وزارة التعليم العالي والبحث العلمي
جامعة عين تموشنت بلحاج بوشعيب
كلية الحقوق
قسم الحقوق

الآليات الدولية لمكافحة الجريمة الإلكترونية

مذكرة مكملة لنيل شهادة الماستر في الحقوق – تخصص : قانون عام

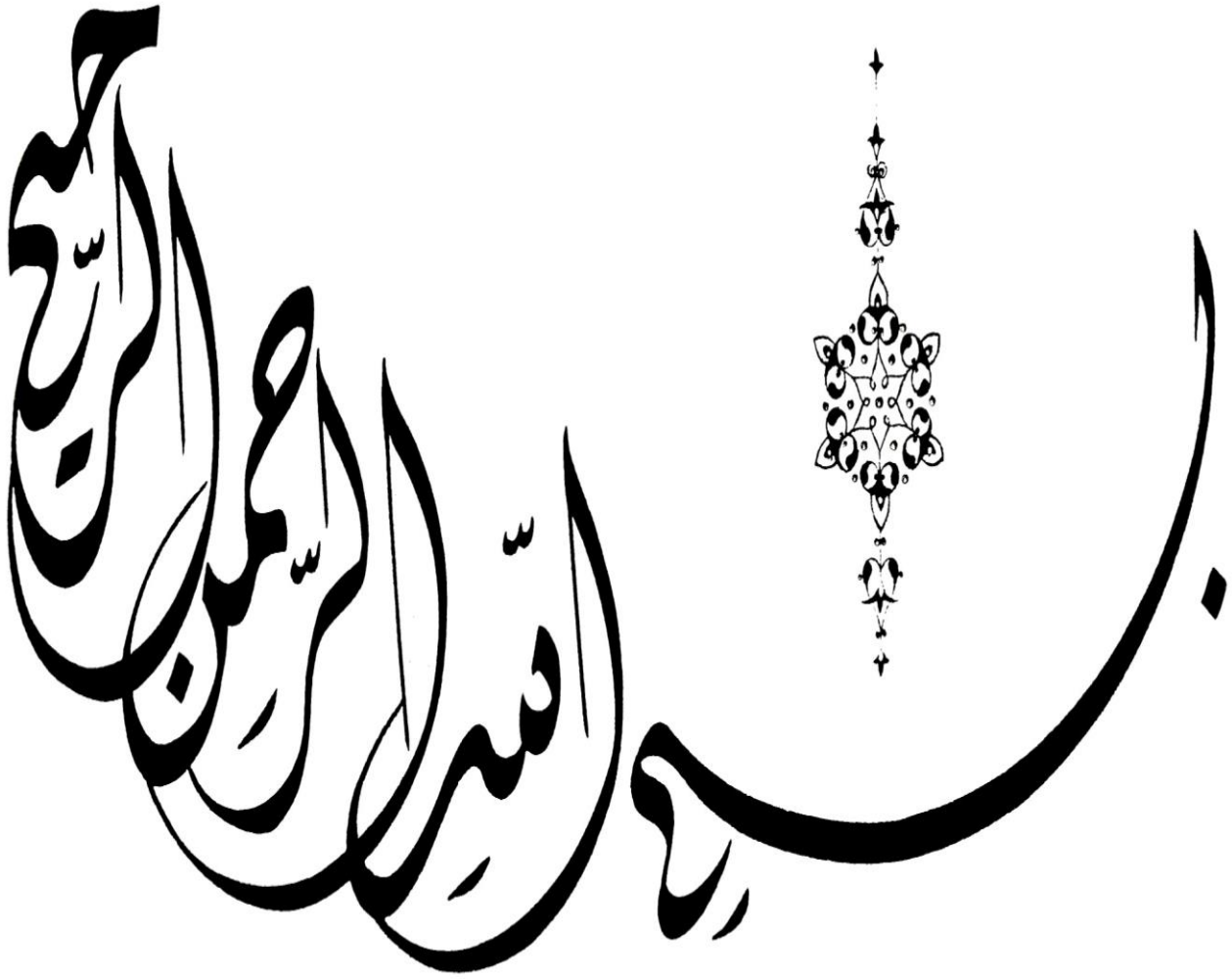
من إعداد الطالبين :
- شهبوني إناس
- طلباوي سيد أحمد

تحت إشراف الأستاذ :
- **خرشي عثمان**

لجنة المناقشة:

الأستاذ الرئيس	**رويس عبد القادر**	**أستاذ محاضر "ب"**
الأستاذ المشرف	**خرشي عثمان**	**أستاذ محاضر "أ"**
الأستاذ الممتحن	**سعدي محمد أمين**	**أستاذ محاضر "ب"**

الدفعة : 2025/2024



قال تعالى: (ومن يشكر فإنما يشكر لنفسه)

لقمان (12)

وقال رسوله الكريم: "من لم يشكر الناس، لم يشكر الله عز وجل" نحمد الله تعالى حمدا كثيرا طيبا مباركة ملئ السماوات والأرض على ما أكرمنا به من إتمام هذه الدراسة التي نرجو أن تنال رضاه.

ثم نتوجه بجزيل الشكر وعظيم الامتنان إلى كل من:

الاستاذ المشرف خرشي عثمان و أستاذة كلية الحقوق الكرام لما كان لهم من نصح و توجيه.

شكر و عرفان

الإهداء

إلى من كانوا السند والدافع في مسيرتي العلمية، إلى والديّ العزيزين، رمز التضحية والعطاء، إلى إخوتي وأصدقائي الذين شاركوني لحظات الجد والتعب، إلى أساتذتي الكرام الذين غرسوا فيّ حب المعرفة والبحث، إلى كل من آمن بي ودعمني بكلمة أو دعاء.

طلباوي سيد أحمد

الإهداء

قال تعالى: (قل اعملوا فسيرى الله عملكم ورسوله والمؤمنون)

تم بفضل الله تخرجي

الحمد لله الذي ما تيقنت به خيراً وأملاً إلا

وأغرقني سروراً

إلى كل من علمني حرفا في هذه الدنيا الفانية.

إلى أمي وأبي حفظهما الله ورعاهما.

إلى وطني الجزائر وشعبها حفظهم الله.

شهبوني إيناس

مقدمـة

تتنوع الجرائم وتختلف باختلاف وسائلها وطرقها، فقد شهد العالم خلال العقود الأخيرة ثورة رقمية هائلة أثّرت بشكل جذري على مختلف مناحي الحياة، حيث أصبحت تكنولوجيا المعلومات والاتصالات المحرك الأساسي لعصر العولمة والتطور الاقتصادي والاجتماعي، ومع ازدياد الاعتماد على الأنظمة الرقمية وتوسع استخدام الإنترنت والحوسبة السحابية والذكاء الاصطناعي، ظهرت تحديات أمنية جديدة ومعقدة تمثلت في بروز نمط جديد من الجرائم يُعرف بالجريمة المعلوماتية أو الجريمة السيبرانية، وهي جرائم تنفذ باستخدام الوسائل الإلكترونية وتستهدف الأفراد، المؤسسات، وحتى الدول.

ولقد أضفت هذه الجرائم بُعدًا جديدًا على مفهوم الإجرام، إذ لم تعد الجريمة محصورة في إطارها التقليدي القائم على العنف أو الأذى المباشر، بل أصبحت تتم عبر "الفضاء الرقمي" بأساليب خفية يصعب اكتشافها أو إثباتها، مما يجعل مكافحتها تحديًا بالغ التعقيد، إذ تعتمد الجرائم المعلوماتية على أدوات ووسائل تقنية متطورة مثل الاختراقات(Hacking) ، البرمجيات الخبيثة، التصيد الاحتيالي، الهندسة الاجتماعية، وتزييف الهويات الرقمية، وكلها تشكّل تهديدًا مباشرًا للأمن العام، الاقتصاد، الخصوصية، وحتى السيادة الوطنية للدول.

هذا وتزداد خطورة هذه الجرائم عندما نُدرك أنها عابرة للحدود الجغرافية، فلا يُشترط أن يكون الجاني والمجني عليه في ذات الدولة، وهو ما يؤدي إلى إشكاليات قانونية وقضائية كبيرة، تتعلق بالاختصاص وتسليم الجناة وتوحيد الأدلة الرقمية وغيرها، ولذلك أصبح من الضروري تبني مقاربة دولية موحدة لمجابهة هذه الظاهرة، لذلك أدرك المجتمع الدولي حجم التهديد الذي تطرحه الجريمة المعلوماتية منذ تسعينيات القرن الماضي، فشهدت هذه الفترة بدايات تنظيم الجهود الدولية من خلال إبرام الاتفاقيات الثنائية والمتعددة الأطراف، وتأسيس آليات وهيئات أمنية متخصصة، كان من أبرزها اتفاقية بودابست لمكافحة الجرائم السيبرانية (2001) التي وضعها المجلس الأوروبي، ووقعت عليها أكثر من 60 دولة من مختلف القارات والتي شكلت مرجعًا دوليًا في تنظيم التعاون القضائي والسياسي في هذا المجال[1].

وفي هذا السياق، برزت منظمة الشرطة الجنائية الدولية (الإنتربول) كفاعل دولي محوري في التنسيق الأمني لمكافحة الجرائم الإلكترونية، حيث أنشأت منذ 2015 مركزًا متقدمًا في سنغافورة خاصًا بتحليل ومكافحة الجرائم السيبرانية، ونجحت في تنسيق عشرات العمليات عبر دول العالم، إلى جانب تدريب الكوادر الأمنية، وتطوير قواعد بيانات ومراكز تحليل رقمية لتبادل المعلومات حول التهديدات الإلكترونية[2].

أما على الصعيد الإقليمي، فقد أدركت الدول العربية حجم التحديات التي تفرضها الجرائم المعلوماتية فبادرت إلى تعزيز جهودها من أجل تكييف تشريعاتها الوطنية مع البيئة الرقمية المتغيرة، وذلك في ظل تنامي الاعتماد على تكنولوجيا المعلومات في مختلف القطاعات، وازدياد حالات الاستغلال الإجرامي للفضاء الإلكتروني،

1 اتفاقية بودابست لمكافحة الجريمة المعلوماتية، مجلس أوروبا، 2001.

2 الإنتربول، *"الجرائم السيبرانية – الاستراتيجية والدور العالمي ."* الموقع الرسمي للإنتربول.

سواء لأغراض الاحتيال، أو التشهير، أو المساس بالأنظمة السيادية للدولة. وفي هذا السياق سعت أغلب الدول العربية إلى سَنّ قوانين خاصة بمكافحة الجرائم المعلوماتية، وإنشاء أجهزة أمنية متخصصة في التحقيق الرقمي.

وفي الجزائر، اتخذ المشرّع خطوات ملموسة لمواكبة هذا التحدي، من خلال إصدار القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته[1]، ويُعد هذا القانون أول نص تشريعي جزائري شامل يُعنى بتجريم الأفعال المرتكبة عبر الوسائط الإلكترونية حيث عرف الجريمة المعلوماتية وحدد نطاق تطبيقها، وجرّم عددًا كبيرًا من السلوكيات، كاختراق الأنظمة والتعدي على البيانات، والاحتيال الإلكتروني، وانتحال الهوية، والتحريض على الجرائم عبر الإنترنت واستغلال الشبكات لأغراض إباحية أو إرهابية.

كما أقرّ القانون ذاته آليات واضحة للتعاون الدولي، إذ نص على أهمية التنسيق بين السلطات الجزائرية ونظيراتها في الدول الأخرى، خاصة فيما يتعلق بتبادل المعلومات والأدلة الرقمية، وتسليم المجرمين وملاحقة الشبكات الإجرامية العابرة للحدود، ويُعد ذلك استجابة واضحة لمتطلبات التعاون الأمني الدولي المنصوص عليها في اتفاقيات متعددة الأطراف، مثل اتفاقية بودابست، وكذلك التوصيات الصادرة عن منظمات دولية كالإنتربول ومكتب الأمم المتحدة المعني بالمخدرات والجريمة.

ولم يتوقف الجهد التشريعي عند هذا الحد، بل تواصل عبر مراجعة مستمرة للقوانين، وإدماج بعض النصوص المكملة ضمن قانون العقوبات، وتطوير البنية التقنية للشرطة الجزائرية، حيث تم إنشاء وحدات مختصة في الجرائم السيبرانية على مستوى الدرك الوطني والأمن الوطني، فضلاً عن تعزيز التعاون مع المنظمات الإقليمية والدولية في مجالات التكوين وتبادل الخبرات والمعلومات.

ومن هنا تبرز أهمية موضوع هذه المذكرة، والذي يحمل عنوان "الآليات الدولية لمكافحة الجريمة المعلوماتية"، حيث يسعى إلى تسليط الضوء على الإطار المفاهيمي لهذا النوع من الجرائم، وشرح طبيعتها وأصنافها وخصائصها، قبل أن ينتقل إلى تحليل آليات التعاون الدولي، سواء الأمنية أو القانونية أو التقنية ومختلف الجهود التي تبذلها المنظمات الدولية والإقليمية لمكافحتها، مع التركيز على دور الإنتربول كحالة تطبيقية رائدة في هذا المجال[2].

كما يسعى الموضوع إلى تسليط الضوء على المكافحة الدولية للجرائم المعلوماتية بوصفها أداة فعّالة من أدوات القانون الدولي العام، ودورها في تعزيز الأمن والاستقرار على الصعيد الدولي وإلى بيان الأهمية البالغة للتعاون الدولي في معالجة الأزمات والقضايا ذات الطابع العالمي كالجريمة المعلوماتية، كما يركّز البحث على استعراض أبرز التحديات والعقبات التي تعيق التعاون الدولي في مجال مكافحة الجرائم المعلوماتية، مع اقتراح سبل فعالة لتجاوزها.

---

[1] القانون رقم 09-04 المؤرخ في 5 أغسطس 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته، ج ر رقم 47، المؤرخة في 16 أوت 2009.

2 بن عاشور، مروان" .الجرائم الإلكترونية والتحديات القانونية في الجزائر"، مجلة العلوم القانونية، العدد 22، 2022.

