6/11/%d9%85%d8%b3%d8%aa%d9%82%d8%a8%d9%84-%d8%a7%d9%84%d8%b0%d9%83%d8%a7%d8%a1-%d8%a7%d9%84%d8%a7%d8%b5%d8%b7%d9%86%d8%a7%d8%b9%d9%8a-%d9%85%d8%a7-%d9%87%d9%8a-%d8%a3%d8%b3%d9%88%d8%a3>

المبحث السابع

الذكاء الاصطناعي واستخدامه في إجراءات التقاضي

يحدث الذكاء الاصطناعي تغييرات كبيرة في مجال التقاضي، حيث يساهم في تسريع الإجراءات، ويمكن استخدام الذكاء الاصطناعي لتحليل البيانات القضائية الكبيرة واستخراج المعلومات الهامة التي يمكن أن تساعد القضاة في اتخاذ قراراتهم. يمكن استخدام التقنية لفحص النصوص القانونية وتحديد التشابه والاختلاف في القوانين، مما يوفر الكثير من الوقت والجهد للقضاة والمحامين. كما يمكن استخدام الذكاء الاصطناعي لتوفير حلول توجيهية للمحاكم وتوصية بأفضل الممارسات القانونية.

وعليه سوف نقوم بتقسيم هذا المبحث إلى المطالب التالية:

- 1- المطالب الأول: دور الذكاء الاصطناعي في تعزيز العدالة الناجزة أمام القضاء.
- 2- المطالب الثاني: الدول التي تستخدم الذكاء الاصطناعي في إجراءات التقاضي.
- 3- المطالب الثالث: تحديات ومخاطر الذكاء الاصطناعي على إجراءات التقاضي.

المطلب الأول

دور الذكاء الاصطناعي في تعزيز العدالة الناجزة أمام القضاء

يتميز الذكاء الاصطناعي في إجراءات التقاضي بقدرته على تحليل البيانات وإجراء البحث بسرعة قصوى من شأنها إرشاد القانونيين وتمكينهم من وضع استراتيجيات قانونية تتميز بالدقة والشمولية بالإضافة إلى استنتاجه تصوراً شاملاً بشكل استباقي لنتائج الدعاوى القضائية الأكثر احتمالاً. لذا تدرس الخدمات القضائية وخدمات الادعاء العام وغيرها من الهيئات القضائية المختصة في العالم، استخدام الذكاء الاصطناعي في النظم القضائية؛ للمساعدة في التحقيقات وفي أتمتة عمليات اتخاذ القرارات⁽¹⁾.

حيث يسعى القضاة والمحامون إلى تحقيق العدالة السريعة وتحسين كفاءة العمل القضائي، وهنا تأتي تكنولوجيا الذكاء الاصطناعي لتلعب دوراً مهماً في تطوير أداء المحاكم. يعتبر الذكاء الاصطناعي أداة قوية تستخدم في إدارة الملفات القضائية الإلكترونية، وتحليل البيانات، وتسهيل اتخاذ القرارات القضائية. بفضل تلك التقنيات، يمكن للمحاكم تحسين الكفاءة والدقة في التحقيقات وإجراءات المحاكمة.

بالإضافة إلى ذلك، يمكن استخدام الذكاء الاصطناعي في تحسين إجراءات التحقيق وتسريع عمل المحاكم. يمكن للتكنولوجيا تحليل البيانات الرقمية المرتبطة بالجرائم وتحديد الأنماط والاتجاهات التي يصعب اكتشافها بواسطة البشر. بفضل ذلك، يمكن تحديد المشتبه بهم الرئيسيين وجمع الأدلة بشكل أسرع وأكثر دقة، مما يساعد في تقديم العدالة السريعة وتحسين عمل المحاكم⁽¹⁾.

وهناك أسباب كثيرة تعوق أعمال القضاة لتحقيق العدالة الناجزة، بعضها مرتبط بنصوص قانونية، والبعض الآخر مرتبط بكثرة عدد القضايا وطول الإجراءات وقلة عدد القضاة، وطول أمد تنفيذ الأحكام وتعطيله أو الامتناع عنه. إن التعلل ببطء

(1) أنظر: د. جلال فضل محمد، دور الذكاء الاصطناعي في تعزيز العدالة الناجزة أمام القضاء، صحيفة القضائية، وزارة العدل - الجمهورية اليمنية، العدد (7)، الأربعاء 31 يوليو 2024 م، ص 5.

(1) أنظر الموقع الإلكتروني:

<https://kharchoufa.com/%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1-%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A-%D9%88%D8%A7%D9%84%D9%82%D8%B6%D8%A7%D8%A1>

التّقاضى لا يعنى تقييد لجوء المواطنين للقضاء من أجل الحصول على حقوقهم أو القصاص من المعتدين، فلا بُدَّ من نشر الثقافة القانونية بين المواطنين والموظفين الذين يتلقون التّبليغات وكيفية التّصرف فيها بالسرعة الممكنة، وانفتاح المحاكم أمام المجتمع بما يحقق إرساء مبدأ علانية المحاكمات.

فقد ظهرت الحاجة الملحة إلى استخدام الذكاء الاصطناعيّ الذي يتمتع بإمكانات هائلة يُمكن استخدامها لتحقيق المنفعة الاجتماعية وبلوغ أهداف التنمية المستدامة، خاصّة على صعيد الأنظمة القضائية، فلقد أثبت قدرته على تعزيز كفاءة هذه الأنظمة من خلال اعتماد منصّات العدالة الرّقمية التي تعمل على تسريع إجراءات التّقاضى وتختصر وقت وجهد المتقاضين. وإذا كان النّظر للعدالة النّاجزة يقتضي النّظر للجوانب الاجتماعية والاقتصادية والتّشريعية، فإنّه لتحقيقها لا بُدَّ من دراسة كلّ الجوانب بشكل معمق.

وبالنّظر إلى ما يقدمه الذكاء الاصطناعيّ في مجال العدالة النّاجزة، فهو يوفر كلّ الاحتياجات، فلا يتطلب زيادة عدد الأفراد أو عدد الأماكن، فقط الحاجة إلى توفير الأجهزة الإلكترونية المناسبة في المحاكم وتجديدها باستمرار لمواكبة التّكنولوجيا الحديثة باستمرار، والتّوسع في المحاكمات المصورة وسماع الشّهود عن بعد. لا شك أنّ مجالات الذكاء الاصطناعيّ تنمو بشكل كبير جدّاً، الأمر الذي يحتم على الجهات المعنية السّعي لإعداد تشريعات قانونية تضبط استخداماتها، وتحدد المسؤوليات في نتائج الممارسات والأعمال، لخلق بيئة استثمارية متطورة ورائدة في التّقنيات التّكنولوجية المرتبطة بالذكاء الاصطناعيّ⁽¹⁾.

فدمج أدوات الذكاء الاصطناعي والتّقنيات التكنولوجية ضمن أنظمة المحاكم أمر في غاية الأهمية، وتختلف كل محكمة عن الأخرى، من حيث عدد القضايا، والاختصاصات القضائية، سواء مدنية، تجارية أو جنائية، ويفضي هذا الاختلاف إلى الحاجة إلى الابتكار وإيجاد أنظمة تلبي احتياجات كل محكمة على حدة، الأمر الذي قد ينشأ بعض التحديات المالية وضخ الاستثمارات في هذا المجال من قبل المحاكم.

ومع اتساع حركة التجارة عالمياً، والذي نتج عنه زيادة متوقعة ومتوازية في عدد النزاعات الناشئة من حركة المال والأعمال، أصبح من المرجح أن يزيد الطلب على

(1) أنظر: د. جلال فضل محمد، دور الذكاء الاصطناعي في تعزيز العدالة الناجزة أمام القضاء، مرجع سابق، ص5.

