

القواعد الإجرائية والموضوعية للجريمة المعلوماتية في التشريع الجزائري

Procedural and substantive rules for information crime in Algerian legislation



شاكر سليمان^{*1}

¹ جامعة تيسمسيلت، الجزائر

chaker.slimane@univ-tissemsilt.dz

تاريخ النشر: 2024/06/01

تاريخ القبول: 2024/05/28

تاريخ الإرسال: 2024/03/14

ملخص:

تزايدت الجرائم المعلوماتية بشكل مستمر مع توسع استخدام شبكة الإنترنت وانتشارها في جميع جوانب الحياة، حيث أصبحت تشمل جميع شرائح المجتمع، ومع هذا النمو، بدأت أشكال جديدة من الجرائم تظهر على الإنترنت، مما دفع المشرع الجزائري إلى إقرار قوانين جديدة تتعامل مع هذه الظواهر المتنامية، تشمل الأنشطة غير القانونية التي تستهدف البيانات الرقمية أو تستخدم التكنولوجيا لارتكاب أفعال غير قانونية أنماطاً متعددة من الاحتيال والاختراقات والسرقات الإلكترونية، مما يمكن أن يتسبب في أضرار محتملة أو فورية للأفراد والمؤسسات بالتالي، اتخذت السلطات المختصة إجراءات لمكافحة ومعاينة هذه الجرائم لحماية الأنظمة الرقمية والبيانات، تعتبر الجرائم المعلوماتية صعبة في التحقيق وتحديد المتورطين فيها نظراً للتقنيات المتقدمة والمعقدة المستخدمة، وبسبب الطبيعة العابرة للحدود لعمليات الجريمة المعلوماتية، فإن التحقيق والمكافحة يتطلبان تعاوناً دولياً فعّالاً، تابع المشرع الجزائري التطورات الدولية في مجال مكافحة الجريمة المعلوماتية وقد قام بإصدار قوانين لحماية الخصوصية ومكافحة هذه الجرائم بشكل خاص، مواكباً بذلك القوانين الدولية المتعلقة بالموضوع.

الكلمات المفتاحية: الجريمة الإلكترونية، المساس بأنظمة المعالجة الآلية للمعطيات، الجرائم المستحدثة، الجريمة السيبرانية، الأنشطة الإجرامية باستخدام التكنولوجيا.

Abstract:

Information crimes have increased continuously with the expansion of the use of the Internet and its spread in all aspects of life, as it has come to include all segments of society. With this growth, new forms of crimes began to appear on the Internet, which prompted the Algerian legislator to pass new laws that deal with these growing phenomena. E, Illegal activities that target digital data or use technology to commit illegal acts include multiple types of fraud, hacks, and cyber

theft, which can cause potential or immediate harm to individuals and organizations. Therefore, the competent authorities have taken measures to combat and punish these crimes to protect digital systems and data. Cybercrimes are difficult to investigate and identify those involved due to the advanced and complex technologies used. Due to the cross-border nature of cybercrime operations, investigation and control require effective international cooperation. The Algerian legislator has followed international developments in the field of combating information crime and has issued laws to protect privacy and combat these crimes in particular, keeping pace with international laws related to the subject.

Key words: Electronic crime, Compromising automated data processing systems, information attack, new crimes, cyber crime, Criminal activities using Technology.

*المؤلف المرسل

مقدمة:

تعد جرائم الحوسبة الإلكترونية من بين الجرائم المستجدة التي لا تقتصر على حدود جغرافية محددة، بل تتعلق بالتكنولوجيا الحديثة والتواصل الإلكتروني، وقد أصبحت واقعاً لا مفر منه في ظل التقدم التكنولوجي المتسارع. ومع ذلك، فإن التشريعات في الجزائر كانت متأخرة بعض الشيء مقارنة بالتشريعات الأخرى في مجال مكافحة جرائم الحوسبة الإلكترونية، ولكن مع تزايد الوعي بخطورة هذه الجرائم وتأثيرها السلبي على الدولة والمجتمع، بدأت الجزائر في اتخاذ خطوات لتحديث قوانينها وتكييفها مع هذه التحديات، في الآونة الأخيرة، وصادقت الجزائر على عدد من الاتفاقيات والمعاهدات الدولية التي تهدف إلى مكافحة جرائم الحوسبة الإلكترونية، مما يشير إلى التزامها بالعمل على مواجهة هذه الظاهرة بفعالية. ومن الجدير بالذكر أن الجرائم في هذا المجال لم تعد تقتصر على القيم المادية فقط، بل تمتد لتشمل القيم المعنوية أيضاً، مثل التعدي على برامج الحاسوب الخاصة أو سرقة البيانات المخزنة، ومن الجدير بالذكر أن الجرائم الإلكترونية تشمل طرفين، الجاني والمجني عليه، وقد تتعرض المؤسسات العامة التي تمتلك صفة الشخص المعنوي أيضاً لهذه التعديات، ورغم وجود وسائل حماية متعددة، إلا أنها غالباً ما تكون غير فعالة أمام قرصنة الشبكة، مما يتطلب تطوير استراتيجيات أمنية أكثر تطوراً للحفاظ على سلامة البيانات والمعلومات، منذ سنة 2004، بدأت الجزائر في تشريع قوانين تطبق على نظم المعلوماتية، ولكن قد تكون هذه القوانين بحاجة إلى التحديث والتعديل لمواكبة التطورات الحديثة في مجال الحوسبة الإلكترونية والأمن السيبراني، بهدف توفير بيئة أكثر أماناً للمعلومات والبيانات في البلاد، خلال فترة قصيرة، شهد قانون العقوبات الجزائري تحولات تطويرية مهمة، مما أدى إلى إحداث تعديلات تتعلق بالمواد ذات الصلة بمجال الجرائم المعلوماتية.

