

مجلة العلوم القانونية والاجتماعية

Journal of legal and social studies

Issn: 2507-7333

Eissn: 2676-1742

فعالية أنظمة الذكاء الاصطناعي في مكافحة الاحتيال الإلكتروني

The Effectiveness of Artificial Intelligence Systems in Combating Cyber Fraud

حمزة غندور¹ ، سليمة قواسمية²

¹ جامعة الشاذلي بن جديد - الطارف، (الجزائر)، h.ghandour@univ-eltarf.dz

² جامعة باجي مختار - عنابة، (الجزائر)، gouasmia.salima36@gmail.com

تاريخ النشر: 2025/03/01

تاريخ القبول: 2025/01/01

تاريخ ارسال المقال: 2024/12/02

*المؤلف المرسل

الملخص:

هدفت هذه الدراسة للبحث في واقع استخدام برامج الذكاء الاصطناعي، من خلال التطرق إلى أهم مخاطره وسلبياته على الأفراد والجماعات، كما سعت كذلك إلى تقصي ظاهرة الاحتيال الإلكتروني المعزز بتقنيات الذكاء الاصطناعي، والبحث في سبل مكافحة هذا الخطر من خلال مختلف البرمجيات والتقنيات التي يطرحها الذكاء الاصطناعي، تم الاستعانة بالمنهج الوصفي كون هذه الدراسة تسعى للبحث في خلفيات الظاهرة ومسبباتها ونتائجها، خرجت الدراسة بمجموعة من النتائج البحثية التي كانت أبرزها أن هناك العديد من البرامج والتقنيات التي تستعين بها المؤسسات في عمليات حماية البيانات العامة والخاصة للأفراد، إضافة إلى ذلك فإن العديد من الهيئات الدولية بادرت لتبني استراتيجيات أمنية لتحقيق أقصى درجات الأمان السيبراني، كما أن عمليات الاحتيال الإلكتروني تتطور بشكل مستمر مما جعل من عمليات التصدي لها بالغة الصعوبة بحكم تعدد أساليب وأشكال الاختراق والاحتيال التي يتبعها لصوص الإنترنت.

الكلمات المفتاحية: الأمن السيبراني ; الاحتيال الإلكتروني ; الذكاء الاصطناعي ; الهجمات السيبرانية

Abstract :

This study aimed to investigate the current state of artificial intelligence software usage, delving into its significant risks and negative impacts on individuals and societies. It further sought to explore the phenomenon of AI-enhanced cyber fraud and to examine methods of combating this threat through various software and technologies offered by artificial intelligence. A descriptive approach was employed, given that this study aimed to explore the background, causes, and consequences of this phenomenon. The study yielded a set of research findings, most notably that numerous institutions are utilizing various software and technologies to protect the public and private data of individuals. Additionally, many international organizations have taken the initiative to adopt security strategies to achieve the highest levels of cybersecurity. Moreover, cyber fraud is continually evolving, making countermeasures exceedingly challenging due to the multitude of hacking and fraud methods employed by cybercriminals.

Keywords: cybersecurity ; cyberscam ; artificial intelligence ; cyberattacks

مقدمة:

لقد أدت التطورات السريعة في مجال تكنولوجيا المعلومات والاتصالات إلى إحداث ثورة رقمية متسارعة على خلفية ما أنتجته الثورة الصناعية الرابعة التي أنتجت ما يعرف بالتنافس السيبراني أو السباق نحو اكتساب الذكاء الاصطناعي وجعله جزءاً لا يتجزأ من الحياة الاقتصادية والاجتماعية للأفراد والجماعات والحكومات، فنجد اليوم أن البرمجيات الذكية المعززة بالذكاء الاصطناعي غزت مختلف المجالات "كالصحة" التي ظهرت فيها روبوتات متطورة قادرة على القيام بعمليات جراحية دقيقة، وكذا "التعليم" من خلال تلك التطبيقات الذكية CHAT GPT ناهيك عن الطائرات المسييرة والروبوتات التي تستخدم في الإنقاذ والتنبؤ بالحوادث والطقس...، وهو ما جعل هذه البرمجيات الذكية تصنف في خانة الفائدة الحيوية التي تسه حياة البشر.

غير أن هذا التطور الرهيب بفعل الذكاء الاصطناعي المتعدد المجالات خلق نوعاً من الشك والارتباك لدى العديد من الأفراد والحكومات والمؤسسات على خلفية التهديدات الأمنية التي أصبحت تشكلها تلك التطبيقات والروبوتات الذكية، فالانتشار الكبير للخروقات الأمنية بفعل البرامج الخبيثة "برامج الفدية"، وكذا التعدي على الخصوصية العامة والخاصة للأفراد من خلال الاستيلاء على البيانات الضخمة والتحكم في مختلف المعلومات الخاصة، ناهيك عن التهديدات الوجودية للعديد من الحكومات والمؤسسات عن طريق الاحتيال الإلكتروني المختلف الأساليب والطرق التي تعددت باختلاف الغايات والمقاصد، خاصة تلك المتعلقة بالنصب والاحتيال على الحسابات البنكية والمصارف، وهو ما أحدث أضراراً اقتصادية واجتماعية كبيرة قدرت بملايير الدولارات سنوياً بفعل الهجمات السيبرانية، فأكبر خطر يفرضه الاحتيال الإلكتروني هو الخسائر المالية، حيث تظهر الإحصائيات والاتجاهات أن الهجمات الإلكترونية هي واحدة من أكثر التهديدات تكلفة للشركات والمؤسسات على المستوى العالمي ما يقدر بنحو 24 تريليون دولار خلال عام 2024، ناهيك عن تهديدات الاستيلاء على البيانات الشخصية الخصوصية وهو ما يبرز حجم الخطر الذي يهدد أمن المجتمعات والمؤسسات، الأمر الذي دفع بالعديد من الحكومات والهيئات الدولية لتبني استراتيجيات ومبادرات أمنية استعجالية للحد من تفشي هذا الخطر الإلكتروني الذي عزز بذكاء الآلة الاصطناعية، رغبة منها في حماية الأفراد والمؤسسات من الاحتيال الإلكتروني (المعلوماتي)، من خلال تفعيل الذكاء الاصطناعي للتصدي للهجمات الاحتيالية الرقمية (الإلكترونية)، وهو ما نسعى له في هذه الدراسة من خلال طرح التساؤل الرئيسي التالي:

ما هو دور الذكاء الاصطناعي في التصدي للاحتيال للإلكتروني؟ والذي تفرعت عنه الأسئلة الفرعية التالية:

- فيما تتمثل أبرز المخاطر المرتبطة بالذكاء الاصطناعي؟
- ما هي أبرز مظاهر الاحتيال الإلكتروني المعزز بالذكاء الاصطناعي؟
- فيما تتمثل أبرز المبادرات والحلول الإستراتيجية في مكافحة الاحتيال الإلكتروني؟

أهداف الدراسة:

يعتبر موضوع الاحتيال الإلكتروني من بين المواضيع الحديثة والمتجددة بحكم ارتباطها بالتطور التكنولوجي والرقمي الذي تشهده المجتمعات، حيث تمثلت أبرز أهداف الدراسة في:

- _ التعرف على مفهوم الذكاء الاصطناعي وأبرز خصائصه وأشكاله ووسائله.
- _ البحث في واقع الاحتيال الإلكتروني المتصل بالذكاء الاصطناعي وتداعياته.
- _ التعرف على طرق وأساليب مكافحة الاحتيال الإلكتروني من خلال الذكاء الاصطناعي.

أهمية الدراسة:

تبرز الأهمية العلمية والعملية لهذه الدراسة في كونها تعالج موضوعاً جديداً ومتشعباً بالنظر لكم المعلومات النظرية التي يشتمل عليها، لذلك فهي تعتبر دراسة مكتملة للعديد من الدراسات التي بحثت في واقع استخدامات الذكاء الاصطناعي في جانبها السلبي، من خلال التعرف على مخاطره وسلبياته التي أدت إلى ظهور مجموعة من الظواهر والممارسات الانحرافية كالاختيال الإلكتروني المتعدد الأشكال، كما أنها تشكل انطلاقة حقيقية من أجل معالجة المشاكل التي انجرت عن الاستخدام السيء لبرامج الذكاء الاصطناعي.

منهج الدراسة:

تعد هذه الدراسة النظرية من بين الدراسات الكيفية التي تبحث في الظاهرة بشكل معمق من خلال تحديد مسبباتها الرئيسية وكذا خلفياتها، الأمر الذي استدعى استخدام المنهج الوصفي الذي يعد من بين المناهج الملائمة لكذا دراسات كيفية تبحث في حثيات الظاهرة وتحاول إيجاد حلول لها وفق ما تمليه خطوات المنهج العلمي.

المبحث الأول: الذكاء الاصطناعي كتقنية تكنولوجية

سنعالج في هذا المبحث مختلف المفاهيم الأساسية لمصطلح الذكاء الاصطناعي وخصائصه، ناهيك عن مجالات استخدامه، إيجابياته وكذا سلبياته على الأفراد والجماعات والحكومات باعتباره توجه رقمي جديد فرض واقعه في الحياة العامة والخاصة داخل المجتمعات كافة.

المطلب الأول: مفهوم الذكاء الاصطناعي

أنظمة الذكاء الاصطناعي هي أنظمة برمجية وربما أيضاً أجهزة صممها البشر والتي تعمل - نظراً لهدف معقد - في البعد المادي أو الرقمي عن طريق إدراك بيئتها من خلال الحصول على البيانات، وتفسير البيانات المجمعة المنظمة أو غير المنظمة والتفكير في المعرفة، أو معالجة المعلومات المستمدة من هذه البيانات، وتحديد أفضل الإجراءات الذي يجب اتخاذها لتحقيق الهدف المحدد، وبإمكان أنظمة الذكاء الاصطناعي إما استخدام قواعد رمزية أو تعلم نموذج رقمي، ويمكنها أيضاً تكييف سلوكها من خلال تحليل كيفية تأثير البيئة بأفعالهم السابقة⁽¹⁾.

وهو ذلك العلم الذي يجعل الحواسيب تتصرف وتعمل بطريقة تحاكي وتناهي الذكاء البشري، أو هو عبارة عن برامج وتقنيات حاسوبية طوّرت أساساً لكي تفكر كالإنسان، من خلال ما تتميز به من قدرات على القيام بالاستنتاجات والتحليلات المختلفة، وقدرتها على التعلم من أخطائها، وهو ما يجعلها تؤدي مهامها وأعمالها بسرعة ومهارة فائقة.

كما يدعم الذكاء الاصطناعي من خلال أنظمتها المتطورة تشغيل الأدوات العملية المتوفرة حولنا في كل مكان وتشغل هذه التقنيات مساحة في حياتنا اليومية لمساعدتنا على تنظيم الصور على هواتفنا الذكية أو التخطيط

لرحلة عمل، وتعمل هذه التقنيات على رصد المهام التي كانت تتطلب عادة تفكيراً بشرياً دقيقاً وتعمل على إنجازها باستخدام برمجية الحاسوب⁽²⁾.

ويعد الذكاء الاصطناعي أحد أهم مجالات التعلم التفاعلي القائم على الحواسيب، حيث يُشير إلى جهود تطوير نظم المعلومات المحوسبة بطريقة تجعلها تفكر بأسلوب مماثل للبشر تماماً، بحيث تستطيع إنجاز مهام فعلية بتنسيق متكامل، أو استخدام صور وأشكال إدراكية لترشيد السلوك المادي، كما تستطيع في نفس الوقت خزن الخبرات والمعارف الإنسانية المتراكمة⁽³⁾.

يعرفه "جون مكارثي" John McCarthy على أنه علم وهندسة صنع الآلات الذكية، كما أنه علم الحصول على قدرات الآلات وأنظمة الحواسيب واستغلالها لأداء المهام التي تتطلب ذكاء⁽⁴⁾.

