Sana'a University Journal of Human Sciences مجلة جامعة صنعاء للعلوم الإنسانية
Vol. 5 | No.10 | Page 378 – 418 |2026| https://journals.su.edu.ye/index.php/jhs
ISSN : 2958-8677

The Substantive Provisions of Cybercrimes

Mujahid Ahmed Ahmed Al-Amdi [1,*]
[1]Department of Public Law, Faculty of Sharia and Law - Sana'a University, Sana'a, Yemen.
***Corresponding author:** *mojahedalamdy@gmail.com*

Keywords

1. Cybercrimes
2. Substantive Provisions
3. Personal Data
4. Legal Characterization

Abstract:

This study examines the substantive provisions of cybercrimes by classifying them into two main categories: crimes against individuals (such as publication, defamation, slander, and infringement of personal data), and crimes against property (such as attacks on bank accounts, credit cards, digital currencies, and violations of intellectual property rights). The study aims to demonstrate the extent to which traditional criminal theories, such as the elements of publicity and criminal intent, apply to the digital environment, focusing on analyzing the elements of these crimes according to comparative legislation. The study adopted the inductive analytical and comparative methodologies. It concludes that the Yemeni legislator suffers from a clear legislative deficiency and a legal vacuum in regulating crimes related to personal data and digital currencies, which necessitates the urgent enactment of specialized legislation and the harmonization of existing texts with international standards.

Sana'a University Journal of Human Sciences
مجلة جامعة صنعاء للعلوم الإنسانية
Vol. 5 | No. 10|Page 379 – 418| 2026|
https://journals.su.edu.ye/index.php/jhs
ISSN : 2958-8677

الأحكـام الموضوعيـة للجرائـم السيبرانيـة

مجـاهد أحمـد أحمـد العمـدي [1،*]

[1]قسم القانون العام ، كلية الشريعة والقانون - جامعة صنعاء ، صنعاء ، اليمن.

***المؤلف:** mojahedalamdy@gmail.com*

الكلمات المفتاحية

1. الجرائم السيبرانية
2. الأحكام الموضوعية
3. البيانات الشخصية
4. التكييف القانوني

الملخص:

تتناول هذه الدراسة الأحكام الموضوعية للجرائم السيبرانية من خلال تصنيفها إلى فئتين رئيستين: الجرائم الواقعة ضد الأفراد (كجرائم النشر والسب والقذف، والاعتداء على البيانات الشخصية)، والجرائم الواقعة ضد الممتلكات (كالاعتداء على الحسابات البنكية والبطاقات الائتمانية والنقود الرقمية، وانتهاك حقوق الملكية الفكرية). تهدف الدراسة إلى بيان مدى انطباق النظريات الجنائية التقليدية –كركني العلانية والقصد الجنائي– على البيئة الرقمية، مع التركيز على تحليل أركان هذه الجرائم وفقًا للتشريعات المقارنة. اعتمدت الدراسة على المنهجي التحليلي الاستقرائي والمقارن. وتنتهي الدراسة إلى أن المشرع اليمني يعاني من قصور تشريعي واضح ومن فراغ في تنظيم جرائم البيانات الشخصية والأموال الرقمية، مما يستوجب الإسراع بإصدار تشريعات متخصصة ومواءمة النصوص القائمة مع المعايير الدولية.

المقدمة:

وقد تعددت تصنيفات الجرائم السيبرانية بحسب الاتجاهات التشريعية والفقهية السائدة، فنجد بعضهم يركز على نوع المعطيات ومحل الجريمة[1]، وبعضهم يركز في تصنيفها على دور الكمبيوتر في ارتكاب الجريمة[2]، وبعضهم يصنفها بحسب مساسها بالأشخاص والأموال[3]،

(1) إذ صنفها هذا الاتجاه إلى الآتي: أولًا: الجرائم الماسة بقيمة المعطيات الحاسوبية، وتشمل هذه الطائفة الجرائم الواقعة على ذات المعطيات كجرائم الإتلاف والتشويش للبيانات والمعلومات وبرامج الحاسوب بما في ذلك استخدام وسيلة الفيروسات، وكذلك الجرائم الواقعة على ما تمثله المعطيات من أموال أو أصول كجرائم غش الحاسوب التي تستهدف الحصول على المال أو جرائم الاتجار بالمعطيات وجرائم التحويل والتلاعب في المعطيات المخزنة داخل نظم الحاسوب. وثانيًا: الجرائم الماسة بالمعطيات الشخصية أو البيانات المتصلة بالحياة الخاصة، وتشمل جرائم الاعتداء على المعطيات السرية أو المحمية وجرائم الاعتداء على البيانات المتصلة بالحياة الخاصة. وثالثًا: الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه التي تشمل نسخ وتقليد البرامج وإعادة إنتاجها وصنعها دون ترخيص واستغلالها ماديا والاعتداء على العلامة التجارية وبراءة الاختراع. للمزيد انظر: د. يونس عرب: تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، ورقة مقدمة لورشة تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، متاحة على الرابط http://www.assakina.com

(2) إذ قسمت اتفاقية بودابست لمكافحة الجرائم المعلوماتية 2001 الجرائم السيبرانية إلى أربع طوائف: الأولى: الجرائم التي تستهدف عناصر السرية والسلامة وديمومة توفير المعطيات والنظم، وتشمل الدخول غير القانوني، والاعتراض غير القانوني، وتدمير المعطيات، واعتراض النظم، وإساءة استخدام الأجهزة، والثانية: الجرائم المرتبطة بالكمبيوتر وتشمل: التزوير المرتبط بالكمبيوتر، الاحتيال المرتبط بالكمبيوتر. والثالثة: الجرائم المرتبطة بالمحتوى وتضم طائفة واحدة وفق هذه الاتفاقية وهي الجرائم المتعلقة بالأفعال الإباحية واللاأخلاقية. والرابعة: الجرائم المرتبطة بالإخلال بحق المؤلف والحقوق المجاورة قرصنة البرمجيات. للمزيد انظر: الاتفاقية متاحة على الرابط: https://rm.coe.int/special-edition-budapest-convention-en-2022/1680a6992e

(3) كما هو الشأن في تصنيف القانون الأمريكي Model State Computer Crimes Cod حيث نجد هذا التصنيف شائعًا لدى الفقه الأمريكي فقد قسم تلك الجرائم إلى الآتي: أولًا: طائفة الجرائم التي تستهدف الأشخاص، وتشمل طائفتين 1- الجرائم غير الجنسية التي تستهدف الاشخاص Non-Sexual Crimes Against Persons وتشمل القتل بالكمبيوتر Computer Murder، والتسبب بالوفاة وجرائم الإهمال المرتبط بالكمبيوتر Negligent Computer Homicide، والتحريض على الانتحار Soliciting or Encouraging Suicide، والتحريض القصدي للقتل عبر الإنترنت Intentional Internet Homicide Solicitation والتحرش والمضايقة عبر وسائل الاتصال المؤتمتة Harassment via Computerized Communication والتهديد عبر وسائل الاتصال المؤتمتة Intimidation via Computerized Communication والإحداث المتعمد للضرر العاطفي أو التسبب بضرر عاطفي عبر وسائل التقنية Malicious Infliction of Emotional Distress utilizing Computer Communication و Reckless Infliction of Emotional Distress utilizing Computer Communication والملاحقة عبر الوسائل التقنية Stalking وأنشطة اختلاس النظر أو الاطلاع على البيانات الشخصية Online Voyeurism and Online Voyeurism Disclosure وقنابل البريد الإلكتروني E-mail Bombing وأنشطة ضخ البريد الإلكتروني غير المطلوب أو غير المرغوب به Spamming utilizing Computerized Communication وبث المعلومات المضللة أو الزائفة Transmission of False Statements والانتهاك الشخصي لحرمة كمبيوتر (الدخول غير المصرح به) Personal trespass by computer. 2- طائفة الجرائم الجنسية Sexual Crimes: وتشمل حض وتحريض القاصرين على أنشطة جنسية غير مشروعة Soliciting a Minor with a Computer for Unlawful Sexual Purposes وإفساد القاصرين بأنشطة جنسية عبر الوسائل الإلكترونية Corrupting a Minor with the use of a Computer for Unlawful Sexual Purposes. وإغواء أو محاولة إغواء القاصرين لارتكاب أنشطة جنسية غير مشروعة Luring or Attempted Luring of a Minor by Computer for Unlawful Sexual Purposes أو تلقي أو نشر المعلومات عن القاصرين عبر الكمبيوتر من أجل أنشطة جنسية غير مشروعة Receiving or Disseminating Information about a Minor by Computer for Unlawful Sexual Purposes والتحرش الجنسي بالقاصرين عبر الكمبيوتر والوسائل التقنية Sexually Harassing a minor by use of a Computer for Unlawful Sexual Purposes ونشر وتسهيل نشر واستضافة المواد الفاحشة عبر الإنترنت بوجه عام وللقاصرين تحديدًا Posting Obscene Material On The Internet. و Posting Or Receiving Trafficking In و Obscene Material On The Internet Sending Obscene و Obscene Material On The Internet ونشر الفحش والمساس بالحياء (هتك العرض بالنظر) عبر الإنترنت Material To Minors Over The Internet Indecent Exposure On The Internet وتصوير أو إظهار القاصرين ضمن أنشطة جنسية Depicting Minors Engaged In Sexually Explicit Conduct– واستخدام الإنترنت Pandering Obscenity Involving A Minor لترويج الدعارة بصورة قسرية أو للإغواء أو لنشر المواد الفاحشة التي تستهدف استغلال عوامل الضعف والانحراف لدى المستخدم Using the Internet for Compelling Prostitution و Using the Internet for Pimping و Using the Internet for Soliciting و Using the Internet for Promoting Prostitution و الحصول على الصور والهويات بطريقة غير مشروعة لاستغلالها في أنشطة جنسية Unauthorized Appropriation of Identity, Image, or Likeness for Unlawful Sexual Purposes وبإمعان النظر في هذه الأوصاف نجد أنها تجتمع جميعًا تحت

وبعضهم قيد منها فجعلها الجرائم المتعلقة بالإنترنت فقط[4]، وعلى ذلك سوف يعتمد الباحث على مزج تلك التصنيفات وتبويبها بما يتفق مع طبيعة هذه الدراسة ويحقق حصرًا لأنواع الجرائم السيبرانية بما يضمن

صورة واحدة هي استغلال الإنترنت والكمبيوتر لترويج الدعارة أو إثارة الفحش واستغلال الأطفال والقصّر في أنشطة جنسية غير مشروعة.

وثانيا: طائفة جرائم الأموال–عدا السرقة– أو الملكية المتضمنة أنشطة الاختراق والإتلاف Property Damage (Other than Theft) and Crimes Involving Intrusions وتشمل أنشطة اقتحام أو الدخول أو التوصل غير المصرح به مع نظام الكمبيوتر أو الشبكة إما مجردا أو لجهة ارتكاب فعل آخر ضد البيانات والبرامج والمخرجات Aggravated Computer Trespass و Computer Trespass و Disorderly Persons Offense وتخريب المعطيات والنظم والممتلكات ضمن مفهوم تخريب الكمبيوتر Computer Vandalism وإيذاء الكمبيوتر Computer Mischief واغتصاب الملكية Extortion وخلق البرمجيات الخبيثة والضارة Creation of Harmful Programs و نقلها عبر النظم والشبكات Transmission of Harmful Programs واستخدام اسم النطاق أو العلامة التجارية أو اسم الغير دون ترخيص Cybersquatting وإدخال معطيات خاطئة أو مزورة إلى نظام كمبيوتر Introducing False Information Into a Computer or Computer System والتعديل غير المصرح به لأجهزة ومعدات الكمبيوتر Unlawful Modification of Computer Equipment or Supplies والإتلاف غير المصرح به لنظم الكمبيوتر (مهام نظم الكمبيوتر الأدائية) Unlawful Modification of Computer Equipment or Supplies وأنشطة إنكار الخدمة أو تعطيل أو اعتراض عمل النظام أو الخدمات Unlawful Denial, Interruption, or Degradation of Access to Computer و Unlawful Denial, Interruption, or Degradation of Access to Computer Services وأنشطة الاعتداء على الخصوصية Computer Invasion of Privacy (وهذه تخرج عن مفهوم الجرائم التي تستهدف الأموال لكنها تتصل بجرائم الاختراق) وإفشاء كلمة سر الغير Disclosure of Another's Password والحيازة غير المشروعة للمعلومات Unauthorized Possession of Computer Information وإساءة استخدام المعلومات Misuse of Computer Information و نقل معلومات خاطئة Transmission of False Data.

وثالثًا: جرائم الاحتيال والسرقة Fraud and Theft Crimes وتشمل جرائم الاحتيال بالتلاعب بالمعطيات والنظم Fraud by Computer Manipulation واستخدام الكمبيوتر للحصول على أو استخدام البطاقات المالية للغير دون ترخيص Using a Computer to Fraudulently Obtain and Use Credit Card Information أو تدميرها Damaging or Enhancing Anothers Credit Rating والاختلاس عبر الكمبيوتر أو بواسطته Computer Embezzlement وسرقة معلومات الكمبيوتر Computer Information Theft وقرصنة البرامج Software Piracy وسرقة خدمات الكمبيوتر (وقت الكمبيوتر) Theft of Computer Services وسرقة أدوات التعريف والهوية عبر انتحال هذه الصفات أو المعلومات داخل الكمبيوتر Computer Impersonation.

ورابعا: جرائم التزوير Forgery وتشمل تزوير البريد الإلكتروني Electronic Mail Forgery (E–Mail Forgery) وتزويرالوثائق والسجلات Document /Record Forgery و تزوير الهوية Identity Forgery.

وخامسا: جرائم المقامرة والجرائم الأخرى ضد الأخلاق والآداب Gambling and Other Offenses Against Morality وتشمل تملك وإدارة مشروع مقامرة على الإنترنت Owning and Operating an Internet Gambling business وتسهيل إدارة مشاريع القمار على الإنترنت Facilitating the operation of an Internet gambling business وتشجيع مشروع مقامرة عبر الإنترنت Patronizing an Internet Gambling Business واستخدام الإنترنت لترويج الكحول ومواد الإدمان للقصّر Using the Internet to provide liquor to minors و Using the Internet to provide cigarettes to و Using the Internet to provide prescription drugs.

وسادسا: جرائم الكمبيوتر ضد الحكومة Crimes Against the Government وتشمل هذه الطائفة كافة جرائم تعطيل الأعمال الحكومية وتنفيذ القانون Obstructing enforcement of law or other government function والإخفاق في الإبلاغ عن جرائم الكمبيوتر Failure to report a cybercrime والحصول على معلومات سرية Obtaining confidential government information والإخبار الخاطيء عن جرائم الكمبيوتر False Reports of Cybercrimes والعبث بالأدلة القضائية أو التأثير فيها Tampering with evidenc وTampering with a Computer Source Document وتهديد السلامة العامة Endangering Public Safety وبث البيانات من مصادر مجهولة Anonymity كما تشمل الإرهاب الإلكتروني Cyber–Terrorism والأنشطة الثأرية الإلكترونية أو أنشطة تطبيق القانون بالذات Cyber–Vigilantism.

(1) في نطاق هذا المعيار يجري التمييز بين الأفعال التي تستهدف المعلومات في نطاق نظام الكمبيوتر ذاته – خلال مراحل المعالجة والتخزين والاسترجاع – وبين الأنشطة التي تستهدف الشبكات ذاتها أو المعلومات المنقولة عبرها، وطبعا الأنشطة التي تستهدف مواقع الإنترنت وخوادمها من نظم الكمبيوتر الكبيرة والعملاقة أو تستهدف تطبيقات واستخدامات وحلول الإنترنت وما نشأ في بيئتها من أعمال إلكترونية وخدمات إلكترونية. وفي إطار هذه الرؤية، نجد بعضهم يحصر أنشطة جرائم الإنترنت بتلك المتعلقة بالاعتداء على المواقع وتعطيلها أو تشويهها أو تعطيل تقديم الخدمة (أنشطة إنكار الخدمة السابق بيانها وأنشطة تعديل وتحوير محتوى المواقع أو المساس بعنصري الموفورية والتكاملية أو سلامة المحتوى) وكذلك أنشطة المحتوى الضار، كترويج المواد الإباحية والمقامرة، وأنشطة إثارة الأحقاد والتحرش والإزعاج ومختلف صور الأنشطة التي تستخدم البريد الإلكتروني والمراسلات الإلكترونية، وأنشطة الاستيلاء على كلمات سر المستخدمين والهوية ووسائل التعريف، وأنشطة الاعتداء على الخصوصية عبر جمع المعلومات من خلال الإنترنت، وأنشطة احتيال الإنترنت كاحتيال المزادات

معالجة لعناصرها الجُرمية بغض النظر عن الأساس في وجود الجريمة.

مشكلة الدراسة:

تكمن مشكلة الدراسة في التناقض الجوهري بين الطبيعة التقنية المستحدثة للجرائم السيبرانية وبقاء النصوص الجنائية التقليدية عاجزة عن استيعابها وتكييفها. ويتجسد هذا القصور بشكل حاد في الواقع اليمني؛ إذ يعاني الإطار التشريعي (وخاصة مشروع قانون مكافحة الجرائم الإلكترونية 2023) من فراغ تشريعي واضح في تنظيم حماية البيانات الشخصية، وغموض في المصطلحات التقنية، وعدم ملاءمة العقوبات لخطورة الاعتداءات على الأموال الرقمية والملكية الفكرية، مما يُضعف قدرة أجهزة العدالة على مواجهة هذا النوع المستحدث من الإجرام.

أهداف الدراسة:

هدفت الدراسة إلى التوصيف الدقيق للأحكام الموضوعية للجرائم السيبرانية وتصنيفها وفقًا لمحل الاعتداء (الأفراد والممتلكات). وبيان مدى تطابق ركني العلانية والقصد الجنائي في جرائم النشر الرقمي مع مفاهيم القانون الجنائي التقليدي، وتحليل صور الاعتداء على البيانات الشخصية والأموال الرقمية وفق التشريعات المقارنة، وتشخيص مواطن القصور والخلل في التشريع اليمني ومشروع قانون الجرائم الإلكترونية، وتقديم رؤية تشريعية مقترحة لتطوير المنظومة العقابية اليمنية لمواكبة المستجدات السيبرانية.

منهجية الدراسة:

اعتمدت الدراسة على المنهج التحليلي الاستقرائي: لتحليل نصوص القوانين اليمنية (كقانون الجرائم والعقوبات) ومشروع قانون مكافحة الجرائم الإلكترونية، لبيان مدى صلاحيتها لتطبيقها على الوقائع السيبرانية المستحدثة. والمنهج المقارن: لمقارنة التشريع اليمني بالتشريعات العربية والأجنبية الرائدة (كالمصري والفرنسي) في مجال تجريم الاعتداء على البيانات الشخصية والأموال الرقمية وحقوق الملكية الفكرية، لاستجلاء أوجه القصور واستنباط أفضل الحلول التشريعية.

أهمية الدراسة: تنقسم أهمية الدراسة إلى:

الأهمية النظرية: تثري الفقه الجنائي بدراسة تطبيقية للأركان العامة للجريمة في البيئة الرقمية، وتسد فجوة علمية في المكتبة القانونية اليمنية حول التكييف القانوني للجرائم السيبرانية.

الأهمية العملية: تُعد مرجعية علمية هامة للمشرع اليمني لتدارك نواحي القصور في مشروع قانون مكافحة الجرائم الإلكترونية (خاصة فيما يتعلق بحماية البيانات الشخصية). كما تفيد القضاة وأعضاء النيابة العامة في

وعدم التسليم الفعلي للمنتجات والخدمات، وأنشطة نشر الفايروسات والبرامج الخبيثة عبر الإنترنت، وأنشطة الاعتداء على الملكية الفكرية التي تشمل الاستيلاء على المواد والمصنفات المحمية وإساءة استخدام أسماء النطاقات أو الاستيلاء عليها أو استخدامها خلافا لحماية العلامة التجارية وأنشطة الاعتداء على محتوى المواقع والتصميم، وأنشطة الروابط غير المشروعة وأنشطة الأطر غير المشروعة (وهي أنشطة يقوم من خلالها أحد المواقع بإجراء مدخل لربط مواقع أخرى أو وضعها ضمن نطاق الإطار الخارجي لموقعه هو، وغيرها من الجرائم التي يجمعها مفهوم (جرائم الملكية الفكرية عبر الإنترنت).

أما جرائم الكمبيوتر فإنها وفق هذا التقسيم تعاد إلى الأنشطة التي تستهدف المعلومات والبرامج المخزنة داخل نظم الكمبيوتر وتحديدا أنشطة التزوير واحتيال الكمبيوتر وسرقة المعطيات وسرقة وقت الحاسوب واعتراض المعطيات خلال النقل (مع أنه مفهوم يتصل بالشبكات أكثر من نظم الكمبيوتر) طبعا إضافة للتدخل غير المصرح به والذي يتوزع ضمن هذا التقسيم بين دخول غير مصرح به لنظام الكمبيوتر ودخول غير مصرح به للشبكات فيتبع لمفهوم جرائم الإنترنت تشارلز هورنجور: الجرائم الإلكترونية والمعلوماتية، مرجع سابق، ص164، د. عادل عزام سقف الحيط: جرائم القدح والذم والتحقير المرتكبة عبر الوسائط الإلكترونية، دار الثقافة، عمان 2015، ص123 وما بعدها.

تكييف الوقائع السيبرانية وتطبيق النصوص العقابية بدقة، مما يسهم في تحقيق العدالة الجنائية.

وعلى هذا النحو سوف يقسم الباحث هذا البحث إلى مبحثين وذلك على النحو الآتي:

المبحث الأول: للجرائم الواقعة ضد الأفراد

المبحث الثاني: للجرائم ضد الممتلكات.

المبحث الأول الجرائم الواقعة ضد الأفراد

تمهيد: تعد الجرائم ضد الأفراد من أكثر الجرائم انتشارًا، وهي تلك الجرائم التي يكون فيها الاعتداء على حقوق ذات طابع شخصي، تعد لصيقة بشخص المجني عليه، وهي جزء أساسي من مقومات الشخصية للإنسان، وتصنف هذه الحقوق بأنه لا يمكن تقديرها بمال[5]، وأنها تخرج من دائرة التعامل فيها، ويقسمها الفقه بصفة عامة إلى الحق في الحياة، والحقوق التي تمس السلامة الجسدية للإنسان، والحقوق التي تمس الشرف والاعتبار[6]. وقد وضع المقنن مجموعة من القواعد التي تحمي تلك الحقوق وتعاقب كل فعل من شأنه المساس بها أو الانتقاص منها[7].

ومع التطور التقني وظهور المجتمع المعلوماتي أو الفضاء السيبراني، فقد تطورت تلك الجرائم وأخذت خصوصية من خصوصية البيئة المرتكبة فيها. وهنا سوف يركز الباحث على أهم صور الجرائم السيبرانية الواقعة ضد الأفراد، كونها تتمتع بخصوصية في المجتمع السيبراني.

وعليه سوف يقسم هذا المبحث إلى مطلبين على النحو الآتي:

المطلب الأول: جرائم النشر والبث العلني في الفضاء السيبراني.

المطلب الثاني: جرائم الاحتيال والاعتداء على البيانات الشخصية.