أدوات الذكاء الاصطناعي والحلول التكنولوجية ضمن أنظمة المحاكم، لتتواءم مع زيادة الطلب والحد من أي تأخير في تسوية النزاعات، الأمر الذي سيسهم بشكل أو بآخر إلى رؤية تحول في أنظمة العدالة والقضاء.

إن أدوات الذكاء الاصطناعي لها جوانب إيجابية ومفيدة كثيرة يمكن للمحاكم الاستفادة منها كل حسب احتياجاتها وطبيعة اختصاصها وأنظمتها، ورغم أن الاستثمار في الذكاء الاصطناعي مكلف إلا أنني أتوقع زيادة استخدامه في أنظمة المحاكم في المستقبل القريب، وذلك لما تمتلكه هذه التقنيات من أدوات تعمل على تسريع إجراءات التقاضي وجعلها أكثر كفاءة وفعالية⁽¹⁾.

ويمكننا القول أن للذكاء الاصطناعي في إجراءات التقاضي دور إيجابي تتمثل في:

1. الكفاءة في البحث القانوني: أدوات الذكاء الاصطناعي قادرة على إجراء أبحاث قانونية واسعة وشاملة بشكل أسرع من المحامين التقليديين، مما يوفر الوقت ويقلل التكاليف.

2. تحليل البيانات: يمكن للذكاء الاصطناعي تحليل كميات ضخمة من البيانات القانونية واستخلاص أنماط وتوجهات يمكن أن تكون مفيدة في التنبؤ بالنتائج أو تقديم المشورة القانونية.

3. التنبؤ بالأحكام: تستخدم بعض الأدوات الذكاء الاصطناعي لتحليل السوابق القضائية والأنماط القانونية لتوقع نتائج القضايا، مما يساعد المحامين في إعداد استراتيجياتهم القانونية.

(1) أنظر الموقع الإلكتروني:

<https://www.qicdrc.gov.qa/ar/media-center/news/oped-role-digital-technology-and-ai-enhancing-court-efficiency>

4. أتمتة الأعمال الروتينية: العديد من العمليات القانونية الروتينية، مثل إعداد الوثائق أو تحليل العقود، يمكن أتمتتها باستخدام الذكاء الاصطناعي، مما يقلل من العبء الإداري على المحامين وموظفي المحاكم .

5- الذكاء الاصطناعي يمتلك قدرة كبيرة على دعم حوكمة القضاء والإفتاء من خلال تعزيز الدقة والاتساق، زيادة الكفاءة، وتقديم تحليلات متعمقة. ومع ذلك، لتحقيق إمكاناته الكاملة، يجب أن يتم تطويره واستخدامه ضمن إطار قانوني وأخلاقي واضح، مع التركيز على التوافق مع المقاصد الشرعية وحفظ العدالة. يظل الذكاء الاصطناعي أداة مساعدة قوية، ولكن يجب أن تظل السلطة النهائية في يد الإنسان لضمان تحقيق التوازن بين الابتكار والتقيد بالقيم الأخلاقية والشرعية حيث أنه يعمل على تحسين الكفاءة وتوفير أدوات لتحليل البيانات القانونية. ومع ذلك، لا يمكن أن يحل الذكاء الاصطناعي محل الحكم البشري بالكامل، خاصة في المسائل التي تتطلب فهماً عميقاً للأخلاقيات والقيم الإنسانية وما يتعلق بأصول وقواعد الدين⁽¹⁾.

(1) أنظر الموقع الإلكتروني:

المطلب الثاني

الدول التي تستخدم الذكاء الاصطناعي في إجراءات التقاضي

استخدمت العديد من الدول العالم تقنية الذكاء الاصطناعي في إجراءات التقاضي ومن تلك الدول على سبيل المثال للحصر:

1- الولايات المتحدة الأمريكية: عندما طورت إحدى الشركات برنامجًا يُستخدم في جلسات الحكم وإطلاق السراح المشروط في جميع أنحاء البلاد، وبعض الشركات استخدمت صفحات من قواعد المحكمة الفيدرالية لتوليد الأفكار وتقديم التنبؤات، وتوصلت إحدى الدراسات إلى تصميم برنامج يعتمد على الذكاء الاصطناعي يمكن من خلاله التنبؤ بقرارات القضاة في المحاكم الأمريكية؛ استنادًا إلى البيانات التي جمعها عن القضايا وأحكام القضاة، وقدرت شركة مكنزي الأمريكية أن ما نسبته 20% - 30% من القضايا يمكن استبدالها بالذكاء الاصطناعي، فدراسة القضايا يمكن وضعها في إطار يسهل صناعة ذكاء اصطناعي يقوم بالمهمة، إلا أنه قد تبين للباحثين أن النظام يسئ تقدير مخاطر معاودة الإجرام لدى مختلف المدانين بالقضايا، من ذلك التحيز العنصري، فقد كان يجري تصنيف المدانين السود أعلى من غير السود، حتى عندما ارتكب المدانون غير السود جرائم أشد خطورة.

2- الصين: تمتلك الصين أكثر من مئة روبوت موزعة في المحاكم في جميع أنحاء البلاد الصينية، وتعمل هذه الروبوتات على استرجاع بيانات القضايا والأحكام الماضية، كما تلجأ المحاكم الصينية إلى استخدام الذكاء الاصطناعي في التحقيق في الأدلة المقدمة لها، والتعرف على الوجوه، وتعد تطبيقات الذكاء الاصطناعي في الصين مساعدة للقضاة في أداء عملهم لا حالة مكانهم، وتستخدم الصين الروبوتات في تقديم المشورة القانونية، ومساعدة الجمهور على فهم المصطلحات القانونية، على سبيل المثال تقف (زياوفا) - روبوت - في إحدى المحاكم الصينية لتقديم المشورات القانونية؛ فهي تعرف الإجابة عن أكثر من أربعين ألف سؤال في مجال النزاعات القضائية، وتستطيع التعامل مع ثلاثين ألف مشكلة قانونية.

3- محكمة شنغهاي المالية تعتمد على الذكاء الاصطناعي والتحول النوعي التي أحدثته في الطريقة التي تعمل بها المحكمة. ومن بين هذه الابتكارات، برنامج يعمل عن طريق الذكاء الاصطناعي يقوم بمراجعة المذكرات القانونية تلقائيًا. وفي حالة اكتشاف

أي أوجه قصور، يقوم النظام بتنبيه الأطراف بالتعديلات التي يجب القيام بها وذلك قبل تقديمها، مما يساعد في تقليل مدة

الإجراءات من خلال تجنب الأخطاء الإدارية. وعلاوة على ذلك، بمجرد اكتمال المذكرات، يضمن البرنامج توفير الخدمات الإلكترونية لجميع الأطراف ذات الصلة بالقضية - مما يلغي التدخل البشري ويساهم في تسريع إجراءات التقاضي⁽¹⁾.

أما القضاء العربي لا شك أن التحول الرقمي فيه يمثل تحدياً هاماً، ولكنه يتيح فرصاً كبيرة لتحسين العمل القضائي وتوفير العدالة الرقمية. يجب على الدول العربية الاستثمار في التكنولوجيا وتكريس الجهود لتحقيق التحول الرقمي في القضاء، مع الحفاظ على الشفافية والمساءلة وحماية البيانات القضائية. من خلال استراتيجيات فعالة وتعاون واسع النطاق بين المؤسسات القضائية والتكنولوجية، سيكون بإمكان القضاء العربي الوصول إلى العدالة الرقمية وتحقيق التحول الرقمي الشامل في القطاع القضائي، ومن ضمن الدول العربية التي أدخلت تقنية الذكاء الاصطناعي في إجراءات التقاضي منها:

1- قدمت محاكم دبي، خلال مشاركتها في الدورة التاسعة والثلاثين من «أسبوع جيتكس للتقنية»، مجموعة من خدماتها الذكية لتعزيز كفاءة المنظومة القضائية، حيث عرضت «منصة العدالة الرقمية» التي تعمل على تسريع إجراءات التقاضي في القضايا التجارية، وتختصر وقت وجهد أطراف القضية بنسبة 80%، وتعتمد على أحدث تقنيات الاتصال عبر الفيديو في العالم، و«خدمة الدفع الذكي لرسوم وأمانات وغرامات القضايا»، التي توفر منصة موثوقة ومتكاملة للدفع الإلكتروني والذكي دون الحاجة إلى تسجيل الدخول أو زيارة مقر المحاكم، وخدمتي «الزواج الذكي» و«الإشراكات»، اللتين تسهلان إجراءات التقاضي من خلال مزاياهما التفاعلية المتطورة التي تتيح للمتعاملين إتمام الإجراءات عن بعد بسرعة وسلاسة ووفق أعلى معايير الموثوقية والكفاءة.