المطلب الثاني: خصائص الذكاء الاصطناعي

يمتلك الذكاء الاصطناعي خصائص كثيرة جعلت منه استثماراً حقيقياً ذا فعالية في كثير من المجالات، حيث تمثلت أبرز خصائصه فيما يلي⁽⁵⁾:

- تطبيقات الذكاء الاصطناعي ومستقبل تكنولوجيا التعليم، فتطبيقات الذكاء الاصطناعي على الأجهزة والآلات تمكنها من التخطيط وتحليل المشكلات باستخدام المنطق.
- التعرف على على الأصوات والكلام والقدرة على تحريك الأشياء، حيث تستطيع الأجهزة المعززة بالذكاء الاصطناعي فهم المدخلات وتحليلها جيداً لتقديم مخرجات علمية دقيقة.
- تلبية احتياجات المستخدم بكفاءة عالية من خلال التعلم المستمر، حيث تكون عملية التعلم آلية وذاتية دون خضوعه للمراقبة.
- القدرة على معالجة كم هائل من المعلومات والبيانات التي يتعرض لها، خاصة تلك التي تعتبر أمنية وسرية.
- يستطيع ملاحظة الأنماط المتشابهة في البيانات وتحليلها بفعالية أكثر من الأدمغة البشرية.
- يستطيع إيجاد الحلول للمشكلات غير المألوفة باستخدام قدراته المعرفية التي زرعها فيه الإنسان بفعل مكتسباته وخبراته كونه مشابه للعقل البشري.
- القدرة على محاكاة العقل البشري في كثير من المجالات خاصة في مجال المراقبة والتصنيع.
- السرعة الكبيرة والدقة التي تسمح له بالقيام بمجموعة من المهام دون تعب أو خطأ⁽⁶⁾.

المطلب الثالث: مجالات استخدام الذكاء الاصطناعي

إن الطلب المتزايد على التقنية المتطورة والسرعة بحكم تزايد سوق المال والأعمال والاحتياجات، جعل العقل البشري يخترع برامج الذكاء الاصطناعي التي أصبحت تستخدم في العديد من المجالات الحيوية، حيث تمثلت أبرز المجالات في⁽⁷⁾:

أ- **الذكاء الاصطناعي في الرعاية الصحية:** من خلال تطبيقات ونظم الذكاء الاصطناعي توجد شواهد ملموسة على إمكانية تحسينه نتائج تشخيص وعلاج المرضى وتقليل الذكاء الاصطناعي التكليف.

صارت الشركات المختلفة تطبق تعلم الآلة لعمل تشخيصات أسرع وأحسن مما يقوم به الأطباء بدون الاستعانة بتطبيقات الذكاء الاصطناعي، ومن الأساليب الأكثر شيوعاً ومعرفة نظام IBM Watson الذي في قدرته فهم اللغة الطبيعية والاستجابة للأسئلة المطروحة له، ويبحث هذا النظام في بيانات المريض ومصادر البيانات المتوفرة الأخرى لتشكيل الفرضية التي تعرض مع مخطط تسجيل الثقة من النتائج المستنتجة.

كما تتضمن تقنيات الذكاء الاصطناعي الأخرى استخدام مساعدتي صحة افتراضيين ونظم Chatbots لمساعدة المرضى وعملاء الرعاية الصحية في إيجاد المعلومات الطبية المحتاج لها مثل جدولة المواعيد، فهم أبعاد عملية التسعير، وإكمال العمليات الإدارية الأخرى، بالإضافة لذلك تستخدم تكنولوجيات الذكاء الاصطناعي للتنبؤ ومقاومة الأمراض والأوبئة وفهمها كما هو الوضع في السابق مع وباء كورونا المستجد كوفيد - 19.

ب- الذكاء الاصطناعي في الأعمال: صارت خوارزميات تعلم الآلة تتكامل مع منصات التحليلات وإدارة علاقة العملاء (CRM) لكشف المعلومات، كما أن برمجيات Chatbots صارت متضمنة في مواقع الويب لتقديم خدمة فورية للعملاء، وفي نفس الوقت أصبحت آلية الأوضاع الوظيفية من المجالات التي تحظى باهتمام الأكاديميين إلى جانب تحليل تكنولوجيا المعلومات.

ج- الذكاء الاصطناعي في التصنيع: صار التصنيع في مقدمة المجالات التي توظف الروبوتات في تدفق العمل، على سبيل المثال، وعلى الرغم من أن الروبوتات الصناعية كانت مبرجة في الماضي لأداء مهام فردية ومتفرقة، أما حديثاً وبشكل متزايد فقد تم تطوير الروبوتات التعاونية Cobots، التي صارت حديثاً أصغر حجماً ومتعددة المهام والتي تتعاون مع البشر وتحمل كامل المسؤولية لأجزاء وظيفية أكثر كما في المستودعات المخازن المصانع وكثير من أماكن العمل الأخرى.

د- الذكاء الاصطناعي في التعليم: الذكاء الاصطناعي يمكن أن يؤدي لآلية رصد الدرجات المتعلقة بإنجازات واختبارات الطلاب، مما يعطي التربيين وقتاً أطول للعمل التربوي البناء، كما في قدرته تقييم الطلاب والتكيف لاحتياجاتهم، ومساعدتهم في التحصيل، إلى جانب تقديم برمجيات المقررات الدراسية الذكية (ITS) في مساندة إضافية للطلاب، مع التأكد من بقائهم ملتزمين بالمسار التعليمي. وإضافة لكل ذلك، في مقدرة تطبيقات الذكاء الاصطناعي أن تغير أين وكيف يتعلم الطلاب ومتى قد يحل الذكاء الاصطناعي محل المعلم البشري في إطار الإنسان الافتراضي⁽⁸⁾.

و- الذكاء الاصطناعي في التمويل: الذكاء الاصطناعي في تطبيقات التمويل الشخصية كما في حالات التعاملات المالية مع الضرائب والجمارك والرواتب وغيرها من أبعاد الشمول المالي صار معمولاً به في التقديرات التي تقوم بها المؤسسات المالية، حيث إن تطبيقات مثل جمع البيانات الشخصية تم تطبيقها من خلال عمليات التسويق والشراء من المنزل، إلى جانب توافر برمجيات الذكاء الاصطناعي في أداء كثير من الأعمال التجارية وأعمال البورصة وغيرها.

ي- الذكاء الاصطناعي في البنوك: صارت البنوك تطبق نظم برمجيات Chatbots بنجاح لجعل عملائها ملمين بالخدمات التي تقدمها البنوك إلى جانب تداول التصرفات المالية التي لا تتطلب تدخلاً بشرياً مباشراً. كما صارت برمجيات مساعدتي الذكاء الاصطناعي الافتراضية Virtual AI Assistants مستخدمة لتحسين وتقليل

تكاليف الالتزام مع اللوائح المصرفية، وفي نفس السياق تستخدم التنظيمات المصرفية الذكاء الاصطناعي لتحسين اتخاذ قراراتها التي تتعلق بالقروض ووضع حدود الائتمان، وتعريف فرص الاستثمار المتاحة والمتوقعة.