وتنطلق هذه الدراسة من إشكالية رئيسية مفادها ما مدى فاعلية الآليات الدولية في التصدي للجريمة المعلوماتية؟ وإلى أي حد استطاعت هذه الجهود الحد من هذا النوع المستحدث والمعقد من الإجرام؟

وللإجابة عن الإشكالية الرئيسية المطروحة، اعتمدنا على المنهج الوصفي، والمنهج التحليلي وذلك بهدف تقديم عرض دقيق لأساليب ارتكاب الجرائم المعلوماتية، وآليات مكافحتها دوليا، وذلك بالاستناد إلى النصوص القانونية على الصعيدين الوطني والدولي، إضافة إلى تقارير الهيئات الأمنية، ومساهمات الفقه القانوني، بهدف تقديم دراسة تجمع بين الجانب النظري والتحليل العملي للموضوع

هذا وقد واجهتنا عدة صعوبات خلال إعداد هذه الدراسة، أبرزها ندرة المراجع والمصادر التي تناولت هذا الموضوع بعمق، إذ إن معظم الكتابات المتوفرة تطرقت إليه بشكل موجز ومقتضب، مما صعّب عملية جمع المعلومات وتحليلها، ولضمان معالجة الموضوع بصورة منهجية ومنظمة، قمنا بتقسيم الدراسة إلى فصلين رئيسيين؛ حيث خُصّص الفصل الأول للإطار المفاهيمي للجريمة المعلوماتية، وتناولناه من خلال مبحثين تناولنا في المبحث الأول ماهية الجريمة المعلوماتية، بينما ركز المبحث الثاني على أبرز مجالات التعاون الدولي في مواجهة هذه الجرائم، بينما في الفصل الثاني تكلمنا عن الآليات القضائية لمكافحة الجريمة المعلوماتية وقسمناه إلى ثلاث مباحث: تطرقنا في المبحث االأول إلى آلية تسليم المجرمين، أما المبحث الثاني فخصصناه لآلية المساعدة القضائية، و في الأخير المبحث الثالث عالجنا فيه آليات التغلب على تحديات التعاون الدولي في مكافحة الجرائم المعلوماتية.

وننوه إلى أنّ أهمية هذا البحث لا تقتصر فقط على البعد الأكاديمي، بل تنبع من الحاجة الملحة لتطوير التشريعات الوطنية والمنظومات الأمنية، لمواجهة التحديات الرقمية المعاصرة، خاصة في ظل ضعف التنسيق الدولي في بعض المناطق، وتفاوت القدرات التكنولوجية بين الدول. ونأمل أن تُسهم هذه الدراسة المتواضعة في تعزيز الوعي القانوني والبحثي لدى الطلبة والباحثين وصناع القرار، وأن تكون إضافة علمية في مسار بناء منظومة قانونية وأمنية رقمية فعالة.

أهمية الموضوع:

تتمثل أهمية موضوع هذه المذكرة، في أنها تسلط الضوء على الجرائم المعلوماتية، عبر إبراز الإطار المفاهيمي لهذا النوع من الجرائم، وشرح طبيعتها وأصنافها وخصائصها، ثم التطرق إلى تحليل آليات التعاون الدولي، سواء الأمنية أو القانونية أو التقنية ومختلف الجهود التي تبذلها المنظمات الدولية والإقليمية لمكافحتها، مع التركيز على دور الإنتربول كحالة تطبيقية رائدة في هذا المجال.

كذلك، أهمية هذا البحث لا تقتصر فقط على البعد الأكاديمي، بل تنبع من الحاجة الملحة لتطوير التشريعات الوطنية والمنظومات الأمنية، لمواجهة التحديات الرقمية المعاصرة، خاصة في ظل ضعف التنسيق الدولي في بعض المناطق، وتفاوت القدرات التكنولوجية بين الدول، ونأمل أن تُسهم هذه الدراسة المتواضعة في تعزيز

الوعي القانوني والبحثي لدى الطلبة والباحثين وصناع القرار، وأن تكون إضافة علمية في مسار بناء منظومة قانونية وأمنية رقمية فعالة.

أهداف الموضوع:

– هدف هذا البحث إلى تسليط الضوء على مكافحة الجرائم المعلوماتية بوصفها أداة فعّالة من أدوات القانون الدولي العام، ودورها في تعزيز الأمن والاستقرار على الصعيد الدولي.

– يسعى الموضوع إلى بيان الأهمية البالغة للتعاون الدولي في معالجة الأزمات والقضايا ذات الطابع العالمي.

– يركّز البحث على استعراض أبرز التحديات والعقبات التي تعيق التعاون الدولي في مجال مكافحة الجرائم المعلوماتية، مع اقتراح سبل فعالة لتجاوزها.

تنطلق هذه الدراسة من إشكالية رئيسية مفادها:

ما مدى فاعلية الآليات الدولية في التصدي للجريمة المعلوماتية؟ وإلى أي حد استطاعت هذه الجهود الحد من هذا النوع المستحدث والمعقد من الإجرام؟

المنهج المتبع:

للإجابة عن الإشكالية، اعتمدنا على المنهج الوصفي، والمنهج التحليلي وذلك بهدف تقديم عرض دقيق لأسلوب ارتكاب الجرائم الإلكترونية.

الصعوبات:

قد واجهتنا عدة صعوبات خلال إعداد هذه المذكرة، أبرزها ندرة المراجع والمصادر التي تناولت هذا الموضوع بعمق، إذ إن معظم الكتابات المتوفرة تطرقت إليه بشكل موجز ومقتضب، مما صعّب عملية جمع المعلومات وتحليلها.

تقسيمات الموضوع:

لضمان معالجة الموضوع بصورة منهجية ومنظمة، قمنا بتقسيم الدراسة إلى فصلين رئيسيين؛ حيث خُصّص الفصل الأول للإطار المفاهيمي للجريمة المعلوماتية، وتناولناه من خلال مبحثين: حيث تناولنا

في المبحث الأول ماهية الجريمة المعلوماتية، بينما ركز المبحث الثاني على أبرز مجالات التعاون الدولي في مواجهة هذه الجرائم.

بينما في الفصل الثاني تكلمنا عن الآليات القضائية لمكافحة الجريمة المعلوماتية وقسمناه إلى ثلاث مباحث: تطرقنا في المبحث الأول إلى آلية تسليم المجرمين، أما المبحث الثاني فخصصناه لآلية المساعدة القضائية وفي الأخير المبحث الثالث عالجنا فيه آليات التغلب على تحديات التعاون الدولي في مكافحة الجرائم المعلوماتية.

الفـصل الأول:

ماهية الجريمة المعلوماتية

تمهيد

الجريمة المعلوماتية واحدة من الظواهر الإجرامية المستحدثة، والمجرم يحاول دائما الاستفادة من أية وسيلة لارتكاب جرائمه، والتقدم التكنولوجي قدم له وسائل مستحدثة للوصول إلى غايته، والمشرع لا يقف مكتوف الأيدي عندما يجد تهديدا للمصالح الأساسية التي يقوم عليها المجتمع، والحقيقة أن التقدم التكنولوجي خاصة في مجال الاتصالات تسبب إلى جانب خلق وسائل جديدة في ارتكاب الجريمة التقليدية إلى خلق جرائم مستحدثة تتعلق بهذا الكيان التكنولوجي الجديد[1].

وتعد الجرائم المعلوماتية أي الإلكترونية صنفا مستحدثا من الجرائم التي وجب التنبه لمخاطرها وحجم الأضرار الناتجة عنها، لذلك سنحاول التطرق في هذا الفصل للإطار المفاهيمي للجريمة المعلوماتية وذلك بتبيان التعاريف المتعلقة بهذه الظاهرة، أنواعها، خصائصها وكيفية تصنيفها كل هذا في المبحث الأول.

أمّا المبحث الثاني فسيكون تحت عنوان أهم مجالات التعاون الدولي لمكافحة الجرائم المعلوماتية خصص هذا الأخير لمكافحة هذه الجريمة في القانون الجزائري، ماهية التعاون الدولي دون أن ننسى تبيان جهود المنظمة الدولية للشرطة الجنائية والإنتربول في مكافحة الجرائم المعلوماتية.

المبحث الأول: الإطار المفاهيمي للجريمة المعلوماتية

من المؤكد أن الجريمة قد تطورت مع تطور الإنسان ونمط حياته، وقد وصل هذا التطور إلى ذروته مع بروز وسائل وتقنيات الاتصال الحديثة، خاصة الإنترنت، التي أصبحت جزءاً لا يتجزأ من مختلف مجالات الحياة بما في ذلك ارتكاب الجرائم. ومع التزايد الهائل في عدد مستخدمي الشبكة، بدأت تظهر آثار سلبية لهذا الاستخدام، إذ وجد فيها بعض المجرمين وسيلة جديدة لتنفيذ أفعالهم غير المشروعة، وقد أدى ذلك إلى نشوء جرائم مستحدثة لم تكن معروفة من قبل، حيث تحولت شبكة الإنترنت ومختلف الأجهزة المرتبطة بها إلى بيئة خصبة لارتكاب انتهاكات تمس الحياة الخاصة للأفراد، وتتسبب في مضايقتهم أو التشهير بهم أو حتى توجيه اتهامات كاذبة بحقهم، مما جعل من الفضاء الرقمي أداة سهلة لاستهداف الآخرين بطرق متعددة.

الأمر الذي يتعين معه بيان ماهية الجريمة المرتكبة عبر الإنترنت عن طريق الاتصال بشبكة المعلومات الدولية، سواء أكان الاتصال بواسطة حاسب آلي أو كمبيوتر لوحي، أو كمبيوتر محمول أومن خلال أي من أجهزة الاتصالات الحديثة كالتليفونات الذكية أو سواء كانت هذه الأجهزة متصلة بهذه الشبكة بواسطة هاتف سلكي أو لا سلكي، أم عن طريق شريحة خط تليفوني عبر شبكات الهواتف النقالة[2].

[1] ياسر سيد فهمي، المواجهة الموضوعية للجرائم الإلكترونية، دار النهضة العربية، القاهرة، مصر، 2023، ص 07.

[2] بهاء المرى، شرح قانون مكافحة جرائم تقنية المعلومات وحجية الدليل الرقمي في الإثبات، العربية للنشر والتوزيع، أفنان للطباعة، مصر، 2019، ص 13.

المطلب الأول: مفهوم الجريمة المعلوماتية

تعتبر الجريمة المعلوماتية من الظواهر الحديثة وذلك لارتباطها بتكنولوجيا حديثة هي تكنولوجيا المعلومات والاتصالات والكمبيوتر، وقد أحاطت بتعريف الجريمة المعلوماتية الكثير من الغموض حيث تعددت الجهود الرامية إلى ضع تعريف محدد جامع مانع لهما ولكن الفقه لم ينفق على تعريف محدد، بل أن البعض ذهب إلى ترجيح عدم وضع تعريف بحجة أن هذا النوع من الجرائم ما هو إلا جريمة تقليدية ترتكب بأسلوب إلكتروني.

و نتيجة التطور المستمر واللامتناهي التكنولوجيا المعلومات والاتصالات حتى الآن حال ذلك دون وضع تعريف فقهي جامع وشامل المفهوم الجريمة المعلوماتية أو الإلكترونية، وما ورد من تعريفات في الفقه إنما اقتصر على الناحية محل بحث الفقيه[1].

ومما لا شك فيه أن عدم وضع تعريف للجريمة المعلوماتية يثير العديد من المشكلات العملية لعل أهمها صعوبة مواجهتها، وتعذر إيجاد الحلول المناسبة لمكافحتها[2].

وسنحاول في هذا المطلب التعرض إلى التعاريف المختلفة للجريمة المعلوماتية وتبيان أنواعها وخصائصها من خلال ما يلي:

الفرع الأول: تعريف الجريمة المعلوماتية

أولا: تعريف الجريمة لغة:

الجريمة لغة مأخوذة من الجرم وهي الذنب والجناية جمعها جرائم، وجرم الشيء قطعه وجريمة الرجل على قومه وإليهم أذنب وجنى جناية[3].

ثانيا: تعريف الجريمة اصطلاحا:

إن تعريف الجريمة في اصطلاح فقهاء الشريعة الاسلامية له اتجاهان:

أ- **عام:** وهو قولهم (الجريمة هي: فعل ما نهى الله عنه وزجر وعصيان ما أمر الله به)

ب- **خاص:** وهو قولهم (الجريمة هي: محظورات شرعية زجر هللا تعالى عنها بحد أو تعزير) وخير دليل ما ورد في القران الكريم ((قال تعالى " ثم بعثنا من بعدهم موسى وهارون إلى فرعون وملئه بآياتنا فاستكبروا وكانوا قوما مجرمين" يونس – 75–) [4].

---

[1] هشام محمد فريد رستم، قانون العقوبات مخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، مصر، 1995.

[2] نفس المرجع.

[3] احسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة، ط: 03، 2006، ص 3.

[4] القرآن الكريم: سورة يونس، الآية: 75.

ثالثا: تعريف الجريمة الإلكترونية فقها:

تعرّف الجريمة عموما في نطاق القانون الجنائي العام بأنها سلوك الفرد عملا كان أو امتناعا يواجهه المجتمع بتطبيق عقوبة جزائية وذلك بسبب الاضطرابات التي يحدثه في النظام الاجتماعي[1].

وهو التعريف الذي يستند على عناصر الجريمة إلى جانب تبيانه لأثرها (السلوك المشروع، والسلوك غير المشروع وفق القانون للإدارة الجنائية، وأثرها العقوبة أو التدبير الذي يفرضه القانون)؛ وهي الأوصاف التي تميز بين الجريمة عموما وبين الأفعال المستهجنة في نطاق الأخلاق أو الجرائم المدنية أو التأديبية[2]. لقد اختلف الفقهاء حول وضع تعريف موحد للجريمة الإلكترونية ويعود ذلك للاختلاف حول تحديد نطاق هذه الجريمة، فالبعض من الفقهاء ينظر إليها بمفهوم ضيق، والبعض الآخر ينظر إليها بمفهوم موسع، هذا ما سيتم تبيانه من خلال[3]:

أ- **التعريف الضيق**

تعرف الجريمة المعلوماتية على أنها: " كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكاب من ناحية لملاحقته وتحقيقه من ناحية أخرى. "

يرى الأستاذ Mass أن المقصود بالجريمة المعلوماتية: " الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح."