تبرز أهمية هذا الموضوع من خلال الناحية النظرية والعلمية حيث يتناول حماية مصالح خاصة تحظى بأهمية كبيرة في العصر الرقمي، ويتعلق ذلك بالمعلومات الحساسة والبيانات الشخصية التي تحتاج إلى حماية فعالة، نال الناحية الإجرائية، أصبح من الضروري مراجعة وتعديل الإجراءات القانونية لتكون متناسبة مع التحديات الجديدة التي تطرأ مع التطور التكنولوجي يجب زيادة الجهود لضمان فاعلية النصوص القانونية في منع الجريمة، وذلك من خلال تحسين الإجراءات التحقيقية وتعزيز التعاون الدولي في مجال مكافحة الجرائم المعلوماتية.

ومنه نطرح الإشكالية التالية:

إلى أي مدى تُعتبر الآليات القانونية والموضوعية فعّالة في الجرائم المعلوماتية في القانون الجزائري؟ وهذا ما سنحاول الإجابة عليه.

المبحث الأول: ماهية الجريمة المعلوماتية

مصطلح المعلوماتية هو مشتق من كلمة المعلومات Information وهي الكلمة التي شاع استعمالها منذ خمسينيات القرن الماضي في مجالات مختلفة وسياقات شتى مما جعل لها في الاستعمال الدارج مفاهيم متنوعة¹، فالجريمة المعلوماتية هي نوع من الجرائم يتم ارتكابها باستخدام التكنولوجيا والأنظمة الحاسوبية. تشمل هذه الجرائم مجموعة واسعة من الأنشطة غير القانونية التي تستهدف البيانات الرقمية أو تستخدم التكنولوجيا للقيام بأعمال غير قانونية وتشمل الاحتيال الإلكتروني هذا النوع من الجرائم يستخدم الإنترنت أو البريد الإلكتروني للتلاعب بالأفراد أو الشركات بهدف الحصول على معلومات شخصية أو مالية بطرق غير قانونية، وتوزيع البرامج الفيروسية وتشمل هذه الجرائم إنشاء ونشر الفيروسات الكمبيوترية وبرامج التجسس وبرامج الفدية للإضرار بأنظمة الكمبيوتر والبيانات الرقمية، واستخدام معلومات شخصية مسروقة للقيام بعمليات احتيالية أو الوصول إلى حسابات مالية أو معلومات حساسة، واختراق أنظمة الكمبيوتر أو الشبكات الإلكترونية بغرض الوصول غير المشروع إلى معلومات سرية أو الإضرار بالنظام. من خلال هذا المبحث نتطرق إلى ماهية الجريمة المعلوماتية وتضمن المطلب الأول تعريف الجريمة المعلوماتية التي استخدمت لضبط هذا النوع من الإجرام وكذلك خصائصها وهذا ما سنتطرق إليه في المطلب الثاني.

المطلب الأول: تعريف الجريمة المعلوماتية

سبب التطور السريع في التكنولوجيا، تتغير طبيعة الجرائم المعلوماتية باستمرار، مما يجعل الجهود المبذولة في تحديد تعريف دقيق لها أمراً صعباً فالمرشع الجزائري لم يعطي تعريف للجريمة المعلوماتية غير أن

¹د/ عزة محمود أحمد خليل- مشكلات المسؤولية المدنية في مواجهة فيروس الحاسب الآلي دراسة مقارنة في القانون المدني والشرعية الإسلامية- أطروحة دكتوراه، كلية الحقوق جامعة القاهرة، 1994، ص 18.

قانون الاتصالات السمعية والبصرية الفرنسي الصادر في 29 جويلية 1982 أشار صراحة إلى تعريف عام للمعلوماتية وبوصفها بـ صوت أو صور أو وثائق أو بيانات أو رسائل من أي نوع.

اختلفت التسميات فمن أطلق عليها الاحتيال المعلوماتي، ثم الجرائم التي يساعد على ارتكابها الحاسب الآلي، ثم التعسف في استعمال الحاسب الآلي أو إساءة استعمال الحاسب الآلي للدلالة على هذه الظاهرة باعتبارها أشمل وأوسع وهناك من فضل تسميتها بجرائم الحاسب الآلي، كما أطلقوا عليها مصطلح الجريمة المعلوماتية لينتقلوا إلى مصطلحات أكثر حداثة ودقة وهي جرائم التقنية العالية، جرائم الهاكرز أو جرائم ذوي الياقات البيضاء ثم جرائم الكمبيوتر والإنترنت¹، فالجرائم المعلوماتية هي صنف جديد من الجرائم ذلك أنه مع ثورة المعلومات والاتصالات ظهر نوع جديد من المجرمين، انتقل بالجريمة من صورها التقليدية إلى أخرى إلكترونية قد يصعب التعامل معها²، فالجريمة المعلوماتية هي استخدام التكنولوجيا والأنظمة الحاسوبية في ارتكاب أنواع مختلفة من الجرائم ويشمل ذلك الاختراقات الإلكترونية، والاحتيال الإلكتروني، بالإضافة إلى أنواع أخرى من الأنشطة غير القانونية التي تستهدف البيانات الرقمية أو تستفيد من استخدام التكنولوجيا للقيام بأعمال غير مشروعة، وكذلك هي عبارة عن أفعال غير مشروعة يكون الحاسب الآلي محلا لها أو وسيلة لارتكابها فهذا النوع من الجرائم ما هو إلا جريمة تقليدية ترتكب بأسلوب إلكتروني حديث تستهدف المعلومات.

