ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639
Volume 11 issue 3
N:64 June 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

جريمة سرقة الهوية في النظام القانوني القطري والمقارن

IDENTITY THEFT CRIME IN THE QATARI AND COMPARATIVE LEGAL SYSTEM

باحث أول / إبراهيم محمد المفلحي
باحث ثاني الأستاذ الدكتور / أكرم طراد الفايز
كلية القانون ، جامعة لوسيل/ قطر

الملخص

تعد سرقة الهوية من الجرائم المستحدثة التي برزت مع التطور التكنولوجي المتسارع، وانتشار المعاملات الإلكترونية في مختلف جوانب الحياة اليومية سواءً في المجال التجاري أو المصرفي أو حتى في العلاقات الاجتماعية. وتقوم جريمة سرقة الهوية باستيلاء الجاني على بيانات شخصية أو مالية أو إلكترونية تخص الغير، لاستخدامها بصور على نحو غير مشروع من أجل تحقيق منافع مادية أو معنوية للإضرار بالمجني عليه. وقد دفعت هذه المخاطر التشريعات الوطنية والدولية إلى البحث عن تنظيم قانوني محكم يواكب طبيعة الجريمة ويوازن بين حماية الحقوق الفردية وضمان سير المعاملات الإلكترونية بثقة وأمان.

وتتجلى أهمية هذا البحث بإثراء المكتبة القانونية بدراسة معمقة في تحليل مفهوم سرقة الهوية الرقمية وبيان خصائصها المميزة وتمييزها عن الجرائم التقليدية مع استعراض الأطر التشريعية والقواعد العامة التي تحكمها، سواء على المستوى القانوني الوطني أو على المستوى الدولي وما أفرزته الاجتهادات الفقهية في ذلك الجانب والاجتهادات القضائية بما يضع إطاراً نظرياً متكاملاً لفهم أبعاد هذه الجريمة.

الكلمات المفتاحية: سرقة الهوية – الجريمة الإلكترونية – حماية البيانات الشخصية – حماية البيانات المالية – حماية البيانات الإلكترونية – المخاطر القانونية – الجرائم التقليدية – تحقيق المنافع بطرق غير شرعية - حماية الحقوق الشخصية والفردية – صون المعاملات الإلكترونية.

Abstract

Identity theft is a relatively new crime that has emerged with rapid technological advancements and the widespread adoption of electronic transactions in various aspects of daily life, whether in commerce, banking, or even social interactions. The crime of identity theft involves the perpetrator seizing personal, financial, or electronic data belonging to another person for unlawful use to gain material or moral benefits, thereby harming the victim. These risks have prompted national and international legislation to seek robust legal frameworks that keep pace with the nature of the crime and balance the protection of individual rights with ensuring the secure and reliable conduct of electronic transactions.

The importance of this research lies in enriching the legal literature with an in-depth study analyzing the concept of digital identity theft, highlighting its distinctive characteristics, and differentiating it from traditional crimes. It also reviews the legislative frameworks and general rules governing it, both at the national and international legal levels, as well as the resulting scholarly and judicial interpretations in this area, thus establishing a comprehensive theoretical framework for understanding the dimensions of this crime.

Keywords: Identity theft – Cybercrime – Personal data protection – Financial data protection – Electronic data protection – Legal risks – Traditional crimes – Illicit enrichment – Protection of personal and individual rights – Safeguarding electronic transactions.

Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

المقدمة:

سرقة الهوية تعد من الجرائم المستحدثة التي برزت مع التطور التكنولوجي المتسارع، وانتشار المعاملات الإلكترونية في مختلف جوانب الحياة اليومية سواءً في المجال التجاري أو المصرفي أو حتى في العلاقات الاجتماعية، ويراد بسرقة الهوية أن يقوم الجاني بالاستيلاء على بيانات شخصية أو مالية تخص الغير، مثل الاسم أو الرقم القومي أو بيانات البطاقات البنكية أو الحسابات الإلكترونية واستخدامها بصور توحي بأن صاحب الهوية الحقيقي هو من يقوم باستخدامها، فيستخدمها على نحو غير مشروع من أجل تحقيق منافع مادية أو معنوية للإضرار بالمجني عليه، وتكمن خطورة هذه الجريمة في كونها غالباً ما ترتكب بوسائل تقنية يصعب تتبعها، مما يجعلها تتجاوز الحدود الوطنية وتتسم بالطابع العابر للحدود.

وقد دفعت هذه المخاطر التشريعات الوطنية والدولية إلى البحث عن تنظيم قانوني محكم يواكب طبيعة الجريمة ويوازن بين حماية الحقوق الفردية وضمان سير المعاملات الإلكترونية بثقة وأمان، فمن جانب نجد بأن بعض التشريعات الجنائية التقليدية لم تكن تتضمن نصوصاً صريحة تجرم هذا الفعل، فكان يصار إلى تكييفه في إطار جرائم الاحتيال أو التزوير أو الدخول غير المشروع إلى الأنظمة المعلوماتية غير أن خصوصية سرقة الهوية وما تثيره من آثار خطيرة على الحياة الاقتصادية والاجتماعية دفعت كثيراً من الدول إلى إدراج نصوص خاصة تجرم هذا السلوك بشكل مستقل مع تغليظ العقوبات إذا ارتكبت الجريمة باستخدام شبكة الإنترنت أو استهدفت بيانات ذات طبيعة مصرفية أو مالية.

وعلى الصعيد الدولي اهتمت الاتفاقيات الدولية متعددة الأطراف مثل اتفاقية بودابست بشأن الجريمة الإلكترونية بتعزيز التعاون بين الدول لمواجهة هذه الظاهرة من خلال تحديد الأسس التشريعية وتسيير آليات تبادل المعلومات والأدلة وبهذا يمكن القول إن التنظيم القانوني لجريمة سرقة الهوية يمثل استجابة تشريعية وقضائية لمخاطر الواقع الرقمي، ويهدف إلى حماية الأفراد والمجتمع من الانتهاكات المتزايدة للبيانات الشخصية بما يحافظ على الثقة في البيئة الإلكترونية ويضمن استقرار المعاملات الحديثة.

أهمية الدراسة:

تتجلى أهمية الدراسة في كونها تسعى إلى حماية الحقوق والحريات الشخصية للأفراد وصون المعاملات الإلكترونية من مخاطر الاستغلال غير المشروع وهو ما يعزز الثقة في البيئة الرقمية وعلى هذا فيمكن تمييز الأهمية إلى أهمية نظرية وأهمية عملية:

فمن الجانب النظري: تتجلى أهمية الدراسة النظرية بإثراء المكتبة القانونية بدراسة معمقة في تحليل مفهوم سرقة الهوية الرقمية وبيان خصائصها المميزة وتمييزها عن الجرائم التقليدية مع استعراض الأطر التشريعية والقواعد العامة التي تحكمها، سواء على المستوى القانوني الوطني أو على المستوى الدولي وما أفرزته الاجتهادات الفقهية في ذلك الجانب والاجتهادات القضائية بما يضع إطاراً نظرياً متكاملاً لفهم أبعاد هذه الجريمة.

ومن الناحية العملية: تتناول الدراسة الكيفية التي يتم من خلالها تطبيق النصوص القانونية على أرض الواقع من خلال بيان ممارسات القضاء في التصدي لحالات سرقة الهوية واستعراض أبرز التحديات العملية في كشف الجناة وجمع الأدلة الرقمية في مواجهة هذه الجريمة المستحدثة.

إشكالية وتساؤلات الدراسة:

تتمحور إشكالية الدراسة حول الإشكاليات القانونية متعددة الأبعاد والتي تثيرها جريمة سرقة الهوية، والتي تتمثل في صعوبة تكييف الجريمة ضمن الأطراف الجنائية التقليدية، فضلاً عن الطابع التقني والافتراضي الذي تتميز به، والذي يجعل من إثباتها وملاحقة مرتكبيها تحدياً حقيقياً أمام أجهزة العدالة كما أن هذه الجريمة عادةً ما تتخذ طابعاً عابراً للحدود، وهو ما يثير تساؤلات حول مدى كفاية التنظيمات الوطنية في مواجهتها وحول الحاجة إلى التعاون الدولي وآليات تبادل المعلومات والأدلة ومن هنا تنشأ ضرورة البحث في مدى فاعلية التنظيم القانوني الحالي لردع هذه الجريمة وضمان حماية البيانات والحقوق الفردية.

التساؤل الرئيسي:

Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

ما مدى كفاية وفعالية التنظيم القانوني في مواجهة جريمة سرقة الهوية وحماية الحقوق المرتبطة بها؟

التساؤلات الفرعية:

1- ما المقصود بجريمة سرقة الهوية وما خصائصها المميزة عن غيرها من الجرائم المعلوماتية؟
2- كيف تناولت التشريعات الوطنية والدولية هذه الجريمة من حيث التجريم والعقاب؟
3- ما دور التعاون الدولي في مكافحة سرقة الهوية ذات الطبيعة العابرة للحدود؟
4- ما التوصيات التشريعية والعملية لتعزيز الحماية من جريمة سرقة الهوية في البيئة الرقمية؟

أسباب اختيار موضوع الدراسة:

تم اختيار هذا الموضوع لما له من أهمية حيث إنه يمس صميم حماية الحقوق الفردية في البيئة الرقمية، وهو ما يعكس الحاجة الملحة لتطوير التشريعات بما يواكب التحديات التقنية المتسارعة.

السبب الذاتي: يرجع السبب الذاتي في اختيار هذا الموضوع لاهتمامي الشخصي بدراسة الجرائم المستحدثة في ظل الثورة التكنولوجية ورغبتي في الإسهام بإثراء المكتبة القانونية ببحث يتناول جانباً معاصراً على درجة كبيرة من الأهمية النظرية والعملية.

الأسباب الموضوعية:

1. تزايد جرائم سرقة الهوية على المستويين الوطني والدولي وما يلحق ذلك من أضرار جسيمة.
2. غياب أو قصور بعض التشريعات الوطنية عن معالجة الظاهرة بشكل صريح ومستقل.
3. الطابع التقني المعقد لجريمة سرقة الهوية وما يطرحه من تحديات في الإثبات والتحقيق.
4. الطبيعة العابرة للحدود للجريمة مما يفرض الحاجة إلى تعاون دولي فعال.
5. أهمية تعزيز ثقة الأفراد في البيئة الرقمية والمعاملات الإلكترونية.

أهداف الدراسة:

تهدف الدراسة إلى تحقيق جملة من الغايات النظرية والعملية والتي يمكن إجمالها في الآتي:

1. توضيح الإطار المفاهيمي لجريمة سرقة الهوية من خلال تحديد ماهيتها وعناصرها وخصائصها المميزة.
2. تحليل الأطر التشريعية الوطنية والدولية ذات الصلة مع بيان أوجه القوة والقصور في معالجة هذه الجريمة.
3. بيان دور التعاون الدولي والاتفاقيات متعددة الأطراف في مكافحة الطابع العابر للحدود لهذه الجريمة.
4. تقديم التوصيات التشريعية والعملية والتي تسهم في تعزيز فعالية التنظيم القانوني وحماية الحقوق الفردية في البيئة الرقمية.

منهج الدراسة:

تتبع الدراسة المنهج الوصفي التحليلي من استعراض النصوص القانونية الوطنية والدولية المتعلقة بجريمة سرقة الهوية وتحليلها للكشف عن مدى وضوحها وفعاليتها، بالإضافة إلى استخدام المنهج المقارن عن طريق دراسة بعض التشريعات المقارنة التي تناولت هذه الجريمة، مع الوقوف على أوجه التشابه والاختلاف بينها وبين التشريع الوطني للاستفادة من التجارب الناجحة في معالجة هذه الجريمة.

صعوبة الدراسة:

ترجع صعوبة هذه الدراسة إلى حداثة الموضوع وتشعبه، وهو أدى إلى قلة المراجع العربية المتخصصة والتي تناولت هذه الجريمة بشكل معمق، وهو الأمر الذي يفرض على الباحث الاعتماد على المصادر الأجنبية أو التشريعات المقارنة، بالإضافة إلى أن الطبيعة التقنية البحتة لهذه الجريمة تجعل الإلمام بالجوانب الفنية المتعلقة بآليات ارتكابها وإثباتها تحدياً إضافياً، ويضاف إلى ذلك التباين

Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

بين التشريعات الوطنية من دولة لأخرى، فضلاً عن بطء التوافق الدولي بشأن صياغة قواعد موحدة لمكافحتها، كل تلك العوامل جعلت من البحث في هذا الموضوع مهمة دقيقة تتطلب جهداً مضاعفاً في الجمع والتحليل والمقارنة.

ولتحليل الموضوع فقد ارتأيت تقسيم هذا البحث إلى مبحثين يتناول الأول ماهية جريمة سرقة الهوية وأسباب انتشارها وآثارها، ويتناول الثاني جريمة سرقة الهوية في القانون القطري والمقارن.