كما عرفها الفقيه الألماني Tiedemann بأنّها: " كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب. فهو يرتكز في تعريفه على وسيلة ارتكاب الجريمة[4]."

يتضح من خلال هذه التعاريف أن الإلمام الواسع بتكنولوجيا الحاسوب لا يُعد ضروريًا فقط لارتكاب الجريمة المعلوماتية، بل هو أيضًا عنصر أساسي في تعقبها والتحقيق فيها، فكل من الجناة والمختصين بملاحقة هذا النوع من الجرائم يحتاجون إلى مستوى عالٍ من المعرفة التقنية، وقد تبنّت وزارة العدل الأمريكية هذا الفهم في تقريرها الصادر سنة 1989 بشأن الجرائم المعلوماتية[5]، وقد انتقد هذا التعريف لكونه يحضر الجريمة المعلوماتية في الحالات التي تتطلب قدرا كبيرا من المعرفة التقنية في ارتكابها، إذ أنه في كثير من الحالات يرتكب الفعل دون الحاجة إلى هذا القدر من المعرفة ورغم ذلك لا يمكننا إنكار أن هذه الأفعال تدخل في عداد الجرائم

---

[1] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، 2005، ص 28.

[2] سميرة معاشي، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني، ع 07، جامعة محمد خيضر بسكرة، افريل 2010 ص276.

[3] نداء نائل فايز المصري، خصوصية الجرائم المعلوماتية، مذكرة لنيل شهادة الماجستير، جامعة النجاح الوطنية فلسطين2017، ص 11.

[4] بعرة سعيدة، الجريمة الالكترونية في التشريع الجزائري، دراسة مقارنة، مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق، كلية الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2016/2015، ص 11.

[5] Benson (Carl), Jablon (Andrew), Kaplan (Paul) & Resenthal (Mara), Computer Crimes, Americain C‹L‹Review, vol‹34, N°21,997, p‹410.

المعلوماتية كإتلاف البيانات المخزنة داخل النظام المعلوماتي، كما أن هذا الفعل محرم قانونا عند معظم التشريعات بما فيها التشريع الجزائري كما سنرى لاحقا.

ويستند أنصار هذا الاتجاه إلى أن الجرائم التي تفتقر إلى هذا القدر من المعرفة تعد جرائم عادية تخضع للنصوص التقليدية للقوانين الجنائية، ومن ثم فلا حاجة إلى نصوص جديدة لتجريمها[1].

كما تحدر الملاحظة أن جانب من هذا الاتجاه يرى أن الجرائم المعلوماتية ليس هي التي يكون الحاسب الآلي أداة لارتكابها، بل هي التي تقع على الحاسب الآلي أو على نظامه المعلوماتي فقط فيعرفون هذه الجريمة بأنها نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي أو تلك التي يتم تحويلها عن طريقه، وما يعاب على هذا التعريف أنه يخرج من نطاق الجريمة المعلوماتية عدد كبير من الأفعال غير المشروعة والتي يستخدم فيها الحاسب الآلي كأداة لارتكابها كالاحتيال المعلوماتي والذي سنتناوله فيما بعد[2].

ب- التعريف الواسع:

هناك تعريفات حاولت التوسع في مفهوم الجريمة المعلوماتية فعرفوها كالآتي: كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الاعتداء على الأموال أو الأشياء المعنوية الخبير الأمريكي parker مفهوما واسعا للجريمة المعلوماتية أنها: كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل.

كما يعرفها الأساتذة Vivant و Lestanc الجريمة المعلوماتية أنها: " مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب."

كما أن الخبير الأمريكي Parker تبنى مفهوما واسعا للجريمة المعلوماتية على أنها: " كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل[3]".

كما عرفتها منظمة التعاون الاقتصادي والتنمية (OCDE) بأنها: " كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة ثم غير مباشرة عن تدخل التقنية المعلوماتية " كما تعرف أيضا: " تلك الجرائم المرتكبة ضد الأملاك باستعمال التقنية أو المعلوماتية."

تُعد هذه التعريفات شاملة وواسعة النطاق، مما يسمح بإحاطة دقيقة بظاهرة جرائم التقنية بمختلف أشكالها، فهي تبرز الطابع التقني الذي يميز هذا النوع من الجرائم، وتوفر إطارًا مرنًا يمكن من خلاله مواكبة التغيرات والتطورات التكنولوجية المستقبلية، ويعتمد هذا النهج التعريفي على المفهوم الواسع للجرائم الإلكترونية، سواء

[1] د الله عادل محمد فريد قورة ، المرجع السابق، ص 29.

[2] سوير سفيان، "جرائم المعلوماتية"، مجلد مذكرة لنيل شهادة الماجستير في العلوم الجنائية و علم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبوبكر بلقايد، تلمسان، 2010، ص 13.

[3] نهلة عبد القادر المومني، الجرائم المعلوماتية، ط1، دار الثقافة للنشر والتوزيع، عمان، 2008، ص 49.

كانت تُرتكب باستخدام الحاسوب كوسيلة أو كهدف، أو من خلال شبكة الإنترنت، أو عبر أي وسيلة إلكترونية أخرى قد تظهر لاحقًا مثل وسائل الاتصال الحديثة كالهاتف المحمول أو جهاز الفاكس وغيرها[1].

جريمة الإلكترونية هي ببساطة استخدام التقنيات الرقمية لإخافة الآخرين.

الفرع الثاني: خصائص الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية، وذلك نتيجة ارتباطها بتقنية المعلومات والحاسب الآلي مع ما يتمتع به من تقنية عالية، وقد أضفت هذه الحقيقة على هذا النوع من الجرائم عدد من السمات والحقائق، والتي انعكست بدورها على مرتكب هذه الجريمة الذي أصبح يعرف بالمجرم المعلوماتي لتميزه أيضا عن المحرم التقليدي، وقد كان لظهور شبكة المعلومات وتطورها إلى الصورة التي أصبحت عليها الآن فيما يعرف بالأنترنت أثره في إعطاء شكل جديد للجريمة المعلوماتية[2].

أولا: الجرائم الإلكترونية جرائم عابرة للحدود

إن تبادل البيانات عبر الشبكات المفتوحة لا صلة له بالمكان والحدود الجغرافية فالجريمة المرتكبة عبر الشبكة الالكترونية جريمة عابرة للحدود والقارات وهذا ما يدرجها في موضوعات القانون الجنائي الدولي.

فمسرح الجريمة لم يعد محليا بل أصبح عالميا إذا أن الفاعل لا يتواجد ماديا على مسرح الجريمة وهذا التباعد في المسافات بين الفعل المرتكب من خلال الحاسوب والفاعل وبين المعلومات التي كانت محل الاعتداء فالجاني يستطيع القيام بجريمته بالدخول إلى ذاكرة الحاسوب الآلي الموجود في بلد أخر وهذا الفعل قد يضر شخصا ثالثا في بلد أخر[3].

ومع القدرة التي يتمتع بها الحاسب أدى ذلك إلى أمكانية حدوث الجريمة الإلكترونية في أماكن متعددة من العالم وفي وقت واحد، كما يمكن أن يكون المجني عليه في غير الدولة التي يقوم فيها الجاني.

ومن خلال هذه الخاصية الدولية يثار إشكال حول الاختصاص القضائي في محاكمة المجني عليه، كون الجاني غير موجود في مكان ما وخلفت الجريمة أثار لها وبالتالي صعوبة تحديد الاختصاص القضائي وإجراءات الملاحقة الجنائية[4].

---

[1] يزيد أبو حليط، الجرائم الالكترونية والوقاية منها في القانون الجزائري، في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، قانون العقوبات –قانون الإجراءات الجزائية– قوانين خاصة، د،ط، دار الجامعة الجديدة للنشر الإسكندرية 2019 ص 51.

2 خالد ممدوح ابراهيم، التقاضي الالكتروني "الدعوى الالكترونية وإجراءاتها أمّام المحاكم"، دار الفكر الجامعي، الإسكندرية

3 سعيد نعيم، المرجع السابق، ص32.

4 صورية بوربانة، التعاون الدولي في مكافحة الجرائم المعلوماتية، مجلة القانون الدولي للدراسات البحثية، ع 01، جامعة طاهري محمد، بشار 2019، ص 93.

فالقضايا المعقدة في هذا المجال كثيرة والتي تضفي إشكالات من الناحية الإجرامية حول الطبيعة الدولية لجرائم الحاسبات الآلية، وللوصول إلى حل أنسب فعلى الدول أن تتطابق تشريعاتها الداخلية، وغياب الاتفاقيات الدولية التي هي الأخرى لما لها من أساليب التي تعالج مثل هذه الأنواع من الجرائم[1].

ثانيا: صعوبة اكتشاف وإثبات الجرائم الإلكترونية

إقامة الدليل وإسناده إلى المجرم هو الأصل في الجريمة ومع التطورات العلمية الحاصلة يمكن نقل بسرعة البيانات المأخوذة من شبكات الالكترونية ومن التجهيزات الحاسوبية من مكان إلى آخر أو العبث بها وإلغاءه نظرا لطبيعة هذه البيانات التي تسمى بالدليل الرقمي.[2]

فالجريمة الالكترونية لا تترك أثارا ملموسة وبذلك لا تترك شهودا يمكن الاستدلال بأقوالهم ولا أدلة مادية يمكن فحصها لأنها تقع في بيئة افتراضية يتم فيها نقل المعلومات وتناولها بواسطة نبضات الكترونية غير مرئية.

و اثبات الجريمة الالكترونية صعب مرجعه لعدة أسباب منها وسيلة التنفيذ التي تتسم في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد ومن ثم فإنها تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها، لأنها تتطلب إلماما خاصا بتقنيات الكمبيوتر ونظم المعلومات [3].

حيث تتجلى صعوبة إثباتها كون الجاني لا يترك خلفه أي أثر مادي ملموس يمكن فحصه مما يصعب إجراءات اكتشافها فكثير من الأحيان لا يتم اكتشافها إلا صدفة فهي جرائم مخفية لا تتقيد بمكان ولا زمان[4].

ثالثا: الجرائم الالكترونية من الجرائم الناعمة

إن الجرائم الالكترونية تستهدف المعنويات لا الماديات فهي لا تتطلب جهدا عضليا ولا عنفا على عكس الجرائم التقليدية التي تتطلب استعمال الأدوات والعنف في السرقة والسطو المسلح فنقل بيانات حاسوب إلى أخر لا يتطلب العنف[5].

إن هذه الجريمة تعتمد على الدراية الذهنية والتفكير العلمي المدروس القائم على معرفة بتقنيات الحاسب الآلي وفي الواقع ليس هناك شعور بعدم الأمان تجاه المجرمين في مجال المعرفة المعلوماتية لأن مرتكبيها ليسوا محترفي الإجرام[6].

1 نائلة عادل محمد فريد قورة، مرجع سابق، ص 55.

2 صورية بوربانة، مرجع سابق، ص 93.

[3] سعيدة بعرة، مرجع سابق، ص34.

[4] صورية بوربابة، المرجع السابق ص 93.

[5] نفس المرجع ، ص 94.

[6] سعيدة بعرة، نفس المرجع السابق ص38.

رابعا: تتطلب خبرة وتحكما في تكنولوجيا المعلوماتية عند متابعتها

إن الجريمة الالكترونية لها طبيعة تقنية وبذلك لا يستطيع رجال الضبطية القضائية التعامل باحترافية ومهارة أثناء البحث والتحري، لذلك لابد أن يكون المحقق متخصص في الجريمة الالكترونية حتى لا يتسبب في إتلاف الدليل الالكتروني[1].

خامسا: اعتماد الجريمة الالكترونية على الخداع والتضليل

يتميز مرتكبو الجرائم الالكترونية بالذكاء والدراية بالأساليب المستخدمة في أنظمة المعالجة الآلية وطريقة تشغيلها وكيفية تخزين المعلومات إذ يعتبر الإجرام الالكتروني إجرام الأذكياء مقارنة مع الإجرام التقليدي كما أن الدافع لارتكابها في اغلب الحالات هو إثبات الذات في التغلب على الأنظمة[2].

الفرع الثالث: أنواع وأركان الجريمة المعلوماتية

أولا: أنواع الجريمة المعلوماتية

الجرائم التي تقع على الأشخاص، هي الجرائم المرتكبة ضد الأشخاص هي تلك التي تستهدف الحقوق الشخصية الأساسية، أمّا من خلال الاعتداء المباشر عليها أو بتهديدها بالخطر، وتشمل هذه الحقوق ما يرتبط بالكيان الإنساني للفرد ولا يمكن أن تكون محلاً للتعامل الاقتصادي، ومن أبرز هذه الحقوق: الحق في الحياة، الحق في سلامة الجسد، الحق في الحرية، والحق في صون الكرامة والشرف.

أ- **الجريمة انتحال الشخصية:** هي جريمة قديمة جدا تتمثل صورها في الكثير من الجرائم التي ترتكب بالطرق التقليدية، إلا أنه ومع انتشار شبكة الانترنت فقد أخذ هذا النوع شكلا جديدا وهي انتحال شخصية الفرد على الشبكة الالكترونية واستغلالها أسوء استغلال وذلك بأخذ البيانات الشخصية كالعنوان و تاريخ الميلاد ورقم الضمان الاجتماعي وما شابهها من أجل الحصول على بطاقات ائتمانية وغيره، ومن خلال هذه المعلومات يستطيع المحرم إخفاء شخصيته الحقيقية والتصرف بحرية تحت اسم مستعار، وغالبا ما يتحصل المنتحل على تلك المعلومات عن طريق الكم الهائل من الإعلانات التي تزدحم بها شبكة الأنترنت[3].

