



الجريمة الالكترونية في ظل القانون 09/04 " بين الواقع والمأمول" Cybercrime under Law 04/09: "Between Reality and Hope"

روايح إلهام شهرة زاد

جامعة لوئيسي علي-بليدة2، الجزائر

البريد الالكتروني

I.rouabah@univ-blida2.dz

مخبر الرقمنة

عناصر خيرة¹

جامعة لوئيسي علي، بليدة 2، الجزائر

البريد الالكتروني

anasserkeira1983@gmail.com

مخبر الرقمنة

تاريخ القبول للنشر: 2025-05-28

تاريخ الاستلام: 2025-05-20

ملخص:

تتناول هذه الدراسة موضوع الجريمة الالكترونية لكونها واحدة من أكثر الجرائم خطورة والتي نتجت عن التطور المعلوماتي، حيث يعد من المبادئ الأساسية لأخلاقيات تكنولوجيا المعلومات والاتصال حماية حق الافراد في التحكم بمعلوماتهم الشخصية وضمان عدم المساس بها، الا ان تطور السريع لهذه التقنيات خلق تحديات تقنية معقدة متمثلة في الهجمات الالكترونية المتطورة وهو ما اصطلح عنه بالجريمة الالكترونية التي تلحق اضرار بمختلف شرائح المجتمع (بالشركات، و افراد)، وتتميز الجرائم الإلكترونية بخصائص تختلف تماماً عن الجرائم التقليدية، حيث إنها جرائم عالمية وصعبة الإثبات، بالإضافة إلى انخفاض معدلات الإبلاغ عنها، لذلك ومن أجل التكيف مع التشريعات الحديثة في المجال المعلوماتي، قام المشرع الجزائري بتعديل قانون الإجراءات الجزائية لعام 2006، كما أصدر القانون رقم 04-09 الذي يتعلق بالقواعد الخاصة للوقاية من الجرائم المرتبطة بتكنولوجيا المعلومات والاتصال ومكافحتها.

الكلمات المفتاحية: جريمة الكترونية – عقوبة – الشبكة المعلوماتية

¹ عناصر خيرة

Abstract:

This study deals with cybercrime as one of the most serious crimes resulting from information development, where it is considered one of the fundamental principles of IT ethics and communication is to protect the right of individuals to control their personal information and ensure Tahiti has not compromised. However, the rapid development of these technologies creates complex technical challenges of sophisticated cyber-attacks, which is termed cybercrime that damages various segments of society (companies, individuals...). In addition, cybercrime have very different characteristics from traditional crimes, as they are global and difficult to prove, as well as low reporting rates. Therefore, in order to adapt to modern legislation in the field of information technology, Algeria's legislation amended the Code of Criminal Procedure of 2006 and promulgated Act No. 09-04 on special rules for the prevention and control of ICT-related offences.

Keywords: Cybercrime - Punishment - Information Network

المقدمة:

ان الجريمة ظاهرة اجتماعية ظهرت بظهور الانسان ولازالت مستمرة الى يومنا هذا، فقد كانت سابقا الجريمة تقتصر على الأفعال الاجرامية المادية المتمثلة في السرقة والقتل وغيرها.

الا انه مع التطور السريع في التكنولوجيا وانتشار الإنترنت في جميع جوانب الحياة، أصبح العالم أكثر ترابطاً من أي وقت مضى وذلك من خلال تسهيل عملية التواصل بين مختلف افراد المجتمع عن طريق الأجهزة التكنولوجية الحديثة (رسائل الكترونية، تجارة الكترونية، أجهزة اللاسلكية ...).

وعليه فإن تزايد استخدام هذه التقنيات بأساليب مختلفة أدى الى ظهور بعض تصرفات التي تمثل تجاوزا وانحرافا في استغلالها الاستغلال الحسن وذلك لحساب فرد على فرد اخر او جماعة مما يشكل انتهاكا لذات الاخر.

فبالرغم من الفوائد العديدة التي جلبتها هذه الطفرة الرقمية، إلا أنها أدت أيضاً إلى ظهور تهديدات جديدة، من أبرزها الجرائم الإلكترونية.

وباتت هذه الجرائم في وقتنا هذا تمثل تحديًا كبيرًا للأفراد والشركات والحكومات، حيث يستغل المجرمون الفضاء الإلكتروني لتنفيذ أنشطة غير قانونية التي تهدد أمن المعلومات وخصوصية الافراد .