المطلب الأول جرائم النشر والبث العلني في الفضاء السيبراني

شبكة الإنترنت تعد أهم أدوات ووسائل النشر والبث العلني، فهي شبكة عالمية تربط ملايين الأشخاص في وقت واحد ومن مختلف دول العالم[8]، وهذا الانتشار الواسع يجعل من جرائم النشر أكثر خطورة ومساسًا بحياة الإنسان، فالنشر عبر الإنترنت أكثر خطورة من وسائل النشر التقليدية لسرعة انتشارها واتساع مساحة نشرها والاطلاع عليها[9]، ما جعلها مرتعًا لأصحاب النفوس المريضة؛ إذ نشروا فيها أحقادهم وأصبحت مرتعًا لشهواتهم، فلم يبق شيء تحت ستر، ولم يسلم شخص من شائعة مغرضة كاذبة، واستوى في ذلك الأشخاص العاديون وكبار الشخصيات والرموز السياسية أو الدينية أو الاجتماعية أو الفكرية، فطال التشهير الجميع، وبلغ

(1) د. عبد الله المخلافي: المدخل لدراسة القانون، مكتبة الصادق، 2004، ص182.

(2) د. حسن كيرة: المدخل إلى القانون، منشأة المعارف الإسكندرية– 1972م، ص448.

(3) د. عوض محمد يعيش: شرح قانون الجرائم والعقوبات اليمني، القسم الخاص، مكتبة الصادق، صنعاء 2014م، ص34.

(4) فكل ثانية يبدأ 15 شخصًا جديدًا حول العالم استخدام الشبكات الاجتماعية، وكل يوم يستخدم الشبكات الاجتماعية عبر الهواتف الذكية 1.5 مليون شخص لأول مرة، يعني بمعدل 18 شخصًا كل ثانية، ذلك أن عدد مستخدمي الشبكات الاجتماعية عمومًا يصل إلى 2.7 مليار مستخدم، فإذا تم نشر مقالة أو كتاب أو صورة أو مقطع فيديو، انتشر حيث يبلغ متابعي ذاك المقطع أو المقالة ملايين الأشخاص في ثوان معدودة.

(5) تحتل مواقع التواصل الاجتماعي مركز الصدارة كأفضل وسائل النشر والبث العلني، فالنشر والبث العلني في الفضاء التقليدي يعتمد بشكل أساسي على النقل من شخص إلى آخر، أما في الفضاء السيبراني فإنه يمكن لأي شخص الوصول إلى المعلومات المنشورة من أي مكان في العالم وفي أي وقت، كما أنها تبقى مدة أطول وفي الوقت ذاته مادتها وأدواتها أكبر وأبلغ فهي تستخدم الصورة والصوت والرسوم وغيرها من الوسائل التي تعبر عن المعنى المراد إيصاله، للمزيد انظر: د. راشد أحمد المنصوري، جرائم نشر الشائعات الإلكترونية عبر مواقع الإعلام الاجتماعي، أطروحة دكتوراه، جامعة عين شمس 2021م، ص110.

بعضه حد السب والقذف[10]. وتتخذ جرائم النشر عبر الإنترنت عدة أشكال، ذكرها قانون الجرائم والعقوبات، أو قانون الصحافة والنشر، أو القوانين الخاصة، على سبيل المثال لا الحصر[11]. وسوف يركز الباحث على الأحكام العامة والمشتركة لجرائم النشر والبث العلني عبر الفضاء السيبراني، ثم توضيح الأحكام الخاصة ببعض جرائم النشر والبث العلني عبر الفضاء السيبراني، على النحو الآتي:

أولًا: الأحكام العامة والمشتركة لجرائم النشر والبث العلني في الفضاء السيبراني:

في جرائم النشر عمومًا لا تقوم الجريمة إلا عندما يتحقق لها ركنان الركن الأول: هو العلانية المتمثلة في التعبير عن الفكرة محل الجريمة بإحدى طرق العلانية، التي يكون من شأنها المساس بمصلحة محمية بقوة القانون، وهنا يتحقق النشاط الجرمي المتمثل في التعبير عن الفكرة المجرمة بالعلانية، أي أن الركن المادي لجريمة النشر قام بتحقق العلانية.

والركن الثاني: وهو القصد الجنائي المتمثل في اتجاه إرادة الجاني الذي قام بالنشر إلى تحقيق جميع العناصر المادية للجريمة، وهذا يعني أن جرائم النشر جرائم عمدية لا تقع على سبيل الخطأ وإنما بقصد وإرادة[12].

1. مدى تحقق الركن المادي – العلانية – لجرائم النشر عبر الفضاء السيبراني:

يقصد بالعلانية "اتصال علم الجمهور بمعنى مؤذ معين، ثم التعبير عنه بالقول أو الفعل أو بالكتابة أو بأي وسيلة أخرى من وسائل التعبير عن الرأي أو المعنى"[13]، بمعنى أن علم الناس واطلاعهم على الفكرة المؤذية هو جوهر الجريمة، فإذا لم تتحقق العلانية فلا تقوم الجريمة. وتتحقق العلانية باستخدام وسائل من شأنها إبراز أفكار ومشاعر الإنسان وإظهارها للعلن[14]؛ إذ نص المقنن اليمني على ذلك في المادة 192 عقوبات بقوله: " يقصد بالعلانية في تطبيق هذا الباب الجهر أو الإذاعة أو النشر أو العرض أو اللصق أو التوزيع على الأشخاص دون تمييز بينهم في مكان عام أو مباح للكافة أو في مكان يستطيع سماعه أو رؤيته من كان موجودا في مكان عام، وذلك بالقول أو الصياح أو الكتابة أو الرسوم أو الصور أو أية وسيلة أخرى من وسائل التعبير عن الفكر، ويعتبر من العلانية مجرد التوزيع على الأشخاص دون تمييز بينهم ولو كان ذلك في مكان غير عام".

(1) د. هروال هبة نبيلة: أطروحة دكتوراه، جامعة آبي بكر بالقايد، الجزائر 2014، ص74، د. راشد أحمد المنصوري، جرائم نشر الشائعات الإلكترونية عبر مواقع الإعلام الاجتماعي، مرجع سابق، ص31 وما بعدها.

(2) ويمكن حصر تلك الجرائم في: جريمة نشر الأخبار الكاذبة وجريمة ترويج الإشاعات، وجريمة الترويج للأفكار المخالفة للدين أو ثقافة المجتمع، بث دعايات مثيرة إذا كان من شأن ذلك تكدير الأمن العام أو إلقاء الرعب بين الناس أو إلحاق الضرر بالمصلحة العامة، وجريمة إذاعة أسرار الدفاع والتحريض على القتل أو النهب أو الحرق والإخلال بأمن الحكومة والتحريض على قلب نظام الحكم وتغيير الدستور، وجريمة تحريض الجند وجريمة تحريض طائفة على طائفة أخرى و جريمة التحريض على عدم الانقياد للقوانين وإهانة مجلس النواب أو الشورى أو الهيئات النظامية أو الجيش أو المحاكم أو السلطات أو المصالح الحكومية وسب موظف عام بسبب أداء الوظيفة، والتأثير في سير العدالة بنشر أمور من شأنها التأثير في القضاة الذين يناط بهم الفصل في دعوى مطروحة أمام أية جهة من جهات القضاء في البلاد أو في رجال القضاء أو النيابة أو غيرهم من الموظفين المكلفين بالتحقيق أو التأثير في الشهود الذين قد يطلبون لأداء الشهادة في تلك الدعوى أو في ذلك التحقيق أو أمورًا من شأنها منع شخص من الإفضاء بمعلومات لأولي الأمر أو التأثير في الرأي العام لمصلحة طرف في الدعوى أو التحقيق أو ضده، و نشر ما جرى في الدعاوى وما منع نشره، ونشر المرافعات السرية وما تم بالجلسات العلنية بسوء قصد.

(3) د. راشد أحمد المنصوري، مرجع سابق، ص132 وما بعدها، د. محمد رمضان عشري السيد: الأحكام الموضوعية لجرائم الاتصالات، أطروحة دكتوراه، جامعة عين شمس 2021، ص219.

(4) انظر: سليمان أحمد فضل: المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية،2013، ص28.

(5) د. سمير عالية: الجرائم الإلكترونية، منشورات الحلبي 2020، ص283.

وهنا يقصد بالقول أو الصياح: كل ما خرج من الفم في صورة كلمات أو عبارات يعبر من خلالها على معنى معين، ولا فرق بعد ذلك أن يكون مباشرًا أو غير مباشر، فقد يتم تسجيله ثم ينشر بعد ذلك بفترة. أما الكتابة أو الرسم فيقصد بها: كل ما يمكن تدوينه أيًّا كانت اللغة المكتوب بها بشرط أن يدل على معنى معين، والأمر ذاته ينطبق على الرسم والصور، أيًّا كان وضعها شمسية أو يدوية[15].

وقد وسع المقنن من وسائل العلانية في نص المادة 192 عقوبات بقوله "... الجهر أو الإذاعة أو النشر أو العرض أو اللصق أو التوزيع"، فالجهر أو الإذاعة هو إظهار ما كان مخفيًّا سواء كان قولًا أو صورة أو سلوكًا، ولم يشترط المقنن وسيلة معينة لهذا الجهر أو الإذاعة بل اكتفى بالإجهار أو الإذاعة كعنصر لتحقق الجريمة أيًا كانت طريقته، بل جاء في عجز المادة 192 عقوبات" أو أي وسيلة أخرى من وسائل التعبير عن الفكر"، ولا شك أن وسائل الإنترنت والسوشيال ميديا أو أية وسيلة تعد من وسائل الجهر والإذاعة الحديثة، إذ يتحقق بها الشيوع والإذاعة[16].

ثم أردف المقنن شرطًا مفاده أن تكون هذه العلانية والنشر في مكان عام؛ إذ جاء النص كالآتي "... في مكان عام أو مباح للكافة أو في مكان يستطيع سماعه أو رؤيته من كان موجودًا في مكان عام" فالمكان العام هو المكان الذي يستطيع أن يرتاده كافة الناس دون تفرقة بينهم، سواء كان ذلك على وجه دائم أو في أوقات محددة، وسواء كان ذلك بشروط أو دون قيد أو شرط. وقد نصت المادة 20 من مشروع قانون مكافحة الجرائم الإلكترونية المقترح في 2023م[17]على الآتي "يعاقب بالحبس مدة لا تزيد على–ثلاث سنوات، أو غرامة لا تزيد على– ثلاثة ملايين ريال أو بالعقوبتين معًا: (أ) كل من استخدم موقعا إلكترونيًا أو نظام معلومات إلكترونيًا أو شبكة معلوماتية أو وسيلة تقنية معلومات في الاعتداء على الآداب العامة للمجتمع اليمني، أو للتحريض على الكراهية. (ب) كل من استخدم موقعًا إلكترونيًا أو نظام معلومات إلكترونيًا أو شبكة معلوماتية أو وسيلة تقنية معلومات لإجراء أي تعديل أو معالجة معطيات شخصية للغير لربطها بمحتوى مناف للآداب العامة أو لإظهارها بطريقة من شأنها المساس باعتباره وشرفه أو بقصد التشهير أو الإساءة إلى شخص آخر أو الاعتداء على خصوصيته أو انتهاكها".

وإذا طبقنا هذه النصوص على تطبيقات الفضاء السيبراني نجدها أكثر ملاءمة لهذا الوصف القانوني، فالتقاء الناس على وسائل السوشيال ميديا هو أكثر من التقائهم على الواقع، فالفيسبوك والتويتر وغيرها من التطبيقات أصبحت هي المجتمع الحقيقي والمحفل الذي يمكن أن يلتقي فيه الناس؛ إذ يستطيع الجميع التعبير عن آرائهم وأفكارهم، ويتحقق بها الإذاعة والجهرة بالقول أو الكتابة أو الصور [18].

(1) د. راشد أحمد المنصوري، مرجع سابق، ص135، د.هروال هبة نبيلة: مرجع سابق، ص78.

(2) فقد قضت محكمة التمييز الكويتية بأن " برنامج تويتر يعتبر مكانًا عامًا ومن ثم يخضع لقانون الجزاء الكويتي لتحقق ركن العلانية في مواقع التواصل الاجتماعي على المغردين" انظر: الطعن رقم 2012/278 جزائي جلسة 2013/12/15م؛ إذ رأت محكمة التمييز هنا إن تطبيق التويتر يحقق العلانية " حيث يتاح للكافة دون تمييز الولوج إليها وقراءة ومشاهدة ما ينشر عليها" طعن رقم 2014/163 جزائي جلسة 2014/6/26م.

(3) هذا المشروع بدأ بمشروع 2018 ثم أعقبه تعديل في 2020 ثم تعديل 2021 وأخيرا في 2023 وكلها محاولة لإصلاح وضع القانون والخروج به إلى النور لمواجهة القصور التشريعي في الجمهورية اليمنية.

(4) وقد عبر عن ذلك القضاء الفرنسي حيث رفض دفع متهم بمخالفة قانون الملكية الفكرية، أسسه على أن نسخه لأغنية شهيرة لأحد المغنين الفرنسيين

وخلاصة الأمر: أن العلانية كركن من أركان جرائم النشر المنصوص عليها في المادة 192 من قانون الجرائم والعقوبات تتحقق بمجرد النشر على تطبيقات الإنترنت أيًا كانت هذه التطبيقات[19]، إلا ما كان منها مخصصًا للتواصل بين الأطراف– الجاني والمجني عليه– تواصلًا مباشرًا وليس متاحًا لوصول الغير إليه[20]، أما إذا أتيح التواصل للغير أو تعدد المتصلون بهذا التطبيق فيعد محفلًا عامًا مثل الفيديو كنفرناس أو صفحات السوشيال ميديا وغيرها من الوسائل، فيتحقق ركن العلانية[21].

فإذا قام شخص بعمل تغريدة على تويتر أو منشور على صفحة الفيس أو التلجرام أو نشر مقطع فيديو على اليوتيوب أو التيك توك وغيرها من التطبيقات، اشتملت على إحدى جرائم النشر كتسريب معلومات أو الإساءة لموظف عام أو التقليل من هيبة الدولة أو اشتمل ذلك المنشور على سب أو قذف لأحد ما، فقد تحقق ركن العلانية[22].

وعلى ذلك، فإن تحقق الركن المادي للجريمة يقوم بتحقق السلوك الإجرامي المتمثل في المعلومات أو الأخبار أو البيانات أو الإشاعات على موقع إلكتروني أو شبكة معلوماتية أو وسيلة تقنية معلومات، وتتحقق النتيجة المجرَّمة وهي الاعتداء على المصلحة المحمية بالقانون أو تهديدها بالخطر سواء كان ضررًا ماديًا أو معنويًا، وقيام علاقة السببية بين الفعل والنتيجة[23].

2. الركن المعنوي – القصد الجنائي – في جرائم النشر عبر الفضاء السيبراني:

جرائم النشر من الجرائم العمدية يتطلب لها تحقق الركن المعنوي المتمثل في القصد الجنائي، ومعنى هذا: أن الخطأ غير العمدي حتى لو كان جسيمًا لا يكفي لقيام الجريمة، والأصل هنا أن يتوافر القصد الجنائي العام المتمثل في العلم والإرادة، فأما العلم فيكون الجاني عالما بما تم نشره من صور أو فيديو أو تغريدة أو منشور فيه تجريح أو إساءة أو تسريب أو انتقاص أو مساس بدين أو طائفة أو غيرها من جرائم النشر، وأما الإرادة فهي اتجاه الفاعل إلى نشر تلك الأفعال أو المنشورات أيًا كان الشكل الذي اتخذته[24].

وهنا يجب أن يعلم الجاني بما يتضمنه الفيديو أو المنشور أو التغريدة التي قام بنشرها على التويتر أو الفيس بوك أو التلجرام أو غيرها من وسائل التواصل الاجتماعي أو عبر صفحات الويب، ويعلم معناها، وأن يعلم أنه أنما ينشرها عبر وسيلة علنية يمكن للكافة الاطلاع اليها، وهنا يكون العلم مفترضًا، وهنا على مأموري الضبط القضائي أثبات تلك العبارات أو الصور أو الفيديوهات وذكرها في محاضر الضبط، كما يجب

ووضعها على موقع الويب هو بغرض الاستعمال الشخصي؛ إذ رأي القاضي أن مجرد وضعها على الويب يدل على رغبة المتهم بالاستعمال الجماعي لها ولا يمكن اعتبار صفحة الويب بمثابة الصفحة الخاصة أو منزل المتهم، طالما أن بإمكان الغير الوصول اليها، انظر: د. سليمان أحمد فضل: مرجع سابق، ص34، د. محمد رمضان عشري السيد: مرجع سابق، ص221.

(1) فشبكة الويب العالمية تتيح للمتصفح جميع المعلومات ويرتادها الكثير، والمجموعات الإخبارية، وغرف الدردشة، البريد الإلكتروني، وتطبيقات السوشال ميديا كالفيس والتويتر والوتس آب والتلجرام والانستجرام التيك توك وغيرها من الوسائل التي تحقق العلانية لاريب في ذلك.

(2) والحقيقة ان وسائل التواصل المباشر بين الطرفين كالوتس آب أو الفيس أو غيرها من البرامج والتطبيقات التي تتيح التواصل الخاص بين الطرفين يمكن اختراقها ونشر ما فيها من مراسلات مكتوبة أو مرئية أو مسموعة وقد حصل الكثير من الحالات في تهكير حساب المستخدم ومن ثم أصبح ما كان مستورًا عرضة للنشر، والتساؤل هنا هل تنطبق عليها قواعد العلانية أو لا ؟

(3) غير أن بعضهم يرى أن ركن العلانية ينتفي في جرائم التحقير عبر شبكة الإنترنت والهواتف النقالة، للمزيد انظر: عادل عزام سقف الحيط: جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونية، دار الثقافة للنشر، عمان 2019م، ص221.

(4) للمزيد انظر: د. هروال هبة نبيلة: مرجع سابق، ص86، عمر محمد أبو بكر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، القاهرة 2004، ص442.

(5) للمزيد انظر: د. راشد أحمد المنصوري، مرجع سابق، ص137.

(6) د. سليمان أحمد فضل: مرجع سابق، ص35.

إثبات أن المعتدي قصد بها العلانية والنشر والاعتداء على الغير[25].

أما الإرادة فيجب أن يكون نشاط الجاني إراديًا، بأن تتجه إرادته إلى النشر أو إفشاء الأسرار أو المساس بالشرف والاعتبار لشخص ما أو الانتقاص من هيبة الدولة أو القضاء...إلخ، بمعنى أن تتجه إرادة الجاني إلى الفعل المكون للجريمة والذي يمثل تعديًا على حق يحميه القانون، وأن تتجه إرادته إلى النتيجة مثل السخرية أو تعريض الغير للخطر[26]، أما إذا كان مكرهًا على فعل ذلك أو ارتكبه نتيجة لوقوعه في خطأ مادي، فلا تتحقق الإرادة[27].

وبناء على ذلك اذا تحقق عنصرا العلم والإرادة فلا عبرة بعد ذلك بالباعث، بأن يكون قصد الجاني من وراء نشره المزاح أو اعتقاده بأنه يقول الحقيقة، أو أنه يقوم بمراقبة سلوك الموظف العام وله حق نشر ما يقوم به[28]، أو أنه يقوم بتقويم عوج نشاط ذلك الشخص أو الطائفة أو الديانة.

ثانيًا: الأحكام الخاصة لبعض جرائم النشر والبث العلني في الفضاء السيبراني:

لما كان الشرف والاعتبار هما الحصيلة النهائية لمجموع تصرفات الفرد، وهما محل الحماية القانونية فإنه يلزم بيان المقصود بكلّ منهما:

يقصد بالشرف: "قيمة الإنسان وحياته الاجتماعية التي تتكون من سلوكه التي تتأثر به"[29]، ويمثل ذلك حق الفرد في قدر من الاحترام المرتبط بمكانته الاجتماعية في وسطه الاجتماعي.

أما الاعتبار فيقصد به: "ما يتمتع به الشخص من سمعة، ويرتبط بالصفات وبالمركز الذي يحتله الإنسان في مجتمعه ويتصل بصلاحيته لأداء دوره، كما يتعلق بواجباته نحو الغير وعلاقاته والتزاماته الوظيفية والمهنية"[30].

ثالثًا: جرائم السب والقذف عبر الفضاء السيبراني[31]:

نص المقنن اليمني على السب في المادة 291 من قانون الجرائم والعقوبات بأن " السب هو إسناد واقعة جارحة للغير لو كانت صادقة لأوجبت عقاب من أسندت اليه قانونا، أو أوجبت احتقاره عند أهل وطنه، وكذلك كل إهانة للغير بما يخدش شرفه أو اعتباره دون أن يتضمن ذلك إسناد واقعة معينة إليه". وهو قريب من النص في القانون المصري في تعريف القذف؛ إذ نص قانون العقوبات المصري على الآتي " يعد قاذفًا كل من أسند بواسطة إحدى الطرق المبينة في المادة 171 من هذا القانون أمورًا لو كانت صادقة لأوجبت عقاب من أسندت إليه بالعقوبة المقررة قانونًا أو أوجبت احتقاره عند أهل وطنه"[32].

ومما سبق يتبين لنا أن جريمة السب والقذف عبر الإنترنت يتطلب لقيامها ركنان ركن مادي وركن معنوي كما يلي:

(7) د. محمد رمضان عشري السيد: مرجع سابق، ص227، د.هروال هبة نبيلة:، مرجع سابق، ص94.

(1) د. راشد أحمد المنصوري، مرجع سابق، ص147.

(2) د. سليمان أحمد فضل: مرجع سابق، ص35.

(3) كما هو الحال عند من ينشئ صفحات افضحوهم، أو تسريبات ويكيليكس وهكذا.

(4) د. سليمان أحمد فضل: المرجع السابق، ص36.

(5) د. سمير عالية: الجرائم الإلكترونية، مرجع سابق، ص297.

(6) للمزيد في جرائم السب والقذف والتشهير عبر الإنترنت انظر: عمر محمد أبو بكر بن يونس: مرجع سابق، ص464، د. عادل عزام سقف الحيط: جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونية، دار الثقافة للنشر والتوزيع، عمان 2019، ص63.

(7) ويحمل ذات المعنى عن المقنن الكويتي والأردني والفلسطيني واللبناني وان كان ورد بمعان مختلفة منها جرائم الذم.

الركن المادي لجريمة السب والقذف عبر الفضاء السيبراني:

يتمثل الركن المادي في جريمة السب والقذف بفعل أو نشاط يصدر من الجاني عن علم وقصد وإرادة وذلك بإسناد واقعة إلى شخص المجني عليه بأي وسيلة من وسائل الفضاء السيبراني تنال من شرفه أو اعتباره[33].

ويتحقق الركن المادي من خلال ثلاثة عناصر مجتمعة نوردها على النحو الآتي[34]:

الإسناد: هو عنصر أساسي ومهم في واقعة السب والقذف، وذلك بإسناد أمر معين إلى شخص معين بالقول أيًا كانت اللغة المستخدمة في ذلك الإسناد، ويستوي في ذلك استخدام جملة واحدة أو عدة جمل بصفة تأكيدية أو تشكيكية، ويمكن أن يكون بالكتابة سواء كانت مطبوعة أم مخطوطة أيًا كانت الوسيلة التي أفرغت فيها، ويأخذ ذات الحكم الرموز والرسوم والصور التي تستخدم في التعبير في المراسلات والدردشات عبر التطبيقات الإلكترونية المختلفة، كما هو الحال فيما لو نشر شخص عبر حسابه في أحد التطبيقات الإلكترونية وقائع مسيئة كقيام أشخاص بالاختلاس أو ارتكاب وقائع معينة دون أن يحددهم أو يشير إليهم، فيدخل شخص آخر ويرسل تعليقًا بصورة شخص معين، أي أنه يقصد أن هذه الوقائع تنطبق على هذا الشخص فقد تحققت واقعة الإسناد[35].