ودعمت محاكم دبي مسار التحول الذكي في المجال القضائي في دولة الإمارات تماشياً مع استراتيجية دبي للمعاملات اللاورقية، إذ سبق لها أن أطلقت مشروع «تقاضٍ بدون قاضٍ» باستخدام الذكاء الاصطناعي الذي يقوم بعمل القاضي الجزائي فيما يتعلق بإصدار وتنفيذ الأحكام المتعلقة في الدعاوى البسيطة، خلال عدة دقائق، وعلى

(1) أنظر مقال منشور على الموقع الإلكتروني:

<https://www.qicdrc.gov.qa/ar/media-center/news/oped-role-digital-technology-and-ai-enhancing-court-efficiency>

مدى اليوم، إذا أقر المتهم بتهمة، حيث يفصل في نحو 70% من القضايا الجنائية التي تكون عقوبتها الغرامة المالية من دون الجُنح.

ومن خلال مبادراتها وتطبيقاتها الذكية المعتمدة على الذكاء الاصطناعي، تقطع محاكم دبي شوطاً طويلاً في التخلص من المعاملات الورقية، حيث يتيح لها الاعتماد على التقنيات الذكية تسهيل إجراءات المتعاملين، وتقديم الخدمات بطريقة سهلة توفر وقت وجهد موظفي القطاع القضائي والمتعاملين على السواء، ما يسهم في تعزيز رضا المتعاملين وخفض التكاليف وحماية البيئة.

وترى محاكم دبي أن الذكاء الاصطناعي يمكن في مرحلة ما في المستقبل أن يقوم بدور القاضي، خاصة من حيث تحليل بيانات المتعاملين والتصنيف الدقيق للقضايا وأنواعها، فضلاً عن كل ما يتعلق بالقوانين والتشريعات.

2- في المملكة العربية السعودية: بدت الجهود واضحة في الاهتمام بجانب الذكاء الاصطناعي، فقد أنشأت مدينة الملك عبد العزيز للعلوم والتقنية مركزاً وطنياً لتقنية الذكاء الاصطناعي والبيانات الضخمة، والإدراك حكومة المملكة أن الذكاء الاصطناعي هو أحد الركائز الأساسية للثورة الصناعية وعصب اقتصاد المستقبل، أعلنت في 2018م عن استثمارها بميزانية غير مسبقة بقيمة 500 بليون دولار لبناء دولار مدينة "نيوم" المستقبلية القائمة على الذكاء الاصطناعي وتقنيات أخرى مستقبلية؛ مثل إنترنت الأشياء والروبوتات، كما أنشئت هيئة خاصة بالذكاء الاصطناعي باسم "الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)" بالأمر الملكي رقم 74167 وتاريخ 29 / 12 / 1440هـ الموافق 2019/8/30م، وترتبط مباشرة برئيس مجلس الوزراء، ويرأس مجلس إدارتها نائب رئيس مجلس الوزراء.

وقد كان لهذا الاهتمام أثره في الأنظمة العدلية ولوائحها التنفيذية، فقد جاء التصريح في المادة (24) من اللائحة التنفيذية لنظام المحاكم التجارية، الصادرة بالقرار الوزاري رقم (8344) تاريخ 26 / 10 / 1441هـ، ونصها "يجوز الاستفادة من تقنيات الذكاء الاصطناعي في الإجراءات الإلكترونية، ويُستغنى عن أي إجراء تحققت غايته باستخدام تلك التقنيات"⁽¹⁾.

3- وفي جمهورية مصر العربية عملت وزارة العدل على مشروع تحويل الصوت إلى نص مكتوب باستخدام الذكاء الاصطناعي من خلال برنامج يحول كافة ما يجري من حوار داخل قاعة الجلسة كمرافعات المحامين الشفوية وطلباتهم، وقرارات القضاة

(1) أنظر: د. جلال فضل محمد، دور الذكاء الاصطناعي في تعزيز العدالة الناجزة أمام القضاء، مرجع سابق، ص5.

إلى محرر مكتوب يطبع في نهاية الجلسة ليوقعه القاضي وسكرتير الجلسة؛ وتأتي أهمية المشروع أن التفريغ الصوتي يعد من ثمار التطور التكنولوجي لما يتضمنه من توفير نقل الألفاظ كما هي دون لبس أو تحريف على مستند

مقروء ومؤمن تسهيلاً لنقله وحفظه. وفي مراسيم افتتاح الرئيس عبد الفتاح السيسي لمجمع الإصدارات المؤمنة والذكية في إبريل 2021م، أعلن وزير العدل عن دراسة مشروع لميكنة محاضر الجلسات، وهو المشروع الذي يحقق الريادة لجمهورية مصر العربية في مجال استخدام الذكاء الاصطناعي في منظومة العدالة. كما بدأت وزارة العدل في 4 سبتمبر 2021 بالمرحلة التجريبية من المشروع من خلال تطبيقه في جلسات نظر تجديد الحبس عن بعد بمحكمة القاهرة الجديدة الابتدائية وجلسات المحاكم الاقتصادية. وفي نوفمبر 2021 أصدر وزير العدل القرار الذي حمل رقم 8901 لسنة 2021، ويعمل به من يناير 2022 متضمناً السماح للقضاة عقد جلسات نظر تجديد الحبس الاحتياطي واستئنافه عن بعد باستخدام التقنيات الحديثة، ويجوز تسجيل محاضر الجلسات، عن طريق تقنية تحويل الكلام الشفوي إلى محضر مكتوب، يوقع عليه كل من رئيس المحكمة وسكرتير الجلسة، وفي نفس الشهر - يناير 2022م - تم تطبيق المشروع عملياً بمحكمة القاهرة الجديدة، ومحكمة جنوب القاهرة، وقاعة الجنايات بأمورية طرة، ومحكمة القاهرة الاقتصادية، وكذلك تم تركيب الشبكة الداخلية وتوريد أجهزة الصوتيات بقاعات محاكم (شمال القاهرة الابتدائية - شمال الجيزة الابتدائية - جنوب الجيزة الابتدائية - مجمع محاكم عابدين - مجمع محاكم مصر الجديدة). كما تمكنت وزارة العدل من تسجيل المشروع في هيئة الملكية الفكرية باعتباره مشروعاً مصرياً من تنفيذ وزارتي العدل والاتصالات ومجمع الوثائق المؤمنة وفي 7 فبراير 2022م⁽¹⁾.