إن هذه الدراسة ذات أهمية كبيرة لأنها تلقي الضوء على مفهوم وخصوصية هذا النوع من الجرائم، على مستوى مختلف الأنظمة القانونية بصفة عامة والتشريع الجزائري بصفة خاصة الذي تبني تجريم هذه الأفعال في قانون 09-14 ولو بصفة متأخرة.

يهدف هذا البحث إلى استكشاف الجرائم المعلوماتية، وهي من القضايا الحديثة التي أصبحت بارزة بشدة على المستويين الوطني والدولي .

وعلى ضوء ما تقدم فإن الإشكالية المطروحة تتمثل في: ما هي طبيعة الجرائم الإلكترونية وأبرز تحديات مكافحتها؟

وفيما تتمثل الحلول التشريعية والمؤسسية لمكافحة الجريمة الالكترونية؟.

للإجابة على هذه التساؤلات تم الاعتماد على المنهج التحليلي والمنهج الوصفي وذلك من خلال تحليل النصوص القانونية المتعلقة بالجريمة الالكترونية وتم تقسيم الى :

المبحث الأول: ماهية الجريمة الالكترونية

المطلب الأول: تعريف الجريمة الالكترونية

المطلب الثاني: اركان الجريمة الالكترونية

المبحث الثاني: اليات مكافحة الجريمة الالكترونية

المطلب الأول: اليات القانونية لمكافحة الجريمة الالكترونية في الجزائر

المطلب الثاني: اليات المؤسساتية لمكافحة الجريمة الالكترونية

1-المبحث الأول: ماهية الجريمة الالكترونية

تُعتبر الجرائم الإلكترونية نوعًا حديثًا من أنواع الجرائم، وذلك بسبب ارتباطها بالتكنولوجيا المتطورة، مما نتج عنه طمس بعض جوانبها، ولذا

فإنه من الضروري قبل التطرق إلى الإجراءات المعمول بها لمكافحة الجرائم الإلكترونية أن أشير إلى بعض القواعد الأساسية المرتبطة بهذه الظاهرة الإجرامية، وعليه ينبغي أن نكون على دراية كاملة بماهية الجرائم الإلكترونية وطبيعتها مع توضيح أنواعها وأركانها.

وبناءً على ذلك، سنقوم بتقسيم هذا المبحث إلى مطلبين، حيث يغطي المطلب الأول تعريف الجريمة الإلكترونية، بينما سيتناول المطلب الثاني الأركان التي تقوم عليها الجرائم الإلكترونية.

1.1-المطلب الأول: تعريف الجريمة الإلكترونية

تتعدد تعريفات الجريمة الإلكترونية وذلك يعود لكون الجريمة الإلكترونية ظاهرة حديثة فهي نوع جديد من انواع الجريمة برزت بمرور الثورة التكنولوجية (المعلوماتية) وعليه فالجريمة المعلوماتية تكاد تستعصي على التعريف.

فكل له زاوية دراسة يتناول من خلالها موضوع هذه الجريمة فهناك من يراها من زاوية فكرية تتعلق بالمضمون، والأخرى تسلط الضوء على الشق القانوني .

وبعضهم خصص لها تعريفاً آخر يعتمد على وسيلة ارتكاب هذه الجريمة، أو موضوع الجريمة، أو حتى مدى معرفة المُركب باستخدام الحواسيب أو عدم استخدامها لارتكاب هذه الأفعال، أو بناءً على معايير أخرى.

وهذه اهم التعريفات الواردة على الجريمة المعلوماتية " الإلكترونية "

الفرع الأول: التعريف الفقهي للجريمة الإلكترونية

تعرف الجريمة الإلكترونية بأنها الجرائم المعلوماتية أو ما يعرف في اللغة الفرنسية بمصطلح *le délit informatique* وهي كل فعل إجرامي

تستعمل فيها التقنية المعلوماتية عن طريق استخدام نظام الحاسب الآلي بأي شكل (عبدالله عبدالكريم عبدالله، 2007).

يمكن تصنيف سلاسل هذه الجريمة على أنها جرائم من السهل إخفاء معالمها لقيامها على شبكة معلوماتية تتسم بنوع من التعقيد مما يصعب تتبع الشخص القائم بها

وعليه فصعوبة تقفي أثر هذه الجريمة يصعب على المحقق التقليدي التعامل مع هذه الأفعال / النشاطات الاجرامية، كونها تتسم بالغموض، والتحقيق فيها يختلف عن التحقيق في الجرائم التقليدية، وكل هذا بسبب الطابع التقني الصرف الذي تتميز به عن الجرائم العادية الأخرى

أولاً: في الفقه الأجنبي

يعرف الفقيه الفرنسي (MASS) جريمة الكمبيوتر بأنها: "الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح وجرائم الكمبيوتر"

يرى هذا الفقيه بأنها جرائم ضد الأموال وقد استخدم لهذا التعريف معيارين هما الوسيلة، وتحقيق الربح المستمد من معيار محل الجريمة المتمثل في المال.