وقد يكون إسناد الواقعة ذما صريحًا واضحًا وظاهرًا، وهنا لا يحتاج إلى بذل جهد لفهمه أو التبين منه، وقد يكون ضمنيًا كان يتستر الفاعل وراء ألفاظ مستعارة أو الاستفهام، وهنا على القاضي تقدير مرامي تلك العبارات وفحص مدى اشتمالها على السب أو القذف، وهل قصد من ورائها التشهير أم لا؟ والعبرة هنا بما يطمئن إليه قاضي الموضوع، ولا رقابة عليه من المحكمة العليا في ذلك ما دام لم يخطئ في تطبيق القانون على الواقعة[36].

وتتحقق هذه الجريمة سواء كان المجني عليه شخصًا طبيعيًا أو اعتباريًا، في حضوره أو في غيابه، وسواء علم بها أم لم يعلم، أو كانت تشكيكيه أو تأكيدية، صريحة أو ضمنية، حقيقية أو كاذبة. وتتحقق الجريمة سواء بالإسناد أو الإخبار عن الغير، كأن يعاد نشر تغريدة أو مقطع فيديو أو غيرها تضمنت سبًا أو قذفًا، فلا يعفى الناقل حتى لو سبق نشرها وتداولها ما دام أنها قد تضمنت إساءة إلى الغير[37].

موضوع الإسناد: يتمثل في الواقعة المحددة التي أسندها الجاني للمجني عليه التي من شأنها المساس بشرفه واعتباره، فهذه الواقعة هي التي من شأنها تحقيق احتقار الناس له، ويشترط لها بعض الشروط: فيجب أن تكون الواقعة محددة: سواء كانت الواقعة إيجابية أم سلبية حدثت فعلًا أم كان من المتوقع حدوثها، على أنه إذا كانت الواقعة مستحيلة فإن الجريمة لا تقوم. كما يشترط أن يكون من شأن الواقعة عقاب المجني عليه بالعقوبة المقررة قانونًا، أو تؤدي إلى احتقاره عند أهل وطنه[38].

وتطبيقًا لذلك نجد أن المحكمة أدانت أحد الأشخاص لقيامه بنشر حملة سب وقذف على أحد الفنادق وإدارته؛ إذ نشر ما يفيد قيام إدارة الفندق بالدعارة والقمار، وهي

(8) د. نور سليمان يوسف يعقوب البالو: الأحكام الموضوعية لجرائم المعلوماتية، أطروحة دكتوراه، جامعة عين شمس 2021، ص 120.

(9) د. ربيع محمود محمد الصغير القصد الجنائي دراسة تطبيقية على الجرائم المتعلقة بالإنترنت، أطروحة دكتوراه، جامعة عين شمس 2015، ص250 وما بعدها، د. هروال هبة نبيلة: جرائم الإنترنت، مرجع سابق، ص77.

(1) د. سمير عالية: الجرائم الإلكترونية، مرجع سابق، ص300، د. نور سليمان يوسف يعقوب البالو: مرجع سابق، ص 121.

(2) حكم محكمة التمييز الكويتية في الطعن رقم 2007/155، جلسة 2007/9/4.

(3) د. نور سليمان يوسف يعقوب البالو: مرجع سابق، ص 121.

(4) د. سليمان أحمد فضل: مرجع سابق، ص 37.

عبارات لو صحت لأوجبت معاقبة مدير الفندق واحتقاره بين الناس، وهوما أدى إلى خسائر مادية ومعنوية جسيمة[39].

ولا يشترط أن تكون الواقعة المسندة محددة تحديدًا تفصيليًا، كما لا يشترط لهذا التعيين معرفة الاسم أو تعيينه صراحة بل يكفي تحديد شخصيته، "وضابط هذا التحديد: أن يكون من الممكن لفئة من الناس التعرف عليه، ويعتبر التحديد كافيًا إذا ذكر المتهم الأحرف الأولى من اسم المجني عليه أو حدد مهنته أو القرية أو الحي الذي ولد ونشأ فيه أو وضع صورة المقال الذي تضمن عبارات القذف"[40].

علانية الإسناد: ومعنى ذلك أن التصرف الصادر من الجاني صدر بصورة تمكن العامة من الوصول إليها، سواء كانت مرئية أو مقروءة أو مكتوبة، وهنا لا يشترط أن تكون بوسيلة محددة فقد ترك المقنن الأمر مفتوحًا على جميع الوسائل، وينطبق هذ الأمر على الوسائل الحديثة، كتطبيقات السوشيال ميديا، والبريد الإلكتروني، وشبكة الويب، وغرف المحادثات والدردشة، وغيرها من التطبيقات[41].

وخلاصة الأمر: أن المقنن اليمني كغيره من المقننين قد استخدم ألفاظًا وعبارات فضفاضة بشأن وسائل العلانية، ومن هنا فإن كل من تعمد الإساءة لغيره عن طريق استعمال أي وسيلة من وسائل الاتصال الحديثة يقع تحت طائلة المسؤولية القانونية متى تحققت أركان الجريمة.

الركن المعنوي لجريمة السب والقذف عبر الفضاء السيبراني:

السب والقذف من الجرائم العمدية التي يتطلب لقيامها توافر القصد الجنائي، المتمثل في إرادة الجاني ارتكاب الجريمة، أي لابد من العلم والإرادة وذلك باتجاه إرادة الجاني إلى نشر أو إذاعة الأمور المتضمنة القذف أو السب مع علمه أن من شأنها أن تجعل من أسندت إليه محلًا للعقاب أو الازدراء[42].

وعلى ذلك يتحقق الركن المعنوي لجريمة السب والقذف متى توافر له عنصران: الأول: علم القاذف بحقيقة الأمور التي يسندها إلى المجني عليه، وهذ العنصر مفترض، خصوصًا عندما تكون عبارات القذف أو السب شائنة في ذاتها[43]، والثاني: أن تكون إرادة القاذف قد اتجهت إلى ذيوع عبارات القذف ونشرها للجمهور، وهذا العنصر يستفاد عادة من علانية الإسناد ذاته.

وعلى ذلك فإن القصد الجنائي في جريمة السب والقذف يتحقق متى أذاع القاذف أو نشر المحتوى المتضمن للقذف أو السب وهو عالم أن هذا المحتوى فيه مساس بشرف وسمعة المجني عليه أو أنه إذا صح ما أسند اليه لأوجب عقابه، ولا عبرة بعد ذلك بالبواعث سواء كانت شريفة أو غير شريفة، فالغاية لا تبرر الوسيلة[44].

(5) القضية رقم 5408 جنح الساحل 2004م، جمهورية مصر العربية، مشار اليه عند د. نور سليمان يوسف يعقوب البالو: مرجع السابق، ص 121.

(6) المرجع السابق، ص 127.

(7) د. سمير عالية: الجرائم الإلكترونية، مرجع سابق، ص29، ربيع محمود محمد الصغير: مرجع سابق، ص279، محمد أمين الشوابكة: جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمان 2007، ص32.

(1) ربيع محمود محمد الصغير: القصد الجنائي دراسة تطبيقية على الجرائم المتعلقة بالإنترنت، مرجع سابق، ص264.

(2) فقد قضت محكمة النقض المصرية في ذلك بقولها " لا يتطلب القانون في جريمة القذف قصدًا خاصًا، بل يكتفى بتوافر القصد العام الذي يتحقق من نشر القاذف الأمور المتضمنة للقذف وهو عالم أنها لو كانت صادقة لأوجبت عقاب المقذوف أو احتقاره، ولا يؤثر في توافر هذا القصد أن يكون القاذف حسن النية، أي معتقدًا صحة ما رمى به المجني عليه من وقائع القذف، وهذا العلم مفترض إذا كانت العبارات شائنة في ذاتها ومفزعة". نقض مصري 1959/ منشور في مجموعة الأحكام س 10 رقم 163، ص348.

(3) د. نور سليمان يوسف يعقوب البالو: مرجع سابق، ص134.

وخلاصة القول: إن قيام جريمة السب والقذف في الفضاء السيبراني يكون من خلال استخدام أي تطبيق إلكتروني يتم النشر فيه لأي محتوى يعد إساءة للغير، سواء الفيس بوك أو انستغرام أو يوتيوب أو واتس آب أو تويتر أو لينكد أن أو اسناب شات أو تلغرام أو تيك توك أو غيرها من البرامج، وسواء كان الفعل توجيه الإهانة أو التشهير بالغير أو إرسال رسالة منافية للآداب أو نقل خبر بقصد إثارة النعرات أو الفزع في المجتمع أو اصطناع الصور المخلة بالآداب أو التقاط صوره بغير إذنه.

فالبعد الجغرافي بين الجاني والمجني عليه- نظرًا لخصوصية الفضاء السيبراني- يشجع على ارتكاب جرائم السب والقذف للنيل من شرف الغير أو اعتباره أو تعريضه إلى بغض الناس واحتقارهم، وتتنوع أساليب السب والقذف بتنوع الغرض من استخدام شبكة الإنترنت وشبكة الهواتف النقالة، سواء من خلال المراسلات والنشر الإلكتروني الكتابي أو الصوتي أو الفيديو، وسواء كانت الجريمة موجهة عبر الاتصال المباشر أو غيابيًا[45]، فشبكة الإنترنت وتطبيقاتها المختلفة تحقق العلانية.

ولا تسقط المسؤولية الجنائية عن الشخص الذي ينشر عبر تطبيقات خاصة أو مواقع خاصة على شبكة الإنترنت؛ ذلك أن مواقع الويب الشخصية تؤدي إلى الاستعمال الجماعي ومن ثم يمكن الوصول إلى المحتوى المنشور المتضمن عناصر جريمة السب والقذف، وذلك بمجرد الحصول على عنوان الموقع، وهو الأمر ذاته بالنسبة لبقية التطبيقات الأخرى المرتبطة عبر شبكة الويب وهوما يؤدي إلى اطلاع الغير عليه.

المطلب الثاني جرائم الاعتداء على البيانات الشخصية

الحياة المعاصرة تعتمد بشكل أساسي على المعلومات والبيانات، فكثير من الأنشطة الاقتصادية والتجارية والاجتماعية والسياسية باتت تعتمد بشكل أساسي على تلك البيانات والمعلومات، حتى تسهل الحياة وتحقق الرفاهية للبشرية، وهنا تبدو القيمة الحقيقية لها حيث أضحت تمثل عمودًا لاقتصاد كثير من الدول، ونشأت هناك بنوك عالمية للمعلومات والبيانات[46]، بل وتتسابق الدول إلى حماية البيانات والمعلومات وإنشاء البنوك الخاصة بها[47]، ونظرًا لهذه الأهمية البالغة فقد أضحت هذه البيانات عرضة للتخريب والسرقة وسوء الاستخدام. ولأن جمع البيانات المتعلقة بالأشخاص وحفظها وتبادلها مع الجهات المختلفة أمر ضروري تقتضيه المصلحة العامة والخاصة، وتظهر أهمية حماية البيانات حماية أوسع من الحماية التقليدية لها في ظل البيئة التقليدية، سواء من خلال إفراد قوانين خاصة بحمايتها أو من خلال تكييف وملاءمة القوانين الحالية لحماية تلك البيانات في الفضاء السيبراني؛ إذ تمثل البيانات الشخصية القيمة الحقيقية للإنسان، فعدم الحماية يعني أنهم معرضون للابتزاز أو المساءلة القانونية في حال تم

(4) د. نور سليمان يوسف يعقوب البالو، مرجع سابق، ص155.

(1) وبصفة عامة فإن تأثير الثورة التكنولوجية على البيانات الشخصية والخصوصية تمثل ثلاثة أبعاد: الأول: تراكم كم هائل من البيانات والمعلومات حتى بات النظام الإلكتروني يعرف عن الإنسان أكثر مما يعرفه عن نفسه. الثاني: ازدهار سوق المعلومات وظهور بنوك المعلومات وتسابقها لجمع المعلومات والبيانات الشخصية. الثالث: ضعف الحماية القانونية والفنية للبيانات والمعلومات الشخصية في الفضاء السيبراني.

(2) من ذلك قانون حماية المعطيات الشخصية التونسي لسنة 2004م، وقانون حماية المعطيات ذات الطابع الشخصي المغربية لسنة 2009م، وقانون حماية البيانات الشخصية الإماراتي رقم 45 لسنة 2021م، والقانون المصري رقم 151 لسنة 2020 بشأن حماية البيانات الشخصية، والقانون البحريني رقم 30 لسنة 2018 بشأن حماية البيانات الشخصية، والقانون القطري رقم 13 لسنة 2016 بشأن حماية خصوصية البيانات الشخصية ونظام حماية البيانات الشخصية السعودي لسنة 2023م أما بالنسبة للدول الغربية فنذكر منها البريطاني والاتحاد الأوربي.

استخدامها بشكل غير مشروع[48]، وهو ما نلاحظه في تطبيقات الديب فيكنج[49].

أولا: تعريف البيانات الشخصية[50]

سعت كثير من التشريعات إلى تعريف البيانات الشخصية، من ذلك تعريف المقنن المصري في قانون حماية البيانات الشخصية رقم 151 لسنة 2020 في المادة (1) منه؛ إذ عرف البيانات الشخصية أنها " أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى كالاسم، أو الصوت أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الإنترنت أو أي بيانات تحدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية"[51].

ولم يشر مشروع قانون مكافحة الجرائم الإلكترونية اليمني إلى هذا النوع من البيانات وإنما عرف البيانات بصفة عامة، وهنا نوصي المقنن اليمني إلى تبني النهج المعتمد في غالبية التشريعات الحديثة.

أما الفقه فقد عرف البيانات الشخصية بأنها: "هي المعلومات التي تحدد هوية الإنسان كالاسم والجنس والسكن والديانة وفصيلة الدم، والوضع الاجتماعي، والشهادات المدرسية والوظيفة والمهنة والخدمة العسكرية الإلزامية، وتاريخ الدخول أو الخروج من الدولة، أي هي المعلومات المتعلقة بشخص الإنسان"[52]، كما عرفها بعضهم بأنها " تلك التي تتعلق بالحياة الخاصة للفرد، مثل البيانات الخاصة بحالته الصحية، والمالية، والمهنية أو الوظيفية، والعائلية"[53].

(3) انظر: الحسين محمد يحيى، سيد محمد سيد أحمد: الحماية القانونية للبيانات الشخصية، مجلة القضاء والقانون، مركز البحوث والدراسات القضائية، أبوظبي،العدد4–2018م، ص6

(4) تقنية الديب فيك Deepfake تُسمى أيضًا بتقنية التزييف العميق، يُشير مصطلح الديب فيك إلى تقنية التلاعب بالبرمجيات لتشكيل مجموعة صور ومقاطع فيديو مزيفة لشخص ما بطريقة احترافية، ويتم كل هذا بطريقة نظيفة بحيث يصبح من الصعب التمييز بين الصور ومقاطع الفيديو الحقيقية والمزيفة، هذا هو سبب تسميته بتقنية ديب فيك. وهناك أسباب متعددة لاستخدام تقنية الديب فيك أهمها: الابتزاز والإباحية، وهناك أسباب سياسية، وجوانب انتقامية وإجرامية.

(5) بعض التشريعات تسميها المعطيات الشخصية كما هو في التشريع التونسي والتشريع المغربي، ويطلق عليها بعض الفقه المعلومات الشخصية والمعلومات الاسمية وجميعها مشتقة من المصطلح الإنجليزي Personal data للمزيد انظر: الشيخ الحسين محمد يحيى، سيد محمد سيد أحمد: الحماية القانونية للبيانات الشخصية، مرجع سابق ص 8، د. ربيع محمود محمد الصغير: القصد الجنائي دراسة تطبيقية على الجرائم المتعلقة بالإنترنت، مرجع سابق، 309، د. عمر محمد أبو بكر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص614.

(1) نشر في الجريدة الرسمية، العدد 28 مكرره 15يوليو 2020م، وهو قريب من التعريف الذي جاء في قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، ويتفق هذا التعريف مع تعريف المشرع الفرنسي في قانون حماية البيانات الشخصية "كل معلومة ترتبط بشخص طبيعي محدد الهوية، أو من الممكن تحديدها، كما يتحقق وصف الشخص الطبيعي الممكن تحديد هويته، على كل شخص طبيعي يمكن تحديد هويته، سواء بطريقة مباشرة أو غير مباشرة، وبشكل خاص بالرجوع إلى معرف مثل الاسم أو رقم الهوية أو بيانات الموقع أو معرف الهوية عبر الإنترنت أو إلى عنصر أو أكثر من العناصر النوعية الخاصة بهويته العضوية أو الفسيولوجية أو الجينية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية"، وهو ما يتفق مع التوجيه الأوربي رقم 2016/679. وهنا نشدد إلى ضرورة التنبه لوضع تعريف لهذه البيانات في مشروع مكافحة الجرائم الإلكترونية اليمني.

(2) د. نعيم مغبب: مخاطر المعلومات والإنترنت، المخاطر على الحياة الخاصة وحمايتها، بدون ناشر، 1998م، ص 185.

(3) د. أسامة عبد الله قايد: الحماية الجنائية للحياة الخاصة وبنوك المعلومات، مرجع سابق، ص134. وفي ذات المعنى انظر: شادي محمد عدرة: الحماية الجنائية للمعلومات الشخصية، أطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، 2021، ص35.

وتتعد صور البيانات الشخصية في ظل الفضاء السيبراني فمنها: 1– البيانات الشخصية الجينية والبومترية، مثل بصمة الأصبع وبصمة العين، بصمة الصوت، بصمة الحمض النووي. 2– عنوان البريد الإلكتروني. 3– عنوان بروتكول الإنترنت IPحيث أقرت محكمة النقض الفرنسية أن عنوان بروتكول الإنترنت IP Address ايعد من البيانات الشخصية. حكم محكمة النقض الفرنسية 3 نوفمبر 2016.

ثانيًا: جرائم الاعتداء على البيانات الشخصية من قبل القائم بالمعالجة:

تتعلق هذه الجرائم بمخالفة الشخص القائم بمعالجة البيانات الشخصية[54] لشروط وأحكام العمل، وتتخذ هذه الجرائم عدة صور وأشكال أهمها:

1. جريمة الجمع غير المشروع للبيانات الشخصية:

تنص كثير من التشريعات على هذه الجريمة وحددت لها عقوبة، من ذلك نجد أن المقنن المصري قد نص على تجريم هذا الفعل في المادة 37 من قانون حماية البيانات الشخصية حيث نصت على الآتي "ويعاقب – بغرامة لا تقل عن مائتي ألف جنيه ولا تتجاوز مليوني جنيه– كل من جمع بيانات شخصية بدون توافر الشروط المنصوص عليها في المادة 3 من هذا القانون"، كما نصت المادة 18– 226 من قانون العقوبات الفرنسي "يعاقب– بالحبس خمس سنوات وغرامة ثلاثمائة ألف يورو– كل من جمع البيانات الشخصية بوسائل غير مشروعة أو غير عادلة أو احتيالية"[55].

ولم يشر مشروع قانون مكافحة الجرائم الإلكترونية إلى مثل هذا النوع من الجرائم، وهو ما نوصي به المقنن اليمني أن يتنبه إلى مثل هذا النوع من الجرائم عند إصدار القانون.

وتتحقق جريمة الجمع غير المشروع للبيانات الشخصية بتحقق أركانها: فالركن المادي المتمثل في تجميع البيانات الشخصية بوسيلة غير مشروعة أو غير عادلة أو احتيالية أو بدون توافر الشروط المقررة قانونًا، ويشمل ذلك الحصول على البيانات الشخصية بأي إجراء أو فعل– استراق سمع، أو التقاط صور، أو نقل محادثات، أو تسجيل مكالمات[56]– لا يحافظ على الحقوق الممنوحة للأشخاص المعنيين بموجب قوانين حماية البيانات الشخصية خاصة حق الاعتراض[57]. ويتخذ

(4) وقد برز خلاف في الفقه حول مدى اعتبار المعلومات والبيانات الشخصية مالًا، وقد انتهى الفقه إلى أنها مالٌ مملوك لصاحبه ويصلح أن يكون محلًا للحيازة، ومن ثم يصلح أن يكون موضوعًا للجريمة، للمزيد انظر: محمد عادل عبد السلام: الأحكام الموضوعية والإجرائية في جريمة السرقة المعلوماتية، أطروحة دكتوراه، كلية الحقوق جامعة عين شمس 2021، ص43.

(5) انظر: نص المادة 18 – 226 من قانون العقوبات الفرنسي بلغتها الأم التي جرى نصها على النحو الآتي:

Article 226-18: "Le fait de collecter des données à caractère personnel par un moyen frauduleux déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende."

(1) د. خالد عبد الباقي محمد الخطيب: شرح قانون الجرائم والعقوبات القسم الخاص، مكتبة خالد بن الوليد، صنعاء 2021، ص323.

(2) د. محمد عادل علي عبد السلام: الأحكام الموضوعية والإجرائية في جريمة السرقة المعلوماتية، مرجع سابق، ص 102 شادي محمد عدرة: الحماية الجنائية للمعلومات الشخصية، مرجع سابق، ص156، د. عبد الفتاح بيومي حجازي: مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، بدون دار نشر 2009، ص632. ومن التطبيقات القضائية التي تتصل بهذه الجريمة: أنه في عامي 2003-2002، أرسلت شركة رسائل بريد إلكتروني غير مرغوب فيها إلى أفراد تم الحصول على عناوين بريدهم الإلكتروني من المنطقة العامة لشبكة الإنترنت، وذلك باستخدام برنامج في البداية يُخزن هذه المعلومات في ملف لاستخدامها لاحقًا، ثم في مرحلة ثانية، باستخدام برنامج آخر يوجه الرسائل الإعلانية إلى العناوين التي تم جمعها دون حفظها في ملف. ولإدانة الشركة ومديرها بالجريمة المنصوص عليها في المادة 18-226 من قانون العقوبات الفرنسي، بنسخته التي كانت سارية المفعول آنذاك؛ صرحت بحق محكمة الاستئناف: أنها أي الشركة جمعت عناوين إلكترونية، التي تشكل بيانات شخصية بطريقة غير عادلة من حيث إنها قد استخدمت بشكل غير مرتبط بالغرض من نشرها. وفي الواقع هذا يشكل جمعًا للبيانات الشخصية عن طريق تحديد عناوين البريد الإلكتروني واستخدامها، حتى بدون تسجيلها في ملف الإرسال رسائل إلكترونية إلى أصحابها من ناحية، فضلًا عن أنه من غير المنصف أن تجمع عناوين البريد الإلكتروني الشخصية للأشخاص الطبيعيين من المنطقة العامة لشبكة الإنترنت بدون علمهم، فهذه العملية تعرقل حقهم في الاعتراض من ناحية أخرى. انظر:

Cass. Crim., 14 mars 2006, N° de pourvoi: 05-83423, Bull. crim. 2006, N° 69, p. 267, Disponible sur www.legifrance.gouv.fr.

وقد اعتبرت محكمة العدل في الاتحاد الأوروبي أن مدير موقع إلكتروني مجهز بزر "Like" في فيس بوك، قد يكون مسؤولًا بشكل مشترك مع فيس بوك عن جمع ونقل البيانات الشخصية لزوار الموقع إلى فيس بوك. للمزيد انظر:

CJUE, 29 juillet 2019, C-40/17, Fashion ID GmbH & Co. KG c/ Verbraucherzentrale NRW Ev, Disponible sur: https://www. legipresse.com/011-50484-arret-fashion-id-

ركنها المعنوي في صورة القصد الجنائي المتمثل في القصد العام بعنصريه العلم والإرادة[58]، وهو مستفاد من طبيعة الأفعال المرتكبة؛ لأنه لا يتصور وقوعها في صورة غير عمدية[59].