ه- الذكاء الاصطناعي في النقل: بالإضافة لدور الذكاء الاصطناعي في تفعيل المركبات ذاتية القيادة، تستخدم تكنولوجيا الذكاء الاصطناعي في صناعة النقل لإدارة المرور، التنبؤ بتأخير الرحلات، وجعل الشحن البحري والجوي أسلم وأكثر كفاءة.

ن- الذكاء الاصطناعي في الأمن: يعتبر استخدام الذكاء الاصطناعي وتعلم الآلة في قمة قائمة الألفاظ المترددة حديثاً بكثافة عن أمن المعلومات، وأمن الشبكات وأجهزة الحاسب الآلي لدى مطوري وموردي وبائعي البرمجيات في تمييز العروض⁽⁹⁾، وهو ما سنتطرق له في العناصر الموالية.

المطلب الرابع: إيجابيات للذكاء الاصطناعي

لقد أدى استخدام تقنيات وأنظمة الذكاء الاصطناعي إلى تحقيق مجموعة من المصالح والفوائد التي عادت بالنفع على الأفراد والجماعات والمؤسسات وهو ما شكل جانباً إيجابياً مهماً تمثل في⁽¹⁰⁾:

العمل المستمر: ستوفر تكنولوجيا الذكاء الاصطناعي العديد من الأجهزة التي باستطاعتها العمل المستمر وبدون توقف مما يعطي إنتاجية عالية وبالتالي سينعكس على الكلفة لأن هذه الأجهزة ليس لديها أي مطالبات مادية ولا حقوق أو غيرها بحسب حاجتها إلى الصيانة الدورية لضمان جودة نوعية المنتج وسهولة إنتاجه، كذلك القيام ببعض الأعمال التي يقوم فيها الإنسان بشكل يومي وأكبر مثال على ذلك استخدام الهاتف الذكي وتطبيقاته المختلفة كاستخدام تحديد المواقع وهي إحدى أشكال الذكاء الاصطناعي وغيرها من الأدوات التي من الممكن التفاعل معها عن طريق الصوت أو التلفزيونات الذكية، هذا إضافة إلى:

- استخدام الذكاء الاصطناعي في العديد من الشركات والبنوك في الرد على المتصلين وتوصيلهم بالخدمة التي يريدونها وفي أي وقت من ساعات النهار والليل، وبهذا يتم الاستغناء عن العامل البشري في تلك المهمة، أي خدمة العملاء الإلكترونية. وبهذا يتم التخلص من الأعمال الروتينية المتكررة والمملة أحياناً للموظفين.

- الدقة والتقليل من نسبة الخطأ في استخدام أنظمة الذكاء الاصطناعي، والدقة الكبيرة في أداء المهمات الصعبة.

- القيام بالأعمال الصعبة التي قد يعجز عن أدائها البشر كعمليات التنقيب في باطن الأرض والبحار والمحيطات وغيرها.

- الاستخدامات في مجال الرعاية الطبية، فهناك العديد من الأجهزة الطبية الحديثة التي تعتمد على أنظمة الذكاء الاصطناعي مثل الجراحات الإشعاعية التي تساعد على استئصال الأورام من دون إتلاف الأنسجة السليمة، والتنظيرات المختلفة، وكشف الاضطرابات العصبية والآثار الجانبية للأدوية وغيرها الكثير.

- قدرة أنظمة الذكاء الاصطناعي على معالجة كم هائل من البيانات وتخزينها ومعالجتها وبسرعة فائقة.

- استخدام الذكاء الاصطناعي بدلاً من الإنسان في بعض الوظائف قد يكون أكثر فاعلية في الإنتاج المستمر، حيث أن أجهزة الذكاء الاصطناعي على عكس الإنسان لا تتفاعل بالعاطفة وليست لديها حقوق وواجبات تجاه العمل ورأس المال، فيمكنها العمل من دون تعب أو ملل وتكرار العمل ملايين المرات وبلا توقف. قد يكون هذا

هو السبب الأكثر ملائمة للملاك من حيث ملكيتهم المطلقة لوسائل الإنتاج وأدواتها، وبهذه الحالة فالآلة التي تعمل بدلا من الإنسان هي ملك له فهي عبيد إلكترونية⁽¹¹⁾.

المطلب الخامس: سلبيات الذكاء الاصطناعي

تنطوي أنظمة الذكاء الاصطناعي على مجموعة من السلبيات التي قد تسبب مخاطر متنوعة على الأفراد والجماعات، حيث سنستعرض في هذا العنصر أبرز السلبيات التي جاءت بها برامج الذكاء الاصطناعي، حيث كانت كالتالي⁽¹²⁾:

التكلفة العالية: قد يكلف إنشاء الروبوتات وإعادة بنائها وإصلاحها مبالغ طائلة من المال والوقت. ويمكن أن يؤدي الإصلاح الآلي إلى تقليل الوقت ورغبة البشر في إصلاحها، ولكن هذا سيكلف أموالاً وموارد إضافية.

البطالة: يمكن للروبوتات مع استبدالها للوظائف، أن تسبب بطالة شديدة ما لم يتمكن البشر من حل مشكلة البطالة بوظائف لا يستطيع الذكاء الاصطناعي القيام بها أو تغيير الحكومة بشكل جذري إلى الشيوعية، وهو ما نلاحظه اليوم حيث أن انتشار استخدام الذكاء الاصطناعي والروبوتات المتطورة أدى إلى التخلص من اليد العاملة البشرية وتعويضها بالآلة الذكية.

عدم القدرة على التحكم: يمكن للآلات أن تسبب الدمار بسهولة إذا وضعت في الأيدي الخطأ، وهو ما تنجر عنه مخاطر أمنية ووجودية مرعبة من ناحية الاستيلاء على البيانات والتحكم في الأنظمة عن بعد وغيرها.

التبعية: إن الذكاء الاصطناعي يجعل البشر كسالى من خلال تطبيقاته التي تعمل على أتمتة الجزء الأكبر من العمل، ويميل البشر إلى التعلق بهذه الاختراعات التي قد تسبب عبئا على الأجيال القادمة.