كما عرفها الفقيه (ROS BLAT) بأنها "كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي وإلى تحويل طريقه."

ثانياً: في الفقه العربي

عرف الأستاذ محمد صالح العادلي الجريمة الالكترونية انها: الابن غير الشرعي الذي جاء نتيجة للتزاوج بين ثورة تكنولوجيا المعلومات مع العولمة

أو هي: المارد الذي خرج من القمقم ولا تستطيع العولمة أن تصرفه بعد أن احضرته

الممارسة السيئة لثورة تكنولوجيا المعلومات (صاع فتحة، 2012-2011، ص 36).

الفرع الثاني: التعريف التشريعي للجريمة الإلكترونية

أولاً: على المستوى الدولي :

عرف المؤتمر العاشر للأمم المتحدة لمنع الجريمة ومعاقبة المجرمين الجريمة المعلوماتية بأنها: "أية جريمة يمكن ارتكابها في بيئة الكترونية" كما تم تعريف الجريمة الإلكترونية في اتفاقية مجلس أوروبا للجريمة الإلكترونية لعام 2001 وعرفت الاتفاقية جرائم الحاسب الآلي في الفصل الثاني بأنها: (اتفاقية بودابست، 23 نوفمبر سنة 2001).

أولاً: الجرائم ضد السرية والنزاهة وتوافر البيانات وأنظمة الحاسب الآلي في المواد من 02 الى 12 حيث تم بالترتيب تعريف الدخول غير المشروع، الاعتراض غير القانوني، التدخل في البيانات، التدخل في النظام، إساءة استخدام أجهزة.

ثانياً: الجرائم ذات الصلة بالحاسوب: الجرائم المتعلقة بالتزوير، والجرائم المتعلقة بالغش

ثالثاً: الجرائم المتعلقة بالمحتوى الجرائم المتعلقة بالمواد الإباحية عن الأطفال

رابعاً: الجرائم المتعلقة بانتهاك حقوق الطبع والحقوق المجاورة الجرائم المتعلقة بالتعدي على حقوق المؤلف والحقوق المجاورة.

خامساً: المسؤولية الإضافية: المحاولة والعون والتحريض والمسؤولية المؤسسية (الجريمة الإلكترونية في المجتمع الخليجي وكيفية معالجتها، د مؤلف، ص24).

ثانياً: موقف المشرع الجزائري من الجريمة الإلكترونية

قامت السلطات التشريعية في الجزائر مؤخرا، ولو بصورة جزئية، بمعالجة نقص القوانين المتعلقة بالجرائم الإلكترونية (المادة الثانية من القانون 09_04).

وذلك تم من خلال إضافة مواد قانونية تعاقب الاعتداءات المتعلقة بالنظام المعلوماتي والمتمثلة في الجريمة الالكترونية وذلك بموجب القانون 04/15 الذي تم إصداره في 10 نوفمبر 2004 والذي يتضمن تعديلات على قانون العقوبات.

ونجد ان المشرع الجزائري نص على تجريم الجريمة الالكترونية في مختلف نصوص القانونية نذكر منها :
تتمثل صور الجرائم الالكترونية في قانون العقوبات وتتمثل هذه الجرائم في :

- جريمة التوصل أو الدخول غير المصرح به نصت عليه المادة 394 مكرر من قانون العقوبات بقولها "يعاقب بالحبس والغرامة كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك . (المادة 394 مكرر من قانون العقوبات)

وقد نص المشرع في المادة المذكورة على تجريم فعل الشروع في جريمة الدخول غير المصرح به وذلك بقوله "أو يحاول ذلك . (المادة 394 مكرر من قانون العقوبات)

- جريمة تزوير المعلومات: نص عليها المشرع في نص المادة 394 مكرر

- جريمة الاستيلاء على المعطيات: نصت عليها المادة 394 مكرر 2 بقولها "كل من يقوم عمدا وبطريق الغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية، حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا

القسم. (المواد 394، 394 مكرر 1 و2 من قانون 04/15 الذي تم إصداره في 10 نوفمبر 2004)

من خلال تعريفات السابق للجريمة الالكترونية نستنتج ان هذه الأخيرة تقوم على خصائص تميزها عن غيرها من الجرائم التقليدية.