2. جريمة معالجة البيانات الشخصية[60] على رغم اعتراض صاحب الشأن:

نص المقنن الفرنسي على هذه الجريمة في المواد 1-226-18 من قانون العقوبات المعدل بالقانون رقم 801 لسنة 2004 التي جرى نصها على أن "يعاقب بالحبس خمس سنوات وغرامة ثلاثمائة ألف يورو كل من يجري أو يطلب إجراء معالجة إلكترونية لبيانات شخصية تتعلق بشخص طبيعي على الرغم من اعتراضه، وكان الغرض من هذه المعالجة استيفاء بحث ما، خاصةً إذا كان يتعلق بالتجارة، أو كان هذا الاعتراض يستند إلى أسباب مشروعة"[61].

وعلى ذلك فإن هذه الجريمة تتحقق بتحقق ركنها المادي المتمثل في قيام الشخص بمعالجة البيانات الشخصية رغم اعتراض الشخص المعني على ذلك، بشرط أن يقوم هذا الاعتراض على سبب مشروع، مثل: احتفاظ جمعية خيرية ببيانات شخص في ملفاتها رغم أنه قد أعلن اعتراضه على ذلك، أو الاحتفاظ بأرقام أو إيميلات المشتركين لتلقي العروض التجارية[62]، وركنها المعنوي المتمثل في القصد الجنائي بشقيه العلم والإرادة؛ إذ يكون الجاني على علم بالطبيعة الشخصية للبيانات وأنه يقوم بمعالجتها رغم اعتراض المعني على ذلك، وعلى ذلك فلا تقوم الجريمة إذا اعتقد الجاني رضا صاحب الشأن[63].

---

de-la-cjue-la-mode-est-a-la -protection-pas-a-linterdiction.html.

(3) د. خالد عبد الباقي محمد الخطيب: مرجع سابق، ص325.

(4) شادي محمد عدرة: مرجع سابق، ص165.

(5) للمزيد في مفهوم نظام معالجة البيانات انظر: إبراهيم السيد حسانين زيد: المواجهة الجنائية لظاهرة التحويل الإلكتروني غير المشروع للأموال، أطروحة دكتوراه، جامعة عين شمس 2021، ص127.

وتتعد صور البيانات الشخصية في ظل الفضاء السيبراني فمنها: 1- البيانات الشخصية الجينية والبومترية، مثل بصمة الأصبع وبصمة العين، بصمة الصوت، بصمة الحمض النووي. 2- عنوان البريد الإلكتروني. 3- عنوان بروتوكول الإنترنت IP حيث أقرت محكمة النقض الفرنسية أن عنوان بروتوكول الإنترنت IP Address يعد من البيانات الشخصية. حكم محكمة النقض الفرنسية 3 نوفمبر 2016.

(1) انظر: النص بلغته الأصلية:

Article 226-18-1: "Le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende."

وهو ذاته النص في القانون اللبناني للمعاملات الإلكترونية والبيانات الشخصية رقم 81 لسنة 2018 في المادة 106 الفقرة 1 التي نصت على أن " يعاقب بالغرامة من مليون ليرة لبنانية إلى ثلاثين مليون ليرة لبنانية وبالحبس من ثلاثة أشهر حتى ثلاث سنوات أو بإحدى هاتين العقوبتين: كل من أقدم على معالجة بيانات ذات طابع شخصي دون تقديم تصريح، أو دون الاستحصال على ترخيص مسبق قبل المباشرة بعمله وفقًا لأحكام الفصل الثالث من هذا الباب".

(1) انظر: حكم محكمة النقض الفرنسية:

Cass. crim., 29 Juin 1999, N° de pourvoi: 97-84166, Bull. crim. 1999, N° 158, p. 431, Disponible sur www.legifrance.gouv.fr.

(2) على أن المشرع اللبناني قد وضع حالات يجوز فيها معالجة البيانات حتى لو لم يوجد ترخيص بذلك كما هو الشأن في المادة 94 من قانون المعاملات الإلكترونية ومعالجة البيانات الشخصية التي جرى نصها على أن " لا يتوجب التقدم بأي تصريح أو طلب أي ترخيص لمعالجة بيانات ذات طابع شخصي في الحالات الآتية :١ – في المعالجات التي يجريها أشخاص الحق العام كل في نطاق صلاحياته .٢ – في حال قيام جمعيات لا تبغي الربح، بمسك السجلات الخاصة بأعضائها والمتعاملين معها ضمن نطاق ممارستها بشكل طبيعي وقانوني لمهامها ٣ في المعالجات التي يكون موضوعها مسك سجلات مخصصة، بموجب أحكام قانونية أو تنظيمية، لإعلام الجمهور التي يمكن أن يطلع عليها كل شخص أو أشخاص لهم مصلحة مشروعة.٤ – في المعالجات التي يكون موضوعها التلاميذ والطلاب من قبل المؤسسات التربوية لغايات تربوية أو إدارية خاصة بالمؤسسة .٥ – في المعالجات التي يكون موضوعها الإجراءات أو الأعضاء في المؤسسات والشركات التجارية والنقابات والجمعيات وأصحاب المهن الحرة، وذلك في حدود ولحاجات ممارسة نشاطاتهم بشكل قانوني.٦ – في المعالجات التي يكون موضوعها الزبائن والمتعاملين مع المؤسسات والشركات التجارية والنقابات والجمعيات وأصحاب المهن الحرة، وذلك في حدود ولحاجات ممارسة نشاطاتهم بشكل قانوني.٧ – إذا وافق الشخص المعني مسبقًا على معالجة بياناته

3. جريمة الحفظ غير المشروع للبيانات الشخصية الحساسة:

تعرف البيانات الشخصية الحساسة أنها البيانات التي ترتبط بحرية المعتقد ومنع التمييز ضد حرية الرأي وكذا البيانات الشخصية التي تبين العرق والأصل والانتماء أو الفلسفة أو السياسة أو الحياة الصحية أو الجنسية أو البيانات المتعلقة بالملاحقة القضائية والإدانات والعينات البيولوجية المميزة للشخص(64)، فهذا النوع من البيانات تهدد فيما لو تم استخدامها أو التعامل معها بطريقة خاطئة حريات الأفراد، ولهذا السبب صنفت على أنها حساسة أو غير عادية، وهنا نجد أن المقنن تدخل لحماية هذا النوع من البيانات فنجد أن قانون حماية البيانات الشخصية المصري قد جرم المساس بتلك البيانات في المادة 41 التي جرى نصها على أن " يُعاقب بالحبس مدة لا تقل عن ثلاثة شهور وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز خمسة ملايين جنيه، أو بإحدى هاتين العقوبتين، كل حائز أو متحكم أو معالج جمع أو أتاح أو تداول أو عالج أو أفشى أو خزن أو نقل أو حفظ بيانات شخصية حساسة بدون موافقة الشخص المعني بالبيانات أو في غير الأحوال المصرح بها قانونًا"(65).

وعلى ذلك تقوم الجريمة بتحقق ركنها المادي المتمثل في النشاط المجرم وهو جمع هذه البيانات أو حفظها أو تسجيلها أو إتاحتها أو تداولها أو نقلها أو معالجتها أو إفشائها دون موافقة الشخص المعني أو أن يكون في غير الأحوال المصرح بها في القانون. وركنها المعنوي المتمثل في العلم المتمثل في معرفة طبيعة البيانات الشخصية والصفة الخاصة لهذه البيانات، مع علمه بعدم مشروعية هذا الحفظ أو المعالجة، وأن تتجه إرادة الجاني إلى معالجة هذه البيانات بالمخالفة للقانون، مع الأخذ في الاعتبار أن الجاني يجب أن يكون حائزًا أو متحكمًا أو قائمًا بمعالجة هذه البيانات، وأن تكون هذه المعلومات من النوع الحساس(66).

4. جريمة معالجة معلومات طبية بغرض البحث العلمي بصورة غير مشروعة:

حرص المقنن الفرنسي في النص على هذه الجريمة من خلال المواد 1-19-226 من قانون العقوبات الفرنسي

الشخصية إذا لم يوجد مانع قانون .يمكن أيضًا إعفاء بعض المعالجات أو بعض فئاتها من إجراءات التصريح أو الترخيص إذا تبين أن وضعها قيد التنفيذ لا يستتبع أي خطر يهدد الحياة الخاصة أو الحريات الشخصية، وذلك بموجب مرسوم يتخذ في مجلس الوزراء بناء على اقتراح وزيري العدل والاقتصاد والتجارة.٨ – في المعالجات المنصوص عليها في القانون رقم /١٤٠ ٩٩ وضمن حدوده". د. شادي محمد عدرة، مرجع سابق، ص165، سمير عالية: مرجع سابق، ص129، محمد أمين الشوابكة: مرجع سابق، ص87

(3) د. نعيم سعيداني: الحماية الجنائية للحق في الخصوصية في مجال المعلوماتية، أطروحة دكتوراه، جامعة باتنة 1، الجزائر، 2021، ص124.

(4) وقد سبقه المشرع الفرنسي إلى ذلك فنجد نص المادة 19-226 من قانون العقوبات المعدلة بالمرسوم رقم 1125 لسنة 2018، تنص على أن " يعاقب بالحبس خمس سنوات وغرامة ثلاثمائة ألف يورو كل من يسجل أو يحفظ في ذاكرة معلوماتية، بدون موافقة صريحة من الشخص المعني، البيانات الشخصية التي تكشف بصورة مباشرة أو غير مباشرة عن الأصول العنصرية أو العرقية أو الآراء السياسية أو الفلسفية أو الدينية أو الانتماءات النقابية للأشخاص، أو التي تتعلق بصحة الشخص أو ميوله الجنسية أو هويته الجنسية، بخلاف الحالات التي ينص عليها القانون. ويعاقب بالعقوبات ذاتها كل من يسجل أو يحفظ في ذاكرة معلوماتية البيانات الشخصية المتعلقة بالجرائم أو أحكام الإدانة أو التدابير الاحترازية بخلاف الحالات التي ينص عليها القانون تتطبق أحكام هذه المادة على المعالجة غير الإلكترونية للبيانات الشخصية التي لا يقتصر تنفيذها على ممارسة الأنشطة الشخصية المحضة".

(1) د. شادي محمد عدرة: مرجع سابق، ص173، وتجدر الإشارة هنا إلى أن التشريعات المقارنة ومنها المشرع الفرنسي قد حرصت على إلزام الجهات المعنية بضرورة مسح البيانات الشخصية بعد انقضاء مدة زمنية معينة بحيث يكون من حق الشخص المعني التأكد من عدم حفظ هذه البيانات من خلال الحصول على شهادة خالية من البيانات الشخصية التي كانت مدونة عنه وهو ما يعرف بالحق في النسيان، وفي هذا السياق قضت محكمة النقض الفرنسية بقيام جريمة الحفظ غير المشروع للبيانات الشخصية الحساسة في حق شخص قام بتجميع أو تخزين البيانات المتعلقة بعدد حالات الزواج المختلط بين الفرنسيين والأجانب والآراء السياسية الخاصة بهم دون موافقة الأشخاص المعنيين. للمزيد انظر: حكم محكمة النقض الفرنسية:

Cass. Crim., 16 mars 2004, N° de pourvoi: 04-80048, Disponible sur www.legifrance.gouv.fr.

حيث جاء نصها على النحو الآتي" يعاقب بالحبس خمس سنوات وغرامة ثلاثمائة ألف يورو كل من يجري معالجة إلكترونية للبيانات الشخصية بهدف البحث في مجال الصحة، وذلك في الحالات الآتية:

1- عدم الإعلام السابق للأشخاص المعنيين بما يجمع عنهم من بيانات شخصية وحقهم في الاطلاع عليها وتصحيحها، والاعتراض عليها، وبطبيعة هذه البيانات والجهة المرسلة إليها.

2- إذا كان هناك اعتراض من الشخص المعني أو كان الحظر بمقتضى القانون أو في حالة غياب الرضا الواضح والصريح من الشخص المعني بها، أو إذا تعلقت البيانات بشخص متوفى كان قد رفض معالجتها بشكل صريح خلال حياته"[67].

من النص السابق يتبين أن جريمة معالجة معلومات طبية بغرض البحث العلمي بصورة غير مشروعة تتحقق بتحقق أركانها؛ فركنها المادي يتمثل في قيام الجاني بمعالجة بيانات شخصية ذات طابع طبي وكان الغرض من ذلك هو البحث في المجال الطبي دون الحصول على موافقة ذوي الشأن[68] أو إخطارهم بحقهم في الاطلاع عليها أو تصحيحها أو الاعتراض عليها أو الاعتراض على الجهات التي سوف تزود بها[69]، وركن معنوي متمثل في العلم بطبيعة المعلومات وأن تكون هذه المعلومات شخصية وأنها لغرض البحث العلمي في المجال الطبي مع العلم أنه لم يتم إبلاغ ذوي الشأن أو إعلامهم بحقهم في الاعتراض، ويجب أن تتجه إرادته إلى السلوك الإجرامي[70].

فلو أن شركة تأمين صحي قامت بحفظ بيانات بعض مشتركيها لفترة أطول من الفترة المحددة قانونًا أو قامت بتداولها مع جهات أخرى لأي سبب كان، فإنها بذلك تكون قد ارتكبت جريمة الحفظ غير المشروع للبيانات الشخصية الحساسة، وتحقق بشأنها أركان الجريمة

(2) انظر: النص بلغته الأصلية:

Article 226-19-1: "En cas de traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende le fait de procéder à un traitement:

1-Sans avoir préalablement informé individuellement les personnes sur le compte desquelles des données à caractère personnel sont recueillies ou transmises de leur droit d'accès, de rectification et d'opposition, de la nature des données transmises et des destinataires de celles-ci;

2-Malgré l'opposition de la personne concernée ou, lorsqu'il est prévu par la loi, en l'absence du consentement éclairé et exprès de la personne ou s'il s'agit d'une personne décédée, malgré le refus exprimé par celle-ci de son vivant".

(3) وقد قضت محكمة النقض الفرنسية بمعاقبة مديري نقابة أطباء العمل بدفع غرامة مالية قدرها 12500 يورو وذلك لقيامهم بوضع نظام لمعالجة مبرمجة لملفات طبية، دون أن يقوموا بالإعلان السابق للجنة الوطنية للمعلوماتية والحريات ولعدم اتخاذهم التدابير التي تمنع الاطلاع على الملفات من جانب الغير، ودون التصريح لهم. فقد تعلق الأمر في هذه القضية بقيام الجهات الإدارية غير المصرح لهم بالاطلاع خلال هذه المدة على الملفات الطبية، وكذلك أسند لهؤلاء المديرين إهمالهم في ضمان حسن إدارة النظام بصورة كاملة، وتأهيل لأشخاص غير مؤهلين لإدارة باس ورد الدخول لهذه الملفات؛ ما أدى إلى توزيع هذه الكلمات للدخول للموقع بشأن هذه الملفات بين الأطباء وطاقم السكرتارية والإداريين. انظر:

Cass. Crim., 30 octobre 2001, N° de pourvoi: 99-82136, Disponible sur www.legifrance.gouv.fr.

(4) د. نعيم سعيداني: الحماية الجنائية للحق في الخصوصية في مجال المعلوماتية، مرجع سابق، ص361، د. شادي محمد عدرة: مرجع سابق، ص183.

(5) عبد الفتاح بيومي حجازي: مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، مرجع سابق ص641، د. شادي محمد عدرة: مرجع سابق، ص183.

المحددة قانونًا، مع الأخذ في الاعتبار أن تكون هذه البيانات خاصة وحساسة[71].

5. جريمة حفظ البيانات الشخصية خارج الوقت المسموح به قانونًا:

تحدد التشريعات مددًا معينة للاحتفاظ بالبيانات الشخصية للشركات والمؤسسات والجهات المختلفة، ومن أجل ذلك وضعت نصوصًا تجرم الاحتفاظ بالبيانات لدى هذه الجهات خارج الوقت المسموح به قانونًا[72]، ومن ذلك نجد نص المادة 38 من قانون حماية البيانات الشخصية المصري "يعاقب بغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تتجاوز ثلاثة ملايين جنيه، كل متحكم أو معالج لم يلتزم بواجباته المنصوص عليها في المواد (4، 5، 7) من هذا القانون"[73]، والأمر نفسه جاء في قانون العقوبات الفرنسي في المواد 20-2؛ إذ جاء النص على النحو الآتي:" يعاقب بالحبس خمس سنوات وغرامة ثلاثمائة ألف يورو كل من يقوم بالاحتفاظ ببيانات شخصية لمدة أكثر من المدة المنصوص عليها في القانون أو اللائحة ؛ بناءً على الترخيص (الإذن) أو الإشعار أو الإخطار (الإعلان) المسبق الموجه للجنة الوطنية للمعلوماتية والحريات ؛ ما لم يتم حفظها لأغراض تاريخية أو إحصائية أو علمية على النحو المنصوص عليه في القانون، ويعاقب بالعقوبات ذاتها كل من يقوم بالمعالجة للبيانات الشخصية لأغراض تاريخية أو إحصائية أو علمية بعد انقضاء الفترة المذكورة في الفقرة الأولى، بخلاف ما هو منصوص عليه في القانون"[74].

بناء على ما سبق فإن جريمة حفظ البيانات الشخصية خارج الوقت المسموح به قانونا تتحقق بقيام الجاني بحفظ البيانات الشخصية لمدة أطول من المدة المسموح بها قانونًا أو معالجتها بعد المدة المسموح بها، وبهذا يقوم الركن المادي للجريمة[75]، ويتحقق الركن المعنوي للجريمة من خلال الاحتفاظ بالبيانات الشخصية عن علم وبصيرة أنه الاحتفاظ بها خارج المدة المسموح بها قانونًا ولا بد من إدراك الجاني لطبيعة المعلومات، وأن تتجه إرادة الجاني إلى تحقيق ذلك مخالفا الحظر الذي قرره القانون[76].

6. جريمة الانحراف عن الغرض من المعالجة الإلكترونية للبيانات الشخصية:

الأصل في جمع البيانات والمعلومات أنه لابد أن يكون له هدف واضح ومحدد وفي الوقت ذاته يكون مشروعًا فإذا انحرف القائم بالمعالجة عن الغرض المحدد لذلك يكون قد ارتكب جريمة يعاقب عليها القانون، فقد نص

(6) د. هروال هبة نبيلة: مرجع سابق، ص272.
(7) د. نعيم سعيداني: مرجع سابق، ص76.
(1) د. شادي محمد عدرة: مرجع سابق، ص185.
(2) انظر: النص بلغته الأصلية:
Article 226-20: "Le fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi. Est puni des mêmes peines le fait, hors les cas prévus par la loi, de traiter à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa."
(1) د. نعيم سعيداني: الحماية الجنائية للحق في الخصوصية في مجال المعلوماتية، مرجع سابق، ص352، د. شادي محمد عدرة: مرجع سابق، ص185.
(2) وتطبيقًا لذلك قضت محكمة النقض الفرنسية بإدانة المدير الفعلي لشركة احتفظت بشكل غير قانوني بشفرات البطاقات الائتمانية للعملاء، انظر: هذا الحكم في الآتي:
Cass. Crim., 3 mars 2015, N° de pourvoi: 13-88079, Disponible sur: www.legifrance.gouv.fr.

قانون حماية البيانات الشخصية المصري في المادة 38 على أن " يعاقب بغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تتجاوز ثلاثة ملايين جنيه، كل متحكم أو معالج لم يلتزم بواجباته المنصوص عليها في المواد (4، 5، 7) من هذا القانون"[77].

والأمر ذاته جاء في قانون العقوبات الفرنسي مع إضافة عقوبة الحبس خمس سنوات كما هو في نص المادة 21 – 226 التي جرى نصها على أن " يعاقب بالحبس خمس سنوات وغرامة ثلاثمائة ألف يورو كل من حاز بيانات شخصية بمناسبة قيامه بتسجيلها أو تصنيفها أو نقلها أو معالجتها تحت أي شكل، إذا غير من الوجهة النهائية المقررة لهذه البيانات وفقًا للقانون أو للقرار الصادر في شأنها أو في الإخطار المسبق على القيام بالمعالجة"[78].

وبهذا تتحقق جريمة الانحراف عن الغرض من المعالجة الإلكترونية للبيانات الشخصية بتحقق ركنها المادي المتمثل في قيام الجاني بإساءة استخدام أو استغلال البيانات الشخصية بخلاف الغاية المحددة لذلك، سواء كان ذلك في مرحلة تسجيل البيانات أم تصنيفها أم نقلها[79]، وأما الركن المعنوي لهذه الجريمة فإنه يتحقق باتجاه نية الجاني إلى ارتكاب هذا الفعل عن علم وبصيرة، وأنه قد خرج بفعله هذا عن الغاية أو الغرض الذي يعالج البيانات من أجله[80].

7. جريمة عدم اتخاذ الإجراءات الأولية لمعالجة البيانات الشخصية

نص المقنن الفرنسي في المواد 16-226 من قانون العقوبات على هذه الجريمة بقوله" يعاقب بالحبس خمس سنوات وغرامة ثلاثمائة ألف يورو كل من أجرى، ولو بإهمال، أو طلب إجراء معالجة إلكترونية للبيانات الشخصية دون مراعاة الشكليات التي يتطلبها القانون قبيل معالجة تلك البيانات. ويعاقب بالعقوبات ذاتها كل من أجرى، ولو بإهمال، أو طلب إجراء معالجة كانت موضوعًا لأحد التدابير المنصوص عليها في الفقرة الثالثة- البند3 من المادة 20 من القانون 78-17 الصادر بتاريخ 6 يناير 1978 بشأن تكنولوجيا المعلومات والملفات والحريات"[81].

(3) وتطبيقًا لذلك قضت محكمة النقض الفرنسية بإدانة المدير الفعلي لشركة احتفظت بشكل غير قانوني بشفرات البطاقات الائتمانية للعملاء، انظر: هذا الحكم في الآتي:

Cass. Crim., 3 mars 2015, N° de pourvoi: 13-88079, Disponible sur: www.legifrance.gouv.fr.

(3) انظر: النص بلغته الأصلية:

Article 226-21: "Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende".

(4) محمد أمين الشوابكة: جرائم الحاسوب والإنترنت، مرجع سابق، ص99، د. شادي محمد عدرة: الحماية الجنائية للمعلومات الشخصية، مرجع سابق، ص185.

(5) د. عبد الفتاح بيومي حجازي: مرجع سابق، ص644، د. شادي محمد عدرة: مرجع سابق، ص185.

(1) وقد جرى النص بلغته الأصلية على النحو الآتي:

Article 226-16 (Modifié par Ordonnance n°2018-1125 du 12 décembre 2018 art. 13): "Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 3° du III de l'article 20 de la loi n° 78-17 du 6

من النص السابق يتبين أن جريمة عدم اتخاذ الإجراءات الأولية لمعالجة البيانات الشخصية تقوم في حق الجاني متى تحقق **الركن المادي** الذي يتمثل في امتناعه عن القيام بالإجراءات الأولية التي يتطلبها القانون عند إجراء أي معالجة إلكترونية للبيانات الشخصية، بمعنى آخر مخالفة الجاني للواجبات المنصوص عليها في القانون، ويعد الركن المادي في هذه الجريمة مركبًا له عنصران: الأول: الفعل المجرم والمتمثل في القيام بإجراءات المعالجة وجمع المعلومات دون سبب مشروع، والثاني: عدم اتخاذ الإجراءات الأولية التي نص عليها القانون[82]. والركن المعنوي للجريمة: يتمثل في اتجاه إرادة الجاني إلى معالجة البيانات الشخصية وهو عالم بموضوع الحق المعتدى عليه ودون اتخاذ الإجراءات التي نص عليها القانون[83].

8. جريمة عدم اتخاذ التدابير اللازمة لتأمين البيانات الشخصية:

اهتمت كثير من التشريعات في حماية البيانات الشخصية وألزمت الجهات المتعاملة مع هذه البيانات باتخاذ مجموعة من التدابير اللازمة لتأمين تلك البيانات[84]، ومن ذلك ما جاء في المواد 17-226 من قانون العقوبات الفرنسي فقد نصت على أن "يعاقب بالحبس خمس سنوات وغرامة ثلاثمائة ألف يورو كل من أجرى أو طلب إجراء معالجة إلكترونية للبيانات الشخصية دون اتخاذ التدابير المنصوص عليها في المواد 24 و 25 و 30 و 32 من اللائحة الأوروبية رقم 4 المؤرخة في 27 أبريل 2016 أو الفقرة (6) من المادة)2016/679 E([85].