4- تماشياً مع رؤية قطر الوطنية 2030 واستراتيجية التنمية الوطنية، تعمل محكمة قطر الدولية ومركز تسوية المنازعات على تعزيز دور الذكاء الاصطناعي في القطاع القانوني. وباعتبارها أحد المؤسسات الرائدة في هذا المجال، ونظراً لطبيعة الهيكل التنظيمي للمحكمة، فإنه بإمكان المحكمة تبني أحدث التقنيات بسلاسة وسرعة مما يساهم في تعزيز تجربة المستخدم والجمهور بشكل عام. وعلاوة على ذلك، ونظراً للعلاقات المتميزة للمحكمة في الساحة القضائية والدولية ومشاركتها المستمرة في التجمعات القضائية والقانونية، تعمل المحكمة باستمرار على رصد أحدث التقنيات

(1) أنظر: إبراهيم قاسم - أحمد عبد الهادي، تيسير إجراءات التقاضي.. تطبيق الذكاء الاصطناعي في تحويل الكلام إلى نص مكتوب بالمحاكم، على الموقع الإلكتروني:

<https://www.youm7.com/story/2023/5/30/%D8%AA%D9%8A%D8%B3%D9%8A%D8%B1>

المعمول بها في القطاع القانوني والقضائي، والعمل على تطبيقها لديها وتحسينها مما يتلائم مع طبيعة عملها، ومن ثم مراقبة وتقييم تأثيرها، حيث يسهل الهيكل التنظيمي للمحكمة

تأثيرها على مستوى جميع المحاكم الوطنية، الأمر الذي يتطلب برنامج مراقبة شامل وموسع عملية مراقبة تأثير هذه الأدوات بشكل أسرع وأكثر دقة إذا تمت مقارنة مراقبة.

وانطلاقاً من التزامها بالتطوير المستمر لخدماتها، شرعت المحكمة في تبني عدة مبادرات متعلقة بالذكاء الاصطناعي، منها Courts for Webex وبرنامج المحادثة الذاتي المدعوم بالذكاء الاصطناعي Ask QICDRC، وملخصات القضايا والتي تم إنشاؤها بواسطة الذكاء الاصطناعي، والتي تمكن القارئ من الاطلاع على تفاصيل الدعوى بشكل مبسط وسريع، دون العودة ومراجعة الاحكام الصادرة. وفي هذا الصدد، تحرص المحكمة على تعزيز شراكاتها الاستراتيجية مع الجهات والمؤسسات في مجال الذكاء الاصطناعي والعمل على دمجها ضمن منظومتها القضائية، مما يعزز ريادتها في تقديم خدمات قضائية مبتكرة تعمل على تسهيل تجربة المستخدمين والجمهور بشكل عام (1).

مع العلم أن القضاء الدولي يشهد تطوراً مستمراً في استخدام تقنية الذكاء الاصطناعي لتحسين إجراءات القانون الدولي. يعزز تطبيق الذكاء الاصطناعي في القضاء الدولي فعالية العمل القضائي وتسريع تنفيذ القوانين وتحسين العدالة. يعتبر تحليل البيانات والتعرف الضوئي على الحروف والترجمة الآلية أمثلة على استخدامات التكنولوجيا في التحقيق والمحاكمة في القضاء الدولي. تساهم هذه التقنيات في زيادة دقة وفعالية التحقيق وتحسين جودة القرارات القضائية.

واحدة من الفوائد الرئيسية لتقنية الذكاء الاصطناعي في القضاء الدولي هي تحسين إجراءات القانون الدولي. من خلال استخدام أنظمة إدارة الملفات الإلكترونية والتحليل الذكي للبيانات، يمكن للقضاة والمحامين والمحققين العمل بكفاءة أعلى واتخاذ القرارات بشكل أسرع. كما يمكن استخدام التكنولوجيا في تحسين التواصل والتنسيق بين المحاكم الدولية وتسهيل التعاون الدولي في قضايا تجاوز الحدود (2).

(1) أنظر مقال منشور على الموقع الإلكتروني:

<https://www.qicdrc.gov.qa/ar/media-center/news/oped-role-digital-technology-and-ai-enhancing-court-efficiency>

(2) أنظر: د. جلال فضل محمد العودي، الذكاء الاصطناعي واستخدامه في إجراءات التقاضي، بحث مقدم للورشة التدريبية (تبادل الخبرات في مجال الذكاء الاصطناعي المطبقة على الأنظمة القضائية) المنعقدة في معهد القضاء الاردني بتاريخ 18/ 6/ 2025م، ص24.

المطلب الثالث

تحديات ومخاطر الذكاء الاصطناعي على إجراءات التقاضي

يواجه استخدام التكنولوجيا في القضاء تحديات مهمة تتعلق بالتحقق من الأمان وحماية الحقوق الرقمية. إن تطبيقات الذكاء الاصطناعي وتكنولوجيا القضاء الرقمي تعتمد على جمع وتحليل كميات ضخمة من البيانات الشخصية والمعلومات القانونية، وهذا يتطلب ضمان سلامة وأمان هذه البيانات وحماية خصوصية الأفراد.

من التحديات الرئيسية التي تواجه التكنولوجيا في القضاء هو التحقق من الأمان، حيث يجب ضمان سلامة البيانات وحمايتها من الاختراقات والتلاعب. يجب أن يتم توفير نظم إدارة البيانات القضائية الآمنة والموثوقة، وتكون معايير الأمان والحماية متقدمة وفعالة لمنع أي انتهاكات أو تسريبات للمعلومات الحساسة.

بالإضافة إلى ذلك، يتعين على التكنولوجيا في القضاء أن تضمن حقوق المتهمين والمحامين وجميع الأطراف المعنية. يجب أن يتم التعامل مع البيانات القضائية بشكل عادل ومتوازن، وأن تكون للأفراد الحق في الدفاع عن أنفسهم والوصول إلى المعلومات اللازمة للقضية. يجب أن تحترم التكنولوجيا في القضاء الحقوق الرقمية للأفراد وتعزز الشفافية والعدالة في العمل القانوني⁽¹⁾.

فالتقاضي الإلكتروني يمثل تحولاً جذرياً في المشهد القانوني، حيث يستفيد من الأدوات الرقمية لتبسيط إجراءات المحكمة، من تقديم الوثائق إلى إصدار الأحكام. ومع تبني المحاكم في جميع أنحاء العالم بشكل متزايد لهذا النهج القائم على التكنولوجيا، فإنه لا يعد فقط بكفاءة محسنة ولكنه يفرض أيضاً تحديات كبيرة تتعلق بالأمن السيبراني والتي يجب معالجتها لحماية نزاهة العملية القضائية.

(1) أنظر: د. جلال فضل محمد العودي، الذكاء الاصطناعي واستخدامه في إجراءات التقاضي، ص 27.

إن التحول إلى التقاضي الإلكتروني يستلزم تخزين وإدارة الوثائق القانونية الحساسة في صيغ رقمية، مما يجعلها أهدافًا محتملة للهجمات الإلكترونية. وتعتبر سرية هذه الوثائق وسلامتها وتوافرها أمرًا بالغ الأهمية، حيث أن أي تسوية قد تؤدي إلى إجهاض العدالة أو انتهاك حقوق الخصوصية. وبالتالي، فإن الأمن السيبراني في التقاضي الإلكتروني لا يصبح مجرد قضية فنية، بل جانبًا أساسيًا من جوانب الحفاظ على ثقة الجمهور في نظام العدالة الرقمي.

إن أحد أهم المخاوف المتعلقة بالأمن السيبراني في مجال التقاضي الإلكتروني هو خروقات البيانات. ويمكن أن تحدث هذه الخروقات من خلال وسائل مختلفة مثل القرصنة أو هجمات التصيد الاحتيالي أو حتى التهديدات الداخلية. والعواقب المترتبة على مثل هذه الخروقات عميقة. على سبيل المثال، قد يؤدي الوصول غير المصرح به إلى الوثائق القانونية السرية إلى التلاعب بالأدلة أو تسريب المعلومات الحساسة، وبالتالي تقويض نزاهة المحاكمات. ولمكافحة هذا، تعد بروتوكولات التشفير القوية وضوابط الوصول الآمنة ضرورية. وتضمن هذه التدابير أن الأفراد المصرح لهم فقط يمكنهم الوصول إلى البيانات الحساسة، وحتى في حالة اعتراض البيانات، تظل المعلومات غير مفهومة للمستخدمين غير المصرح لهم.