2.1-المطلب الثاني: اركان الجريمة الالكترونية

رغم أن الجرائم الإلكترونية تحدث في مساحة رقمية، فإنه لإيجادها تحتاج إلى ثلاثة أركان: الركن المعنوي، الركن المادي، والركن الشرعي. إن هذه الأركان تعتبر افتراضية لأنها تتم في عالم غير حقيقي

الفرع الأول: الركن المادي

يفرض القانون عقوبات على الأفعال المادية التي تتوافق مع نصوص التجريم، حيث تمثل هذه الأفعال الجوانب الملموسة للجريمة، لأنه لا يمكن للقانون أن يعاقب على نوايا الأفراد مهما كانت خطيرة إذا لم تظهر في سلوك مادي .

يتمثل الركن المادي في تصرف إجرامي يتمثل في احتمالين، إما الدخول أو البقاء. حيث تعد الجرائم الإلكترونية كغيرها من الجرائم والتي تفترض بالأساس وجود القصد العلم والإرادة لتحديد المسؤولية الجنائية.

وقد لم يحدد النص في المادة 394 مكرر تعريفاً للدخول أو البقاء، ولكن هناك تعريفات توضح أن الدخول غير المصرح به يعني الوصول إلى المعلومات الموجودة داخل نظام الحاسوب دون إذن الشخص المسؤول عن هذا النظام. (محمد خليفة، ص379)

أما البقاء فيشير إلى الوجود داخل نظام معالجة البيانات دون رغبة من يملك الحق في السيطرة على هذا النظام (علي عبد القادر القهوجي، 2000، ص52)، إذا كان دخولاً غير قانوني، فإنه يعد جريمة فقط عندما يكون مقصوداً، لأن الشخص قد يدخل قاعدة بيانات أو نظام معلومات ملك للغير عن طريق الصدفة، وإذا أدرك ذلك وغادر، فلا يعد ذلك جريمة.

لكن إذا استمر في الوجود داخل النظام دون وجه حق، فإن ذلك يعد جريمة، خصوصاً إذا ترتب على الدخول أو البقاء تأثيرات على البيانات، مثل تغييرها أو حذفها أو تعديلها.

لقيام الركن المادي، يتطلب الأمر وجود ثلاث عناصر:

- السلوك الإجرامي، وهو الفعل المادي الملموس الذي يشكل النشاط الإجرامي؛

- النتيجة، وهي التأثير السلبي الناتج عن القيام بالسلوك الإجرامي؛

- والعلاقة السببية، التي تربط بين الفعل والنتيجة. المادة 394 مكرر من القانون رقم 04-15 المعدل والمضاف عليه للأمر رقم 156-66 الذي يحتوي على قانون العقوبات.

الفرع الثاني: الركن الشرعي

وفقاً لمبدأ "لا جريمة دون نص قانوني"، (انظر للمادة 1 من قانون العقوبات الجزائري) يستلزم هذا الركن وجود نص قانوني يحظر الفعل ويجب أن يكون السلوك قد حدث بعد إصدار هذا النص وليس قبله فإذا تم إلغاء هذا القانون، فلا يمكن محاسبة الشخص بدون نص يجرم الفعل المرتكب.

نجد أن المشرع الجزائري قد تبني الجرائم الالكترونية في مختلف النصوص التشريعية ونخص منها قانون العقوبات رقم 04-15 حيث خصص قسماً كاملاً لتلك الجرائم، وهو القسم السابع مكرر، الذي يحتوي على المواد من 394 مكرر إلى 394 مكرر 7، والتي تجعل من كل التصرفات المتعلقة بمعالجة المعلومات بطريقة آلية جريمة.

إلى جانب ذلك، هناك القانون رقم 04-09 الذي يتناول القواعد المتعلقة بمنع الجرائم المرتبطة بتكنولوجيا المعلومات والتواصل ومكافحتها.

ومختلف النصوص القانونية المتعلقة بالجرائم الالكترونية مثل: قوانين معالجة الأنظمة الآلية، وحماية البيانات الشخصية....