وهنا يتحقق الركن المادي لجريمة عدم اتخاذ التدابير اللازمة لتأمين البيانات الشخصية بقيام الجاني بإجراءات المعالجات للبيانات الشخصية دون اتخاذ التدابير التي نص عليها القانون واللازمة لحماية تلك البيانات، أو عدم اتخاذ جميع الإجراءات التقنية والتنظيمية وتطبيق المعايير القياسية اللازمة لحماية البيانات الشخصية وحفظها من التسرب أو الاختراق أو الإتلاف أو التغيير أو العبث[86]. وأما الركن المعنوي فإنه يتحقق بتوجه إرادة الجاني إلى معالجة البيانات الشخصية دون اتخاذ الاحتياطات التي أوجبها القانون مع علمه بطبيعة تلك البيانات[87].

9. جريمة الإفشاء غير المشروع للبيانات الشخصية:

جرم المشرع المصري قيام من له سيطرة على البيانات الشخصية لأي سبب من الأسباب إفشاء تلك البيانات وتسريبها للغير فقد نصت المادة 36 من قانون حماية البيانات الشخصية على أن "يعاقب بغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه كل حائز أو

janvier 1978 relative à l'informatique, aux fichiers et aux libertés."

(2) د. نعيم سعيداني: مرجع سابق، ص379، د. شادي محمد عدرة: مرجع سابق، ص200، عبد الفتاح بيومي حجازي: مرجع سابق، 629.

(3) محمد أمين الشوابكة: مرجع سابق، ص93، د. شادي محمد عدرة: مرجع سابق، ص203.

(4) د. عبد الفتاح بيومي حجازي: جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، مرجع سابق، 631.

(5) انظر: النص بلغته الأصلية:

Article 226-17 (Modifié par Ordonnance n°2018-1125 du 12 décembre 2018-art. 13): "Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites aux articles 24,25,30 et 32 du règlement (UE) 2016/679 du 27 avril 2016 précité ou au 6° de l'article 4 ."

(6) وقد ذهبت محكمة النقض الفرنسية في كثير من أحكامها إلى تجريم الأفعال التي من شأنها الإخلال بتلك التدابير التي نص عليها القانون من ذلك انظر:

Cass. Crim., 30 octobre 2001, N° de pourvoi: 99-82136, Cass. Crim., 19 décembre 1995, N° de pourvoi Cass. Crim., 13 avril 1999, N° de pourvoi: 98-87873, Disponible sur www.legifrance.gouv.fr.

(1) د. شادي محمد عدرة: مرجع سابق، ص212.

متحكم أو معالج... أفشى أو أتاح... بيانات شخصية معالجة إلكترونيًا بأي وسيلة من الوسائل في غير الأحوال المصرح بها قانونًا أو بدون موافقة الشخص المعني بالبيانات" [88] كما نصت المادة 38 من ذات القانون على أن "يُعاقب بغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز ثلاثة ملايين جنيه، كل متحكم أو معالج لم يلتزم بواجباته المنصوص عليها في المواد (٤، ٥، ٧) من هذا القانون" كما نصت المادة ٤٤ منه، على أن "يعاقب بغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز ثلاثة ملايين جنيه، كل عضو مجلس إدارة أو أي من العاملين بالمركز خالف الالتزامات المنصوص عليها في المادة (٢٤) من هذا القانون"[89].

على أن المقنن اللبناني جعل الإهمال سببًا للتجريم وتوافر القصد الجنائي وهو البين من نص المادة 106 من قانون المعاملات الإلكترونية ومعالجة البيانات الشخصية التي جرى نصها على أن "يعاقب بالغرامة من مليون ليرة لبنانية إلى ثلاثين مليون ليرة لبنانية وبالحبس من ثلاثة أشهر حتى ثلاث سنوات أو بإحدى هاتين العقوبتين:...كل من أقدم، ولو بالإهمال، على إفشاء معلومات ذات طابع شخصي موضوع معالجة لأشخاص غير مخولي الاطلاع عليها"[90].

وعلى ذلك فإن جريمة الإفشاء غير المشروع للبيانات الشخصية تتحقق بتحقق ركنها المادي المتمثل في قيام الجاني بإفشاء البيانات الشخصية أو إتاحتها للغير بأي وسيلة من الوسائل حتى ولو لم يترتب على ذلك وقوع ضرر بالمجني عليه، فهي جريمة قائمة بذاتها[91]. وقيام ركنها المعنوي المتمثل في القصد الجنائي والذي هو علم الجاني بماهية الجريمة واتجاه إرادته إلى ارتكابها على الرغم من هذا العلم، فهو يعلم بطبيعة هذه البيانات وأن هذه البيانات تتمتع بصفة السر وأنه لا يجوز للغير الاطلاع عليها بمقتضى واجباته المهنية، وأن عليه عدم إتاحتها أو إطلاع الغير عليها[92].

10.جريمة عدم مراعاة أحكام حركة البيانات الشخصية عبر الحدود

نص المقنن المصري على هذه الجريمة في المادة 42 من قانون حماية البيانات الشخصية التي جرى نصها على أن "يعاقب بالحبس مدة لا تقل عن ثلاثة شهور وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تتجاوز

(2) ويقابل هذا النص نص المادة 22/226 من قانون العقوبات الفرنسي.

(3) وقد نصت المادة 31 من قانون مكافحة جرائم تقنية المعلومات على أن " يعاقب بالحبس مدة لا تقل عن سنة, وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز عشرين ألف جنيه، أو بإحدى هاتين العقوبتين، كل مقدم خدمة خالف الأحكام الواردة بالبند (2) من الفقرة أولا من المادة (2) من هذا القانون، وتتعدد عقوبة الغرامة بتعدد المجنى عليهم من مستخدمي الخدمة" وهو ذات النص الذي جاء عند المشرع الفرنسي في المادة 22-226 من قانون العقوبات التي جرى نصها على أن " يُعاقب بالحبس لمدة خمس سنوات والغرامة ثلاثمائة ألف يورو كل من حاز بيانات شخصية بمناسبة تسجيلها أو تصنيفها أو نقلها أو لعلاجها إلكترونيًا تحت أي شكل، التي يترتب على إفشائها الإضرار باعتبار الشخص المعني أو حرمة حياته الخاصة، ومن ثم قام بنقلها إلى علم شخص طرف ثالث غير مختص أو مخول بتلقي هذه البيانات، بدون تصريح أو إذن سابق من الشخص المعني. ويعاقب على الكشف أو الإفشاء المنصوص عليه في الفقرة السابقة بالحبس لمدة ثلاث سنوات والغرامة مائة ألف يورو إذا ارتكب عن طريق الرعونة أو عدم الاحتياط أو الإهمال. وفي الحالات الواردة بالفقرتين السابقتين، لا يجوز تحريك الدعوى الجنائية إلا بناء على شكوى المجني عليه أو ممثله القانوني أو خلفه". للتعليق على هذا النص انظر: محمد امين الشوابكة: جرائم الحاسوب والإنترنت، مرجع سابق، ص101.

(4) للمزيد في التعليق على هذا النص انظر: سمير عالية: الجرائم الإلكترونية، مرجع سابق، ص141.

(5) د. محمد رمضان عزمي السيد: الأحكام الموضوعية لجرائم الاتصالات، ص 243، د. سمير عالية: مرجع سابق، 138، د. عبد الفتاح بيومي حجازي: جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، مرجع سابق، ص646، د. شادي محمد عدرة: الحماية الجنائية للمعلومات الشخصية، مرجع سابق، ص212.

(6) د. نعيم سعيداني: الحماية الجنائية للحق في الخصوصية في مجال المعلوماتية، مرجع سابق، ص346، د. شادي محمد عدرة: المرجع السابق، ص228.

خمسة ملايين جنيه، أو بإحدى هاتين العقوبتين، كل من خالف أحكام حركة البيانات الشخصية عبر الحدود المنصوص عليها في المواد (14، 15، 16) من هذا القانون"، وهو الأمر الذي نصت عليه المادة 1-22-226 من قانون العقوبات الفرنسي[93].

وعلى ذلك فإن جريمة عدم مراعاة أحكام حركة البيانات الشخصية عبر الحدود تقوم في حق الجاني بتحقق ركنها المادي المتمثل في قيام الجاني بنقل البيانات الشخصية إلى دولة أجنبية بالمخالفة للحظر المحدد في القانون أيًا كانت وسيلة هذا النقل[94]. وأما ركنها المعنوي فيتمثل في العلم والإرادة؛ إذ يكون الجاني عالمًا بموضوع الجريمة وأنه من البيانات الشخصية وعلمه بعناصر الركن المادي للجريمة واتجاه إرادته إلى ارتكاب الفعل رغم ذلك[95].

وخلاصة لما سبق نجد أن التشريعات المقارنة قد سعت إلى وضع تنظيم كامل لحماية البيانات الإلكترونية الشخصية من خلال مجموعة من النصوص، إلا أن المقنن اليمني قد تخلف عن هذه التشريعات فلم ينظم تلك الجرائم بل لم يتطرق لها في مشروع قانون مكافحة الجرائم الإلكترونية، وهو ما نوصي معه المقنن اليمني بضرورة تضمين القانون الجديد نصوصًا تحقق الحماية الكاملة للبيانات الشخصية ذات الطبيعة الإلكترونية، وليكن ذلك فرصة لضبط النصوص واستدراك النقص والقصور الذي اعتور المشروع المطروح.

ثالثًا: جرائم الاعتداء على سرية وسلامة المعلومات الشخصية:

وهذا النوع من الجرائم يتولد عن إساءة استخدام شبكة الإنترنت حيث يتم الاعتداء على سرية وسلامة البيانات الشخصية للمستخدمين وتتنوع هذه الجرائم على النحو الآتي:

1. جريمة اعتراض المعلومات عبر الشبكة:

فقد نصت المادة 16 من قانون مكافحة جرائم تقنية المعلومات المصري على أن " يُعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتين وخمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعترض بدون وجه حق أي معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها"[96]. وقريبًا من هذا النص جاء نص المادة (6) من مشروع مكافحة الجرائم الإلكترونية التي جرى نصها

(1) حيث جرى نصها باللغة الأصلية:

Article 226-22-1 "Le fait de procéder ou de faire procéder à un transfert de données à caractère personnel faisant l'objet ou destinées à faire l'objet d'un traitement vers un Etat n'appartenant pas à l'Union européenne ou à une organisation internationale en violation du chapitre V du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, ou des articles 112 à 114 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende".

(2) وقد قضت محكمة العدل الأوروبية أن نشر البيانات الشخصية على موقع عبر شبكة الإنترنت لا يعد نقلًا لهذه البيانات خارج دول الاتحاد الأوروبي؛ وذلك لأن أي شخص في العالم يمكن أن يدخل إلى هذا الموقع. فعكس ذلك سيؤدي إلى منع نشر أي بيانات شخصية على شبكة الإنترنت، فمجرد اطلاع شخص في دولة أخرى على بيانات شخصية على شبكة الإنترنت لا يعد نقلًا لهذه البيانات من قبل من يقوم بمعالجتها.

CJUE, 6 novembre 2003, C-101/01, Bodil lindqvist, disponible sur http://www.crid.be/pdf/public

(3) د. شادي محمد عدرة: مرجع سابق، 246.

(4) وهو ذات النص عند المشرع الفرنسي في المادة 15-226 من قانون العقوبات المعدل التي جرى نصها على أن:

"Est puni des mêmes peines le fait, commis de mauvaise foi, de divulguer des d'intercepter, de détourner, d'utiliser correspondances émises, transmises ou reçues par la voie électronique ou de procéder à l'installation d'appareils de nature à permettre la réalisation de telles interceptions."

على أن " يعاقب بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن مليون ريال، أو بالعقوبتين معًا، كل من اعترض بدون وجه حق أية معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها"[97].

وبذلك فإن جريمة اعتراض المعلومات عبر الشبكة تتحقق بتوافر ركنها المادي المتمثل في قيام الجاني باعتراض أو التقاط أو تحويل أو كشف أو استخدام البيانات الشخصية المنقولة أو المتلقاة عبر شبكة الإنترنت[98]، ما لم يكن من الأشخاص المرخص لهم بذلك بسبب عملهم أو بأمر قضائي. كما يتحقق الركن المعنوي عن طريق العلم بطبيعة البيانات والمعلومات التي تم اعتراضها كونها شخصية، وأن تتجه إرادته إلى ارتكابها[99].

2. جريمة خداع المستخدمين على شبكة الإنترنت:

نص المقنن السوري على هذه الجريمة بشكل واضح في المادة 18/ب من قانون مكافحة الجريمة المعلوماتية؛ إذ جاء نصها على النحو الآتي" يعاقب بالحبس من شهر إلى ستة أشهر والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية كل من استخدم الخداع للحصول على معلومات شخصية، أو سرية من المستخدمين على منظومة معلوماتية أو الشبكة يمكن استغلالها لأغراض إجرامية"[100].

وفي ذات السياق جاء نص المادة 12 من مشروع قانون مكافحة الجرائم الإلكترونية حيث جرى نصها على أن "يعاقب بالحبس مدة لا تزيد على سنة، أو بغرامة لا تزيد على مليون ريال أو بالعقوبتين معًا، كل من استخدم موقعًا إلكترونيًا أو نظام معلومات إلكترونيًا أو شبكة معلوماتية أو وسيلة تقنية معلومات في الوصول دون وجه حق إلى أرقام أو بيانات أو خدمات بطاقات الائتمان أو البطاقات الإلكترونية أو أرقام أو بيانات حسابات مصرفية أو غيرها من وسائل الدفع الإلكتروني".

إذًا فموضوع الجريمة هنا هو المعلومات الشخصية أو السرية المتعلقة بالمستخدم، وتتحقق هذه الجريمة بتوافر الركن المادي المتمثل في قيام الجاني بارتكاب فعل الخداع بغرض الحصول على معلومات أو بيانات شخصية أو سرية تتعلق بالمستخدمين للشبكة العنكبوتية واستغلالها لأغراض غير مشروعة. وقيام ركنها المعنوي المتمثل في القصد الجنائي العام: العلم بفعل الخداع وأن من شأن هذا الفعل إيقاع المجني عليه في الغلط الذي يدفعه إلى تقديم بياناته الشخصية التي يطلبها الجاني منه، وبجانبه القصد الجنائي الخاص المتمثل في الحصول على بيانات أو معلومات شخصية وسرية من المستخدمين مثل الباسورد أو أرقام بطاقات الائتمان أو الحسابات[101]. [102].

(1) وقد نصت المادة 3 من اتفاقية بودا بست 2001 على نفس الحماية، للمزيد في التعليق على هذا النص انظر: هلالي عبد الإله أحمد: جرائم المعلوماتية عابرة للحدود، دار النهضة العربية 2007.

(2) للمزيد في بيان عناصر هذه الجريمة انظر: د. شادي محمد عدرة: مرجع سابق، 269، د. عماد مجدي عبد الملك: جرائم الكمبيوتر والإنترنت، مرجع سابق، ص130.

(3) د. عمر محمود الجوني: الوجيز في الحماية الجنائية من جرائم تقنية المعلومات، دار النهضة العربية، 2021، ص87، د. عبد الفتاح بيومي حجازي: مرجع سابق، 654، د. نعيم سعيداني: مرجع سابق، ص387.

(4) وفي ذات المعنى جاء نص المادة 36 و37 من قانون حماية البيانات الشخصية المصري والمادة 18-226 من قانون العقوبات الفرنسي المعدل.

(5) وقد نصت المادة 3 من اتفاقية بودا بست 2001 على نفس الحماية، للمزيد في التعليق على هذا النص انظر: هلالي عبد الإله أحمد: جرائم المعلوماتية..، مرجع سابق.

(6) د. شادي محمد عدرة: المرجع السابق، ص293، د. نعيم سعيداني: المرجع السابق، 339، د. إبراهيم السيد حسانين زايد: المواجهة الجنائية لظاهرة التحويل الإلكتروني غير المشروع للأموال، مرجع سابق، ص127.

3. جريمة انتحال الهوية الرقمية[103]:

نص الشرع الفرنسي على هذه الجريمة في المواد 1-226-4 من قانون العقوبات المعدل، وقد جرى نصها على أن" يعاقب بالحبس سنة وغرامة خمسة عشر ألف يورو كل من يقوم بانتحال هوية الغير أو باستخدام واحد أو أكثر من بيانات ذات طبيعة تسمح بتحديد هويته، وذلك بهدف إقلاق هدوئه أو هدوء الآخرين، أو بهدف المساس بشرفه أو اعتباره، ويعاقب على هذه الجريمة بالعقوبة ذاتها عند ارتكابها من خلال شبكة الاتصالات المخصصة للعموم عن طريق خط الإنترنت"[104].

وقد تصدى مشروع قانون مكافحة الجرائم الإلكترونية لهذه الجريمة في المادة 14 منه التي جرى نصها على أن " يعاقب بالحبس مدة لا تزيد على سنتين، أو بغرامة لا تزيد على مليوني ريال أو بالعقوبتين معًا، كل من استخدم إحدى وسائل تقنية أو بالعقوبتين المعلومات في انتحال هوية شخص طبيعي أو معنوي".

وتتحقق هذه الجريمة بقيام الركن المادي المتمثل في قيام الجاني بالاستيلاء على البيانات الشخصية المتعلقة بالهوية الشخصية للمجني عليه، سواء كان ذلك عن طريق بروتوكول الإنترنت أو كلمة السر أو الاستدراج عن طريق الخداع أو التصيد أو الهاكر أو التجسس، واستخدامها في سبيل انتحال هوية المجني عليه[105]. وأما الركن المعنوي لهذه الجريمة فإنه يتحقق بعلم الجاني باركان الجريمة واتجاه إرادته إلى ارتكابها، وكذا يتطلب المقنن الركن الخاص المتمثل في اتجاه إرادة الجاني إلى المساس بشرف واعتبار المجني عليه[106].

4. جريمة إتلاف المعلومات أو البيانات الشخصية:

نص المقنن المصري على هذه الجريمة في المادة (17) من قانون مكافحة جرائم تقنية المعلومات وقد جرى نصها على أن " يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين, كل من أتلف أو عطل أو عدل مسارًا أو ألغى كليًا أو جزئيًا متعمدًا وبدون وجه حق البرامج والبيانات أو المعلومات المخزنة، أو المعالجة، أو المولدة أو المخلقة على أي نظام معلوماتي وما في حكمه، أيا كانت الوسيلة التي استخدمت في الجريمة"[107].

(1) الهوية الرقمية (بالإنجليزية: Digital Identity) هي عبارة عن معلومات عن كيان تستخدمه أنظمة الكمبيوتر لتمثيل وكيل خارجي، وقد يكون هذا الوكيل شخصًا أو مؤسسة أو تطبيقًا أو جهازًا؛ ويعرّف المعيار " ISO / IEC 24760-1" الهوية الرقمية على أنها عبارة عن مجموعة من السمات المتعلقة بالكيان؛ ووفقًا لمنهج "Feher" الأكاديمي، فإن الهوية الرقمية تشير إلى مجموعة البيانات الرقمية التي يتم بناؤها بواسطة المستخدمين والأنظمة الرقمية.

(2) انظر: النص بلغته الأصلية:

Article 226-4-1: "Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne

(3) وقد تشدد المشرع الفرنسي في مدى تحقق الركن المادي لهذه الجريمة واشترط أن يكون الجاني قد استهدف من خلال ذلك الشرف والاعتبار للمجني عليه وإقلاق هدوئه وسكينته. للمزيد انظر: د. شادي محمد عدرة: مرجع سابق، ص305، محمد أمين الشوابكة: مرجع سابق، ص183.

(4) د. شادي محمد عدرة: مرجع سابق، ص311.

(5) وهو الأمر الذي تصدى له المشرع الفرنسي في المادة 3- 226 من قانون العقوبات التي جرى نصها على أن:

Article 323-3: "Le fait d'introduire frauduleusement des données de modifier dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende. Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat,

وقد نصت المادة 5 من مشروع قانون مكافحة الجرائم الإلكترونية على الآتي "... فإذا ترتب على أي من الأفعال السابقة إلغاء أو حذف أو نسخ أو تغيير أو تعديل أو إتلاف أو محو أو إخفاء أو إضافة أو تعطيل أو تخريب أو إعاقة أو توقيف أو نقل أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي، تكون العقوبة الحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن مليوني ريال أو بإحدى هاتين العقوبتين"[108].

وتتمثل أركان هذه الجريمة في الركن المادي من حيث قيام الجاني بإتلاف أو تعطيل أو التعديل أو الإلغاء أو المحو أو النسخ أو الاستخراج غير المشروع للبيانات الشخصية، فجميع هذه الأفعال أو أحدها يعد جريمة وتعديًا على البيانات الشخصية[109]. وأما الركن المعنوي فيتمثل في العلم والإرادة من حيث قيام الجاني بجميع الأفعال المكونة للركن المادي وهو عالم بها وبما سوف تؤول إليه واتجاه إرادته إلى ارتكابها، مع علمه بموضوع الجريمة أنها بيانات شخصية[110].

5. جريمة إخفاء الأدلة الرقمية أو العبث بها:

تصدى المقنن المصري لهذه الجريمة في المادة (28) من قانون مكافحة جرائم تقنية المعلومات وقد جرى نصها على أن "يعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن عشرين ألفًا ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين، كل مسؤول عن إدارة موقع أو حساب خاص أو بريد إلكتروني أو نظام معلوماتي، إذا أخفى أو عبث بالأدلة الرقمية لإحدى الجرائم المنصوص عليها في هذا القانون التي وقعت على موقع أو حساب أو بريد إلكتروني بقصد إعاقة عمل الجهات الرسمية المختصة".

وقد سار في هذا الاتجاه مشروع قانون مكافحة الجرائم الإلكترونية في المادة 18 إذ جرى نصها على أن "يعاقب بالحبس مدة لا تزيد على ثلاث سنوات، أو بغرامة لا تزيد على ثلاثة ملايين ريال أو بالعقوبتين، كل مسؤول عن إدارة موقع إلكتروني أو نظام معلوماتي أو شبكة معلوماتية أو وسيلة تقنية معلومات أو بريد إلكتروني أو حساب خاص إذا أخفى أو عبث بالأدلة الرقمية والإلكترونية لإحدى الجرائم المنصوص عليها في هذا القانون أو التي وقعت على أي منها".

وتعد جريمة إخفاء البيانات الشخصية أو التلاعب بها قد تمت متى تحقق ركنها المادي المتمثل في قيام الجاني بإخفاء الدليل الرقمي أو الاحتفاظ به أو نقله على نحو يمنع اكتشافه، وقيام الجاني بالعبث بالدليل الرقمي من خلال إحداث خلل أو تغيير أو تعديل أو إفساد أو تشويه بحيث تفقد قيمتها وحقيقتها. وقيام الركن المعنوي المتمثل في القصد العام العلم بعناصر الجريمة واتجاه إرادة

la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende

(1) وقد كان نص المادة 4 من اتفاقية بودا بست أكثر وضوحا في ضبط هذه الجريمة، للمزيد انظر: د. هلالي عبد الإله أحمد: جرائم المعلوماتية عابرة للحدود، مرجع سابق، ص68.

(2) د. سمير عالية: الجرائم الإلكترونية، مرجع سابق، ص163، د. عبد الفتاح بيومي حجازي: جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، مرجع سابق، ص376.