علاوة على ذلك، تلوح قضية سلامة البيانات في الأفق. ففي عالم التقاضي الإلكتروني، يمكن لأي تغيير في السجلات الرقمية، سواء كان عرضيًا أو خبيثًا، أن يؤدي إلى قرارات غير صحيحة من جانب المحكمة. لذلك، يعد تنفيذ أنظمة قوية للتحقق من صحة البيانات وكشف العبث بها أمرًا بالغ الأهمية. يمكن لهذه الأنظمة التحقق من صحة المستندات وتسجيل أي تعديلات، مما يوفر مسارًا واضحًا للتدقيق. وهذا لا يساعد فقط في الحفاظ على دقة المستندات القانونية، بل يساعد أيضًا في غرس الثقة بين أصحاب المصلحة حول موثوقية نظام التقاضي الإلكتروني.

إن التحدي الكبير الآخر الذي يواجهنا الآن هو ضمان توافر خدمات المحكمة الرقمية. فالهجمات الإلكترونية مثل هجمات الحرمان من الخدمة الموزعة (DDoS) قد تطغى على أنظمة المحاكم، مما يؤدي إلى تأخير أو حتى إغلاق مؤقت. ولا تعيق مثل هذه الاضطرابات العملية القضائية فحسب، بل قد تؤدي أيضًا إلى تآكل الثقة في قدرة النظام على العمل بشكل فعال. وبالتالي، فإن نشر استراتيجيات مكافحة هجمات الحرمان من الخدمة الموزعة والحفاظ على أنظمة قوية وزائدة عن الحاجة أمر بالغ

الأهمية لضمان استمرار عمليات المحكمة دون انقطاع حتى في ظل الهجوم الإلكتروني.

وعلاوة على ذلك، بما أن التقاضي الإلكتروني يشمل أصحاب المصلحة المختلفين بما في ذلك المحامين والقضاة وموظفي المحكمة الذين قد لا يكونون على دراية بالتكنولوجيا بطبيعتهم، فهناك خطر كبير من الخطأ البشري الذي يؤدي إلى ثغرات أمنية. إن برامج التدريب الشاملة على أفضل ممارسات الأمن السيبراني لا غنى عنها في هذا السياق. إن تثقيف جميع المشاركين حول التهديدات السيبرانية المحتملة وكيفية التخفيف منها أمر حيوي لتعزيز إطار التقاضي الإلكتروني ضد الهجمات⁽¹⁾.

ويذكر أن البرامج الذكية تتمتع باستقلالية غير متوقعة، وفقاً لما تمليه عليها البيئة المحيطة، وتتخذ قراراتها دون الرجوع إلى مستخدميها، ما قد يخلق مخاوف بشأن المسؤولية القانونية والأخلاقية التي قد تترتب على أعمال هذه البرامج، مثل أن تلحق مركبة ذاتية القيادة أضراراً بالغة، نتيجة عوامل لا يمكن التنبؤ بها أو دفعها.

فضلاً عن أن استخدام الذكاء الاصطناعي يثير مجموعة كبيرة من الصعوبات مثل اتخاذ خوارزميات الذكاء الاصطناعي قرارات متحيزة، لكن كل هذه الأمور ستصبح سهلة إذا بدأنا فيها بخطوات جادة⁽²⁾.

ويمكننا القول أن للذكاء الاصطناعي في إجراءات التقاضي دور سلبي تتمثل في:

1- الاعتماد الزائد على التكنولوجيا: قد يؤدي الاعتماد الكبير على الذكاء الاصطناعي إلى تقليل الحاجة إلى التفكير النقدي البشري أو الخبرة القانونية، مما قد يؤثر على جودة العمل القانوني في بعض الحالات.

2- التحيزات في البيانات: يمكن أن يعكس الذكاء الاصطناعي التحيزات الموجودة في البيانات التي يتم تدريبه عليها، مما قد يؤدي إلى نتائج غير عادلة أو تمييزية. فهو ينقصه عنصر التفاعل البشري والذي يستخدمه المحقق عند استجواب الأطراف والشهود بالاعاوي⁽³⁾.

(1) أنظر: الموقع الإلكتروني:

<https://hzlegal.ae/ar/%D8%A7%D9%84%D8%AA%D9%82%D8%A7%D8%B6%D9%8A>

(2) أنظر: د. جلال فضل محمد، دور الذكاء الاصطناعي في تعزيز العدالة الناجزة أمام القضاء، مرجع سابق، ص5.

(3) أنظر الموقع الإلكتروني:

<https://mebusiness.ae/ar/news/show/93874>

3- الخصوصية والأمان: استخدام الذكاء الاصطناعي يتطلب الوصول إلى كميات كبيرة من البيانات، مما يثير مخاوف حول حماية البيانات الشخصية وحفظ السرية.

4- المساءلة القانونية: مسألة تحديد من يتحمل المسؤولية في حالة وقوع خطأ في عملية إديرها الذكاء الاصطناعي ما زالت غير واضحة تمامًا.

5- استخدام تقنية الذكاء الاصطناعي في القضاء الدولي، تواجه تحديات واحدة من هذه التحديات هي التحقق من الأمان وحماية البيانات الشخصية في السياق الدولي. يجب أن تتم معالجة هذه المخاوف بشكل جذري لضمان استخدام آمن وموثوق للتكنولوجيا في القضاء الدولي والحفاظ على حقوق المتهمين والمحامين⁽¹⁾.

(1) أنظر: د. جلال فضل محمد العودي، الذكاء الاصطناعي واستخدامه في إجراءات التقاضي، ص30.

الفهرس

المقدمة ص2

المبحث الأول

الجريمة الالكترونية ص3

المطلب الأول: تعريف الجريمة الالكترونية وخصائصها ص4

المطلب الثاني: تقسيم الجرائم الالكترونية ص8

المبحث الثاني

ماهية الدليل الالكتروني ص13

المطلب الأول: تعريف الدليل الإلكتروني ص14

المطلب الثاني: خصائص الدليل الإلكتروني ص16

المطلب الثالث: أنواع الأدلة الالكترونية وشروط قبولها ص20

المبحث الثالث

الحلول العملية والقانونية لحل مشاكل الجرائم الإلكترونية ص25

المطلب الأول: الحلول العلمية لحل مشاكل الجرائم الإلكترونية ص26

المطلب الثاني: الحلول التشريعية لحل مشاكل الجرائم الإلكترونية ص31

المبحث الرابع

سلطات القاضي في تقييم الدليل الإلكتروني.....ص35

المطلب الأول: مبدأ قناعة القاضي والضوابط التي تحكمه.....ص 36

المطلب الثاني: الدور الإيجابي القاضي الجزائية في تقييم الأدلة الإلكترونية....ص39

المطلب الثالث: صلاحية القاضي في تقدير الأدلة في الاتجاهات المختلفة للدول...ص 43

المبحث الخامس

دور الأمن السيبراني في مكافحة الجريمة السيبرانية.....ص46

المطلب الأول: مفهوم الأمن السيبرانيص47

المطلب الثاني: أهمية الأمن السيبراني وأهدافهص51

المطلب الثالث: أبعاد الأمن السيبراني والمخاطر والتهديدات المرتبطة به ...ص55

المطلب الرابع: استراتيجيات مواجهة تهديدات الأمن السيبرانيص62

المبحث السادس

الذكاء الاصطناعي وأثره على الأمن السيبراني.....ص65

المطلب الأول: الذكاء الاصطناعي ومشروعيته الدوليةص66

المطلب الثاني: الآثار الإيجابية والسلبية التي يحدثها الذكاء الاصطناعي في الأمن السيبراني.....ص72

المبحث السابع

الذكاء الاصطناعي واستخدامه في إجراءات التقاضي...ص81

المطلب الأول: دور الذكاء الاصطناعي في تعزيز العدالة الناجزة أمام القضا...ص82

المطلب الثاني: الدول التي تستخدم الذكاء الاصطناعي في إجراءات التقاضي...ص86

المطلب الثالث: تحديات ومخاطر الذكاء الاصطناعي على إجراءات التقاضي...ص91

المراجع

أولاً: المعاجم.