الفرع الثالث: الركن المعنوي

هو الركن لا يعكس الأمور المادية مثل الركن المادي، بل يتعلق بالجانب النفسي أو الحالة المزاجية للأفراد الذين يقومون بارتكاب الجرائم الإلكترونية، ومدى نيتهم في القيام بالجريمة وما هي الأسباب وراء ذلك. تظهر المادة 394 مكرر من قانون العقوبات الجزائري بوضوح ضرورة أن تكون جريمة الدخول أو البقاء دون تصريح جريمة عمدية، حيث تشير إلى أن "كل من يدخل أو يبقى عن طريق الغش". (محمد خليفة، مرجع سابق، ص380).

ومن المنطقي أن تكون هذه الجريمة متعمدة، نظراً لأن دخول أنظمة الحاسوب والبقاء فيها يحدث بشكل متكرر وبأعداد كبيرة يومياً، لا سيما في ظل الانفتاح المتزايد على شبكة الإنترنت

2-المبحث الثاني: اليات مكافحة الجريمة الالكترونية

تستند مكافحة الجرائم الإلكترونية إلى مجموعة متنوعة من الاستراتيجيات التي تتضمن الأطر القانونية والتشريعية، والتقنيات المتقدمة للأمن، والتعاون الدولي، حيث تعمل الجهات المعنية، على صياغة قوانين صارمة تسعى لتطبيقها بكفاءة.

وعليه سنقوم بتقسيم هذا المبحث الى مطلبين، يتناول المطلب الأول الاليات التشريعية لمكافحة الجريمة الالكترونية بينما سيتناول المطلب الثاني الاليات المؤسسية.

1.2- المطلب الأول: اليات القانونية لمكافحة الجريمة الالكترونية في الجزائر

في ظل تزايد الجرائم الإلكترونية وتوسع نطاقها، سعت الجزائر إلى وضع إطار قانوني متكامل لمواجهةها والحد من أثارها السلبية. وتشمل هذه الآليات مجموعة من القوانين والتشريعات التي تجرم الأفعال المرتبطة بالجرائم السيبرانية

الفرع الأول : مكافحة الجريمة الالكترونية من خلال قانون العقوبات

تبنى المشرع الجزائري تجريم الاختراق الالكتروني للمعلوماتي في مختلف النصوص القانونية و حدد العقوبات التي تقع على كل فرد يرتكب افعالا إجرامية موصوفة بأنها جرائم معلوماتية و نجد العقوبات منصوصا عليها في الفصل السابع مكرر .

وهي تتضمن عقوبات رئيسية مثل الحبس والغرامة بالإضافة إلى ذلك، هناك عقوبات تكميلية وفقاً للمادة 394 مكرر 6 ، هذه العقوبات تشمل مصادرة الأجهزة والبرامج ووسائل الاستخدام، وأيضاً إغلاق المواقع أو المحلات إذا كان مالکها على علم بالجريمة ، مثال لذلك هو إغلاق مقهى الإنترنت الذي تُرتكب فيه هذه الجرائم بشرط أن يكون المالك معلوماً بذلك .

وقد وضع المشرع بعض الظروف التي تشدد العقوبة في حالات الدخول غير القانوني والإقامة غير المصرح بها، خصوصاً إذا أدت هذه الأفعال إلى حذف أو تغيير بيانات النظام أو تخريبه، أيضاً، إذا كانت الجريمة تستهدف الدفاع الوطني أو المؤسسات العامة، فإنه يتم تشديد العقوبة.

بحسب المادة 394 مكرر 4: يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المذكورة في الفصل السابع مكرر بغرامة تصل إلى خمس مرات الحد الأقصى للغرامة التي تطبق على الأفراد (المادة 394 مكرر 37 من قانون العقوبات).

كما نصت المادة 394 مكرر 5 على تجريم الاشتراك، سواء كان شخصاً طبيعياً أو معنوياً، في مجموعة تهدف لإعداد جريمة ضد الأنظمة المعلوماتية، وكانت هناك أفعال فعلية تمثل هذا التحضير.

ولكن، المسؤولية الجنائية للشخص المعنوي لا تعفي الأفراد من المسؤولية كفاعلين أو شركاء في نفس الجريمة.

وهذا يعني أن المشرع استثنى الأعمال التحضيرية التي يرتكبها فرد بمفرده من العقوبات

أيضاً، المشروع في الجريمة المعلوماتية يعاقب بنفس العقوبة التي تحدد للجريمة الأصلية، وفقاً لما ورد في المادة 394 مكرر 7 من قانون العقوبات.