(3) د. شادي محمد عدرة: الحماية الجنائية للمعلومات الشخصية، مرجع سابق، ص319.

الجاني إليها، والقصد الخاص وهو إعاقة عمل الجهات الرسمية المختصة[111].

المبحث الثاني الجرائم ضد الممتلكات

تمهيد:

مع تطور الحياة المعاصرة وازدهار تكنولوجيا المعلومات وتغلغلها في حياة البشر وخلقها مجتمعًا موازيًا للمجتمع التقليدي، فقد برزت جرائم من نوع خاص تتلاءم مع المجتمع الجديد المجتمع الافتراضي؛ إذ يتم الاعتداء فيه على الأموال عن طريق اختراق الشبكة المعلوماتية وإجراء التحويلات البنكية من أقصى الشرق إلى أقصى الغرب في لحظات معدودة ودون حاجة لانتقال المجرمين أو النقل التقليدي للأموال، وهذه الجريمة تختلف جذريا عن جرائم السرقات التقليدية، وأضحت القوانين التقليدية متخلفة عن مواكبتها[112].

وعلى ذلك فالجرائم السيبرانية تختلف عن الجرائم التقليدية حتى تلك التي يتم استخدام الحاسوب فيها، ذلك أن الجريمة تبقى تقليدية وأن الحاسوب فيها مجرد أداة لارتكاب الجريمة، فالجريمة السيبرانية تتصف بأن المال فيها يختلف عن المال التقليدي والوسيلة المستخدمة فيها تتفق مع هذا النوع من الجرائم.

فلو نظرنا إلى النقود الإلكترونية فإنها تعد قيمة نقدية مخزنة على الوسيلة الإلكترونية مدفوعة مقدما وغير مرتبطة بحساب بنكي وهي محل قبول من الجميع، والأمر كذلك في البطاقات الائتمانية، وجميعها عبارة عن بيانات مالية إلكترونية يتم إدخالها مباشرة في الجهاز دون حاجة إلى وثائق أو مستندات وإنما من خلال برامج معدة لذلك، وهنا يمكن أن تقع عليها جرائم معينة تتلاءم مع بيئتها الإلكترونية، ما يتعين معه وجود الخبرة لدى المعنيين من أجهزة العدالة.

وفي ضوء ما سبق سوف نقسم هذا المبحث إلى مطلبين وذلك على النحو الآتي:

المطلب الأول: الجرائم المتعلقة بالحسابات البنكية وبطاقات الائتمان والنقود الرقمية.

المطلب الثاني: جريمة انتهاك حقوق الملكية الفكرية.

المطلب الأول الجرائم المتعلقة بالحسابات البنكية وبطاقات الائتمان والنقود الرقمية

الحسابات البنكية والبطاقات الائتمانية والنقود الرقمية من أكثر الممتلكات التي تتعرض للاعتداء من قبل المجرمين والمحتالين، فقد يسعى بعضهم للحصول على كسب مادي غير مشروع من خلال الدخول إلى معطيات الحاسوب والتلاعب بها وتحويل الأموال من خلالها إلى حسابه الخاص أو للغير بطريقة احتيالية مستغلا الثغرات البرمجية في الحساب أو في كود التوقيع الإلكتروني أو في أذونات الوصول[113].

(4) د. هروال هبة نبيلة: الجرائم الإلكترونية، مرجع سابق، ص156، د. عبد الفتاح بيومي حجازي، مرجع سابق، ص704، د. شادي محمد عدرة: مرجع سابق، ص319.

(1) فهذه القوانين وجدت لتتلاءم مع البيئة التقليدية فهي تجرم السرقة والاحتيال والنصب وخيانة الأمانة والاختلاس الذي ينصب على الأوراق النقدية والكمبيالات والسندات والشيكات، وكأن هذه الأموال لها إحرازها الخاص.

(2) هناك مجموعة من الوسائل الفنية لتحويل الأموال إلكترونيًا، بحيث يتم استغلالها من خلال التحويل غير المشروع للأموال بعدة وسائل يصعب حصرها لسرعة وتيرة التطور في هذا المجال لكن يمكن الإشارة إلى أكثرها انتشارا:

- استخدام برامج معدة خصيصا لتنفيذ الاختلاس أشهر هذه الوسائل هو تصميم برامج معينة تهدف إلى إجراء عمليات التحويل الآلي من حساب إلى آخر سواء كان ذلك من المصرف نفسة، أو من حساب آخر في مصرف آخر على أن يتم ذلك في وقت معين يحدده مصمم هذا البرنامج، وأشهر هذه الوقائع قيام أحد العاملين بمركز الحاسبات المتعاقد مع مصرف الكويت التجاري لتطوير أنظمة المعلومات بالاستيلاء على مبالغ طائلة من المصرف بعد أن تمكن من اختيار خمسة حسابات رائدة في خمس فروع محلية للمصرف وأعد لها برنامجا تمثلت مهمته في تحويل مبالغ معينة من هذه الحسابات إلى حسابات أخرى فتحت باسمه في الفروع نفسها على أن تتم عملية التحويل أثناء وجوده بالطائرة في طريقه إلى المملكة المتحدة عائدا إلى بلاده بعد انتهاء عقد عمله، ثم فتح حسابات أخرى فور وصوله وطلب من المصرف تحويل هذه المبالغ إلى حساباته الجديدة في بريطانيا.

- كما توجد برامج أخرى تقوم بخصم مبالغ ضئيلة من حسابات الفوائد على الودائع المصرفية بإغفال الكسور العشرية عن طريق استخدام شبكة معلوماتية

أولًا: جريمة الدخول غير المشروع على الحسابات البنكية:

تتمثل الجريمة هنا بالدخول غير المشروع في النظام المعلوماتي للمجني عليه؛ إذ يتم التقاط رقم الحساب السري للعميل عبر شبكة الإنترنت، واستغلال ذلك في تحويل أموال من حساب الضحية إلى حساب المجرم أو حسابات مرتبطة به، أو تحويلها لحسابات أخرى وفاء بما عليه من التزامات، فجميع تلك الأفعال تعد تدخلًا في النظام المعلوماتي للجهة المسؤولة على النظام[114]. كما يجري التلاعب بالبرامج والبيانات والمعلومات المخزنة على أجهزة الحاسوب بقصد الاستيلاء على الأموال بدون وجه حق، وتعد هذه الوسيلة من أخطر الوسائل تعقيدًا؛ لصعوبة اكتشافها؛ إذ يتم تغيير مضمون البيانات وتوجيه الأوامر بطريقة خاطئة؛ للتوصل إلى تنفيذ رغبات الجاني وغرائزه ومنع إدخال البيانات الصحيحة، وقد صنفها بعضهم من صور الغش المعلوماتي الذي يهدف إلى الحصول على الأموال بطريقة غير مشروعة[115].

وتتخذ هذه الجريمة عدة صور: منها: إعداد مزادات خادعة عبر الإنترنت، ونظام السمسرة الخاصة عبر الإنترنت، والاستيلاء على الهوية الرقمية، أو استخدام أساليب الاستثمار وبيع الأسهم للشركات عبر الإنترنت وانتحال الشخصية، والاعتداء على أرقام بطاقات الائتمان[116]، كما يمكن للجاني القيام بالاحتيال عن طريق تزوير الصفحات الرسمية للبنوك المعتمدة لدى العملاء لإيهام العملاء بصحتها وجعلهم يقدمون بياناتهم المالية وأرقام حساباتهم ثم يتم السطو عليها من خلال الدخول إلى حسابات العملاء والاستيلاء على هذه الأموال[117].

وقد نصت المادة 4 من قانون مكافحة جرائم تقنية المعلومات الأردني على أن " أ- يعاقب بالحبس مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن (2500) ألفين وخمسمائة دينار ولا تزيد على (10000) عشرة آلاف دينار كل من:

1- حصل قصدا ودون تصريح أو بما يجاوز التصريح عن طريق الشبكة المعلوماتية أو تقنية المعلومات أو

بحيث يتحول الفارق مباشرة إلى حساب الجاني لأنها برامج تعتمد على التكرار الآلي لمعالجة معينة ومما يؤدي إلى صعوبة اكتشاف هذه الطريقة رغم ضخامة المبلغ هو أن هذه الاستقطاعات تتم على مستوى آلاف الأرصدة في وقت واحد مع ضآلة المبلغ المخصوم من كل حساب على حدة بحيث يصعب أن ينتبه إليه العميل.

- التحويل المباشر للأرصدة يتم ذلك عن طريق اختراق أنظمة الحاسب وشفرات المرور أشهرها قيام أحد خبراء الحاسب الآلي في الولايات المتحدة باختراق النظام المعلوماتي لأحد المصارف وقيامه بتحويل ١٢ مليون دولار إلى حسابه الخاص في ثلاث دقائق فقط وعادة ما يتم ذلك أيضا عن طريق إدخال معلومات مزيفة وخلق حسابات ومرتبات وهمية وتحويلها إلى حساب الجاني ويمكن أن يتم التحويل المباشر أيضا عن طريق التقاط الاشعاعات الصادرة عن الجهاز إذا كان النظام المعلوماتي متصلا بشبكة تعمل عن طريق الأقمار الصناعية فهناك بعض الأنظمة التي تستخدم طابعات سريعة تصدر أثناء تشغيلها إشعاعات كهرومغناطيسية ثبت أنه من الممكن اعتراضها والتقاطها أثناء نقل الموجات وحل شفراتها بواسطة جهاز خاص لفك الرموز وإعادة بثها مرة أخرى بعد تحويرها. وهو ما نصت عليه اتفاقية بودابست في المادة (٥). للمزيد انظر: د. نور سليمان يوسف يعقوب البالو: مرجع سابق، ص237، د. إبراهيم السيد حسانين زايد: مرجع سابق، ص31.

(1) د. عماد مجدي عبد الملك: مرجع سابق، ص110، عمر محمد الجوني: مرجع سابق، ص114.

(2) د. نور سليمان يوسف يعقوب البالو: الأحكام الموضوعية لجرائم المعلوماتية، مرجع سابق، ص239.

(3) د. عمر محمد أبو بكر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص415.

(4) وقد أدانت محكمة المنصورة الاقتصادية مجموعة من الجناة المصريين والأمريكيين باعتبار أنهم قد قاموا بالاحتيال والنصب على عملاء بنوك في الولايات المتحدة الأمريكية وتحويلها إلى حساباتهم الخاصة من خلال إنشاء مواقع مزورة لتلك البنوك، حكم غير منشور لمحكمة المنصورة الاقتصادية، جلسة 2017/4/23 مشار إليه لدى: إبراهيم السيد حسانين زايد: المواجهة الجنائية لظاهرة التحويل الإلكتروني غير المشروع للأموال، مرجع سابق، ص93.

نظام المعلومات على بيانات أو معلومات تتعلق بوسائل الدفع الإلكتروني أو في تنفيذ المعاملات المالية أو المصرفية الإلكترونية أو استخدم أو نشر أيا من هذه البيانات.

2- اصطنع أو أنشأ أو وضع أو صمم أي وسيلة من وسائل تقنية المعلومات أو برنامج معلومات أو أمرًا برمجيا بقصد تسهيل الحصول على البيانات المنصوص عليها في البند (1) من هذه الفقرة.

3- قبل التعامل بالبطاقات المزورة أو المقلدة أو المنسوخة أو غيرها من وسائل الدفع الإلكتروني أو بيانات وسائل الدفع الإلكتروني المستولى عليها بطريقة غير مشروعة مع علمه بعدم مشروعيتها.

ب- إذا جرى استخدام البيانات والمعلومات للحصول على أموال الغير أو الاستفادة مما تتيحه من خدمات ولم يفض الاستخدام إلى نتيجة يعاقب بالحبس مدة لا تقل عن سنتين ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن (5000) خمسة آلاف دينار ولا تزيد على (15000) خمسة عشر ألف دينار.

ج- إذا نجم عن الأفعال المنصوص عليها في الفقرتين (أ) و(ب) من هذه المادة الاستيلاء لنفسه أو لغيره على مال مملوك للغير أو الاستفادة مما تتيحه من خدمات فتكون العقوبة الحبس مدة ثلاث سنوات وغرامة لا تقل عن (10000) عشرة آلاف دينار ولا تزيد على (20000) عشرين ألف دينار"[118].

وقد نص مشروع قانون مكافحة الجرائم الإلكترونية على هذه الجريمة " يعاقب بالحبس مدة لا تزيد على سنة، أو بغرامة لا تزيد على مليون ريال أو بالعقوبتين معًا، كل من استخدم موقعًا إلكترونيًا أو نظام معلومات إلكترونيًا أو شبكة معلوماتية أو وسيلة تقنية معلومات في الوصول دون وجه حق إلى أرقام أو بيانات أو خدمات بطاقات الائتمان أو البطاقات الإلكترونية أو أرقام أو بيانات حسابات مصرفية أو غيرها من وسائل أو أدوات الدفع الإلكتروني".

وبناء على النصوص السابقة تتمثل أركان هذه الجريمة في الركن المادي الذي يتحقق بقيام الجاني بأحد الأفعال المنصوص عليها في نص المادة 4 من قانون مكافحة الجرائم الإلكترونية الأردني ومنها: الحصول على بيانات الحسابات البنكية أو المالية أو تلك المتعلقة بوسائل الدفع الإلكتروني أو في تنفيذ المعاملات المالية أو المصرفية الإلكترونية أو استخدم أو نشر أيا من هذه البيانات بطريقة غير مشروعة، أو قيام الجاني باصطناع أو إنشاء أو وضع أو تصميم أي وسيلة من وسائل تقنية المعلومات أو برنامج معلوماتي أو أمر برمجي بقصد تسهيل الحصول على البيانات المالية[119]، إذا تم استخدام البيانات والمعلومات المذكورة للحصول على أموال الغير أو الاستفادة مما تتيحه من خدمات. ويتحقق ركنها المعنوي في القصد الجنائي العام المتمثل بقيام الجاني بجميع الأفعال السابقة الإشارة إليها عن وعي وبصيرة واتجهت إرادته إلى القيام بها وهو عالم بنتائجها وآثارها في المجني عليه[120].

(1) وقد سار على ذات النهج كثير من التشريعات العربية، والاتفاقيات الدولية.

(2) د. إبراهيم السيد حسانين زايد: مرجع سابق، ص183.

(3) د. عمر محمود الحوني: مرجع سابق، ص115.

ثانيًا: جريمة الاستغلال غير المشروع لبطاقات الائتمان[121] والتعدي على النقود الرقمية:

ازدهرت العمليات المصرفية في الآونة الأخيرة بشكل مطرد، وأصبحت هذه الخدمات تقدم بسرعة وإتقان عبر وسائل إلكترونية مستحدثة سواء في البنوك أم المؤسسات المالية، وقد كان على رأس تلك الوسائل بطاقة الائتمان الممغنطة التي أضحت تمثل نسبة كبيرة من المعاملات المالية، ما يعني أن هناك ضرورة ملحة لحماية جميع المتعاملين بهذه البطاقات وحماية حقوقهم وأموالهم ومنع الاعتداء عليها[122].

وتعددت الجرائم الواقعة على بطاقات الدفع الإلكتروني أو بطاقات الائتمان[123]، ولعل جريمة الاستغلال غير المشروع لبطاقات الدفع الإلكتروني تعد من أبرز صور الجرائم الإلكترونية والأكثر انتشارا في الوقت الحالي[124]، وهي تهدد أمن واقتصاد الدول بصفة عامة والمؤسسات المالية والمصرفية وكذا الأفراد بصفة خاصة، خاصة مع ازدهار التجارة الإلكترونية التي أصبحت تعتمد على البطاقات المالية في معاملاتها بشكل كبير، وتعد البطاقات المالية نقودا إلكترونية يتم الاستيلاء عليها عن طريق استخدام أساليب غير

(4) تعرف بطاقات الائتمان التي يطلق عليها بالإنجليزية Credit cards، بأنها بطاقات بلاستيكية صغيرة الحجم مع شريط مغناطيسي يحتوي على رمز يتم قراءته من الصراف الآلي، وتكون صادرة من مؤسسات مالية معتمدة وتستعمل في عمليات البيع والشراء إضافة إلى التجارة الإلكترونية؛ إذ تقوم الشركات المصنعة للبطاقات الائتمانية بوضع سقف أعلى من النقود التي يتم استخدامها في البطاقة، وتمتاز بطاقات الائتمان بأن كمية النقود المدفوعة من خلالها لا يتم خصمها من الحساب البنكي مباشرة وإنما يتم خصمها من كمية النقود الدائنة من الشركة المزودة؛ إذ يتم دفع النقود مرة واحدة كل 30 يومًا، ويمكن للعميل عن طريق بطاقة الائتمان دفع النقود المدينة كاملة أو على أجزاء بإضافة نسبة فائدة بنكية. وتتنوع هذه البطاقات فمنها ما يطلق عليه الفيزا كارد، وأخرى فيزا إلكترونية، الماستر كارد، وهكذا، ومن ناحية العمليات المالية التي تقوم بها فقد تعددت بطاقات الائتمان فمنها: 1- بطاقات السحب الآلي و هي عبارة عن بطاقة يلتصق بها شريط ممغنط تسجل عليه معلومات عن رقم حساب العميل وأسمه ورقم البطاقة يتأكد من صحتها جهاز الحاسوب عند سحب النقود بواسطتها من جهاز الصراف الآلي بعد إعطائه الرقم السري لحساب العميل، فإذا ما تم سحب المبلغ أعاد الجهاز البطاقة لحاملها بعد أن يكون قد قيد فورا القيمة وبعد سحب النقود تسجل آليا في حساب العميل. 2- بطاقات الوفاء وتستعمل بطاقات الوفاء لدفع قيمة السلع والخدمات للمحلات التجارية وتستوفى من البنك الذي أصدر هذه البطاقات؛ إذ يقوم التاجر بتدوين العملية وإرسال نسخة منها إلى البنك المصدر لها لتسديد الثمن ويقوم البنك أيضا بتزويد العميل بكشف حساب في ميعاد دوري محدد ليتم تسديد قيمة المشتريات للبنك الذي قام بدفعها أو أن يقوم بقيد هذا المبلغ في حسابه الذي يحتفظ فيه العميل عادة في البنك، وتسمى طريقة الدفع هذه بطريقة الدفع غير المباشر. 3- أما بطاقات ذات الدفع الفوري (online) حيث يسلم العميل بطاقته إلى محاسب المحل التجاري الذي يقوم بتمرير البطاقة على جهاز موجود لديه للتأكد من وجود رصيد للعميل في البنك المصدر للبطاقة لتسديد قيمة المشتريات، والذي لا يتم إلا بعد أن يدخل العميل رقما سريا في الجهاز، فإذا قام العميل بإدخال هذا الرقم في الجهاز فإنه يكون قد فوض البنك بتحويل القيمة المطلوبة من حسابه إلى حساب التاجر؛ إذ تتم عملية التحويل هذه بشكل مباشر وفي نفس اللحظة في قيود بنك العميل وبنك التاجر، وبذلك تكون بمثابة دفع فوري بواسطة ترحيل المبالغ من حساب العميل إلى حساب التاجر. 4- بطاقة ضمان الشيكات تضمن البنوك الدفع للتجار عند استعمال العملاء لهذا البطاقة في حدود المبالغ المعينة بها، وعند إعطاء الشيك لأحد التجار تبرز البطاقة ويدون رقمها على ظهر الشيك، وعلى التاجر أن يتحقق من مطابقة البيانات المدونة على البطاقة مع البيانات المدونة على الشيك، وتعطي هذه البطاقة العميل إمكانية السحب الأسبوعي أو الشهري المبلغ محددًا بواسطة شيك، وذلك من كل البنوك التي تنضم لهذا النظام. 5- بطاقة الاعتماد تمنح هذه البطاقة لحاملها الحصول على تسهيل ائتماني من البنك حسب الشروط المتفق عليها، فهي بطاقة وفاء تمنح لحاملها ائتمانا بقدر معين من النقود يزيد عن المبلغ الموجود في حساب العميل، وتعطي البنوك مهلة معينة لتسديد قيمة المشتريات بعد أن يكون البنك قد سدد قيمتها. للمزيد انظر: د. عبد الكافي مريم، د. بوريابة صورية: جريمة الاحتيال المعلوماتي الواقعة على البطاقات المالية الإلكترونية، مجلة القانون والعلوم السياسية، المجلد 8 العدد 1، 2022، ص406، حفيظة قايد: الآليات القانونية لحماية بطاقة الائتمان الإلكترونية على الصعيد الوطني والدولي، مجلة معارف العلوم القانونية والاقتصاد، المجلد2العدد2021،2ص112، عادل يوسف الشكري الحماية الجنائية لبطاقات الدفع الإلكتروني، مجلة جامعة الكوفة، العدد 11، 2008، ص88، محمد عادل علي عبد السلام: الأحكام الموضوعية والإجرائية في جريمة السرقة المعلوماتية، مرجع سابق،ص274، د. أمير فرج يوسف: بطاقات الائتمان والحماية الجنائية لها، دار المطبوعات الجامعية2008، ص31 وما بعدها، د. عبد الفتاح بيومي حجازي: مرجع سابق، ص548.

(1) د. نور سليمان يوسف يعقوب البالو: مرجع سابق، ص252.

(2) د. محمد عادل علي عبد السلام: الأحكام الموضوعية والإجرائية في جريمة السرقة المعلوماتية، مرجع سابق، ص274، د. باهة فاطمة: الاعتداءات الواقعة على بطاقات الدفع الإلكتروني، المجلة الجزائرية للعلوم القانونية والسياسية والاقتصادية، المجلد 57 العدد 4، 2020، ص173.

(3) د. امير فرج يوسف: المرجع السابق، ص190.

مشروعة، ما دفع بالمقننين إلى تجريم هذه الصور الحديثة للجرائم والتصدي لها[125].

فقد نص المقنن المصري على هذه الجريمة بشكل واضح في المادة 23 من قانون مكافحة جرائم تقنية المعلومات؛ إذ نصت على أن " يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر والغرامة التي لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، في الوصول بدون وجه حق إلى أرقام أو بيانات أو بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الإلكترونية، فإن قصد من ذلك استخدامها في الحصول على أموال الغير أو ما تتيحه من خدمات فيعاقب بالحبس مدة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين. وتكون العقوبة الحبس مدة لا تقل عن سنة، والغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز 200 ألف أو إحدى هاتين العقوبتين، إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على تلك الخدمات أو مال الغير".

أما المقنن الإماراتي فقد كان أكثر وضوحًا في تحديد عناصر هذه الجريمة حيث نص على هذه الجريمة في المادة 15 من قانون مكافحة الشائعات والجرائم الإلكترونية وقد جرى نصها على أن "يعاقب بالحبس والغرامة التي لا تقل عن (200,000) مائتي ألف درهم ولا تزيد على (2,000,000) مليوني درهم، أو بإحدى هاتين العقوبتين، كل من زور أو قلد أو نسخ بطاقة ائتمانية أو بطاقة مدينة أو أي وسيلة من وسائل الدفع الإلكتروني أو استولى على بياناتها أو معلوماتها، وذلك باستخدام وسائل تقنية المعلومات، أو نظام معلوماتي. ويعاقب بذات العقوبة كل من:

1. صنع أو صمم أي وسيلة من وسائل تقنية المعلومات، أو برنامج معلوماتي، بقصد تسهيل أي من الأفعال المنصوص عليها في الفقرة الأولى من هذه المادة.

2. استخدم بدون تصريح بطاقة ائتمانية أو إلكترونية أو بطاقة مدينة أو أي وسيلة من وسائل الدفع الإلكتروني أو أيًا من بياناتها أو معلوماتها، بقصد الحصول لنفسه أو لغيره، على أموال أو أملاك الغير أو الاستفادة مما تتيحه من خدمات يقدمها الغير.

