AGJSLS; ISSN: 2749-7976; 2025, Volume 03, Issue 01, 57-80

Original Article 57

Arab German Journal of Sharia and Law Sciences المجلة العربية الألمانية لعلوم الشريعة والقانون

Criminal confrontation of digital piracy of bank cards and ways to prevent it in Moroccan legislation

المواجهة الجنائية للقرصنة الرقمية للبطاقة المصرفية وسبل الوقاية منها بالتشريع المغربي

يونس نفيد[1]*، حابس مشهور الفواعرة[1]، محمد وهّاب[2]، سارة جوريش[3]

1 قسم القانون الجنائي، كلية العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية.

2 المركز العربي للتعاون الفني في إدارة الهجرة والحدود، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية.

3 كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة شعيب الدكالي، الجديدة، المملكة المغربية.

Youness Nafid [1]*, Habis AL Fawara[1], Mohamed Wahab[2], Sara Joraiche[3]

1 Department of Criminal Law, Naif Arab University for Security Sciences, Riyadh, Kingdom of Saudi Arabia.

2 Arab Center for Technical Cooperation in Migration and Border Management, Naif Arab University for Security Sciences, KSA.

3 Faculty of Legal, Economic, and Social Sciences, Chouaib Doukkali University, El Jadida, Marroco.

Received 12 Jul. 2024; Accepted 01 Oct. 2024; Available Online 20 Dec. 2024

Check for updates

https://birne-online.de/journals/index.php/agjsls

Keywords:
Cybercrime, Digital Hacking, Bank Card, Criminal Confrontation, Moroccan Law.

الكلمات المفتاحية:
الجرائم المعلوماتية،
القرصنة الرقمية،
البطاقة المصرفية،
المواجهة الجنائية،
القانون المغربي.

Abstract

Cybercrime has evolved in light of the rapid pace of the electronic revolution that has touched all aspects of life. This progress has not been without its drawbacks, as various financial and banking institutions have been affected by the increase in criminal activities that have exploited the rapid pace of e-commerce and the use of bank cards as a tool for monetary transactions. This paper focuses on the digital hacking crimes that have affected bank cards, which is one of the serious forms of electronic hacking that threatens the security of personal data and banking security according to Moroccan legislation and means of prevention.

The study addressed the concepts of cybercrime and digital hacking, and discussed Moroccan legislation related to the offence of bank card hacking, starting with the law on terrorism, Law 03-07 supplementing the Criminal Code and Law 43-20, and legal approaches to this offence. One of the most important findings of the research is that the Moroccan legislator, in order to better protect automated data processing systems, updated its legal arsenal by issuing Law No. 07-03, under which the offence of bank card hacking falls within the scope of the offences of fraudulent access, forgery and information fraud. The problem is manifested in the multiplicity of texts criminalising and punishing this offence and the overlap between them, which makes them all applicable due to their multiple descriptions. Draft Law No. 03. 23, amending and supplementing the Code of Criminal Procedure, addresses many important issues related to this subject.

The study recommends strengthening and updating the legal system in accordance with the latest developments and best practices, considering fair trial guarantees. The study also recommends strengthening the technical preventive role and professional training in the competent authorities and updating it regularly to keep abreast of the latest security threats and address them effectively, develop awareness and education campaigns, and strengthen institutional, regional and international cooperation.

* Corresponding Author: Youness Nafid
Email: Ynafid@nauss.edu.sa
doi: 10.51344 /agjslsv3i13

المستخلص

تطورت الجرائم المعلوماتية في ظل سرعة وثيرة الثورة الإلكترونية التي مسَّت مختلف مناحي الحياة. ولَم يَخْلُ هذا التقدم من سلبيات، فقد تأثرت مختلف المؤسسات المالية والمصرفية بسبب تزايد الأنشطة الإجرامية التي استغلت سرعة وثيرة التجارة الإلكترونية، واستخدام البطاقات المصرفية كأداة للمعامَلات النقدية. ركزت هذه الورقة على مواجهة جرائم القرصنة الرقمية التي طالت البطاقة المصرفية التي تُعد أحد أشكال الاختراق الإلكتروني الخطيرة والمهدِّدة لأمن البيانات الشخصية والأمن البنكي وفق التشريع المغربي وسبل الوقاية منها.

تناولت الدراسة مفهومي الجريمة المعلوماتية والقرصنة الرقمية، وناقشت التشريعات المغربية المتعلقة بجريمة القرصنة الإلكترونية للبطاقة البنكية بداية بالقانون المتعلق بالإرهاب، وقانون 30-70 المتمم لمجموعة القانون الجنائي والقانون 34 - 02، والمقاربات القانونية لهذه الجريمة. ومن أهم النتائج التي توصل إليها البحث أن المشرع المغربي عمل بهدف حماية أفضل لنظُم المعالَجة الآلية للمعطيات على تحيين ترسانته القانونية بإصدار القانون رقم 70-30 وبموجبه فإن جريمة القرصنة الإلكترونية للبطاقة البنكية تدخل ضمن نطاق جرائم الدخول الاحتيالي، والتزييف، والنصب المعلوماتي، ويتجلى الإشكال في تعدد النصوص المجرِّمة والمعاقِبة لهذه الجريمة والمتداخِلة فيما بينها؛ ما يجعلها جميعها قابلة للتطبيق؛ وذلك لعلّة تعدد أوصافها، وقد تدارك مشروع القانون رقم 32.30 القاضي بتغيير وتتميم قانون المسطرة الجنائية العديد من الأمور المهمة المتعلقة بهذا الموضوع.

وتوصي الدراسة بتقوية وتحيين المنظومة القانونية وفْق آخِر المستجدات، وأفضل الممارسات مع مراعاة ضمانات المحاكمة العادلة. وتعزيز الدور الوقائي التقني والتدريب المهني في الجهات المختصة، وتحديثه بانتظام لمواكَبة أحدث التهديدات الأمنية ومعالجتها بفاعلية، وتنمية حملات التوعية والتثقيف وتعزيز التعاون المؤسساتي والإقليمي والدولي.

1. المقدمة

يعيش عالم التجارة والمال اليوم ثورة تكنولوجية مذهلة، تجلَّت ملامحها وبوادرها مع ظهور الحواسيب وسرعة وترابُط الأسواق المالية في ظل ما يُعرف بالشبكة العالمية للمعلومات (الإنترنت)، وما تفرضه طبيعة المعاملات التجارية والمالية. ولقد شملت هذه التغيرات القطاع المصرفي أيضًا في ظل تزايد التوجه والتكامل الاقتصادي، وانتشار المنافسة بين البنوك من تطور واضح في مجال تنفيذ العمليات المصرفية باستخدام شبكات الاتصال الإلكترونية، وذلك عبر الاعتماد على وسائل الدفع الإلكتروني.

وكما هو الحال مع بروز أي ظاهرة جديدة في المجال التكنولوجي، نجد هناك تطورًا في الوسائل الإلكترونية وشبكات التحويل الإلكتروني للأموال؛ ما أدى إلى ظهور نوع جديد من الجرائم الرقمية المرتبطة بالقرصنة الرقمية للبطاقة المصرفية والمعاملات المالية، وهذا يمثل تهديدًا مباشرًا لحاملي هذه البطاقات والجهات المُصْدِرة لها من جهة، وللاقتصاديات الوطنية والدولية من جهة أخرى.

ومن هنا، فإن هناك حاجة مُلحة لمعالجة هذا النشاط الإجرامي من خلال تجريم الاختراق الرقمي لأنظمة المعلومات، بالإضافة إلى إيلاء الاهتمام للتدابير الوقائية والزجرية ضد الجرائم الناجَمة عنها، مع التركيز أكثر على جريمة القرصنة الرقمية للبطاقة المصرفية.

أهمية البحث

تتجلى الأهمية العلمية لهذا البحث في استحضار الإطار العام للجرائم المتعلقة بالبطاقة المصرفية على مستوى القوانين الإجرائية والموضوعية للقانون المغربي. وتحديد الآليات القانونية والأمنية والتقنية المتَّبَعة لحماية البطاقات المصرفية من جريمة القرصنة الرقمية، وتقييم فاعليتها وكفايتها. والعمل على تقديم الحلول ورفع التوصيات الضرورية لمنْع وقوع هذا النوع المتطور من الجرائم المعلوماتية على وسائل الدفع الإلكتروني، خاصة بطاقات الائتمان، وذلك من خلال التقريب بين التشريعات المقارنة لتوسيع نطاق النقاش واستكشاف جوانب الموضوع المتعلقة بالبحث.

إشكالية البحث

بالرغم من الدور الإيجابي الذي تؤديه البطاقة المصرفية الإلكترونية كأحد أنظمة الوفاء الرقمي، فإن تعرضها للاختراق أو القرصنة الرقمية، أفرز إشكاليات جعلت من مسألة التعامل بها محط خوف وحيطة مِن طرف مستخدميها. وتتميز جريمة القرصنة الرقمية للبطاقة المصرفية بطبيعة خاصة أدت إلى تباين تطبيقاتها بين المحاكم نتيجة لتشتت وتنوع النصوص القانونية المتعلقة بالموضوع؛ حيث جعل هذا التنوع تطبيق وتشريع هذه الجرائم يواجه مجموعة من التحديات القانونية. ولذلك فالتحديات تشمل ليس فقط تحديد الإطار القانوني الزجري الذي يجب تطبيقه على هذه الجرائم، بل أيضًا الإجراءات اللازمة لتنفيذ القوانين المتعلقة بها.

وتؤدي البطاقة البنكية دورًا كبيرًا في تيسير التجارة الإلكترونية، وتطويق رواج الأوراق المالية، وتتبّع مسارات حركة الأخيرة، ودفع الاقتصاد الوطني نحو مصاف الاقتصاد الدولي المعتمِد على الحوكمة والشّفّافية، وأصبح من الضروري دراسة مسألة الحماية الجنائية للبطاقة البنكية ضد القرصنة الرقمية ومقتضياتها الزجرية. وعليه تتركز إشكالية هذا البحث حول جريمة القرصنة الرقمية للبطاقة المصرفية، وتحديد الإشكاليات الناجمة عن ذلك.

أهداف البحث

تهدف الدراسة إلى استعراض ومناقشة النصوص القانونية الموضوعية لمعالجة الغموض وسد الثغرات القانونية التي قد تسمح للجناة بالإفلات من العقاب، واقتراح وضع إستراتيجية شاملة ومتكاملة لمراقبة أمن تقنية المعلومات؛ نظراً لدور هذا الأخير في استقرار المعاملات الرقمية التجارية والمالية، وتطوير أنظمة أمنية حساسة لإثارة الانتباه إلى جرائم القرصنة الرقمية للبطاقة المصرفية، وكذلك التعرف على الممارسات الفضلى الدولية الرائدة في مجال زجْر ومكافحة جرائم القرصنة الرقمية.

الدراسات السابقة

تطرقت مجموعة من الدراسات لموضوع البحث من زوايا مختلفة، ومن بين هذه الدراسات دراسة بعنوان «الحماية الأمنية لأنظمة الدفع الإلكترونية» للباحث رواد ميلود صقر تناولت آليات الحماية الأمنية لمكافحة جرائم أنظمة الدفع الإلكترونية، ورصد الصعوبات التي قد تجابه أجهزة العدالة الجنائية في تحديد أنماط الحماية الأمنية الخاصة بهذه الأنظمة[1]. ودراسة بعنوان

1 صقر، رواد ميلود. (2020). الحماية الأمنية لأنظمة الدفع الإلكترونية. مجلة الحقوق، سلسلة المعارف القانونية والقضائية، م. 74.

«الحماية الجنائية للبطاقة البنكية» للباحث عبد الله محمد أحمام التي تناقش الحماية الجنائية للبطاقة البنكية، وأثر التشريع الجنائي المغربي عليها، واستجلاء الفراغات التنظيمية والتناقضات التشريعية في هذا السياق[2]. وركزت دراسة بعنوان «الحماية التقنية والجنائية للنظم المعلوماتية» للباحثين أمين أعزان وعبد السلام جاكيمي: البحث في الجوانب التقنية والجنائية للحماية في مجال النظم المعلوماتية[3].

وسلطت هذه الدراسات الضوء على جوانب متعددة من الموضوع، ولكنها لم تركز بشكل مباشر على جريمة القرصنة الرقمية للبطاقات المصرفية؛ ما يسمح باستخدام هذه الدراسات كمرجعية لفهْم السياق العام والتحديات المرتبطة بالموضوع المقترَح في البحث. وقد ركزت هذه الدراسات على وسائل الأمن التقني المستخدَمة في بيئة الكمبيوتر والإنترنت؛ لمواجهة مخاطر الإرهاب المعلوماتي والجريمة الرقمية؛ بُغية المُسَاهَمَة في التقليل من خطر الاختراق الإلكتروني بشكل متفاوِت؛ حيث عدت الدراسات مِن بين هذه الوسائل ما يلي:

- استخدام تطبيقات «الجدران النارية» التي تساعد في تصفية حركة المرور الواردة والصادرة مِن وإلى الشبكة.
- استخدام الشبكات الافتراضية الخاصة التي توفِّر بيئة آمِنة لتبادل البيانات بين المستخدمين.
- استخدام تقنية «المفتاح العام» لتشفير البيانات وتأمينها أثناء النقل عبر الشبكة.