عدم الكفاءة الكاملة: مع استبدال الذكاء الاصطناعي بأغلب المهام المتكررة والأعمال الأخرى بالروبوتات، أصبح التدخل البشري أقل، مما قد يسبب مشكلة كبيرة في معايير الاستخدام، وهو ما نلاحظه اليوم حيث تتطلع كل مؤسسة إلى استبدال الأفراد المؤهلين على الأقل بروبوتات الذكاء الاصطناعي التي يمكنها القيام بعمل مماثل بكفاءة أكبر.

غياب المشاعر: لا شك أن الآلات أفضل بكثير عندما يتعلق الأمر بالعمل بكفاءة، لكنها لا تستطيع أن تحل محل الاتصال البشري الذي يخلق الفريق، ولا تستطيع الآلات أن تنشئ رابطة مع البشر، وهي سمة مهمة عندما يتعلق الأمر بإدارة الفريق.

الصيانة الدورية: لا يمكن للآلات أن تؤدي إلا المهام التي تم تصميمها أو برمجتها للقيام بها، وأي شيء خارج هذا الإطار فإنها تميل إلى التعطل أو إعطاء مخرجات غير ذات صلة والتي قد تشكل خلفية خطيرة، كما تحتاج هذه الآلات المتطورة إلى صيانة دورية حتى لا تتعطل.

المبحث الثاني: أنظمة الذكاء الاصطناعي والاحتيال الإلكتروني

سننظر في هذا المبحث الثاني إلى مختلف المفاهيم الخاصة بالاحتيال الإلكتروني وأشكاله وخصائص وكذا فعالية تقنيات الذكاء الاصطناعي في الحد من الاحتيال الإلكتروني، الذي يعد من بين الجرائم التي أصبحت تشكل خطرا كبيرا على الحياة العامة للأفراد والجماعات بحكم ارتباطها بالتقنيات الرقمية المتطورة.

المطلب الأول: مفهوم الاحتيال الإلكتروني

يعرّف منتدى الاحتيال الإلكتروني النيجيري الاحتيال الإلكتروني بأنه "سلوك احتيالي مرتبط بالحوسبة يهدف من خلاله شخص ما إلى الحصول على ميزة غير شريفة. ويعرّفه الممارس القانوني فيما يتعلق بالخداع غير المشروع أو الجنائي الذي يؤدي إلى مكاسب مالية أو شخصية، فالاحتيال الإلكتروني هو احتيال أو سرقة تُرتكب باستخدام التكنولوجيا عبر الإنترنت لسحب الأموال بشكل غير قانوني من حساب مصرفي و/أو تحويل الأموال إلى حساب في بنك مختلف. الاحتيال الإلكتروني أو الاحتيال المصرفي عبر الإنترنت هو شكل من أشكال سرقة الهوية وعادة ما يتم ذلك من خلال تقنيات مثل التصيد الاحتيالي والاستيلاء على البنوك والمعلومات المتعلقة بالأفراد⁽¹³⁾.

كما يمكن تعريف الاحتيال عبر الإنترنت بأنه أي نوع من المخططات التي تستخدم مكونًا واحدًا أو أكثر من مكونات الإنترنت (على سبيل المثال، الدردشة، أو البريد الإلكتروني، أو موقع الويب) لنشر طلبات احتيالية، أو إجراء معاملات احتيالية⁽¹⁴⁾.

استعملت الكلمة أو المصطلح لأول مرة في القانون الفرنسي واعتبرت جريمة قائمة بذاتها في المادة 405 أما في القانون الجزائري فجرم الاحتيال الإلكتروني واعتبر أن كل من يتلقى أموال أو سندات وأوراق مالية، أو سلب أموال الغير أو الشروع في ذلك أو استعمال صفات أو أسماء كاذبة أو مواقع وهمية لتضليل الزبائن والمستهلكين⁽¹⁵⁾. وعليه يمكن تعريف التحايل الإلكتروني على أنه عمليات إجرامية تتم من خلال برامج حاسوبية أو تطبيقات رقمية معزز بالذكاء الاصطناعي، يراد منها الاستيلاء على بيانات ومعلومات خاصة بالأفراد يمكن استغلالها في عمليات القرصنة أو الابتزاز، كما تنطوي تحتها كل العمليات الإلكترونية التي يتحايل فيها لصوص الإنترنت على الأفراد والمؤسسات والحكومات بما فيها البنوك والمصارف والشركات الكبرى.

المطلب الثاني: أشكال الاحتيال الإلكتروني

يستخدم مجرمو الإنترنت مجموعة متنوعة من نواقل الهجوم والاستراتيجيات لارتكاب عمليات الاحتيال عبر الإنترنت، ويشمل ذلك البرامج الضارة وخدمات البريد الإلكتروني والمراسلة الفورية لنشر البرامج الضارة، ومواقع الويب المزيفة التي تسرق بيانات المستخدمين، وعمليات الاحتيال المعقدة والواسعة النطاق، ويمكن تقسيم الاحتيال عبر الإنترنت إلى عدة أنواع رئيسية من الهجمات، بما في ذلك⁽¹⁶⁾:

- **التصيد الاحتيالي والانتحال:** استخدام البريد الإلكتروني وخدمات المراسلة عبر الإنترنت لخداع الضحايا ودفعهم إلى مشاركة البيانات الشخصية وبيانات اعتماد تسجيل الدخول والتفاصيل المالية.
- **خرق البيانات:** سرقة البيانات السرية أو المحمية أو الحساسة من موقع آمن ونقلها إلى بيئة غير موثوقة، ويشمل ذلك سرقة البيانات من المستخدمين والمؤسسات.
- **رفض الخدمة:** مقاطعة الوصول إلى حركة المرور إلى خدمة أو نظام أو شبكة عبر الإنترنت للتسبب في نية خبيثة.
- **البرمجيات الخبيثة:** استخدام البرمجيات الخبيثة لإتلاف أو تعطيل أجهزة المستخدمين أو سرقة البيانات الشخصية والحساسة.

- **برامج الفدية:** نوع من البرامج الضارة التي تمنع المستخدمين من الوصول إلى البيانات المهمة ثم تطلب الدفع مقابل استعادة الوصول، يتم تقديم برامج الفدية عادةً عبر هجمات التصيد الاحتيالي.
- **اختراق البريد الإلكتروني للشركات (BEC):** شكل متطور من الهجمات يستهدف الشركات التي تقوم بشكل متكرر بإجراء مدفوعات عبر التحويلات المالية. وهو يخرق حسابات البريد الإلكتروني المشروعة من خلال تقنيات الهندسة الاجتماعية لتقديم مدفوعات غير مصرح بها⁽¹⁷⁾.