الفرع الأول: التعريف اللغوي والفقه للجريمة المعلوماتية

دور الفقه في تحديد تعريف الجريمة المعلوماتية يعتمد على فهمه للقواعد الشرعية وتطبيقها على الظواهر الحديثة المتعلقة بالتكنولوجيا والمعلوماتية، وبالنظر إلى هذا الإطار، يمكن صياغة تعريف للجريمة المعلوماتية بما يتوافق مع المبادئ الفقهية، ومن ذلك الجريمة المعلوماتية هي كل فعل أو امتناع يقوم به فرد أو جماعة، يقصد منه التعدي على الأموال المادية أو المعنوية للآخرين، سواء كان هذا التعدي ناتجا مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية، بما يخالف القوانين والأحكام الشرعية والمعايير الأخلاقية³، تُعرف الجريمة المعلوماتية لغوياً بأنها مشتقة من كلمة "الجريمة" التي تأتي من "الجرم"، وتعني التعدي أو الذنب، وجمعها جرائم. وقد يُقال جرم، يجرم، فهو مجرم، والجريمة كفعل إجرام⁴.

¹ د/ جعفر حسن جاسم الطائي- جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة الحديثة - دار البداية، عمان، الأردن، 2010، ص 108.

² Pierre Catala « la propriété de l'information » Cité par F.Toubal;le logiciel- analyse juridiqueFUDUL .L.G.D.J.1986 P 126-127.

³ شام محمد فريد جستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الكاتبة، مصر 1990، ص34.

⁴ ابن منظور أبو الفضل جمال الدين مكرم لسان العرب بيروت دار صابر ص54

أما من الناحية الفقهية، يطلق البعض عليها الاختلاس المعلوماتي، أو ظاهرة الغش المعلوماتي، تُعرف الجريمة المعلوماتية بأنها كل فعل ضار يستخدم فيه الفاعل نظامًا حاسوبيًا أو شبكة للوصول إلى البيانات والمعلومات بهدف حذفها أو تغييرها، أو تزويرها أو نشرها بشكل غير قانوني¹.
والبعض يعرفها بأنها تشمل أية جريمة ضد المال مرتبطة باستخدام المعالجة الآلية للمعلومات²، وكذلك من يعرفها بأنها كل فعل إجرامي متعمدا أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل³، من خلال هذه التعاريف لا يوجد تعريف فقهي محدد للجريمة المعلوماتية ولم يتفق فقهاء القانون على إعطاء وصف قانوني دقيق وذلك لوجود عدة مفاهيم مشتقة من الإجرام الإلكتروني و متقاربة في المعنى ونستنتج أن هذه الجريمة المستحدثة يستخدم فيها الحاسب الآلي وشبكة الانترنت وسيلة أو أداة رئيسة في ارتكاب الجريمة.

الفرع الثاني: التعريف التشريعي للجريمة المعلوماتية:

تشمل جرائم التقنية المعلوماتية استخدام التكنولوجيا الحديثة والأنظمة الحاسوبية في ارتكاب الجرائم، أو تسهيلها، أو إخفاءها عالج المشرع الجزائري قواعد قانونية لمواجهة هذه الجريمة في القانون رقم 04-15⁴ المتضمن تعديل قانون العقوبات الذي نصت أحكامه في القسم السابع مكرر على المساس بأنظمة المعالجة الآلية للمعطيات، وبعده فـقانون 04-09 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، حيث نظم هذا القانون الجريمة المتصلة بتكنولوجيا الإعلام والاتصال وكل ما يتعلق بالمنظومة المعلوماتية، والمعطيات المعلوماتية، ومقدمو الخدمات والمعطيات المتعلقة بتسيير الاتصالات الإلكترونية من مراقبة وتفتيش المنظومات المعلوماتية عند الضرورة وحجز المعطيات المعلوماتية، وحفظ المعطيات المتعلقة بحركة السير على الالتزامات الخاصة بمقدمي خدمة الإنترنت، وإنشاء مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وبالتالي لم يعرف المشرع الجزائري الجريمة المعلوماتية لا في قانون العقوبات ولا في القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، فبالرجوع لتعديل قانون العقوبات 04-15 من خلال المواد 394 مكرر و 394 مكرر 1 و 394 مكرر 2 حدد المشرع الجزائري مفهوم المساس بأنظمة المعالجة الآلية للمعطيات وذلك في المادة 394 مكرر وهو الدخول والبقاء في كل أو جزء من منظومة للمعالجة الآلية

¹ نهلا عبد القادر المومني، الجريمة المعلوماتية . ط 2010. دار الثقافة للنشر والتوزيع، ص 48

² K.Tiédemans ,Freude et autres de lits d'affaires ccommis a l'aided'ordinateurs électroniques , Rev. dr .pén .crim , 1984 , P(612)

³ D .B .parker, Combattre la criminalité informatique, 1985, P18.

⁴ قانون رقم 04-15 المؤرخ في 11 ربيع الثاني عام 1436 الموافق 01 فبراير سنة 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية العدد 06.

للمعطيات أو محاولة ذلك، كذلك حذف أو تغيير لمعطيات المنظومة إذا ترتب عن الدخول أو البقاء غير المشروع بغرض تخريب نظام اشتغال المنظومة.

وبالنسبة للمادة 394 مكرر 1 أشارت إلى إدخال بطريق الغش معطيات في نظام المعالجة الآلية أو إزالة تعديل بطريق المعطيات التي يتضمنها، أما المادة 394 مكرر 2 عالجت تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلّة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم، وكذلك حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

أما القانون 104-09 حدد مفهوم الجريمة الإلكترونية في نص المادة التي نصت على الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

الفرع الثالث: خصائص وأركان الجريمة المعلوماتية

من خلال هذا الفرع سنحاول التطرق إلى خصائص الجريمة المعلوماتية أولاً، ثم الانتقال إلى أركانها

أولاً: خصائص الجريمة المعلوماتية :

تُعتبر جرائم الكمبيوتر جرائم مستحدثة، مما يميزها عن الجرائم التقليدية من حيث أسلوبها، نطاقها، ووسائل ارتكابها، ومن أبرز هذه الخصائص ما يلي:

1/ الجريمة المعلوماتية عابرة للحدود: المجتمع الدولي لا يعترف بالحدود الجغرافية، فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود. مع ظهور شبكات المعلومات، لم تعد هناك حدود مرئية أو ملموسة تعيق تدفق المعلومات بين الدول المختلفة. القدرة التي تتمتع بها الحواسيب وشبكتها في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة تفصل بينها آلاف الأميال قد أدت إلى تأثير متعدد الأماكن في دول مختلفة بالجريمة المعلوماتية الواحدة في آن واحد.