وقد تناولت هذه الدراسات أيضًا الحماية التقنية والقانونية للنظم المعلوماتية، ولاسيما ما تطرق إليه الباحثان في الدراسة الأخيرة حوْل طبيعة المقاربة السياسية الجنائية في مجال وسائل الأداء والائتمان، وتحليل التوافق بين مصلحة النظام الاقتصادي العام وحماية الأطراف المتعاملة في النظام الاقتصادي.

وناقشت دراسة بعنوان «توجهات السياسة الجنائية في مجال وسائل الأداء والائتمان»[4]، تحليلًا للسياسة الجنائية المغربية في مجال وسائل الأداء والائتمان، خلال الفترة بين عام 2004 و2018 مركزةً على طبيعة المقاربة التي اعتمدتها السياسة الجنائية في هذا النطاق، مع التركيز على جانبَي التجريم والعقاب؛ ومدى توافق النصوص المغربية مع مصلحة النظام الاقتصادي العام، وما إذا كانت هذه التشريعات قادرة على حماية الأطراف المتعاملة في النظام الاقتصادي من التجاوزات والمخاطر المحتملة؛ و أهمية توافق السياسة الجنائية مع الواقع الاقتصادي والاجتماعي للمجتمع؛ وتحليل فاعلية التشريعات في تحقيق التوازن بين حماية المصلحة العامة وحماية حقوق الأفراد والمؤسسات في النظام الاقتصادي.

منهج وخطة البحث

تتطلب خصوصية موضوع «المواجَهة الجنائية للقرصنة الرقمية للبطاقة المصرفية وسبل الوقاية منها بالتشريع المغربي» مقاربة تقتضي الاعتماد على عدة مناهج؛ فقد تم استخدام المنهج الوصفي لبيان الاعتداءات التي تحدث على بطاقات الدفع المصرفية، وبالأخص من خلال قرصنتها رقميًّا، بشكل دقيق ومنهجي، وتوضيح كيفية وقوع هذه الاعتداءات والطرق التي يتم

2 أحمام، عبد الله محمد. (2014). الحماية الجنائية للبطاقة البنكية، دراسة مقارنة. دار أبي رقراق للطباعة والنشر، الرباط.

3 أعزان، أمين، وجاكيمي، عبد السلام. (2016). الحماية التقنية والجنائية للنظم المعلوماتية. المجلة المغربية للقانون الجنائي والعلوم الجنائية، م. 2016، ع. 3.

4 الرحالي، نور الدين. (2018). توجهات السياسة الجنائية في مجال وسائل الأداء والائتمان. الندوة العلمية السياسة الجنائية بالمغرب: الواقع والآفاق 2004-2018، الرباط، المطبعة الأمنية.

من خلالها استهداف البطاقات المصرفية واختراقها رقميًّا، إضافةً إلى تحليل الأساليب والتقنيات المستخدَمة في القرصنة الرقمية لبطاقات الدفع، بما في ذلك البرمجيات الخبيثة والاختراقات السحابية والاحتيال الإلكتروني، بهدف فهْم عمليات الهجوم، وتقديم رؤية شاملة لهذه الظاهرة الإجرامية.

كما استخدام المنهج الاستنباطي في دراسة الإطار العام للجرائم المرتبطة بالقرصنة الرقمية للبطاقة المصرفية، باعتبارها جُزْءًا من سياق أوسع يمكن أن يتضمن أشكالًا أخرى من الاعتداءات الإلكترونية. والمنهج التحليلي في دراسة التشريعات والقوانين المتعلقة بحماية البطاقات المصرفية من القرصنة الرقمية، والتعرف على الجوانب القانونية المتعلقة بتلك الجرائم، علاوة على دراسة السياق التاريخي والاجتماعي لهذه الجرائم، وتحليل الأسباب والعوامل التي تؤدي إلى ارتكابها.

ومن خلال ذلك تم العمل على فهم الجوانب الأساسية لتلك الجرائم، وتحديد السياق القانوني والاجتماعي الذي يحيط بها؛ نظرًا لأهمية الحماية الجنائية للبطاقة البنكية في تشجيع الناس على التعامل بهذه الوسيلة بثقة، وتعزيز دور القطاع المصرفي في تقديم خدماته بشكل آمِن وسَلِس وسهْل للعملاء. وتستعرض الدراسة الموضوع بشكل مفصل من خلال مبحثين رئيسين، يناقش المبحث الأول المواجهة الجنائية الموضوعية للبطاقة المصرفية من القرصنة الرقمية، ويناقش المبحث الثاني سبل الوقاية من القرصنة الرقمية للبطاقة المصرفية.

2. المبحث الأول: المواجهة الجنائية الموضوعية للبطاقة المصرفية من القرصنة الرقمية

نظرًا لوقوع جريمة القرصنة الإلكترونية للبطاقة البنكية في بيئة يتم فيها معالجة آلية للمعطيات تكون فيها المعلومات محل الاعتداء عبارة عن نبضات إلكترونية، فإننا أمام ظاهرة إجرامية ذات طبيعة خاصة، وترتبط بما يعرف بقانون الجرائم المعلوماتية.

وعلى هذا فإن جريمة القرصنة الإلكترونية للبطاقة البنكية كصورة من صور الجريمة المعلوماتية وكغيرها من الظواهر الجنائية المستحدَثة تفرض تدخُّل الفقه، ومعه التشريع لتحديد مفهومي الجريمة المعلوماتية، وكذا القرصنة الرقمية (المطلب الأول)، مع تبيان التشريع الجنائي المقرر للحماية من القرصنة الإلكترونية للبطاقة البنكية كصورة من صور الجريمة المعلوماتية (المطلب الثاني).

2. 1. المطلب الأول: مفهومي الجريمة المعلوماتية والقرصنة الرقمية

2. 1. 1. الفرع الأول: مفهوم الجريمة المعلوماتية

تُعتبر الجريمة المعلوماتية من الظواهر التي أثارت إشكالاً جوهريًّا على مستوى المفهوم، فعند الرجوع إلى الآراء الفقهية التي ناقشت هذا الموضوع، نجد تقسيمًا متنوعًا، فبعضها ينظر إلى الجريمة المعلوماتية بصورة ضيّقة، وبعضها الآخَر ينظر إليها بشكل أوسع.

وقد عرّف أنصار التعريف الضيق الجريمة المعلوماتية على أنها سلوك غير مشروع أو غير مرخّص به يهم المعالجة الآلية للمعطيات أو إرسالها[5]، مشيرين إليها بأنها «تشمل فقط الجرائم

5 بن سليمان، عبد السلام. (2020). الإجرام المعلوماتي في التشريع المغربي: دراسة نقدية مقارنة في ضوء آراء الفقه وأحكام القضاء، ط. 2، دار الآفاق المغربية للنشر والتوزيع، الدار البيضاء، ص. 26.

التي تكون فيها المعلومات والبيانات والوثائق المضمنة والمخزّنة بالحاسوب، أو بالأنظمة المعلوماتية، أو البرامج التطبيقية، أو برامج التشغيل المتعلقة بها موضوعًا أو محلًا لها، وذلك سواء أكانت هذه المعطيات متاحة للجمهور أو سريّة يتطلب الأمر توفر شروط معينة لولوجها، وسواء كان مرتكبها مؤهلًا لهذا الولوج المشروع بتوفره على كلمات المرور مثلًا، أو كان يستعمل في ذلك أسلوبًا غير مشروع عن طريق الاختراق»[6].

وفي مقابل ذلك فإن أنصار التعريف الواسع للجريمة المعلوماتية حاولوا إحاطتها بتعاريف عديدة تعكس مقاربتها من زوايا مختلفة: فالدكتور سامي الشوا عرفها بكونها «كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية، ويهدف إلى الاعتداء على الأموال المادية أو المعنوية». بينما عرفها المهندس حسن طاهر داود بأنها «السلوك السيء المتعمد الذي يستخدم نظم المعلوميات لإتلاف المعلومات أو إساءة استخدامها، مما يتسبب إما في إلحاق الضرر بالضحية أو حصول الجاني على فوائد لا يستحقها»[7].

وفي نفس السياق أكد الفقيهان Michel et Credo أن سوء استخدام الحاسب أو جريمة الحاسب تسهل استخدام الحاسب كأداة لارتكاب الجريمة، بالإضافة إلى الحالات المتعلقة بالولوج غير المصرّح به لحاسب المجني عليه أو بياناته، كما تمتد لتشمل الاعتداءات المادية، سواء على جهاز الحاسب ذاته، أو المعدات المتصلة به، وكذلك الاستخدام غير المشروع لبطاقات الائتمان، وانتهاك «ماكينات» الحاسب الآلية، بما تتضمنه من شبكات تحويل الحسابات المالية بطرق إلكترونية، وتزييف المكونات المادية، أو المعنوية للحاسب، وتمتد أيضًا لتشمل سرقة جهاز الحاسب أو مكوناته[8].

وقد تبنى مؤتمر الأمم المتحدة العاشر لـ «منْع الجريمة ومعاقبة المجرمين»[9] تعريفًا جامعًا لجرائم الحاسب الآلي وشبكاته، حيث عرَّف الجريمة المعلوماتية بأنها: «أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية»[10].

ويعد هذا التعريف من أفضل التعريفات التي تناولت ظاهرة الإجرام المعلوماتي، إذ إنها تشمل كلا الجانبين المادي والمعنوي للحاسب الآلي، ومنها شبكة الإنترنت، وكذلك فإنه لا يقتصر على مجرد كون الحاسب الآلي وشبكاته محلًا للاعتداء، بل أيضًا بوصفه وسيلة للاعتداء وارتكاب الجرائم [11].

2. 1. 2. الفرع الثاني. مفهوم القرصنة الرقمية

تُعتبر القرصنة الرقمية نوعًا من الممارسات غير المشروعة التي تهدف إلى التحايل على نظام المعالجة الآلية للبيانات؛ بهدف إتلاف المستندات المعالَجة إلكترونيًّا. ويتم ذلك عادةً عن طريق استخدام برامج الكمبيوتر الجاهزة والتقنيات «الهكْرية». وتختلف أسباب القرصنة الرقمية أو

6 فالي، علال. (2013). خصوصيات الجريمة المعلوماتية على ضوء التشريع والقضاء المغربي. مجلة القضاء التجاري، ع. 2، الرباط، ص. 4.

7 بلمحجوب، إدريس. (2014). تأثير الجريمة الإلكترونية على الائتمان المالي. سلسلة ندوات محكمة الاستئناف ندوة خاصة بمناسبة الذكرى المئوية، مطبعة الأمنية، الرباط، ص. 28.

8 هلالي، عبد الإله أحمد. (2000). التزام الشاهد بالإعلام في الجرائم المعلوماتية: دراسة مقارنة، دار النهضة العربية، القاهرة، ص. 14.

9 مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين. (10 - 17 أبريل، 2000). الجريمة والعدالة: مواجهة تحديات القرن الحادي والعشرين. فيينا.

10 بنسليمان، عبد السلام. (2020). مرجع سابق، ص. 27.

11 الشوابكة، محمد أمين. (2007). جرائم الحاسوب والإنترنت: الجريمة المعلوماتية. دار الثقافة للنشر والتوزيع، عمّان، الأردن، ص. 9-10.

الإلكترونية من حالة إلى أخرى، حيث يُمكِن أن تكون بغرض تدمير أو تعطيل الأنظمة الحاسوبية، أو لتحقيق مكاسب مالية شخصية. وعلى سبيل المثال، قد يستخدم القراصنة تقنيات الاختراق الإلكتروني بُغْيَة سرقة معلومات شخصية أو بطاقات ائتمان، أو لتحويل الأموال مِن حسابات بنكية مختلفة إلى حساباتهم الخاصة أو حسابات أخرى.

ولقد أضْحت عمليات القرصنة والسرقة، وتزوير بطائق الائتمان البنكية من أسهل العمليات وأكثرها انتشارًا في الوقت الراهن، والشكاوى التي تقدمها البنوك ومؤسسات القروض والشركات بهذا الشأن دليل على خطورة الأمر، ولاسيما في ظل انتشار عمليات الشراء والبيْع عبر الإنترنت بواسطة هذه البطاقات التي أصبحت الوِجْهَة المُفَضَّلة لدى مُستعمِلي الشبكات[12].