ب- **جريمة المضايقة والملاحقة:** وهو نوع حديث من الجرائم المتزايدة باستمرار مع كل إضفاء وتحديث يطال برامج الحوارات المتبادلة والدردشة، وهي عبارة عن مساحات معروفة في الفضاء الإلكتروني تتيح لمستخدميها الاشتراك في محادثات بين بعضهم البعض.

---

[1] نفس المرجع، ص38.

[2] صورية بوربابة، المرجع السابق ص ص 93، 94.

[3] منير محمد الجنبيهي ممدوح محمد الجنبيهي، جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية 2005 ص ص 42،43

وجرائم الملاحقة تشمل رسائل تهديد وتخويف ومضايقة وقد شبه القضاة هذه الجريمة خارج الشبكات بجرائم التهديد العلني، ولا تتطلب الجريمة المرتكبة عبر الإنترنت أي اتصال مادي بين المجرم والضحية مما يدل أن لها تأثيرات سلبية نفسية فهي لا تؤدي إلى أي تصرفات عنف مادية[1].

ج- **جرائم التغرير والاستدراج:** جرائم التغرير والاستدراج تُعد من أبرز وأوسع الجرائم المعلوماتية انتشار ًالاسيما بين الفئات الصغيرة سناً ومستخدمي الإنترنت بشكل عام، تعتمد هذه الجرائم بشكل أساسي على الخداع حيث يعمد الجاني إلى إيهام الضحية برغبته في بناء علاقة صداقة أو زواج عبر الإنترنت، وغالباً ما تتطور هذه العلاقات الزائفة إلى لقاءات واقعية، مما يزيد من خطورتها، وتكمن خطورة هذا النوع من الجرائم في عدم خضوعها لأي حدود جغرافية أو سياسية أو اجتماعية، إذ يمكن لأي شخص في أي مكان أن يرتكبها بسهولة، كما يمكن أن يقع في شراكها أي مستخدم حسن النية[2].

د- **جرائم التشهير وتشويه السمعة:** مع انتشار الشائعات والأخبار الكاذبة التي تطول وتمس رموز الشعوب سواء كانت تلك الرموز فكرية أو سياسية أو حتى دينية، وقد ظهرت على شبكة الانترنت بعض المواقع والتي جندت نفسها لهدف واحد هو خدمة تلك الشائعات والأخبار الكاذبة وذلك بهدف تشهير وتشويه سمعة تلك الرموز، وكذلك لتسميم أفكار الناس أو محاولة ابتزاز بعض الأشخاص بنشر الشائعات عنهم،

وأبرز وسائل ارتكاب هذه الجريمة إنشاء مواقع على الشبكة تحتوي المعلومات المطلوب إدراجها ونشرها أو إرسالها عبر المواقع الإلكترونية، ومن أمثلتها إرسال الصور الغير اللائقة أو معلومات غير صحيحة[3].

هـ- **الجرائم المخلة بالأخلاق والآداب العامة :** إذا كانت شبكة الأنترنت تتسم بالعالمية ولا تقتصر على مستخدم دون الآخر، فإن ما يتم عرضه من مواد تعد مخلة بالآداب والأخلاق العامة في بلد معين قد تشكل جريمة يعاقب عليها القانون في حين أنها ال تكون كذلك في أي بلد آخر، وتشمل هذه الجرائم تحريض القاصرين على أنشطة جنسية غير مشروعة فسادهم عبر الوسائل الإلكترونية أو محاولة إغوائهم لارتكاب هذه الأنشطة، أو نشر معلومات عنهم عبر الحاسب الآلي ودعوتهم إلى القيام بالأعمال الفاحشة و تصوير قاصرين ضمن أنشطة للجنس، فالأعمال الإباحية هي من أشهر الأعمال الحالية وأكثرها رواجا خاصة في الدول العربية وأوروبا والدول الآسيوية، وتشمل الجرائم المخلة بالأخلاق والآداب العامة على الأنترنت كافة الإشكال سواء كانت صور أو فيديو أو حوارات أو أرقام هاتفية مما خول هذه الشبكة أن تكون في متناول أيدي الجميع ودون أي حواجز[4].

---

[1] محمد أمين احمد الشوابكة، جرائم الحاسوب الأولى والإنترنت، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، 2004، ص45.

[2] عبد الكريم شيباني، الحماية الإجرائية والموضوعية للجريمة المعلوماتية، مذكرة لنيل شهادة ماستر، كلية الحقوق والعلوم السياسية، جامعة الطاهر موالي، سعيدة، 2015/2016، ص 19.

[3] منير محمد الحنبيهى، ممدوح محمد الجنبيهي، المرجع السابق، ص 34.

[4] محمد امين احمد الشوابكة، المرجع السابق، ص 114.

و- **الجرائم التي تقع على الأموال:** هي جرائم الاعتداء على الأموال والتي تهدد الحقوق ذات القيمة المالية ويدخل في نطاق هاته الحقوق الحق ذو قيمة اقتصادية، فإذا كان موضوع الاعتداء على الأموال في نطاق ما ينصب على الحاسب الآلي ذاته وما يرتبط به من أسلاك وما يتصل به من ملحقات فأنه هنا لا يثير أي صعوبة في تطبيق النصوص الجزائية التقليدية كون الأمر يتعلق بمال عادي منقول أمّا إذا وقع الاعتداء على ما يتعلق بفن الحاسب الآلي من برمجيات ونظم فإن النصوص التشريعية التقليدية قاصرة عن حمايتها لما لهذا المجال من طابع خاص غير تقليدي[1].

ز- **جرائم صناعة ونشر الفيروسات:** الفيروس هو برنامج مثل أي برنامج آخر موجود على جهاز الحاسب الآلي، ولكنها مصممة بحيث يمكنها التأثير على كافة البرامج الأخرى الموجودة على الجهاز بأن تجعل تلك البرامج نسخة منها أو أن تعمل على مسح كافة البرامج الأخرى وبالتالي تعطلها عن العمل.

أمّا عن مبدأ عملها فيتحدد طبقا لأسلوب تصميمها، فقد تبدأ بالعمل بمجرد فتح الرسالة الموجودة بها و قد تبدأ بمجرد تشغيل البرنامج الموجودة عليه، وتعتبر هذه الصناعة من أهم جرائم الأنترنت وأكثرها اتساعا و انتشار ويعود تاريخ الفيروسات لأول مرة في أربعينيات القرن الماضي حين تحدث عنها العالم الرياضي "فون نيو مان" على صعيد الحاسب الآلي دون الأنترنت، ومن أشهرها فيروس رسائل الحب، فيروس الدودة الحمراء، وقد أحدث هذا الأخير أعطالا في أكثر من ربع مليون جهاز كمبيوتر في أقل من 9 ساعات عام 2001[2].

ح- **جرائم الاختراقات:** الاختراق هو عبارة عن عملية دخول غير مصرح به إلى أجهزة الغير والشبكات الإلكترونية، ويتم هذا الاختراق بواسطة برامج متطورة يستخدمها كل من يملك الخبرة وله القدرة على تخطي أي إجراءات أو أنظمة حماية اتخذت لحماية تلك الحاسبات أو الشبكات.

وتختلف أسباب الاختراق باختلاف أهداف المخترق، فمنهم من يخترق أجهزة البعض أو مواقعهم لمجرد الفضول والبعض الأخر لسرقتها، وهذا هو السبب الأبرز الذي يدفع المخترقين إلى الدخول إلى مواقع الحواسيب الأخرى لسرقة معلوماتهم التي قد يكونون قد عرضوها مقابل مبلغ مالي للاطلاع عليها.

وقد يكون السبب تبديل أو تحريف أو تعطيل المعلومات في أجهزة الغير، وهو أخطر أنواع الاختراق، ومن أبرز ضحايا الاختراق فهي مواقع الأنترنت التي يقوم المخترقون بتحريف تصاميمها ومعلوماتها، هذه العملية تسمى تغيير وجه الموقع[3].

ط- **جريمة تعطيل الأجهزة والشبكات:** يطال التعطيل أجهزة الحاسب الآلي عبر برابحها، كما قد يؤدي تعطيل البرامج إلى أعطال فنية تقع على القطع الإلكترونية للجهاز والهدف من التعطيل منع الحواسيب والشبكات من تأدية عملها دون أن تتم عملية اختراق فعلية لتلك الأجهزة وتتم عملية تعطيل الأجهزة عن طريق إرسال

[1] نفس المرجع، ص 136.

[2] منير محمد الحنبيهى، ممدوح محمد الحنبيهى، المرجع السابق، ص 36.

[3] نفس المرجع، ص37.

عدد هائل من الرسائل بطرق فنية معينة إلى الأجهزة أو الشبكات المراد تعطيلها، الأمر الذي يعيفها عن تأدية عملها[1].

ي- **جريمة النصب والاحتيال** مع التطور السريع للتكنولوجيا، بات التعاقد عبر الإنترنت يشكل ضرورة ملحة وأداة عملية، لما يوفره من سرعة وسهولة في إبرام المعاملات. غير أن هذه المزايا لم تخلُ من سلبيات إذ سرعان ما ظهرت إلى السطح ممارسات إجرامية تمثلت في أفعال النصب والاحتيال، ومن أبرزها:

✓ خرق التعاملات عبر طرق احتيال جديدة تم ابتكارها، وكذلك زادت من وقوع جرائم النصب التي لا يزال يقع فيها عدد كبير من مستخدمي الأنترنت.

✓ أمّا المظهر الأبرز للاحتيال فهو سرقة معلومات البطاقات الائتمانية واستخدام هذه المعلومات لسرقة المبالغ الموجودة داخل حسابات الضحايا، ومرتكبو الجرائم عبر تلك الوسائل يسهل هروبهم وتواريهم لذلك من الصعب جدا ملاحقتهم والقبض عليهم[2].

الجدول التالي يلخص أنواع الجريمة الإلكترونية:

- **جدول رقم 01: أنواع الجريمة الإلكترونية:**

نوع الجريمة	اسم الجريمة	الشرح
الجرائم الواقعة على الأشخاص	انتحال الشخصية	ستغلال هوية شخص آخر على الإنترنت للحصول على بياناته واستعمالها في أنشطة غير مشروعة، كالحصول على بطاقات ائتمانية.
	المضايقة والملاحقة	إرسال رسائل تهديد أو تخويف عبر برامج المحادثة والدردشة دون اتصال مادي مباشر مما يترك أثراً نفسياً كبيراً.
	التغرير والاستدراج	خداع الضحية، خاصة من الفئات الصغيرة سناً بهدف بناء علاقة زائفة تؤدي أحيانًا إلى لقاءات خطيرة في الواقع.
	التشهير وتشويه السمعة	نشر شائعات أو أخبار كاذبة بهدف الابتزاز أو التأثير في الرأي العام، باستخدام مواقع إلكترونية أو وسائل تواصل

[1] نفس المرجع، ص 38.

[2] عبد الكريم شيباني، مرجع سابق، ص 23.

	الجرائم المخلة بالأخلاق والآداب العامة	تشمل التحريض على أنشطة جنسية غير مشروعة، ونشر مواد إباحية أو صور وفيديوهات فاحشة، خصوصًا التي تستهدف القاصرين
الجرائم الواقعة على الأموال	صناعة ونشر الفيروسات	تصميم برامج تخريبية تعطل البرامج أو تمسحها أشهرها فيروس "الدودة الحمراء" و"رسائل الحب"
	الاختراقات	دخول غير مصرح به إلى أجهزة أو مواقع الغير بهدف سرقة أو تحريف المعلومات، ويُستخدم لذلك برامج متطورة.
	تعطيل الأجهزة والشبكات	إرسال كم هائل من الرسائل يؤدي إلى شلل الأجهزة أو الشبكات دون اختراق فعلي مما يمنعها من أداء وظائفها.
	النصب والاحتيال	استغلال الإنترنت لإبرام صفقات وهمية أو سرقة بيانات بطاقات ائتمان، مع صعوبة تتبع الجناة بسبب إخفاء هويتهم.

المصدر: سعيد بن بوزيد، *الجرائم الواقعة على الأشخاص عبر الوسائط الإلكترونية*، ع 6، مجلة الحقوق والعلوم السياسية، جامعة بسكرة، 2020، ص 101.

ثانيا: أركان الجريمة المعلوماتية:

أ- الركن الشرعي للجريمة المعلوماتية: إن الجريمة هي نتيجة الأفعال المادية الصادرة عن الإنسان هذه الأفعال تختلف حسب نشاطات الإنسان، وهذا ما جعل المشرع يتدخل لتجريم هذه الأفعال الضارة بموجب نص قانوني يحدد فيه الفعل الضار أو المجرم والعقوبة المقررة لارتكابه[1].

القاعدة الأساسية الناتجة عن مبدأ الشرعية وهي عدم رجعية القانون الجنائي بمعنى لا يمكن معاقبة شخص ارتكب فعلا لم يجرمه القانون[2] ، وهذا ما نصت عليه المادة الأولى من قانون العقوبات "لا جريمة ولا عقوبة أو تدبير أمن بغير نص قانوني"[3].

[1] أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة، الجزائر، ط: 10، 2011، ص 27.

[2] أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط: 02، 2006، ص 78.

[3] المادة 1 في الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون العقوبات، المعدل والمتمم.

حيث يتميز هذا المبدأ أن القاضي الجنائي عند تفسيره لنصوص القانون أن يفسره تفسيرا ضيقا، بالإضافة إلى منع اللجوء إلى القياس بمعنى عدم لجوء القاضي الجنائي إلى قياس فعل لم يرد نص بتجريمه على فعل ورد نص بتجريمه فيقرر القاضي الجنائي للأول عقوبة الثاني للتشابه بين الفعلين[1].

