

الحماية الجنائية للأنظمة الذكية والمعلوماتية في التشريع القطري: دراسة تحليلية

الباحث: تميم ياسر عبد الله محمد البلوشي

باحث متخصص في العلوم القانونية

ملخص:

اهتمت دراستنا بموضوع غاية في الأهمية العملية والقانونية ألا وهو " الحماية الجنائية للأنظمة الذكية والمعلوماتية في التشريع القطري- دراسة تحليلية" وذلك في إطار ثلاث مباحث تعلق المبحث الأول بتعريف الأنظمة الذكية وأهميتها القانونية وبيان ماهية البلوك تشين ومفهوم الحماية الجنائية للأنظمة الذكية. وفي المبحث الثاني درس الباحث أبرز صور الجرائم التي تستهدف الأنظمة الذكية والبلوك تشين وهي جريمة اختراق الأنظمة الذكية، وجريمة اطلاقات الفيروسات الضارة، وجريمة الاحتيال المعلوماتي وبعض الصور الأخرى. أما المبحث الثالث فقد خصصه الباحث لدراسة التحديات القانونية والتقنية في مكافحة هذه الجرائم وإثباتها وبيان الإجراءات الوقائية والحماائية من جرائم البلوك تشين. الكلمات المفتاحية: مكافحة الجرائم، الإجراءات القانونية، الإجراءات الحماائية، جرائم البلوك تشين.

Criminal Protection of Smart and Information Systems in Qatari Legislation: An Analytical Study

Tamim Yasser Abdullah Mohammed Al-Balushi

Researcher in Legal Sciences, Ministry of Interior – Qatar

Abstract

Our study focused on a subject of great practical and legal importance, namely "Criminal Protection of Smart and Information Systems in Qatari Law- Analytical study." The research was structured into three main chapters. The first chapter addressed the definition of intelligent systems, their legal significance, the concept of blockchain, and the notion of criminal protection for intelligent systems. The second chapter examined the most prominent types of crimes targeting intelligent systems and blockchain, including the crime of hacking intelligent systems, the crime of launching harmful viruses, computer fraud, and other related offenses. The third chapter was devoted to studying the legal and technical challenges in combating and proving such crimes, as well as outlining preventive and protective measures against blockchain-related offenses.

Keywords: Combating Crime, Legal Procedures, Protective Measures, Blockchain Crimes.

المقدمة :

إن نمط الحياة المتسارع في شتى مجالاتها يجعل من الواجب على الإنسان أن يساير هذا التطور التقني الهائل الذي تغلغل في كل أركانها، مما يسر أمر المعاملات التجارية التي كانت تحتاج وقتاً طويلاً، وإجراءات معقدة في الحياة العادية، فمن السهل الآن بالضغط على زر الحاسوب أن يعقد الشخص صفقة وهو في مكانه، وخصوصاً بعد ظهور العملات الافتراضية، والتوقيع الرقمي وغيره من العمليات الذكية التي تساعد في الاستيثاق من صحة المعاملات الإلكترونية والتأكد من نسبتها للطرف المتعاقد، وإمكانية حفظها

والرجوع لها، وهو ما يعرف بسلسلة الكتل، حتى تطور الأمر ووصل إلى ظهور العقود الذكية. وقد فرض هذا الواقع تحديات جديدة على القواعد التقليدية للمسؤولية الجنائية. (342)

أولاً: أهمية البحث: تكتسب الدراسة أهمية بالغة، سواء من الناحية العملية أم من الناحية القانونية. مع استخدام الأنظمة المعلوماتية والذكاء في التعاقد عن بعد لاشباع الاحتياجات الأساسية أو إبرام الصفقات التجارية، مع خلو جميع تشريعات الدول العربية - بما فيها التشريعات القطرية - وكذلك بعض التشريعات المقارنة من أي تنظيم قانوني مفصل للذكاء الاصطناعي بوجه عام، أو للمسؤولية الجنائية للأنظمة المعلوماتية والذكاء أو للمعاملات المالية التي تُجرى عبر تقنية سلسلة الكتل، أم الأضرار التي تسببها هذه الأنظمة، والمسؤولية الجنائية للأشخاص المتسببين في ذلك (343).

ثانياً: إشكالية البحث: تدور الإشكالية الرئيسة للدراسة حول الوصول إلى أحكام الحماية الجنائية للأنظمة الذكية والمعلوماتية في التشريع القطري، مع التركيز على صور هذه الجرائم والتحديات القانونية والتقنية في مكافحة هذه الجرائم وكيفية إثباتها.

ثالثاً: تساؤلات البحث: يتمثل السؤال الرئيس لهذا البحث في الآتي: ما هي أحكام الحماية الجنائية للأنظمة الذكية والمعلوماتية في التشريع القطري؟ ويتفرع عن هذا السؤال عدد من التساؤلات الفرعية أهمها ما يلي:

س: ما هي الأهمية القانونية للأنظمة المعلوماتية والعقود الذكية؟

س: ما هي أبرز صور الجرائم التي تستهدف الأنظمة المعلوماتية والبلوك تشين؟

س: ما هي التحديات القانونية والتقنية في مكافحة هذه الجرائم وإثباتها؟

رابعاً: منهج البحث: لأجل معالجة الإشكالية الرئيسة المتقدمة، والإجابة عما سبق طرحه من تساؤلات، وبسبب عدم وجود تنظيم تشريعي متكامل لموضوع البحث في دولة قطر، فقد اقتضى ذلك أن يستعين الباحث بكل من المنهج التحليلي والمنهج الوصفي.

المبحث الأول: التعريف بالأنظمة الذكية وأهميتها القانونية

تمهيد وتقسيم: مصطلحي الأنظمة الذكية والعقود الذكية إحدى المصطلحات الاقتصادية الحديثة، التي أطلقها علماء الاقتصاد والفقه القانوني على صنف مستحدث من العقود؛ والتي ارتبطت بالتطور التكنولوجي الرقمي المعاصر، فهي إحدى تطبيقات البلوك تشين جنباً إلى جنب مع العملات الافتراضية المشفرة (344)، ولزيد من التوضيح عن هذه المصطلحات لابد من الوقوف على الأهمية القانونية للأنظمة الذكية ومفهوم الحماية الجنائية لها؛ وذلك في المطالب الثالث التالية:

● **المطلب الأول: ماهية الأنظمة الذكية والبلوك تشين وخصائصها.**

● **المطلب الثاني: الحماية الجنائية للأنظمة الذكية**

● **المطلب الثالث: الأهمية القانونية للأنظمة الذكية**

المطلب الأول: ماهية الأنظمة الذكية والبلوك تشين وخصائصها

تمهيد

نتناول من خلال هذا المطلب تحديد مفهوم الأنظمة الذكية في اللغة موضحاً معنى العقود الذكية (أولاً) ثم نستعرض ماهية البلوك تشين (ثانياً) وأخيراً نوضح أهم السمات (خصائص) التي تتسم بها الأنظمة الذكية (ثالثاً)، وذلك على النحو التالي:

342 - الباحث/ محمد بدر احمد الكوح، ماهية العقود الذكية، مجلة كلية الشريعة والقانون بطنطا، جامعة الأزهر، الإصدار الأول 3/ 3 - العدد التاسع والثلاثون يناير / مارس 2024، ص 1316

343 - د/ مها رمضان محمد بطيخ، المسؤولية المدنية عن أضرار أنظمة الذكاء الاصطناعي: دراسة تحليلية مقارنة، المجلة القانونية، كلية الحقوق، جامعة القاهرة، فرع الخرطوم، مج 9، ص 5، 2021م، ص 1521.

344 - د/ وائل عبد الكريم حسن الحشاش، العقود الذكية "دراسة فقهية"، رسالة دكتوراه، جامعة النجاح الوطنية- كلية الدراسات العليا، نابلس، 2024م، ص 12.

أولاً: مفهوم الأنظمة الذكية : الذكاء لغة: الفطنة وسرعة البديهة وسرعة فهم وتوقد، يُقال: ذكاً يذكُو ذكاءً، وذكُو فهُوَ ذكي، وذكاء الإنسان: قدرته على الفهم والاستنتاج والتحليل والتمييز والاختيار والتكيف، وذكاء اصطناعي: قدرة الآلة أو الجهاز على أداء بعض الأنشطة التي تحتاج إلى ذكاء مثل الاستدلال العقلي والإصلاح الذاتي(345).

ولذلك لا بد من التنبيه هنا إلى أنّ استعمال وإطلاق مصطلح الذكاء في البحث ليس مقصوده نقيض الغباء، وإنما يطلق على كل منتج أو اختراع يقوم بوظائفه عن طريق التقنية الرقمية الحديثة بشكل آلي دون تدخل العنصر البشري، فهي منتجات تحاكي الذكاء البشري لأداء المهام، لذلك ظهرت نسمع مصطلحات الحياة الذكية والألعاب الذكية والأجهزة الذكية والبرامج الذكية ... إلخ. بالتالي يعرف الذكاء الاصطناعي: (Artificial Intelligence) بأنه سلوك وخصائص معينة تتسم بها البرامج الحاسوبية تجعلها تحاكي القدرات الذهنية البشرية وأنماط عملها، فإذا ما أضيفت هذه البرامج إلى الآلات والحواسيب تصبح ذات قدرات تحاكي القدرات الذهنية البشرية وأنماط عملها(346).

أما الأنظمة فقد عرف نظام المعالجة الآلية هو مجموعة الوحدات المترابطة التي تألفت معاً لتشكل كل لا يتجزأ وليعمل معاً كوحدة واحدة. فهو يقوم بالعديد من الوظائف الهامة والتي يتوقف عليها سير عمل النظام ومن أهم هذه الوظائف عمليات جمع المعلومات وتحليلها وتصنيفها ونقلها أو معالجتها(347).

وأما العقود الذكية (Smart Contracts) كمصطلح مركب فلها عدة أسماء تعبر عنها(348) ومن ذلك عقود البلوك تشين (Block chain Contracts) تبعاً للمنصة التي لا يمكن إجراء العقود إلا عليها، والعقود الرقمية (Digital Contracts) لأنها تعتمد التقنية الرقمية، والعقود ذاتية التنفيذ (Self-executing Contracts) لأنّ خطوات تنفيذ العقد مبرمجة مسبقاً وتنفذ تلقائياً بتحقيق شروط وواجبات الأطراف دون تدخل بشري، والعقود المشفرة (Crypto contracts) لأنها تكتب بلغة خاصة مبنية على رموز رياضية تسمى خوارزميات، وقد تعددت التعريفات بناء على تعدد الأسماء لما تحمله من معان، أو الخلاف كون هل يصدق عليه مسمى العقد أم هي مجرد برنامج؟ رغم أنها تدل كلها على مسمى واحد، فقد عرفها البعض بأنها: "اتفاقية محوسبة تروم تبسيط وتسهيل تنفيذ المعاملات التجارية بين الأطراف بشكل مباشر ودون الحاجة لوسيط ثالث(349)، وعرفها البعض الآخر بقوله: "عقود إلكترونية آلية التنفيذ تعمل على أتمتة عمليات التعاقد(350)، وعرفها البعض الثالث بأنه: "العقود التي تدون باستخدام الرموز المشفرة حيث يمكن تفعيل الالتزامات بموجب الاتفاق وتنفيذها بصورة تلقائية(351)، وعرفت بأنها: "عقود ذاتية التنفيذ تبنى وتبرمج في إطار شبكة توزيع لا مركزية تنظم شروطها وأحكامها العلاقة بين البائع والمشتري دون الحاجة لوجود سلطة مركزية(352)، وهذه التعريفات تؤكد كونه عقدًا؛ لأنه ناتج عن اتفاق إرادتين أو أكثر وتترتب عليه آثار، وهو ما أكده المجمع الفقهي حيث عرفها بأنها: "عقد بين طرفين ينفذ تلقائياً يقوم على فكرة الند للند Peer to peer (دون وسيط) من خلال شبكة توزيع لا مركزية (سلسلة الكتل Block chain) ويتم بالعملة المرمزة (المشفرة) مثل البيتكوين وغيرها(353)، بينما التعريفات الأخرى تعتبره مجرد برنامج

345 - الامام العلامة/ محمد بن مكرم بن علي، أبو الفضل، جمال الدين ابن منظر الأنصاري الرويفي الإفريقي(711هـ)، ط3، دار صادر: بيروت، 1414 هـ، ج 14، ص 287، أيضا انظر، مصطفى، إبراهيم وآخرون، المعجم الوسيط، 1/314، أيضا انظر عمر، أحمد (1424هـ) وآخرون، معجم اللغة العربية المعاصرة، 1429هـ، عالم الكتب، 1/818.