وعلى الرغم من التقنيات الأمنية المعقَّدة التي تستخدِمها البرامج والأنظمة للحفاظ على أمان البيانات والمعلومات، فإن إمكانية الاختراق الإلكتروني لهذه البرامج ليست أمرًا صعب المنال بالنسبة للقراصنة ذوي الخبرة العالية في هذا المجال. وعليه رغم جهود الحماية والتشفير، فإن وجود ثغرات أمنية في البرمجيات، أو في الشبكات يمكن أن يسمح للمهاجمين بالوصول إلى الأنظمة والبيانات.

وبغض النظر عن الصور المتعددة للقرصنة، ومجالاتها المتنوعة[13]، فإن ما يهمنا في هذا الصدد هو القرصنة الإلكترونية للبطاقة البنكية، والكيفية التي تتم بها. وفي هذا الإطار، تمثِّل القرصنة الإلكترونية سرقة المعلومات المُضَمَّنة بالبطائق البنكية، ولاسيما منها تلك المعلومات غير الظاهرة، وأساسًا الأرقام السرية الخاصة بتلك البطاقات، والتوقيع الإلكتروني الخاص بأصحابها الذي يتكون في الغالب من أربعة أرقام سرية.

أمّا عن الطرق التي تُستعمَل في ذلك، فتتم بالاستعانة ببعض الآليات التقنية، حيث يقوم الرأس المدبِّر للعملية بالبحث عن شركاء التنفيذ. وهم المُستخدمون بالمؤسسات التجارية والسياحية التي تَستقطِب زبائن من الشريحة الاجتماعية الراقية الذين يؤدّون مشترياتهم، وما يحصلون عليه من خدمات بواسطة بطاقاتهم البنكية.

وغالبًا ما يتم تسليمهم بعض الآليات التكنولوجية التي تستعمل في قراءة محتويات البطاقات البنكية، وتسجيلها تحْت إغراء مادي لهؤلاء المستخدمين مِن أجل تمرير كل بطاقة بنكية داخل تلك الآلة لبضع ثوانٍ، بعد ذلك تسلّم هذه الآلات إلى خبير في المعلومات الذي يربطها بالحاسوب ليطّلع على عدد العمليات التي قام بها المستخدم، وجمع المعلومات المتعلقة بها، ثم تنسخ هذه المعلومات على بطاقات بنكية بيضاء، يتم صنعها بواسطة أجهزة معدة لهذه الغاية، ويطبع اسم الفاعِل/ المُقَرْصِن على ظهرها أو أسماء مستعارة، وتنسخ البطاقة المقرصَنة إلى عدة نظائر. وبواسطتها يتمكن الجناة من تسديد مبالغ الفواتير المتعلِّقة بجميع الخدمات المقدَّمة لهُم مِن طرف المؤسسات التجارية، أو السياحية داخل التراب الوطني أو الدولي، وسحْب مبالغ مالية من أرصدة الضحايا[14]. هذه الطريقة في القرصنة الإلكترونية للبطائق البنكية هي ما يصطلح عليها Skimming.

12 الجرائم البنكية. (16 مايو، 2013). مجلة القانون والأعمال الدولية، جامعة الحسن الأول، تم الاطلاع بتاريخ 01 مارس 2024 من https://l1nq.com/PqmPD.

13 هناك صور متعددة من القرصنة، كقرصنة البرامج المعلوماتية، وقرصنة المعطيات التي تنظمها تلك البرامج، وقرصنة الأفلام والشرائط الموسيقية...انظر فرام، كوثر. (2007-2009). الجريمة المعلوماتية على ضوء العمل القضائي المغربي، بحث نهاية التدريب في المعهد العالي للقضاء، المغرب، ص. 28.

14 أحمام، عبد الله محمد. (2014). مرجع سابق، ص. 31.

كما يمكن أن تتم عملية القرصنة الإلكترونية للبطاقة البنكية عن طريق سرقة البطاقة وقراءة المعلومات التي تتضمنها ذاكرتها المغناطيسية بواسطة أجهزة وآلات للقراءة، ونقل هذه المعلومات وطبْعها في بطاقات بيضاء فارغة بواسطة آلات وأجهزة للكتابة والطبْع. وهي أجهزة متواجِدة بوفرة في الأسواق. وبعد ذلك توزَّع هذه البطاقات على أكبر عدد مِن الجناة الذين يقومون بسحب جماعي للأموال من مختلف الشبابيك الإلكترونية في نفس فروع البنك وفي نفس التوقيت. وهناك طرق أخرى يصعب حصرها كأن يقوم الأشخاص المولعون بالإعلاميات بحل نظام الرقم السري عبر تقنية «الديكوداج» (فَكّ الرّمز). ويعتمد بعض المحترِفين على نشْر الأرقام السرية لبطائقهم على مواقع إلكترونية بعْد إجرائهم عمليات شراء كبيرة مِن شركة معيَّنة، بُغْيَة التحايل عليها بدعوى أن بطائقهم البنكية قد تم تعرضها للقرصنة الإلكترونية وأنَّهُم لَمْ يقوموا بأية عمليات شراء أو اقتناء من الشركات المذكورة، وأنهم كانوا ضحايا قرصنة إلكترونية، مطالبين باسترداد المال بدعوى أنَّ السلع قدْ توصَّلت بها جهات وعناوين أخرى[15].

وتجْدر الإشارة إلى أنه بالإضافة إلى الصورة التقليدية للقرصنة التي تتم مباشرة من الشبابيك الآلية البنكية يوجد نوعٌ ثانٍ يتم عبْر الروابط الإلكترونية، والتي من خلالها يقوم المُقرصِن بصناعة واجهة لموقع وهْمي، وانطلاقًا منه، يبعث رسائل نصية شبيهة بتلك التي اعتاد الضحايا التوصل بها من وكالاتهم المالية يلزمهم من خلالها بتأكيد معلوماتهم؛ مما يدفعهم لِمَلْءِ بياناتهم الشخصية الخاصة ببطائقهم البنكية بما فيها الرمز السري ليتوصل بها المجْرِم ويقوم بتنزيلها بتطبيقات خاصة بالهاتف النقال، ويستعملها لأداء الخدمات والمشتريات لدى التجار المتوفرين على أجهزة الدفع الإلكتروني TPE وذلك دون الحاجة إلى إبراز البطاقة البنكية، بل فقط وضع الهاتِف النقّال فوق هذا الجهاز لتتم القراءة المسْحية، ومِن ثَمَّ اقتطاع ثمنها مباشرة من حساب صاحبها الأصلي.

ويلاحَظ مِن خلال الإشارة إلى أهم التقنيات المستخدَمة في مجال جرائم البطائق البنكية، أن المشرِّع الفرنسي كان له السبْق التشريعي في التطرق إلى هذه الأنواع المستعمَلة في الجرائم الالكترونية، حيث أوْجَد لها تنظيمًا تشريعيًّا خاصًّا يعرف بقانون GodFran الصادر بتاريخ 5 يناير 1988م المنظِّم للتعريف بالاحتيال الإلكتروني، والذي يُعتبَر مِن القوانين التي تدخَّلَت مبكِّرًا في هذا المجال مِن أجْل مكافَحة الجرائم الحديثة الخاصة بالمعلوميات؛ مثل: الفيروسات والقنابل المعلوماتية Bombe logique، كما يعاقب على الجرائم المسماة حصان طروادة، وبرامج التجسس التي من شأنها ملاحظة موقع ما، أو شبكة معلومات خاصة. بالإضافة إلى ذلك كله، فهو يعاقب منتِجي البرامج التي تسهل للقراصنة ارتكاب جرائمهم؛ مثل: الجرائم المتعلقة باستخدام أرقام البطاقات البنكية باعتبارهم شركاء في الجريمة عن طريق إمداد الجناة بالوسائل المستخدَمة في ارتكاب الجريمة[16].

2. 2. المطلب الثاني: التشريع الجنائي المعلوماتي المقرر للحماية من القرصنة الإلكترونية للبطاقة البنكية

يتعلق الأمر في هذا المطلب بالحالة التي تكون فيها شبكة الإنترنت أداة سلبية لارتكاب الجريمة؛ أي محلًّا لها، إذْ يكون هدف المجْرِم البيانات والمعلومات المخزَّنة والمنقولة عبْر هذه الشبكة[17].

15 الجرائم البنكية، (16 مايو, 2013). مرجع سابق.
16 أحمام، عبد الله محمد. (2014). مرجع سابق، ص. 32.
17 لامية، طالة. وكهينة، سلام. (2020). الجريمة الإلكترونية: بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل

ونعني بها تلك الجرائم التي تنال بالاعتداء أو تهدِّد بالخطر الحقوق ذات الطابَع المالي، حيث يدخل في نطاق هذه الجرائم الحقوق ذات الأصول المالية كجريمة إساءة الائتمان، وإتلاف النظُم، ثم جرائم التلاعُب في التجارة الإلكترونية[18].

وإذا كانت جرائم الأموال المعلوماتية متعددة، فإننا سنقتصر على تحليل جريمة القرصنة الإلكترونية للبطاقة البنكية مِن خلال التطرق لبعض جرائم القرصنة الإلكترونية للبطاقة البنكية كصورة من صور القرصنة الرقمية. وأمام الزيادة الملحوظة في مختلف جرائم تكنولوجيا المعلومات، شعر المشرِّع المغربي، على غرار باقي التشريعات، بالحاجة الملحة إلى حماية الأنظمة المعلوماتية ومكوناتها، بهدف الحد من الجرائم التي ترتكب ضدها أو باستخدامها.

وفي هذا الصدد، تم إصدار القانون المتعلق بالإرهاب الذي وردت فيه إمكانيّة ارتكاب أفعال إجراميّة إرهابيّة عن طريق نظم المعالجة الآليّة للمعطيات، إلا أن القانون الجنائي لم ينص على مقتضيات قانونيّة تخصّ الجرائم المتعلقة بالنظم الآليّة للمعطيات، الشيء الذي دفع بالمشرع إلى تبني قانون 07-03 المتمم لمجموعة القانون الجنائي[19]. ويمكن حصر الجرائم الماسّة بالنظم الآليّة للمعطيات في فئتين: الجرائم التي تستهدف المسّ بسلامة وسريّة نظُم المعالجة الآليّة للمعطيات، والجرائم التي تستهدف المعطيات والوثائق المعلوماتية.

2. 2. 1. الفرع الأول: الجرائم التي تستهدف المس بسلامة وسرية نظم المعالجة الآلية للمعطيات

يتجلّى الاعتداء على نظام المعالجة الآليّة المعطيات[20] في الصور الآتية: الدخول أو البقاء غير المشروع في النظام، أو عرقلة سير النظام، أو إحداث خلل فيه، أو الإعداد لارتكاب المسّ بالنظام. وبخصوص الاعتداء المعلوماتي بالدخول، أو البقاء غير المشروع، فقدْ جرّمه المشرِّع في الفصل 3-607 الذي نصّ على ما يلي: «يعاقب بالحبس من شهر إلى ثلاثة أشهر وبالغرامة من 2.000 إلى 10.000 درهم أو بإحدى هاتين العقوبتين فقط كل من دخل إلى مجموع أو بعض نظام للمعالجة الآلية للمعطيات عن طريق الاحتيال. ويعاقب بنفس العقوبة من بقي في نظام للمعالجة الآلية للمعطيات، أو في جزء منه، كان قد دخله عن طريق الخطأ، وهو غير مخول له حق دخوله. تضاعَف العقوبة إذا نتج عن ذلك حذف، أو تغيير المعطيات المدرجة في نظام للمعالجة الآلية للمعطيات أو اضطراب في سيره».

يتضح من هذا النص القانوني أن جريمة الدخول أو البقاء في النظام لا تقوم إذا كان الولوج متاحًا للعموم، بمعنى أنها لا تنطبق على المواقع المخصصة للاستخدام العام. بل تنطبق هذه الجريمة في حالة الولوج إلى أنظمة معلوماتية حيث يُمنع التواجد فيها، كما هو الحال مع العمال الذين يتجاوزون اختصاصهم، ويدخلون إلى أجزاء من النظام المعلوماتي التي ليست لهم صلاحية التواجد فيها[21].

كما تقع الجريمة سواء تم الدخول إلى النظام كله أو جزء منه فقط، كالدخول لبعض عناصر النظام، أو عنصر واحد منه، أو في الحالة التي يسمح فيها للجاني بالدخول إلى جزء من النظام؛

الاجتماعي. مجلة الرواق للدراسات الاجتماعية والإنسانية، م. 6، ع. 2، ص. 71.

18 بلميلود، سارة. والسائح، إيمان. (2015). الحماية القانونية لمستهلكي تكنولوجيا المعلومات. مجلة المنبر القانوني، ع. 9.

19 ظهير شريف رقم 1- 03- 197 صادر في 16 من رمضان 1424 (11 نوفمبر 2003) بتنفيذ القانون رقم 03- 07، بتنفيذ القانون 03- 07 بتتميم مجموعة القانون الجنائي فيما يتعلق بالجرائم المتعلقة بنظم المعالجة الآلية للمعطيات.