3. قبل التعامل بهذه البطاقات المزورة أو المقلدة أو المنسوخة أو غيرها من وسائل الدفع الإلكتروني ببيانات وسائل الدفع الإلكتروني المستولى عليها بطريقة غير مشروعة مع علمه بعدم مشروعيتها".

وهو ذاته نص المادة 12 من مشروع قانون مكافحة الجرائم الإلكترونية السابقة الإشارة إليها، ونتمنى عند إصدار القانون في صورته النهائية أن يضع المقنن نصوصًا لتشديد العقوبة في حال كان هناك استغلال لبطاقات الائتمان أو النقود الإلكترونية كما هو الشأن في التشريعات المقارنة.

من النصوص السابقة يتبين أن جريمة الاستغلال غير المشروع لبطاقات الائتمان أو البطاقات المالية تقوم في حق الجاني متى تحقق ركناها المادي المتمثل في السلوك الإجرامي غير المشروع والمجرم من قبل المقنن [126] المتمثل في تزوير أو تقليد أو نسخ بطاقة ائتمانية أو بطاقة مدينة أو أي وسيلة من وسائل الدفع الإلكتروني أو استولى على بياناتها أو معلوماتها أو صنع أو صمم أي

(4) د. عبد الكافي مريم، د. بوربابة صورية: مرجع السابق، ص411، د. هروال هبة نبيلة: مرجع سابق، ص293.

(1) د. محمد عادل عبد السلام: الأحكام الموضوعية والإجرائية في جريمة السرقة المعلوماتية، مرجع سابق، ص167 وخصوصًا ص310.

وسيلة من وسائل تقنية المعلومات، أو برنامجًا معلوماتيًا، للتزوير أو التقليد أو النسخ أو الاستيلاء على بيانات البطاقات المالية أو استخدم بدون تصريح بطاقة ائتمانية أو إلكترونية أو بطاقة مدينة أو أيًا وسيلة من وسائل الدفع الإلكتروني أو أيًا من بياناتها أو معلوماتها، بقصد الحصول لنفسه أو لغيره، على أموال أو أملاك الغير أو الاستفادة مما تتيحه من خدمات يقدمها الغير[127]، ويشمل ذلك قبول الجاني التعامل بهذه البطاقات المزورة أو المقلدة أو المنسوخة أو غيرها من وسائل الدفع الإلكتروني. وأما ركنها المعنوي فإنه يتحقق بتحقق العلم بعناصر الجريمة واتجاه إرادته إلى ارتكابها على الرغم من ذلك وهو ما يعرف بالقصد الجنائي العام[128].

ثالثًا: جريمة تقليد واستعمال النقود الإلكترونية:

تعد النقود الإلكترونية[129] الوسيلة المثلى في معاملات التجارة الإلكترونية، ورغم خصائصها المميزة قد تثير الكثير من المخاطر، ولذلك فقد حرصت التشريعات الحديثة على وضع حماية لها ضمانًا لاستقرار التعامل بها ومنحها الثقة والائتمان، من ذلك نجد نص المادة

(1) د. نور سليمان يوسف يعقوب البالو: الأحكام الموضوعية لجرائم المعلوماتية، مرجع سابق، ص259.

(2) د. إبراهيم السيد حسانين زايد: التحويل الإلكتروني، مرجع سابق، ص178.

(3) تعرف النقود الإلكترونية E-MONEY قيمة نقدية مخزنة أو منتَجًا مدفوع القيمة مقدما؛ إذ يتم تخزين سجل بالأموال أو القيمة المتاحة لاستخدام المستهلك في أغراض متعددة داخل بطاقة مدفوعة مسبقا أو جهاز إلكتروني مثل الكمبيوتر أو الهاتف. والنقود الإلكترونية أداة دفع مقبولة لجميع الأطراف بخلاف الجهة المُصْدِرة لها (للاستخدام في أغراض متعددة). وتمثل القيمة المُخزنة استحقاقًا إلزاميا على مُصْدِر النقود الإلكترونية لسداد الرصيد بالكامل عند الطلب. وتشمل أنواع المعاملات النقدية الإلكترونية وهي ما تعرف بسلسلة البلوك تشين أو العملات المشفرة: عملة البنك المركزي الرقمية Central Bank Digital Currency ربما تصبح شكلا رقميا جديدا من نقود البنك المركزي يختلف عن الاحتياطيات أو أرصدة التسوية التي تحتفظ بها البنوك التجارية لدى البنوك المركزية. وتمثل هذه العملة التزاما على البنك المركزي مقوَّما بوحدة حساب موجودة بالفعل، وتعمل وسيطا للتبادل ومخزنا للقيمة. والعملات الرقمية للبنوك المركزية (CBDC) ليست أصولا مشفرة. الشمول المالي Financial Inclusion إمكانية حصول الأفراد ومؤسسات الأعمال على ما يلبي احتياجاتهم من منتجات وخدمات مالية نافعة وذات تكلفة ميسورة – مثل المعاملات والمدفوعات والمدخرات والائتمان – ويتم تقديمها بشكل مسؤول ومستدام. العملة الرقمية المستقرة Stablecoin أصل مشفر يهدف إلى الحفاظ على قيمة ثابتة مقابل أصل محدد أو سلة أصول. التمويل اللامركزي decentralized finance (DEFI) مجموعة بديلة من الأسواق والمنتجات والأنظمة المالية تستخدم الأصول والبرمجيات المشفرة المعروفة باسم "العقود الذكية" المصممة باستخدام تكنولوجيا دفاتر الحسابات الرقمية الموزعة أو تكنولوجيا مماثلة. الأصل المالي غير المدعوم UNBACKED CRYPTO ASSET أصول مشفرة لا تندرج تحت الأصول المشفرة المرمّزة ولا العملات الرقمية المستقرة. الأوراق المالية المُرَمَّزة SECURITY TOKENS أصول مشفرة ينطبق عليها تعريف الورقة المالية في البلد الذي يتم فيه إصدارها أو تسويقها أو تحويلها أو تبادلها أو تخزينها. سلسلة الكتل (البلوك تشين)BLOCKCHAIN دفتر حسابات رقمية موزع يُحْتَفظ فيه بتفاصيل المعاملات في شكل كتل من المعلومات. وتُرفَق كتلة جديدة بسلسلة الكتل الموجودة من خلال عملية محوسبة تصادق على صحة المعاملات. الأصول الرقمي DIGITAL ASSETS أداة رقمية يتم إصدارها أو تمثيلها باستخدام دفتر الحسابات الموزع أو غيره من التكنولوجيات المماثلة. وتُستبعد من ذلك الأدوات الرقمية الممثِّلة للعملات الورقية الإلزامية. تكنولوجيا دفاتر الحسابات الرقمية الموزعة distributed ledger technology (DLT) وسيلة لحفظ المعلومات بواسطة دفتر حسابات رقمية موزع، كأنها نسخة رقمية مكررة من البيانات تتاح في عدة مواقع. وتمثل هذه الوسيلة قاعدة بيانات يتم تخزينها وإتاحتها للمستخدمين وضمان تزامنها على شبكة كمبيوتر. ويتم تحديث البيانات على أساس توافق الآراء بين المشاركين في الشبكة. ومن أمثلتها تكنولوجيا سلسلة الكتل، لكنها لا تعتمد بالضرورة على هيكل سلسلة الكتل ذاته في حفظ السجلات. الأصل المشفر Crypto Asset يُعْرَف أيضا باسم العملة المشفرة، وهو عملة رقمية يصدرها القطاع الخاص وتعتمد بشكل أساسي على علم التشفير ودفاتر الحسابات الموزعة أو تكنولوجيا أخرى مماثلة. رموز المنفعة Utility Tokens أصول مشفرة تعطي لحاملها حق الحصول على منتَج أو خدمة قائمَين أو مرتقبين من جهة الإصدار أو الشبكة المُصْدِرة. للمزيد انظر: موقع صندوق النقد الدولي على الرابط الآتي:
https://www.imf.org/ar/Publications/fandd/issues/2022/09/Digital-Money-101-explainer
وفي الفقه العربي انظر: محمد دمان ذبيح: النقود الإلكترونية، مجلة الشريعة والاقتصاد جامعة الأمير عبد القادر للعلوم الإسلامية، العدد 1 المجلد 10 -2021، ص133 وما بعدها، د. أحمد يوسف جمعة: الإرهاب السيبراني، دار الأهرام 2022، ص100 وما بعدها، د. إبراهيم السيد حسانين زايد: المواجهة الجنائية لظاهرة التحويل الإلكتروني غير المشروع للأموال، مرجع سابق، د.هيثم محمد حرمي شريف: النقود الإلكترونية، مجلة الشريعة والقانون، جامعة الإمارات، العدد 84 – 2020، ص405، يوسف بن هزاع بن مساعد الشريف، الأحكام والضوابط الفقهية المتعلقة بالنقود الرقمية الإلكترونية، مجلة جامعة الملك عبد العزيز، العدد 5، ص29، عبد الله لعور، عبد الرزاق كبوط: العلاقة بين النقود الرقمية والعملات الرقمية والعملات الافتراضية والعملات المشفرة، مجلة الاقتصاد الصناعي، خزارتك، مجلد 11 العدد 2 – 2021، ص4.

116 الفقرة رقم 5 من قانون المعاملات الإلكترونية اللبناني إذ جرى نصها بما يأتي "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبالغرامة من عشرة ملايين إلى مئتي مليون ليرة لبنانية أو بإحدى هاتين العقوبتين كل من قلد نقودًا إلكترونية أو رقمية"، وقد جاء مشروع قانون مكافحة الجرائم الإلكترونية بنص عام حيث جرم الأفعال المكونة لجريمة التزوير الإلكتروني، بما يضمن ذلك ربما النقود الإلكترونية، وكان الأحرى بمقترحي المشروع أن يعالجوا جميع الصور خصوصا في ظل تطور فكرة النقود الإلكترونية ويبدأ من حيث أنتهى الآخرون لا من حيث بدايتهم.

وتتنوع الجرائم التي تقع على النقود الإلكترونية ولعل أبرزها هي جريمة تقليد النقود الإلكترونية، والجريمة الأخرى جريمة استعمال النقود الإلكترونية، فأما جريمة التقليد للنقود الإلكترونية فتتخذ صورة تقليد البرمجيات الخاصة بالنقود الإلكترونية لتظهر كأنها نسخة طبق الأصل من النقود الإلكترونية الأصلية، وتتحقق أركان جريمة تقليد النقود الإلكترونية بتحقق أركانها، فأما ركنها المادي فيتمثل في واقعة التقليد ذاتها للنقود الإلكترونية كقيام الجاني بصناعة الدعامة الإلكترونية أو البرمجية على خلاف حقيقتها الأصلية ووضع فئة نقدية[130]. وأما ركنها المعنوي فيتمثل في القصد الجنائي العام حيث يجب أن تنصرف إرادة الجاني إلى فعل تقليد العملة الرقمية ومعالجتها إلكترونيا، واتجاه فعل التقليد على معطيات لا أصل لها، ومن جهة أخرى يتطلب لهذه الجريمة القصد الجنائي الخاص المتمثل في دفع النقود غير الصحيحة في التعامل على أنها عملة صحيحة[131].

أما جريمة استعمال النقود الإلكترونية المقلدة فتتحقق بتحقق ركنها المادي المتمثل في استعمال الجاني للنقود الإلكترونية المقلدة سواء كانت من تقليده وإنتاجه، أم كانت من إنتاج برمجة الغير، وهنا لا يكفي أن تكون هذه العملات الرقمية في حيازة الجاني فقط بل يجب أن يقوم باستعمالها من خلال دفعه للغير هذه النقود سواء باستعمال مباشر بأن يقوم بالدفع من خلالها في معاملاته مع الغير أم ترويج هذه العملات للغير. وأما ركنها المعنوي فيتمثل في القصد الجنائي المتمثل في قيام الجاني باستعمال النقود الإلكترونية وهو عالم أنها مقلدة واتجهت إرادته إلى ذلك على الرغم من هذا العلم، مع توافر القصد الخاص المتمثل في نية الاستعمال أو التعامل[132].

المطلب الثاني جريمة انتهاك حقوق الملكية الفكرية

مع التحول الكبير في تكنلوجيا المعلومات وما ترتب على ذلك من أنتشار التعاملات الإلكترونية التي طالت أرجاء المعمورة، وما صحب ذلك من الاعتداءات المتزايدة على حقوق الملكية الفكرية بجميع صورها[133]؛ إذ يصعب مع هذه التقنيات المتطورة المحافظة على حقوق الملكية الفكرية؛ لأننا أمام عالم مفتوح[134]، وهنا سعت كثير من التشريعات إلى وضع نصوص تشريعية تحمي حقوق الملكية الفكرية في الفضاء السيبراني، كما تركزت الجهود الدولية لحماية الملكية الفكرية فبرزت إلى النور اتفاقيات

(1) د. سامي منصور: الأعمال الجرمية التي تستهدف الأنظمة المعلوماتية، المنشورات الحقوقية، 2011، ص76.
(2) د. سمير عالية: الجرائم الإلكترونية، مرجع سابق، 192 وما بعدها.
(1) د. سمير عالية: مرجع سابق، ص197.

(2) للمزيد حول جرائم الاعتداء على حقوق الملكية الفكرية وصوره انظر: د. عمر محمد أبو بكر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق 481 وما بعدها، أسامة أحمد المناعي (وآخرون) جرائم الحاسب الآلي والإنترنت، وائل للنشر والتوزيع، 2001، ص144.
(3) د. هروال هبة نبيلة: مرجع سابق، ص206.

ومنظمات تعمل على تنظيم مسألة حماية الملكية الفكرية في تعاملات الإنترنت[135].

وتعرف الملكية الفكرية بأنها إبداعات الإنسان وأفكاره وكل ما يتعلق بالإنتاج الفكري له، وقد جرى تعريفها من قبل المنظمة العالمية للملكية الفكرية أنها " الحقوق الخاصة بالأعمال الأدبية والفنية والعلمية، كالعروض الفنية وألونجرام والأعمال الإبداعية والاختراعات في جميع المجالات والاكتشافات العلمية والتصميمات الصناعية والعلامات التجارية وعلامات الخدمات والأسماء التجارية والحماية من المنافسة غير العادلة وأي حقوق أخرى تكفلها الأنشطة الفكرية في المجالات الصناعية والعملية والأدبية والفنية"[136].

وتتنوع صور وأشكال التعدي على حقوق الملكية الفكرية في نطاق شبكة الإنترنت إلى الحد الذي يصعب معه حصرها فهي متجددة ومتطورة مع تطور التكنلوجيا، وتتمثل أغلب صور المنازعات حول العلامات التجارية وأسماء المواقع بتسجيل أسماء متطابقة أو متشابهة مع العلامة التجارية المشهورة وتسجيلها بقصد منع أصحاب هذه العلامات المشهورة من تسجيل عناوينهم الإلكترونية وابتزازهم إذا ما رغبوا في تسجيلها عن طريق الحصول على تلك العناوين عن طريق طلب مبالغ مالية باهظة مقابل التنازل عن ذلك العنوان أو الموقع وهو ما بات يعرف ب Cybersquatting والأمر ذاته في تقليد مواقع لشركات تجارية وتسجيل مواقع مشابهة لعلامة تجارية مشهورة مع تعديل طفيف عليها ما يوقع المتعاملين في لبس حول حقيقة هذه العلامة مثل موقع www.abidas.com لتضليل مستخدمي الشركة الأم Adidas[137].

ومن ناحية أخرى نجد أن جريمة تقليد البرامج الإلكترونية تأخذ مساحة كبيرة في حيز جرائم انتهاك الملكية الفكرية عبر شبكة الإنترنت[138]؛ إذ نجد أن كثيرًا من المهكرين يقومون بتقليد برامج إلكترونية مهمة ويقومون بإنزالها بأسعار زهيدة مقارنة بالبرامج الأصلية، وقد شجع على هذه الجريمة ضعف العقوبة التي يواجه بها المجرم؛ إذ تصنف هذه الجريمة أنها من ضمن مخالفات حقوق التأليف، وذلك لأن البرامج الإلكترونية مدرجة ضمن المصنفات التي يحميها حقوق التأليف[139]، وتأخذ جريمة الاعتداء على البرامج الإلكترونية أشكالًا متعددة منها: نسبة البرنامج إلى شخص على خلاف الحقيقة؛ إذ يقوم الشخص بنسبة البرنامج إلى نفسه بوضع اسمه عليه، وكذا إعادة إنتاج البرنامج بصورة غير مشروعة أو تقليده له على الرغم من عدم الترخيص له بذلك، وتعد

(4) من ذلك دور المنظمة العالمية لحقوق الملكية الفكرية WIPO حيث أدت دورا مهمًا وأساسيًا في هذا الشأن، فقد عملت على إصدار وثيقتين مهمتين لحماية الملكية الفكرية وهما: معاهدة حماية حقوق الطبع والنشر WCT التي عرفت بمعاهدة الإنترنت الأولى، ومعاهدة أخرى لعمليات الأداء والفنوجرام المعروفة ب WPPT التي سميت فيما بعد بمعاهدة الإنترنت الثانية، للمزيد انظر: محمد حسين منصور: المسؤولية الإلكترونية، مرجع سابق، ص259، وقد جاءت اتفاقية بودابست لتنظم هذه المسألة من خلال المادة 10 حيث جرمت الاعتداء على الملكية الفكرية والحقوق المجاورة لها، للمزيد انظر: هلالي عبد الإله أحمد: جرائم المعلوماتية عابرة للحدود، مرجع سابق، ص127.

(5) د. هشام مسعودي: حماية الملكية الفكرية لحقوق المؤلف للمصنفات الرقمية، مجلة الدراسات القانونية، المجلد 8 العدد 2، 2022، ص848.

(6) د. عاقلي فضيلة: حماية حقوق الملكية الفكرية والصناعية من الجريمة المعلوماتية، مجلة الاقتصاد الصناعي، جامعة باتنة 1 الحاج لخضر الجزائر، العدد 12، 2017م، ص238، د.هروال هبة نبيلة: مرجع سابق، ص206.

(1) وقد عرفت البرامج الإلكترونية بأنها " مجموعة من المعطيات والمعلومات المكتوبة بإحدى لغات البرمجة التي يفهمها جهاز إلكتروني معلوماتي سواء أكان حاسوبًا أو جهازًا إلكترونيًا للتعامل معها بغرض استقبال الاستفهامات من قبل المستخدم لتحليلها ومعالجتها ومن ثم إعطاء النتائج المطلوبة"، انظر: د. نور سليمان يوسف يعقوب البالو: مرجع سابق، ص264.

(2) د. عيسائي طه، عبد الله فوزية: المصنفات الرقمية المشمولة بالحماية بموجب قوانين الملكية الفكرية في الاتفاقيات الدولية والقانون الجزائري، دفاتر السياسة والقانون، المجلد 13 العدد 1، 2021، ص134.

جريمة سرقة البرنامج بجميع مكوناته باعتباره مالًا متقوما، أو بقيامه بتعديل البرنامج أو تزويره من خلال الإضافة أو المحو أو التغيير، أو قيام الجاني بإتلاف البرنامج أو تعطيله، أو قيامه بالاستنساخ غير المشروع للبرامج وبيعها والمتاجرة بها[140].

كما تعد جريمة النشر الإلكتروني للمصنفات [141] المختلفة من الجرائم البارزة عبر شبكة الإنترنت التي تخضع لحماية الملكية الفكرية [142]، فحماية المصنفات على شبكة الإنترنت باتت من أهم المجالات التي عملت الاتفاقيات الدولية إلى حمايتها ووضع تنظيم يكفل عدم التعدي عليها، وقد سعت منظمة الوايبو منذ وقت مبكر إلى تنظيم حماية المصنفات من خلال اتفاقية الوايبو لحقوق المؤلف المعروفة باتفاقية الإنترنت الأولى وهو كذلك في اتفاقية الوايبو الثانية[143].

ويمكن أن نجمل بعض أنماط جرائم الاعتداء على حقوق الملكية الفكرية في البيئة الرقمية وآلية حمايتها في ظل قانون حماية حق المؤلف والحقوق المجاورة اليمني رقم 15 لسنة 2012م[144]، وكذا قانون براءة الاختراع ونماذج المنفعة اليمني رقم 2 لسنة 2011م[145]، والقانون رقم 28 لسنة 2010م بشأن التصاميم الصناعية[146]، والقانون رقم 23 لسنة 2010م بشأن العلامات التجارية والمؤشرات الجغرافية[147]، والقانون رقم 20 لسنة 2003م بشأن الأسماء التجارية[148]، وكذا ما جاء في الاتفاقيات الدولية، كل ذلك على النحو الآتي:

أولًا: جريمة بيع أو تأجير أو عرض أو استيراد أو تصدير أو – وضع للتداول – مصنف أو تسجيل صوتي أو برنامج إذاعي:

نصت على هذه الجريمة المادة 77 الفقرة 2 من قانون حماية حق المؤلف والحقوق المجاورة اليمني؛ إذ نصت على الآتي " دون الإخلال بأية عقوبة أشد منصوص عليها في أي قانون آخر، يعاقب بغرامة لا تقل عن (خمسمائة ألف ريال يمني) أو الحبس مدة لا تقل عن شهر حسب جسامة الجُرم كل من ارتكب أيًا من المخالفات الآتية: ... 2- بيع أو تأجير أو عرض أو استيراد أو تصدير أو وضع – للتداول – مصنف أو تسجيل صوتي أو برنامج إذاعي، محمي طبقًا لأحكام هذا القانون، دون إذن كتابي مسبق من المؤلف أو صاحب الحقوق المجاورة".

وبناء على ذلك فإن تتحقق الجريمة بقيام الركن المادي للجريمة المتمثل في قيام الجاني بارتكاب إحدى صور السلوك المجرم في النص المشار إليه وهي: البيع، والتأجير، أو عرض المصنف أو وضعه للتداول، أو استيراد أو تصدير المصنف عبر شبكة الإنترنت، وكل ذلك مشروط بأن يكون دون إذن كتابي مسبق من المؤلف أو صاحب الحق المجاور. ويتحقق الركن المعنوي لهذه الجريمة المتمثل في القصد الجنائي العام

(3) د. بقنيش عثمان محاضر، مصطفى منشور وسيمة: حماية الملكية الفكرية عبر الإنترنت في إطار المنظمة العالمية للملكية الفكرية، مجلة البحوث في الحقوق والعلوم السياسية، العدد2، 2015، ص262.

(4) د. هشام مسعودي: مرجع سابق، ص850.

(5) د. سلام منعم مشعل، د. محمد سمير صالح: الحماية القانونية لحقوق الملكية الفكرية الرقمية، المجلة الأكاديمية للبحث القانوني، المجلد 15 العدد 1، 2017، ص115.

(6) انظر: الاتفاقيتين على موقع المنظمة الدولية لحماية الملكية الفكرية: www.wipo.int

(7) منشور في الجريدة الرسمية العدد 14 لسنة 2012م.

(8) منشور في الجريدة الرسمية العدد 1ج1 لسنة 2011م.

(9) منشور في الجريدة الرسمية العدد 24 ج1 لسنة 2010.

(10) منشور في الجريدة الرسمية العدد 22 لسنة 2010.

(11) منشور في الجريدة الرسمية العدد 5 لسنة 2003.

بعنصريه–العلم والإرادة–وذلك بأن يعلم الجاني أنه يقوم بارتكاب السلوك المجرم وتتجه إرادته إلى تحقيقه[149].

ثانيًا: جريمة تقليد واستغلال البرامج الإلكترونية[150].