كذلك تستمد الجرائم الإلكترونية شرعيتها من مختلف التشريعات الوطنية الصادرة بشأن الجريمة الإلكترونية فقد بذلت هيئة الأمم المتحدة جهودا كبيرة إضافة إلى جهود المجلس الأوروبي لإقناع الدول بوضع تشريعات للتصدي ومواجهة ومكافحة جرائم الإلكترونية وتعزيز التعاون الدولي في هذا المجال. وسنرى فيما يلي نماذج لبعض التشريعات على المستوى الدولي:

تؤدي العديد من الهيئات والمنظمات دورا ملحوظا في إبرام الاتفاقيات وذلك كمحاولة لترسيخ وجوب التعاون الدولي لمواجهة الجريمة الإلكترونية وكمثال على ذلك الاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية "بودبست "وقعت هذه الاتفاقية سنة 2001 ببودابست، ودخلت حيز التنفيذ في جويلية سنة 2004 وهي وثيقة دولية ملزمة بالنسبة للدول الأطراف فيها. وتناولت الجريمة الإلكترونية من كل جوانبها سواء ما يقع ضد الشبكات أو الجرائم التقليدية التي تستخدم في ارتكابها الشبكات الإلكترونية[2].

ب- الركن المادي للجريمة المعلوماتية: لا بد من فعل أو امتناع يمكن إثباته إذ لا عبرة بما في خلد الإنسان من أفكار لأنها لا تدخل دائرة التجريم، والركن المادي هنا يختلف من حال لآخر حسب التصنيف الذي يقع على الفعل وعليه لا يمكن حصر الجريمة المعلوماتية تحت تكييف واحد، فقد تشكل الواقعة المرتكبة والتي تحمل وصف الجريمة المعلوماتية واقعة قذف أو تهديد أو تحريض وبشكل مطابق تماما لمّا يجري عليه قانون العقوبات من خلال بعض القواعد التي ينطبق حكمها حتى على الجرائم الواقعة عن طرق جهاز الكمبيوتر وهذا لا يسبب إشكالا، إذ يمكن تطبيق نصوص قانون العقوبات على هذه السلوكيات التقليدية، إلا أن هناك أنواعا من السلوك يتطلب التمييز بينها وبين سابقتها، و هذا ما يدعو للتدخل التشريعي[3].

يتمثل الركن المادي في الجريمة الإلكترونية في عناصر ثلاثة: السلوك الإجرامي، والنتيجة، وعلاقة السببية بينهما، وتجدر الإشارة إلى أن هذا الركن قد يتحقق أحيانًا حتى في غياب النتيجة الفعلية للجريمة.

كما هو الحال عند الإبلاغ عن الفعل الإجرامي قبل تحقق آثاره، كمن يُنشئ موقعًا بقصد التشهير بشخص معين دون أن يقوم بنشره أو إتاحته على الشبكة، إلا أن مجرد إنشاء الموقع يحمل طابعًا إجراميًا يستوجب المساءلة القانونية؛ تتعدد صور الركن المادي في الجرائم المعلوماتية بحسب طبيعة الفعل الإيجابي

[1] معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة مكملة لنيل شهادة الماجستير وعلوم الجنائية، 2011-2012، ص 25.

[2] علي جبار الحسناوي، جرائم الحاسوب والأنترنت، دار اليازوري، الأردن 2009، ص ص 147، 148.

[3] بن غدفة شريفة والقص صليحة، الجريمة الإلكترونية الممارسة ضد المرأة على صفحات الأنترنت وطرق محاربتها أعمال الملتقى الوطني، "آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، الجزائر، 29 مارس 2017، ص 48.

المرتكب، فعلى سبيل المثال يتمثل الركن المادي في جريمة الغش المعلوماتي في القيام بتغيير الحقيقة في البيانات أو الوثائق الإلكترونية سواء كانت تلك التعديلات واقعة على سجلات رقمية أو محررات إلكترونية[1].

يقوم الركن المادي للجريمة الإلكترونية على صورتين أساسيتين:

الصورة الأولى: متمثلة في الاعتداء على نظام المعالجة الآلية وتحتوي على نوعين من الاعتداء:

النوع الأول: وهو الدخول والبقاء الغير مشروع في نظام المعالجة الآلية يشمل هذا النوع ثالث أفعال فعل الدخول والبقاء والعرقلة أو التعطيل.

النوع الثاني: متمثل في الاعتداء العمدي على نظام المعالجة الآلية للمعطيات وتندرج تحت هذا النوع كذلك ثالث أفعال وهي فعل الإدخال والمحو والتعديل.

الصورة الثانية: متمثلة في الاعتداء على منتجات العالم الآلي وتحتوي هذه الصورة على فعل التزوير المعلوماتي.[2]

ج- الركن المعنوي للجريمة المعلوماتية: تُعد الجرائم المعلوماتية، شأنها شأن باقي الجرائم، قائمة في أساسها على توافر القصد الجنائي العام، الذي يتمثل في العلم بالفعل المرتكب وإرادة ارتكابه، كشرط جوهري لتحقق المسؤولية الجنائية، و لا يمكن تصور تحقق القصد الخاص في هذه الجرائم من دون أن يُسبق بوجود القصد العام، أمّا القصد الخاص، فيرتبط بطبيعة الجريمة المعلوماتية ذاتها، ويُستدل عليه من النية المحددة التي يحملها الجاني عند إقدامه على الفعل غير المشروع. وبذلك، يتكوّن الركن المعنوي للجريمة الإلكترونية من عنصرين أساسيين :العلم بمدى عدم مشروعية الفعل، والإرادة الحرة في ارتكابه أي بمعنى آخر:

العلم: هو إدراك الفاعل للأمور.

أمّا **الإرادة:** فهي اتجاه السلوك الإجرامي لتحقيق النتيجة.

وفقًا للمبادئ العامة في قانون العقوبات، يُمكن أن ينقسم القصد الجنائي إلى نوعين: قصد عام وقصد خاص، فالقصد الجنائي العام يتمثل في نية الجاني عند ارتكاب السلوك الإجرامي، أي الإرادة الحرة الواعية في تنفيذ الفعل المجرَّم قانونًا، أمّا القصد الجنائي الخاص، فهو عنصر إضافي يُشترط في بعض الجرائم دون غيرها إذ لا يكتفي الجاني بمجرد ارتكاب الفعل، بل يكون لديه نية محددة لتحقيق نتيجة معينة فعلى سبيل المثال في جريمة القتل، لا يكفي أن يعتدي الجاني على المجني عليه، بل يجب أن يكون هدفه إزهاق روحه من هذا المنطلق، يُطرح التساؤل: ما هو نوع القصد الجنائي المطلوب توافره لقيام الجريمة الإلكترونية؟ وهل يكفي القصد العام، أم يجب أن يقترن بقصد خاص حسب نوع الجريمة المرتكبة في الفضاء الرقمي؟

---

[1] فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر " الجرائم الإلكترونية "، طرابلس، بتاريخ 25-24 مارس 2017، ص 118.

[2] اسامة احمد المناعسة، جلال محمد الزغبي، جرائم تقنية نظم المعلومات الإلكترونية، ط3، دار الثقافة للنشر والتوزيع، عمان 2004، ص48.

الأصل إن الفاعل في الجريمة الالكترونية يوجه سلوكه الإجرامي نحو ارتكاب فعل غير مشروع أو غير مسموح به مع علمه وقاصدا ذلك ومهما يكن لا يستطيع انتفاء علمه كركن للقصد الجنائي العام.

إذن فالقصد الجنائي العام متوافر في جميع الجرائم الإلكترونية دون أي استثناء ولكن هذا لا يمنع أن بعض الجرائم الإلكترونية يتوافر فيها القصد الجنائي الخاص (مثال: جرائم تشويه السمعة عبر الأنترنت وجرائم نشر الفيروسات عبر الشبكة). وفي كل الأحوال يرجع الأمر للسلطة التقديرية للقاضي[1].

أمّا عن الإثبات في توافر الركن المعنوي في الجرائم المعلوماتية فهو يقع على عاتق النيابة العامة والمحكمة المختصة بالنظر في مثل هذا النوع من القضايا، والمحكمة صاحبة الصلاحية بتقدير وجود سوء النية من عدمها ووزن البيانات تمحيصها بما لها من صلاحية باعتبارها صاحبة القرار النهائي بالفصل في الدعاوى المرفوعة أمامها[2].

المطلب الثاني: تصنيف الجرائم المعلوماتية

للجرائم المعلوماتية صور متعددة لا يمكن حصرها، كونها متجددة ومتزايدة باستمرار وبصورة مطردة مع التطور التكنولوجي من جهة، لكن مع ذلك فقد حاول بعض الفقهاء ودارسو الجرائم المعلوماتية تقسيم إلى فئات متعددة تختلف حسب الأساس والمعيار الذي يستند إليه تقسيم المعنى، وبالتالي سنورد أهم هذه المعايير كالآتي:

الفرع الأول: تصنيف الجرائم المعلوماتية تبعا لنوع المعطيات ومحل الجريمة

يعكس هذا التصنيف والتطور التاريخي لظاهره الجرائم المعلوماتية وهذا التصنيف كان سائد في مختلف كتابات الفقهاء، ولهذا نجد أن الجرائم المعلوماتية بحسب هذا المعيار تنقسم الى ما يلي:

أولا: الجرائم الماسة بقيمة معطيات الحاسوب: تنقسم هذه الجرائم على فئتين:

أ- **الفئة الأولى:** الجرائم الواقعة على ذات المعطيات:

كإتلاف البيانات والمعلومات واتلاف برامج الحاسوب ذاتها بما في ذلك استخدام الفيروسات

ب- **الفئة الثانية:** الجرائم الواقعة على ما تمثله هذه المعطيات:

اليا من أموال أو أصول كجرائم غش الحاسوب التي تستهدف الحصول على المال او جرائم الاتجار بالمعطيات وجرائم التلاعب بالمعلومات المخزنة داخل الحاسوب واستخدامها دون وجه حق كتزوير المعالجة الآلية واستخدامها[3].

ثانيا: الجرائم الماسة بالمعطيات الشخصية البيانات المتصلة بالحياة الخاصة:

---

[1] فضيلة عاقلي، المرجع السابق، ص 120.

[2] لورنس سعيد الحوامدة، "الجرائم المعلوماتية أركانها وآلية مكافحتها" دراسة تحليلية مقارنة، مجلة ميزان للدراسات القانونية والشرعية، الأردن، 2016/08/13، ص 24.

[3] يوسف المصري، الجرائم المعلوماتية والرقمية للحاسوب والأنترنت، ط 1، دار العدالة، عمان، 2011، ص ص 26،27.

تشمل هذه الفئة الجرائم الاعتداء على المعلومات والبيانات الشخصية المتعلقة بالحياة الخاصة، تعد هذه الجرائم من أخطر الصور لأنها تنطوي على الاعتداء على المعلومات المخزنة في الحاسوب واستغلالها بأمور مشروعة بصور مختلفة.

قد تأخذ جرائم المعلوماتية الماسة بالمعطيات الشخصية صورة نقل او تسجيل المحادثات الخاصة وسائط الاتصال والتصنت عليها وهذا يمثل اعتداء على الحياة الخاصة، كذلك يعد انشاء البيانات الشخصية السرية سواء تم من قبيل الخطأ او بقصد التشهير او تهديد من صور الاعتداءات الحياة الخاصة؛ لان قيام شخص بإيداع بياناته لدى مؤسسه تحوز على ثقته وقيام تلك المؤسسة بإفشائها باي وسيله من الوسائل سالفة الذكر تعد من الجرائم التي تمس حياته الخاصة ولا يشترط القانون في بعض الدول ان تكون هذه البيانات حقيقية او مزورة بل يكفي ان تمس بشرف.

أمّا بالنسبة للأشخاص الاعتبارية فانقسم الفقه بشأن وجوب حماية خصوصيتها الى رأيين:

° الرأي الأول: أنكر عليها هذا نظرا لعدم تمتعها بالشخصية القانونية حيث حصر الشخصية القانونية في الشخص الطبيعي.

° الرأي الثاني: اقر لها بالحماية استنادا الى ان هؤلاء الاشخاص تمنح لها حق الجنسية كالشخص الطبيعي وبالتالي كل ما يتمتع بالجنسية يمكن اعتباره مواطن فله الحماية القانونية للمعلومات الخاصة به[1].

ثالثا الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه

تشمل نسخ وتقليد البرامج و اعاده إنتاجها دون ترخيص وبالنظر في هذه الفئات نجد تداخل في ما بينها إذ أن الاعتداء على معطيات الحاسوب بالنظر إلى قيمتها الذاتية أو ما تمثله هو اعتداء على امن المعطيات لكن الغرض المباشر الذي يستهدفه الاعتداء ينصب على قيمتها، والاعتداء على حقوق الملكية الفكرية لبرامج الحاسوب هو اعتداء على حقوق المالية واعتداء على الحقوق الأدبية لكنها تميزت عن باقي الفئات بأنها محلها هو البرامج فقط والاستخدام الغير مشروع لها.

ومن جهة أخرى نجد أن الحماية الجنائية في القانون المقارن اعتمدت على نحو غالبا لتقسيم المتقدم فظهرت حماية حقوق الملكية الأدبية للبرامج وأيضا حماية البيانات الشخصية المتصلة بالحياة الخاصة وحماية المعطيات بالنظر إلى قيمتها أو ما تمثله والذي عرف بحماية الأموال كل في ميدان وموقع مستقل وهو في الحقيقة تمييز ليس مطلقا بين حماية قيمة المعطيات وأمنها وحقوق الملكية الفكرية ولا بدا من الإشارة إلى أن حماية أمن المعطيات (الطائفة الثانية) انحصر في حماية البيانات الشخصية المتصلة بالحياة الخاصة أو حماية البيانات والمعلومات السرية والمحمية، فقد تم تناوله في نطاق جرائم الطائفة السابقة الماسة بقيمة المعطيات.

[1] ممدوح بحر، حماية الحياة الخاصة في القانون الجنائي، دار الثقافة للنشر، عمان، 1996، ص 288.