20 ظهير شريف رقم -1 -20 100 صادر في 16 جمادى الأولى 1442 (31 ديسمبر 2020) بتنفيذ القانون رقم -20 43 المتعلق بخدمات الثقة بشأن المعاملات الإلكترونية.

21 بنسليمان، عبد السلام. (2020). مرجع سابق، ص. 73.

فينتهز الفرصة ويدخل إلى جزء آخَر غير مسموح له الدخول إليه، شرْط أن يكون العنصر الذي تم الولوج إليه يدخل في برنامج متكامل قابل للتشغيل[22].

ويُقصد بفعل البقاء في النظام أو جزء منه، التواجد داخل نظام المعالَجة الآلية للمعطيات دون إرادة صاحب النظام أو المخول له السيطرة عليه. ويمكن أن يحدث البقاء غير المشروع بصور مختلفة، مثل: الدخول العرَضي إلى النظام، أو عن طريق الخطأ أو السهو. وفي هذه الحالات، قد يكون الشخص غير ملتزم بالانسحاب أو الخروج من النظام بعد فترة معينة، ما يعتبر فعلًا معاقبًا عليه قانونيًّا[23].

أما بخصوص عرقلة سير نظام المعالجة أو إحداث خلل فيه، فيتمثل الركن المادي لهذه الجريمة في فِعْل التعطيل الذي يندرج ضمن إعاقة النظام أيًّا كانت الوسيلة المستخدَمة في ذلك، فقد تكون بطريقة مادية كأعمال العنف على أجهزة الحاسوب وشبكة الإنترنت، وقد تكون بطريقة معنوية عندما تقع على الكيانات المنطقية للنظام مِثْل البرامج والمعطيات[24].

وتتجلى الصورة الرابعة للاعتداء على النظم الآلية للمعطيات في الإعداد لارتكاب المسّ بالنظم من خلال صنع تجهيزات، أو أدوات أو إعداد برامج للمعلوماتيات، أو أية معطيات أعِدَّت أو اعتُمِدت خصّيصًا لارتكاب جرائم سير نظُم المعالَجة أو تملُّكها أو حيازتها، أو التخلي عنها للغير أو عرْضها أو وضْعها رهْن إشارة الغير[25].

2. 2. 2. الفرع الثاني: الجرائم التي تستهدف المعطيات والوثائق المعلوماتية

إضافة إلى الاعتداءات التي تؤثر على سلامة أنظمة المعالجة الآلية للمعطيات، هناك أنواع أخرى من الاعتداءات التي يمكن أن تكون مدمِّرة أو مُؤْذِية أيضًا، ويشمل ذلك:

إدخال معطيات جديدة: عملية إدخال معلومات غير صحيحة أو مُضَلِّلة إلى النظام، مما يؤثر على دقة البيانات ويضرّ بمصداقيتها.

الإتلاف أو الحذف أو التغيير: عمليات التلاعب بالبيانات الموجودة في النظام بشكل غير مشروع، سواء عن طريق الحذف العشوائي أو التغيير السلبي، مما يمكن أن يتسبب في فقدان البيانات أو تشويهها.

التزوير أو التزييف: عمليات تعديل الوثائق المعلوماتية بطريقة غير قانونيّة، سواء بتزوير الوثائق أو التزييف، مما يؤثر على صحة ومصداقيّة البيانات.

وتُشكِّل جميع هذه الأنواع من الاعتداءات تهديدًا خطيرًا على أمن المعلومات والخصوصيّة، وتستوجب اتخاذ إجراءات قانونيّة وتقنيّة للوقاية منها ومعاقبة المتسبِّبين فيها.

---

22 قورة، نائلة عادل. (2005). جرائم الحاسب الآلي الاقتصادية: دراسة نظرية وتطبيقية. منشورات الحلبي الحقوقية، ط. 1، بيروت، ص. 315.

23 زيدان، ربيحة. (2011). الجريمة المعلوماتية في التشريع الجزائري والدولي. دار الهدى للطباعة والنشر والتوزيع عين مليلة، الجزائر، ص. 50-51.

24 درامي، محمد. (2010/2009). الحماية الجنائية للبيانات المعلوماتية، رسالة لنيل دبلوم الماستر في القانون الخاص، وحدة القانون المدني، كلية الحقوق الدار البيضاء، ص. 85.

25 ينص الفصل 10-607 من القانون 03-07 على ما يلي: «يعاقب بالحبس من سنتين إلى خمس سنوات وبالغرامة من 50.000 إلى 2.000.000 درهم كل من صنع تجهيزات أو أدوات أو أعد برامج للمعلوماتيات أو أية معطيات أعدت أو اعتمدت خصيصًا لأجل ارتكاب الجرائم المعاقب عليها في هذا الباب أو تملكها أو حازها أو تخلى عنها للغير أو عرضها أو وضعها رهن إشارة الغير».

ونجد أن المشرِّع المغربي فيما يتعلق بالاحتيال أو الغش المعلوماتي قد عاقب بموجب الفصل 607-6 من القانون الجنائي «بالحبْس مِن سنة إلى ثلاث سنوات، وبالغرامة من 10.000 إلى 200.000 درهم، أو بإحدى هاتين العقوبتين كل مَن أدْخَل معطيات في نظام للمعالجة الآلية للمعطيات أو أتْلَفها أو حذَفَها منه أو غيَّر المعطيات المُدْرَجة فيه، أو غيَّر طريقة معالجتها أو طريقة إرسالها عن طريق الاحتيال».

ويتبين من خلال هذا الفصل أن المشرع المغربي يعاقب على الاحتيال أو الغش المعلوماتي بصرامة وحزم، حيث يتضمن الفصل 607-6 من القانون الجنائي عقوبة الحبس والغرامة لمن يقوم بأفعال تشمل إدخال المعطيات في نظام معالجة البيانات أو تدميرها أو تغييرها بطريقة غير قانونية عن طريق الاحتيال. وهذا يعكس التزام السلطات بمكافحة الجرائم الإلكترونية وحماية البيانات والأمن المعلوماتي في البلاد. ويتكون الركن المادي لهذه الجريمة من الأفعال الآتية: إدخال المعطيات (l'intrusion)، الإتلاف (détruire)، الحذف (l'effacement)، والتغيير (Modification) [26،27].

وتُعتبَر جريمة التلاعب في المعطيات جريمة عمدية تتطلب وجود إرادة متعمدة من الجاني للقيام بعمليات مثل الإدخال غير القانوني للبيانات، أو الإتلاف والحذف، أو التغيير في البيانات الموجودة. كما يجب أن يكون الجاني على عِلْم بأنه يقوم بالتلاعب بالمعطيات، وأنه ينتهك القانون بهذا الشكل.

أما فيما يتعلق بجريمة تزوير الوثائق المعلوماتية، فإنها تُعَدُّ مِن أخطر صور التزوير؛ لكونه يمس بالثقة الواجبة في الوثائق والمحرَّرات المعلوماتية، حيث مِن شأن هذا الفِعْل إحداث أضرار مادية أو معنوية متنوعة، يمكن أن تمسّ بالأفراد، أو بالمؤسسات الخاصة والعامة، وقد تم التنصيص على هذه الأفعال بمقتضى الفصل 7-607 من القانون الجنائي الذي جَرَّم كلًّا من التزوير أو التزييف في وثائق المعلوميات أيًّا كان شكلها إذا كان مِن شأن ذلك إلْحاق ضرر بالغير، وكذا استعمال تلك الوثائق المزوَّرة أو المزيَّفة مع العلم بذلك[28].

وقد ذهبت بعض القرارات الصادرة عن محكمة الاستئناف بالرباط إلى اعتبار القرصنة الإلكترونية للبطائق البنكية مِن قِبَل مجموعة من الأشخاص بمثابة تزوير في وثائق المعلومات. ومن هذه القرارات، قرار عدد 299 الذي جاء فيه: «حيث إن الأفعال التي اقترفها المتَّهَم (أ. ز.) المتمثلة في اتفاقه مع المسميين (م. ت.) و(ع. ه.) على سرقة الأشخاص؛ وذلك عن طريق قرصنة بطائق بنكية وطبْعها في اسم مستعار، وتزوير وثيقة هوية، وتوفره على بطاقة وطنية فرنسية في اسم (س. ك.) تحمل صورته واستعماله 23 مرة لبطاقة بنكية مزوَّرة ،كلها تشكل من حيث الوصف القانوني للتجريم جرائم السرقة الموصوفة والمشارَكة في تزوير بطائق الائتمان؛ ما تكون معه العناصر التكوينية لهذه الجرائم ثابتة في حقه، ويتعيَّن بالتالي التصريح بمؤاخذَته»[29] .

تكشف هذه الحيثية عن جرأة المتهم في ارتكاب سلسلة من الجرائم بشكل منظم ومنسق، ما يبرز خطورة تلك الأفعال على المجتمع والأفراد. ويظهر القرار كذلك جرأة القضاء في مواجهة

26 أي إزالة المعطيات من النظام، إما عن طريق تخريب الدعامة التي تحمي المعطيات، أو نقل البيانات من مكانها إلى مكان آخر داخل نفس النظام أو إلى نظام آخر، مما يؤدي إلى عرقلة وظيفته.

27 ويعني استبدال معطيات بمعطيات أخرى، أو تغيير الطريقة التي تعالج بها أو طريقة إرسالها، والنتيجة هي إحداث عبث بالنظام، والذي من شأنه أن يحول دون أدائه وظيفته، أو دون بقائه على الحالة التي كان عليها في السابق. انظر بنسليمان، عبد السلام، (2020)، مرجع سابق، صفحات متفرقة 89 - 92.

28 درامي، محمد. (2009- 2010)، مرجع سابق، ص. 88.

29 قرار صادر عن محكمة الاستئناف بالرباط، عدد 299، بتاريخ 23-3-2006، ملف عدد 22/05/736.

الجرائم الإلكترونيّة والتصدي للأنشطة غير القانونيّة التي تهدد الأمان المالي والشخصي للأفراد. ويعكس هذا التعليق دور القانون في حماية المجتمع وتطبيق العدالة بحزم على الجرائم الإلكترونيّة.

وفي قرار آخَر تحت عدد 633 اعتبرت ما يلي:» حيث ثبَتَ للمحْكَمة أن المتهَم كان يعلم أن البطائق البنكية التي تسلّمَها مِن المتهَم (ح. ك.) مزيَّفة، وأنه ولج الشبابيك الأوتوماتيكية البنكية، واستعملها في سحْب المبالغ المالية لفائدته ولفائدة غيره دون وجه حق ... وحيث ثبت للمحكمة أن الأفعال المنسوبة إلى المتهَم توصف بجريمة استعمال وثائق المعلوميات (بطاقة بنكية) وهو يعلم أنها مزيَّفة حسب الفقرة الثانية من الفصل 607-7 «[30].

يوضح هذا القرار أن المتهم كان على علم بأن البطاقات البنكية التي حصل عليها مزورة، ومع ذلك، قام بإدخالها في أجهزة الصراف الآلي، واستخدامها لسحب الأموال لصالحه، ولصالح آخرين بطريقة غير قانونية. حيث يؤكد القرار أن هذه الأفعال تشكل جريمة استخدام وثائق معلوماتية (البطاقة البنكية) مع علمه بأنها مزورة، وفقًا للفقرة الثانية من الفصل 607-7 من القانون الجنائي.

3. المبحث الثاني: سبل الوقاية من القرصنة الإلكترونية للبطاقة البنكية

كثرت في السنوات الأخيرة فرص السطو الإلكتروني على البطائق البنكية لاتصال هذا النوع من الوفاء بشبكة الإنترنت التي تعد مكانًا مفتوحًا لكل الناس بلا حدود، أو قيود. لذا بات من الضروري التفكير الجِدّي في الإجراءات الدفاعية لحماية هذه الوسيلة (المطلب الثاني). والتي من الأجدر أن تسبقها إجراءات وقائية من شأنها الحيلولة دون المساس بهذه الوسيلة من الأساس (المطلب الأول).

3. 1. المطلب الأول: التدابير الوقائية المتخذة لحماية البطاقة البنكية من القرصنة الإلكترونية

حتى يتم التغلب على مخاطر الوفاء الإلكتروني بواسطة البطاقة البنكية لابد من إيجاد مجموعة من الحلول الإدارية والتقنية كآليات للوقاية من قرصنة البطاقة البنكية.

3. 1. 1. الفرع الأول: دور البنوك في مجال الوقاية من جريمة القرصنة الإلكترونية للبطاقة البنكية

لكي تستطيع البنوك ضمان وحِفْظ حقوق المستهلِك الإلكتروني في إطار الخدْمة المصرفية التي يحصل عليها، لابد من توافُر عدد مِن الآليات الإدارية التي يجب الحرص على إعمالها داخل المؤسسات البنكية والتي من شأنها تحقيق نوع من الوقاية ضد الجرائم المعلوماتية الواقعة على وسائل الدفع الإلكتروني، وبالخصوص البطاقة البنكية.