- 1- جميل صليبا، المعجم الفلسفي، ط: لأولى، دار الكتاب اللبناني، بيروت 1970م.
- 2- راتب أحمد قبيعة، القاموس العربي الوسيط، ط: الأولى، دار الراتب، بيروت 1670م

ثانياً: الرسائل العلمية.

- 1- أحمد ضياء الدين، مشروعية الدليل في المواد الجنائية، رسالة دكتوراه قُدمت إلى كلية الحقوق جامعة عين شمس، القاهرة 1984م.
- 2- اسامة مهمل ، الاجرام السيبراني ، رسالة ماجستير ، كلية الحقوق والعلوم السياسية – جامعة محمد بوضياف الجزائر 2017م – 2018م.
- 3- الحسين الطيب عبد السلام الأسمر الحضيري ، الاثبات الجنائي بالوسائل العلمية الحديثة ، رسالة ماجستير مقدمة إلى جامعة مولانا مالك إبراهيم الإسلامية ، السودان 2016م .
- 4- براهيمي جمال ، التحقيق الجنائي في الجرائم الالكترونية ، رسالة دكتوراه مقدمة إلى كلية الحقوق والعلوم السياسية – جامعة مولود معمري – الجزائر .
- 5- بشرى عواطة، حجية الدليل الالكتروني في الاثبات الجنائي، ، رسالة ماجستير مقدمة إلى كلية الحقوق والعلوم السياسية – جامعة 8 مايو 1945، الجزائر 2017م – 2018م.
- 6- خالد ساسوي، محمد بن حسين، الحروب السيبرانية والأمن العالمي التحديات والمواجهة، رسالة ماجستير مقدمة إلى كلية الحقوق والعلوم السياسية – جامعة زيان عاشور 2019م – 2020م.
- 7- سعيداني نعيم آية البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير قدمت إلى كلية الحقوق والعلوم السياسية – جامعة الحاج لخضر، الجزائر 2013م.

- 8- شهر زاد حداد، الدليل الإلكتروني في مجال الاثبات الجنائي، رسالة ماجستير قُدمت لكلية والعلوم السياسية- جامعة العربي مهدي أم البواقي 2016م – 2017م.
- 9- عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية، رسالة ماجستير مقدمة إلى جامعة الشرق الأوسط 2014م.
- 10- فوزي عمارة، اعتراض المرسلات وتسجيل الأصوات والتقاط الصور والتسرب كالأجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية – جامعة قسنطينة، الجزائر ، العدد (33) يونيو 2010م.
- 11- عبد المطلب طاهري، الاثبات الجنائي بالأدلة الرقمية، رسالة ماجستير مقدمة إلى كلية الحقوق والعلوم السياسية – جامعة المسيلة 2014م – 2015م.
- 12 محمد أحمد لريد، نظرية ظروف الجريمة في الفقه الجنائي الإسلامي وقانون العقوبات الجزائري، رسالة دكتوراه مقدمه إلى كلية العلوم الإنسانية – جامعة وهران، الجزائر 2008م – 2009م.
- 13- محمد بن أبي بكر عبد القادر الرازي، مختار الصحاح، المطبعة الاميرية، القاهرة 2016م.
- 14- ناصر آل ثنيان، إثبات الجريمة الإلكترونية – دراسة تأصيلية تطبيقية -، (رسالة ماجستير)، جامعة نايف للعلوم الأمنية، كلية الدراسات العليا، الرياض 2012م.
- 15- نورة طرشي، مكافحة الجرائم المعلوماتية، رسالة ماجستير مقدمة إلى كلية الحقوق – جامعة الجزائر 2011م – 2012م.

ثالثاً: الكتب

- 1- أبو العباس أحمد بن إدريس القرافي، الذخيرة - المجلد الأول -، الطبعة الأولى، دار الكتب العلمية ، بيروت 1974م .
- 2- أحمد ابراهيم، طرق الاثبات الشرعية، مطبعة القاهرة الحديثة للطباعة، القاهرة، مصر.
- 3- أحمد أبو القاسم، الدليل الجنائي المادي ودوره في اثبات جرائم الحدود والقصاص، الجزء الأول ، دار النشر بالمركز العربي للدراسات الأمنية والتدريب ، الرياض 1993م.

- 4- أحمد عبيد المجيد الحاج ، جرائم النشر الصحفي الالكتروني وأحكام المسؤولية الجنائية (دراسة مقارنة) ، وزارة الاعلام الإماراتية العربية 2007م
- 5- أحمد محمد العمر، الدليل الرقمي وحجته في الإثبات الجزائي، مجلة المعهد العالي للقضاء، العدد الثالث، يناير 2020م.
- 6- احمد فتحي زغلول، شرح القانون المدني، المطبعة الاميرية، مصر، 1913.
- 7- أحمد يوسف الطحاوي، الأدلة الالكترونية ودرها في الاثبات الجنائي، دراسة مقارنة، دار النهضة العربية، القاهرة 2015م
- 8- أسامة أحمد المناعسة وآخرون ، جرائم الحاسب الآلي ، دراسة تحليلية مقارنة ، ط : الأولى ، دار وائل للنشر ، عمان 2001م .
- 9- أشرف عبد القادر قنديل، الاثبات الجنائي في الجريمة الالكترونية، دار الجامعة الجديدة، الإسكندرية 2009م.
- 10- آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط: الثانية، دار هومو الجزائر 2007م.
- 11- بارة سمير، الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر، جامعة قاصدي مرياح ورقلة – كلية الحقوق والعلوم السياسية 2001م.
- 12- د/ جلال فضل محمد العودي، القرصنة البحرية وحرية أعالي البحار، الطبعة: الأولى، دار النشر المصرية للنشر والتوزيع، القاهرة 2020م.
- 13- جلال فضل محمد العودي، مقالات في الجرائم السيبرانية، شبكة أجهزة إنفاذ القانون بشأن مكافحة الجريمة الإلكترونية، مكتب النائب العام عدن 2022م.
- 14- جلال فضل محمد العودي، الإرهاب السيبراني، شبكة أجهزة إنفاذ القانون بشأن مكافحة الجريمة الإلكترونية، مكتب النائب العام عدن 2022م.
- 15- دكتور جلال فضل محمد العودي، مخاطر الذكاء الاصطناعي على الأمن السيبراني، بحث مقدم للندوة العلمية (التعاون الدولي في قضايا الأمن السيبراني) المنعقدة في المعهد القضاء الأردني بتاريخ 16 ديسمبر 2024م
- 16- د. جلال فضل محمد العودي، الذكاء الاصطناعي واستخدامه في إجراءات التقاضي، بحث مقدم للورشة التدريبية (تبادل الخبرات في مجال الذكاء الاصطناعي المطبقة على الأنظمة القضائية) المنعقدة في معهد القضاء الاردني بتاريخ 18/6/2025م .