وبالنظر إلى أن الدافع الرئيسي للاعتداء والغرض من معرفة أو إفشاء هذه المعلومات غالبا ما يكون الحصول على مقابل مالي مما يعد من اعتداءات التي تندرج تحت نطاق الجرائم الماسة بقيمة المعطيات التي تتطلب توفير الحماية الجنائية للحقوق المتصلة بالذمة المالية التي تستهدفها هذه الجرائم[1].

الفرع الثاني: تصنيف الجرائم المعلوماتية تبعا لدور الحاسب الآلي في الجريمة

يُعد الحاسوب والتقنيات المعلوماتية عنصرًا محوريًا في الجريمة المعلوماتية، إذ يمكن أن يكون هدفًا مباشراً للسلوك الإجرامي، وذلك عندما يتم استهداف البيانات التي تُعالج أو تُخزن أو تُنقل عبر الأجهزة التقنية والشبكات، وهو ما يُعرف بالمفهوم الضيق للجريمة المعلوماتية.

كما قد يُستخدم الحاسوب وغيره من الوسائل الإلكترونية كأداة لارتكاب جرائم أخرى، أو قد يُشكّل البيئة التي تُرتكب فيها الجريمة، وفي هذا السياق، يظهر نوع من الخلط بين مفهومين يُستخدمان لوصف هذا الدور المتعدد للحاسوب في ارتكاب الجرائم، وهو ما يستدعي التمييز بينهما بدقة.

الأول: جرائم التخزين ويقصد بها تخزين المواد المستخدمة في ارتكاب الجريمة.

الثاني: جرائم المحتوى او ما يعبر عنه بالمحتوى غير القانوني او المحتوى غير المشروع.

أصبح يُقصد بالمحتوى غير القانوني، ذلك النوع من الجرائم المرتبط بنشر المواد الإباحية، والمقامرة وغيرها من الأنشطة غير المشروعة، خاصة مع تحوُّل مواقع الإنترنت إلى منصات لترويج مثل هذه الأفعال.

والواقع أن هذين المفهومين – أي استخدام الحاسوب كوسيلة وبيئة للجريمة – يرتبطان بشكل مباشر بدور التكنولوجيا الحديثة، حيث تُستغل الأجهزة والوسائط الإلكترونية ليس فقط كأدوات لتنفيذ الجريمة، بل أيضًا كفضاء افتراضي تُرتكب فيه، وبناءً على هذا التصور، يمكن تقسيم الجرائم المعلوماتية إلى عدة أنواع وفقًا لطبيعة العلاقة بين الجريمة والوسيلة الإلكترونية المستخدمة.

– تستهدف نظام المعلوماتية نفسه على المعلومات واتلافها وجرائم ترتكب بواسطة الحاسوب وغيره من التقنيات كجرائم احتيال الحاسوب أمّا تقسيمها كجرائم هدف ووسيلة ومحتوى فانه الاتجاه العالمي في ضوء تطور التدابير القانونية والتشريعية للجرائم المعلوماتية حيث انه هناك اتجاه الى وضع إطار عام لتصنيف الجرائم الإلكترونية ويمكن تقسيمها تبعا لدور الحاسوب والتقنية المعلوماتية في الجريمة كما يلي[2]:

الطائفة الأولى: الجرائم التي تستهدف عناصر السرية والسلامة الخاصة بالمعطيات والنظم:

وتضم هذه الطائفة الدخول غير القانوني أي غير المصرح به والاعتراض غير القانوني، وتدمير المعطيات والمعلومات واعتراض النظم أو إساءة استخدم الأجهزة الإلكترونية.

[1] يوسف المصري، المرجع السابق، ص 26 وما بعدها.

[2] اتفاقية اتفاقية بوداست لمكافحة الجريمة المعلوماتية، تم اعتمادها من قبل لجنة وزراء مجلس أوروبا في دورته التاسعة بعد المائة بتاريخ 8 نوفمبر لعام 2001، وفتح باب التوقيع عليها في بودابست في 23 نوفمبر ودخلت حيز النفاذ في 1 يوليو لعام 2004. ص 13

الطائفة الثانية: الجرائم المرتبطة بالحاسوب والتقنية المعلوماتية ونذكر من هذه الطائفة التزوير والاحتيال الإلكتروني.

الطائفة الثالثة: الجرائم المرتبطة بالمحتوى: وتشمل طائفة واحدة وفق هذه الاتفاقية، وهي الجرائم المتعلقة بالأفعال اللاأخلاقية.

الطائفة الرابعة: وهي طائفة الجرائم المرتبطة بالإخلال بحقوق الفكرية كقرصنة البرمجيات[1].

الفرع الثالث: تصنيف الجرائم المعلوماتية تبعا لمساسها بالأشخاص والأموال

يمكن تقسيم الجرائم المعلوماتية طبقا لهذا المعيار الى ما يلي:

أولا: الجرائم التي تستهدف الاشخاص

و تضم هذه الفئة نوعين رئيسين من الجرائم:

النوع الأول: الجرائم غير الجنسية، وتشمل مجموعة من الأفعال الإجرامية التي تُرتكب عبر الوسائل الإلكترونية، مثل: التحريض على الانتحار، الملاحقة أو التتبع الإلكتروني، نشر المعلومات الكاذبة، القتل باستخدام الحاسوب أو التسبب في الوفاة عن طريقه، جرائم الإهمال الناتجة عن استخدام التكنولوجيا، الرسائل الإلكترونية المزعجة(Spam) ، إضافة إلى الأفعال التي تؤدي عمدًا إلى الإضرار بالحالة النفسية والعاطفية للضحية عبر الوسائل التقنية.

النوع الثاني: الجرائم الجنسية وتشمل: (حض وتحريض القاصرين على أنشطة جنسية غير مشروعة إفساد القاصرين بأنشطة جنسية عبر الوسائل الإلكترونية وإغواء أو محاولة إغواء القاصرين لارتكاب أنشطة جنسية غير مشروعة – التحرش الجنسي بالقاصرين عبر الحاسب الآلي والوسائل التقنية الحديثة نشر وتسهيل نشر واستضافة المواد الفاحشة عبر الإنترنت بوجه عام وللقاصرين تحديدا المساس بالحياء عبر الإنترنت استخدام الإنترنت لترويج الدعارة بصورة قصرية أو للإغواء أو النشر المواد الفاحشة التي تستهدف استغلال عوامل الضعف والانحراف لدى المستخدم – الحصول على الصور والهويات بطريقة غير مشروعة لاستغلالها في أنشطة خبيثة)، وبالتركيز في هذه الأوصاف نجد أنها تجتمع جميعا تحت صورة واحدة ألا وهي استغلال الإنترنت والحاسوب لنشر الدعارة واستغلال الأطفال و القصر في الأنشطة الجنسية غير المشروعة[2].

[1] يوسف المصري، المرجع السابق، ص ص 28،29.

[2] غانم مرضي الشمري، الجرائم المعلوماتية، ط 1، دار الثقافة، عمان، 2016، ص 58.

ثانيا: طائفة جرائم الاموال عدا السرقة

يقصد بذلك تلك الأفعال التي تنطوي على الولوج أو الاقتحام غير المصرح به إلى أنظمة المعلومات عبر الشبكة، سواء تم ذلك بشكل مجرد أو بغرض ارتكاب أفعال أخرى تمس البيانات، البرامج، أو النظم المعلوماتية؛ تشمل هذه الأفعال مفاهيم متعددة مثل: تدمير الحواسيب، التعدي على الملكية الرقمية، إنتاج الفيروسات الخبيثة، استخدام الأسماء التجارية الإلكترونية دون ترخيص، الإتلاف غير المشروع لنظم الحاسوب، تنفيذ هجمات إنكار الخدمة (DDoS)، الحيازة غير المشروعة للمعلومات، وسوء استخدام البيانات والمعلومات الرقمية[1].

ثالثا: جرائم الاحتيال والسرقة

تتفق جريمة النصب (الاحتيال) مع جريمتي السرقة وخيانة الأمانة في أنها أيضا تطال مال الغير إلا أنها تختلف عنهما في أن محلها يمكن أن يكون عقارا أو منقولا، أمّا جريمتي السرقة وخيانة الآمنة فلا تردان إلا على مال منقول إضافة إلى أن السلوك في جريمة النصب يتخذ صورة للقيام بالطرق الاحتيالية أمّا في جريمة خيانة الأمانة يتخذ صورة الكتمان أو التبديد أو إتلاف مال سبق تسلمه بموجب عقد أمانة.

من بعض التعريفات الفقهية لجريمة الاحتيال استعمال الجاني وسيله من وسائل التدليس المحددة على سبيل الحصر ودفع المجني عليه بذلك على تسليم الجانّي مالا منقولا للغير[2].

أمّا مصطلح التحايل المعلوماتي فهو مصطلح حديث النشأة فعرفته هيئة الامم المتحدة الاحتيال بأنه "الادخال أو المحو أو التعديل للبيانات أو برامج الحاسوب او تدخل المؤثر في معالجه البيانات التي تسبب خسارة اقتصادية أو فقد حيز ملكيه شخص اخر بقصد الحصول على كسب اقتصادي غير مشروع لها ولشخص آخر"[3].

تشمل جرائم الاحتيال على التلاعب بالنظم المعلوماتية او استخدام البطاقات بدون ترخيص وقرصنه البرامج هو سرقه خدمات الحاسوب.

رابعا: جرائم التزوير

لقد انتشر استخدام الحاسوب انتشارا واسعا في شتى المجالات في التعامل بين الأفراد ويمكن القول أنه حل محل الأوراق العادية في أغلب نظم المعالجة الآلية للمعلومات ومع تزايد حجم الاعتداءات الواقعة على البيانات والمعلومات التي تمس الأفراد في حقوقهم وأموالهم، في مقابل ذلك تزايدت فرص الأشخاص للعبث والتلاعب في معطيات الحاسوب بتبديلها وتحويرها بالشكل الذي يفقد الثقة بالتقنية ويمس مراكز الأفراد وبات من الواجب بسط الحماية لهذه المعلومات وضمان أمنها وسلامتها من هذا التبديل والتزوير.

---

[1] نفس المرجع، ص 58.

[2] فوزية عبد الستار، قانون العقوبات –القسم الخاص– دار النهضة العربية، القاهرة، 1990، ص817.

[3] غانم مرضي الشمري، نفس المرجع السابق، ص 59.

يمكن التأكيد على أن التشريعات القانونية هي الضمانة الأبرز لحماية هذه المعلومات فبالاطلاع على أغلب التشريعات العربية نجد إنّها بالرغم من بسطها الحماية القانونية للمحررات والمعلومات المتجسدة فيها من كل تزوير أو تبديل إلا إنّ هذه التشريعات تتباين فيما بينها، فإذا كانت بعض التشريعات قد أوردت تعريفا للتزوير في نصوصها كالقانون العقوبات الفلسطيني رقم 74 لعام 1936 مثلا الذي نص في المادة (332) على تعريف التزوير بإنّه تحريف معدل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطط يحتج بهما نجم أو يمكن إنّ ينجم عنه ضرر مادي أو معنوي أو اجتماعي، و غيرها من القوانين إلا أنه هناك تشريعات أخرى لم تورد تعريفا للتزوير كالقانون الجزائري والمصري فإنّها تبقي الباب مفتوحة لدخول أنماط مستحدثة من الأفعال التي قد تعد تزوير بخلاف الاتجاه الأول الذي يعتبر مقيدا[1].

ويمكننا القول إنّ جريمة التزوير الإلكتروني يمكن إنّ تشمل تزوير البريد الإلكتروني الخاص بفرد أو مؤسسة معينة أو تزوير للوثائق والسجلات وأيضا تشمل تزوير الهوية.

خامسا: جرائم المقامرة والجرائم الأخرى ضد الأخلاق والآداب وجرائم الحاسوب ضد الحكومة:

تشمل جرائم المقامرة والجرائم الأخرى ضد الأخلاق والآداب جريمة تملك وإدارة مشروع مقامرة على الإنترنت وتسهيل إدارة مشاريع القمار على الإنترنت وتشجيع المقامرة عبر الإنترنت لترويج الكحول ومواد الإدمان للقصر، وتشمل جرائم الحاسوب ضد الحكومة كافة جرائم تعطيل الأعمال الحكومية وتنفيذ القانون والإخفاق في الإبلاغ عن جرائم الكمبيوتر والحصول على معلومات سرية والأخبار الخاطئ عن جرائم الحاسوب والعبث بالأدلة القضائية أو التأثير فيها وتهديد السلامة العامة وبث البيانات من مصادر مجهولةكما تشمل الإرهاب الإلكتروني[2].

المطلب الثالث: المجرم والمجني عليه في الجرائم المعلوماتية

يُطلق مصطلح "المجرم المعلوماتي" على الشخص الذي يُعد الفاعل الأساسي في ارتكاب الجريمة الإلكترونية وهو غالبًا ما يتمتع بمستوى عالٍ من الذكاء والمعرفة التقنية، اكتسبها من خلال التعلم والتجربة العملية في بيئة الإنترنت، وتختلف هذه الجرائم عن نظيرتها التقليدية من حيث الطبيعة والوسائل، فهي لا تُرتكب في الواقع المادي ولا تُستخدم فيها أدوات ملموسة، كما لا تترك آثارًا مرئية كالدماء أو الإصابات الجسدية بل تُنفذ ضمن فضاء رقمي باستخدام تقنيات متقدمة مرتبطة بشبكة الإنترنت، مما يجعلها جرائم عابرة للحدود. ويتسم مرتكبوها بصفات غير مألوفة في المجرمين التقليديين، كالمهارة العالية، والمعرفة التقنية والتحكم في الوسائل، بالإضافة إلى دافع قوي يوجه سلوكهم الإجرامي، وهو ما جعل بعض الفقه يصفهم بـ «المجرمين ذوي المهارة والمعرفة والسلطة والدافع »

[1] محمد عقاد، جريمة التزوير في المحررات للحاسب الآلي، دراسة مقارنة، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي،1993، ص 394.

[2] يوسف المصري، المرجع السابق، ص33.