الفرع الثاني: مكافحة الجريمة الالكترونية من خلال قانون الخاص

نص المشرع الجزائي في الأمر 05/03 على جريمة التقليد والجرائم المشابهة لها، حيث تنص المادة 151 منه عن وجود جنحة التقليد في الحالات التالية: (المادة 151 من الامر 05/03 المتعلق بحقوق المؤلف)

- الكشف غير المشروع عن مصنف أو أداء فني.
 - المساس بسلامة مصنف أو أداء فني.
 - استنساخ مصنف أو أداء فني بأي أسلوب من الأساليب في شكل نسخ مقلدة أو مزورة. استيراد نسخ مقلدة أو تصديرها.
 - بيع نسخ مزورة من مصنف أو أداء فني.
 - تأجير مصنف أو أداء فني أو عرضه للتداول.
- لقد ربط المشرع الجزائي الحماية بتاريخ الانتهاء من الابتكار أو تاريخ النشر أو التوزيع لأول مرة، حيث أصبحت الدعوى الجزائية أو المدنية مقبولة حتى ولو لم يتم الإيداع.
- وقد نصت المادة 165 الأمر 10/97 المعدل والمتمم بالأمر 03/05 المتعلق بحقوق المؤلف على العقوبات على النحو التالي
- للقاضي أن يطبق كعقوبة أصلية: الحبس من 06 أشهر إلى 03 سنوات والغرامة من 500.000 دج إلى 1.000.000 دج وذلك سواء تمت عملية النشر داخل الجزائر أو خارجها وللقاضي سلطة تقرير عقوبات تكميلية تتمثل في مصادرة المبالغ المساوية لمبلغ الإيرادات الناتجة عن الاستغلال غير الشرعي لمصنف أو أداء محمي، ومصادرة وإتلاف كل عتاد أنشئ خصيصاً لمباشرة النشاط غير المشروع وكل النسخ المقلدة، والمصادرة هنا وجوبية (المادة 394 مكرر 1).

2.2 المطلب الثاني: اليات المؤسساتية لمكافحة الجريمة الالكترونية

وضعت الجزائر منظومة مؤسساتية متكاملة تضم عدة جهات رسمية تعمل بشكل مشترك لضمان الأمن السيبراني، وحماية البيانات، وإنفاذ القوانين. وتتمثل هذه الآليات في هيئات أمنية، قضائية، وتقنية متخصصة، إلى جانب التعاون الوطني والدولي لتعزيز الحماية الرقمية.

الفرع الأول: مكافحة الجريمة الالكترونية على المستوى المؤسسي

الدولي

أولاً: الجمعية العامة للأمم المتحدة

أصدرت الجمعية العامة للأمم المتحدة في حماية الحق في الخصوصية الرقمية تحت عنوان "الحق" في الخصوصية في العصر الرقمي تناولت الجمعية العامة هذه المسألة الناشئة ضمن القرار رقم 167/68 المؤرخ في 18/12/2013، حيث أكدت على أن الحق في الخصوصية هو حق من حقوق الانسان الأساسية يجب حمايته على الانترنت ودعت الدول إلى احترام وتعزيز حماية الحق في الخصوصية، بما في ذلك في سياق الاتصالات الرقمية.

أيضا أكدت الجمعية العامة على هذا الحق من خلال تقريرها رقم 166/69 المؤرخ في 18/12/2014

حماية واحترام الحق في الخصوصية بما في ذلك في سياق الاتصالات الرقمية.

أن تتخذ ما يلزم من التدابير لوضع حد لانتهاكات تلك الحقوق، وأن تعمل على تهيئة الظروف الملائمة والكفيلة بالحيلولة دون حدوث هذه الانتهاكات، بطرق تضمن من خلالها توافق تشريعاتها الوطنية في هذا الصدد مع التزاماتها بموجب القانون الدولي لحقوق الانسان .

إعادة النظر في إجراءاتها وممارساتها وتشريعاتها المتعلقة بمراقبة الاتصالات واعتراضها وجميع البيانات على نطاق واسع.

ثانياً: المفوضية السامية لحقوق الإنسان ومختلف المنظمات الدولية الأخرى في حماية الحق في الخصوصية الرقمية:

لقد صدر تقرير عن المفوضية السامية لحقوق الإنسان بتاريخ 16/09/2022 حذر من خطورة تعرض الحق في الخصوصية لضغوط متزايدة بسبب استخدام التكنولوجيات الرقمية الحديثة المتصلة بالشبكات التي حولتها إلى أدوات للمراقبة والسيطرة والقمع تناول هذا التقرير ثلاث مسائل رئيسية هي:

- إساءة سلطات الدول استخدام أدوات الاختراق الحاسوبي "برامج التجسس".