346 - لمزيد عن مفهوم الذكاء الاصطناعي انظر: د/ مراد بن عودة، إشكالية تطبيق أحكام المسؤولية الجنائية على جرائم الذكاء الاصطناعي، مجلة الحقوق والعلوم الإنسانية- جامعة زيان عاشور بالجلفة، مج 15، ع 1، 2022م، ص 189.

347 - د/ زياد القاضي، مبادئ تحليل نظم الحاسوب وتعميمها، الطبعة الأولى، دار الصفاء للنشر، عمان 1997م، ص 13؛ د/ طارق عفيفي صادق، الخطر محل التأمين من المسؤولية المدنية في مجال المعلوماتية، رسالة دكتوراه، كلية الحقوق، جامعة بني سويف، مصر، 2011م، ص 32.

348 - د/ نصر أبو الفتوح فريد، العقود الذكية ماهية والأحكام - دراسة تحليلية، دار النهضة العربية، 2022م، ص 13.

349 - د/ قطب مصطفى سانو، العقود الذكية في ضوء الأصول والمقاصد والمآلات رؤية تحليلية، مؤتمر مجمع الفقه الإسلامي الدولي، الإمارات العربية المتحدة، دبي، الدورة الرابعة والعشرون، 2019م، ص 12.

350 - د/ منير الشاطر، تقنية البلوكتشين وتحديات المالية الإسلامية، مجلة دراسات اقتصادية معاصرة، مج 25، ع 1، المعهد الإسلامي للبحوث والتدريب، 2019م، ص 24.

351 - العياشي الصادق فداد، العقود الذكية "Smart Contracts"، مؤتمر مجمع الفقه الإسلامي الدولي، الدورة الرابعة والعشرون، 2019م، دبي، ص 14.

352 - انظر: مقال بعنوان العقود الذكية، متاح على الرابط التالي: <https://sa.investing.com/analysis/article> 200227791 - تم الإطلاع عليه في: 5-8-2025.

353 - انظر: قرار رقم 230 (1/24)، مجمع الفقه الإسلامي الدولي المنبثق عن منظمة التعاون الإسلامي، قرارات وتوصيات مجمع الفقه الإسلامي، الإصدار الرابع، 1442هـ، ص 828.

حاسوبي يرافق عقداً مبرماً سابقاً ولا يرتقي لمستوى العقد (354)، فعرف بأنه: "رمز إلكتروني يعمل على طبقة سلسلة الكتل ويحتوي على مجموعة من القواعد التي يتفق بموجبها الطرفان على التفاعل مع بعضهما البعض، وعندما يتم استيفاء الشروط المحددة مسبقاً، يتم تنفيذ الاتفاقية تلقائياً" (355)، كما عرف بأنه: "عبارة عن برمجيات حاسوبية مشفرة لا مركزية مضمنة لشروط اتفاقية تنفذ تلقائياً" (356)، وعرفتها معداوي: "تعليمات برمجية قائمة بذاتها، تنفذ تلقائياً أحكام وشروط العقد، دون الحاجة إلى تدخل بشري، وتتضمن هذه العقود جميع المعلومات حول شروط العقد وواجبات وحقوق الأطراف" (357)، وبالتالي يرى الباحث أن العقد الذكي هو: "اتفاق إرادات متعاقدين أو أكثر، تعتمد على برنامج رقمي إلكتروني مشفر، يتضمن تنفيذ عملية تعاقدية بين طرفي العقد بشكل آلي ذاتي، ضمن شروط وضوابط وحقوق مبرمجة على منصة سلسلة الكتل لا تحتاج إلى طرف ثالث، وتتم بالعملات الرقمية أو التقليدية".

ثانياً: تعريف البلوك تشين: تقنية البلوك تشين وهي نوع خاص من قاعدة البيانات اللامركزية، والتي تمثل السجل العام للمعاملات التي قد تم تنفيذها بين الأعضاء المشاركة، وتتكون من سلسلة من الكتل المرتبطة ببعضها بطريقة مشفرة، ويتم التحقق من معاملاتها بتوافق آراء أغلبية المشاركين فيها (358).

ثالثاً: خصائص العقود الذكية: تتمتع العقود الذكية وما يرتبط بها من أنظمة ذكية بالعديد من الخصائص المميزة لها كونها ترتبط بأحد تطبيقات سلسلة الكتل التي تعمل على تخزين أكواد العقود الذكية على السلسلة ومن ثم تفعيل هذه العقود، فهذه التقنية (سلسلة الكتل) تمثل قاعدة بيانات خاصة بالمعاملات. وهي نظام إلكتروني وأكبر سجل رقمي موزع ومفتوح يسمح بنقل أصول الملكية من شخص إلى آخر في الوقت ذاته، دون الحاجة إلى وسيط، مع توفير درجة كبيرة من الأمان لعملية التحويل في مواجهة محاولات الغش أو التلاعب، ويشارك في هذه الشبكة أو السجل جميع الأفراد حول العالم (359). ومن ثم يمكن القول بأن العقود الذكية مختلفة عن باقي العقود سواء التقليدية أو الإلكترونية. فالعقود الذكية ليست هي الصورة الوحيدة من العقود التي تعتمد على الأتمتة والتشغيل الذاتي دون تدخل العنصر البشري، بل هناك صور أخرى للعقود الإلكترونية التي تتم بشكل مؤتمت من خلال شبكة الإنترنت، ولكن يبرز الاختلاف من خلال النظام الذي يتم من خلاله إبرام العقود الذكية، فهي تنشأ وتنفذ عبر شبكة لامركزية موزعة تعرف بسلسلة الكتل والتي لا يتحكم بها جهة مركزية، بخلاف العقود الإلكترونية الأخرى التي تبرم أو تنفذ من خلال نظام مركزي يتحكم فيه جهة واحدة مركزية أو أكثر من جهة (360).

فالعقود الذكية التي تنشأ من خلال هذا النظام اللامركزي تتأثر به وتكتسب من خصائصه، فهي تستمد منه طبيعتها وتتأثر به، مما يكسبها خصائص فريدة تميزها عن غيرها، ومن هذه الخصائص البيئة الإلكترونية التي يتواجد فيها العقد الذكي، فالوسيط الذي يقوم عليه هذا العقد (الذكي) عبارة عن شبكة لامركزية رقمية مفتوحة تبنى على لغات برمجية مشفرة (نظام معلوماتي ذكي)، فلا يمكن أن يوجد العقد الذكي إلا في شكل إلكتروني، واستخدام التوقيعات الرقمية الإلكترونية، والتي تقوم على خاصية التشفير عبر المفتاح العام والمفتاح الخاص بالمتعاقد، وكلاهما (المفتاح العام والمفتاح الخاص) يمنح التعامل مزيداً من الأمان والخصوصية (361).

354 - د/ نجية معداوي، العقود الذكية والبلوك تشين، مجلة المفكر للدراسات القانونية والسياسية، 2021م، مج 4، ع 2، ص 67.

355 - د/ عبد الله السفري، استخدام سلسلة الكتل في حفظ حقوق الملكية الفكرية، مجلة العلوم الاقتصادية والإدارية والقانونية، مج 4، ع 5، 2020م، ص 16.

356 - د/ عمر الجميلي، العقود الذكية "Smart Contracts" واقعها وعلاقتها بالعملات الافتراضية، مؤتمر مجمع الفقه الإسلامي الدولي، الدورة الرابعة والعشرون، أرات العربية المتحدة، دبي، 2019م، ص 13.

357 - د/ نجية معداوي، العقود الذكية والبلوك تشين، مرجع سابق، ص 68.

358 - د/ سامي البعول، العقود الذكية باستخدام تقنية البلوك تشين - دراسة تأصيلية فقهية تطبيقية، رسالة دكتوراه، الجامعة الأردنية، عمان، 2022م، ص 86.

359 - د/ إيهاب خليفة، البلوك تشين الثورة التكنولوجية القادمة في عالم المال والإدارة، المستقبل للأبحاث والدراسات المتقدمة، العدد الثالث، مارس ٢٠١٨م، ص ١.

360 - د/ هيثم السيد أحمد عيسى، نشأة العقود الذكية في عصر البلوك تشين، دار النهضة العربية، القاهرة، ٢٠٢١م، ص ٤٧.

361 - الباحث/ محمد بدر أحمد الكوح، ماهية العقود الذكية، مرجع سابق، ص 1337 وما بعدها.

ويمثل التحقق الذاتي أهم خصائص العقود الذكية، حيث يتم التحقق ذاتيا من حدوث الشروط التعاقدية المتفق عليها مسبقا في العقد، عبر سلسلة الكتل بشكل لامركزي موزع، دون جهة أو سلطة مركزية تخضع لها، ويتم هذا التحقق وفقا لآليات التوافق بين أعضاء الشبكة والمستخدمين لها، وذلك من خلال بروتوكولات تمكن في التحقق من صحة المعاملة أو البيانات في الشبكة⁽³⁶²⁾. ويترتب على ما سبق أنه يمكن القول أن العقود الذكية تعد عقود ذاتية التنفيذ، فلا تتطلب قيام البشر بتنفيذ التزاماتها، وذلك ما يميز العقود الذكية عن غيرها من العقود التقليدية، فهي عقود تنفي الوساطة بين أطراف العقد، حيث تتيح التقنية للمتعاقدین ضمان تنفيذ العقد بصورة ذاتية دون الحاجة إلى سلطة مركزية⁽³⁶³⁾. كما أن هذه العقود توثق بطريقة آلية، دون تدخل أي شخص أو جهة مركزية، ويتم ذلك من خلال تقنية سلسلة الكتل- السابق الإشارة إليها- حيث ينشر العقد على المستخدمين عبر شبكات المعلومات، الذين يقومون بدورهم بالمصادق عليه، وإضافة المعاملة بشكل كتلة في السلسلة، بطريقة مرتبطة بالكتل السابقة، وتحمل طابع زمني يحدد وقت الإضافة في السلسلة، مما يجعلها غير قابلة للتعديل، أو التبديل، وذلك بخلاف العقود التقليدية، التي تتطلب في بعض الحالات وجود جهات متخصصة لتوثيقها وتسجيل العقد كما في البيوع العقارية⁽³⁶⁴⁾.