المطلب الثالث: خصائص جريمة الاحتيال الإلكتروني

تعد جريمة الاحتيال الإلكتروني من بين الجرائم الخطيرة والمنتشرة التي أصبحت تشكل هاجسا يؤرق الأفراد والجماعات والمؤسسات، حيث يشتمل هذا النوع من الجرائم المعلوماتية على مجموعة من الخصائص، حيث تمثلت أبرزها في⁽¹⁸⁾:

- **الاحتيال الإلكتروني من الجرائم العابرة للحدود:** يعني ذلك انها تمثل شكلا من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كله، مع وجود أجهزة الحاسوب المرتبطة بالشبكة العنكبوتية من غير ان تخضع لحدود الزمان والمكان، لذلك كان من السهولة ارتكاب الاحتيال مع عدم القدرة على كشفه، وهذه الخاصية خلقت العديد من المشاكل حول تحديد الدولة التي تكون صاحبة الاختصاص القضائي في حالة ما إذا كان المجرم من دولة والضحية من دولة أخرى، وكذا الاشكالية في القانون الواجب التطبيق وإجراءات الملاحقة القضائية.
- وبالنظر الى الطبيعة الخاصة لهذه الجريمة وخطورتها على المستوى الدولي، كان من الضروري التعاون الدولي في المعاهدات والاتفاقيات الدولية التي تعمل على توفير جو من التنسيق بين الدول الأعضاء من اجل التكفل بالإيقاع بالمجرم المعلوماتي ومحاكمته.

- **الاحتيال الإلكتروني من الجرائم التي يصعب اكتشافها:** تقع جريمة الاحتيال الإلكتروني في بيئة افتراضية لا تترك أية آثار على مرتكبها، لأن الضحية لا يلاحظها رغم أنها تقع أثناء وجوده على الشبكة، وهذا بفضل القدرات الفنية والتقنية التي يتمتع بها الجاني والتي تمكنه من جرمته بدقة.

- **الاحتيال الإلكتروني من الجرائم التي لا تقوم على العنف:** يعتمد ارتكاب هذا النوع من الجريمة على أسلوب لا يحتاج فيه الى مجهود عضلي كجرائم القتل والسرقة التقليدية، فهي تنفذ بأقل جهد ولا تتطلب نوعا من الإيذاء او الاختطاف او التكبسير، بل تعتمد فقط المعرفة الواسعة بتقنية المعلوماتية وشبكة الإنترنت والإحاطة ببعض البرامج التشغيلية، لذلك يطلق على هذا النوع من الجرائم بالجرائم الناعمة.

- **خصوصية المجرم المعلوماتي:** يطلق على المجرم الذي يرتكب هذا النوع من الجرائم بالمجرم المعلوماتي، ويتسم بخصائص معينة تميزه عن المجرم التقليدي، لأن جريمة الاحتيال الإلكتروني من الجرائم التقنية التي يرتكبها ذوي الاختصاص في مجال المعلومات الإلكترونية أو على الأقل الأشخاص الذين يكون لديهم حد أدنى من الدراية الكافية بالاستخدام والمعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الإنترنت.

المطلب الرابع: الحماية من الاحتيال الإلكتروني

بما أن جريمة الاحتيال الإلكتروني تعد من بين المخاطر الكبيرة التي تهدد أمن الأفراد والجماعات والمؤسسات، وبما أن الانتشار الرهيب لعمليات القرصنة وتخريب البيانات وانتهاك الخصوصية فإن العديد من الهيئات والمؤسسات الحكومية والغير حكومية لجأت إلى انتهاج مجموعة من الاستراتيجيات التي تريد من خلال التقليل من شدة الهجمات السيبرانية، وهو ما دفعها إلى تعزيز الدفاعات بأساليب رقمية معززة بالذكاء الاصطناعي، تمثلت أبرزها في⁽¹⁹⁾:

4-1- أساليب الأمن المعلوماتي: يمكن تجنب العديد من الاعتداءات التي تتعرض لها البيانات والمعلومات المدونة إلكترونياً، والتحكم في الدخول إليها إلا لمن له الحق بذلك، وفقاً لمجموعة من الآليات الدفاعية التي تمنع حدوث الاحتيال والاختراق للمواقع والبيانات، من خلال:

أ- التحكم بالدخول للأصول المعلوماتية: يكون هذا الإجراء عن طريق جهاز رقابة إيجابي يقوم بتحديد عما إذا كان الشخص طالب الدخول مصرحاً له بذلك أم لا والعمل بموجب ذلك، كما يقوم هذا الجهاز الإيجابي بالتحري عن شخصية المتصل بربط عملية تصريح الدخول والتحري عن الشخصية فتكون سرية المعلومات مضمونة وغير متاحة للكافة للاطلاع عليها أو الاحتمالات بغير وجه حق، ويدخل في إطار هذا العنصر سياسات السماح بالدخول التي تساعد عملية التحكم بالدخول في فرض النشطة والأشخاص المسموح لهم بالدخول.

ب- ترشيح المعلومات: يتمثل ترشيح المعلومات في وجود برنامج وتقنيات أو جهاز يقوم بمراقبة المعلومات الداخلية والخارجية من شبكة المعلومات، ينبنى هذا القرار على المعلومات في مقدمة الرسالة المرسلية التي تشمل عناصر أساسية خاصة بالحاسب بالمرسل كالعنوان، ونوع الخدمة بالإنترنت بريد الكتروني، ويب وغيرها، وتتجسد هذه المرشحات في كل من جدار الحماية الأمنية الذي هو عبارة عن مراقب بين الشبكة الداخلية للمنظمة وشبكة الإنترنت، أو بين شبكتين محليتين، يهدف إلى منع دخول المتطفلين والبرمجيات القائمة على الاحتيال مرشحات البريد غير المرغوب فيه بريد القمامة)، تستخدم هذه البرامج عدة استراتيجيات لتحديد أي الرسائل التي يتم التخلص منها، بقراءة خانة المرسل فإذا تبين من أحد العناوين ضمن قائمة عناوين محددة لمن يقومون بهذه الأعمال يتم إزالة الرسالة ومسحها، أما مرشحات الشبكة فتستخدم لمنع إنزال مواد غير مرغوب فيها من الشبكة أثناء التصفح، وتعتبر بديلاً عن التشريعات القانونية لحماية الأطفال خاصة من أخطار الإنترنت.