- تفشي ظاهرة الرصد الرقمي للأماكن العامة، خاصة في ظل جائحة كوفيد 19 عبر عديد الدول وذلك باستعمال أحدث التكنولوجيا في تتبع الأشخاص ورصد أماكن تواجدهم

- دور التشفير وتشفير البيانات "في ضمان حماية حقوق الإنسان عبر الانترنت.

- نظم معلوماتية قوية جيدة التصميم وتفعيل مراقبتها لمنع محاولات اختراقها

الفرع الثاني: مكافحة الجريمة الالكترونية على المستوى المؤسساتي الوطني

أولاً: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

نص على هذه الهيئة قانون 04/09 (قانون رقم 04-09 مؤرخ في 14 شعبان عام 1430 الموافق لسنة 2009) ، والمرسوم الرئاسي 261/15 المحدد



لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال صادر بتاريخ 8 أكتوبر 2015، وهي سلطة إدارية مستقلة لدى ومراقبة يترأسها وزير العدل وتشكل من أعضاء معينين من الحكومة وقاضين إثنين من المحكمة العليا يعينيهما المجلس الأعلى للقضاء ومسؤولي مصالح الأمن وضباط وأعوان من الشرطة القضائية تابعين لمصالح الاستعلام العسكري والدرك والأمن الوطني وفقا لقانون الإجراءات الجزائية (المرسوم الرئاسي تحت رقم 15-261 مؤرخ في 8 أكتوبر 2015)

مهام الهيئة : (انظر الى قانون 04/09 والمرسوم الرئاسي 15/261 سابق الذكر)

- الحفاظ على سرية المراسلات والاتصالات
- القيام بالتحريات والتحقيقات القضائية وتجميع وتسجيل محتواها .
- القيام بالترتيبات التقنية المراقبة للاتصالات الإلكترونية
- إجراء التفتيش والحجر داخل المنظومة المعلوماتية

ثانيا: الضبطية القضائية في مواجهة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال

إن لسلطة الضبط القضائي دور فعال في ضبط أدلة الجرائم ورتكيبها وكشف كل ما يتعلق بها حال وقوعها لهذه الأسباب كانت من أولويات السياسة الوطنية لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال تكوين وتأهيل سلك ضباط الشرطة القضائية وأعوانهم

فمنذ سنة 2003 وفي إطار إصلاح العدالة، قامت وزارة العدل بإطلاق برنامج تكوين خاص بالقضاة هدفه رفع مستوى أداء القضاة، ليوكب التطور القانوني الجاري الخاص بجرائم المعلوماتية لأجل هذا تم إجراء :

إدراج مادة "الجريمة المعلوماتية" وذلك ضمن برنامج تأهيل الطلاب في المدرسة الوطنية للقضاء حيث يتم عبر ملتقيات يشرف عليها مختصون في المجال المعلوماتي، ويجري تنظيم العديد من دورات التدريب في مجالات متعددة من الجرائم المرتبطة بالتكنولوجيا الإعلامية والاتصالات بالخارج لفائدة القضاة وموظفي وزارة العدل في إطار تعاون ثنائي.

مراقبة الاتصالات الالكترونية نصت المادة 04 من هذا القانون على الحالات التي تسمح باللجوء إلى المراقبة الالكترونية وهي على النحو التالي (المادة 04 من القانون 09-04 مرجع سابق):

1- بآمن الدولة. الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب والجرائم الماسة

2- حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام.

3- أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

4- مقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية. في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة تفتيش المنظومة المعلوماتية يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في الحالات الضرورية اللجوء إلى المراقبة الالكترونية والدخول إلى منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها ولو عن بعد لغرض التفتيش.

الخاتمة

في ختام دراستنا لموضوع الجريمة الالكترونية يتضح لنا أن الاستخدام الواسع لوسائل تكنولوجيايات الاعلام والاتصال، تمخض عنه مخرجات سلبية وذلك نتيجة سوء استخدامها وتوظيفها لأغراض إجرامية،

إذ تحولت هذه التكنولوجيات إلى فضاء خصب للمتسللين والمخترقين للبيانات الشخصية.