ويمكن حصر هذه الآليات فيما يلي:

- تدريب موظفي البنوك على اكتشاف الوسائل الاحتيالية والتعامل معها بحسْم، وأن يكون هذا التدريب أساسيًّا للعاملين قبْل السماح لهم باستخدام الشبكة المعلوماتية للمؤسَّسة البنكية، وجعله تكوينًا مستمرًا يستوعب أحدث التقنيات التكنولوجية.
- دعْم أساليب الرقابة الداخلية على البيانات.

اتّباع سياسات وإجراءات، تُحَقِّق تأمين الاتصالات مِن وإلى النظم لمنْع أو الحدّ مِن اختراق غير المرخَّص لهُم[31].

30 قرار عدد 633، بتاريخ 26-06-2006، ملف عدد22/05/461، ص. 11-12. انظر فرام، كوثر. (2007- 2009). مرجع سابق، ص. 12.

31 انظر القانون رقم 43.05 المتعلق بمكافحة غسل الأموال الصادر بتنفيذه ظهير شريف رقم 1.07.79 بتاريخ 28

- وجود نظام دقيق للمراجَعة الفورية لحركات اليوم التي تمت على مستوى النظام المعلوماتي قبْل الإقفال، لاكتشاف الأخطاء في وقت مبكِّر، ومعالجتها في الحين، والحرص ما أمكن على ما يسمى برقابة الجهاز نفسه، ويُقصَد به إجراءات الرقابة التي يقوم بها الجهاز مِن تلقاء نفسه لاكتشاف الأخطاء.

- الفصل الوظيفي للمسؤوليات، وعدم السماح بقيام شخص واحد بتنفيذ العملية بالكامل، ومنح كل مستخدم مرخَّص له بالدخول إلى قاعدة البيانات أرقامًا سرية خاصة به واستمرار تعديلها على فترات دورية[32].

تؤدي البنوك دورًا حيويًّا في الوقاية من جرائم الاختراق الإلكتروني للبطائق البنكية، من خلال تبني إستراتيجيات مُسبقة للحماية مِن عمليات التجسس على برامجها الإلكترونية. وتشمل هذه الإستراتيجيات وضع قواعد أَمنية صارمة، وتطوير التقنيات لمكافَحة الاختراقات الإلكترونية، إضافة إلى تعزيز التوعية الأَمْنية للموظفين والعملاء وتكثيف التعاون مع السلطات الأمنية المختَصَّة.

ومن مظاهر الدور الوقائي للبنوك في مجال المحافَظة على سرية وأمان البيانات والمعلومات الخاصة بأصحاب البطائق البنكية، إحداث ضمانة فنية تمكن من تحديد الفعل المُجَرَّم، ومَن قام به، سواء أكان شخصًا طبيعيًّا أو معنويًّا، وذلك بتزويد الحاسب الآلي ببرنامج رقابي يستطيع أن يكشف الفعل، ويتيح بالتالي لفرَق البحث والتحري الوسائل الكفيلة بتتبُّع مرتكِبي الجرائم ومُلاحَقَتهم[33].

3. 1. 2. الفرع الثاني: الآليات التقنية لحماية البطاقة البنكية من القرصنة المعلوماتية

بهدف تأمين معامَلات مستعمِلي شبكة الإنترنت هناك مجموعة من التطبيقات التي يقوم بها مُرسِل أو مستعمِل شبكات الاتصال لتنفيذ عملية مالية بواسطة إلكترونية، وهي كالتالي:

أولًا - تطبيقات الجدران النارية

يُقصَد بتطبيقات الجدران النارية تأمين خطوط الدفاع الأمامية باعتبارها تقنية تقوم على تأمين المنافذ التي تحصل من خلال التطبيقات على خدمات الشبكة العنكبوتية، وتشتغل كمصفاة تمنع وصول الطلبات المشبوهة إلى الأجهزة.

وتنقسم الجدران النارية إلى صِنْفَيْن:

- الجدران النارية المؤسَّسية التي تقوم بحماية تطبيقات المؤسسات على مستوى الأجهزة المزودة.

- الجدران النارية الشخصية التي تستعمل خصوصًا في الجيل الحديث المُعتمِد على الاستخدام المتنقل للشبكة، وكذا العمل المنزلي، وهي جدران تحظى بأهمية خاصة[34].

ثانيًا - الرقم السري

يُعتبَر الرقم / الْقِنّ السري واحدًا مِن أهم الإجراءات الأمنية المستخدَمة في البيئة الرقمية، حيث يُمكن لهذا الرقم التحقُّق من هوية المستخدِم الذي يحاول الدخول إلى العناوين الإلكترونية.

من ربيع الأول 1428 (17 إبريل، 2007)، الجريدة الرسمية عدد 5522 بتاريخ 15 ربيع الثاني 1424 (3 مايو، 2007)، ص. 1359.

32 حسن، هشام فتحي سيد. (2003). وسائل حماية المستهلك الإلكتروني بين الشريعة والقانون. مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، 12 أكتوبر، 2003، غرفة تجارة وصناعة دبي، م. 3، ص. 1200.

33 أحمام، عبد الله محمد. (2020). مرجع سابق، ص. 87-88-90.

34 أعزان، أمين. وجاكيمي، عبد السلام. (2016). مرجع سابق، ص. 60.

ويُعتبَر استخدام كلمات المرور أحد أرخص الوسائل الأمنية أيضًا. ولضمان نجاح هذا النهج، يجب على مستخدمي البطاقات البنكية أن يكونوا مُدرِكين لأهمية حفْظ كلمات المرور الخاصة بهِم، وعدم مشاركتها مع أي شخص آخر. كما ينبغي عليهم تغيير كلمات المرور بانتظام، وتشفيرها عند تخزينها على الأجهزة الحاسوبية. علاوة على ذلك، يجب أن تُخفى حروف كلمات المرور عند إدخالها في النظام، لتجنب كشفها أمام أي متطفل[35].

كما تتَّبِع بعض الجهات أسلوب تخصيص كلمات المرور بواسطة الشبكة أو مسؤول أمن نظام، وذلك للحد من المحاولات البسيطة لتخمين كلمة المرور، والتي قد تكون اسم أحد أبناء المستخدم، أو تاريخ ميلاده مثلًا. ومن عيوب هذا الأسلوب أنه يمكن كسره بسهولة بواسطة برامج تقوم بجعل عدد لا نهائي من المحاولات حتى تتوصل إلى الكلمة الصحيحة[36].

ثالثًا - التوقيع الإلكتروني

تعددت مجالات استخدام التوقيع الالكتروني؛ وذلك لإبرام مختلف العقود والمعاملات البنكية، فمع ازدهار التجارة الإلكترونية ظهرت وسائل حديثة للدفع كالنقود الإلكترونية، البطاقة الذكية وبطاقة الائتمان، كل هذه الوسائل لا تتم إلا بالاعتماد على التوقيع الإلكتروني لإثبات صحتها.

وتحتوي جميع أنواع الدفع الإلكتروني على التوقيع الإلكتروني الذي بدأ استخدامه مع ظهور البطاقة الذكية المزوَّدة بذاكرة إلكترونية تحتوي على رقم سري والتي تشكِّل تطبيقًا عمليًّا لهذا التوقيع من خلال التعامل مع جهاز الصراف الآلي في إتمام عملية سحب النقود.

ويؤدي التوقيع الإلكتروني دورًا مهمًّا في تأمين مجال الدفع الإلكتروني عامةً والبطاقة البنكية خاصةً لما يمكن أن يعتري الأجهزة والنظم الإلكترونية المستخَدمة من خروقات، ولما يحققه من سريّة وخصوصيّة للمراسَلات والبيانات والاتصالات المستخدمة في العمليات التجارية، موفرًا التأمين في التعامل بواسطة البطاقة البنكية كوسيلة للدفع الإلكتروني بإعطائها هوية رقمية وحُجية في التعامل والإثبات.

رابعًا - تقنية المفتاح العام

تعتمِد تقنية المفتاح العام باعتبارها تقنية تشفير بيانات على استخدام مفتاحين مترابطين: مفتاح عام ومفتاح خاص. ويُعرف التشفير بأنه العملية التي تُغيِّر طبيعة البيانات باستخدام الرياضيات، مما يسمح بتخزين المعلومات السرية، أو إرسالها عبْر قنوات غير مُؤَمَّنَة مثل: الإنترنت دون أن يكون بإمكان أي شخص آخَر قراءتها أو تغييرها. ويُستخدم هذا النوع من التشفير بشكل خاص في حماية معلومات بطاقات الائتمان، حيث يسهم في تقليل احتمالية سرقة المعلومات الشخصية واستخدامها بطرق غير مشروعة بعد الاعتداء عليها[37] .

3. 2. المطلب الثاني: الآليات الحمائية للبطاقة البنكية من القرصنة المعلوماتية

نظرًا للدور الإيجابي الذي تؤديه أنظمة الدفع الإلكتروني عامةً والبطاقة البنكية خاصةً بات من الضروري إيجاد نظام قانوني متكامل على المستوى الموضوعي (الفرع الأول) أو الإجرائي (الفرع الثاني)؛ وذلك في سبيل تحقيق الحماية القانونية لها ولأطرافها من الجرائم الواقعة عليها.

35 خنفوسي، عبد العزيز. (2018). مدخل إلى قانون الدفع الإلكتروني. مركز الكتاب الأكاديمي، الأردن، ط.1، ص. 26.

36 داود، حسن طاهر. (2000). الحاسب وأمن المعلومات. معهد الإدارة العامة، مكتبة الملك فهد الوطنية، الرياض، ص. 310-311.

37 خنفوسي، عبد العزيز. (2018). مرجع سابق، ص. 32.

3. 2. 1. الفرع الأول: المقاربة القانونية لجريمة قرصنة البطاقة البنكية بين غياب دينامية النص وإشكالية التكييف

تظل المقتضيات القانونية جامدة، حتى إذا خرجت إلى حيز التطبيق العملي ظهرت نواقصها وعيوبها، ما يؤثر على توجه القضاء أثناء الفصل في المنازعات المتعلقة بمجال تدخل تلك النصوص[38]، وهو شأن الجريمة موضوع الدراسة، حيث إن التأخر في تصدي المشرِّع المغربي للجرائم المعلوماتية عمومًا انعكس على التوجه القضائي في تعامله معها والذي انقسم إلى اتجاهين، اتجاه سار في اعتماد القواعد التقليدية العامة كأساس للإدانة (أولًا) واتجاه آخَر ذهب إلى ضرورة إفراد قواعد جديدة تتماشى والطبيعة الخاصة لهذا النوع من الإجرام (ثانيًا).

أولًا - التكييف التقليدي لجريمة قرصنة البطاقة البنكية

ذهب اتجاه من الفقه إلى أن جريمة القرصنة الإلكترونية للبطاقة البنكية لا تتطلب بالضرورة وجود نصوص خاصة لتجريمها، وإنما يتعين على القضاء اللجوء إلى تأويل النصوص الجنائية القائمة، ولاسيما تلك المتعلقة بالسرقة والنصب.

جريمة قرصنة البطاقات البنكية في إطار السرقة

ذهب جانب من الفقه إلى عدم إمكانية تكييف جريمة قرصنة البطاقة البنكية في إطار السرقة على اعتبار كون محل السرقة يشترط فيه أن يكون مالًا ماديًّا منقولًا ما دام أن السرقة لا تتحقق إلا بفعل الاختلاس؛ أي إخراج الشيء من حيازة الجاني عليه دون رضاه، وهو ما لا يتصور إلا بالنسبة للأشياء المادية القابلة للنقل.

في حين يرى البعض الآخَر إمكانية توفُّر الحيازة في سرقة بيانات البطاقة البنكية متى ما اعتبرنا أنها تكون مُسَيَّجة بنظام حمائي لا يمكن عبوره إلا بوجود كلمة سرّ تجسد حيازة صاحب البيانات، وكل ولوج لها دون رضى صاحبها يعد اعتداءً على الحيازة واختلاسًا لمال الغير.

وقد ذهب جانب آخر من الفقه إلى أنه يمكن اختلاس البيانات المعلوماتية للبطاقة البنكية باعتبارها مالًا من الأموال ذات القيمة الاقتصادية، إذ يمكن سرقة هذه الأموال قياسًا على سرقة الطاقة الكهربائية والتي تعتبر أيضًا غير مادية.

جرائم قرصنة البطاقات البنكية في إطار النصب

اعتبر الفقه المغربي وسايرته في ذلك بعض المحاكم المغربية أن هذا السلوك يُعَدّ نصبًا على اعتبار أن المتهَم قد انتحل اسمًا كاذبًا، ما يكون معه قد استخدم وسيلة احتيالية لإقناع المجني عليه بوجود ائتمان[39].