- 17- حياة البشيرى ، دور الدليل الإلكتروني في الإثبات الجنائي ، المعهد العالي للقضاء وزارة العدل المغربية 2015 – 2017م.
- 18- خالد عياد الحلبي، إجراءات التحري والتحقيق في جريمة الحاسوب والانترنت، ط: الأولى، دار الثقافة للنشر والتوزيع، عمان – الأردن، 2011.
- 19- خالد مصطفى الجسمي، الإثبات الجنائي بالأدلة الرقمية، مجلة القانون المغربي، دار السلام للطباعة والنشر، العدد (34) 2007م.
- 20- خالد مصطفى فهمي ، الحماية القانونية لبرنامج الحاسب الالى في ضوء قانون الحماية الفكرية ، دار الجامعة الجديدة للنشر ، الإسكندرية 2005.
- 21- خلية وريدة، إشكالية المواطنة في ظل قيم التكنولوجيا الحديثة بين حرية المواطن والأمن السيبراني، حوليات جامعة الجزائر، المجلد (35) العدد (2)، كلية الإعلام والاتصال – جامعة الجزائر 2021م.
- 22- دنيازاد ثابت، مطبوعات محاضرات مقباس الإثبات الجنائي، كلية الحقوق والعلوم السياسية- جامعة العربي النبسي، الجزائر 2020م – 2021م.
- 23- رامي القاض، مكافحة الجرائم المعلوماتية في التشريعات المقارنة في ضوء الاتفاقيات والمواثيق الدولية، دار النهضة العربية، ط: الأولى القاهرة 2011م.
- 24- سناء منعم: "اللسانيات الحاسوبية والترجمة الآلية"، عالم الكتاب الحديث، ط1.
- 25- صالح بن علي بن عبد الرحمن الربيعه، الأمن القومي وحماية المستخدم من مخاطر الانترنت، هيئة الاتصالات وتقنية المعلومات، المملكة العربية السعودية 2020م.
- 26- طارق أحمد ماهر زغلول، شرح قانون الإجراءات الجزائية العمانية – الجزء الثاني -، المحاكمة وطرق طعن في الاحكام، ط: الأولى، دار الكتاب الجامعي، 2016.
- 27- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة 2010م.
- 28- عادل عبد النور، مدخل إلى عالم الذكاء الاصطناعي، دار النشر مدينة الملك عبد العزيز للعلوم والتقنية، السعودية.

- 29 د/ عادل مختاري، دور القاضي الجزائري في ظل مبدأ الاقتناع القضائي، مجلة المنتدى القانوني، العدد الخامس، مارس 2008م، كلية الحقوق والعلوم السياسية، بجامعة محمد خضير، بسكرة.
- 30- عبد الرزاق السنهوري، الوسيط في نظرية الالتزام بوجه عام، دار احياء التراث العربي، بيروت 2007م .
- 31- عبد الفتاح بيومي حجازي، الاثبات في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، القاهرة 2007م.
- 32- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جريمة الكمبيوتر والانترنت، دار الكتل القانونية، القاهرة 2005.
- 33- عبد الفتاح بيومي حجازي لحماية التجارة الالكترونية - الكتاب الأول -، نظام التجارة الالكترونية وحمايتها مدنيا، دار الفكر الجامعي، الإسكندرية 2002.
- 34- عبد الإله أحمد الهلالي، حجية المخرجات الكمبيوترية في المواد الجنائية -دراسة مقارنة-، دار النهضة العربية، القاهرة 2008م .
- 34- علي حسن الشرفي، النظرية العامة للجريمة - شرح قانون العقوبات اليمني(القسم العام - الجزء الأول)، مكتبة الوسيلة للنشر والتوزيع، صنعاء 2014.
- 35- نهلا عبد القادر المومني، الجرائم المعلوماتية، ط: الأولى، دار الثقافة للنشر والتوزيع، عمان - الأردن 2008م.
- 36 عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والانترنت، بهجت للطباعة والتجليد، مصر 2009م
- 37- محمد أمين الشوابكة، جرائم الحاسوب والانترنت (الجريمة المعلوماتية)، دار الثقافة للنشر والتوزيع، عمان - الأردن 2009
- 38- محمد الألفي، المسؤولية الجنائية عن الجرائم الأخلاقية عبر الانترنت، المكتب المصري الحديث، القاهرة.
- 39- محمد الأمين البشري، التحقيق في الجرائم المستحدثة، أكاديمية نايف العربية للعلوم الأمنية، الرياض 2004م.
- 40- د/ محمد رضا فودة، "الاستراتيجية والأمن القومي، المكتب العربي للمعارف"، القاهرة 1995م.

41- د/ محمد عبد الحميد عرفة، مدى حُجِّيَّة الأدلة الإلكترونية الرقمية في الإثبات الجنائي – دراسة مُقارنة -، مجلة الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية العدد 1، سنة 2018م.

42- محمود أحمد القرعان، الجرائم الإلكترونية، دار وائل للنشر والتوزيع، ط: الأولى، عان – الأردن 2017م.

43- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر، دار الكتب القانونية، القاهرة 2009م

44- منى الأشقر حبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت 2017م.

45- مولاى امحمد، صعوبات تطبيق الإدارة الإلكترونية بالجزائر،: الجريمة الإلكترونية نموذجاً، المؤتمر العالمي الأول للإدارة الإلكترونية، مركز المدنية للوسائل المتعددة، طربلس 2010م.

رابعاً: المجالات والدوريات:

1- د. إبراهيم الدستوقي أبو الليل، العقود الذكية والذكاء الاصطناعي ودورها في أتمتة العقود والتصرفات القانونية، مجلة الحقوق، جامعة الكويت 2020م.

2- أحمد محمد العمر، الدليل الرقمي وحجتيه في الإثبات الجزائي، مجلة المعهد العالي للقضاء، العدد الثالث، يناير 2020م.

3- آمنة على البشير محمد، الأمن السيبراني في فضاء مقاصد الشريعة، مجلة كلية الدراسات الإسلامية والعربية للبنات بالإسكندرية، العدد (37)، المجلد الأول.

4- الأمن السيبراني، مجلة الأمن السياسي، مجلة صادرة عن الجهاز المركزي للأمن السياسي بالجمهورية اليمنية العدد(11)، أكتوبر 2023م.

5- د. جلال فضل محمد، دور الذكاء الاصطناعي في تعزيز العدالة الناجزة أمام القضاء، صحيفة القضائية، وزارة العدل – الجمهورية اليمنية، العدد(7)، الأربعاء 31 يوليو 2024م

- 6- د. جمال بوازدية، الإستراتيجية الجزائية في مواجهة الجرائم السيبرانية " التحديات والافاق المستقبلية، مجلة العلوم القانونية والسياسية، المجلد (10)، العدد (1)، جامعة الجزائر 2019م.
- 7- خالد مصطفى الجسمي، الاثبات الجنائي بالأدلة الرقمية، مجلة القانون المغربي، دار السلام للطباعة والنشر، العدد (34) 2007م.
- 8- سميرة معاشي، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني، العدد السابع، كلية الحقوق والعلوم السياسية – جامعة محمد خضيرة، سكرة 2010م.
- 9- سوسن سعيد شندي ، دليل الاثبات الالكتروني ، مجلة جامعة شندي بالسودان ، العدد يوليو 2011 م .
- 10- عبد الرحمن حسن، ورقة عمل بحثية مقدمة لمؤتمر تمكين الأول للذكاء الاصطناعي والابتكار وريادة الاعمال، بريطانيا 2024م.
- 11- عبد السلام محمد المايل، د/ عادل محمد الشرجي، د/ علي قابوسة، الجريمة الإلكترونية في الفضاء الالكتروني، بحث منشور في مجلة أفاق للبحوث والدراسات سداسية، المركز الجامعي ايليزي – طرابلس، العدد (4) يونيو 2019م
- 12- فاطمة يوسف المنتشري، دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات، المجلة العربية للعلوم التربوية والنفسية، المجلد الرابع، العدد (17) يوليو 2020م.
- 13- فوزي عمارة، اعتراض المرسلات وتسجيل الأصوات والتقاط الصور والتسرب كالأجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية – جامعة قسنطينة، الجزائر، العدد (33) يونيو 2010م.
- 14- لورنس سعيد الحوامدة، حجية الأدلة الرقمية في الاثبات الجنائي – دراسة تحليلية مقارنة -، مجلة البحوث الفقيه والقانونية، العدد السادس والثلاثون، أكتوبر 2021 م ، جامعة طيبة.
- 15- محمد الأمين البشري، التحقيق في الجرائم المستحدثة، أكاديمية نايف العربية للعلوم الأمنية، الرياض 2004م.
- 16- محمد عبد الحميد عرفة، مدى حُجِّية الأدلة الالكترونية الرقمية في الاثبات الجنائي – دراسة مُقارنة -، مجلة الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية العدد 1، سنة 2018م.