المطلب الثاني : الحماية الجنائية للأنظمة الذكية : مع تزايد القيمة الاقتصادية والمالية للمعلومات والأنظمة الإلكترونية، فقد كان لزاماً على الدول والمجتمعات العمل على توفير الحماية الجنائية لهذه المعلومات وتلك الأنظمة بوجه عام وعلى وجه الخصوص الأنظمة الذكية المالية وتلك المسؤولة عن إبرام العقود عن بعد، وهو ما أدى إلى ابتكار العديد من الوسائل التقنية المتنامية لتأمين هذه الحماية ككلمات السر والتشفير الإلكتروني... الخ لضمان حماية تبادل المعلومات بشكل صحيح، إذ تؤدي إلى توفير ثقة واسعة بنظم التقنية لدى المستخدمين لهذه الأنظمة الذين تسود عندهم قناعة بأنها بيئة ليست آمنة بقدر الوسائل التقليدية للأعمال القائمة على الورق والدليل الكتابي أو المادي. كما تطلب ذلك ضرورة الاعتراف القانوني بالمصالح المشروعة المتولدة عن هذه الأنظمة وتوفير الحماية الجنائية لها من مخاطر وعيوب التكنولوجيا وتطبيقاتها، نتيجة ظهور طائفة جديدة من الجرائم وهي ظاهرة الجريمة المعلوماتية أو الجرائم الإلكترونية، ويمكن للباحث القول بأن الحماية الجنائية لتكنولوجيا الأنظمة الذكية هي " الطرق القانونية الواردة في القانون الجنائي لحماية حق من الحقوق أو مصلحة من المصالح الجديرة بالحماية والتي ترتبط بالأنظمة الذكية"⁽³⁶⁵⁾.

ولذلك أصدر المشرع القطري قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014، والذي تضمن الفصل الأول من الباب الثاني من هذا القانون "جرائم التعدي على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية" (المواد 2-4)؛ إذ جرم المشرع القطري في هذا الفصل الدخول إلى موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها⁽³⁶⁶⁾، وكذلك الدخول العمدي- بأي وسيلة كانت- إلى أي موقع إلكتروني أو نظام معلوماتي آخر أو شبكة

Alexander Savelyev. 2016, Contract law 2.0: smart contracts as the beginning of the end of classic contract law, National research university, higher school of economics, P.12.

362 - هيثم السيد أحمد عيسى، نشأة العقود الذكية في عصر البلوك تشين، مرجع سابق، ص ٤٥.

363 - د/ أحمد سعد البرعي، إنشاء عقود المعاملات وتنفيذها بين الطرق التقليدية وتقنية البلوك تشين والعقود الذكية، دراسة فقهية مقارنة، المجلة العلمية لكلية الدراسات الإسلامية والعربية للبنين، جامعة الأزهر، القاهرة، العدد التاسع والثلاثين، ديسمبر ٢٠٢٠ م، ص ٢؛ د/ نصر أبو الفتوح فريد، العقود الذكية بين الواقع والمأمول، دراسة تحليلية، مجلة الأمن والقانون، أكاديمية شرطة دبي، المجلد ٢٨، العدد الثاني، ٢٠٢٠ م، ص ٥١٠.

- Alexander Savelyev. 2016, ibid, p.14

364 - د/ حسام الدين محمود محمد، العقود الذكية المبرمة عبر تقنية البلوك تشين، المجلة القانونية، مجلة متخصصة في الدراسات والبحوث القانونية، 2022 م، ص ١٤.

365 - الباحثة/ انسام سمير طاهر الحجامي، الحماية الجنائية لتكنولوجيا المعلومات، رسالة ماجستير، كلية القانون- جامعة كربلاء، 1434هـ/ 2013 م، ص 77.

366 - انظر: المادة (2) من قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014 م، والتي تنص على أن: "يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، كل من تمكن عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، بغير وجه حق، من الدخول إلى موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها. وتضاعف العقوبة المنصوص عليها في الفقرة السابقة، إذا ترتب على الدخول الحصول على بيانات أو معلومات

معلوماتية، أو وسيلة تقنية معلومات أو جزء منها، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك. وتُضعف العقوبة إذا ترتب على الدخول إلغاء أو حذف أو إضافة أو إفشاء أو إتلاف أو تغيير أو نقل أو التقاط أو نسخ أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي، أو إلحاق ضرر بالمستخدمين أو المستفيدين، أو تدمير أو إيقاف أو تعطيل الموقع الإلكتروني أو النظام المعلوماتي أو الشبكة المعلوماتية، أو تغيير الموقع الإلكتروني أو إلغاءه أو تعديل محتوياته أو تصميماته أو طريقة استخدامه أو انتحال شخصية مالكة أو القوائم على إدارته⁽³⁶⁷⁾؛ هذا إلى جانب تجريم المشرع القطري للتقاط أو اعتراض أو التنصت العمدي - دون وجه حق - لأية بيانات مرسلة عبر الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، أو على بيانات المرور التي يمكن أن تتعلق بالنظم الذكية⁽³⁶⁸⁾.

المطلب الثالث : الأهمية القانونية للأنظمة الذكية

تتطلب العقود التقليدية الكثير من الوقت والجهد والمال، فتكون أكثر كلفة مادية على أطراف التعاقد لحاجتها عادة للتوثيق وطرف ثالث عند إبرام العقد وسريانه، كما تحتاج إلى الوقت لإعداد المستندات وتوثيقها، وعند حدوث نزاع بسبب الإخلال بالالتزامات تتطلب تدخل طرف ثالث لحل النزاع؛ لذا، كان الهدف الأساسي من إنشاء العقود الذكية هو التخلص من تلك المشكلات أو الحد منها، وذلك من خلال التنفيذ الذاتي التلقائي لشروط الاتفاقية المبرمة بين الطرفين، وذلك بمجرد استيفاء الشروط المحددة، والمتفق عليها مسبقاً بينهم، حيث يهدف العقد الذكي إلى فرض مبدأ القوة الملزمة للعقد من حيث تنفيذه، وإلغاء فكرة عدم التنفيذ. كما كان الغرض من وراء أتمتة التعاقد الذكي هو إلغاء أو تقليص دور الغير (الوسيط) سواء كان موثقاً أو وكيلاً أو محامياً في المسار التعاقدية، مما يؤدي إلى قلة التكاليف والسرعة في الإنجاز.

وتتمثل أهم الأهداف القانونية المبتغاة من العقود الذكية في الآتي:

- 1- يهدف الأطراف عند الشروع بالتعاقد عبر الأنظمة الذكية إلى إيجاد مجموعة من الإرشادات والتوجيهات القابلة للتنفيذ والمعالجة حاسوبياً بشكل آمن.
- 2- التنفيذ التلقائي للعقد - على النحو الذي بينه الباحث عند دراسته لخصائص هذه العقود - والذي يكون بمجرد توقيع العقد من قبل أطرافه وتسجيله في سلسلة الكتل (Block chain)، حيث لا يمكن إيقافه أو التراجع عنه إلا بموافقة الأطراف على الإلغاء⁽³⁶⁹⁾.
- 3- العمل على تسهيل التنفيذ واستبدال الطرف الوسيط ببرنامج يقوم بالعمل بدلاً عنه.
- 4- إمكانية التعاقد بين طرفين مجهولي الهوية، وتنفيذ المعاملة من خلال الكمبيوتر بسرية تامة وأمان، مما يخفف من أخطار عدم الوفاء.

إلكترونية، أو الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني أو أية بيانات حكومية سرية بطبيعتها أو بمقتضى تعليمات صادرة بذلك، أو إلغاء تلك البيانات والمعلومات الإلكترونية أو إتلافها أو تدميرها أو نشرها، أو إلحاق الضرر بالمستخدمين أو المستخدمين، أو الحصول على أموال أو خدمات أو مزايا غير مستحقة".
367 - انظر: المادة (3) من القانون سالف الذكر والتي تنص على أن: "يعاقب بالحبس مدة لا تتجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من دخل عمداً، دون وجه حق، بأي وسيلة، موقعاً إلكترونياً، أو نظاماً معلوماتياً، أو شبكة معلوماتية، أو وسيلة تقنية معلومات أو جزء منها، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك. وتُضعف العقوبة المنصوص عليها في الفقرة السابقة، إذا ترتب على الدخول إلغاء أو حذف أو إضافة أو إفشاء أو إتلاف أو تغيير أو نقل أو التقاط أو نسخ أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي، أو إلحاق ضرر بالمستخدمين أو المستفيدين، أو تدمير أو إيقاف أو تعطيل الموقع الإلكتروني أو النظام المعلوماتي أو الشبكة المعلوماتية، أو تغيير الموقع الإلكتروني أو إلغاءه أو تعديل محتوياته أو تصميماته أو طريقة استخدامه أو انتحال شخصية مالكة أو القوائم على إدارته".

368 - انظر: المادة (3) من قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014م والتي تنص على أن: "يعاقب بالحبس مدة لا تتجاوز سنتين، وبالغرامة التي لا تزيد على (100,000) مائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من التقط أو اعتراض أو تنصت عمداً، دون وجه حق، على أية بيانات مرسلة عبر الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، أو على بيانات المرور". لمزيد انظر: محكمة التمييز القطرية - الطعن رقم: 203 لسنة 2017 تمييز جنائي - جلسة 4 من ديسمبر سنة 2017: محكمة التمييز القطرية، الطعن رقم 63 لسنة 2017 تمييز جنائي، جلسة 2017/10/16م، هذه الأحكام متاحة على الرابط التالي:

<https://encyclopc.sjc.gov.qa/Portal1/ahkam/detailspage.aspx?txtSearch=1&Ino=2606&gcc=1>

369 - هناء محمد الحنيطي، ماهية العقود الذكية، مؤتمر مجمع الفقه الإسلامي الدولي، الدورة الرابعة والعشرون، منظمة التعاون الإسلامي، دبي، ١٩-٢٠ ص ٢٧ وما بعدها.

٥- فرض مبدأ القوة الملزمة للعقد، وإلغاء فكرة عدم التنفيذ.

٦- القدرة على إمكانية التدقيق وتقييم المخاطر من قبل المستخدمين في الشبكة، مع حفظ وتخزين البيانات والمعلومات في سلسلة الكتل بطابع زمني متسلسل، يمكن الرجوع لها في أي وقت (370).

المبحث الثاني : صور الجرائم التي تستهدف الأنظمة الذكية والبلوك تشين

تمهيد وتقسيم

غالبية الجرائم الإلكترونية التي يتم ارتكابها للاعتداء على النظم الذكية أو تستخدم فيها هذه الأنظمة يكون الهدف منها الحصول على المعلومات الإلكترونية، التي تكون إما محفوظة على النظم الذكية أو على أجهزة الحاسب الآلي المتصلة بها، أو منقولة عبر شبكة الإنترنت، وغالباً ما يتم الاعتداء على هذه المعلومات بالاستيلاء عليها، أو تغييرها، أو حذفها، أو إلغائها نهائياً، ويكون الدافع من ذلك التنافس، أو الابتزاز، أو تحقيق مكاسب، أو الحصول على مزايا أخرى (371)؛ وحيث تتمثل أبرز صور الجرائم التي تستهدف الأنظمة الذكية والبلوك تشين في جريمة اختراق الأنظمة الذكية بغرض الدخول إليها أو البقاء فيها بدون وجه حق، وجريمة إطلاقات الفيروسات الضارة وجريمة الاحتيال المعلوماتي فسوف يفصل الباحث هذه الجرائم في المطالب الثلاث التالي:

- **المطلب الأول: اختراق الأنظمة الذكية.**
- **المطلب الثاني: إطلاق الفيروسات الضارة.**
- **المطلب الثالث: الاحتيال المعلوماتي والصور الأخرى.**

المطلب الأول: اختراق الأنظمة الذكية

تشمل جرائم اختراق الأنظمة الذكية- من وجهة نظر الباحث- جريمة الدخول غير المشروع – أي الدخول العمدي بدون وجه حق- للأنظمة الذكية، وجريمة البقاء داخل هذه الأنظمة بدون وجه حق أي تجاوز حدود الدخول. والملاحظ أن المادتين (2)، (3) من القانون القطري رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية لم تفرق بين هذه الجرائم. إلا أن هاتين المادتين فرقتهما بين الاعتداء على موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها وبين الاعتداء على الأنظمة الذكية المملوكة للأشخاص العاديين (أشخاص القانون الخاص) (372).