في حين ذهب البعض الآخَر إلى أن جريمة النصب لا تقوم إلا إذا خدع شخص شخصًا طبيعيًّا، وبالتالي لا يمكن تصور وقوع جريمة النصب على الحاسب الآلي[40]. وهذا ما أكده القضاء المغربي معتبرًا أن القرصنة الإلكترونية للبطاقات البنكية واستعمالها بعد ذلك لا يمكن تكييفه نصبًا، مُعَلِّلا قراره، بما يلي:

«...أمّا جنحة النصب، فإن التكييف الذي أعطي لهذه القضية لا ينطبق عليها، وذلك لأن هذه الجريمة يجب أن ترتكب وفق ما هو محرَّر في الفصل 540 من القانون الجنائي، ذلك أن

38 بنسليمان، عبد السلام. (2020). مرجع سابق، ص. 105.
39 أحمام، عبد الله محمد. (2014). مرجع سابق، ص. 105.
40 داري، إبراهيم. (2013). الجريمة المعلوماتية. سلسلة فقه القضاء التجاري، منشورات مجلة العلوم القانونية، الرباط، ع. 2، ص. 189.

المتهمين جميعهم لم يكن لهُم أي اتصال مباشِر مع الضحايا الذين ارتكبت في حقهم هذه الأفعال، ولا معرفة للمتهَمين بهِم، وكذا الشأن بالنسبة للضحايا...»[41].

ثانيًا - التكييف المستحدث للقرصنة الإلكترونية للبطاقة البنكية

عمل المشرع المغربي لحماية أفضل لنظُم المعالَجة الآلية للمعطيات على تحيين ترسانته القانونية؛ وذلك بإصدار القانون رقم 07-03 المتمم للقانون الجنائي. وبدراسة مقتضيات هذا القانون يتبين لنا أن جريمة القرصنة الإلكترونية للبطاقة البنكية تحمل بين طياتها الجرائم التالية:

- جريمة الدخول الاحتيالي والبقاء في نظام المعالجة الآلية للمعطيات يترتب عليه تغيير في المعطيات المدرجة فيه.
- جريمة تزييف البطاقة البنكية.
- جريمة النصب المعلوماتي أو الغش المعلوماتي.

وبالاطلاع على المقتضيات الجنائية المعاقِبة على تزوير البطاقات البنكية نجد أنها تتعدد وتتنوع، وذلك على النحو التالي:

- جريمة التزوير في وسيلة أداء طبقًا للمادة 331 من مدونة التجارة[42].
- جريمة التزوير في محرر تجاري أو بنكي طبقًا للفصل 357 من القانون الجنائي.
- جريمة التزوير في وثيقة معلوماتية طبقًا للمادة 607-7 من القانون الجنائي.

وفي ختام دراستنا لمسألة التكييف الجنائي المناسِب لجريمة القرصنة الإلكترونية للبطاقة البنكية نجد أن الإشكال المطروح يتجلى بالأساس في تعدد النصوص المجرِّمة والمعاقِبة للقرصنة الإلكترونية للبطاقة البنكية والمتداخِلة فيما بينها، ما يجعلها جميعها قابلة للتطبيق؛ وذلك لعلّة تعدد الأوصاف التي تحملها هذه الوسيلة المستحدثة للوفاء الإلكتروني.

3. 2. 2. الفرع الثاني: القرصنة المعلوماتية للبطاقة البنكية في مواجهة تحديات وإكراهات القواعد الإجرائية الجزائية

تقنيات البحث والتحري ومدى كفايتها في توفير الحماية

يَعرِف موضوع البحث والتحري في جريمة القرصنة المعلوماتية للبطاقة البنكية إشكالات متعددة نتيجةً للطبيعة الخاصة لهذا النوع مِن الإجرام، وذلك بالنظر لطبيعة المجُرِم مِن جهة، ووسائل ارتكاب الجريمة مِن جهة أخرى. بالإضافة إلى أن التطور الحاصل في مجال المعلوميات أرخى بظلاله على أجهزة العدالة الجنائية التي لم تعُد تقدِر على مواكَبة التقنيات المتطورة لهذا النظام بشكل يسمح بمواجهة تحدي السرعة والفاعلية في مواجَهة هذه الجريمة.

ولتسليط الضوء على التقنيات المتعلقة بالبحث والتحري في مجال جرائم البطاقة البنكية، سنقتصر على الإجراءات المسطرية التي تجد الضابطة القضائية بُدًّا من القيام بها للحصول على الدليل الخاص بهذا النشاط الإجرامي، وما قد تفيده بعض الإجراءات كالمعاينة، التفتيش، وحجْز الدليل المعلوماتي في التثبت مِن وقوعها وضبْط مرتكِبيها.

41 ملف جنائي عدد 22/04/971 بتاريخ 2007/05/07 ص. 10، انظر فرام، كوثر. (2007- 2009). مرجع سابق، ص. 46.

42 القانون رقم 15.95 المتعلق بمدونة التجارة الصادر بتنفيذه ظهير شريف رقم 1.96.83 بتاريخ 15 ربيع الأول 1417 (فاتح أغسطس، 1996)، الجريدة الرسمية عدد 4418 بتاريخ 19 جمادى الأولى 1417 (3 أكتوبر، 1996)، ص. 2187.

أولًا - المعاينة

بمقتضى المادة 57 من قانون المسطرة الجنائية وضَع المشرِّع الجنائي الإجرائي على عاتق ضابِط الشرطة القضائية التزامًا بمقتضاه يتعين عليه كلّما بلغ إلى عِلمه خبَر وقوع جناية أو جنحة متلبَّس بها، أن يُشْعِر بها النيابة العامة، ثم ينتقل حالًا إلى عين المكان الذي ارتُكِبت فيه، وذلك لإجراء كل المعايَنات المفيدة، والمحافَظة على الأدلة، والقيام بحجْز الأشياء التي استُعمِلت في ارتكاب الجريمة [43].

لكن وفي ظل غياب الدليل المادي في الجرائم المعلوماتية يطرح التساؤل حول مدى إمكانية تطبيق هذا المقتضى على جريمة القرصنة الإلكترونية للبطاقة البنكية، فالجاني المعلوماتي عادة ما يقوم بالعبث بوسائل ارتكاب جريمته سواء بالحذف أو التغيير أو غيرها من الأفعال المنصوص عليها قانونًا، ناهيك أن جريمة القرصنة الإلكترونية للبطاقة البنكية في أغلب الأحيان تكون غيرَ مُتلبَّس بها، الأمر الذي يؤكِّد ضعْف أهمية المعايَنة فيها، فحتّى لو سلّمْنا أن تنصيص المشرِّع على عبارة «أو أشياء أخرى» يمكن أن يشمل المعطيات والبيانات المعالَجة إلكترونيا أيضًا، فإنَّ مسرح الجريمة قد تطرأ عليه تغييرات تَحُول دون اكتشاف الْجاني [44].

إضافةً إلى ذلك، يُظهر التحقيق في جرائم القرصنة الإلكترونية للبطاقة البنكية تحديات إضافية بسبب طبيعتها الرقمية، فعملية معاينة مسرح الجريمة لا تتطلب الانتقال إلى موقع الجريمة؛ لأن الجريمة تحدث عادةً عن بُعد. وهذا ما يُعرَف في بعض الأوساط القانونية بـ «الانتقال في العالَم الافتراضي»، حيث يشمل ذلك تحليل الرسائل المُرسَلة والمُستَلَمة، وجميع الاتصالات التي تمت عبر الإنترنت والشبكة العالمية. ومن خلال دراسة هذه البيانات الرقمية، يمكن للمحققين تتبُّع أنشطة المتهمين والبحث عن الأدلة الرقمية التي تثبت علاقتهم بارتكاب الجريمة. ومن ثم، فإن التحقيق في جرائم البطاقات البنكية يتطلب فهْمًا عميقًا للتكنولوجيا الرقمية والقدرة على التحليل الشامل للبيانات الإلكترونية [45].

ثانيًا - التفتيش وحجْز الدليل المعلوماتي في جرائم القرصنة المعلوماتية للبطاقات البنكية

سيتم التطرق في هذه النقطة إلى إجراء التفتيش في جريمة القرصنة الإلكترونية للبطاقة البنكية، ثم حجْز المعطيات المعلوماتية.

إجراء التفتيش في جريمة القرصنة الإلكترونية للبطاقة البنكية

يمكن القول: إن التفتيش ذلك الإجراء الذي يهدف إلى البحث عن الأفعال المجرَّمة قانونًا، والوسائل المستعمَلة فيها، قصْد جمْع الأدلة الحاسمة عن جريمة مِن الجرائم يجري البحث بصددها، وللتفتيش مدلول واحد، سواء تعلق الأمْر بالجرائم العادية أو الجرائم المعلوماتية، لكن تطبيق هذا الإجراء على جريمة القرصنة المعلوماتية للبطاقة البنكية يثير العديد من الصعوبات التي تحول دون تحقيق الغاية منه؛ نظرًا للصعوبات التي تطرحها الطبيعة الافتراضية لهذا النوع من الإجرام؛ ما يستوجب معه اعتماد قواعد خاصة تتماشى وطبيعتها.

وفي هذا الإطار نجد أن بعض التشريعات المقارنة أفردت مجموعة من القواعد الخاصة في مجال تفتيش الجرائم الإلكترونية، سواء على مستوى الأماكن التي يقع فيها التفتيش، أو على مستوى الأوقات التي يسمح فيها التفتيش.

---

43 العلمي، عبد الواحد. (2018). شروح في القانون الجديد المتعلق بالمسطرة الجنائية، مطبعة الناشر الجديدة، الدار البيضاء، ج. 1، ط. 7، ص. 403.

44 بنسليمان، عبد السلام. (2020). مرجع سابق، ص. 148.

45 المرجع السابق، ص. 149.

على مستوى مكان التفتيش: قد يصطدم ضابط الشرطة القضائية، أو قاضي التحقيق على إثر تفتيش الحاسب الخاص بالمتهم بارتباط حاسب هذا الأخير بحاسبات أخرى توجد داخل إقليم الدولة، أو في دولة أخرى. فالسؤال المطروح هل تستطيع الأجهزة المكلفة بالبحث والتحقيق تمديد التفتيش إلى أيّ حاسب آخَر مُتَّصِل بحاسِب المُتَّهَم؟

ونجد أمام سكوت المشرع المغربي أن بعض التشريعات المقارنة[46] قد قامت بالتنصيص على قواعد خاصة تسمح بامتداد التفتيش المعلوماتي بشكل يسمح للسلطات القضائية المختصة بالدخول إلى مجموع نظام معلوماتي آخَر إذا قام الاعتقاد بأن البيانات المطلوبة مُخَزَّنَة داخل هذا النظام المعلوماتي أو جزء منه، أو في دعامة إلكترونية[47].

على مستوى زمان التفتيش: بموجب المادة 62 من قانون المسطرة الجنائية المغربي «لا يمكن الشروع في تفتيش المنازل أو معاينتها قبل الساعة السادسة صباحًا، وبعْد الساعة التاسعة ليلًا». ومن شأن هذا الإجراء أن يضعف فاعلية التفتيش في جريمة القرصنة الواقعة على البطاقات البنكية.

ومن أجل تجاوز ذلك، عمدت بعض التشريعات المقارنة[48]، إلى استثناء القاعدة العامة التي تفرض أن التفتيش يكون في مدد زمنية محددة بنص القانون، مانحة بذلك لأجهزتها سلطة التفتيش في كل الأوقات.

ولَمّا كان أثر وخطر الجريمة المعلوماتية عابِرَيْن للحدود، نجد عدم انتباه المشرِّع المغربي لهذا المقتضى، ما يجعل الحاجة ماسّة إلى التفاعل الإيجابي مع هذه التشريعات مِن خلال الأخذ بالقواعد الخاصة بالتفتيش في هذا الصنف من الجرائم[49].

حجْز المعطيات المعلوماتية

عندما تكتشف أجهزة العدالة الجنائية التي تباشر التفتيش في منظومة معلوماتية معطيات مُخَزَّنَة مِن شأنها الكشْف عن الجرائم المرتكَبة، أو عن مرتكِبيها، فإنها تقوم بحجْز تلك المنظومة، أو الحفاظ عليها لتقديمها إلى المحكمة. وفي الحالات التي لا يكون فيها الحجْز ضروريًّا، فإن تلك الأجهزة تعمل على نسْخ المعطيات محَل البحث، وكذا المعطيات اللازمة لفهمها على دعامة إلكترونية تكون قابلة للحجْز والوضع في أغلفة أو أوعية وفقًا للقواعد المقرَّرة قانونًا[50].