تأسيسا على ما سبق، فإنّ المجرم المعلوماتي يتصف بخصائص معينة تميزه عن المجرم الذي يرتكب الجرائم التقليدية، فإذا كانت الجرائم التقليدية لا تتطلب مستوى علمي معرفي للمجرم في عملية ارتكابها فإنّ الأمر يختلف بالنسبة للجرائم الإلكترونية، فهي جرائم فنية تقنية في الغالب.

أمّا "المجني عليه المعلوماتي" فشكّل محورًا أساسيًا لفهم وتطبيق العدالة في قضايا الجرائم الإلكترونية، لذا فإنّ تطوير الإطار القانوني، والتقني، والاجتماعي لحمايته، أصبح ضرورة ملحة في ظل التوسع الكبير في استخدام الفضاء الرقمي. كما إنّ رفع الوعي وتوفير آليات دعم فعالة للمجني عليهم سيساهم في تحقيق الردع وحماية الحقوق في العصر الرقمي. وعلى هذا سوف ندرس من خلال هذا المطلب من هو المجرم المعلوماتي، سماته وطائفه وفي الفرع الأخير نعرف من هو المجني عليه المعلوماتي.

الفرع الأول: التعريف بالمجرم المعلوماتي

من الناحية الجنائية تعني تسمية "المجرم المعلوماتي" ذلك الشخص الذي يمتلك مهارات تقنية أو دراية بالتكتيك المستخدم في نظام الحاسوب الإلكتروني، والقادر على استخدام هذا التكتيك لاختراق الرقم السري لتغيير المعلومات، أو تقليد البرامج أو التحويل من الحسابات عن طريق استخدام الحاسوب نفسه، أمّا خبراء الحاسوب والإنترنت، بل وحتى العديد من كتاب القانون في هذا المجال، ذهبوا إلى أن المجرم المعلوماتي يظهر بأحد الصورتين، الأولى هي « Hackers » هم من يتحدون إجراءات أمن النظم والشبكات دون إنّ تتوافر لديهم في الغالب دوافع حاقدة أو تخريبية، إنّما ينطلقون ثبات المقدرة.

أمّا الثانية فهي الـ « Cracker »، وهم ممن تعكس اعتداءاتهم ميولا إجرامية خطرة، وهذا المعيار تعتمد عليه التشريعات الأمريكية في التمييز بين النوعين من المجرمين، فيما يميل البعض إلى تسمية المجرم المعلوماتي بـ "المجرم الإلكتروني الرقمي"، ويعرف بإنّه "من لديه القدرة على تحويل لغته إلى لغة رقمية وتخزينها واسترجاعها باستخدام الحاسوب الإلكتروني أو الرقمي وملحقاته ووسائل الاتصال الرقمية، وذلك بأداء فعل أو امتناع عنه، مما يحدث اضطرابات في المجتمع الدولي أو المحلي نتيجة مخالفة قواعد الضبط الاجتماعي محليا أو دوليا."

ويمكن القول أنّ صورة " الإجرام المعلوماتي" أو "المجرم المعلوماتي" باتت غير واضحة بين من يرى إنّ المجرم المعلوماتي ينتمي إلى "طائفة المجرمين بطبيعتهم" أو ما يسمون بـ "المجرمين ذوي الياقات الزرقاء" وبين من يرى أنهم ينتمون إلى طائفة "الإجرام المكتسب"، أو ما يسمون بـ "المجرمين ذوي الياقات البيضاء"[1].

على العموم فإنّ تسمية "الهاكرز" تعود إلى ستينيات القرن الماضي، حيث أطلقت على الشخص الذي لديه قدرات متميزة في مجال الحاسوب، مستغل برامجه أقصى استغال، وفي بداية السبعينيات تمكن شخصان من ولاية كاليفورنيا من فك رموز الشفرة الخاصة بالاتصالات الهاتفية، متمكنا من اختراق نظام الهواتف من دون

[1] مصطلح المجرمون ذو الياقات البيضاء مصطلح متداول في ميدان علم الاجتماع أول من استخدمه الأستاذ "سندرلاند"، دلالة على أولئك المجرمين الذين تظهر عليهم عوامل الإجرام لتمتعهم بمناصب إدارية أو مكانة اجتماعية، حيث يرتكبون هذه الجرائم وهم جالسون في أمّاكنهم ومكاتبهم الراقية دون أن تتلوث أيديهم فعليا بها، ومن أشهر جرائم ذوي الياقات البيضاء جريمة غسيل الأموال وجرائم التزوير والاحتيال وتجارة الرقيق الأبيض، ص29.

دفع رسوم "فواتير" المكالمات، وفي مطلع الثمانينات تمت أول عملية اعتقال للهاكرز حيث قامت الشرطة الفدرالية في مدينة "ملوكي" بضبط مجموعة كبيرة من الهاكرز، قاموا باختراق ستين موقعا في مختلف أنحاء الواليات المتحدة، ثم صدر بعد ذلك قانون "السيطرة على الجريمة المتكاملة"، والذي أتاح للشرطة الأمريكية القبض على منفذي عمليات الاحتيال المتعلقة بالبطاقات الائتمانية و الكمبيوتر.

أمّا في أواخر الثمانيات فقد صدر قانون جديد في الواليات المتحدة عرف بـ "قانون الاحتيال بالكمبيوتر وسوء الاستخدام"، و الذي زاد من سلطات الشرطة الفيدرالية قياسا بالقانون الأول، غير أنها هجمات الهاكرز باتت تتزايد مع تزايد المواقع الإلكترونية. ففي عام 1999 شهدت الواليات المتحدة خمسة ألاف حالة اختراق وفي عام 2000 بلغت هذه الحالات سبعة عشر ألف، علما إنّ هذه الحالات هي المسجلة فقط، أمّا حصيلة الأضرار الناجمة عن هذه الجرائم والتي أعلنت عنها الواليات المتحدة عام 2000 بلغت (1.5 تريليون دولار)، جديرا بالذكر إنّ صورة "الهاكرز" لم تظهر بشكل واضح في مطلع ستينيات القرن الماضي، ذلك بسبب كبر حجم الحاسبات الآلية آنذاك، فضال، و وجود الحراسات عليها، إضافة إلى وجودها في غرف ذات درجات حرارة معينة، مما يحول بين هؤلاء المجرمين وبين الوصول إليها.

مع ذلك فإنّ "درينيسريتشي "و"كيننومبسون " يعدان من أوائل وأشهر الهاكرز آنذاك لتصميمهما عام 1969 برنامج سمي الـ"**يونكس**" والذي يعد الأسرع في ذلك الوقت غير إنّ المدة الزمنية المنحصرة بين 1980 1989 تعد الفترة الذهبية للهاكرز بسبب تصميم الحاسب الإلكتروني IBM، وأصبح الحاسب صغير الحجم وسهل النقل.

ويمكن استخدامه في أي مكان أو زمان ولهذا بدأ الهاكرز في هذه الحقبة بالعمل الحقيقي على الاختراق والتخريب[1]، لهذا ظهرت مجموعات الهاكرز التي كانت تقوم بتخريب أجهزة المؤسسات التجارية، أمّا الفترة الممتدة بين الأعوام 1990 و 1994 فقد كانت البدايات الأولى لحرب الهاكرز، حيث أنشأ شخص يدعى" ليكس لوثر" مجموعة أطلق عليها اسم LOD وهي عبارة عن مجموعة من الهاكرز الهواة يقومون باختراق أجهزة الآخرين والقرصنة، وكانت تلك المجموعة هي الأذكى بين مجموعات الهاكرز حتى ظهرت مجموعة أخرى تسمى MOD بقيادة شخص يدعى "فيبر"، وهي مجموعة منافسة للمجموعة الأولى، ومع بداية عام 1990 بدأت المجموعتان بحرب كبيرة أطلق عليها "حرب الهاكرز"، استمرت ما يقارب الأربع سنوات، وكان كل طرف في هذه الحرب يحاول اختراق أجهزة وأنظمة الطرف الآخر حتى انتهت بالقبض على "فيبر" رئيس مجموعة MOD، ولكن حرب الهاكرز ومجموعاته لم تنته اليوم[2].

الفرع الثاني: سمات وطوائف المجرم المعلوماتي

لم يكن لارتباط الجريمة المعلوماتية بالحاسب الآلي أثره على تميز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية فحسب، وإنما كان له أثره أيضا على تمييز المجرم المعلوماتي عن غيره من المجرمين.

[1] عمار عباس الحسني، المرجع السابق، ص ص 58، 59.

[2] عمار عباس الحسني، المرجع السابق، ص 60

واختلف الباحثون في تحديد هذه السمات، ويعد الأستاذ Parker واحدا من أهم الباحثين الذين عنوا الجريمة المعلوماتية بالدراسة بصفة عامة وبالمجرم المعلوماتي بصفة خاصة، ومع ذلك يعد المجرم المعلوماتي مجرما لارتكابه فعل إجرامي يتطلب توقيع العقاب عليه، وكل ما في الأمر أنه ينتمي إلى طائفة خاصة من المجرمين تقترب في سماتها من جرائم ذوي الياقات البيضاء، وإن كانت في رأيه لا تتطابق معها[1].

فالمجرم المعلوماتي من ناحية ينتمي في أكثر الحالات إلى وسط اجتماعي متميز كما أنه يكون على درجة من العلم والمعرفة[2].

يتفق مجرمو المعلوماتية مع ذوي الياقات البيضاء في كون إنّ الفاعل في الحالتين بيور جريمته كونه لا ينظر إلى سلوكه باعتباره جريمة أو فعل يتناقل مع الأخلاق.

ويتميز المجرم المعلوماتي بالإضافة إلى ذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المحرمين ويرمز إليها الأستاذ Parker بكلمة S.K.R.A.M وهي تعني المهارة Skills، المعرفة Knowledge الوسيلة Ressources، السلطة Anthority، وأخيرا الباعث Motive[3].

تعد المهارة المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المحرم المعلوماتي، والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات، أو بمجرد التفاعل الاجتماعي مع الآخرين.

إلا أن ذلك لا يعني ضرورة إنّ يكون المحرم المعلوماتي على قدر كبير من العلم في هذا المحال بل إنّ الواقع العملي قد أثبت إنّ بعض أنجح محرمي المعلوماتية لم يتلقوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال.

أمّا المعرفة: فتتلخص في التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها بكامل ملابساتها ومدى إمكانية نجاحها أو فشلها، إذ إنّ المحرم المعلوماتي باستطاعته أن يكون تصورا كاملا الجريمة كون مسرح الجريمة المعلوماتية هو النظام المعلوماتي، فالفاعل يستطيع أنّ يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته[4].

أمّا الوسيلة: فيراد بها الإمكانيات التي يتزود بها الفاعل الارتكاب جريمته ففيما يتعلق بالمحرم المعلوماتي فإن الوسائل المتطلبة التلاعب بأنظمة الحاسبات الآلية في أغلب الحالات تتميز نبيها بالبساطة وبسهولة الحصول عليها كما أنه نظرا المهارته وقدرته يستطيع حتى ابتكارها، إذ أنّ الواقع أثبت أنه كلما كان النظام المعلوماتي غير مألوف ويتميز بالخصوصية كانت الوسائل المنطقة. لارتكاب الجريمة أكثر صعوبة.

---

[1] ناطقة عادل محمد فريد قورة، المرجع السابق، ص 54.

[2] ليس من الضروري أن ينتمي إلى مهنة وتكتب من خلالها الفعل الإجرامي كما هو الحال في حراكم قوي الياقات البيضاء ص31، أنظر: Suthreland (Eduin H) « White collar criminality » Gers (Gilbert) in white collar criminal the offender in business the professions atherton press 1968

[3] Parker (Doun B3) Figding computer crime A new Framework for protecting information 1998/ p 114.

[4] ناطقة عادل محمد فريد قورة، المرجع السابق، ص 54

أمّا السلطة: فيقصد بها الحقوق أو المزايا التي يتمتع بها المحرم المعلوماتي والتي تمكنه من ارتكاب جريمته، وهذه السلطة أمّا تكون مباشرة كالشفرة الخاصة بالدخول إلى النظام المعلوماتي التي تعطي للمفاعل مزايا متعددة مثل فتح الملفات و محو أو تعديل محتوياتها أو مجرد قراءها أو كتابتها[1].

وقد تتمثل هذه السلطة في حق استعمال الحاسب الآلي نفسه أو الدخول إلى مكان تواجده كما هو الحال في الشبكات الداخلية بعض الإدارات مثلا؛ قد تكون هذه السلطة غير مباشرة كما في حالة استخدام شفرة الدخول الخاصة بشخص آخر.

أخيرا يأتي الباعث لارتكاب الجريمة، الذي قد لا تختلف في كثير من الأحيان عن الباعث الارتكاب غيرها من الجرائم الأخرى والرغبة في تحقيق الربح المادي بطريق غير مشروع يظل الباعث الأول وراء ارتكاب الجريمة المعلوماتية، ثم يأتي بعد ذلك مجرد الرغبة في قهر نظام الحاسب وتخطي حواجز الحماية المضروبة حوله، وأخيرا الانتقام من رب العمل أو أحد الزملاء.

يفرق مرتكبي هذه الجرائم بين الإضرار بالأشخاص الأمر الذي يعدونه غاية لا أخلاقية، وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم، وهو ما يطلق عليه أعراض روبن هود The Roben Hood Syndrome.[2]

الفرع الثالث: المجني عليه المعلوماتي

يُعد المجني عليه في الجريمة الإلكترونية هو الطرف الذي يتعرض لاعتداءات غير مشروعة تمس مكونات النظام المعلوماتي. وقد يكون هذا الطرف شخصًا طبيعيًا، أو شركة، أو مؤسسة تعمل في مجال الحوسبة ضمن إطار أنشطتها التجارية أو الاقتصادية أو السياسية، حيث تعتمد هذه الكيانات على الحاسوب كأداة أساسية في إدارة أعمالها. وتشير تقديرات بعض خبراء صندوق النقد الدولي إلى صعوبة تحديد نطاق الجرائم الإلكترونية بدقة، نظرًا لأن العديد من الضحايا لا يكتشفون تعرضهم للاعتداء إلا عندما تصبح أنظمتهم المعلوماتية هدفًا للهجوم. وحتى في حال علمهم بالجريمة، فإن كثيرًا منهم يفضلون التزام الصمت وعدم الإبلاغ، لما قد يسببه ذلك من ضرر لسمعتهم أو مكانتهم المؤسسية.