المبحث الأول: ماهية جريمة سرقة الهوية وأسباب انتشارها و آثارها

يسعى هذا المبحث إلى بيان الإطار المفاهيمي للجريمة، من حيث توضيح مفهومها وبيان طبيعتها، والعوامل التي ساهمت في انتشارها والآثار المترتبة عليها سواء على المستوى الفردي أو المجتمعي، وهذا العرض التمهيدي يمثل مدخلاً ضرورياً لفهم الإطار القانوني والواقعي للجريمة.

المطلب الأول: ماهية جريمة سرقة الهوية

يتناول هذا المطلب ماهية الجريمة من خلال تحديد مفهومها وخصائصها التي تنفرد بها وتميزها عن غيرها من الجرائم المعلوماتية، والتي تتصل بالبيانات الشخصية، ويعد هذا التحديد خطوة رئيسية لتهيئة الإطار المفاهيمي الذي يبني عليه التنظيم القانوني والتطورات التشريعية التي تتعلق بجريمة سرقة الهوية في المباحث اللاحقة.

الفرع الأول: التعريف بجريمة سرقة الهوية وتميزها عن غيرها من الجرائم

البيانات الشخصية في العصر الرقمي تمثل الامتداد المباشر للشخص نفسه حيث أنها تعبر عن هذا الشخص أمام المؤسسات والأنظمة والمصارف والمتاجر الإلكترونية وتحدد مكانه في العالم الافتراضي والواقعي على حد سواء ومع انتقال جانب واسع من المعاملات إلى المنصات الرقمية تعددت صور استخدام تلك البيانات حتى صارت جزءاً لا ينفصل عن هوية الفرد اليومية فالموظف يباشر أعماله من خلال حسابات إلكترونية والطالب يعتمد على منصات تعليمية مرتبطة ببياناته والمواطن ينفذ معاملاته الحكومية والمصرفية من خلال أنظمة رقمية تعتمد بشكل كامل على هويته الرقمية ، وهذا التحول الكبير فتح الباب أمام ظهور جريمة سرقة الهوية التي لم تكن معروفة في صورتها الحالية قبل انتشار التكنولوجيا بهذا الاتساع فهي جريمة تستغل الثغرات التقنية وغفلة الأفراد وثقة المؤسسات في البيانات المقدمة إليها وتتجاوز أحياناً الحدود الجغرافية فتقع في دولة بينما يعيش المتضرر في دولة أخرى وهو ما يجعلها من أصعب الجرائم تعقيدا في الكشف والإثبات[1812].

وقد برزت خطورة ذلك مع ظهور أساليب عدة لجمع البيانات مثل التصيد الإلكتروني - الهندسة الاجتماعية - تسريب قواعد البيانات من المؤسسات - اختراق الأجهزة الشخصية - واستخدام الذكاء الاصطناعي في انتحال الهوية البصرية والصوتية وقد أثبت الواقع أن مجرد تسرب رقم وطني أو عنوان إلكتروني أو بيانات بنكية بسيطة قد يتيح للجاني فتح حسابات أو طلب تحويلات أو تقديم طلبات رسمية باسم المجني عليه دون علمه ، ومن هنا جاءت الحاجة إلى تحديد مضمون هذه الجريمة بدقة وتوضيح نطاقها والتمييز بينها وبين غيرها من الجرائم القريبة منها وفيما توضيح لتعريف سرقة الهوية ثم تميزها عن غيرها من الجرائم وذلك على النحو التالي:

أولاً: التعريف بجريمة سرقة الهوية

نظرا لحداثة الجريمة وتعدد صورها لا يوجد تعريف واحد متفق عليه لها، بل حاول كل اتجاه فقهي وقانوني الاقتراب من مضمونها حسب الزاوية التي يراها مركزية في الفعل الإجرامي ومن أبرز هذه التعريفات أنها وضع اليد على بيانات تخص شخصاً آخر ثم استخدامها في نشاط غير مشروع مع إيهام الجهات المعنية بأن المستخدم الحقيقي هو صاحب الهوية الأصلي حيث يركز هذا التعريف على عنصر الاستيلاء باعتباره بوابة الجريمة ثم الاستخدام المخادع للبيانات باعتباره محل التجريم الرئيسي[1813].

1812 السليطي، حمد عبد الله حي بو غانم، تجريم الاحتيال الالكتروني في القانون القطري والمقارن، رسالة ماجستير، كلية القانون، جامعة قطر، 2018، ص1.

1813 العصيمي، صالح بن فهد، السياسات الجنائية، تعريفها، ومجالاتها، وتطبيقاتها، مكتبة الملك فهد الوطنية، 2023، ص 101.

جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال
Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

كما تم تعريف سرقة الهوية على أنها استخدام بيانات شخصية صحيحة تخص الغير في سياق غير مشروع سواء حصل الجاني على تلك البيانات عن طريق اختراق، أو تسريب، أو مصادر عامة، أو بوسائل احتيالية ويركز هذا التعريف على فكرة أن محور الجريمة هو استغلال البيانات وليس طريقة الحصول عليها وهو ما يعني أن مجرد استخدام البيانات دون إذن صاحبها يعد جوهر الجريمة، حتى لو لم يسبق ذلك أي اعتداء تقني[1814].

وعرفت كذلك بأنها كل سلوك يهدف إلى الحصول على وسائل التعريف الخاصة بشخص ما واستخدامها لتحقيق منافع مالية أو قانونية أو اجتماعية أو لإيقاع ضرر به مثل الدخول إلى حساباته الدفترية أو طلب خدمات باسمه أو إنشاء التزامات تلحق به، وهذا التعريف يجمع بين عناصر الاستيلاء والاستخدام والغاية الضارة، كما عرفت جريمة سرقة الهوية بأنها فعل يراد منه التعدي على حق الفرد في السيطرة على بياناته لأن هذه السيطرة تمثل الجانب المعنوي للهوية الشخصية وبالتالي فإن أي استخدام غير مرخص للبيانات يشكل اعتداء على شخصية الفرد وليس على أمواله أو ممتلكاته فقط.

وفي ضوء ما سبق يتبين بأن هناك مجموعة من العناصر تشكل الهيكل العام للجريمة أولها موضوع الجريمة وهو البيانات الشخصية التي يمكن أن تشمل الاسم الرقم الوطني البيانات البنكية كلمات المرور الحسابات الحكومية والمالية الرموز السرية بيانات التواصل المعلومات المخزنة لدى المؤسسات التعليمية أو الصحية أو المصرفية، وثانيها فعل وضع اليد ويشمل الحصول على البيانات عبر أي وسيلة سواء كانت تقنية أو اجتماعية أو من خلال التسريب أو الجمع غير المشروع أو حتى عبر الشراء من الأسواق السوداء للبيانات أما العنصر الثالث فيتمثل في الاستخدام في نشاط غير مشروع ويقصد به توظيف البيانات في معاملات أو طلبات أو تصرفات ينتج عنها ضرراً أو منفعة غير مستحقة للجاني، والعنصر الرابع هو النتيجة الضارة وهي الضرر المالي أو القانوني أو الاجتماعي الذي يلحق بالمجني عليه وتشمل الديون الوهمية الالتزامات القانونية العمليات البنكية غير المصرح بها المساس بالسمعة أو تورطه في إجراءات ادارية أو قضائية ليس له علاقة بها[1815].

وتكمن خطورة الجريمة في أن عملية ارتكابها لا تحتاج حضوراً مادياً للجاني فقد يكون في دولة بعيدة وقد يعتمد على تطبيقات آلية أو برمجيات معينة للحصول على البيانات كما أن المجني عليه غالباً لا يعلم بوقوعها إلا بعد مرور وقت طويل حين يفاجأ بمعاملات تمت باسمه أو طلبات لم يقدمها أو التزامات لم يوافق عليه، ولذا فيصعب تحديد بداية الجريمة ومكان وقوعها ووسيلة ارتكابها.

ثانيا تمييز جريمة سرقة الهوية عن غيرها من الجرائم

تتشابه سرقة الهوية مع جرائم أخرى ترتبط بالبيانات أو استخدام الوسائل التقنية، ولذا فإن التمييز بينها وبين تلك الجرائم يعد ضرورياً لعدم الخلط في التكييف القانوني ولتطبيق النصوص المناسبة بدقة ويمكن توضيح ذلك فيما يلي:

1. **التمييز بين سرقة الهوية والاحتيال الالكتروني**

يتمحور الاحتيال الالكتروني حول استخدام وسائل تضليل من أجل إقناع المجني على بتسليم بيانات أو أموال أو اتخاذ إجراء معين طواعية، حيث يقوم الجاني بإيهام الضحية برسالة كاذبة أو موقع مزيف أو وعد غير صحيح من أجل دفعه هو إلى القيام بتصرف ما في حين أن سرقة الهوية لا تعتمد على إرادة المجني عليه ولا تحتاج إلى تضليله بل يكفي أن يحصل الجاني على البيانات من أي مصدر ثم يستخدمها مباشرةً بدون تواصل مع الضحية ومن ثم فإن جوهر الاحتيال هو الاستغلال إرادة المجني عليه بينما فإن جوهر سرقة الهوية هو استغلال شخصيته الرقمية[1816].

2. **التمييز بين سرقة الهوية والتزوير المعلوماتي**

1814 عبد الحق، خالد، وعبد العال، دعاء، الجرائم الالكترونية والتحقيقات الجنائية، دار اليازوري العلمية، 2025، ص 27.

1815 حبابية، ميرفت محمد، مكافحة الجريمة الإلكترونية، دار اليازوري العلمية، 2022، ص 56.

1816 عبد الحق، خالد، وعبد العال، دعاء، المرجع السابق، ص 48.

جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال
Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

التزوير المعلوماتي يقوم على تغيير الحقيقة في محرر أو نظام إلكتروني سواء أكان ذلك عن طريق تعديل البيانات أو محوها أو بإضافة بيانات جديدة ويتمحور جوهره حول التغيير في الوثيقة بينما في سرقة الهوية لا يقوم الجاني عادة بتغيير البيانات، بل يستخدمها كما هي حيث يظل المحرر صحيحاً والبيانات تظل سليمة وقد تكون صادرة من جهة رسمية لكن استخدامها يكون في سياق غير مشروع وهذا الفارق يجعل التزوير اعتداء على الموثوقية بينما سرقة الهوية اعتداء على الشخصية الرقمية[1817].

3. التمييز بين سرقة الهوية والدخول غير المشروع

الدخول غير المشروع هو اقتحام نظام إلكتروني أو جهاز ما دون إذن أو على خلاف شروط الاستخدام وقد يؤدي هذا الدخول إلى الحصول على البيانات لكن وقوع دخول غير مشروع لا يعني بالضرورة وقوع سرقة هوية كما أن سرقة الهوية قد تقع دون دخول غير مشروع لأن البيانات قد تتسرب من مصادر اخرى أو يتداولها الجاني في السوق السوداء أو يحصل عليها من جهة داخلية وهكذا يكون التركيز في الدخول غير المشروع على النظام وليس على الشخص بينما في سرقة الهوية يكون التركيز على البيانات والهوية وليس على النظام الذي يحفظها[1818].

4. التمييز بين سرقة الهوية و انتحال الشخصية

انتحال الشخصية يقوم على تقمص شخصية حقيقية أو وهمية أمام الغير لكن دون ضرورة استخدام بيانات صحيحة فقد يستخدم الجاني اسم شخص دون تفاصيل دقيقة أو يقدم نفسه بهوية كاذبة تماما أما سرقة الهوية فتتعلق باستخدام بيانات حقيقية تخص شخصا قائماً له وجود فعلي وعلى ذلك فكل سرقة هوية تتضمن انتحالاً لكن ليس كل انتحال يتضمن سرقة هوية إذ قد ينتحل الجاني صفة ليست قائمة أو لا تستند إلى بيانات صحيحة[1819].

الفرع الثاني: الخصائص المميزة لجريمة سرقة الهوية

مع زيادة الاعتماد على الأنظمة الرقمية وتوسع التعاملات الإلكترونية باتت الهوية الرقمية امتداداً للشخص في الكثير من شؤون حياته المهنية والمالية والاجتماعية وصار أي اعتداء على هذه الهوية لم يعد مجرد واقعة تقنية وإنما تحول إلى جريمة تمس استقرار حياة الفرد وحقوقه الأساسية ويكتنف جريمة سرقة الهوية مجموعة من الخصائص والتي تميزها عن غيرها من الجرائم المعلوماتية وتتمثل هذه الخصائص فيما يلي:

أولاً: الجريمة تقوم على بيانات غير مادية يسهل تداولها و انتقالها

من أبرز ما يميز جريمة سرقة الهوية أن موضوع الاعتداء فيها هو البيانات الشخصية وهي بيانات غير مادية يمكن نسخها وإرسالها وتخزينها دون أن يظهر أي أثر يدل على عملية النقل وهذا الطابع غير المادي للبيانات يجعل الجريمة أكثر تعقيداً من الجرائم التي يقع الاعتداء فيها على أشياء مادية يمكن تتبعها أو استعادتها. فمجرد حصول الجاني على الاسم الكامل، أو الرقم الشخصي، أو بيانات البطاقة البنكية، أو معلومات الحسابات الإلكترونية يمنحه القدرة على استخدامها في عدة معاملات دون أن ينتقص ذلك من قدرة الضحية على استخدامها في الوقت ذاته وهو ما يشكل فرقاً جوهرياً عن السرقات المادية والتي ينتقل فيها الشيء من يد إلى أخرى كما أن سهولة انتشار البيانات وسرعة انتقالها عبر شبكات مختلفة تجعل من الصعب تحديد اللحظة التي تمت فيها الجريمة أو حصر الأجهزة والوسطاء الذين انتقلت عبرهم المعلومات[1820].