وبالرجوع إلى مقتضيات قانون المسطرة الجنائية نلاحظ أن المشرِّع بصريح المادة 59 نصَّ على ما يلي: «إذا كان نوع الجناية أو الجنحة مما يُمْكن إثباته بحجْز أوراق ووثائق أو أشياء أخرى في حوزة أشخاص يظن أنهم شاركوا في الجريمة، أو يحوزون مستندات أو أشياء تتعلق بالأفعال الإجرامية...». ويُستشَفّ من عبارة «أشياء أخرى» أو أشياء تتعلق بالأفعال الإجرامية» إمكانية أن تشمل العناصر المعنوية في الجرائم المعلوماتية.

لكن السؤال المطروح هو كيف يمكن حجز العناصر المعنوية للجريمة المعلوماتية؟، وخصوصًا إذا

---

46 انظر المادة 1-57 من قانون المسطرة الجنائية الفرنسية.

47 بنسليمان، عبد السلام. (2020). مرجع سابق، ص. 169.

48 نصّ المشرع الفرنسي في المادة 5-102-L706 من قانون المسطرة الجنائية على ما يلي:

« En vue de mettre en place le dispositif technique mentionné à l'article 706-102-1, le juge d'instruction peut autoriser l'introduction dans un véhicule ou dans un lieu privé, y compris hors des heures prévues à l'article 59...S'il s'agit d'un lieu d'habitation et que l'opération doit intervenir hors des heures prévues à l'article 59 ...la mise en place du dispositif technique... »

49 بنسليمان، عبد السلام. (2020). مرجع سابق، ص. 171.

50 المرجع السابق، ص. 174.

ما سلّمنا بأنّ كافة الأدلّة وحتى يمكن الاعتداد بها يجب أن تحترم فيها جميع القيود والضوابط والشكليات التي تتوقف عليها صحتها من حيث الشكل أو المضمون؛ إذ إن الدليل يمكن أن يمسّ بقرينة البراءة، ويصبح مفتقدًا للمشروعية ما يوجب بطلانه، وهذا ما نصت عليه المادة 751من قانون المسطرة الجنائية التي تعتبر كل إجراء يأمر به هذا القانون ولم يثبت إنجازه على الوجه القانوني يعد كأنه لم ينجز. ولذلك لا يكون الدليل مشروعًا إلا إذا كانت طرق الحصول عليه مشروعةً وذلك طبقًا لمقتضيات الدستور والقوانين الإجرائية الجاري بها العمل وهو الأمر الذي يكرسه الفقه جملةً وتفصيلًا[51].

ويُلاحَظ مِن خلال ما سبق ذكره أن المقتضيات التشريعية المُكَرَّسة مِن قِبَل المشرِّع المغربي لا تتماشى وطبيعة الحجْز في الجرائم المعلوماتية. فهي ليست أشياء مادية يمكن لضابط الشرطة القضائية حجْزها ووضعها في كيس وتسليمها للعدالة، وإنما هي عبارة عن برامج معلوماتية تتطلب تعامُلًا خاصًّا في سبيل الحفاظ على الدليل المعلوماتي حتى يؤدِّي دوره الكامل في مجال الإثبات الجنائي.

وعلى أساسه فإن تطبيق النصوص القانونية التقليدية لمواجَهة جريمة القرصنة الإلكترونية للبطاقة البنكية لا يتماشى مع هذا النوع من الجرائم، فالواقع العملي سيقف حجَرَ عثْرة أمام حجْز العناصر المعنوية غيْر الملموسة، ويتعين معه مُلاءَمَة التشريع مع الخصوصية التي تطرحها الجريمة الإلكترونية.

وبالاطلاع على المشروع الأولي الجديد رقم 03.23 القاضي بتغيير وتتميم قانون المسطرة الجنائية والمصادق عليه من قبل مجلس الحكومة بتاريخ 29 غشت 2024 نجد أن المُشَرِّع تدارَك هذا النقص التشريعي، إذْ قام بإدخال هذا الصنف مِن المستنَدات ضِمْن الأشياء التي يمكن لأجهزة العدالة حجْزها والاحتفاظ بها كدليل لإثبات الجريمة المعلوماتية أو نفيها.

ففي هذا الإطار نصت المادة 59 من المشروع على ما يلي: «يتم حجز المعطيات والبرامج المعلوماتية الضرورية لإظهار الحقيقة بوضع الدعامات المادية المتضمنة لهذه المعلومات، أو بأخذ نسخ منها، بحضور الأشخاص الذين حضروا التفتيش، ويوضع ما تم حجزه رهن إشارة العدالة.

لا يحجز ضابط الشرطة القضائية إلا المستندات أو الوثائق أو المعطيات أو الأدوات أو البرامج المعلوماتية أو الأشياء الأخرى المفيدة في إظهار الحقيقة.

يمكن بعد موافقة النيابة العامة حجز كل شيء يتم العثور عليه عرضًا خلال التفتيش وله علاقة بجريمة أخرى.

يمكن لضباط الشرطة القضائية، بمناسبة إجراء تفتيش وفقًا للشروط المنصوص عليها في هذا القانون، الولوج إلى المعطيات المفيدة في البحث الجاري والمخزنة بنظام معلوماتي يوجد بالمكان الذي يجري فيه التفتيش أو بنظام معلوماتي آخر متصل به.

تخزن المعطيات التي تم الولوج إليها وفقًا للفقرات السابقة على أي دعامة إلكترونية، أو يتم حجز هذه الدعامة ووضعها في غلاف أو وعاء أو كيس، ويختم عليها ضابط الشرطة القضائية وفقًا للشروط المنصوص عليها في هذه المادة.

يمكن لضابط الشرطة القضائية انتداب أي شخص لمساعدته للولج للمعطيات المذكورة.

يمكن للوكيل العام للملك أو وكيل الملك كلٌّ فيما يخصه، أن يأمر بالحذف النهائي للمعطيات أو البرامج المعلوماتية الأصلية من الدعامة المادية التي لم توضع رهن إشارة المحكمة بعد أخذ

51 نفيد، يونس. (2021). الدليل الإلكتروني وحجيته في التشريع الجنائي المغربي. Journal Geostrategic and Intelligence ، م. 3، ع. 3، ص. 256.

نسخة منها إذا كانت حيازتها أو استعمالها غير مشروع، أو كانت تشكل خطرًا على أمن الأفراد أو الممتلكات أو منافيًا للأخلاق العامة. كما يمكن لهما أن يأمرا بإيقاف بث أو حجب نشر معطيات رقمية يشكل مضمونها جريمة، ويحرر محضر بالحذف أو الحجب أو بإيقاف البث يضاف إلى المسطرة.

تحصى المستندات أو الوثائق أو المعطيات أو الأدوات أو البرامج المعلوماتية أو الأشياء الأخرى المحجوزة فورًا وتلف أو توضع.....عليها بطابعه».

4. الخاتمة

يظهر جليًّا أن حماية البطاقة البنكية من القرصنة الرقمية أصبحت أمرًا ضروريًّا في ظل تزايُد التهديدات السيبرانية، وذلك من خلال الاعتماد على مجموعة متنوعة من الآليات الإدارية والتقنية، بما يُمكن المؤسسات المصرفية والفردية من تعزيز الأمان والحماية لمعاملات الدفع الإلكتروني.

وبناءً عليه فوُجود تقنيات مثل: الجدران النارية وبرامج الحماية تؤدي دورًا حاسمًا في منع الوصول غير المصرَّح به إلى البيانات المصرفية الحساسة. بالإضافة إلى ذلك، يعد التدريب المستمر للموظفين على كشف الاحتيال وتطبيق سياسات الأمان والمراقبة الداخلية أساسيًّا للحفاظ على سلامة النظام المصرفي.

ونظرًا لاستمرار التطور التكنولوجي، يجب على البنوك والمؤسسات المالية والمؤسسات التشريعية والقضائية الاستمرار في تطوير إستراتيجياتها لمواجَهة التهديدات الجديدة. وذلك بالعمل المشترك واتخاذ الإجراءات اللازمة، حيث يمكن تحقيق بيئة مالية إلكترونية أكثر أمانًا وثقة لجميع المستخدمين.

4. 1. النتائج

من خلال دراسة المواجهة الجنائية للبطاقة المصرفية ضد القرصنة الرقمية وتحليلها، استخلصنا عدة نتائج مهمة:

عمل المشرع المغربي عمل بهدف حماية أفضل لنظُم المعالَجة الآلية للمعطيات على تحيين ترسانته القانونية بإصدار القانون رقم 07-03 وبموجبه، فإن جريمة القرصنة الإلكترونية للبطاقة البنكية تدخل ضمن نطاق جرائم الدخول الاحتيالي، والتزييف، والنصب المعلوماتي.

يتجلى الإشكال في تعدد النصوص المجرِّمة والمعاقِبة لهذه الجريمة والمتداخِلة فيما بينها، ما يجعلها جميعها قابلة للتطبيق؛ وذلك لعلّة تعدد أوصافها.

تدارك مشروع القانون رقم 03.23 القاضي بتغيير وتتميم قانون المسطرة الجنائية العديد من الأمور المهمة المتعلقة بهذا الموضوع.

أهمية التدريب المنتظِم لموظفي البنوك والجهات المختصة لتعزيز القُدرات وفْق الممارسات الفضلى في مجال اكتشاف ومعالَجة الاحتيال؛ بُغْيَة تعزيز الأمان والمكافحة الاستباقية والزجرية للجريمة المعلوماتية.

إن تأمين البطاقة المصرفية من القرصنة الرقمية يتطلب جهودًا مشترَكة ومتواصِلة من البنوك والمؤسسات المالية والسلطات المختصة، بالإضافة إلى استخدام التقنيات الحديثة وتبني السياسات الوقائية الملائمة.

4. 2. التوصيات

بناءً على النتائج المستخلَصة أعلاه، يمكن تقديم التوصيات التالية:

تقوية وتحيين المنظومة القانونية وفْق آخِر المستجدات وأفضل الممارسات، من خلال التشريع الفعال، مع الضرورة القانونية الزجرية مِن خلال مواكَبة التشريعات الجنائية المغربية للتطورات التكنولوجية، وتحديد عقوبات مناسِبة لجرائم القرصنة الرقمية.

تفعيل الدور الوقائي والاستثمار في أحدث التقنيات الأمنية من خلال تبني البنوك والجهات ذات العلاقة لإجراءات وسياسات وقائية لمنْع أو تقليل احتمالات الاختراق والقرصنة الرقمية للبطاقات المصرفية.

التعاون والتنسيق من خلال الحاجة المُلِحَّة إلى تعاون مُشترَك بين البنوك والسلطات المختصة والجهات القانونية لمكافحة الجريمة الإلكترونية بفاعلية.

تعزيز التدريب لموظفي مختلف البنوك المغربية والجهات ذات العلاقة وتحديثها بانتظام للاطّلاع ومواكَبة أحدث التهديدات الأمنية ومعالجتها بفاعلية.

تعزيز حملات التوعية والتثقيف بين المستخدمين حول مخاطر القرصنة الرقمية وكيفية حماية بياناتهم المصرفية.

تعزيز التعاون على مستوى البنوك والمؤسسات المالية والسلطات المختصة والجهات القانونية المغربية ونظيرتها الإقليمية والدولية؛ بغية تبادُل المعلومات وتكثيف الجهود في مواجهة ومكافحة الجريمة الإلكترونية.

وبناء عليه، يسهم العمل على هذه التوصيات في تعزيز أمان البطاقات المصرفية وحماية المعلومات البنكية للمستخدمين من التهديدات الرقمية، وبالتالي في حماية المصالح المالية للأفراد والمجتمع والدولة.

المراجع

المراجع العربية

أحمام، عبد الله محمد. (2014). الحماية الجنائية للبطاقة الجنائية للبطاقة البنكية، دراسة مقارنة. دار أبي رقراق للطباعة والنشر الرباط.

أعزان، أمين. وجاكيمي، عبد السلام. (2016). الحماية التقنية والجنائية للنظم المعلوماتية. المجلة المغربية للقانون الجنائي والعلوم الجنائية، م. 2016، ع. 3.

بلمحجوب، إدريس. (2014). تأثير الجريمة الإلكترونية على الائتمان المالي. سلسلة ندوات محكمة الاستئناف ندوة خاصة بمناسبة الذكرى المئوية. مطبعة الأمنية، الرباط.

بلميلود، سارة. والسائح، إيمان. (2015). الحماية القانونية لمستهلكي تكنولوجيا المعلومات. مجلة المنبر القانوني، ع. 9.

بنسليمان، عبد السلام. (2020). الإجرام المعلوماتي في التشريع المغربي: دراسة نقدية مقارنة في ضوء آراء الفقه وأحكام القضاء. ط. 2، دار الآفاق المغربية للنشر والتوزيع، الدار البيضاء.

الجرائم البنكية. (16 مايو, 2013). مجلة القانون والأعمال الدولية، جامعة الحسن الأول، تم الاطلاع بتاريخ 01 مارس 2024 من https://l1nq.com/PqmPD.

حسن، هشام فتحي سيد. (2003). وسائل حماية المستهلك الإلكتروني بين الشريعة والقانون. مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، 12 أكتوبر، 2003، غرفة تجارة وصناعة دبي، م. 3.