2/ صعوبة اكتشاف وإثبات الجريمة المعلوماتية: تمتاز الجريمة المعلوماتية بصعوبة الاكتشاف والإثبات، نظراً لعدم ترك الجاني آثار تدل على إجرامه. الجرائم التي تتم بواسطة إدخال الرموز والأرقام تكون دقيقة ويصعب اكتشافها وإثباتها، لهذا السبب، غالباً ما يتم اكتشافها بالصدفة ونادراً ما يُعاقب المجرمون لعدم وجود أدلة كافية ضدهم.

¹ قانون رقم 04-09 المؤرخ في 14 شعبان عام 1430 الموافق 05 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 47.

3/ خصوصية المجرم الإلكتروني : المجرم المعلوماتي يمكن أن يكون أي شخص، سواء كان طفلاً أو رجلاً أو امرأة، يقوم بأفعال إرادية تؤدي إلى سلوك إيجابي أو سلبي باستخدام تقنية المعلومات لإحداث فعل إجرامي على حق أو مصلحة محمية قانوناً¹.

ثانياً: أركان الجريمة المعلوماتية :

كما أن للجريمة المعلوماتية ركن مادي ومعنوي كبقية الجرائم حيث يمكن تحقيق الركن المادي من خلال اثنتين من الطرق، الأولى هي اختراق الأجهزة الرئيسية بطريقة الغش للوصول إلى نظام المعالجة الآلية للبيانات، والثانية هي البقاء أو الاستمرار بطريقة غير مشروعة في نظام المعالجة الآلية للبيانات، ينص القانون 06-24 المتضمن قانون العقوبات الجزائري في المادة 394 مكرر على أن الدخول أو البقاء غير المشروع في هذا النظام يُعتبر جريمة، ويُعتبر هذا الفعل من أهم جرائم البيانات والجرائم المعلوماتية بشكل عام؛ لأن معظم جرائم البيانات لا يمكن ارتكابها إلا بعد دخول الفاعل للنظام.

أما بخصوص الركن المعنوي لجريمة الدخول والبقاء غير المشروعين يتجلى في القصد الجنائي، حيث يُعتبر من الجرائم العمدية التي يتوجب فيها وجود علم وإرادة، تعبر المادة 394 مكرر عن هذا القصد الجنائي العام بمطلبه بأن يكون الدخول أو البقاء عن طريق الغش، استخدام هذه العبارة يعني أن الشخص المتورط يعلم بأن دخوله أو بقاءه في نظام المعالجة الآلية للبيانات غير مشروع.

المطلب الثاني: مميزات الجريمة المعلوماتية

في مجال معالجة البيانات الإلكترونية، يتم استخدام البيانات التي يقوم الجاني بإدخالها بغرض الحصول على المعلومات اللازمة لتنفيذ الجريمة الإلكترونية عبر الحاسب الآلي. بالنسبة لمجال معالجة النصوص والكلمات، يمكن للمستخدم الحاسوبي كتابة الوثائق المطلوبة بدقة عالية باستخدام الأدوات المتاحة، مما يسهل عملية إنتاج المحتوى بشكل دقيق ومتقن، وإمكانات الحاسب الآلي أيضاً لها دور كبير في تيسير ارتكاب الجريمة، فكلما ارتفعت إمكانيات الحاسب تمكن المستخدم من تصحيح والتعديل والمحو والتخزين والاسترجاع والطباعة²، استحدث المشرع الجزائري قسم مميزات في القسم السابع مكرر من قانون العقوبات في الفصل الثالث الخاص بالجنايات والجنح ضد الأموال بعنوان المساس بأنظمة المعالجة الآلية للمعطيات.

الفرع الأول: صعوبة إظهار الجريمة المعلوماتية

مواجهة تحدي استخراج الدليل الإلكتروني يتجاوز مجرد فحص كميات هائلة من المعلومات؛ بل تمتد لتشمل إجراءات الحصول عليه وضمان سلامته من التلاعب والتعديل الذي يمكن أن يستخدمه الجناة

¹ نهلا عبد القادر المومني، الجريمة المعلوماتية، مرجع سابق، ص 41.

² د/ محمد علي العريان- الجرائم المعلوماتية- دار الجامعة الجديدة، الإسكندرية، مصر، 2004، ص 37.

لتعطيل العدالة والإفلات من العقاب. هذا التحدي يشكل عائقاً أمام جهود التحقيق والتحري بسبب الطبيعة التقنية المعقدة للدليل الإلكتروني. إذ يمكن رد أسباب صعوبة اكتشاف الجريمة المعلوماتية التي عادة ما تنكشف بمحض الصدفة إلى عدم تركها أثراً خارجياً لأنها من الجرائم التي تتسم باللاعنف¹، وفي هذه الحالة التي قد تعلم بها فإنه يستهدف بالمحو السريع عدم استطاعة هذه السلطات إقامة الدليل ضده²، فالجريمة الإلكترونية لا تترك أثر بعد ارتكابها والوصول إلى دليل يدين الجناة، وكذلك صعوبة اكتشاف المجني عليه للجريمة المعلوماتية فأغلب الجهات المعنية تحرص على التي تتعرض أنظمتها للقرصنة إلى عدم إبلاغ السلطات المختصة تجنباً للأضرار بسمعتها، ولإثبات الجريمة المعلوماتية قد يكون تحدياً بالفعل.