ثانياً: إمكان ارتكاب الجريمة دون وجود صلة مباشرة بين الجاني والضحية

1817 مدين، محمود، الجريمة الالكترونية وتحديات الأمن القومي، المصرية للنشر، 2025، ص 78.

1818 حبابية، ميرفت محمد، المرجع السابق، ص 49.

1819 عبد الحق، خالد، وعبد العال، دعاء، المرجع السابق، ص 48.

1820 الزنداني، إبراهيم محمد، إجراء الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية، جامعة فطاني، 2020، ص 131.

جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال
Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

من الخصائص اللافتة لجريمة سرقة الهوية أن الجاني غالبا لا يحتاج إلى الاتصال المباشر بالضحية أو التواصل معها فقد تتحقق الجريمة من خلال اختراق قاعدة بيانات تابعة لجهة حكومية أو مؤسسة مالية أو نتيجة تسريب داخلي من موظف لديه صلاحيات الاطلاع على السجلات أو عبر مواقع عرض البيانات المسربة أو حتى من خلال تتبع حسابات مفتوحة على شبكات التواصل الاجتماعي. وهذا الانفصال التام بين الجاني والضحية يخلق حالتين خطيرتين: الأولى وهي أن الضحية قد لا تشعر بأي مؤشر يدل على وقوع الجريمة لأسابيع أو أشهر والثانية أن الجاني قد يستغل البيانات في دول أخرى أو عبر منصات خارج الحدود مما يجعل تتبع المسؤولية القانونية أمرا شديد التعقيد، وهذا البعد بين الطرفين يفتح المجال لظهور مجموعات منظمة تعمل على جمع وبيع الهويات المسروقة بحيث يصبح الجاني النهائي الذي يستخدم الهوية مختلفا عن الشخص الذي استولى عليها أول مرة[1821].

ثالثاً: تعدد الأساليب ومرونة الوسائل المستخدمة في ارتكاب الجريمة

تتسم جريمة سرقة الهوية بتنوع طرق ارتكابها وتطورها المستمر فالجاني قد يعتمد على اختراقات تقنية أو على أساليب الهندسة الاجتماعية أو على شراء بيانات مسربة أو على تتبع تفاعلات الأشخاص في المواقع المفتوحة. وقد يكفي أن يستخدم الضحية كلمة مرور موحدة في أكثر من منصة أو يسجل بياناته في موقع غير آمن أو يتفاعل مع رسالة احتيالية مصممة بعناية حتى يحصل الجاني على المعلومات المطلوبة وهذه المرونة في الوسائل تجعل الجريمة قابلة للوقوع حتى مع وجود أنظمة حماية متقدمة لأن العنصر البشري يظل الحلقة الأضعف في كثير من الأحيان حيث يستطيع الجاني استغلال الثقة أو استعجال الشخص أو عدم انتباهه للحصول على ما يريد. وبسبب تعدد هذه الأساليب يصبح من الصعب على التشريعات أن تلاحق التطور التقني بسرعة كافية مما يفرض على مؤسسات الحماية أن تعتمد أساليب أكثر مرونة تتكيف مع المستجدات[1822].

رابعا: صعوبة الكشف عن الجريمة و إثباتها أمام جهات التحقيق والقضاء

سرقة الهوية من الجرائم التي قد تمر لفترة طويلة دون اكتشاف لأن الجاني يتصرف باسم الضحية وببيانات صحيحة مما يجعل المعاملات التي يقوم بها تبدو في ظاهرها سليمة ولا تظهر المشكلة إلا عندما تبلغ الجهة التي تعاملت مع الجاني الضحية بوجود التزامات معلقة أو مبالغ مستحقة أو عند تعرض الضحية لإيقاف خدمة أو رفض معاملة بسبب سجل مالي أو قانوني لم يشارك في تكوينه، كما أن إثبات الجريمة يمثل تحديا كبيرا لأن تتبع أثر البيانات الرقمية يستلزم إجراءات تقنية دقيقة وقد تتداخل عدة جهات في مراحل انتقال المعلومات وتوجد أحيانا عقبات مرتبطة بتبادل البيانات بين الدول أو الشركات الخاصة. وتزداد الصعوبة عندما يستخدم الجاني أدوات لإخفاء هويته أو تمرير معاملاته عبر شبكات متعددة مما يجعل عملية الإثبات تحتاج إلى خبرة فنية وقانونية متخصصة[1823].

المطلب الثاني: أسباب انتشار جريمة سرقة الهوية و آثارها

يتناول هذا المطلب العوامل التي ساهمت في انتشار نطاق جريمة سرقة الهوية وما يرتبط بها من آثار تمس الأفراد والمجتمع والاقتصاد على حد سواء، وعليه فينقسم هذا المطلب إلى فرعين أولهما يتناول الأسباب التقنية والاجتماعية لانتشار الجريمة، وثانيهما يتناول الآثار التي تخلفها الجريمة سواء اقتصادية أو اجتماعية أو فردية.

الفرع الأول: أسباب انتشار جريمة سرقة الهوية (التقنية والاجتماعية)

تعد جريمة سرقة الهوية من أكثر الجرائم انتشارا في البيئة الرقمية الحديثة نظرا لتداخل عوامل تقنية واجتماعية جعلت هذا الفعل غير المشروع يجد لنفسه بيئة خصبة تسمح بوقوعه وتعدد صوره وتطور أساليبه بصورة دائمة، ومع التحول الواسع نحو الخدمات الإلكترونية واعتماد الأفراد والمؤسسات على النظم الرقمية في إجراء معاملاتهم اليومية برزت مجموعة من الأسباب التي

1821 العازمي، فيصل جعلان، إشكالية الملاحقة الجزائية في الجرائم الإلكترونية، ع39، 2024، ص 781.

1822 سلامة، مأمون محمد، شرح قانون العقوبات، القسم العام، دار النهضة العربية، 2003، ص 80.

1823 المناعسة، أسامة أحمد، جرائم الحاسب الآلي والانترنت، دراسة تحليلية مقارنة، دار وائل للنشر، 2001، ص107.

جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال
Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

أسهمت بشكل مباشر في توسع نطاق هذه الجريمة سواء من خلال توفير ادوات التنفيذ التقنية أو من خلال خلق ظروف اجتماعية تزيد من هشاشة المستخدمين وقدرتهم المحدودة على حماية بياناتهم الشخصية.

أولاً: الأسباب التقنية

1. تطور ادوات الاختراق

شهد العالم خلال السنوات الاخيرة قفزة كبيرة في برمجيات الاختراق والأدوات المستخدمة في تحليل البيانات والتنقيب عنها وبات في مقدور الأشخاص الذين يمتلكون معرفة تقنية متوسطة الحصول على برامج تمكنهم من كسر كلمات المرور أو اعتراض الاتصالات الرقمية أو تحليل قواعد البيانات المتاحة على الشبكة، وقد انتشرت هذه الادوات على منصات متعددة بعضها يقدم نسخا مجانية أو منخفضة التكلفة مما ساهم في تخفيض العوائق امام الجناة وزاد من قدرة الاشخاص العاديين على الدخول في هذا النوع من السلوك الاجرامي دون الحاجة لخبرة متقدمة، ويؤدي ذلك في النهاية إلى تسهيل عمليات الاستيلاء على البيانات الشخصية وسرقة الهويات الرقمية بمختلف صورها[1824]

2. تعدد الثغرات في المنصات الإلكترونية

تعتمد العديد من المواقع والتطبيقات والخدمات الإلكترونية على نظم حماية تقليدية لا تواكب سرعة تطور الاساليب التي يستعملها المهاجمون، وتسمح هذه الثغرات للمخترقين بالوصول إلى البيانات الشخصية المخزنة على خوادم المؤسسات سواء كانت بيانات مصرفية أو سجلات حسابات أو معلومات اتصال، وقد أثبتت التجارب ان بعض الشركات لا تقوم بتحديث انظمتها الامنية بشكل دوري مما يجعلها عرضة للاختراق ويتيح للجناة الحصول على كميات كبيرة من البيانات التي يتم توظيفها لاحقا في عمليات سرقة الهوية[1825].

3. توسع استخدام تقنيات التواصل السحابية

صار تخزين البيانات عبر الخدمات السحابية ممارسة واسعة لا تقتصر على المؤسسات بل تشمل الأفراد ايضا وهو ما يعني تمركز كميات هائلة من المعلومات في بيئات رقمية يجري الوصول اليها عبر الانترنت وعلى الرغم من المزايا الكبيرة لهذه التقنية الا ان توسعها جعل تلك البيانات هدفا ثمينا للمخترقين بسبب تركيزها في اماكن محددة يمكن مهاجمتها من اي مكان في العالم، وبهذا بات الجاني لا يحتاج إلى الوصول المادي لأجهزة الضحية بل أصبح يستطيع جمع بياناته من منصات التخزين السحابية اذا ما توفرت ثغرة تقنية يتم استغلالها لهذا الغرض[1826].

4. ضعف الوعي بالأمن الرقمي

تختلف درجة الوعي الأمني بين المستخدمين الامر الذي يخلق ثغرات واسعة يستغلها الجناة فكثير من الأفراد يلجؤون إلى كلمات مرور سهلة أو يعيدون استخدام ذات الكلمة في أكثر من حساب أو يقومون بتخزين معلوماتهم الحساسة على اجهزة غير مؤمنة، كما ان عددا كبيرا من المستخدمين يتجاهل إجراءات التحقق الثنائي التي توفر طبقة اضافية من الحماية وبالتالي يصبح حسابهم معرضا للاختراق من خلال وسائل بسيطة، ومن بين الممارسات الشائعة ايضا الضغط على روابط غير موثوقة أو تحميل ملفات مجهولة المصدر دون التحقق من مشروعيتها وهو ما يسهل لبرامج التجسس جمع البيانات وسرقتها[1827].

5. الانتشار الواسع للذكاء الاصطناعي وتقنيات الانتحال الرقمي

1824 مدين، محمود، المرجع السابق، ص56.

1825 اللقاني، عبد الرحمن على، دور الأمن السيبراني في تعزيز أمن المعلومات المالية الإلكترونية، دار اليازوري العلمية، 2022، ص233.

1826 الدسوقي، نورة عبد الهادي، الذكاء الاصطناعي في مواجهة الأخبار الزائفة، العربي للنشر، 2023، ص32.

1827 سلبي، زهراء عادل، جريمة الابتزاز الإلكتروني، دراسة مقارنة، شركة دار الاكاديميون للنشر، 2021، ص12.

جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال
Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

أوجد التقدم في تقنيات الذكاء الاصطناعي ادوات جديدة يمكن استغلالها في انتحال الهوية سواء عبر توليد صور مزيفة أو تسجيلات صوتية مقلدة أو رسائل تحمل اساليب معقدة يصعب على المستخدم التمييز بينها وبين الرسائل الحقيقية وقد اسهم هذا التطور في تسهيل أعمال الاحتيال من خلال خلق بيئات رقمية تحاكي الحسابات الاصلية للضحايا بما يؤدي إلى خداع المستخدمين أو المؤسسات وتحقيق الجريمة دون الحاجة إلى تدخل مادي مباشر.[1828]

ثانياً: الأسباب الاجتماعية

1. زيادة الاعتماد على المعاملات الإلكترونية

فرضت التحولات الاقتصادية والاجتماعية نمطاً جديداً يقوم على انجاز المعاملات عبر الانترنت بدءاً من التسوق الإلكتروني مروراً بالخدمات البنكية وصولاً إلى الخدمات الحكومية ومع هذا التحول أصبح الأفراد يضعون كما كبيراً من بياناتهم الشخصية على منصات متعددة قد لا تتمتع كلها بمستوى الحماية ذاته. وأدى هذا الاعتماد الواسع إلى اتساع مساحة تعرض المستخدمين للجرائم الرقمية ومن بينها جريمة سرقة الهوية[1829].

2. السلوكيات الرقمية غير المنضبطة

تتسم الحياة الاجتماعية الحديثة بحضور مكثف على منصات التواصل الاجتماعي حيث يقوم المستخدمون بمشاركة معلومات كثيرة عن حياتهم اليومية وبياناتهم الشخصية وصورهم ومعلومات الاتصال الخاصة بهم، وقد وجدت الجريمة في هذا السلوك بيئة غنية تسمح للجاني بتجميع معلومات تكفي لانتحال شخصية الضحية أو دخول حساباته. كما ان بعض الأفراد يعرضون بياناتهم عن غير قصد من خلال الاشتراك في تطبيقات مجهولة أو مسابقات عبر الانترنت توفر للجناة مدخلا ملائماً لجمع البيانات[1830].