نصت المادة 77 من قانون حماية حق المؤلف والحقوق المجاورة على الآتي " دون الإخلال بأية عقوبة أشد منصوص عليها في أي قانون آخر، يعاقب بغرامة لا تقل عن (خمسمائة ألف ريال يمني) أو الحبس مدة لا تقل عن شهر حسب جسامة الجُرم كل من ارتكب أيًا من المخالفات الآتية: ... 4- تقليد مصنف أو تسجيل صوتي أو برنامج إذاعي منشور في الجمهورية أو في الخارج، مع العلم بعمل التقليد، وبيعه أو عرضه للبيع أو للتداول أو للإيجار أو تصديره إلى خارج الجمهورية".

كما نصت المادة 36 من قانون براءة الاختراع على أن " يعاقب بغرامة لا تزيد عن مليون ريال كل من: 1- قلد بقصد الاتجار موضوع براءة أو نموذج منفعة أو تصميم دائرة متكاملة مسجلة ومحمية وفقًا لأحكام هذا القانون. 2- باع أو عرض للبيع أو للتداول أو استورد أو حاز بقصد الاتجار منتجات مقلدة لموضوع اختراع مع علمه بذلك"

وبذلك تتحقق هذه الجريمة بتحقق الركن المادي لها والمتمثل في قيام الجاني بارتكاب أحد الأفعال المنصوص عليها في المواد السابقة من حيث تقليد البرامج الإلكترونية أو بيعه أو عرضه للتداول أو الإيجار أو إعادة تصديره وتسويقه للخارج، أو استيراد برامج مقلدة أو حتى الحيازة لبرامج مقلدة، ويجب أن يتحقق الركن المعنوي للجريمة المتمثل في قيام الجاني بالأفعال المجرمة وهو عالم بالتقليد[151]، مع توافر القصد الجنائي الخاص وهو قصد الاتجار، أي أنه لا تقوم الجريمة في هذه الحالة إلا إذا كان القصد من هذه الأفعال هو الاتجار بالبرامج الإلكترونية وتطبيقات الإنترنت أو المنتجات أو المصنفات التي تم تقليدها.

ثالثًا: جريمة وضع بيانات على منتجات أو إعلانات تجارية أو أدوات أو برامج تؤدي إلى الاعتقاد بانتماء البرنامج إليه:

نصت المادة 36 من قانون براءة الاختراع ونماذج المنفعة على أن " يعاقب بغرامة لا تزيد عن مليون ريال كل من: 3- وضع بغير حق على المنتجات أو الإعلانات التجارية أو أدوات التعبئة أو غير ذلك من بيانات تؤدي إلى الاعتقاد بحصوله على براءة اختراع أو براءة نموذج منفعة".

وبناء على هذا النص تتحقق هذه الجريمة بتحقق ركنها المادي المتمثل في قيام الجاني بارتكاب الأفعال المجرمة كان يقوم بوضع اسمه أو علامته التجارية أو أي بيان يجعل المتلقي يعتقد أن هذا البرنامج أو المنتج ينتمي اليه أو أنه يملكه كونه صاحب براءة الاختراع، ويتحقق ركنها المعنوي المتمثل في القصد الجنائي العام من حيث علم

(1) د. هائل حزام مهيوب العامري: حماية حق المؤلف في التشريع اليمني مقارنة ببعض التشريعات الأخرى، مجلة العلوم التربوية والدراسات الإنسانية، العدد 5 ابريل 2019، ص194.

(2) للمزيد في جرائم العدوان على البرامج الإلكترونية ومدى اعتبارها مصنفًا أدبيًا، انظر: د. عمر محمد أبو بكر بن يونس: مرجع سابق، ص545

(3) وقد اعترف القضاء الفرنسي بأن برنامج الحاسوب يتمتع بالحماية المقررة لحق المؤلف لأول مرة في قضية Pacbot وهو أحد مديري الحسابات في شركة BMW وكان قد أعد برنامجًا خاصًا بالمحاسبة يستعين به في ممارسة نشاطه المهني، إلا أنه رفض أن يمنح رب العمل حق عمل نسخة من هذا البرنامج فقررت الشركة فصله واتهمته بالسرقة لأخذه البرنامج لدى تركه العمل، فقضت محكمة Bobigny البدائية في حكمها الصادر عام ١٩٧٨ ببراءته استنادًا إلى أن فعله ليس سوى حبس لما يملكه، وأن إعداد البرنامج يعد عملًا فكريًا مبتكرًا تكون ملكيته قاصرة على مؤلفه (٣)، وقد قدم Pochot دعوى لدى محكمة باريس للنظر في فصله التعسفي قررت في حكمها الصادر عام ١٩٧٩ أن البرنامج يعبر عن جهد فكري شخصي لمؤلفه ويتمتع بالحماية كمصنف. مشار إليه في د. نور سليمان يوسف يعقوب البالو: مرجع سابق، ص272.

الجاني بالأفعال التي يقوم بها واتجاه إرادته إلى ارتكاب الجريمة على الرغم من ذلك[152].

رابعًا: جريمة الاعتداء على الاسم أو العلامة التجارية:

نصت المادة 30 من قانون الأسماء التجارية اليمني على الآتي " مع عدم الإخلال بأية عقوبة أشد منصوص عليها في القوانين الأخرى النافذة يعاقب كل من استعمل عمدًا اسمًا تجاريًا على خلاف أحكام هذا القانون واللائحة بغرامة لا تقل عن 5000 خمسة آلاف ريال ولا تزيد عن 50000 خمسين ألف ريال، وفي حال تكرار المخالفة يعاقب المخالف بالحبس مدة لا تقل عن شهر ولا تزيد عن ستة أشهر".

وقد جاء مشروع قانون مكافحة الجرائم الإلكترونية ليضع عقوبة لمثل هذا السلوك في المادة 16 جرى نصها على أن " يعاقب بالحبس مدة لا تزيد على سنتين، أو بغرامة لا تزيد على مليوني ريال أو بالعقوبتين معًا، كل من أنشأ أو أدار أو استخدم موقعًا إلكترونيًا أو نظام معلومات إلكترونيًا أو شبكة معلوماتية أو وسيلة تقنية معلومات في التعدي أو تسهيل التعدي، بأي وسيلة، وفي أي صورة، على حقوق المؤلف أو براءة الاختراع أو الأسرار التجارية أو العلامات التجارية أو البيانات التجارية أو الأسماء التجارية وغيرها من حقوق الملكية الفكرية المحمية قانونًا".

وهنا نجد أن النص قد حدد أركان الجريمة، فجريمة الاعتداء على الاسم أو العلامة التجارية تتحقق بتحقق الركن المادي المتمثل في استعمال اسم تجاري بالمخالفة لأحكام القانون، ويتحقق الركن المعنوي لهذه الجريمة بتوافر القصد الجنائي العام المتمثل في اتجاه إرادة الجاني إلى استخدام الاسم أو العلامة التجارية وهو عالم باستخدامه غير المشروع للاسم أو العلامة التجارية[153].

الخاتمة

في ختام هذا البحث يسعى الباحث إلى استخلاص أهم النتائج والتوصيات وذلك على النحو الآتي:

أولًا: النتائج:

1. تتسم الجريمة السيبرانية بأنها جريمة ناعمة يصعب اكتشافها وضبطها، كما أنها تتم عن بعد دون مراعاة للحدود الجغرافية للدول، ولذلك فهي دولية ويتم ارتكابها عن بعد، تتركز في أغلبها على البيانات والمعلومات الإلكترونية، وهذا ما يميز مرتكب الجريمة السيبرانية من أنه مجرم محترف ذو تأهيل فني وتقني، ومن هنا يحتاج لكشفها خبراء فنيون وتعاون دولي.
2. قيام جريمة السب والقذف في الفضاء السيبراني، وذلك من خلال استخدام أي تطبيق إلكتروني يتم النشر فيه لأي محتوى يعد إساءة للغير، سواء الفيس بوك أو إنستغرام أو يوتيوب أو واتس آب أو تويتر أو لينكد ان أو اسناب شات أو تلغرام أو تيك توك أو غيرها من البرامج، وسواء كان الفعل توجيه الإهانة أو التشهير بالغير أو إرسال رسالة منافية للآداب أو نقل خبر بقصد إثارة النعرات أو الفزع في المجتمع، أو اصطناع الصور المخلة بالآداب، أو التقاط صورة الشخص بغير إذنه، فشبكة الإنترنت وتطبيقاتها المختلفة تحقق العلانية حتى لو كانت عبر تطبيقات خاصة.
3. تعد البيانات الشخصية المتمثلة في جمع المعلومات المرتبطة بهوية الشخص سواء كان طبيعيًا أو اعتباريًا، كالاسم، أو الصوت، أو الصورة، أو الرقم التعريفي، أو المحدد للهوية عبر الإنترنت أو أي

(1) انظر: د. عمر محمد أبو بكر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص578.

(2) د. عمر محمد أبو بكر، مرجع سابق، ص578.

بيانات تحدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية هي الهدف للمجرم السيبراني حيث يقع عليها الاعتداء سواء بالجمع أو المعالجة أو الحفظ بدون رضا صاحبها، أو عدم الاحتراز لحمايتها، وأهمها اتخاذ التدابير اللازمة لذلك، أو إفشائها، ولذلك فقد سعت التشريعات المقارنة إلى وضع تنظيم كامل لحماية البيانات الإلكترونية الشخصية من خلال مجموعة من النصوص، إلا أن المشرع اليمني قد تخلف عن هذه التشريعات، فلم ينظم تلك الجرائم بل لم يتطرق لها في مشروع قانون مكافحة الجرائم الإلكترونية، ما يشكل عبئًا كبيرًا على أجهزة المكافحة والقضاة في التصدي لها ومواجهتها.

4. على الرغم من سن المشرع لقانون حماية المعاملات المصرفية في المعاملات الإلكترونية رقم 40 لسنة 2006م، يبقى هذا القانون قاصرًا عن معالجة جميع أشكال الجرائم التي تقع على الأموال بصفة عامة، سواء الحسابات البنكية أم بطاقات الائتمان والنقود الرقمية، أو تلك الحقوق المالية المتعلقة بالملكية الفكرية، كتقليد البرامج الإلكترونية واستغلالها والاعتداء على أسماء النطاق والاسم التجاري والعلامات التجارية، كما أنه لم يعالج المشكلة الأهم وهي جرائم غسل الأموال التي باتت شبكة الإنترنت والعملات الرقمية وسيلة مثلى لغسل الأموال دون اكتشافها. فقد توصل الباحث إلى أن هذه الجرائم جميعها هزت اقتصاديات دول عظمى، وهو ما يوجب على المشرع الإسراع إلى وضع منظومة تشريعية متكاملة لمواجهة تلك الجرائم.

ثانيًا: التوصيات:

1. يمثل الإطار التشريعي العمود الفقري لأي نظام عدلي في مواجهة الجرائم السيبرانية؛ إذ تُشكل القوانين المنظمة للتحقيق والضبط والتفتيش الإلكتروني الأساس الذي تستند إليه أجهزة إنفاذ القانون، وتبرز الحاجة إلى تطوير هذا الإطار نتيجة التغير المستمر في أنماط الجريمة الرقمية وتوسعها العابر للحدود، ما يتطلب قواعد إجرائية مرنة ومتكاملة تستوعب المستجدات التقنية، وتحمي في الوقت ذاته الحقوق الدستورية للمواطنين، وهنا يوصي الباحث المشرع اليمني بضرورة الإسراع إلى إصدار القوانين الخاصة بمواجهة الجرائم الإلكترونية والمعاملات الإلكترونية، ونقل البيانات والمعلومات الإلكترونية، وإجراء تعديلات مهمة على القوانين الإجرائية لتتلاءم مع التطور التشريعي، مثل قانون الإجراءات الجزئية والمرافعات وقانون الإثبات.
2. ضرورة إنشاء هيئات قضائية متخصصة في الجرائم الإلكترونية داخل المحاكم الابتدائية والاستئنافية، وتدريب القضاة بشكل مستمر على مفاهيم الدليل الرقمي، ووسائل التحقق من صحته، وإصدار دليل قضائي إرشادي لتقييم الأدلة الرقمية وفقًا للمعايير الفنية والقانونية الدولية، وتشجيع نشر الأحكام القضائية المتعلقة بالدليل الرقمي لتكوين اجتهادات مستقرة.
3. ضرورة إنشاء مختبرات جنائية رقمية مركزية على الأقل، وتدريب الضباط والقضاة على مفاهيم التحليل الرقمي وتقنيات التحقق من الدليل، مع ضرورة اعتماد برامج معترف بها دوليًا في الفحص الرقمي مثل EnCase أو FTK. وإدراج عبارة:

(إلزام توثيق سلسلة الحيازة الرقمية وسلامة البيانات) في اللوائح القضائية، مع ضرورة التعاون مع المنظمات الدولية (مثل UNODC وINTERPOL) في بناء القدرات الفنية.

4. نوصي المشرع الوطني بضرورة مواءمة التشريعات الوطنية مع المعايير الدولية؛ إذ تعد خطوة أساسية نحو تعزيز التعاون السيبراني؛ لما تمثله مواءمة التشريعات الوطنية مع الاتفاقيات الدولية من ضمان التكييف القانوني الموحد للجريمة، فالتفاوت في تعريف الجريمة الرقمية يخلق عقبات أمام تسليم الجناة أو الاعتراف المتبادل بالأدلة. ومن جانب آخر: تعزز هذه المواءمة فعالية التعاون القضائي الدولي؛ إذ لا يمكن تنفيذ طلبات إنابة قضائية أو مساعدة قانونية متبادلة إذا لم تكن هناك جرائم متماثلة، وأخيرًا: تسهم في منع إفلات الجناة من العقاب: الجريمة السيبرانية العابرة للحدود، وقد يستغل الجناة الثغرات التشريعية للاختباء في دول لا تجرّم أفعالهم.

5. إن إصدار أدلة إجرائية وطنية موحدة لضبط الجريمة السيبرانية وجمع الأدلة الرقمية يمثل خطوةً جوهرية في إطار تحقيق العدالة الداخلية وتعزيز التعاون الدولي في مكافحة الإجرام السيبراني؛ إذ تُعد هذه الأدلة مرجعًا رسميًا يضمن التزام الجهات الأمنية والقضائية بالإجراءات الفنية والقانونية المعتمدة، ما يُضفي المشروعية على عمليات جمع وتحليل الأدلة، ويزيد من قابليتها للاعتراف الدولي. فغياب الإطار المعياري لجمع الأدلة الرقمية يعد من أهم أسباب رفض بعض الدول التعاون أو قبول الأدلة الواردة من جهات أجنبية.

المراجـــع:

[1] د. إبراهيم السيد حسانين زيد: المواجهة الجنائية لظاهرة التحويل الإلكتروني غير المشروع للأموال، أطروحة دكتوراه، جامعة عين شمس 2021.

[2] د. أحمد يوسف جمعة: الإرهاب السيبراني، دار الأهرام 2022،

[3] أسامة أحمد المناعي (وآخرون) جرائم الحاسب الآلي والإنترنت، وائل للنشر والتوزيع، 2001.

[4] د. أمير فرج يوسف: بطاقات الائتمان والحماية الجنائية لها، دار المطبوعات الجامعية 2008،

[5] د. باهة فاطمة: الاعتداءات الواقعة على بطاقات الدفع الإلكتروني، المجلة الجزائرية للعلوم القانونية والسياسية والاقتصادية، المجلد 57 العدد 4، 2020.

[6] د. بقنيش عثمان محاضر، مصطفى منشور وسيمة: حماية الملكية الفكرية عبر الإنترنت في إطار المنظمة العالمية للملكية الفكرية، مجلة البحوث في الحقوق والعلوم السياسية، العدد2، 2015،

[7] د. تشارلز هورنجور: الجرائم الإلكترونية والمعلوماتية، ترجمة إبراهيم جابر، مؤسسة شباب الجامعة، الإسكندرية، 2018.

[8] د. حسن كيرة: المدخل إلى القانون، منشأة المعارف الإسكندرية– 1972م.

[9] الحسين محمد يحي، سيد محمد سيد أحمد: الحماية القانونية للبيانات الشخصية، مجلة القضاء والقانون، مركز البحوث والدراسات القضائية، أبو ظبي، العدد 4 – 2018م.

[10]حفيظة قايد: الآليات القانونية لحماية بطاقة الائتمان الإلكترونية على الصعيد الوطني والدولي، مجلة معارف العلوم القانونية والاقتصاد، المجلد 2 العدد 2، 2021.

[11]د. خالد عبد الباقي محمد الخطيب: شرح قانون الجرائم والعقوبات القسم الخاص، مكتبة خالد بن الوليد، صنعاء 2021.

[12]د. راشد أحمد المنصوري، جرائم نشر الشائعات الإلكترونية عبر مواقع الإعلام الاجتماعي، أطروحة دكتوراه، جامعة عين شمس 2021م.

[13]د. ربيع محمود محمد الصغير القصد الجنائي دراسة تطبيقية على الجرائم المتعلقة بالإنترنت، أطروحة دكتوراه، جامعة عين شمس 2015.
[14]د. سامي منصور: الأعمال الجرمية التي تستهدف الأنظمة المعلوماتية، المنشورات الحقوقية، 2011.
[15]سلام منعم مشعل، د. محمد سمير صالح: الحماية القانونية لحقوق الملكية الفكرية الرقمية، المجلة الأكاديمية للبحث القانوني، المجلد 15 العدد 1، 2017.
[16]سليمان أحمد فضل: المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، 2013.
[17]د. سمير عالية: الجرائم الإلكترونية، منشورات الحلبي 2020.
[18]د. شادي محمد عدرة: الحماية الجنائية للمعلومات الشخصية، أطروحة دكتوراه، كلية الحقوق جامعة عين شمس، 2021.
[19]د. عادل عزام سقف الحيط: جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونية، دار الثقافة للنشر والتوزيع، عمان 2019.
[20]عادل يوسف الشكري: الحماية الجنائية لبطاقات الدفع الإلكتروني، مجلة جامعة الكوفة، العدد 11، 2008.
[21]د. عاقلي فضيلة: حماية حقوق الملكية الفكرية والصناعية من الجريمة المعلوماتية، مجلة الاقتصاد الصناعي، جامعة باتنة 1 الحاج لخضر الجزائر، العدد 12، 2017م.
[22]د. عبد الفتاح بيومي حجازي: مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، بدون دار نشر 2009.
[23]د. عبد الكافي مريم، د. بوربابة صورية: جريمة الاحتيال المعلوماتي الواقعة على البطاقات المالية الإلكترونية، مجلة القانون والعلوم السياسية، المجلد 8 العدد 1، 2022.
[24]د. عبد الله المخلافي: المدخل لدراسة القانون، مكتبة الصادق، 2004.
[25]د. عبد الله لعور، عبد الرزاق كبوط: العلاقة بين النقود الرقمية والعملات الرقمية والعملات الافتراضية والعملات المشفرة، مجلة الاقتصاد الصناعي، خزارتك، مجلد11 العدد2 – 2021.
[26]د. عماد مجدي عبد الملك: جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، 2011،
[27]عمر محمد أبو بكر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية القاهرة 2004.
[28]د. عمر محمود الجوني: الوجيز في الحماية الجنائية من جرائم تقنية المعلومات، دار النهضة العربية، 2021.
[29]د. عوض محمد يعيش: شرح قانون الجرائم والعقوبات اليمني، القسم الخاص، مكتبة الصادق، صنعاء 2014م.
[30]د. عيسائي طه، عبد الله فوزية: المصنفات الرقمية المشمولة بالحماية بموجب قوانين الملكية الفكرية في الاتفاقيات الدولية والقانون الجزائري، دفاتر السياسة والقانون، مجلد13العدد1، 2021
[31]محمد أمين الشوابكة: جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمان 2007.
[32]د. محمد رمضان عشري السيد: الأحكام الموضوعية لجرائم الاتصالات، أطروحة دكتوراه، جامعة عين شمس، 2021.
[33]د. محمد دمان ذبيح: النقود الإلكترونية، مجلة الشريعة والاقتصاد جامعة الأمير عبد القادر للعلوم الإسلامية، العدد 1 مجلد 10 –2021.
[34]محمد عادل عبد السلام: الأحكام الموضوعية والإجرائية في جريمة السرقة المعلوماتية، أطروحة دكتوراه، كلية الحقوق جامعة عين شمس، 2021.
[35]د. نعيم سعيداني: الحماية الجنائية للحق في الخصوصية في مجال المعلوماتية، أطروحة دكتوراه، جامعة باتنة 1، الجزائر، 2021.

[36]د. نعيم مغبب: مخاطر المعلومات والإنترنت، المخاطر على الحياة الخاصة وحمايتها، بدون ناشر، 1998م.

[37]د. نور سليمان يوسف يعقوب البالو: الأحكام الموضوعية لجرائم المعلوماتية، أطروحة دكتوراه، جامعة عين شمس 2021.

[38]د. هائل حزام مهيوب العامري: حماية حق المؤلف في التشريع اليمني مقارنة ببعض التشريعات الأخرى، مجلة العلوم التربوية والدراسات الإنسانية، العدد 5 ابريل 2019.

[39]د. هروال هبة نبيلة: جرائم الإنترنت، أطروحة دكتوراه، جامعة ابي بكر بالقايد، الجزائر 2014.

[40]د. هشام مسعودي: حماية الملكية الفكرية لحقوق المؤلف للمصنفات الرقمية، مجلة الدراسات القانونية، المجلد 8 العدد 2، 2022.

[41]هلالي عبد الإله أحمد: جرائم المعلوماتية عابرة للحدود، دار النهضة العربية 2007.

[42]هيثم محمد حرمي شريف: النقود الإلكترونية، مجلة الشريعة والقانون، جامعة الإمارات، العدد 84، 2020.

[43]يوسف بن هزاع بن مساعد الشريف، الأحكام والضوابط الفقهية المتعلقة بالنقود الرقمية الإلكترونية، مجلة جامعة الملك عبد العزيز، العدد 5.

[44]يونس عرب: تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، ورقة مقدمة لورشة تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، متاحة على الرابط: http://www.assakina.com

القوانين والاتفاقيات والأحكام:

[45]اتفاقية بودابست لمكافحة الجرائم المعلوماتية 2001 الجرائم السيبرانية.

[46]محكمة التمييز الكويتية في الطعن رقم 2007/155، جلسة 2007/9/4.

[47]محكمة التمييز الكويتية الطعن رقم 2012/278 جزائي جلسة 2013/12/15م، طعن رقم 2014/163 جزائي جلسة 2014/6/26م.

[48]حكم محكمة النقض الفرنسية 3 نوفمبر 2016.

[49]قانون العقوبات الفرنسي.

[50]القانون اللبناني للمعاملات الإلكترونية والبيانات الشخصية رقم 81 لسنة 2018.

[51]قانون حماية البيانات الشخصية المصري.

[52]قانون حماية المعطيات الشخصية التونسي لسنة 2004م، وقانون حماية المعطيات ذات الطابع الشخصي المغربية لسنة 2009م، وقانون حماية البيانات الشخصية الإماراتي رقم 45 لسنة 2021م، والقانون المصري رقم 151 لسنة 2020 بشأن حماية البيانات الشخصية، والقانون البحريني رقم 30 لسنة 2018 بشأن حماية البيانات الشخصية، والقانون القطري رقم 13 لسنة 2016 بشأن حماية خصوصية البيانات الشخصية ونظام حماية البيانات الشخصية السعودي لسنة 2023م أما بالنسبة للدول الغربية فنذكر منها البريطاني والاتحاد الأوربي.

[53]محكمة النقض المصرية نقض مصري 1959/ منشور في مجموعة الأحكام س 10 رقم 163.

المواقع الإلكترونية

[54]https://rm.coe.int/special-edition-budapest-convention-en-2022/1680a6992e

[55]موقع صندوق النقد الدولي على الرابط الآتي: https://www.imf.org/ar/Publications/fandd/issues/2022/09/Digital-Money-101-explainer

[56]المنظمة الدولية لحماية الملكية الفكريةwww.wipo.int