وقد عاقب المشرع القطري على جرائم الاعتداء على أنظمة الدولة الذكية بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، وتضاعف العقوبة على هذه الجرائم إذا ترتب على الدخول الحصول على بيانات أو معلومات إلكترونية، أو الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني أو أية بيانات حكومية سرية بطبيعتها أو بمقتضى تعليمات صادرة بذلك، أو إلغاء تلك البيانات والمعلومات الإلكترونية أو إتلافها أو تدميرها أو نشرها، أو إلحاق الضرر بالمستفيدين أو المستخدمين، أو الحصول على أموال أو خدمات أو مزايا غير مستحقة (373).

أما جرائم الاعتداء على الأنظمة الذكية الخاصة فقد عاقب عليها المشرع القطري بذات العقوبة (الحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين) وتضاعف هذه العقوبة إذا ترتب

370 - الباحث/ محمد بدر احمد الكوح، ماهية العقود الذكية، مرجع سابق، ص 1316.

371 - د/ حسين الغافري د/ محمد الألفي، جرائم الإنترنت بين الشريعة الإسلامية والقانون، دار النهضة العربية، القاهرة، ٢٠٠٨م، ص ٤٦.

372 - المادتين (2)، (3) من قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014م.

وهذا ما اخذ به كل من المشرع الأردني، والمشرع المصري، اللذين أحاطا البيانات والمعلومات الخاصة بالدولة بقدر من الحماية؛ إذ نصا على تجريم الدخول غير المشروع وتجاوز حدود الدخول المصرح به للأنظمة المعلوماتية الخاصة بالدولة بنص خاص غير النص المتعلق بفرضية الاعتداء على المواقع أو الأنظمة الخاصة بالأفراد – المادة الثالثة من قانون الجرائم الإلكترونية الأردني، ونص المادة الرابعة عشرة من قانون مكافحة جرائم تقنية المعلومات المصري- وذلك بالنظر للمصلحة المعتدى عليها، التي تعد ذات أهمية تستوجب تخصيص نص لها، وعدم شمولها مع النص المتعلق بحماية الأنظمة المعلوماتية الخاصة بالأفراد. د/ هيفاء عبد العالي فرج، الحماية الجنائية للمواقع الإلكترونية والأنظمة المعلوماتية للدولة "دراسة مقارنة"، كلية القانون – جامعة المرقب، مجلة العلوم القانونية، المجلد 11، العدد2، ديسمبر 2023 م، ص 67.

373 - المادة (2) من قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014م.

عليها إلغاء أو حذف أو إضافة أو إفشاء أو إتلاف أو تغيير أو نقل أو التقاط أو نسخ أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية مخزنة داخل النظام الذكي، أو إلحاق ضرر بالمستخدمين أو المستفيدين، أو تدمير أو إيقاف أو تعطيل الموقع الإلكتروني أو النظام المعلوماتي أو الشبكة المعلوماتية، أو تغيير الموقع الإلكتروني أو إلغائه أو تعديل محتوياته أو تصميماته أو طريقة استخدامه أو انتحال شخصية مالكة أو القائم على إدارته(374).

ويرى الباحث أن الاختلاف القائم بين جرمي الدخول إلى الأنظمة الذكية والبقاء غير المصرح به في هذه الأنظمة يتمثل في أن جريمة الدخول إلى الأنظمة الذكية جريمة ايجابية تقتضي إتيان فعل الدخول، في حين تقوم جريمة البقاء في الأنظمة الذكية بسلوك إجرامي سلبي، ورغم دخول الجاني صدفة أو خطأ، ورغم علمه بأن ذلك غير مشروع فهو يرفض الخروج من النظام وبمعنى آخر يمتنع عن الخروج، لذلك فالنشاط الإجرامي - حسب رأي هذا الجانب- يمثل في هذه الصورة سلوكا سلبيا من الجاني. وإن كان جانب من الفقه يرى أن الإمتناع عن الخروج من النظام الذكي الذي تم الدخول إليه ليس منطوق التجريم، بل أن السلوك المجرم هو البقاء داخل هذا النظام بعد الدخول إليه مع العلم بأن هذا البقاء غير مصرح به وهو ما يشكل سلوكا ايجابيا(375).

كما يرى الباحث أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي ينذر فيها المتدخل بأن تواجهه غير مشروع فإذا لم ينسحب يرتكب منذ تلك اللحظة جريمة البقاء داخل النظام، وهذا مع مراعاة أن الفقه يجمع على أن البقاء غير المصرح به داخل نظام المعلوماتية جريمة مستمرة، نظرا لاستمرار الإعتداء على المصلحة التي يحميها القانون كلما استمر البقاء غير المصرح به، كما أن الدخول غير المصرح به مجرم بمجرد الدخول إلى النظام أو بالوصول إلى المعلومات التي يحتوي عليها، لأنه في كلتا الحالتين تتم الجريمة بمجرد الدخول إلى النظام أو بالوصول إلى المعلومات(376).

المطلب الثاني

إطلاق الفيروسات الضارة

تشابه فيروسات الحاسب الضارة مع الفيروسات الحية في مجموعة من الخصائص منها القدرة على التخفي والخداع عن طريق الارتباط ببرامج أخرى للتمويه كالدخول إلى ملفات مخفية، والقدرة على العدوى فبمجرد تحميل الفيروس إلى النظام ينتقل وينسخ نفسه من حاسب أو جهاز لآخر بسرعة كبيرة. كما يتمتع الفيروس بقدرة فائقة على الدخول للنظام والتسلل إليه واختراق كل سبل الحماية والهدف الأساسي للفيروسات هو تخريب وتعطيل البرامج(377).

وتنص المادة (376) من قانون العقوبات القطري رقم (11) لسنة 2004م، على أن: " يقصد بفيروس الحاسب الآلي، ذلك البرنامج الذي يتم تسجيله، أو زرعه على الأقراص، أو الإسطوانات الخاصة بالحاسب، ويظل خاملاً لفترة محددة، ثم ينشط فجأة في توقيت معين ليبدأ تأثيره على جهاز الحاسب الآلي، أو برامجه، أو البيانات المخزنة فيه."

ويتفق هذا التعريف مع التعريفات المقترحة للفيروسات من قبل الفقه ومنها أنها: "برمج صغير تم تصميمه بهدف لا يخدم نظام الحاسب، ويرمج عادة بحيث لا يبدأ نشاطه إلا بعد فترة كافية من الوقت حتى يضمن حرية الانتشار دون أن يلفت الانتباه ليتمكن من إصابة أكبر عدد ممكن من الملفات في النظام"(378).

374 - المادة (3) من قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014م.

375 - د/ عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2006م، ص 360؛ الباحثة/ نجاة عباوي، الإشكالات القانونية في تجريم الاعتداء على أنظمة المعلومات، دفاثر السياسة والقانون، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية، الجزائر، ع 16، 2016م، ص 283.

376 - الباحثة/ نجاة عباوي، مرجع سابق، ص 284.

377 - د/ محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، 2003م، ص 294.

378 - وتجدر الإشارة إلى أن أبرز أنواع الفيروسات الضارة- والتي يصعب حصرها في قائمة واحدة- تتمثل في الآتي: برامج الدودة، وبرنامج حصان طروادة، والقنبلة المعلوماتية، والقنبلة المنطقية- هذا النوع ينشط بمجرد حدوث واقعة معينة مثل بدأ تشغيل الجهاز أو عند إنجاز أمر معين في الحاسب الآلي أو عند بدأ تشغيل برنامج معين- وهناك فيروس القنبلة الزمنية والتي ينشط في تاريخ معين محدد بالذات. لمزيد انظر: الباحث/ محمد أمين الشوابكة، جرائم الحاسوب والإنترنت "الجريمة المعلوماتية"، دار الثقافة للنشر والتوزيع، عمان، الاردن،

وعلى كل فإنه تتعدد البواعث الاجرامية لاستخدام فيروسات الحاسب الضارة ومنها الاعتداء على حقوق الملكية الفكرية والقرصنة على البرامج المحمية(379)، ومنها استخدام فيروسات الحاسب لتدمير المعلومات وهو ما حدث عند زراعة فيروس القنبلة الموقوتة Donald Gen information distraction time bomb virus بالولايات المتحدة الأمريكية من قبل دونالد جين بيرلسون (380)Burleson.

يضاف لما سبق استخدام فيروسات الحاسب لسرقة المعلومات والبيانات التي تتضمنها الأنظمة الذكية، وفي هذه الصورة يقوم المجرم المعلوماتي باستخدام فيروس الحاسب في الإعتداء على معلومات الغير وذلك عن طريق نقل المعلومات Information أي البيانات المعالجة إلكترونياً والخاصة بهذه الغير إلى النظام المعلوماتي الخاص بالمجرم المعلوماتي(381). وقد ثار خلاف كبير بين رجال القانون في كل من دول النظام اللاتيني والنظام الأنجلوأمريكي حول مدى توفر ركن الخطأ في هذا الفعل خاصة وأن المعلومات لا تخضع للحماية بموجب قواعد حماية الملكية الفكرية لأن القانون حتى الآن لم يحم من مصنفات الحاسب إلا البرامج وقواعد البيانات أما المعلومات فلا تخضع للحماية ولأن الإعتداء على المعلومات في حد ذاتها دون الوسيط المدون عليه هذه المعلومات لا يقع تحت طائلة قانون العقوبات فالسارق في عين القانون هو ذلك الذي يأخذ ويحمل بعيداً takes and carries away أي شئ قابل للسرقة دون رضا مالكه وبنية حرمان هذا المالك منه وبناء عليه فالشخص الذي يتعدى على المعلومات لإقتباسها أو نقلها دون إذن صاحبها لا يعد سارقاً لأنه لا يحرم مالك هذه المعلومة من الإنتفاع بها(382) وقد اعتبر المشرع القطري في الفصل الرابع- وهو بعنوان جرائم بطاقة التعامل الإلكتروني- من القانون سالف الذكر سرقة البيانات الخاصة بطاقات التعامل الإلكتروني إذ نصت المادة (12) من قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014م، على أن: "يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (200,000) مائتي ألف ريال، أو بإحدى هاتين العقوبتين، كل من ارتكب فعلاً من الأفعال التالية:

1- استخدام أو حصل أو سهل الحصول دون وجه حق على أرقام أو بيانات بطاقة تعامل إلكتروني عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.....".