3. ضعف الثقافة القانونية

حيث إن الكثير من الأفراد يجهل بطبيعة مخاطر جريمة سرقة الهوية والعقوبات التي ترتبط بها وسبل الوقاية منها ويؤدي هذا الجهل إلى التساهل في التعامل مع البيانات الشخصية أو قبول شروط استخدام منصات رقمية دون قراءتها أو معرفة ما تتضمنه من مخاطر فضعف الوعي القانوني يجعل المستخدم غير مدرك لما يمكن ان يترتب على افشاء بيانات بسيطة قد تبدو غير مهمة لكنها في الواقع تمثل خيطاً رئيسياً لبناء ملف كامل للضحية[1831].

4. تغير أنماط الحياة وازدياد الضغوط الاجتماعية

مع تسارع وتيرة الحياة أصبح الأفراد يعتمدون على السرعة في التعامل مع الخدمات الإلكترونية مما يقلل من حرصهم على التحقق من الروابط والمواقع، كما أن ضغوط الحياة تجعل البعض يبحث عن حلول سريعة مثل التسجيل في مواقع غير موثوقة أو استخدام شبكات الاتصال اللاسلكي Wi-Fi عامة لا توفر الحماية المطلوبة وهو ما يزيد فرص كشف البيانات الشخصية[1832].

5. تنامي الاقتصاد الرقمي و انتشار الاسواق الموازية

انتشرت على شبكة الإنترنت منصات تبيع بيانات شخصية مسروقة وبطاقات مصرفية وهو ما خلق سوقاً موازية لبيع الهويات، ووجود هذه السوق شجع الجناة على القيام بعمليات اختراق متكررة لبيع البيانات وتحقيق مكاسب مالية كبيرة دون الحاجة إلى

1828 المايل، عبد السلام محمد، والشربجي، عادل محمد، الجريمة الإلكترونية في الفضاء الإلكتروني، مجلة أفاق للبحوث والدراسات سداسية، دولية محكمة، المركز الجامعي، ع4، 2019، ص 248.

1829 عبد الحق، خالد، وعبد العال، دعاء، المرجع السابق، ص 112.

1830 عبد السلام، محمد محسن، دور جامعة دمياط في تنمية المواطنة الرقمية، دراسة ميدانية على عينة من طلبة الجامعة، أكتوبر 2023، ص 25.

1831 فرج، همت، دور الثقافة القانونية في تحقيق الأمن الاجتماعي لدى طلاب الجامعة، مجلة كلية التربية ببنها، ع131، يوليو 2022، ص573.

1832 النمر، مصطفي صابر، الدراما الأجنبية وانحرافات المراهقين السلوكية، العربي للنشر والتوزيع، 2016، ص11.

جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال
Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

الاحتفاظ بالبيانات أو استخدامها شخصيا، وترتب على هذا الأمر احاطة البيانات الشخصية بقيمة اقتصادية شجعت على تصاعد معدلات سرقتها.

ويتضح مما سبق أن انتشار جريمة سرقة الهوية لا يعود إلى عامل واحد، بل نتيجة تفاعل معقد بين أسباب تقنية واجتماعية تتشابك فيما بينها لتوفر البيئة الخصبة لهذا النوع من الجرائم مما يجعل مواجهتها تتطلب سياسات شاملة تجمع بين التوعية المجتمعية وتعزيز أمن المعلومات وتطوير الأطر التشريعية القادرة على مواكبة التطور التقني المتسارع[1833].

الفرع الثاني: الآثار المترتبة على الجريمة (الفردية والمجتمعية والاقتصادية)

جريمة سرقة الهوية من الجرائم التي تتجاوز في نتائجها حدود الاستيلاء على بيانات شخصية لتترك خلفها سلسلة من الآثار العميقة التي تطال الفرد والمجتمع والاقتصاد على حد سواء فهذه الجريمة لا تقف عند مرحلة الاستيلاء على البيانات وإنما تمتد إلى استخدام تلك البيانات في اعمال احتيالية أو معاملات وهمية أو ممارسات غير مشروعة قد تحمل الضحية تبعات قانونية ومالية لا علاقة له بها، ومع توسع البيئة الرقمية وانتشار الاعتماد على الهوية الإلكترونية في مختلف أوجه الحياة اصبحت الاثار المترتبة على هذه الجريمة أكثر تعقيدا واشد ضررا مما كانت عليه في السابق.

أولاً: الآثار الفردية

1. الأضرار المالية

والتي تتمثل في الآثار التي يتعرض لها الفرد في الخسائر المالية التي قد تنتج عن استخدام بياناته في تنفيذ عمليات شراء أو تحويلات مالية أو سحب مبالغ من حساباته دون علمه وقد يجد الضحية نفسه في مواجهة التزامات مالية ضخمة نتيجة معاملات أجراها الجاني مستخدما هويته الرقمية ولا تقتصر الخسائر على ما يتم الاستيلاء عليه مباشرة من أموال، بل تشمل أيضا ما يتحمله الفرد من تكاليف لإعادة ضبط حساباته واستعادة السيطرة على بياناته وإثبات عدم مسؤوليته عن التصرفات التي قام بها الجاني.

2. الأضرار المعنوية والنفسية

إن الضحية إذا ما سرقة هويته فإنه يتعرض لقدر كبير من الاضطراب النفسي نتيجة اختراق خصوصيته ووضعه في موقف العاجز عن حماية بياناته الشخصية ويشعر كثيرون بفقدان الأمان وبالخوف من تكرار الحادثة مما يؤثر على ثقتهم في استخدام الانترنت أو التعامل مع الخدمات الإلكترونية وفي بعض الحالات يؤدي الامر إلى مشكلات اجتماعية وأسرية عندما يتم استخدام الهوية المسروقة في مراسلات مخلة أو ممارسات قد تتسبب في تشويه السمعة، كما قد يواجه الضحية معاناة نفسية طويلة نتيجة اضطراره للتعامل مع الجهات الرسمية والمصرفية لتصحيح اثار الجريمة وإثبات براءته[1834].

3. الآثار القانونية والإدارية

جريمة سرقة الهوية من الجرائم التي قد تقحم الضحية في مشكلات قانونية عندما يستخدم الجاني الهوية المسروقة في ارتكاب أفعال غير مشروعة مثل الاحتيال أو التعاقد باسم الضحية أو ارتكاب مخالفات وقد يتلقى الضحية اشعارات قانونية أو مطالبات مالية أو استدعاءات قضائية بسبب تصرفات لم يقم بها مما يضعه في مواجهة إجراءات تحقيق أو مساءلة قد تستغرق وقتا طويلاً، ويترتب على ذلك تعطيل مصالحه وتقييد حركته ووقوع اضرار إدارية مثل تعطيل الخدمات التي ترتبط ببياناته أو تعليق بعض معاملاته الرسمية إلى حين حل الاشكاليات.

4. المساس بالخصوصية

تعتبر الخصوصية من أكثر الحقوق الفردية تأثراً بهذه الجريمة حيث يتمكن الجاني من الاطلاع على معلومات شخصية قد تتضمن بيانات عائلية ووثائق خاصة وسجلات طبية أو مصرفية ومثل هذا الاطلاع غير المشروع يضع الضحية في حالة انكشاف تام يمكن

1833 بختة، بظاهر، توجهات الاقتصاد الرقمي في البلدان العربية في ظل رغبتها في تطبيقه، مجلة المنتدى للدراسات والأبحاث الاقتصادية، مج2، 2019، ص150.

1834 عبد الحق، خالد، وعبد العال، دعاء، المرجع السابق، ص 26.

جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال
Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

للجاني استغلاله في الابتزاز أو الضغط النفسي، وفي بعض الحالات قد تنتشر هذه البيانات على منصات متعددة وهو ما يجعل السيطرة عليها أو ازالتها أمراً بالغ الصعوبة[1835].

ثانياً: الأثار المجتمعية

1. تراجع الثقة في المعاملات الرقمية

جريمة سرقة الهوية تؤدي إلى زعزعة ثقة المستخدمين في البيئة الرقمية خصوصا عندما تتكرر حالات الاختراق وتتسع دائرة المتضررين ويؤثر هذا التراجع في الثقة بشكل مباشر على توجهات المجتمع نحو الخدمات الإلكترونية ويحد من إقبال الأفراد على اعتمادها في معاملاتهم اليومية ومع تزايد هذه الحالات قد يتردد المواطنون في استخدام الخدمات المصرفية الإلكترونية أو إجراء عمليات الشراء عبر الانترنت مما يعرقل خطط التحول الرقمي التي تبذل الدول جهودا كبيرة لتحقيقها.

2. زيادة الاعباء على الأجهزة الأمنية والقضائية

تفرض هذه الجريمة ضغوطاً كبيرة على الأجهزة المختصة نظرا لطبيعتها التقنية وحداثة اساليب ارتكابها وتتطلب عمليات التحقيق والتتبع جهدا مكثفا وادوات فنية متقدمة مما يشكل تحدياً على الجهات الامنية، كما تستقبل المحاكم عدداً متزايداً من القضايا المتعلقة بهذه الجريمة والتي تتسم بالتعقيد وصعوبة الإثبات نظراً لاعتمادها على الأدلة الرقمية ويؤدي ذلك إلى زيادة الإجراءات وتكدس القضايا وتأخر الفصل فيها في بعض الحالات.

ثالثاً: الاثار الاقتصادية

1. تكاليف معالجة الضرر

تتحمل المؤسسات المالية والشركات وشركات الاتصالات جزءً كبيراً من تكاليف تعويض الضحايا أو إصلاح الخسائر الناتجة عن استغلال بياناتهم وتشمل هذه التكاليف تحديث نظم الحماية وتطوير برامج الكشف المبكر عن الاختراقات وتوظيف خبراء امن المعلومات، كما تتحمل الدول نفقات اضافية لتطوير التشريعات والآليات التقنية اللازمة لمواجهة الجريمة وملاحقة مرتكبيها.

2. الآثار السلبية على بيئة الاستثمار

مع انتشار هذه الجريمة يشعر المستثمرون بأن السوق الرقمية المحلية لا توفر الحماية الكافية للبيانات الشخصية أو أن معدلات الجريمة الإلكترونية مرتفعة فإن ذلك ينعكس على قراراتهم الاستثمارية، ويؤدي هذا الشعور إلى تراجع الاستثمارات خصوصاً في القطاعات المرتبطة بالتكنولوجيا والخدمات المالية ومن ثم يؤثر في معدلات النمو الاقتصادي.

المبحث الثاني: التنظيم القانوني الوطني لجريمة سرقة الهوية

يسعي هذا المبحث إلى بيان الإطار القانوني المنظم لجريمة سرقة الهوية بداخل بعض النظم الوطنية عن طريق تحليل موقع الجريمة في التشريعات الجنائية والقوانين الخاصة المعنية بمكافحة الجرائم الإلكترونية، كما يهدف المبحث إلى بيان مدى جاهزية النصوص الحالية وقدرتها على مواجهة التطورات المتسارعة في أساليب الاعتداء على الهوية الرقمية.

وعليه سيتم تقسيم هذا المبحث إلى مطلبين رئيسيين أولهما يتناول التنظيم التشريعي لجريمة سرقة الهوية في قانون العقوبات ومدى قدرته على استيعاب صور الجريمة الحديثة، بينما يركز المطلب الثاني على النصوص الخاصة في قوانين مكافحة الجرائم الإلكترونية وما تضمنته من تطبيقات قضائية وعملية.

المطلب الأول: التنظيم التشريعي لجريمة سرقة الهوية في القانون الجنائي

يسعي هذا البحث إلى بيان الإطار التشريعي الذي يتعامل من خلال القانون الجنائي مع جريمة سرقة الهوية وذلك عن طريق دراسة النصوص العقابية التقليدية ومدى قدرتها على استيعاب هذا النمط المستحدث من الجرائم الرقمية، ويكشف هذا التحليل عن موقع الجريمة ضمن البناء القانوني العام وما يطرحه هذا من تحديات تشريعية تستلزم المراجعة والتطوير.

1835 الزنداني، ابراهيم محمد، والزنداني، بكيل أحمد، الجرائم السيبرانية ودور السياسة الجنائية في مواجهتها والحد منها، دار الكتب اليمنية، 2021، ص 232.

جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال
Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

وعليه ينقسم هذا المطلب إلى فرعين أولهما يتناول موقف قانون العقوبات من جريمة سرقة الهوية بينما يتناول الفرع الثاني مدى كفاية النصوص التقليدية في مواجهة صور الجريمة الحديثة واتساع نطاقها التقني.