خنفوسي، عبد العزيز. (2018). مدخل إلى قانون الدفع الإلكتروني. مركز الكتاب الأكاديمي، الأردن، ط.1.

داري، إبراهيم. (2013). الجريمة المعلوماتية. سلسلة فقه القضاء التجاري، منشورات مجلة العلوم القانونية، الرباط، ع. 2.
داود، حسن طاهر. (2000). الحاسب وأمن المعلومات. معهد الإدارة العامة، مكتبة الملك فهد الوطنية، الرياض.
درامي، محمد. (2010/2009). الحماية الجنائية للبيانات المعلوماتية، رسالة لنيل دبلوم الماستر في القانون الخاص. وحدة القانون المدني، كلية الحقوق الدار البيضاء.
الرحالي، نور الدين. (2018). توجهات السياسة الجنائية في مجال وسائل الأداء والائتمان. الندوة العلمية السياسة الجنائية بالمغرب: الواقع والآفاق 2004-2018، الرباط، المطبعة الأمنية.
زيدان، ربيحة. (2011). الجريمة المعلوماتية في التشريع الجزائري والدولي. دار الهدى للطباعة والنشر والتوزيع عين مليلة، الجزائر.
الشوابكة، محمد أمين. (2007). جرائم الحاسوب والإنترنت: الجريمة المعلوماتية. دار الثقافة للنشر والتوزيع، عمّان، الأردن.
صقر، رواد ميلود. (2020). الحماية الأمنية لأنظمة الدفع الإلكترونية. مجلة الحقوق، سلسلة المعارف القانونية والقضائية، م. 74.
العلمي، عبد الواحد. (2018). شروح في القانون الجديد المتعلق بالمسطرة الجنائية. مطبعة الناشر الجديدة، الدار البيضاء، ج. 1، ط. 7.
فالي، علال. (2013). خصوصيات الجريمة المعلوماتية على ضوء التشريع والقضاء المغربي. مجلة القضاء التجاري، ع. 2، الرباط.
فرام، كوثر. (2007-2009). الجريمة المعلوماتية على ضوء العمل القضائي المغربي، بحث نهاية التدريب في المعهد العالي للقضاء، المغرب.
قورة، نائلة عادل. (2005). جرائم الحاسب الآلي الاقتصادية: دراسة نظرية وتطبيقية. منشورات الحلبي الحقوقية، ط. 1، بيروت، ص. 315.
لامية، طالة؛ وكهينة، سلام. (2020). الجريمة الإلكترونية: بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الاجتماعي. مجلة الرواق للدراسات الاجتماعية والإنسانية، م. 6، ع. 2، ص. 71.
مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين. (10- 17 أبريل، 2000). الجريمة والعدالة: مواجهة تحديات القرن الحادي والعشرين. فيينا.
نفيد، يونس. (2021). الدليل الإلكتروني وحجيته في التشريع الجنائي المغربي. Journal of the Geopolitics and Geostrategic Intelligence ، م. 3، ع. 3.
هلالي، عبد الإله أحمد. (2000). التزام الشاهد بالإعلام في الجرائم المعلوماتية: دراسة مقارنة. دار النهضة العربية، القاهرة.

القوانين

الجريدة الرسمية المغربية. (22 ديسمبر، 2003. ع. 5171). ظهير شريف رقم -1 -03 197 صادر في 16 من رمضان 1424 (11 نوفمبر 2003) بتنفيذ القانون رقم -03 07، بتنفيذ القانون -03 07 بتتميم مجموعة القانون الجنائي فيما يتعلق بالجرائم المتعلقة بنظم المعالجة الآلية للمعطيات.
الجريدة الرسمية المغربية. (11 يناير، 2021. ع. 6951). ظهير شريف رقم -1 -20 100 صادر في 16 جمادى الأولى 1442 (31 ديسمبر 2020) بتنفيذ القانون رقم -20 43 المتعلق بخدمات الثقة بشأن المعاملات الإلكترونية.
الجريدة الرسمية المغربية. (3 مايو، 2007. ع. 5522). القانون رقم 43.05 المتعلق بمكافحة غسل الأموال الصادر بتنفيذه ظهير شريف رقم 1.07.79 بتاريخ 28 من ربيع الأول 1428 (17 أبريل، 2007)، ص. 1359.

الجريدة الرسمية المغربية. (3 أكتوبر 1996. ع. 4418) القانون رقم 15.95 المتعلق بمدونة التجارة الصادر بتنفيذه ظهير شريف رقم 1.96.83 بتاريخ 15 ربيع الأول 1417 (فاتح أغسطس 1996)، ص. 2187.

References (Romanization)

Aḥmām, ʿAbd Allāh Muḥammad. (2014). Al-Ḥimāyah al-jināʾiyyah lil-biṭāqah al-bankiyyah, dirāsah muqāranah. Dār Abī Ruqrāq li-al-ṭibāʿah wa-al-nashr, Rabat.

Al-Jarāʾim al-bankiyyah. (May 16, 2013). Majallat al-qānūn wa-al-aʿmāl al-duwaliyya, Jāmiʿat al-Ḥasan al-Awwal. Accessed March 1, 2024 from https://l1nq.com/PqmPD.

Al-Raḥālī, Nūr al-Dīn. (2018). Tawajjuhāt al-siyāsah al-jināʾiyyah fī majāl wasāʾil al-adāʾ wa-al-itiʾmān. Al-nadwah al-ʿilmiyyah: al-siyāsah al-jināʾiyyah bi-al-Maghrib: al-wāqiʿ wa-al-āfāq 2004–2018, Rabat, Maṭbaʿat al-Amniyyah.

Al-Shawābikah, Muḥammad Amīn. (2007). Jarāʾim al-ḥāsib wa-al-internet: al-jarīmah al-maʿlūmātiyyah. Dār al-Thaqāfah lil-nashr wa-al-tawzīʿ, ʿAmmān, Jordan.

Al-ʿIlmī, ʿAbd al-Wāḥid. (2018). Sharūḥ fī al-qānūn al-jadīd al-mutaʿalliqq bi-al-masṭarah al-jināʾiyyah. Maṭbaʿat al-Nāshir al-Jadīdah, Casablanca, vol. 1, 7th ed.

Aʿzān, Amīn; and Jākīmī, ʿAbd al-Salām. (2016). Al-ḥimāyah al-tiqlīniyyah wa-al-jināʾiyyah lil-nuẓum al-maʿlūmātiyyah. Al-Majallah al-Maghribiyyah lil-qānūn al-jināʾī wa-al-ʿulūm al-jināʾiyyah, vol. 2016, no. 3.

Bilmāḥjūb, Idrīs. (2014). Taʾthīr al-jarīmah al-iliktirūniyyah ʿalā al-itiʾmān al-mālī. Silsilat nuduwāt Maḥkamat al-istiʾnāf nadwah khāṣṣah bi-munāsabah al-dhikrá al-miʾawiyyah. Maṭbaʿat al-Amniyyah, Rabat.

Bilmilūd, Sārah; and al-Sāʾiḥ, Īmān. (2015). Al-ḥimāyah al-qānūniyyah li-mustahlikī tikanūlūjiyyat al-maʿlūmāt. Majallat al-minbar al-qānūnī, no. 9.

Binslimān, ʿAbd al-Salām. (2020). Al-ijrām al-maʿlūmāti fī al-tashrīʿ al-Maghribī: dirāsah naqdiyyah muqāranah fī ḍawʾ ārāʾ al-fiqh wa-aḥkām al-qaḍāʾ. 2nd ed., Dār al-Āfāq al-Maghribiyyah lil-nashr wa-al-tawzīʿ, Casablanca.

Dārī, Ibrāhīm. (2013). Al-jarīmah al-maʿlūmātiyyah. Silsilat fiqh al-qaḍāʾ al-tijārī, Manshūrāt Majallat al-ʿulūm al-qānūniyyah, Rabat, no. 2.

Dāwūd, Ḥasan Ṭāhir. (2000). Al-ḥāsib wa-amn al-maʿlūmāt. Maʿhad al-Idārah al-ʿĀmmah, Maktabat al-Malik Fahd al-Waṭaniyyah, Riyadh.

Durāmī, Muḥammad. (20092010/). Al-ḥimāyah al-jināʾiyyah lil-bayānāt al-maʿlūmātiyyah, risālah li-nayl diplūm al-māstir fī al-qānūn al-khāṣṣ. Wahdat al-qānūn al-madanī, Kulliyyat al-ḥuqūq, Casablanca.

Fālī, ʿAllāl. (2013). Khuṣūṣiyyāt al-jarīmah al-maʿlūmātiyyah ʿalá ḍawʾ al-tashrīʿ wa-al-qaḍāʾ al-Maghribī. Majallat al-qaḍāʾ al-tijārī, no. 2, Rabat.

Farrām, Kawthar. (2007–2009). Al-jarīmah al-maʿlūmātiyyah ʿalá ḍawʾ al-ʿamal al-qaḍāʾī al-Maghribī, baḥth nihāyat al-tadrīb fī al-Maʿhad al-ʿĀlī lil-qaḍāʾ, Morocco.

Ḥasan, Hishām Fatḥī Sayyid. (2003). Wasāʾil ḥimāyat al-mustahlik al-iliktrūnī bayna al-sharīʿah wa-al-qānūn. Electronic Banking Conference between Sharia and Law, October 12, 2003, Dubai Chamber of Commerce and Industry, Vol. 3.

Hilālī, ʿAbd al-Ilāh Aḥmad. (2000). Iltizām al-shāhid bi-al-iʿlām fī al-jarāʾim al-maʿlūmātiyyah: dirāsah muqāranah. Dār al-Nahḍah al-ʿArabiyyah, Cairo.

Khanfūsī, ʿAbd al-ʿAzīz. (2018). Madkhal ilá qānūn al-dafʿ al-iliktrūnī. Markaz al-Kitāb al-Akādīmī, Jordan, 1st ed.

Lāmiyah, Ṭālah; and Wahīnah, Salām. (2020). Al-jarīmah al-iliktrūniyyah: buʿd jadīd li-mafhūm al-ijrām ʿabr manāṣāt mawāqiʿ al-tawāṣul al-ijtimāʿī. Majallat al-rūwāq lil-dirāsāt al-ijtimāʿiyyah wa-al-insāniyyah, vol. 6, no. 2, p. 71.

Nafīd, Yūnis. (2021). Al-dalīl al-iliktrūnī wa-ḥujiyyatuh fī al-tashrīʿ al-jināʾī al-Maghribī. Journal of the Geopolitics and Geostrategic Intelligence, vol. 3, no. 3.

Qūrah, Nāʾilah ʿĀdil. (2005). Jarāʾim al-ḥāsib al-ālī al-iqtiṣādiyyah: dirāsah naẓariyyah wa-taṭbīqiyyah. Manshūrāt al-Ḥalabī al-ḥuqūqiyyah, 1st ed., Beirut, p. 315.

Ṣaqr, Rawād Mīlūd. (2020). Al-ḥimāyah al-amniyyah li-anẓimat al-dafʿ al-iliktrūniyyah. Majallat al-ḥuqūq, silsilat al-maʿārif al-qānūniyyah wa-al-qaḍāʾiyyah, vol. 74.

United Nations. (Vienna, 1017- April, 2000). Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders

Zaydān, Rabīḥah. (2011). Al-jarīmah al-maʿlūmātiyyah fī al-tashrīʿ al-Jazāʾirī wa-al-duwalī. Dār al-Hudá lil-ṭibāʿah wa-al-nashr wa-al-tawzīʿ, ʿAyn Mallīlah, Algeria.

Legal References:

Al-Jarīdah al-rasmiyyah al-Maghribiyyah. (December 22, 2003, no. 5171). Ẓahīr sharīf no. 1197-03- issued on 16 Ramaḍān 1424 (November 11, 2003) enforcing law no. 0307- concerning amendments to the penal code regarding crimes related to automated data processing systems.

Al-Jarīdah al-rasmiyyah al-Maghribiyyah. (January 11, 2021, no. 6951). Ẓahīr sharīf no. 1100-20- issued on 16 Jumādá al-Awwal 1442 (December 31, 2020) enforcing law no. 2043- concerning trust services related to electronic transactions.

Al-Jarīdah al-rasmiyyah al-Maghribiyyah. (May 3, 2007, no. 5522). Law no. 43.05 concerning anti-money laundering, enforced by Ẓahīr sharīf no. 1.07.79 dated 28 Rabīʿ al-Awwal 1428 (April 17, 2007), p. 1359.

Al-Jarīdah al-rasmiyyah al-Maghribiyyah. (October 3, 1996, no. 4418). Law no. 15.95 concerning the commercial code, enforced by Ẓahīr sharīf no. 1.96.83 dated 15 Rabīʿ al-Awwal 1417 (August 1, 1996), p. 2187.