2007م، ص 240: د/ طارق عفيفي صادق، جرائم الهاتف المحمول والتعويض عنها، دراسة مقارنة بين القانون المصري والإماراتي والسعودي"، الكتاب الأول: المسؤولية الجنائية الخلوية، المركز القومي للإصدارات القانونية، 2014م، ص 123 – 131..

379 - ومن الأمثلة العملية على ذلك ما قام به موظف بشركة نسي University Computer Company بمدينة بالوالتو Palo-Alto بولاية كاليفورنيا الأمريكية من زراعة فيروس في النظام المعلوماتي لشركة Information System Design وهي شركة منافسة تقع بمدينة أوكلاند بنفس الولاية واستطاع هذا الموظف أن ينقل نسخة كاملة من أحد برامج الحاسب الخاص بالشركة المنافسة إلى حاسبه.

Conish, E.R; Intellectual Property: Patents Copyright. Trade Marks, Sweet and Maxwell, London 1990, p. 115; David Ferbrache, Pathology of Computer Viruses, Springer - Verlag, London Ltd., 1992, p. 115.

380 - وتتلخص وقائع القضية التي حدثت في ولاية تكساس الأمريكية في شركة USPA & IBMA وهي إحدى أكبر شركات السمسرة والتأمين على الحياة في أن المذكور كان يعمل كبير المبرمجين وضابط أمن الحاسب بالشركة المذكورة ثم فصل منها في ٢٨ سبتمبر ١٩٨٥ لإستغلاله إمكانات النظام المعلوماتي لأغراضه الشخصية وفي يوم ٢١ سبتمبر ١٩٨٥ قام عن بعد بمحو عدد ١٦٨٠٠٠ سجل عمولات بيع وذلك باستخدام جهاز المودم ١٦٨٠٠ وعن طريق باب خلفي في النظام يعلمه بحكم وظيفته السابقة. وفي يوم ٢٣ سبتمبر ١٩٨٥ قام المذكور عن بعد بتنشيط فيروس القنبلة الموقوتة الذي قام بزرعه سلفاً قبل فصله بثلاثة أسابيع وكان هذا الفيروس مكوناً من أمر واحد هو Power down system بمعنى إغلاق النظام وقد قام هذا الفيروس بتشغيل نفسه أوتوماتيكياً بمجرد تنشيطه فقام بمسح قطاعين من قطاعات الذاكرة عشوائياً ثم نسخ نفسه وغير إسمه وقدرت الأضرار بـ ١١٨٠٠ دولار. لمزيد انظر: Joyce, Edward; Time Bobm inside the Texas Virus Trial; Computer Descision, Vol. 20 Dec, 1988; Ferbrache David, Pathology of Computer Vireuses, Op. cit., 1992, p. 233.

381 - Bigel, R.; The legal Dimension of Computer Crime, EDP-Auditor - Journal CU. S. A). Vol. 2, 1990 p. 59-67.

382 - Bigel, R.; The legal Dimension of Computer Crime, EDP-Auditor - Journal CU. S. A). Vol. 2, 1990 p. 59- 67.

المطلب الثالث : الاحتيال المعلوماتي والصور الأخرى

نظم المشرع القطري الاحتيال المعلوماتي (الإلكتروني) في الفصل الثالث المعنون بـ "التزوير والاحتيال الإلكتروني" من الباب الثاني من القانون القطري رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية⁽³⁸³⁾؛ ومن ثم يعاقب بالحبس مدة لا تجاوز عشر سنوات، وبالغرامة التي لا تزيد على (200,000) مائتي ألف ريال، كل من زور محرراً إلكترونياً رسمياً أو استعمله- مع علمه بذلك- لإبرام أحد العقود الذكية أو عند استخدام إحدى شبكات البلوك تشين⁽³⁸⁴⁾.

أما إذا وقع التزوير على محرر إلكتروني غير رسمي واستعمله الجاني مع علمه بتزويره فإن العقوبة تكون الحبس مدة لا تجاوز ثلاث سنوات، والغرامة التي لا تزيد على (100,000) مائة ألف ريال، أو بإحدى هاتين العقوبتين⁽³⁸⁵⁾. وهذا مع مراعاة أن كافة العقود الذكية- من وجهة نظر الباحث- هي محررات إلكترونية غير رسمية.

وتجدر الإشارة إلى أن المادة (11) من القانون القطري رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية قد تضمنت عدد من صور الاحتيال المعلوماتي التي تتصور أن ترتكب عبر الأنظمة الذكية أو عند استخدام إحدى شبكات البلوك تشين؛ إذ تنص هذه المادة على أن:

يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (100,000) مائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من ارتكب فعلاً من الأفعال التالية:

- 1- استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في انتحال هوية لشخص طبيعي أو معنوي.
- 2- تمكن عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، من الاستيلاء لنفسه أو لغيره على مال منقول، أو على سند أو التوقيع عليه، بطريق الاحتيال، أو باتخاذ اسم كاذب، أو بانتحال صفة غير صحيحة.

الصور الأخرى للجرائم التي تستهدف الأنظمة الذكية والبلوك تشين

تتمثل أبرز الصور الأخرى للجرائم التي تستهدف الأنظمة الذكية والبلوك تشين في الجرائم التي تستهدف بيانات والمعلومات الإلكترونية المخزنة أو المنقولة عبر الأنظمة الذكية والبلوك تشين وهو ما يفصله الباحث في البنود التالية:

1- جريمة سرقة المعلومات المخزنة أو المنقولة عبر الأنظمة الذكية والبلوك تشين

سبق أن أشار الباحث إلى الخلاف الفقهي حول مدى قابلية المعلومات المخزنة أو المنقولة عبر الأنظمة الذكية والبلوك تشين للسرقة لذلك نحيل إلى ما سبق ذكره في هذا الشأن، كما سبقت الإشارة بأن المشرع القطري جرم التقاط واعتراض المعلومات المخزنة أو المنقولة عبر الأنظمة الذكية والبلوك تشين⁽³⁸⁶⁾.

2- جريمة انتهاك سرية البيانات الإلكترونية والاستيلاء عليها

عرفت المادة (1) من القانون القطري رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية "البيانات والمعلومات الإلكترونية" بأنها: "كل ما يمكن تخزينه أو معالجته أو إنشاؤه أو نقله باستخدام وسيلة تقنية المعلومات، وبوجه خاص الكتابة أو الصور أو الصوت أو الأرقام أو الحروف أو الرموز أو الإشارات وغيرها".

وعرفت البيانات الشخصية في الفقه بأنها: كل بيان يتعلق بشخص محدد أو قابل للتحديد، بصورة مباشرة أو غير مباشرة، ومنها ما قد يتعلق بحرمة الحياة الخاصة للإنسان، ومنها ما يسمح برسم صورة لاتجاهاته وميوله، ومنها تلك التي تتعلق باتجاهاته

383 - انظر: المادتين (10، 11) من قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014م.

384 - انظر: المادة (1/10) من قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014م.

385 - انظر: المادة (2/10) من قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014م.

386 - المادة (4) من قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014م.

كما أن المشرع الفرنسي جرم في الفقرتين (5، 6) من المادة (٤٦٢) من قانون ١٩٨٨م استخدام المستندات المعلوماتية بدون إذن صاحبها، وتطبيقاً لذلك اتجه القضاء الفرنسي إلى وقوع جريمة السرقة بتصوير المستندات بدون موافقة صاحبها، على الرغم من ترك المستندات الأصلية، واتجهت أحكام القضاء الأوروبي نفس الوجهة التي تبناها القضاء الفرنسي، عندما اعتبر نسخ المعلومات صورة من صور جريمة السرقة. لمزيد انظر: د/ مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، ٢٠٠١ م، ص ١٤١.

السياسية، ومعتقداته الدينية، وتعاملاته المالية والبنكية، وجنسيته، وهوياته، وحالته العضوية، أو النفسية، أو العقلية والاقتصادية، أو الثقافية، أو الاجتماعية" (387).

والجدير بالذكر أن البيانات الإلكترونية محل الحماية هنا لا يقصد بها مجرد المعلومات المخزنة في النظام الذي بحد ذاتها، إنما تتمثل في المصالح التي تهددها هذه المعلومات، وبما أن الإنترنت أصبح شبكية عالمية، فإنه يمكن الربط بسهولة بين المعلومات الشخصية التي تجمع عن المستخدم للنظام الذي، سواء تم الحصول على هذه البيانات من خلال الاستثمارات الإلكترونية التي تعبأ من قبل المستخدم، أو من خلال استخدام برمجيات خاصة بالتجسس، تجمع معلومات مختصرة عن طريق استخدام الإنترنت، متضمنة معلومات حساسة، مثل: أرقام بطاقات الائتمان الخاصة، أو تستخدم مثل تلك البيانات لانتحال شخصية صاحب الحق في هذه البيانات، واستخدامها بشكل غير مشروع (388).

وفما يخص العقوبات المقررة للاعتداء على البيانات الإلكترونية المخزنة في الأنظمة الذكية تنص المادة (8) من قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014م، على أن: "يعاقب بالحبس مدة لا تتجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (100,000) مائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من تعدى على أي من المبادئ أو القيم الاجتماعية، أو نشر أخباراً أو صوراً أو تسجيلات صوتية أو مرئية تتصل بحرمة الحياة الخاصة أو العائلية للأشخاص، ولو كانت صحيحة، أو تعدى على الغير بالسب أو القذف، عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات".

وتجدر الإشارة إلى أن المشرع القطري قد عاقب على التقاط أو اعتراض أو التنصت العمدي - لأية بيانات مرسله عبر الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، أو على بيانات المرور التي يمكن أن تتعلق بالنظم الذكية بدون وجه حق بالحبس مدة لا تتجاوز سنتين، وبغرامة لا تزيد على (100,000) مائة ألف ريال، أو بإحدى هاتين العقوبتين (389).

المبحث الثالث: التحديات القانونية والتقنية في مكافحة هذه الجرائم وإثباتها

تمهيد وتقسيم: مع تزايد الوعي بالآثار الضارة للاعتداء على الأنظمة الذكية والبلوك تشين برزت الحاجة الملحة لتطوير استراتيجيات فعالة ومتكاملة لمواجهة لما يمثل اعتداءً على الحقوق الأساسية للأفراد في حرية التعاقد والحفاظ على حقهم في الخصوصية. إلا أن حماية الأنظمة الذكية والبلوك تشين تواجه العديد من التحديات القانونية والتقنية سواء فيما يتعلق بالإجراءات الوقائية من جرائم البلوك تشين أو بإجراءات مكافحتها أو فيما يتعلق بإثبات مسؤولية الجناة بأي بإقامة الدليل أمام القضاء بالطرائق التي حددها القانون، على ارتكاب هذه الجرائم. وسوف يفصل الباحث هذه التحديات القانونية والتقنية في المطالب الثلاث التالية:

- **المطلب الأول: إثبات الجرائم التي تستهدف الأنظمة الذكية والبلوك تشين**
- **المطلب الثاني: الإجراءات الوقائية والحماية من جرائم البلوك تشين**
- **المطلب الثالث: التحديات القانونية والتقنية في مكافحة هذه الجرائم.**

المطلب الأول: إثبات الجرائم التي تستهدف الأنظمة الذكية والبلوك تشين

حيث يبدأ الاتفاق في العقد الذي - كما سبق وذكر الباحث - باستخدام تقنية البلوك تشين - والتي تمثل السجل العام للمعاملات التي قد تم تنفيذها بين الأعضاء المشاركة - عن طريق توقيع العقد عبر مفاتيحهم الخاصة بهم، حيث يتم توقيع العقد الذي عن طريق مفتاح التشفير الخاص بكل طرف من أطراف العقد، حيث يكون لكل شخص توقيع رقمي خاص به وهوية رقمية خاصة به. ويعتمد التوقيع الرقمي في تقنية البلوك تشين على تقنية التشفير اللامتناهات؛ وهو يعتمد على المفتاح العام الذي يمكن مشاركته

387 - د/ مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 8.