الفرع الأول: موقف قانون العقوبات من جريمة سرقة الهوية

يمثل قانون العقوبات القطري (القانون رقم 11 لسنة 2004) الإطار التشريعي الجنائي العام الذي يجرم مجموعة من الأفعال المرتبطة بانتحال الهوية أو استخدام بيانات الغير وإن لم يرد فيه مسمى صريح «سرقة الهوية الرقمية» كما نراه اليوم حيث تطرق القانون إلى أفعال انتحال الشخصية أو استعمال بيانات الغير عبر نصوص متعددة، ويضع عقوبات متنوعة تتناسب مع طبيعة الأفعال المرتكبة.

أولاً: انتحال الصفة والاسم

ينص قانون العقوبات القطري في المادة 209 على أنه "يعاقب بالحبس مدة لا تجاوز سنتين، وبالغرامة التي لا تزيد على عشرة آلاف ريال أو بإحدى هاتين العقوبتين كل من انتحل اسماً غير اسمه، ولو كان الاسم وهمياً أمام إحدى الجهات القضائية أو سلطات التحقيق" وهذا النص يجرم استخدام هوية غير حقيقية أو اسم غير صحيح أمام السلطات، وهو ما يتقاطع جزئياً مع بعض صور جريمة سرقة الهوية حين يدعى استخدام بيانات تعريفية لشخص آخر لتحقيق هدف معين[1836].

وفي السياق ذاته وبموازاة انتحال الاسم يحتوي قانون العقوبات القطري على نص في المادة 170 يعاقب من ادعى كونه موظفا عاما دون أن يكون كذلك "إذا ادعى أنه موظف عام وقام بعمل يدخل في اختصاص الموظف الذي انتحل صفته" هذا الفعل هو تمثيل مزور لصفة، ويشبه إلى حد كبير استخدام الجاني لبيانات تعريفية لشخص آخر من أجل تمثيل دوره أمام الآخرين[1837].

ثانياً: التزوير واستعمال المحرر المزور

ينظم قانون العقوبات القطري جريمة التزوير في عدد من مواده، بدءاً بالمادة 204 التي تحدد مفهوم التزوير في المحررات، حيث "يعد التغيير في المحرر من طرق التزوير" عندما يكون التغيير في الكتابة أو الأرقام أو الإمضاء أو ختم أو ما شابه ذلك بقصد استعمال المحرر المزور كمحرر صحيح[1838].

ثم تنص المادة 206 على عقوبة التزوير في المحرر الرسمي "يعاقب بتزوير المستند الرسمي بالحبس مدة تصل إلى عشرة سنوات"، بينما إذا ارتكب موظف عام التزوير أثناء تأدية عمله فإن العقوبة قد تصل إلى خمسة عشر سنة[1839].

بالإضافة إلى ذلك تنص المادة 210 من القانون نفسه على جزاء من "يستخدم محررا صحيحا باسم شخص غيره أو ينتفع به بغير حق" أي أن استعمال محرر سليم باسم شخص آخر قد يعاقب عليه، هذا النص مهم جداً من منظور سرقة الهوية لأنه يعترف بأن استخدام محرر سليم (وليس بالضرورة مزور) باسم شخص آخر يمكن أن يشكل عملاً مجرماً في ظل القانون الجنائي القطري[1840].

ثالثاً: الأفعال المرتبطة بالدخول غير المشروع أو استخدام بيانات الغير

يتضمن قانون العقوبات القطري نصاً في الباب المتعلق بـ "الجرائم المتعلقة بالثقة العامة" يتصل باستعمال المحررات المزورة أو بيانات الغير فعلى سبيل المثال تشير المادة 210 إلى استخدام محرر ينتمي للغير وهو ما قد يحدث حين يحصل الجاني على بطاقة تعريف أو مستند لشخص آخر، ثم يستعمله بطريقة غير مشروعة.

1836 المادة 209 من قانون العقوبات القطري رقم 11 لسنة 2004.
1837 المادة 170 من قانون العقوبات القطري رقم 11 لسنة 2004.
1838 المادة 204 من قانون العقوبات القطري رقم 11 لسنة 2004.
1839 المادة 206 من قانون العقوبات القطري رقم 11 لسنة 2004.
1840 المادة 210 من قانون العقوبات القطري رقم 11 لسنة 2004.

جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال
Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

كما أن بعض الفصول في قانون العقوبات تتعلق بالتزوير والأختام والطوابع، مثل المادة 211 التي تجرم تزوير الختم الرسمي والمادة 212 التي تجرم استعمال ختم مزور هذه الأفعال يمكن أن تتقاطع مع استخدام الهوية بصورة غير مشروعة إذا كانت البيانات المستخدمة تتعلق بمستندات رسمية مثل الأختام أو الختم الشخصي أو التوقيع[1841].

رابعاً: العلاقة مع التنظيم الخاص في الجرائم الإلكترونية

الدور الذي تلعبه نصوص قانون العقوبات في معالجة بعض صور سرقة الهوية هو دور تمهيدي إذ تكون الأفعال الأساسية مثل انتحال الاسم أو التزوير أو الاستخدام غير المشروع للبيانات مدرجة ضمن التشريع الجنائي العام في حين أن التشريع المتخصص أي قانون الجرائم الإلكترونية يعالج التفاصيل التقنية المرتبطة بارتكاب الجريمة باستخدام الوسائل الرقمية أو عبر شبكة الإنترنت وهذا التنظيم المزدوج يوضح أن هناك اعتماداً تشريعياً على قانون العقوبات كقاعدة أولية لتجريم الأفعال الأساسية قبل الانتقال إلى تطبيق الأحكام المخصصة للأفعال الرقمية المتقدمة[1842].

خامسا: الوضع في بعض التشريعات الوطنية المقارنة

إذا نظرنا إلى تجارب تشريعية في بعض الدول الأخرى نجد أن بعض النصوص الجنائية التقليدية في هذه الدول أيضاً تغطي أفعالاً مشابهة لسرقة الهوية في بعض التشريعات العربية تم استخدام نصوص عقابية عامة مثل انتحال الصفة أو التزوير للتعامل مع استخدام غير مشروع للبيانات الرقمية قبل صدور قوانين متخصصة وهذا النمط التشريعي يعكس وجهة نظر مشروعة في الاعتماد على قانون العقوبات كخط أول لتجريم أفعال بيانات الهوية ونوضح ذلك فيما يلي:

1. **التشريع المصري**

يتضمن قانون العقوبات المصري نصوصاً تتعلق بانتحال شخصية الغير أو ادعاء الصفة التي لا يستحقها الشخص المنتحل حيث تنص المادة 155 من قانون العقوبات على ما يلي "كل من تدخل في وظيفة من الوظائف العمومية ... من غير أن تكون له صفة رسمية ... يعاقب بالحبس مدة لا تزيد على سنتين، وبغرامة لا تزيد على ألف جنيه، أو بإحدى هاتين العقوبتين"، وهذا النص يجرم انتحال الصفة، حتى إذا كان الاسم أو الصفة مدعى من غير وثائق مادية مزورة، وهو ما يمكن أن يوظف أحياناً في سياق استخدام بيانات تعريفية لشخص آخر[1843].

إضافة فإن القانون المصري يلتفت إلى الانتحال سواء في الصفة أو الاسم، ويضع عقوبات تتفاوت حسب الغرض من الانتحال ونتائجه وهذه العقوبات قد ترتبط بالنصب أو الإضرار بالضحية، أو التمثيل الكاذب الذي قد يعيد بناء هوية رقمية مؤقتة باسم الضحية.

2. **التشريع الأردني**

هناك اهتمام تشريعي واضح بجرائم انتحال الهوية في قانون العقوبات الأردني حيث تضمن مجموعة من الأفعال المتعلقة بذلك سواء عن طريق انتحال الهوية بشكل مباشر أو استخدام بيانات شخص آخر بشكل غير مشروع، وإن لم يستخدم المشرع مصطلح "سرقة الهوية"، إلا ان بعض نصوص قانون العقوبات الأردني توفر الأساس القانوني لمعالجة هذه الجريمة والتي تؤدي إلى ضرر أو منفعة غير مشروعة، حيث تنص المادة 212 بأن كل من استسماه قاض أو ضابط شرطة أو أي موظف من الضابطة العدالة وذكر اسماً أو صفة ليست له أو أدلى بإفادة كاذبة أو هوية أو محل إقامته يتم معاقبته بالحبس مدة لا تزيد على شهر أو بالغرامة، وهذا

1841 المواد 211، و212 من قانون العقوبات القطري رقم 11 لسنة 2004.

1842 محمد، شريف حسين، القانون الواجب التطبيق على الجريمة الإلكترونية، المصرية للنشر والتوزيع، 2021، ص 131.

1843 المادة 155 من قانون العقوبات المصري رقم 58 لسنة 1937.

جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال
Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

النص يعاقب كل من استخدم متعمد هوية غير صحيحة أمام السلطة المختصة سواء أكانت الهوية تخص الجاني نفسه أو شخصاً آخر[1844].

بينما تتوسع المادة 269 فتجرم استعمال الهوية الكاذبة بهدف تحقيق منفعة للجاني أو لغيره أو بهدف الإضرار بحقوق الآخرين، وتفرض عقوبة الحبس من شهر إلى سنة ويتضح من النص بأن المشرع الأردني يربط بين فعل الانتحال والغاية المترتبة عليه سواء أكانت مادية أو معنوية، وهو ما يتوافق مع الطبيعة المتعددة الأبعاد لجريمة سرقة الهوية والتي قد تهدف إلى الاحتيال المالي أو إلحاق الضرر المعنوي بالمجني عليه[1845].

وقد أكملت المادة 270 هذا السياق حيث فرضت ذات العقوبة على كل شخص يعرف علماً بالهوية الكاذبة التي يدلي بها غيره أمام السلطات العامة وهو ما يبرز مسؤولية الأطراف المساعدة أو المتواطئة في الجريمة، وهذا النص يوضح بأن المشرع قانون العقوبات الأردني يقتصر على معاقبة مرتكب الفعل الرئيسي، وإنما يمتد إلى الأشخاص الذين يستخدمون أو يساهمون في استخدام الهوية الكاذبة وهو ما يعزز من قدرة القانون على محاصرة الجريمة بمختلف أشكالها[1846].

3. استنتاج من المقارنة التشريعية

من خلال مقارنة هذه التشريعات يتبين بأن التشريعات الثلاث تتشابه في معالجة الانتحال عبر نصوص عامة حول التزوير والانتحال، حيث توجد مواد محددة تتعلق باستخدام البيانات الشخصية، وهذا النهج يمثل السياسة التشريعية المعتدلة والتي تسمح للقضاء بمرونة في التعامل مع الحالات الجديدة من الانتحال أو سرقة الهوية، مع الحفاظ على الأسس التقليدية في إثبات الجريمة وتحديد العقوبة.

الفرع الثاني: مدى كفاية النصوص التقليدية في مواجهة صور الجريمة الحديثة

مع التطورات التكنولوجية المتسارعة عرف العالم جرائم جديدة تتعلق بسرقة الهوية الرقمية، وباتت تمثل تحدياً أمام النصوص الجنائية التقليدية التي صممت في إطار الأفعال المادية التقليدية. وعلى الرغم من أن النصوص القديمة تمثل الأساس القانوني لمعالجة الأفعال غير المشروعة، إلا أنها باتت تواجه صعوبة كبيرة في التكيف مع التعقيدات التقنية الحديثة، مثل الاستيلاء على البيانات الرقمية، استخدام المعلومات الشخصية في الإنترنت، وانتحال هوية الأفراد عبر الوسائل الرقمية.

ويمكن تحليل مدى كفاية النصوص التقليدية في مواجهة سرقة الهوية الرقمية من خلال الأوجه التالية:

أولا: النصوص التقليدية تتعامل مع الجرائم ذو الطبيعة المادية لا التقنية

النصوص الجنائية التقليدية تركز عادة على الأفعال المادية الملموسة، مثل التزوير في المستندات الورقية أو السرقة المادية للأموال أو الممتلكات وهذه الفرضية القانونية تواجه قيوداً كبيرة عند تطبيقها على الجرائم الرقمية، لأن سرقة الهوية الرقمية لا تنطوي بالضرورة على فقدان مادي ملموس، حيث قد يحصل الجاني على بيانات تعريفية أو مالية لشخص آخر ويستخدمها لإجراء معاملات مالية أو فتح حسابات إلكترونية، دون أن يكون هناك أي فقد مادي مباشر للضحية، وفي تلك الحالة يبرز التحدي الأساسي للنصوص التقليدية، إذ أن تعريف الفعل المادي لم يشمل طبيعة البيانات الرقمية، التي يمكن تكرارها ونقلها بلا قيود، ما يجعل الإطار التقليدي غير ملائم لملاحقة هذه الجرائم إلا إذا تم تكييفه عبر الاجتهاد القضائي أو من خلال تفسير موسع للمواد المتعلقة بالتزوير أو انتحال الصفة[1847].

ثانيا: عنصر القصد في سرقة الهوية الرقمية يتسم بالتعقيد

1844 المادة 212 من قانون العقوبات الأردني رقم 16 لسنة 1960.

1845 المادة 269 من قانون العقوبات الأردني رقم 16 لسنة 1960.