17- مسعود بن حميد المعمري، الدليل الالكتروني لإثبات الجريمة الالكترونية، مجلة القانون الكويتية، العدد (6)، 2018م.

18- د. مني عبد الله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية – جامعة المنصورة، العدد 111 – يونيو 2020م.

المراجع الأجنبية

1- أ. أوسوبا أوسوندي، وبلسر الرابع وويليام، مخاطر الذكاء الاصطناعي على الأمن ومستقبل العمل، راند.

-2

Chen, L., Wang, T., & Yang, Z. (2022). Learning from Previous Attacks: AI's Role in Proactive Cybersecurity. Journal of Cyber Intelligence, 8(1), 73-89

-3

Evans, M., & Lee, S. (2021). Bias and Errors in AI-based Cyber Defense Systems. Journal of Cyber Ethics, 3(4), 15-29

-5

Johnson, D., & Smith, A. (2019). The Automated Response of AI in Cybersecurity. IT Security Research, 11(3), 99-114

-6

Kumar, R. (2020). Machine Learning for Early Threat Detection. Cyber Threat Analysis, 6(1), 23-37

-7

Miller, K. (2020). AI-driven Cyber Attacks: A New Wave of Threats. Hacker's Quarterly, 14(2), 40-52

-8

Williams, P. (2019). Reliance on AI in Cyber Defense: Risks and Realities. IT Management Review, 12(4), 56-64

خامساً: المواقع الإلكترونية.

1- أنظر: إبراهيم قاسم - أحمد عبد الهادي، تيسير إجراءات التقاضي.. تطبيق الذكاء الاصطناعي في تحويل الكلام إلى نص مكتوب بالمحاكم، على الموقع الإلكتروني:

<https://www.youm7.com/story/2023/5/30/%D8%AA%D9%8A%D8%B3%D9%8A%D8%B1>

2- الأمن السيبراني / تعريف مقالة على مدونة بالفرنسية على الرابط :

<https://www.sage.com/fr-fr/blog/glossaire/cybersecurite-definition-de-la-cybersecurite>

3- تهديدات للأمن السيبراني للشركات لعام 2023م، مقالة على موقع شركة Ester رابط المقالة :

<https://www.exter.fr/cybersecurite-en-entreprise>

4- ثغرات الأمن السيبراني: ضرورة الاعتراف بالعامل البشري، مقالة على موقع شركة اورانج الفرنسية.

<https://www.orange cyberdefense.com/fr/insights/blog/cyberdefense/failles-de-cybersecurite-la-necessite-de-reconnaitre-le-facteur-humain>

5- سهام عثمانى، الأمن السيبراني في قلب تحديات الأعمال الحديثة، مقالة في ملف عن الامن السيبراني بالفرنسية على الرابط /

<https://www.village-justice.com/articles/cybersecurite-coeur-des-enjeux-entreprise-moderne,39117.html>

6- طلعت الصناديلي، كيف يُقع الجاني ضحيته للجريمة الإلكترونية، صحيفة الاهرم المصرية، الصادرة 2022/12/8م، على الموقع الالكتروني:

<https://gate.ahram.org.eg/News/3871077.aspx>

7- صحيفة الاتحاد الإماراتية الاثنين 12 ديسمبر 2022م على الموقع الالكتروني:

<https://alittihad.ae/news/%D8%AF%D9%86%D9%8A%D8%A7/4337393>

8- ادوارد ماير، الذكاء الصناعي في خدمة الأمن السيبراني، مقالة على الرابط :

<https://maltem.com/en/blog/ia-service-cyber-securite>

9- أمن مواقع الشبكات الاجتماعية، مقالة على الموقع الحكومي الفرنسي حول البرمجيات الخبيثة، على الرابط

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/reseaux-sociaux>

10- الأمن السيبراني، تحدي اساسي للشركات في العام 2023م، مقالة على الرابط:

<https://www.fibre-pro.fr/cybersecurite>

11- تركيز على ادارة مخاطر الاعمال - مقالة بالفرنسية منشورة في موقع ادارة المخاطر، على الرابط:

<https://www.c-risk.com/fr/blog/gestion-des-risques>

12- تهديدات رئيسية، مقالة على الموقع الرسمي للوكالة الوطنية الفرنسية لأمن وحماية أنظمة المعلومات، على الرابط:

<https://www.ssi.gouv.fr/entreprise/principales-menaces>

13- الأمن السيبراني، تحدي أساسي للشركات في العام 2023م، مقالة على الرابط:

<https://www.fibre-pro.fr/cybersecurite>

14- صحيفة الشرق الأوسط السعودية على الموقع الإلكتروني:

<https://aawsat.com/%D9%81%D9%8A-%D8%A7%D9%84%D8%B9%D9%85%D9%82/%D8%AA%D8%AD%D9%82%D9%8A%D9%82%D8%A7%D8%AA-%D9%88%D9%82%D8%B6%D8%A7%D9%8A%D8%A7/4368481-%D9%85%D8%A7-%D9%87%D9%88-%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1-%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A-%D9%88%D9%83%D9%8A%D9%81-%D9%8A%D8%B9%D9%85%D9%84%D8%9F>

15- صحيفة الشرق الأوسط السعودية على الرابط الإلكتروني:

<https://aawsat.com/%D8%A7%D9%84%D8%A7%D9%82%D8%AA%D8%B5%D8%A7%D8%AF/5021709-%D8%A3%D9%88%D8%B1%D9%88%D8%A8%D8%A7-%D8%AA%D8%B9%D8%AA%D9%85%D8%AF>

16- وكالة الأنباء العمانية على الموقع الإلكتروني:

<https://omannews.gov.om/topics/ar/86/show/433504/ona#:~:text=%D9%88%D8%B0%D9%83%D8%B1%20%D8%A7%D9%84%D9%85%D8%AC%D9%84%D8%B3%20%D9%81%D9%8A%20%D8%A8%D9%8A>

17- بون - المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات ECCI - على الموقع الإلكتروني:

<https://www.europarabct.com/%D8%A3%D9%85%D9%86-%D9%82%D9%88%D9%85%D9%8A-%D9%80-%D8%AF%D9%88%D8%B1-%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1-%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7/%D8%B9%D9%8A-%D9%81%D9%8A-%D8%A7%D9%84>

-18

<https://www.skynewsarabia.com/business/1646519-%D8%A7%D9%94%D8%A8%D8%B1%D8%B2-%D8>

19- الموقع الإلكتروني لقناة الجزيرة على الرابط الإلكتروني:

<https://www.aljazeera.net/tech/2023/6/11/%d9%85%d8%b3%d8%aa%d9%82%d8%a8%d9%84-%d8%a7%d9%84%d8%b0%d9%83%d8%a7%d8%a1-%d8%a7%d9%84%d8%a7%d8%b5%d8%b7%d9%86%d8%a7%d8%b9%d9%8a-%d9%85%d8%a7-%d9%87%d9%8a-%d8%a3%d8%b3%d9%88%d8%a3>

20- الموقع الإلكتروني:

<https://unite.ai/ar/%D9%83%D9%8A%D9%81-%D8%B3%D9%8A%D8%A4%D8%AB%D8%B1-%>

21- الموقع الإلكتروني:

<https://kharchoufa.com/%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1-%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A-%D9%88%D8%A7%D9%84%D9%82%D8%B6%D8%A7%D8%A1>



المعهد القضائي الأردني

JUDICIAL INSTITUTE OF JORDAN

المؤلف:

دكتور / جلال فضل محمد العودي
عضو هيئة التدريس في المعهد العالي للقضاء / وزارة العدل
الجمهورية اليمنية
اكاديمي ومعد لعدد من الدراسات والابحاث القانونية المحكمة
والمنشورة