388 - د/ محمد أمين الشوابكة، جرائم الحاسوب والانترنت "الجريمة المعلوماتية"، دار الثقافة للنشر والتوزيع، عمان، الأردن، ٢٠٠٩م، ص ٦٤

389 - المادة (4) من قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014م.

مع الأعضاء المشاركين في البلوك تشين حيث يُمثل هوية صاحبه، والآخر هو المفتاح الخاص الذي يتم الاحتفاظ به بسريّة تامة، ويُستخدم لفك تشفير المعاملة الرقمية. أي أنه يتم استخدامه لإنشاء التوقيعات الرقمية والتحقق من المعاملات، وبمجرد التحقق من المعاملة عن طريق تأكيد التجزئة الموجودة في التوقيع يتم التعاقد⁽³⁹⁰⁾. ورغم من ذلك توجد العديد من التحديات أمام إثبات المسؤولية القانونية داخل هذه الأنظمة⁽³⁹¹⁾ بوجهها المدني والجنائي⁽³⁹²⁾.

وحيث إننا بصدد جرائم الأنظمة الذكية والبلوك تشين فإن الجهات المختصة بكشف حقيقة هذه الجرائم والتحقيق فيها لها الحق في الاستعانة بكافة طرق الإثبات ومنها طرق الإثبات الإلكتروني؛ لذلك تنص المادة (14) من قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014م، على أن: "للنيابة العامة أو من تندبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن وأنظمة المعلومات ذات الصلة بالجريمة.

ويجب أن يكون أمر التفتيش مسبباً ومحددًا، ويجوز تجديده أكثر من مرة ما دامت مبررات هذا الإجراء قائمة. فإذا أسفر التفتيش عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة، يتعين على مأموري الضبط القضائي عرضها على النيابة العامة لاتخاذ ما يلزم بشأنها".

وقد أكد المشرع القطري على الأدلة الإلكترونية في الإثبات في المادة (15، 16) من قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014م، بأن حظر استبعاد أي دليل ناتج عن وسيلة من وسائل تقنية المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الإلكترونية أو البيانات والمعلومات الإلكترونية بسبب طبيعة ذلك الدليل⁽³⁹³⁾.

كما منح المشرع القطري للنيابة العامة أن تأمر بالجمع والتسجيل الفوري لأية بيانات أو معلومات إلكترونية أو بيانات مرور أو معلومات المحتوى التي تراها لازمة لمصلحة التحقيقات، وأن تأمر كل ذي صلة بتسليم الأجهزة أو الأدوات أو الوسائل أو البيانات أو المعلومات الإلكترونية أو بيانات المرور أو معلومات المحتوى ذات الصلة بموضوع الجريمة أو ما يفيد في كشف الحقيقة. كما منح النيابة العامة سلطة الأمر بالتحفظ على الأجهزة أو الأدوات أو الوسائل المستخدمة في ارتكاب الجريمة⁽³⁹⁴⁾. وتحقيقاً للغاية من إجراء التحفظ على الأجهزة أو الأدوات أو الوسائل المستخدمة في ارتكاب الجريمة فقد ألزم المشرع القطري الجهة المختصة بالتحفظ اتخاذ التدابير والإجراءات الكفيلة بالحفاظ على الأجهزة أو الأدوات أو وسائل تقنية المعلومات، أو الأنظمة المعلوماتية أو البيانات أو المعلومات الإلكترونية محل التحفظ، لحين صدور قرار من الجهات القضائية المعنية بشأنها⁽³⁹⁵⁾.

390 - د/ يوسف محمد قاسم عبيدات، لافي محمد موسى درادكة، وسائل حماية التوقيع الرقمي التي جعلته عنصراً مهماً في زيادة التعامل عبر الإنترنت: دراسة تحليلية في قانون المعاملات الإلكترونية الأردني. مجلة مؤتة للبحوث والدراسات- سلسلة العلوم الإنسانية والاجتماعية، (24)، 1، 2009، ص 23؛ د/ طارق عفيفي صادق، دور القانون المدني في دعم التحول الرقمي في مصر، بالتطبيق على قانون التوقيع الإلكتروني والتعديل والمقترح له، بحث مقدم لمؤتمر الإصلاح التشريعي والعدالة الناجزة، تنظيم الجمعية المصرية للاقتصاد السياسي والأحصاء والتشريع، القاهرة، يومي 12، 13 ديسمبر 2020م، ص 15.

391 - د/ فيروز علوش، خصوصية التأمين في عصر الذكاء الاصطناعي، مج 12، ع 2، 2025م، ص 343.

392 - د/ محمد الأميري، د/ عبد الإله النوايسة، الأسس القانونية للمسؤولية الجنائية للذكاء الاصطناعي، مجلة الحقوق العدد 4، 2025م، ص 270.

393 - إذ تنص المادة (15) من قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014م، على أن: "لا يجوز استبعاد أي دليل ناتج عن وسيلة من وسائل تقنية المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الإلكترونية أو البيانات والمعلومات الإلكترونية بسبب طبيعة ذلك الدليل". أما المادة (16) من القانون نفسه فتتص على أن: "لا يجوز استبعاد أي من الأدلة المتحصل عليها بمعرفة الجهة المختصة أو جهات التحقيق من دول أخرى، لمجرد ذلك السبب، طالما أن الحصول عليها قد تم وفقاً للإجراءات القانونية والقضائية للتعاون الدولي".

وهو ما أكد عليه المشرع المصري في المادة (١١) من قانون مكافحة تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨م، والتي تنص على أن: "يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط الدعامة الإلكترونية، أو النظام المعلوماتي أو من برامج الحاسب، أو من أي وسيلة لتقنية المعلومات ذات قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائي متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية لهذا القانون".

394 - المادتين (17، 18) من قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014م.

395 - المادة (18) من قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014م.

كما ألزم المشرع القطري مزود الخدمة تزويد الجهة المختصة، أو جهات التحقيق والمحاكمة، بجميع البيانات والمعلومات اللازمة التي تساعد في كشف الحقيقة، بناءً على أمر من النيابة العامة. والالتزام بالاحتفاظ بمعلومات المشترك لمدة سنة. والاحتفاظ المؤقت والعاجل ببيانات تقنية المعلومات أو بيانات المرور أو معلومات المحتوى لمدة تسعين يوماً قابلة للتجديد، بناءً على طلب الجهة المختصة أو جهات التحقيق والمحاكمة. كذلك ألزم المشرع القطري مزود الخدمة بالتعاون ومساعدة الجهة المختصة في جمع أو تسجيل المعلومات والبيانات الإلكترونية وبيانات المرور، بناءً على الأوامر الصادرة إليها من الجهات القضائية⁽³⁹⁶⁾. وجدير بالذكر أن هناك من الأدلة الإلكترونية الذي يستمد من فحص مسارات الإنترنت (الفحص الإلكتروني) والذي يلجأ إليه في الغالب في حالات استخدام الفيروسات والضارة والمدمرة وكذلك يستخدم في حالات الإجرام والاحتيال الإلكتروني من خلال الهاتف الخليوي⁽³⁹⁷⁾.

وفي كل الأحوال فإنه يجب أن يظل الدليل الإلكتروني خاضعاً لضوابط المشروعية والقانونية المحددة لقبول الأدلة بشكل عام أو الدليل الإلكتروني بشكل خاص، وإن يتم استخلاصه أو مراجعته بمعرفة مختص لديه معرفة تقنية خاصة- بأجهزة الهاتف أو الحواسيب الآلية- مع مراعاة إمكانية العبث بهذا النوع من الأدلة- كما في حالة تسجيلات الهاتف ومراسلات البريد الإلكتروني. هذا بالإضافة إلى ضرورة مراعاة حقوق المتهم الثابتة له بوصفه فرداً طبيعياً أو عضواً في جماعة بشرية، وإن الأصل في الإثبات الجنائي قرينة البراءة⁽³⁹⁸⁾.

كما يجب أن تكون الأدلة الإلكترونية غير قابلة للشك أي يقينية: فيشترط في الأدلة المستخرجة من الحاسوب والإنترنت، أن تكون غير قابلة للشك بالإدانة بناءً عليها إذا وصل اقتناع القاضي إلى حد الجزم واليقين بقوتها الاستدلالية على صدق نسبة الجريمة إلى شخص معين من عدمه ليدحض قرينة افتراض البراءة⁽³⁹⁹⁾.

المطلب الثاني: الإجراءات الوقائية والحماية من جرائم الأنظمة الذكية والبلوك تشين

تساهم تكنولوجيا المعلومات بدور كبير في الحماية من الجرائم بوجه عام، والوقاية من الجرائم الواقعة على الأنظمة المعلوماتية وعلى البلوك تشين على وجه الخصوص⁽⁴⁰⁰⁾.

وقد نصت المادة (22) من قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014م، على أن: "تلتزم أجهزة الدولة ومؤسساتها وهيئاتها والجهات والشركات التابعة لها بما يلي:

1- اتخاذ التدابير الأمنية الوقائية اللازمة لحماية أنظمتها المعلوماتية ومواقعها الإلكترونية وشبكاتها المعلوماتية والبيانات والمعلومات الإلكترونية الخاصة بها.

396 - المادة (21) من قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014م.

397-Richard Sallies, A Look at how U. S. based Yahoo! Was condemned by French law, P.6, university of Montreal, available online at, <http://www.juriscom.net/txt/jurisfr/cit/yauctions.html>.

398- للمزيد راجع: د/ ممدوح عبد الحميد عبد المطلب، د/ زبيده محمد قاسم، عبد الله عبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر، منشور ضمن أعمال مؤتمر " الأعمال المصرفية والإلكترونية " نظمتها كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة وغرفة تجارة وصناعة دبي، الفترة من 10-12/5/2003م، المجلد الخامس، ص225 وما يليها؛ د/ طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية والقانون المنعقد في الفترة من 28-29/10/2009م تنظمه أكاديمية الدراسات العليا - طرابلس، ص 24-29؛ د/ طارق عفيفي صادق، جرائم الهاتف المحمول- دراسة مقارنة، المركز القومي للإصدارات القانونية، 2023م، ص 338.

399 - د/ أحمد عوض بلال، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة، دار النهضة العربية، القاهرة، 2013م، ص 259. وتجدر الإشارة إلى أن محكمة التمييز القطرية قد قضت بالآتي: "2- من المقرر أنه بحسب الحكم كما يتم تدليله ويستقيم قضاؤه أن يورد الأدلة التي صحت لديه على وقوع الجريمة ونسبتها لمرتكبها ولا عليه أن يتعقب المتهم في كل جزئية من جزئيات دفاعه، لأن مفاد التفاته عنها أنه لم ير فيها ما ينال من عقيدته في الدعوى فاطرحها - كالحال في الدعوى - ومن ثم فإن ما ينهه الطاعن على الحكم بدعوى الالتفات عن دفاعه بعدم توافر عناصر الاشتراك في الجرائم في حقه لا يكون له محل". محكمة التمييز - المواد الجنائية - رقم: 168/2014- تاريخ الجلسة: 2014/12/15.