1846 المادة 270 من قانون العقوبات الأردني رقم 16 لسنة 1960.

1847 سكيكر، محمد على، الجريمة المعلوماتية وكيفية التصدي لها، كتاب الجمهورية، 2010، ص 131.

ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

النصوص القانونية التقليدية تشترط في الغالب وجود نية الاحتيال أو تحقيق منفعة غير مشروعة لإثبات الجريمة. في حالة الجرائم الرقمية، يمكن أن تكون النية أكثر تعقيداً ومثال لهذا أن يقوم الجاني بانتحال هوية شخص آخر لأغراض تقنية، مثل اختبار النظام الأمني لمؤسسة أو الوصول إلى معلومات لاستخدامها لاحقاً، دون أن تكون هناك منفعة مالية مباشرة أو ضرر مادي واضح في البداية. هذه الحالات توضح محدودية النصوص التقليدية، لأنها تفترض أن الغرض من الفعل هو تحقيق منفعة محددة أو إلحاق ضرر ملموس، بينما الجرائم الرقمية غالباً ما تنشأ عن استخدام معلومات بطريقة افتراضية قبل أن تتطور إلى أضرار مادية أو معنوية لاحقة، وهذا يجعل من الضروري تفسير النصوص التقليدية بشكل موسع، وربطها بالغاية من الفعل ومدى تأثيره على الضحية[1848].

ثالثاً: اختلاف طريق إثبات سرقة الهوية كجريمة رقمية

تستند النصوص التقليدية إلى أدلة ملموسة مثل المستندات الورقية، التوقيعات، أو الحضور الشخصي لإثبات ارتكاب الجريمة أما الجرائم الرقمية، فهي تتطلب نوعاً مختلفاً من الأدلة، تشمل سجلات الدخول إلى الأنظمة، نسخ من البيانات الرقمية، رسائل البريد الإلكتروني، أو سجلات المعاملات الإلكترونية، كما أن غياب قواعد واضحة في النصوص التقليدية لمعالجة الأدلة الرقمية يحد من قدرتها على إثبات الجرائم أو حماية حقوق المجني عليهم، ومثال لهذا أن قانون العقوبات الأردني يجرم الانتحال واستخدام هوية كاذبة، لكن النصوص لا تتناول بشكل محدد كيفية التعامل مع الأدلة الرقمية، مثل سجلات السيرفرات أو البيانات المخزنة في السحابة الإلكترونية، وهذا الفراغ التشريعي يجعل من الضروري وجود تدابير قانونية وإجرائية لتحديد شروط جمع الأدلة الرقمية، حفظها، والتحقق من صحتها لضمان قبولها أمام القضاء.[1849]

رابعا: الإقليمية كعائق أمام النصوص التقليدية

النصوص التقليدية غالباً ما تتعامل ضمن نطاق الدولة وحدودها الإقليمية، ما يخلق تحديات كبيرة عند مواجهة الجرائم الرقمية العابرة للحدود. سرقة الهوية الرقمية يمكن أن تنفذ من أي دولة في العالم عبر خوادم مختلفة، ويكون الجاني موجوداً في دولة مختلفة عن الضحية، وهذا الوضع يتطلب نصوصاً قانونية محددة للتعاون الدولي، مثل اتفاقيات تبادل الأدلة، المساعدة القضائية، وتسليم المتهمين، وهو ما تفتقر إليه النصوص التقليدية في كثير من التشريعات، وهنا يظهر جليا أن النصوص القديمة وحدها لا تكفي لمواجهة الطبيعة العابرة للحدود لهذه الجرائم، وأن التحديث التشريعي وإدماج آليات التعاون الدولي أصبح ضرورة حتمية.[1850]

خامسا: التدرج العقابي وملاءمته للخطورة

العقوبات في النصوص التقليدية غالبا ما تكون محدودة، مثل الحبس لفترات قصيرة أو الغرامات المالية المحددة، ولا تعكس خطورة الجرائم الرقمية الحديثة. سرقة الهوية الرقمية يمكن أن تؤدي إلى أضرار مالية جسيمة، خسائر سمعة مستمرة، أو فتح المجال لارتكاب جرائم أكبر مثل الاحتيال البنكي أو الابتزاز وهذه العقوبات التقليدية لا تشكل رادعا كافياً للجناة في ظل هذه المخاطر العالية، مما يبرز الحاجة إلى إعادة تقييم العقوبات بما يتناسب مع شدة الأضرار والتأثيرات المحتملة للجرائم الرقمية على الأفراد والمؤسسات والمجتمع. إضافة إلى ذلك، يمثل غياب التخصص التقني لدى القضاة وأجهزة التحقيق تحدياً إضافياً، حيث تتطلب الجرائم الرقمية فهماً دقيقاً لتقنيات القرصنة، أدوات الانتحال، والطرق التي يستخدمها الجناة لاستغلال البيانات الرقمية فهذه النصوص التقليدية لم تضع آليات لتعزيز هذه الخبرة وهو ما يزيد من صعوبة تطبيق القانون بالشكل الأمثل ويحد من فعالية الردع.

1848 الشعار، خالد على نزال، التحقيق الجنائي في الجرائم الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، 2022، ص 19.

1849 العازمي، فيصل جعلان، المرجع السابق، ص 781.

1850 العازمي، فيصل جعلان، المرجع السابق، ص 779.

Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

كما أن النصوص التقليدية تفتقر إلى آليات وقائية حديثة، مثل فرض معايير لحماية البيانات الشخصية على المؤسسات مع إلزام مزودي الخدمات الرقمية بتطبيق معايير أمنية، أو التبليغ الفوري عن أي اختراق وهذه الآليات ضرورية لمنع وقوع الجرائم الرقمية قبل حدوثها، وهو جانب غير مغطى في القوانين الجنائية التقليدية، التي تركز على العقاب بعد وقوع الجريمة وليس الوقاية منها[1851].

وفي ضوء ما سبق يتضح أن النصوص التقليدية تقدم قاعدة أساسية لتجريم بعض مظاهر سرقة الهوية، لكنها غير كافية بمفردها لمواجهة التعقيدات الحديثة ومن ثم تكون هناك حاجة ملحة لتطوير تشريعات متخصصة تشمل التعريفات الرقمية، أساليب الإثبات، العقوبات الملائمة، والتعاون الدولي، مع دمج تدابير وقائية تهدف إلى حماية البيانات ومنع استغلالها، لضمان فعالية الردع وتحقيق الحماية الكاملة للأفراد والمجتمع.

المطلب الثاني: التنظيم التشريعي في قوانين مكافحة الجرائم الإلكترونية

يسعى هذا النص إلى دراسة التنظيم القانوني لجريمة سرقة الهوية في قوانين مكافحة الجرائم الإلكترونية حيث يركز على النصوص القانونية المتخصصة في مكافحة الجرائم الإلكترونية والتي تهدف إلى سد الثغرات التي ظهرت في النصوص التقليدية ويهدف المطلب إلى تحليل المواد القانونية الوطنية المتعلقة بسرقة الهوية الرقمية وبيان كيفية تطبيقها من خلال الممارسات القضائية المحلية وللإلمام بذلك سيتم تقسيم هذا المطلب إلى فرعين رئيسيين الأول يتناول التحليل التفصيلي للنصوص القانونية والثاني يستعرض التطبيقات القضائية والوطنية لهذه النصوص.

الفرع الأول: تحليل النصوص القانونية الخاصة بسرقة الهوية في التشريعات الوطنية

تنظيم جريمة سرقة الهوية في التشريعات الوطنية خطوة ضرورية في مواجهة التحولات المتلاحقة في بيئة التعامل الرقمي وما ينشأ عنها من مخاطر تمس الثقة في المعاملات الإلكترونية ففي ظل انتشار التعامل عبر المنصات الرقمية وتوسع الاعتماد على البيانات الشخصية في خدمات الدولة والقطاع الخاص اصبحت الهوية الرقمية مدخلاً رئيسياً للثقة وللمنفعة معاً الأمر الذي يجعل الاعتداء عليها فعلاً ذو خطورة متزايدة يقتضي معالجة خاصة.

وتكشف قراءة النصوص التشريعية في قطر ومصر والاردن أن كل نظام اختار منهجاً مختلفاً في ضبط الفعل الإجرامي بين من يقرر نصاً مباشراً يجرم انتحال الهوية الإلكترونية وبين من يعتمد الصياغات العامة التي تغطي السلوك ولو لم يرد ذكر هوية الفرد بشكل صريح.

أولاً: التنظيم التشريعي لجريمة سرقة الهوية في القانون القطري

يعد القانون القطري لمكافحة الجرائم الإلكترونية من أكثر التشريعات العربية وضوحاً في النص على تجريم انتحال الهوية باستخدام الوسائل التقنية فقد أفرد المشرع نصاً خاصاً في المادة 11 التي تعد من أهم المواد في ضبط هذا النوع من الاعتداء، وتنص الفقرة الأولى من المادة 11 على معاقبة كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في انتحال هوية لشخص طبيعي أو معنوي وهي صياغة مباشرة لا تحتمل التأويل وتسمح بتجريم السلوك بمجرد توافر واقعة ادعاء شخصية الغير عبر وسيلة تقنية ما دون الحاجة إلى تحقق ضرر فعلي[1852].

ويكشف هذا التوجه ان المشرع ينظر إلى الهوية الرقمية باعتبارها قيمة قائمة بذاتها وأن الاعتداء عليها يهدد الثقة الاجتماعية والاقتصادية، كما تأتي الفقرة الثانية من المادة نفسها لتغطي صورة اخرى من صور الاعتداء قريبة الصلة بسرقة الهوية وهي استخدام الاسم الكاذب أو الصفة غير الصحيحة للاستيلاء على المال أو على السند أو على التوقيع وهي حالة احتيال الكتروني ترتبط عادة باستخدام معطيات هوية غير صحيحة.

1851 ابراهيم، مني غازي حسان، فعالية السياسة الجنائية في مواجهة الجرائم المعلوماتية، دراسة مقارنة في ضوء متطلبات الأمن السيبراني، مجلة الشريعة والقانون، ع45، مايو 2025، ص 2652.

1852 المادة (11) من قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014.

جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال
Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

ومن خلال الجمع بين الفقرتين يتبين أن البناء التشريعي في القانون القطري يوفر حماية مزدوجة تشمل الهوية من جهة وتشمل الاثار المترتبة على استخدامها في سياق الاحتيال من جهة اخرى.

كما يمكن ربط المادة 11 بعدد من النصوص الاخرى ذات الصلة التي توسع دائرة الحماية ومنها النص في المادة 3 التي تعاقب على الدخول غير المشروع إلى النظام المعلوماتي إذا اقترن بانتحال شخصية مالك الموقع أو القائم على إدارته وهي فكرة تكشف أن انتحال الشخصية لا يرتبط فقط بالأشخاص الطبيعيين أو المعنويين، بل يمتد إلى الصفات الوظيفية في البيئة الرقمية.

وكذلك ترتبط المواد 2 و3 و4 التي تنظم جرائم الدخول والالتقاط والتنصت بإطار حماية الهوية لأن الكثير من حالات سرقة الهوية تبدأ بالحصول على البيانات عبر دخول أو اعتراض غير مشروع، وتعكس الصياغة القطرية في مجموعها اتجاهاً تشريعياً واضحاً يقوم على الفصل بين الجريمة الاصلية المتمثلة في انتحال الهوية باستخدام الوسائل التقنية وبين الجرائم المرتبطة بها التي قد تتطور إلى احتيال أو تعد على الخصوصية، وهذا الفصل يضمن وضوح الحدود الجنائية ويمنح جهات الضبط سلطات أوسع في وصف الفعل وتكييفه وفقا لوقائع كل حالة[1853].

ثانياً: النصوص المنظمة لسرقة الهوية في التشريع المصري

لم يتضمن قانون مكافحة جرائم تقنية المعلومات المصري نصاً صريحاً يقرر جريمة بعنوان انتحال الهوية الإلكترونية رغم أنه تناول في مواضع متفرقة سلوكاً يتقاطع مع هذا الفعل ويمكن القول أن المشرع المصري اختار بناء تشريع يقوم على تجريم الافعال المؤدية إلى الإضرار بمصالح الأفراد أو بمصالح الدولة دون أن يستقل بنص خاص يتعلق بالهوية الرقمية، ومع ذلك فإن عدداً من المواد يوفر حماية غير مباشرة بالنسبة لتلك الجريمة، ومن أهم النصوص ذات الصلة المادة 23 التي تعاقب على الاستيلاء على اموال الغير بطريق الاحتيال باستخدام الشبكة المعلوماتية وهي صياغة تشمل حالات انتحال الشخصية اذا كانت وسيلة للحصول على منافع مالية أو عينية[1854].

كما ان المادة 24 تعاقب على الاعتداء على البريد الالكتروني أو الحسابات الخاصة وهو ما قد يحدث ضمن سياق الحصول على البيانات اللازمة لانتحال الهوية، وتغطي المادة 25 الاعتداء على حرمة الحياة الخاصة بنشر المعلومات أو الصور وهي من الافعال التي غالبا ما ترتبط باستخدام الحسابات المنتحلة لأغراض المساس بسمعة الضحية ويظهر من تحليل هذه المواد ان التشريع المصري يعتمد فكرة تجريم المآلات أكثر من تجريم الفعل ذاته[1855].