ج - اكتشاف التطفل وسوء الاستخدام: يهدف التطفل إلى اكتشاف النشاط الضار في بدايته ويتحقق ذلك عن طريق مراقبة النشطة الحالية أو مراجعة القوائم التي يتم تسجيل هذه النشطة فيها، وإن تم الاكتشاف في وقت مبكر يمكن إجهاض محاولة الاعتداء قبل حدوث الضرر، وحتى في حالة عدم التمكن من إيقاف النشاط فالعلم به في حد ذاته ينبئ مسؤولي الأمن إلى الثغرات الأمنية لإتلافها.

4-2- وسائل تحقيق الأمن المعلوماتي: حتى يكون للأمن الرقمي دور إيجابي في الحد من الجرائم التي ترتكب عبر الإنترنت، بما فيها الاحتيال الإلكتروني، يجب على كل الحكومات والمنظمات المعنية التأكيد على أهمية الأخذ بأمن المعلومات والتوجيهات المنظمة له إضافة إلى ضرورة التنسيق والتعاون على تنفيذ هذه كافة المستويات وبالتالي تطوير وسائل من المعلومات التي تتمثل في⁽²⁰⁾:

- إعداد معايير أمن عالمية تكون منسجمة ومتوافقة مع التطبيق الجغرافي المتسع والممتد على أوسع نطاق على العالم.
- ترويج الخبرة والمزاولة الأحسن لكل الأطراف المعنية بأمن نظم المعلومات على كافة مستوياتها، وتنويعها بترويج خبراتها وممارسة الأفضل في إعداد وتنفيذ سياسات أمن المعلومات.
- إبرام العقود الصحيحة بين الأطراف المختلفة المرتبطة بالمعاملات والتصرفات الإلكترونية، والمشاركين في نقل المعلومات سواء كانت الكترونية أو ورقية.

4-3- دور الذكاء الاصطناعي في الدفاع السيبراني: في حين أن الذكاء الاصطناعي قد يستخدم من قبل البعض لتغذية الجريمة والتهديدات السيبرانية ومختلف الانحرافات والسلوكيات الخطيرة، فإنه يعمل كذلك على أنه أداة حيوية في مكافحة الأنشطة الإجرامية الضارة، حيث يتم نشر تقنيات الذكاء الاصطناعي الجيدة لاكتشاف ومنع استخدام برامج الفدية والبرامج الضارة التي تعتمد على الذكاء الاصطناعي، تقوم محركات الكشف المجهزة بقدرات الذكاء الاصطناعي بتحليل النصوص والصور والبيانات التعريفية لتحديد المحتوى الضار وتعيين درجات المخاطر، كما تعمل هذه التقنيات، التي ينشرها موردو خدمات الأمن مثل «كاسبرسكي»، على مستوى المؤسسة والمستخدم على حد سواء، مما يوفر الحماية ضد التهديدات المتطورة.

إن التصدي للتهديدات والمخاطر التي تفرضها الجرائم المعلوماتية التي تعتمد على تقنيات الذكاء الاصطناعي يتطلب جهداً جماعياً داخل المجتمع، حيث يجب على الأفراد توخي الحذر والوعي فيما يتعلق بالمحتوى الرقمي الذي يشاركونه عبر الشبكة العنكبوتية، في حين تقوم المؤسسات الحكومية بسن القوانين واللوائح التي تحكم الاستخدام الأخلاقي للذكاء الاصطناعي⁽²¹⁾، فالعديد من الهيئات الحكومية على غرار الأمم المتحدة من خلال مكتب مكافحة الجريمة والإرهاب السيبراني سارع باتخاذ العديد من الإجراءات الاستعجالية التي تمثلت في شكل اتفاقيات ومبادرات، كمبادرة CT TECH "وهي عبارة عن مبادرة مشتركة بين مركز الأمم المتحدة لمكافحة الإرهاب والإنترنت، تم إطلاق هذه المبادرة في 10 فيفري 2022، حيث استمرت لمدة عامين إلى غاية جويلية 2024 هدفت أساساً لتعزيز قدرات سلطات إنفاذ القانون والعدالة الجنائية على مكافحة سوء استغلال التكنولوجيات الرقمية الحديثة، خاصة تلك المتصلة بالذكاء الاصطناعي الموجهة خصيصاً للقيام بأعمال إرهابية سيبرانية، كما جاءت هذه المبادرة بالعديد من الاقتراحات والنصوص الأخرى المرتبطة بحريات التعبير وحقوق الإنسان وكذا المساواة بين الجنسين وحماية الأفراد والمؤسسات عبر الفضاءات السيبرانية"⁽²²⁾، إضافة إلى مجموعة من البرامج التي تهدف للحد من مخاطر الاستخدام الغير عقلاني لبرامج الذكاء الاصطناعي، ناهيك عن مختلف اللوائح والقرارات كاللائحة رقم 784/2021 للبرلمان الأوروبي والمجلس (الاتحاد الأوروبي) بتاريخ 29 أفريل 2021، حيث جاءت هذه اللائحة على خلفية انتشار الإرهاب السيبراني المتصل بالذكاء الاصطناعي، دخلت حيز التنفيذ في 07 جوان 2022 حيث هدفت أبعديتها الأساسية إلى ضرورة ضمان فعالية عمل الأسواق الرقمية الموحدة المبنية في ضوء مجتمعات مفتوحة وديموقراطية⁽²³⁾، كما أن العديد من المفكرين والباحثين والمخترعين حذروا وسارعوا إلى تصميم برامج مضادة هدفها مجابهة الجرائم السيبرانية والاحتيال الإلكتروني رغبة منهم من الحد من خطر هذه التقنيات الرقمية.