400 - د/ فاطمة ميروك، د/ ذيب محمد، الجرائم المستحدثة، ضبط المفهوم وتحديد الأنماط، مجلة الفكر القانوني والسياسي، مج 7، ع 1، 2023، ص 834.

في الحالات التي يجوز فيها تفتيش مسكن المتهم، ولا بد الأخذ في الاعتبار مراعاة ما إذا كانت مكونات الحاسب الإلكتروني المراد تفتيشها متصلة بحاسبات أخرى في مكان آخر كمسكن غير المتهم مثلاً، أم منعزلة عن غيرها من الحاسبات الإلكترونية(404). كما ثار الخلاف بشأن جواز تفتيش مكونات الحاسب الإلكتروني المنطقية أو الإلكترونية والشبكات، حيث يذهب بعض الفقه القانوني(405) أنه إذا كانت غاية التفتيش هو ضبط الأدلة المادية التي تساهم في كشف الحقيقة، فإن التفتيش يمتد ليشمل البيانات الإلكترونية بمختلف صورها وهذا ما أخذ به المشرع القطري على النحو السابق بيانه عند استعراض سلطات النيابة العامة في التحقيق في الجرائم الإلكترونية(406).

ومما سبق يتضح جلياً أنه يسمح للمحقق تتبع وضبط وفحص بيانات الحاسب غير الملموسة، وعلى النقيض من ذلك يري رأي آخر أنه إذا كانت الغرض من التفتيش هي ضبط الأدلة المادية التي تساهم في كشف الحقيقة، فإن ذلك لا ينطبق على بيانات الحاسب الإلكتروني غير الملموسة، ولمواجهة هذا القصور التشريعي يري هذا الاتجاه حتمية إضافة إلى الهدف التقليدي التفتيش عبارة "المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي"، وفي ظل التطورات التقنية الحديثة المتلاحقة يضحى الغاية الجديدة من التفتيش هي الفحص والبحث عن الأدلة المادية والمواد المعالجة بواسطة الحاسب(407).

أما فيما يخص مدى جواز تفتيش حاسب أو شبكة مملوكة لشخص آخر غير المتهم أو نهاية طرفية موجودة في مكان آخر خارج الدولة، عندما يعتمد معتادي الجرائم الإلكترونية على تخزين بياناتهم على حواسيب إلكترونية خارج الدولة مستخدمين في ذلك شبكة الاتصالات والإنترنت بُغية عرقلة التحقيقات، حيث يمتد التفتيش إلى خارج الإقليم الجغرافي للدولة التي صدر من جهتها المختصة الإذن ودخوله في المجال الجغرافي للدولة الأخرى، وهو ما يسمى بالولوج أو التفتيش عبر الحدود، ولذلك تسمح بعض التشريعات المقارنة بتفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج إقليم الدولة، فقد أجازت المادة ١٧ فقرة (٢) من قانون الأمن الداخلي الفرنسي السالف الذكر لمأموري الضبط القضائي أن يقوموا بتفتيش الأنظمة المتصلة حتى ولو تواجدت في خارج الإقليم مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية(408). كما أجاز المجلس الأوروبي من خلال توصي رقم ١٣ لسنة ١٩٩٥ المتعلقة بالمشكلات القانونية لقانون الإجراءات الجنائية المتصلة بتقنية المعلومات من التفتيش الإلكتروني للحاسب إلى الشبكة المتصلة به ولو كانت تلك الشبكة واقعة في إقليم دولة أخرى، وأكد على أنه يجوز لسلطة التحقيق والاستدلال بمناسبة التفتيش الإلكتروني بسط مجال تفتيش حاسب معين يدخل في دائرة اختصاصها إلى غيرها من الأجهزة الإلكترونية المرتبطة به بواسطة شبكة الإنترنت بما فيها المتواجدة خارج الاختصاص الوطني وضبط المعطيات المتواجدة فيها(409).

إشكالية الاختصاص المكاني للقانون

نظم المشرع القطري السلطة القضائية واختصاص محاكم الدولة في الدولة في الدستور القطري الدائم وفي قانون السلطة القضائية القطري رقم (8) لسنة 2023م، كما أشير لتفصيل هذا الاختصاص في القوانين الإجرائية وخاصة قانون الإجراءات

404 - د/ ممدوح عبد الحميد عبدالمطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، ٢٠٠٦م، ص ٥٨.

405 - John R.Vacca. computer forensics: computer crime scene Investigation- computers, 2005p. 85

406 - وقد ذهب إلى هذا الاتجاه قانون الإجراءات الجنائي اليوناني، حيث تعطي المادة (٢٥١) منه سلطات التحقيق إمكانية القيام بكل ما تراه ضروريا لجمع الأدلة وحمايتها، ويفسر ذلك الفقه اليوناني بأن التفتيش يشمل بالفحص والتتبع والضبط البيانات المخزنة أو المعالجة إلكترونياً، حيث أن ضبط البيانات المخزنة في الذاكرة الداخلية للحاسب الإلكتروني لا تعد مشكلة في اليونان، إذ بإمكان سلطة التحقيق أن تعطي أمراً للخبير بجمع البيانات التي قد تكون مقبولة كدليل في المحاكمة الجنائية، بينما ذهبت المادة (٤٨٧) من القانون الجنائي الكندي إلى أنه لا بد من صدور إذن لضبط أي شيء طالما تتوفر براهين معقولة يعتقد معها بأن الجريمة ارتكبت أو يشتبه في ارتكابها، أو أن هناك نية مبيتة في استخدامه في ارتكاب الجريمة أو اعتبار نتائج دليله على وقوع الجريمة.

Vassil Aki, computer crimes and other crimes against information technology in Greece "R.I.D.P. 1993, p. 355.

407 - Bruce Middleton, Cyber Crime Investigator's Field Guide, Auerbach Publishers, 2022 p. 66.

408 - Loi 18 Mars 2003 pour la sécurité intérieur article 1712.

409 - د/ أحمد لطفي السيد مرعي، الأدلة الرقمية المتحصلة من التفتيش الجنائي الإلكتروني: دراسة مقارنة، مجلة الدراسات القانونية والاقتصادية، جامعة مدينة السادات - كلية الحقوق، المجلد الثامن، العدد الثاني، ٣٠ يونيو ٢٠٢٢، ص ١ - ٥٣

الجنائية، لذا تعد النصوص التي تقرر قواعد الاختصاص من النصوص الأمرة التي تتعلق بالنظام العام ولا تجوز مخالفتها. وبالتالي على المحكمة أن تحكم من تلقاء نفسها بعدم اختصاصها لانتفاء ولايتها، ويجوز للخصوم الدفع به في أية حالة كانت عليها الدعوى (410).

وتعتبر جريمة الاعتداء على الأنظمة المعلوماتية بمثابة نقطة تحول مهمة في مجال تطبيق القانون من حيث تحديد المكان، نظراً لطبيعتها العالمية وتعقيدها، حيث يصعب غالباً تحديد الموقع الدقيق لارتكابها ضمن الحدود المحلية. علاوة على ذلك، تتسبب هذه الجريمة في العديد من التداعيات الجنائية التي تتداخل مع مختلف الأوصاف القانونية، مما يجعل تحديد المحكمة المختصة للنظر فيها أمراً معقداً ويحتاج إلى دراسة معمقة (411).

ولم تحل إشكالية ارتكاب الجريمة الإلكترونية- سواء تعلقت بالأنظمة الذكية أم لا- من شخص خارج إقليم الدولة بحل قانونياً واضحاً مع تمسك الدول بمدى منع تسليم رعاياها مما يترتب عليه إفلات الجناة من العقاب.

لذلك، يرى الباحث ضرورة وضع نص قانوني يتيح فرض اختصاص القانون والمحاكم القطرية لمحاسبة الشخص الذي يضر بالأنظمة الذكية، سواء ارتكب الفعل داخل الدولة أم خارجها وسواء كان الجاني قطرياً أم لا مع منح السلطات الحق في تسليم الجاني للدول المضرومة من الجريمة بما يضمن تحقيق العدالة ومنع مثل هؤلاء المجرمين من التهرب من العقوبة.

الخاتمة :

اهتمت دراستنا بموضوع غاية في الأهمية العملية والقانونية ألا وهو " الحماية الجنائية للأنظمة الذكية والمعلوماتية في التشريع القطري- دراسة تحليلية" وذلك في إطار ثلاث مباحث تعلق المبحث الأول بتعريف الأنظمة الذكية وأهميتها القانونية وبيان ماهية البلوك تشين ومفهوم الحماية الجنائية للأنظمة الذكية. وفي المبحث الثاني درس الباحث أبرز صور الجرائم التي تستهدف الأنظمة الذكية والبلوك تشين وهي جريمة اختراق الأنظمة الذكية، وجريمة اطلاقات الفيروسات الضارة، وجريمة الاحتيال المعلوماتي وبعض الصور الأخرى. أما المبحث الثالث فقد خصصه الباحث لدراسة التحديات القانونية والتقنية في مكافحة هذه الجرائم وإثباتها وبيان الإجراءات الوقائية والحماائية من جرائم البلوك تشين.

وقد انتهى هذا البحث إلى عدد من النتائج والتوصيات، تتمثل في الآتي:

أولاً: النتائج

- 1- عرف المشرع القطري النظام المعلوماتي في قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014م بأنه: "مجموعة برامج وأجهزة، تستخدم لإنشاء أو استخراج المعلومات، أو إرسالها، أو استلامها، أو عرضها، أو معالجتها، أو تخزينها" وهو ما يتفق مع التعريفات المقترحة من قبل الفقه.
- 2- غالبية الجرائم الإلكترونية التي يتم ارتكابها للاعتداء على النظم الذكية أو تستخدم فيها هذه الأنظمة يكون الهدف منها الحصول على المعلومات الإلكترونية، التي تكون إما محفوظة على النظم الذكية أو على أجهزة الحاسب الآلي المتصلة بها، أو منقولة عبر شبكة الإنترنت، وغالباً ما يتم الاعتداء على هذه المعلومات بالاستيلاء عليها، أو تغييرها، أو حذفها، أو إلغائها نهائياً، ويكون الدافع من ذلك التنافس، أو الابتزاز، أو تحقيق مكاسب، أو الحصول على مزايا أخرى.
- 3- تشمل جرائم اختراق الأنظمة الذكية- من وجهة نظر الباحث- جريمة الدخول غير المشروع – أي الدخول العمدي بدون وجه حق- للأنظمة الذكية، وجريمة البقاء داخل هذه الأنظمة بدون وجه حق أي تجاوز حدود الدخول. والملاحظ أن المادتين (2)، (3) من القانون القطري رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية لم تفرق بين هذه الجرائم. إلا أن هاتين

410 - د/ خالد عبدالقادر الأمين محمد، علاقة الاختصاص القضائي بالنظام العام، مجلة القلزم العلمية، مركز بحوث ودراسات دول حوض البحر الأحمر، ع 19، 2022، ص 27 وما بعدها.

411 - د/ نجاه عباوي، الإشكالات القانونية في تجريم الاعتداء على أنظمة المعلومات، دفاتر السياسة والقانون، جامعة قاصدي مرباح ورقلة - كلية الحقوق والعلوم السياسية، ع 16، 2017م، ص 43.