فالمشرع لم يتجه إلى تحديد انتحال الهوية كجريمة قائمة بذاتها، بل فضل تجريم الاضرار التي تتحقق عند استخدام الهوية المنتحلة ورغم أن هذا الاسلوب يضمن تغطية مساحة واسعة من الافعال غير المشروعة إلا انه قد يثير اشكالا في الحالات التي يقع فيها الانتحال دون ان ينتج عنه ضرر محدد وهو ما قد يؤدي إلى افلات بعض السلوكيات من نطاق التجريم.

ثالثاً: تنظيم سرقة الهوية في التشريع الاردني

قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015 من التشريعات الأساسية التي تعالج الجرائم المرتبطة باستخدام التقنية المعلوماتية، ويحتوي على نصوص يمكن ربطها بمفهوم سرقة الهوية أو انتحال الشخصية عبر الوسائط الرقمية حيث أن فحص هذه النصوص يساعد على تحديد مدى قدرة القانون على استيعاب صور الانتحال الرقمي وكيفية معاقبة مرتكبيها في بيئة الإنترنت، فمن النصوص البارزة في القانون ما ورد في المادة (3) التي تجرم الدخول إلى أنظمة المعلومات أو المواقع الإلكترونية بدون تصريح أو بتجاوز تصريح مسموح به، أو الاستمرار في التواجد بعد علم بعدم الحق وفي هذه المادة تبدو صلات قوية مع سرقة الهوية، لأن انتحال الهوية الرقمي غالباً يبدأ بدخول غير مشروع أو استغلال ضعف ضوابط الدخول إلى النظام ليتمكن الجاني من إنشاء

1853 المواد (2،3،4) من قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014.

1854 المادة 23 من قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018.

1855 المادة 24 من قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018.

جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال
Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

حساب باسم شخص آخر، أو الوصول إلى بياناته الشخصية داخل المنصة، ثم استخدامها لتنفيذ عمليات انتحال شخصية. بالإضافة إلى ذلك، تتيح المادة معاقبة من يقوم بالتقاط، أو نسخ، أو تغيير، أو حذف، أو نشر بيانات داخل النظام بعد الدخول غير المصرح به هذه الأشكال من المعالجة توضح أن القانون يعترف بأن الجريمة الرقمية لا تقتصر على مجرد الدخول، بل تشمل استغلال هذا الدخول للوصول إلى بيانات واستخدامها بأغراض غير مشروعة.

كما تنص الفقرة (ج) من المادة الثالثة على معاقبة من يدخل عمداً إلى موقع إلكتروني أو نظام معلوماتي لغايات تشمل "انتحال صفته أو انتحال شخصية صاحبه" وهذا النص واضح جداً فيما يتعلق بالهوية الرقمية؛ فهو يعترف بوجود جريمة تقتضي استخدامها كأداة انتحال، ليس فقط تغيير البيانات، ولكن التصرف باسم شخص آخر داخل النظام نفسه أو في موقع إلكتروني متعلق به فالعقوبة الواردة في المادة تصل إلى الحبس والغرامة مما يضع أسساً لردع تشفير الأفعال التي تستهدف الهوية الرقمية[1856].

كما أن المادة 4 من القانون وسعت نطاق التجريم ليشمل الافعال التي تستهدف البيانات والانظمة وصولا إلى انتحال الصفة أو الشخصية من خلال الشبكة أو نظام المعلومات. ويعد هذا النص من الادوات المباشرة لمواجهة سرقة الهوية الرقمية لان الجاني في العادة يعتمد على برامج أو ادوات تقنية للتلاعب بالبيانات أو نسخها أو استخدامها بما يمكنه من الظهور باسم شخص اخر أو بصفته. ويبين هذا التنظيم ان سرقة الهوية لم تعد ترتبط فقط بالمعطيات التقليدية، بل اصبحت فعلا رقميا محورا يقوم على الدخول غير المصرح والتعديل والاستغلال بهدف تحقيق منفعة أو الاضرار بالغير[1857].

رابعاً: مقارنة بين النماذج التشريعية الثلاثة

في ضوء ما سبق يتضح أن التشريع القطري يمثل النموذج الأكثر اكتمالاً من ناحية وجود نص مباشر وصريح على انتحال الهوية عبر الوسائل التقنية، وهذا النص يمنح السلطة القضائية قدرة مستقلة على التعامل مع الجريمة دون الحاجة لإثبات نتائجها. بينما يذهب التشريع المصري إلى معالجة الفعل من خلال النصوص المرتبطة بالاحتيال أو الاعتداء على الخصوصية دون تخصيص نص مستقل سرقة الهوية أما التشريع الاردني فيوازن بين النصوص التقليدية والنصوص الرقمية وهو ما يجعل البنية التشريعية أكثر تماسكا من الناحية العملية لكنها قد تتطلب جهداً أكبر في عملية التكييف القانوني.

الفرع الثاني: تطبيقات قضائية ووطنية متعلقة بجريمة سرقة الهوية

تظهر التطبيقات القضائية أهميتها في الكشف عن الكيفية التي يتعامل بها القضاء مع وقائع سرقة الهوية سواء تمت بوسائل تقليدية أو عبر الوسائط الرقمية الحديثة حيث تسهم هذه التطبيقات في رسم ملامح التفسير القضائي للنصوص ذات الصلة وتوضيح الحدود التي يقف عندها التجريم والعقاب في ضوء مبدأ الشرعية الجنائية ومقتضيات الدقة في تحديد الفعل المجرم وقد عكست الاحكام الصادرة عن محكمة التمييز اتجاهاً واضحاً يقوم على الالتزام الحرفي بالنص وعدم التوسع في تفسيره وخاصة في القضايا المرتبطة بانتحال الهوية التي تعد من أكثر الجرائم تعقيدا بسبب تعدد صورها واتساع نطاق وسائل ارتكابها.

وقد بين حكم محكمة التمييز الصادر في الطعن رقم 802 لسنة 2022 جلسة 2023/01/16 هذا الاتجاه بصورة جلية حين خلص إلى براءة متهم قدم نفسه بصفة شقيقه عند التقدم لوظيفة حيث اعتبرت المحكمة ان المادة التي اسندت اليه لا تنطبق على الواقعة لان النص جاء محددا بمجالات معينة لا تشمل مثل هذا الفعل واعتبرت المحكمة ان انتحال شخصية الغير خارج اطار الصفات الرسمية والوظيفية لا يدخل ضمن نطاق التجريم الامر الذي يعكس تمسك القضاء بعدم تحميل النص ما لا يحتمل وعدم مد الحظر إلى افعال لم ينص عليها القانون صراحة وهو ما يعد تطبيقا مباشرا لمبدأ لا جريمة ولا عقوبة الا بنص.[1858]

1856 المادة 3/ج من قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015

1857 المادة 4 من قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015

1858 محكمة التمييز القطرية، المواد الجنائية، الطعن رقم 802 لسنة 2022 جلسة 2023/01/16.

جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال
Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

وفي حكم آخر صدر في الطعن 22 لسنة 2022 جلسة 2022/09/29 حيث تناولت المحكمة واقعة انتحال هوية عبر محررات غير رسمية وركزت في تحليلها على بيان عناصر الواقعة وتحديد ما إذا كان ركن الضرر متحققاً حيث شددت على أن القضاء لا يفترض الضرر افتراضاً بل يتعين إثباته بصورة يقينية وإن كل ادعاء يتعلق بالتزوير أو إساءة استخدام البيانات يجب ان يكون مدعوما بوقائع واضحة وادلة فنية تؤكد حصول الاضرار بالفعل وهو ما يظهر حذراً قضائياً في التعامل مع هذا النوع من الجرائم خاصة عندما ترتبط وسائلها بالأنظمة الإلكترونية التي قد تثير التباساً في تحديد طبيعة الفعل المرتكب[1859].

أما حكم محكمة التمييز الصادر في الطعن 143 لسنة 2018 جلسة 2019/01/07 فقد تناول جريمة انتحال الصفة عبر الشبكة المعلوماتية واعتبرها من الجرائم المنصوص عليها صراحة في قانون مكافحة الجرائم الإلكترونية ورفضت المحكمة الدفع بالتصالح لان هذه الجرائم تمس الحقوق المرتبطة بالهوية الرقمية والاعتبار الشخصي وهي من الجرائم التي لا يقبل فيها الصلح لأنها لا تتعلق بمصلحة فردية فحسب، بل تتعلق بحماية الثقة العامة في البيئة الرقمية ومنع استغلالها في الايقاع بالمجني عليهم أو الاضرار بهم[1860].

وفي ضوء هذه الأحكام يتبين أن القضاء الأردني يتعامل مع قضايا سرقة الهوية بمنهج متدرج يقوم على تحليل الواقعة وتحقيق أركان الجريمة بدقة قبل إصدار الحكم وهو منهج يعكس رغبة القضاء في حماية الحقوق دون توسيع نطاق التجريم بصورة تمس مبدأ الشرعية فالهوية بمفهومها التقليدي كانت مرتبطة بالمستندات الرسمية والبيانات الشخصية المباشرة أما في البيئة الرقمية فقد اتسع مفهومها ليشمل الحسابات الإلكترونية وملفات الدخول والبيانات التعريفية التي يستخدمها الأفراد في تعاملاتهم اليومية وهذا التغير فرض على القضاء دورا جديدا يتمثل في تفسير النصوص القائمة بما يتلاءم مع البيئة التقنية دون الخروج عن حدود النصوص التشريعية القائمة.

ويظهر من خلال تتبع اتجاهات محكمة التمييز أن معيار تكييف الفعل هو نقطة الارتكاز الأولى التي ينطلق منها القاضي اذ يميز بدقة بين الانتحال الذي يقع امام السلطات العامة والانتحال الذي يتم بين الأفراد أو في اطار معاملات خاصة وبين الانتحال المتعلق بالمستندات الرسمية والانتحال الذي يتم عبر منصات التواصل الاجتماعي أو المواقع الإلكترونية فالقضاء يعتبر ان لكل صورة طبيعتها القانونية الخاصة ولا يمكن سحب حكم صورة على اخرى دون توافر عناصرها كافة وهو ما يفسر اختلاف النتائج القضائية بين حالات قد تبدو متشابهة للوهلة الأولى لكنها تختلف في بنيتها القانونية أو في توافر ركن القصد الجنائي.

وتكشف بعض الاحكام ان القضاء يركز تركيزاً واضحاً على مسألة القصد الجرمي في جرائم سرقة الهوية حيث لا يكفي مجرد استخدام اسم شخص آخر أو بياناته بل يتعين أن يكون هذا الاستخدام موجها نحو تحقيق منفعة غير مشروعة أو الاضرار بصاحب الهوية فبدون إثبات هذا القصد لا يتحقق الفعل المجرم في نظر القضاء وقد ورد هذا المبدأ في عدد من الاحكام التي أكدت أن مجرد انتحال صفة أو استخدام بيانات دون قصد الاضرار أو الاستفادة لا ينهض إلى مستوى الجريمة وهذا الاتجاه يعكس التزام القضاء بحماية الأفراد من الاتهام دون سند قوي خاصة في الجرائم الإلكترونية التي قد ينشأ البعض منها نتيجة جهل أو سوء استخدام وليس بالضرورة بدافع اجرامي

كما يظهر من تحليل الاتجاه القضائي أن محكمة التمييز تولي أهمية كبيرة للأدلة الفنية ولتقارير الخبرة في القضايا المرتبطة بسرقة الهوية عبر الوسائط الإلكترونية فهذه القضايا غالباً ما تتطلب تتبعاً تقنياً لمسار الدخول إلى الحسابات أو تحليل بصمة الجهاز أو تتبع عنوان الشبكة ولذلك تشدد المحكمة في عدد من احكامها على ضرورة تقديم جهة الادعاء أدلة فنية واضحة وليس مجرد

1859 محكمة التمييز القطرية، المواد الجنائية، الطعن (22) لسنة 2022 جلسة 2022/09/29.

1860 محكمة التمييز القطرية، المواد الجنائية، الطعن (143) لسنة 2018 جلسة 2019/01/07.

Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

افتراضات أو قرائن ضعيفة وهذا التشدد يهدف إلى ضمان عدم إدانة شخص بريء بسبب استخدام مجهول لهويته أو دخول غير مشروع ارتكبه طرف آخر[1861].