خاتمة:

من خلال ما تم عرضه من بيانات كيفية عن ظاهرة الاحتيال الإلكتروني أمكن القول بأن هذه الجريمة السيبرانية تعد من أخطر الجرائم الرقمية الحديثة التي أصبحت تشكل تهديداً سيبرانياً يهدد حياة الأفراد وممتلكاتهم المادية والمعنوية، فالانتشار الرهيب للتطبيقات الرقمية وشبكات التواصل الاجتماعي، وكذا ظهور برمجيات معززة بالذكاء الاصطناعي سمحت لصيغ الإنترنت بالتطوير من جرائمهم التي كانت لا تتعدى اختراق بعض المواقع بأساليب بسيطة، غير أن التطور التقني الذكي سمح للمحتالين عبر الإنترنت من اصطياد البيانات والحسابات الخاصة والعامّة للأفراد والمؤسسات والحكومات بشتى الأساليب والأشكال سواء تمثلت في (النصب الإلكتروني، الاستيلاء على الحاسبات البنكية، انتحال الشخصيات، التعدي على الخصوصيات، قرصنة المواقع الحكومية المهمة...).

الأمر الذي رفع من مستوى الخطر ورجح ضرورة اتخاذ تدابير أمنية سريعة بغية مكافحة عمليات الاحتيال الإلكتروني المعزز بالبرمجيات الذكية، وهذا من خلال تفعيل بعض الاستراتيجيات الأمنية التي يراود منها حماية المعلومات الخاصة للأفراد والجماعات، استعانة بالبرامج الذي أنتجها الذكاء الاصطناعي التي أصبحت مفيدة في عمليات التصدي للهجمات السيبرانية، من خلال مختلف التقنيات واللوائح والقرارات الحكومية الدولية، غير أن هذه الاستراتيجيات لا تعد كافية بالنظر للتطور المستمر الذي يشهده عصر الذكاء الاصطناعي وكذا التطور في الأفكار الاحتيالية السيبرانية التي يستخدمها لصيغ الإنترنت كون هذه الجرائم تتميز بالسرعة والتطور المستمر، وهو ما يستوجب منا طرح بعض التوصيات التي يجب أن لها صدى واقعي، حيث كانت أبرزها كالتالي:

- ضرورة تفعيل الرقابة على المواقع والتطبيقات التي تشكل مصدراً للهجمات الإلكترونية.

- الاعتماد على التقنيات الذكية المعززة بالذكاء الاصطناعي ومحاولة تحديثها دورياً كي تواكب التطور في الهجمات السيبرانية.

- ضرورة تفعيل التعاون الدولي المشترك من أجل وضع استراتيجيات أمنية هادفة لحفظ الأمن السيبراني للأفراد والجماعات.

- توعية الأفراد والجماعات بمخاطر الاحتيال الإلكتروني المتعدد الأشكال والأساليب.

- إعطاء صلاحيات أكثر للأجهزة الأمنية في عمليات مكافحة لصيغ الإنترنت والاحتيال الإلكتروني.

- الاعتماد على الخبرات الأجنبية في مجال التصدي للتهديدات السيبرانية ومحاولة تكوين خبراء محليين.

- إقامة ندوات ومؤتمرات علمية تعالج موضوع الاحتيال الإلكتروني المتصل بالذكاء الاصطناعي.

الهوامش:

¹ - تقرير حول الذكاء الاصطناعي، دليل معلمي الصحافة، منظمة اليونسكو، 2024.

² - أيمن الشريف، الذكاء الاصطناعي وإنترنت الأشياء، مكتبة إقرأ، 2022، ص 07.

³ - أسماء السيد محمد عبد الصمد، كريمة أحمد، تطبيقات الذكاء الاصطناعي ومستقبل تكنولوجيا التعليم، المجموعة العربية للتدريب والنشر، القاهرة، 2020، ص 22.

- ⁴ - عبد النور عبد الحق، حماس عمر، الذكاء الاصطناعي بين ارتكاب الجرائم المالية والوقاية منها، مجلة العلوم القانونية والاجتماعية، المجلد 09، العدد 03، 2024، ص 492: <https://asjp.cerist.dz/en/article/25264>
- ⁵ - المرجع نفسه، ص 23.
- ⁶ - المرجع نفسه، ص 23.
- ⁷ - محمد محمد الهادي، الذكاء الاصطناعي معالمة وتطبيقاته وتأثيراته التنموية والمجتمعية، الدار المصرية اللبنانية، مصر، 2021، ص 149.
- ⁸ - المرجع نفسه، ص 150.
- ⁹ - المرجع نفسه، ص 151.
- ¹⁰ - مهدي حنا، الذكاء الاصطناعي ... واقع وتحديات، الان ناشرون وموزعون، الأردن، 2024، ص 94.
- ¹¹ - المرجع نفسه، ص 95.
- ¹² - Sachin Bhbosale, Vinayak Pujari Zameer Multan, Advantages And Disadvantages Of Artificial Intellegence, National Seminar on “Trends in Geography, Commerce, IT And Sustainable Development” Organizer : I. C. S. Colleg, .Khed, 2020, p229.
- ¹³ - Ibanichuka, E.A.L, Electronic Fraud and Financial Performance of Quoted Commercial Banks in Nigeria, International Journal of Advanced Academic Research Management Practice, Vol. 5, Issue 4 (April 2019), p20.
- ¹⁴ - Internet Fraud, <https://oit.ncsu.edu/home/it-security/safe-computing/internet-fraud/#:~:text=Internet%20fraud%20can%20be%20defined,transmit%20proceeds%20obtained%20through%20fraud,2024>.
- ¹⁵ - حياة هراكي، واقع جريمة الاحتيال الإلكتروني في التجارة الإلكترونية، مجلة التغير الاجتماعي، المجلد 08، العدد 02، 2023، ص 50.
- ¹⁶ - Internet fraud, <https://www.fortinet.com/resources/cyberglossary/internet-fraud> , 2024.
- ¹⁷ - ibid.
- ¹⁸ - شهرة بولحية، دنيا زاد سويح، الاحتيال الإلكتروني، مجلة الدراسات القانونية والاقتصادية، العدد 04، 2029، ص 41.
- ¹⁹ - المرجع نفسه، ص 42.
- ²⁰ - المرجع نفسه، ص 43.
- ²¹ - نسيم رمضان، كيف يمكن للذكاء الاصطناعي أن يؤجج الجرائم الإلكترونية؟: <https://aawsat.com>, 2024.
- ²² - CT TECH Initiative, Office of Counter-Terrorism, Posted at the link: <https://www.un.org/counterterrorism/ct-tech-initiative> , Viewed: 12/10/2024 – 20:43.
- ²³ - REGULATION (EU) 2021/784 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2021, Posted at the link: <https://eur-lex.europa.eu/eli/reg/2021/784/oj> , On 17/05/2021, Viewed: 11/10/2024 – 21:23.