المادتين فرقت بين الاعتداء على موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها وبين الاعتداء على الأنظمة الذكية المملوكة للأشخاص العاديين (أشخاص القانون الخاص).

4- الإختلاف القائم بين جرمي الدخول إلى الأنظمة الذكية والبقاء غير المصرح به في هذه الأنظمة يتمثل في أن جريمة الدخول إلى الأنظمة الذكية جريمة ايجابية تقتضي إتيان فعل الدخول، في حين تقوم جريمة البقاء في الأنظمة الذكية بسلوك إجرامي سلبي، ورغم دخول الجاني صدفة أو خطأ، ورغم علمه بأن ذلك غير مشروع فهو يرفض الخروج من النظام وبمعنى آخر يمتنع عن الخروج، لذلك فالنشاط الإجرامي - حسب رأي هذا الجانب- يمثل في هذه الصورة سلوكا سلبيا من الجاني.

5- تُعتبر جريمة الاعتداء على الأنظمة المعلوماتية بمثابة نقطة تحول مهمة في مجال تطبيق القانون من حيث تحديد المكان، نظراً لطبيعتها العالمية وتعقيدها، حيث يصعب غالباً تحديد الموقع الدقيق لارتكابها ضمن الحدود المحلية. علاوة على ذلك، تتسبب هذه الجريمة في العديد من التداعيات الجنائية التي تتداخل مع مختلف الأوصاف القانونية، مما يجعل تحديد المحكمة المختصة للنظر فيها أمراً معقداً ويحتاج إلى دراسة معمقة.

6- لم تحظى إشكالية ارتكاب الجريمة الإلكترونية- سواء تعلقت بالأنظمة الذكية أم لا- من شخص خارج إقليم الدولة بحل قانونياً واضحاً مع تمسك الدول ببدأ منع تسليم رعاياها مما يترتب عليه إفلات الجناة من العقاب.

ثانياً: التوصيات

1- يجب على المشرع القطري أن يبادر بإصدار تشريع خاص بالعقود الذكية يتضمن بين تنظيمها متكاملًا للحماية المدنية والجنائية للمشاركين في هذه العقود.

2- من الملائم استحداث برامج دراسة خاصة في كليات الدراسات العليا لدراسة الجوانب القانونية والفنية للعقود الذكية.

3- ضرورة وضع نص قانوني يتيح فرض اختصاص القانون والمحاكم القطرية لمحاسبة الشخص الذي يضر بالأنظمة الذكية، سواء ارتكب الفعل داخل الدولة أم خارجها وسواء كان الجاني قاطناً أم لا مع منح السلطات الحق في تسليم الجاني للدولة المضرومة من الجريمة بما يضمن تحقيق العدالة ومنع مثل هؤلاء المجرمين من التهرب من العقوبة.

❖ لائحة المراجع

أولاً: المراجع العامة

- ابن منظور، محمد بن مكرم بن علي، أبو الفضل، جمال الدين الأنصاري الرويفعي الإفريقي. (1414هـ). لسان العرب (الطبعة الثالثة). دار صادر.

- بلال، أحمد عوض. (2013). قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة. دار النهضة العربية.

- صادق، طارق عفيفي. (2014). جرائم الهاتف المحمول والتعويض عنها: دراسة مقارنة بين القانون المصري والإماراتي والسعودي (الكتاب الأول: المسؤولية الجنائية الخلوية). المركز القومي للإصدارات القانونية.

- عمر، أحمد مختار. (2008). معجم اللغة العربية المعاصرة. عالم الكتب.

- القاضي، زياد. (1997). مبادئ تحليل نظم الحاسوب وتعميمها (الطبعة الأولى). دار الصفاء للنشر.

ثانياً: المراجع المتخصصة

- حجازي، عبد الفتاح بيومي. (2006). مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي (الطبعة الأولى). دار الفكر الجامعي.

- رمضان، مدحت. (2001). الحماية الجنائية للتجارة الإلكترونية. دار النهضة العربية.

- الشوابكة، محمد أمين. (2007). جرائم الحاسوب والإنترنت — الجريمة المعلوماتية. دار الثقافة للنشر والتوزيع.

- عيسى، هيثم السيد أحمد. (2021). نشأة العقود الذكية في عصر البلوك تشين. دار النهضة العربية.
- الغافري، حسين، والألفي، محمد. (2008). جرائم الإنترنت بين الشريعة الإسلامية والقانون. دار النهضة العربية.
- فريد، نصر أبو الفتوح. (2022). العقود الذكية: الماهية والأحكام — دراسة تحليلية. دار النهضة العربية.
- منصور، محمد حسين. (2003). المسؤولية الإلكترونية. دار الجامعة الجديدة للنشر.
- ثالثاً: رسائل الدكتوراه والماجستير
- البعول، سامي. (2022). العقود الذكية باستخدام تقنية البلوكشين — دراسة تأصيلية فقهية تطبيقية [رسالة دكتوراه، الجامعة الأردنية].
- الحجامي، أنسام سمير طاهر. (2013). الحماية الجنائية لتكنولوجيا المعلومات [رسالة ماجستير، كلية القانون، جامعة كربلاء].
- الحشاش، وائل عبد الكريم حسن. (2024). العقود الذكية: دراسة فقهية [رسالة دكتوراه، كلية الدراسات العليا، جامعة النجاح الوطنية].
- صادق، طارق عفيفي. (2011). الخطر محل التأمين من المسؤولية المدنية في مجال المعلوماتية [رسالة دكتوراه، كلية الحقوق، جامعة بني سويف].
- رابعاً: المقالات والأبحاث المحكمة
- فداد، العياشي الصادق. (2019). العقود الذكية "Smart Contracts". مؤتمر مجمع الفقه الإسلامي الدولي، الدورة الرابعة والعشرون، دبي.
- محمد، حسام الدين محمود. (2023). العقود الذكية المبرمة عبر تقنية البلوك تشين. المجلة القانونية، جامعة القاهرة — كلية الحقوق — فرع الخرطوم، 16(1).
- محمد، خالد عبد القادر الأمين. (2022). علاقة الاختصاص القضائي بالنظام العام. مجلة القلزم العلمية، مركز بحوث ودراسات دول حوض البحر الأحمر، (19).
- الجميلي، عمر. (2019). العقود الذكية "Smart Contracts": واقعها وعلاقتها بالعملات الافتراضية. مؤتمر مجمع الفقه الإسلامي الدولي، الدورة الرابعة والعشرون.
- السفري، عبد الله. (2020). استخدام سلسلة الكتل في حفظ حقوق الملكية الفكرية. مجلة العلوم الاقتصادية والإدارية والقانونية، 4(5).
- مبروك، فاطيمة، وذيب، محمد. (2023). الجرائم المستحدثة: ضبط المفهوم وتحديد الأنماط. مجلة الفكر القانوني والسياسي، 7(1).
- علوش، فيروز. (2025). خصوصية التأمين في عصر الذكاء الاصطناعي. مجلة [اسم المجلة]، 12(2).
- سانو، قطب مصطفى. (2019). العقود الذكية في ضوء الأصول والمقاصد والمآلات: رؤية تحليلية. مؤتمر مجمع الفقه الإسلامي الدولي، الدورة الرابعة والعشرون.
- الأميري، محمد، والنوايسة، عبد الإله. (2025). الأسس القانونية للمسؤولية الجنائية للذكاء الاصطناعي. مجلة الحقوق، (4).
- بن عودة، مراد. (2022). إشكالية تطبيق أحكام المسؤولية الجنائية على جرائم الذكاء الاصطناعي. مجلة الحقوق والعلوم الإنسانية — جامعة زيان عاشور بالجلفة، 15(1).
- الشاطر، منير. (2019). تقنية البلوكشين وتحديات المالية الإسلامية. مجلة دراسات اقتصادية معاصرة، 25(1).

- بطيح، مها رمضان محمد. (2021). المسؤولية المدنية عن أضرار أنظمة الذكاء الاصطناعي: دراسة تحليلية مقارنة. المجلة القانونية، جامعة القاهرة، كلية الحقوق، فرع الخرطوم، 9(5).
- عباوي، نجا. (2016). الإشكالات القانونية في تجريم الاعتداء على أنظمة المعلومات. دفاتر السياسة والقانون، جامعة قاصدي مرباح ورقلة — كلية الحقوق والعلوم السياسية، 16(1).
- معداوي، نجية. (2021). العقود الذكية والبلوكتشين. مجلة المفكر للدراسات القانونية والسياسية، 4(2).
- فريد، نصر أبو الفتوح. (2020). العقود الذكية بين الواقع والمأمول: دراسة تحليلية. مجلة الأمن والقانون، أكاديمية شرطة دبي، 28(2).
- الحنيطي، هناء محمد. (2019). ماهية العقود الذكية. مؤتمر مجمع الفقه الإسلامي الدولي، الدورة الرابعة والعشرون، منظمة التعاون الإسلامي، دبي.
- عبيدات، يوسف محمد قاسم، ودرادكة، لافي محمد موسى. (2009). وسائل حماية التوقيع الرقمي التي جعلته عنصراً مهماً في زيادة التعامل عبر الإنترنت: دراسة تحليلية في قانون المعاملات الإلكترونية الأردني. مجلة مؤتة للبحوث والدراسات — سلسلة العلوم الإنسانية والاجتماعية، 24(1).
- صادق، طارق عفيفي. (2020، ديسمبر 12-13). دور القانون المدني في دعم التحول الرقمي في مصر، بالتطبيق على قانون التوقيع الإلكتروني والتعديل والمقترح له [بحث مقدم لمؤتمر]. مؤتمر الإصلاح التشريعي والعدالة الناجزة، الجمعية المصرية للاقتصاد السياسي والإحصاء والتشريع، القاهرة.
- خليفة، إيهاب. (2018، مارس). البلوكتشين: الثورة التكنولوجية القادمة في عالم المال والإدارة. المستقبل للأبحاث والدراسات المتقدمة، 3(3).
- البرعي، أحمد سعد. (2020، ديسمبر). إنشاء عقود المعاملات وتنفيذها بين الطرق التقليدية وتقنية البلوكتشين والعقود الذكية: دراسة فقهية مقارنة. المجلة العلمية لكلية الدراسات الإسلامية والعربية للبنين، جامعة الأزهر، 39(3).
- فرج، هيفاء عبد العالي. (2023، ديسمبر). الحماية الجنائية للمواقع الإلكترونية والأنظمة المعلوماتية للدولة: دراسة مقارنة. مجلة العلوم القانونية، كلية القانون، جامعة المرقب، 11(2).
- الكوح، محمد بدر أحمد. (2024، يناير-مارس). ماهية العقود الذكية. مجلة كلية الشريعة والقانون بطنطا، جامعة الأزهر، 39(3).

خامساً: المراجع الأجنبية

- Savelyev, A. (2016). Contract law 2.0: Smart contracts as the end of classic contract law. National Research University, Higher School of Economics.
- Bigel, R. (1990). The legal dimension of computer crime. EDP-Auditor Journal, 2.
- Conish, E. R. (1990). Intellectual property: Patents, copyright, trade marks. Sweet and Maxwell.
- Ferbrache, D. (1992). Pathology of computer viruses. Springer-Verlag.
- Joyce, E. (1988, December). Time bomb inside the Texas virus trial. Computer Decision, 20.
- Vacca, J. R. (2005). Computer forensics: Computer crime scene investigation. Charles River Media.
- Aki, V. (1993). Computer crimes and other crimes against information technology in Greece. R.I.D.P.