بالرغم من التحديات الكبيرة التي تواجه جهود مكافحة الجرائم المعلوماتية، إلا أن القضاء على هذه الجرائم ليس بالأمر المستحيل. فقد شهدت التقنيات الرقمية تطوراً ملحوظاً، وتم تعزيز الإجراءات القانونية لتمكين الأجهزة القضائية من جمع الأدلة الرقمية واستخدامها بفاعلية في ملاحقة المجرمين.

الفرع الثاني: جريمة تجاوز الحدود الجغرافية

الجرائم التي تتجاوز الحدود هي نوع من الجرائم يتم ارتكابه عبر الحدود الوطنية، حيث يتم ارتكابها في إحدى الدول ثم تنتقل إلى دولة أخرى، هذا النوع من الجرائم يمكن أن يشكل تحدياً للسلطات الأمنية والتشريعية لأنه ينطوي على مسائل قانونية معقدة تتعلق بالتعاون الدولي والتنسيق بين القوانين والقواعد القانونية للدول المعنية. يتم ارتكاب هذه الجرائم عن بعد دون تواجد مادي للمجرم في موقع الجريمة، وبالتالي يتم فصل المجرم عن الموقع الفعلي للجريمة، ويتباعد المسافات بين الفعل ونتيجته، حيث يتم تنفيذ الجرائم باستخدام أجهزة الحاسوب والشبكات الإلكترونية، تشمل الجرائم الإلكترونية العابرة للحدود أنشطة جرائم إلكترونية تؤثر على الضحايا في عدة دول، حيث تتجاوز هذه الجرائم الحدود الوطنية وتنتشر عبر الشبكة العنكبوتية، وتعتبر هذه الجرائم غالباً ما تؤدي إلى أضرار للمجني عليه فحسب، بل قد تمتد لتتطلب متضررين آخرين في دول مختلفة لذلك، ينبغي التعاون الدولي لمكافحة هذه الجرائم من خلال المعاهدات والاتفاقيات الدولية المناسبة، تتطور هذه الجرائم وتتغير مع تقدم التكنولوجيا وتغير الظروف الاجتماعية والاقتصادية، مما يتطلب تحديث وتطوير التشريعات والتدابير الأمنية لمكافحتها بفعالية.

¹ جميل عبد الباقي - القانون الجنائي والتكنولوجيا الحديثة- الطبعة الأولى، دار النهضة العربية، مصر، 1992، ص 17.

² د/ علي عدنان فيل - إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية دراسة مقارنة- دار الكتب والوثائق القومية، الإسكندرية، مصر، 2012، ص 80.

المبحث الثاني: الآليات الإجرائية والموضوعية للجريمة المعلوماتية

دراسة الجرائم بشكل عام والجرائم المعلوماتية بشكل خاص تندرج ضمن نطاق قسم القانون الجزائي، الذي يختص بدراسة كل نوع من الجرائم على حدة، ويحدد عناصرها الأساسية والعقوبة المناسبة لكل جريمة. على الرغم من أن الآليات الإجرائية للتعامل مع الجرائم المعلوماتية تختلف من دولة إلى أخرى وتتأثر بالتشريعات المحلية والدولية، إلا أنه يمكن تقديم إطار عام للإجراءات التي قد تُتبع في مثل هذه الحالات، من بين الإجراءات المعتادة في التعامل مع الجرائم المعلوماتية تقديم شكوى، حيث يمكن للضحية تقديم شكوى للجهات المختصة مثل الشرطة أو الجهات القضائية المعنية بالجرائم الإلكترونية، بعد تقديم الشكوى، تقوم السلطات المختصة بفتح تحقيق للتحقق من الحادث وجمع الأدلة والبيانات ذات الصلة، إجراءات التحقيق تتضمن استخدام التقنيات الرقمية وتحليل البيانات الإلكترونية، بالإضافة إلى التعاون مع الجهات الأخرى مثل مقدمي الخدمات الإلكترونية لجمع المعلومات اللازمة بناءً على الأدلة المتوفرة، يتم اتخاذ الإجراءات القانونية اللازمة ضد المتورطين في الجريمة المعلوماتية، ويتم تطبيق العقوبات المناسبة وفقاً للتشريعات السارية، نبين في هذا المبحث القواعد الإجرائية للجريمة الإلكترونية في مطلب أول و المطلب الثاني: القواعد الموضوعية للجريمة الإلكترونية في مطلب ثاني.

المطلب الأول: القواعد الإجرائية للجريمة الإلكترونية

تعديل المشرع الجزائري لقانون الإجراءات الجزائية رقم 06-122 في المواد 56 مكرر 5 و 65 مكرر 11 و 65 مكرر 12 يُنص على أهمية التحقيق في الجرائم المرتكبة باستخدام أنظمة المعالجة الآلية للمعطيات. يتيح هذا التعديل لوكيل الجمهورية أو قاضي التحقيق، بعد إشعار وكيل الجمهورية، السماح بالتحقيق تحت رقابته في هذه الجرائم. بالإضافة إلى ذلك، يُسمح لضباط أو أعوان الشرطة القضائية بمراقبة الأشخاص المشتبه فيهم بجريمة أو جنحة إلكترونية، بترخيص من وكيل الجمهورية، وذلك بغرض اختراق حساباتهم الإلكترونية لكشف الجريمة، يتطلب هذا التعديل تحديد الجريمة الإلكترونية بوضوح لتحديد المسؤولية الجزائية، كما يُشدد على ضرورة أن يتم التحقيق في الجريمة الإلكترونية من قبل الجهات المختصة قانوناً، ويشمل ذلك جمع الأدلة الرقمية وتحليلها بشكل صحيح.

الفرع الأول: التفتيش التكنولوجي للحواسيب:

التفتيش التكنولوجي يمثل عملية تدقيق وفحص للأنظمة الإلكترونية والشبكات الحاسوبية بهدف كشف الثغرات الأمنية ومعالجتها. يهدف هذا النوع من التفتيش إلى حماية سلامة البيانات والمعلومات ومنع التسلات الضارة. تتضمن هذه العملية استخدام أدوات تقنية متخصصة لفحص البرمجيات والأجهزة

¹ القانون رقم 06-22 مؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية العدد 84.