نتائج :

- تميز هذه الجرائم بعدة خصائص تختلف تمامًا عن الجريمة التقليدية، إذ إنها جريمة تتجاوز الحدود الدولية، يصعب إثباتها، ونادرًا ما يتم الإبلاغ عنها .

- على المستوى القانوني والتشريعي نلاحظ قيام المشرع الجزائري بمواكبة التشريعات المتقدمة في مجال التقنية، وتعديل قانون الإجراءات الجزائية لعام 2006،

- بالإضافة إلى سن القانون رقم 09-04 الذي يتناول القواعد الخاصة بالوقاية من الجرائم المتعلقة بتكنولوجيا المعلومات والاتصالات ومكافحتها بالإضافة الى وضع ترسانة قانونية لمحاسبة مرتكبي هذه الأفعال الاجرامية في قانون العقوبات والقوانين الخاصة مع السعي الى تأطير مؤسساتي لمكافحة أي اختراق يشكل جريمة الكترونية

التوصيات :

تطوير البنية التحتية للأمن السيبراني:

• الاستثمار في أنظمة أمن معلومات متطورة قادرة على التصدي للهجمات الإلكترونية.

• تعزيز الحماية الإلكترونية في المؤسسات الحكومية والمالية، باعتبارها من أكثر الجهات استهدافًا.

تعزيز التعاون الدولي في مكافحة الجرائم الإلكترونية:

• إقامة شراكات بين الدول لتبادل المعلومات حول التهديدات الإلكترونية وأفضل سبل مواجهتها.

• توحيد الجهود لملاحقة مرتكبي الجرائم الإلكترونية عبر الحدود، خاصة مع ازدياد النشاط الإجرامي في الفضاء السيبراني العابر للدول.

- دعم الاتفاقيات والمعاهدات الدولية التي تساهم في الحد من الجرائم الإلكترونية وتعزيز الأمن السيبراني العالمي.
- رفع مستوى الوعي بالأمن الرقمي:
- تنظيم حملات توعية حول مخاطر الجرائم الإلكترونية وكيفية الوقاية منها.
- تدريب الأفراد على أفضل الممارسات في حماية البيانات الشخصية والمعلومات الحساسة.

قائمة المصادر والمراجع:

المصادر:

اتفاقيات دولية:

اتفاقية مجلس أوروبا للجريمة الإلكترونية لعام 2001 الموقعة بتاريخ 23 نوفمبر سنة 2001 " معاهدة بودابست لمكافحة جرائم الأنترنت والتي دخلت حيز التنفيذ في 01 جانفي 2004 "

الأوامر:

- الأمر رقم 03، 05 مؤرخ في 19 جمادى الأولى عام 1424 الموافق ل 19 يوليو، 2003 المتعلق بحقوق المؤلف والحقوق المجاورة، ج ر العدد 44.

- الأمر رقم 04، 15 مؤرخ في 10 نوفمبر، 2004 المعدل والمتمم للأمر رقم 66، 156 الصادر في 08 جوان، 1966 المتضمن قانون العقوبات، ج ر العدد 71.

القوانين:

- قانون رقم 04-09 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

المراسيم :

- مرسوم الرئاسي رقم 15-261 مؤرخ في 8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

المراجع :

الكتب

- الجريمة الإلكترونية في المجتمع الخليجي وكيفية معالجتها"، إعداد مجمع البحوث والدراسات، أكاديمية السلطان قابوس العلوم الشرطة، نزوى -سلطنة عمان البحث الفائز بالمركز الأول في المسابقة، سنة 2016، بدون ذكر اسم مؤلف
- عبد الله عبد الكريم، جرائم المعلوماتية والأنترنت (الجرائم الإلكترونية)، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2007 ط 01.

المقالات

- محمد خليفة، خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري في مواجهتها. مقال منشور عبر الموقع ص 379 دون ورود تفاصيل أخرى
- <https://www.asjp.cerist.dz/en/downArticle/20/1/1/4433>

الاطروحات والمذكرات :

- صاع فتيحة، الحماية الجنائية للمعلومات على شبكة الأنترنت، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة أبي بكر بقلاید، تلمسان، 2011-2012.

المحاضرات

- الدكتور محمد صالح العادلي، محاضرات أقيمت على طلبة القانون الجنائي بكلية الحقوق بمسقط، جامعة الأزهر، بمصر، بدون سنة .

- علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونياً، بحث مقدم المؤتمر القانون والكمبيوتر والإنترنت كلية الشريعة والقانون، جامعة الإمارات دولة الإمارات العربية المتحدة، 2000.