كما أكدت التطبيقات القضائية أن القضاء يميز بين انتحال الهوية العادي وانتحال الهوية الذي يتم بهدف ارتكاب جريمة اخرى فاذا تم استخدام هوية شخص ما لارتكاب فعل اشد خطورة مثل الاحتيال أو الحصول على اموال من الغير فان الانتحال يصبح جزءاً من خطة اجرامية أوسع ويعامل القضاء هذه الحالات بجدية أكبر لأنها تمس النظام العام والثقة في المعاملات الإلكترونية اما اذا كان الانتحال محدودا في نطاق ضيق ولا يترتب عليه ضرر ملموس فان المحكمة قد تميل إلى اعتبار الفعل مخالفا بسيطا أو عملا لا تقوم به الجريمة، كما تشير الاحكام ايضاً إلى أن القضاء يسعى إلى بناء توازن بين حماية حقوق الأفراد وبين عدم افراط الدولة في التدخل في الحياة الرقمية فمن جهة يرى القضاء ضرورة تشديد العقوبة على من يتعمد انتحال هوية الغير لتحقيق منافع غير مشروعة أو الاضرار بهم ومن جهة اخرى يحرص على عدم ادانة الأفراد في الحالات التي لا تتوافر فيها العناصر القانونية الكاملة للجريمة وهذا التوازن يعد من اهم ملامح السياسة القضائية في التعامل مع الجرائم المستحدثة[1862].

وفي ضوء هذه التطبيقات يمكن القول ان القضاء يدرك حجم التحديات التي افرزها التطور الرقمي ويعمل تدريجياً على تطوير منهج تفسير النصوص بما يجعلها قابلة للتطبيق على الوقائع الحديثة دون المساس بمبادئ العدالة والشرعية الجنائية كما تعكس هذه الاحكام الحاجة إلى تحديث تشريعي مستمر يعمل على سد الفجوات وتحديد الافعال المجرمة بدقة أكبر لضمان حماية الهوية الرقمية التي باتت جزءاً اساسياً من حياة الأفراد ومعاملاتهم اليومية في العصر الرقمي.

الخاتمة:

التنظيم القانوني لمكافحة جريمة سرقة الهوية يعد محوراً رئيسياً في حماية الأفراد والمؤسسات من الانتهاكات الرقمية، ويظهر من خلال تحليل التشريعات الوطنية، أن هناك توجهاً متزايداً لتغطية كافة صور الجريمة التقليدية والرقمية. وقد كشف المطلب الأول من الدراسة أن النصوص الجنائية التقليدية، رغم أهميتها في معالجة الانتحال والتزوير، تواجه صعوبة في مواجهة التعقيدات الرقمية الحديثة، خصوصاً فيما يتعلق بالبيانات الرقمية والعابرة للحدود والإثبات التقني للقصد والضرر. من جهة أخرى، يظهر المطلب الثاني أن التشريعات المتخصصة في الجرائم الإلكترونية حاولت سد الثغرات عبر نصوص مباشرة، مثل تجريم انتحال الهوية الرقمية، ومعاقبة الاستخدام غير المشروع للبيانات، بما يعزز قدرة الأجهزة القضائية على التعامل مع الوقائع الرقمية بشكل أكثر فعالية.

كما أوضحت التطبيقات القضائية أن القضاة يعتمدون على تكييف النصوص التقليدية والرقمية لتفسير الوقائع الحديثة مع مراعاة مبدأ الشرعية، مع التركيز على إثبات القصد والعنصر الفني للجريمة، واستخدام الأدلة التقنية لإثبات الانتحال أو الدخول غير المشروع. ويبين هذا التوازن بين التشريع التقليدي والمتخصص، وبين النصوص القانونية والتطبيق القضائي، الحاجة إلى تطوير مستمر للتشريعات، وإدراج تعريفات دقيقة للهوية الرقمية، وآليات إثبات مناسبة، وتعاون دولي فعال لمواجهة الطبيعة العابرة للحدود لهذه الجرائم، بما يضمن حماية الأفراد، والمجتمع، والثقة في البيئة الرقمية.

النتائج:

1. النصوص التقليدية في قوانين العقوبات تجرم بعض صور سرقة الهوية لكنها غير كافية لمواجهة الجرائم الرقمية الحديثة.
2. التشريعات المتخصصة في الجرائم الإلكترونية توفر حماية فعالة للهوية الرقمية عبر نصوص واضحة وصريحة.
3. سرقة الهوية الرقمية جريمة معقدة تتطلب فهماً تقنياً من قبل القضاء وأجهزة التحقيق.
4. الأدلة الرقمية ضرورة أساسية لإثبات الجريمة والتمييز بين الانتحال البسيط والانتحال الموجه لأغراض الاحتيال.

1861 العباد، أيمن بن ناصر بن حمد، المسؤولية الجنائية لمستخدمي شبكات التواصل الاجتماعي، مكتبة القانون والاقتصاد، 2015، ص 118.

1862 مدين، محمود، المرجع السابق، ص 295.

Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

5. النصوص التقليدية تركز على الأفعال المادية، بينما الجرائم الرقمية قد تنتج أضراراً غير ملموسة مباشرة.
6. التعاون بين التشريع التقليدي والمتخصص يخلق إطاراً متكاملاً لمواجهة الجريمة.
7. العقوبات التقليدية لم تعد كافية لتحقيق الردع في ظل خطورة الأضرار الرقمية، ما يستلزم تعديلها.
8. التعاون الدولي والإقليمي ضروري لملاحقة الجريمة العابرة للحدود.

التوصيات:

1- يستلزم الواقع العملي تحديث التشريعات الجنائية بصورة دورية لمواكبة التطور التقني، مع اعتماد صياغات مرنة تجرم الأفعال المرتبطة بالاعتداء على البيانات والهوية الرقمية دون التقيد بوسائل تقنية محددة.

2- ينبغي تكييف السياسة العقابية بما يعكس خطورة الجريمة، من خلال الجمع بين العقوبات الأصلية والتكميلية، كالمصادرة والتعويض، بما يحقق الردع الفعلي.

3- يتطلب الحد من هذه الجرائم تعزيز التدابير الوقائية داخل المؤسسات، عبر إلزامها بوضع سياسات فعالة لحماية البيانات وتحمل المسؤولية عند الإهمال.

4- يعد التعاون بين القطاعين العام والخاص ضرورة عملية، لما يوفره من إمكانيات تقنية ومعلوماتية تسهم في رصد الأنشطة المشبوهة والحد من الجرائم.

5- تمثل التوعية المجتمعية أداة أساسية للوقاية، مما يستوجب نشر الثقافة الرقمية وتوضيح أساليب الاحتيال وطرق الحماية بشكل مستمر.

6- يتطلب تعزيز الحماية تطوير البنية التحتية الرقمية، وتطبيق معايير أمن المعلومات، وإنشاء آليات لرصد الهجمات والاستجابة لها.

7- تقتضي مواجهة الجريمة اعتماد نهج متكامل يقوم على التنسيق بين الجهات الوطنية والتعاون الدولي، بما يضمن فعالية المواجهة في مختلف مراحلها.

❖ **قائمة المراجع:**

1. السليطي، حمد عبد الله حي بو غانم، تجريم الاحتيال الالكتروني في القانون القطري والمقارن، رسالة ماجستير، كلية القانون، جامعة قطر، 2018، ص1.
2. العصيمي، صالح بن فهد، السياسات الجنائية، تعريفها، ومجالاتها، وتطبيقاتها، مكتبة الملك فهد الوطنية، 2023، ص 101.
3. عبد الحق، خالد، وعبد العال، دعاء، الجرائم الإلكترونية والتحقيقات الجنائية، دار اليازوري العلمية، 2025، ص 27.
4. حبابية، ميرفت محمد، مكافحة الجريمة الإلكترونية، دار اليازوري العلمية، 2022، ص 56.
5. عبد الحق، خالد، وعبد العال، دعاء، المرجع السابق، ص 48.
6. مدين، محمود، الجريمة الإلكترونية وتحديات الأمن القومي، المصرية للنشر، 2025، ص 78.
7. حبابية، ميرفت محمد، المرجع السابق، ص 49.
8. عبد الحق، خالد، وعبد العال، دعاء، المرجع السابق، ص 48.
9. الزنداني، إبراهيم محمد، إجراء الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية، جامعة فطاني، 2020، ص 131.
10. العازمي، فيصل جعلان، إشكالية الملاحقة الجزائية في الجرائم الإلكترونية، ع39، 2024، ص 781.
11. سلامة، مأمون محمد، شرح قانون العقوبات، القسم العام، دار النهضة العربية، 2003، ص 80.
12. المناعسة، أسامة أحمد، جرائم الحاسب الآلي والانترنت، دراسة تحليلية مقارنة، دار وائل للنشر، 2001، ص107.

13. مدين، محمود، المرجع السابق، ص56.
14. اللقاني، عبد الرحمن على، دور الأمن السيبراني في تعزيز أمن المعلومات المالية الإلكترونية، دار اليازوري العلمية، 2022، ص233.
15. الدسوقي، نورة عبد الهادي، الذكاء الاصطناعي في مواجهة الأخبار الزائفة، العربي للنشر، 2023، ص32.
16. سلبي، زهراء عادل، جريمة الابتزاز الإلكتروني، دراسة مقارنة، شركة دار الاكاديميون للنشر، 2021، ص12.
17. المايل، عبد السلام محمد، والشربجي، عادل محمد، الجريمة الإلكترونية في الفضاء الإلكتروني، مجلة أفاق للبحوث والدراسات سداسية، دولية محكمة، المركز الجامعي، ع4، 2019، ص 248.
18. عبد الحق، خالد، وعبد العال، دعاء، المرجع السابق، ص 112.
19. عبد السلام، محمد محسن، دور جامعة دمياط في تنمية المواطنة الرقمية، دراسة ميدانية على عينة من طلبة الجامعة، أكتوبر 2023، ص 25.
20. فرج، همت، دور الثقافة القانونية في تحقيق الأمن الاجتماعي لدى طلاب الجامعة، مجلة كلية التربية ببنها، ع131، يوليو 2022، ص573.
21. النمر، مصطفي صابر، الدراما الأجنبية وانحرافات المراهقين السلوكية، العربي للنشر والتوزيع، 2016، ص11.
22. بختة، بظاهر، توجهات الاقتصاد الرقمي في البلدان العربية في ظل رغبتها في تطبيقه، مجلة المنتدى للدراسات والأبحاث الاقتصادية، مج2، 2019، ص150.
23. عبد الحق، خالد، وعبد العال، دعاء، المرجع السابق، ص 26.
24. الزنداني، ابراهيم محمد، والزنداني، بكيل أحمد، الجرائم السيبرانية ودور السياسة الجنائية في مواجهتها والحد منها، دار الكتب اليمنية، 2021، ص 232.
25. المادة 209 من قانون العقوبات القطري رقم 11 لسنة 2004.
26. المادة 170 من قانون العقوبات القطري رقم 11 لسنة 2004.
27. المادة 204 من قانون العقوبات القطري رقم 11 لسنة 2004.
28. المادة 206 من قانون العقوبات القطري رقم 11 لسنة 2004.
29. المادة 210 من قانون العقوبات القطري رقم 11 لسنة 2004.
30. المواد 211، و212 من قانون العقوبات القطري رقم 11 لسنة 2004.
31. محمد، شريف حسين، القانون الواجب التطبيق على الجريمة الإلكترونية، المصرية للنشر والتوزيع، 2021، ص 131.
32. المادة 155 من قانون العقوبات المصري رقم 58 لسنة 1937.
33. المادة 212 من قانون العقوبات الأردني رقم 16 لسنة 1960.
34. المادة 269 من قانون العقوبات الأردني رقم 16 لسنة 1960.
35. المادة 270 من قانون العقوبات الأردني رقم 16 لسنة 1960.
36. سكيكر، محمد على، الجريمة المعلوماتية وكيفية التصدي لها، كتاب الجمهورية، 2010، ص 131.
37. الشعار، خالد على نزال، التحقيق الجنائي في الجرائم الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، 2022، ص 19.
38. العازمي، فيصل جعلان، المرجع السابق، ص 781.
39. العازمي، فيصل جعلان، المرجع السابق، ص 779.

Volume 11 issue 3
N:64 June 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/RPDM9639

40. ابراهيم، مني غازي حسان، فعالية السياسة الجنائية في مواجهة الجرائم المعلوماتية، دراسة مقارنة في ضوء متطلبات الأمن السيبراني، مجلة الشريعة والقانون، ع45، مايو 2025، ص 2652.
41. المادة (11) من قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014.
42. المواد (2،3،4) من قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014.
43. المادة 23 من قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018.
44. المادة 24 من قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018.
45. المادة 3/ج من قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015
46. المادة 4 من قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015
47. محكمة التمييز القطرية، المواد الجنائية، الطعن رقم 802 لسنة 2022 جلسة 2023/01/16.
48. محكمة التمييز القطرية، المواد الجنائية، الطعن (22) لسنة 2022 جلسة 2022/09/29.
49. محكمة التمييز القطرية، المواد الجنائية، الطعن (143) لسنة 2018 جلسة 2019/01/07.
50. العباد، أيمن بن ناصر بن حمد، المسؤولية الجنائية لمستخدمي شبكات التواصل الاجتماعي، مكتبة القانون والاقتصاد، 2015، ص 118.
51. مدين، محمود، المرجع السابق، ص 295.