والشبكات لاكتشاف الجرائم الإلكترونية. يُعدّ التفتيش التكنولوجي جزءاً أساسياً من استراتيجيات الأمان السيبراني التي يعتمد عليها الأفراد والشركات والمؤسسات لحماية بياناتهم ومواردهم الرقمية، يُعتبر التفتيش التكنولوجي من أصعب أنواع التفتيش نظراً للتطور السريع في مجال التكنولوجيا، كما يشكل تحدياً للحريات الشخصية التي تضمنها الدستور. يختلف التفتيش التكنولوجي عن التفتيش المنزلي، حيث يوضع المشرع الجزائري إطاراً قانونياً خاصاً للتفتيش المنزلي، فنص المادة 44 من قانون الإجراءات الجزائية على أنه لا يجوز إجراء التفتيش إلا بعد الحصول على إذن مكتوب من وكيل الجمهورية أو قاضي التحقيق المختص، يجب إظهار الإذن قبل الدخول إلى مسكن المشتبه فيه والشروع في تفتيشه، أما التفتيش الإلكتروني هو إجراء البحث في النظم المعلوماتية بجمع أدلة الجريمة المخزنة أو المسجلة بشكل إلكتروني، ويستهدف ضبط أدلة الجريمة مثل البرامج غير المشروعة والملفات المخزنة في الحواسيب والمعدات المعلوماتية والاتصالات الإلكترونية، كما يجيز المشرع الجزائري إجراءات التفتيش الإلكتروني في الجريمة المعلوماتية فنصت المادة 03 و المادة 04 من قانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها مصدر مشروعية التفتيش أي أنه في حالة توفر معلومات عن احتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام والدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني أو مقتضيات التحريات والتحقيقات، وكذلك المادة 05 من نفس القانون ميز المشرع الجزائري في تفتيش المنظومات المعلوماتية بين ما إذا كانت المنظومة متصلة بنظام آخر داخل التراب الوطني أو كانت المنظومة متصلة بمنظومة معلوماتية تقع خارج الإقليم الوطني وحتى يكون إجراء التفتيش سليم وليس باطلا يجب إتباع الإجراءات التالية:

أولاً: سلطات القيام بالتفتيش

وفقاً لأحكام المواد 4 و 5 من قانون 04-09، يتم منح النيابة العامة وقاضي التحقيق وضباط الشرطة القضائية صلاحية التفتيش، حتى عن بعد، بموافقة مكتوبة من السلطة القضائية المختصة. يتخذ الاحتياطات الضرورية لحماية المعلومات والبيانات المخزنة لتقديمها للنيابة أو للقاضي التحقيق، يجب أن يُفهم أن عمليات التفتيش في جرائم المعلوماتية لا تختلف عن تلك في الجرائم الأخرى. ويُشجع على توظيف الأشخاص الذين يمتلكون المعرفة المناسبة بنظم المعلومات لحماية البيانات والمعلومات الموضوعة تحت البحث، سواءً لمساعدتها أو لتوفير المعلومات اللازمة للكشف عن الجريمة، فيما يتعلق بالجرائم المعلوماتية التي يتم تخزينها في أنظمة معلوماتية خارج الإقليم الوطني، يتم الحصول على البيانات وفقاً للاتفاقيات الدولية المعمول بها.

ثانيا: وقت تنفيذ التفتيش

يمكن أن يُعتبر التفتيش الإلكتروني جزءًا من التحقيقات الجنائية التي تطول مدتها، حيث يتم جمع الأدلة الرقمية وتحليلها بعناية. في حالات الطوارئ أو الجرائم ذات الأهمية القصوى، قد يُنفذ التفتيش الإلكتروني على الفور، وفقًا لقانون الإجراءات الجنائية الجزائري الذي ينص على أنه يُسمح بالتفتيش في الفترة من الساعة الخامسة صباحًا وحتى الساعة الثامنة مساءً، خصوصًا فيما يتعلق بالجرائم المتعلقة بأنظمة المعالجة الآلية للبيانات، يجب على الشخص المكلف بالتفتيش أن يلتزم بالوقت المحدد قانونًا لبدء هذا الإجراء، ويأتي هذا الإجراء لحماية الحقوق والحريات المكفولة دستوريًا لضمان عدم تعارضها مع هذا الإجراء. يسمح المشرع الجزائري بتنفيذ التفتيش في أي ساعة من ساعات النهار أو الليل لغايات التحقيق في الجرائم، وذلك استثناء لطبيعة بعض الجرائم التي قد يُخفي فيها المشتبه به الأدلة بشكل متعمد، تتأثر سرعة تنفيذ التفتيش الإلكتروني بعدة عوامل، بما في ذلك طبيعة وتعقيد الجريمة، ونوعها، والإجراءات القانونية المطلوبة لضمان حقوق الفرد والحفاظ على سلامة التفتيش الإلكتروني.

الفرع الثاني: التوقيف للنظر:

يعني التوقيف للنظر في الجرائم الإلكترونية تعليق أو تأجيل النظر في الجرائم المرتبطة بالانتهاكات الإلكترونية أو التي تتم عبر الإنترنت. يُمكن أن يكون التوقيف مؤقتًا لتمكين التحقيق الشامل أو لجمع المزيد من الأدلة الضرورية. لم يكن التوقيف للنظر معروفًا في القانون الجزائري الخاص بالإجراءات الجنائية، إذ يُمنح ضباط الشرطة القضائية صلاحية احتجاز الأشخاص المشتبه بهم للاعتقال لأوامرهم، ويُطبق ذلك في معظم الجرائم المتلبس بها، مع ذلك، يتأسس التوقيف للنظر في المواد 47 و48 من دستور عام 1996، وقد تم تقديمه في المادة 02-15 المؤرخة في 23 جويلية 2015. يُسمح بالتوقيف للنظر وتمديده بموافقة كتابية من وكيل الجمهورية المختص إقليميًا لضباط الشرطة القضائية عند توافر دلائل قوية على ارتكاب الجريمة. يتم وضع المشتبه به في مركز الشرطة أو الدرك لمدة لا تزيد عن 48 ساعة، ما لم يكن الأمر يتعلق بجرائم خطيرة يُمكن فيها تمديد فترة التوقيف للنظر وفقًا للمادة 51 فقرة 05 من القانون الجزائري. في حال اتهام أي شخص، يُمكن تمديد فترة التوقيف بموافقة كتابية من وكيل الجمهورية المختص، فيما يتعلق بالجرائم الإلكترونية، فإن الفقرة 06 من المادة نفسها لا تطبق الأحكام المنصوص عليها في المادة 44، وذلك بموجب التفويض المكتوب من وكيل الجمهورية المختص. يتم مراقبة جميع هذه الإجراءات بإشراف وكيل الجمهورية لضمان صحتها وقانونيتها. ويُحدد التوقيف للنظر وفقًا للمادة 51 من القانون الجزائري فترة لا تتجاوز 48 ساعة.

المطلب الثاني: القواعد الموضوعية للجريمة الإلكترونية

قبل إصدار النصوص القانونية التي تجرم المساس بأنظمة المعالجة الآلية للمعطيات الإلكترونية التعدي الإلكتروني الذي تؤثر على الخصوصية، وضع المرسوم الرئاسي رقم 15-261 أسساً لإنشاء هيئة وطنية مكلفة بالوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال ومكافحتها¹. وقد تبني المشرع الجزائري تطورات التكنولوجيا من خلال قانون 07-18، الذي منح المسؤولية الجزائية لاعتداءات القرصنة والتلاعب بالبيانات، وذلك في الفصل الثالث الذي يتضمن الأحكام الجزائية في المواد من 54 إلى 73، ومع مرور الوقت وتطور التكنولوجيا، فإن الأسس الموضوعية للمسؤولية الجزائية تتغير وتتطور فيما يتعلق بالجرائم الإلكترونية.

الفرع الأول: القواعد الموضوعية للشخص الطبيعي

تختلف المسؤولية الجزائية للجرائم الإلكترونية التي يرتكبها الأفراد حسب القوانين والتشريعات المعمول بها. ومع ذلك، في العديد من الأنظمة القانونية، يتم معاملة الجرائم الإلكترونية بنفس الطريقة التي يتم فيها معاملة الجرائم التقليدية، وفقاً للمادة 59 من قانون 07-18، ينص القانون الجزائري على عقوبة الحبس من سنة إلى ثلاث سنوات وغرامة تتراوح بين 10000 دج إلى 300000 دج لأي شخص يقوم بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة، اشترط القانون الجزائري لقيام هذه الجريمة توافر الركن المادي والمعنوي. الركن المادي يشمل استخدام الطرق التدليسية أو غير النزيهة لجمع المعطيات الشخصية، مما يشكل سلوكاً إجرامياً. وتشمل الطرق التدليسية استخدام وسائل الاحتيال والخداع، بما في ذلك الكذب لتأثير على إرادة الضحية، يُعتبر المشرع الجزائري هذه الجريمة ضمن الجرائم العمدية، حيث يتوجب وجود القصد الجنائي العام، والمتمثل في علم الجاني بجمع المعطيات الشخصية بإحدى الطرق المشار إليها. وبالتالي، تُعتبر هذه الجريمة عمدية بناءً على إرادة الفاعل في ارتكاب الفعل المجرم.

الفرع الثاني القواعد الموضوعية للشخص المعنوي

الأشخاص المعنويون يتحملون مسؤولية جزائية وتفرض عليهم عقوبات قانونية، بما في ذلك الغرامات المالية أو العقوبات الجزائية، وذلك وفقاً لأحكام المواد 18 مكرر و 18 مكرر 1 و 2 و 3 من قانون العقوبات رقم 06-23 و 15-04. تتضمن العقوبات التي يمكن فرضها على الشخص المعنوي في الجنايات والجناح والمخالفات الغرامة التي تتراوح بين مرة وخمس مرات الحد الأقصى المقرر للغرامة للشخص الطبيعي المحكوم بنفس الجريمة، ويمكن أيضاً فرض إحدى أو أكثر من العقوبات التكميلية المنصوص عليها، تحمل الشركات

¹ المرسوم الرئاسي رقم 15-261 المحدد لتشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الصادر بتاريخ 08 أكتوبر 2015، الجريدة الرسمية العدد 16، الصادر بتاريخ 08 أكتوبر 2015.

والمؤسسات مسؤولية ضمان الامتثال للتشريعات القانونية وتنفيذ أنظمة الأمان الإلكتروني المناسبة لحماية بيانات والمعلومات الشخصية للعملاء، وهذا لتجنب المسؤولية الجزائية المحتملة، وتنص المادة 70 من قانون 07-18 على أن الشخص المعنوي الذي يرتكب جرائم وفقاً لأحكام ذلك القانون يُعاقب وفقاً لقواعد العقوبات المنصوص عليها في قانون العقوبات، بالإضافة إلى ذلك، فإن المادة 51 مكرر من قانون العقوبات التي أُضيفت بالقانون رقم 15-04 تنص على مساءلة الشخص المعنوي جزائياً، باستثناء الدولة والجماعات المحلية والأشخاص المعنويين الخاضعين للقانون العام، عن الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه الشرعيين، حيثما ينص القانون على ذلك، لكن، يجب التنويه إلى أن المسؤولية الجزائية للشخص المعنوي لا تمنع مساءلة الأشخاص الطبيعيين كفاعلين أصليين أو كشركاء في نفس الأفعال.

خاتمة:

الجريمة الإلكترونية تمثل تحدياً كبيراً في العصر الرقمي الحديث، حيث تشكل تهديداً لخصوصيات الأفراد والمؤسسات على حد سواء. تتضمن هذه الجرائم مجموعة واسعة من الأنشطة الإجرامية التي تستغل التكنولوجيا الحديثة. تتميز هذه الجرائم بأنها تستلزم جهوداً أقل في التخطيط والتنفيذ مقارنة بالجرائم التقليدية، إذ تعتمد على استغلال الثغرات والضعف في الأنظمة الإلكترونية والشبكات، مما يسمح للمجرمين بالاختراق والوصول إلى المعلومات الحساسة والبيانات الشخصية للأفراد والمؤسسات، وذلك بمعرفة تقنيات الحواسيب. ويرجع ذلك جزئياً إلى أن مرتكبي هذه الجرائم ليسوا بالضرورة محترفي الجريمة بمفهومها التقليدي، تعد جرائم المعلوماتية شكلاً جديداً من الجرائم العابرة للحدود، إذ تحدث عبر أكثر من دولة، حيث يتواجد الجاني عادة في بلد معين والمجني عليه في بلد آخر، تسبب هذه الجرائم خسائر مالية وتنتهك حقوق الأفراد، بالإضافة إلى تأثيرها السلبي على الأمن القومي، مع تزايد استخدام التكنولوجيا وتطورها، فإن التهديدات الإلكترونية تصبح أكثر تعقيداً وتطوراً، وقد قام المشرع الجزائري بمراجعة التشريعات الأجنبية والعربية بدرجة كبيرة، وأضاف نصوصاً قانونية جديدة في قانون العقوبات 04-15 أو قانون 07-18، تتماشى مع التطور السريع الذي تشهده هذه الجرائم، بسبب طبيعة وخصوصية الجريمة المعلوماتية، فقد تم تضمين بعض الاستثناءات في القانون، تختلف عن القواعد والأسس المألوفة في الجرائم التقليدية، لتحديد الأفعال غير المشروعة المرتبطة باستخدام الإنترنت، وتم التوصل إلى النتائج التالية:

1- تعديل التشريعات المحلية لمكافحة الجريمة الإلكترونية ومعاينة المتورطين فيها يعد ضرورياً، مع مقارنتها بالتشريعات الأجنبية، وتطوير أنظمة قانونية لتوفير إطار قانوني فعال لهذا الغرض.

2- الحاجة إلى توحيد الجهود الدولية لتطوير آليات فعالة لمواجهة الجريمة الإلكترونية، وضرورة تكييف الأنظمة القانونية المحلية مع الأنظمة الدولية المتعلقة بمكافحة هذا النوع من الجرائم.

- 3- تطور نمط الجريمة الإلكترونية بشكل مستمر مع تقدم التكنولوجيا وتغير الأساليب المستخدمة في ارتكابها، مما يجعل تحدي مكافحتها مستمراً ويشكل تهديداً مستمراً على حقوق الخصوصية للأفراد.
- 4- تطلب مكافحة الجريمة الإلكترونية التي تعبر الحدود جهوداً دولية مشتركة وتبادل معلومات فعال بين الدول، بالإضافة إلى وضع تشريعات وسياسات تسهل التعاون القضائي الدولي وتمكين السلطات القانونية من ملاحقة المتهمين وتقديمهم للعدالة.
- 5- يمكن لفريق التفتيش الإلكتروني التحقق من تطبيق السياسات الأمنية وتحديد أي تحسينات قد تكون مطلوبة لضمان فعالية الإجراءات.
- 6- يمكن استنتاج تدابير أمنية بناءً على نتائج التفتيش للحفاظ على سلامة البيانات وتعزيز الأمان الإلكتروني.

قائمة المصادر والمراجع

- قانون رقم 04-09 المؤرخ في 14 شعبان عام 1430 الموافق 05 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 47.
- قانون رقم 04-15 المؤرخ في 11 ربيع الثاني عام 1436 الموافق 01 فبراير سنة 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية العدد 06.
- المرسوم الرئاسي رقم 15-261 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الصادر بتاريخ 08 أكتوبر 2015، الجريدة الرسمية العدد 16، الصادر بتاريخ 08 أكتوبر 2015.
- عزة محمود أحمد خليل- مشكلات المسؤولية المدنية في مواجهة فيروس الحاسب الآلي دراسة مقارنة في القانون المدني والشريعة الإسلامية- أطروحة دكتوراه، كلية الحقوق جامعة القاهرة، 1994.
- جعفر حسن جاسم الطائي- جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة الحديثة – دار البداية، عمان، الأردن، 2010.
- شام محمد فريد جستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الكاتبة، مصر 1990.
- مجدي علي العربان- الجرائم المعلوماتية- دار الجامعة الجديدة ، الإسكندرية، مصر، 2004.
- جميل عبد الباقي – القانون الجنائي والتكنولوجيا الحديثة- الطبعة الأولى، دار النهضة العربية، مصر، 1992.
- علي عدنان فيل – إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية دراسة مقارنة- دار الكتب والوثائق القومية، الإسكندرية، مصر، 2012.

- د/ عبد الله حسن علي محمود- سرقة المعلومات المخزنة في الحاسب الآلي- دار النهضة العربية، مصر، 2002،

- أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون رقم 04/09، مذكرة لنيل شهادة الماجستير، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم

السياسية، جامعة قاصدي مرباح، ورقلة، الجزائر، 2012.

- Pierre Catala « la propriété de l'information » Cité par F.Toubal;le logiciel- analyse juridiqueFUDUL .L.G.D.J.1986 P 126-127.
- K.Tiédemans ,Freude et autres de lits d'affaires ccommis a làided'ordinateurs électroniques , Rev. dr .pén .crim , 1984 .
- D .B .parker , Combattre la criminalitéinformatique , 1985.
- Vivant ét Le stanc , Lamy in Droit de L informatique éd , 1989 .