والجدير بالذكر أن سلبية المجني عليهم أو ضحايا الجريمة الإلكترونية، وخوفهم من الإبلاغ حفاظا على سمعتهم التجارية ومكانتهم المرموقة، غير معين على التمادي في اقتراف مثل هذه الجرائم، توجد هذه الجرائم بصفة خاصة إلى البنوك، وإلى المواقع الإلكترونية للمؤسسات المالية، لأن القطاعات المستهدفة من الجريمة

[1] ويرى البعض أن أغلب مجرمي المعلوماتية ليس لديهم أطماع مادية بقدر ما يحاولون حل مشكلات مادية تواجههم لا يستطيعون حلها باللجوء إلى الجرائم الأخرى أنظر، Parker (DonnB)، OP-cit، p 142

[2] أنظر الدكتور هشام محمد فريد رستم، المرجع السابق، ص 38.

الإلكترونية هي تعتمد أكثر من غيرها على أجهزة الحاسوب، وتعتبر البنوك من أهم تلك القطاعات وأكثرها تضررا[1].

وتُعد الحماية القانونية للمجني عليه المعلوماتي أحد أركان مكافحة الجريمة السيبرانية، ولا تقل أهمية عن ملاحقة الجناة أنفسهم، ويتطلب تحقيق هذه الحماية تطويرًا مستمرًا للتشريعات الوطنية، وتعزيز التعاون الدولي، إلى جانب نشر الوعي الرقمي وتوفير آليات إنصاف فعالة تواكب تطور التهديدات المعلوماتية الحديثة؛ فمثلا على الصعيد الدولي:

– اتفاقية بودابست لمكافحة الجرائم السيبرانية: (2001) أول اتفاقية دولية تهدف إلى توحيد الجهود في هذا المجال.

– تعاون الإنتربول والمنظمات الدولية لملاحقة الجرائم العابرة للحدود.

المبحث الثاني: التعاون الأمني الدولي لمكافحة الجرائم المعلوماتية

إن الانتشار الواسع والمتسارع لتقنيات المعلومات، لا سيما الحواسيب وشبكات الاتصال، وتزايد الاعتماد عليها في مختلف جوانب الحياة، أدى إلى وقوع هذه التقنيات في أيدي بعض الأفراد الذين استغلوها في ارتكاب جرائم، مما أدى إلى بروز ما يعرف بالجريمة المعلوماتية. ونظرًا لخطورة هذه الجرائم واتساع رقعتها على المستوى الدولي، حظيت باهتمام عالمي متزايد.

وقد كشفت هذه الظاهرة عن وجود قصور في التشريعات الوطنية لمواجهتها، الأمر الذي استدعى ضرورة وجود تعاون دولي في مجالات متعددة للتصدي لها، انطلاقًا من ذلك، سنعرض في هذا المبحث أبرز مجالات التعاون الدولي في مكافحة الجرائم المعلوماتية، حيث سنتناول في المطلب الأول مفهوم التعاون الأمني الدولي، وفي المطلب الثاني صور التعاون الأمني الدولي في هذا المجال، بينما يتناول المطلب الثالث دور المنظمة الدولية للشرطة الجنائية (الإنتربول) في جهود مكافحة الجرائم المعلوماتية.

المطلب الأول: مفهوم التعاون الأمني الدولي في مجال الجريمة المعلوماتية

أولا: مفهوم التعاون الدولي

التعاون بمفهومه العام، يعني العون المتبادل لتحقيق هدف معين، فغالبا ما يستعين الأفراد بالآخرين من أجل قضاء حوائجهم لأن الإنسان بطبعه لا يستطيع العيش بمفرده، فمصطلح "التعاون" في اللغة هو تقديم العون والمساعدة وتكوين جماعات للقيام بعمل مشترك في مصلحة الأعضاء دون وسيط يقال تعاون القوم أي عاون بعضهم بعضا واستعان فلان فلانا وبه أي طلب منه العون، أمّا مصطلح "الدولي" فيستخدم بوصف حاجة حقيقية لتعريف العلاقات الرسمية بين الدول، كما يوجد اختلاف في مفهوم التعاون الدولي بصفة عامة في الاصطلاح عن المدلول اللغوي لمصطلح التعاون حيث تطورت غالبية المحاولات الفقهية لتعريف التعاون

[1] عبد الفتاح البيومي حجازي، مكافحة جرائم الأنترنت، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2006، ص ص 96، 97.

الدولي بصفة عامة حول محور أساسي تتمثل في تبادل العون والمساعدة بين الدول لتحقيق المنفعة العامة المشتركة لهذه الدول[1].

مصطلح التعاون الدولي لمكافحة الجريمة يعد من المفاهيم التي يصعب وضع تعريف جامع مانع لها ويرجع ذلك لعدة أسباب منها اتساع المجال والصور والأشكال التي يمكن أنّ يتخذها هذا التعاون، وعدم إمكان حصرها أو حصر الوسائل الجديدة والمتجددة التي تجعل هذا التعاون ظاهرة متغير و متطورة بشكل مستمر كذلك ارتباط هذا التعاون بمفاهيم الجريمة والإجرام ومكافحة الجريمة وهي مفاهيم يصعب معها وضع تصور محدد وإطار ثابت لأي منها[2].

ثانيا: تعريف التعاون الأمني الدولي

التعاون الأمني الدولي لا يقتصر على إجراءات ملاحقة الأشخاص المطلوبين للعدالة وحسب، بل يتعدى الأمر ذلك ليشمل مكافحة الجريمة بشقيها الوقائي والقمعي، بل يشمل العناية بحقوق المتهمين والضحايا ومراعاة حقوق الدول وسيادتها، ويعرف التعاون الأمني الدولي بأنه "تبادل العون والمساعدة وتظافر الجهود المشتركة بين طرفين دوليين أو أكثر لتحقيق نفع أو خدمة أو مصلحة مشتركة في مجال تصدي بمخاطر الإجرام وما يرتبط به من مجالات أخرى مثل مجال العدالة الاجتماعية، ومجال الأمن، أو لتخطي مشكلات الحدود والسيادة التي قد تعترض الجهود الوطنية لملاحقه المجرمين وتعقب مصادر التهديد، سواء كانت مساعدة متبادلة قانونيه او قضائية أو شرطية؛ وسواء اقتصرت على دولتين فقط او امتدت إقليميا أو عالميا"[3].

يعد التعاون الدولي الأمني أهم صور التعاون الدولي في مكافحة الجريمة بصفة عامة والجرائم الإلكترونية على وجه الخصوص وفي هذا الصدد تقوم المنظمة الدولية للشرطة الجنائية الإنتربول بدور أساسي في ترسيخ دعائم هذا التعاون.

الفرع الأول: ضرورة التعاون الأمني الدولي في مجال مكافحة الجريمة المعلوماتية

يمثل التعاون الأمني الدولي بين أجهزة الشرطة الجنائية المتخصصة لمكافحة الجرائم المعلوماتية في الدول أحد الوسائل الهامة التي يمكن من خلالها منع هذه الجرائم والإقلال منها، وتؤكد التحقيقات في الجرائم عامة والإلكترونية خاصة على أهمية التعاون الأمني الدولي، حيث يستحيل على دولة بمفردها القضاء على هذه الجرائم الدولية العابرة للحدود، لأنّ جهاز الأمن في هذه الدولة أو غيرها لا يمكنه تعقب المجرمين وملاحقتهم إلا في حدود الدولة التابعة لها[4].

[1] عادل يحي، السياسية الجنائية في مواجهة الجريمة المعلوماتية، ط 1، دار النهضة العربية، القاهر، 2014، ص 92.

[2] علاء الدين شحاتة، التعاون الدولي لمكافحة الجريمة، القاهرة، 2020، ص ص 18، 19.

[3] خالد بن مبارك القحطاني، التعاون الأمني الدولي في مواجهة الجريمة المعلوماتية عبر الوطنية، أطروحة داكتورة، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، دار النهضة العربية الرياض، 2006، ص 38.

[4] جميل عبد الباقي الصغير، الجوانب الإجرائية المتعلقة بالانترنت، دار النهضة العربية، القاهرة، 2001، ص 72.

يعد التعاون الدولي في مجال حماية شبكات المعلومات وتوحيد وتنسيق الجهود لفرض الرقابة الكافية على ما يقدم من خلال هذه الشبكة، وتقوية حماية المواقع الهامة وسد ثغراتها وتوفير التقنيات اللازمة لمواجهتها وتعزيز التعاون بين المجتمع الدولي وذلك من خلال إبرام اتفاقيات دولية في مجال حماية شبكات الانترنت خاصة وأنّ الجرائم المعلوماتية تعد جرائم دولية عابرة للحدود الوطنية، ونظراً لأن معظم الأنظمة القانونية خالية من قانون خاص بمكافحة الجريمة المعلوماتية الرقمية، فتحتم علينا الاستعانة بالقانون المقارن والاتفاقات الدولية لمواجهة تلك الجرائم المعلوماتية[1].

فقد ظهرت العديد من الأجهزة في هذا المجال منها: المنظمة الدولية للشرطة الجنائية "الإنتربول"، مركز الشرطة الأوروبية أو "الأوروبول"، الأورجست، شنجن، المكتب العربي للشرطة الجنائية[2]، أمّا التعاون الإداري فيكون من خلال التعاون على صعيد الإجراءات والأوامر والقرارات التي تتم من أجل المحافظة على النظام العام في المجتمعات الأطراف في المعاهدات والاتفاقيات[3].

الفرع الثاني: أسس التعاون الأمني الدولي لمكافحة الجرائم المعلوماتية

نظرًا للطبيعة الخاصة والمعقدة للجرائم المعلوماتية، ينبغي أنّ يستند التعاون الدولي في مكافحتها إلى مجموعة من الأسس المحددة، وهي على النحو التالي:

أولا: الاعتماد على الدراسة العلمية لفهم ظاهرة الجرائم المعلوماتية بعمق، إلى جانب توفير بيانات إحصائية دقيقة تتعلق بهذه الجرائم، ومرتكبيها، وآليات عمل النظام القضائي الجنائي، لما لهذه المعلومات من دور فعّال في تعزيز جهود المكافحة.

ثانيا: تحديد آليات التعاون في مجالات التدريب الأمني، والعمل على تحقيق التكامل بين أجهزة الشرطة على المستوى الدولي لضمان تنسيق الجهود وتوحيدها في مواجهة هذه الجرائم.

ثالثا: إعداد مشروع اتفاقية دولية تتضمن قانونًا موحدًا لمواجهة الجرائم المعلوماتية، بما يضمن انسجام التشريعات بين الدول ويسهل التعاون القضائي والأمني.

رابعا: وضع استراتيجيات وقائية واحترازية تخلق بيئة مناسبة للقضاء على أنشطة المنظمات الإجرامية مع تعزيز وعي المجتمع من خلال نشر المعلومات الضرورية حول هذه الجرائم ومرتكبيها.

خامسا: تعزيز التنسيق بين المؤسسات الأمنية بمختلف آلياتها على المستويين الإقليمي والدولي من أجل رصد معدلات الجريمة والحد من انتشارها، وسد أي فجوات معلوماتية من خلال تبادل البيانات مما يساعد على كشف أبعاد الجرائم وخطط تنفيذها، وتحديد الثغرات الأمنية والعمل على معالجتها، كما يسهم هذا التنسيق في

[1] فهد عبد الله العبيد العازمي، "الإجراءات الجنائية المعلوماتية"، كلية الحقوق، جامعة عين شمس، دار الجامعة الجديدة 2016، ص 211.

[2] عبد الله سيف المكتوب، المرجع السابق، ص ص، 220، 221

[3] عبد الله سيف المكتوب، المرجع السابق، ص ص، 222، 223.

الاطلاع على تجارب الدول الأخرى وتبادل الخبرات والبحوث ذات الصلة مما يساهم في التعرف على الأساليب الإجرامية المستحدثة وأنماط المجرمين، ويوسع نطاق المعرفة المتعلقة بالجريمة المعلوماتية[1].

المطلب الثاني: صور التعاون الأمني الدولي لمكافحة الجرائم المعلوماتية

أولا: ربط شبكات الاتصال والمعلومات

تحتاج الاتصالات الشرطية إلى وسائل الاتصال تحقق السرعة الملائمة لتتمكن أجهزة العدالة الجنائية من التواصل بين سلطات التحقيق والملاحقة المختلفة، لذا عمدت الدول والمنظمات الدولية تطوير الاتصال وتبادل المعلومات فيما بينها.

ثانيا: القيام ببعض العمليات الشرطية والأمنية المشتركة

تعقب المجرم المعلوماتي وتعقب الأدلة الرقمية وضبطها، والقيام بعملية التفتيش العابر للحدود المكونات الحاسب الآلي والأنظمة المعلوماتية وشبكات الاتصال بحثا عما قد تحويه من أدلة وبراهين على ارتكاب الجريمة المعلوماتية، كلها أمور تستدعي القيام ببعض العمليات الشرطية والأمنية المشتركة، واشتراك الدول فيما بينها للقيام بعمليات شرطية وأمنية يؤدي إلى صقل مهارات وخبرات القائمين على مكافحة تلك الجرائم وبالتالي وضع حد لها[2].

ثالثا: تبادل المعاونة لمواجهة الكوارث والأزمات والمواقف الحرجة

تتعرض كافة دول العالم لاحتمالات وقوع كوارث ضخمة وأحداث جسيمة وبشكل لا يمكن توقعه أو يستحيل التنبؤ بتوقيت حدوثه أو يصعب معه مواجهته بالإمكانيات القومية للدولة المنكوبة بمفردها هذه الكوارث أو الأزمات غالبا ما يكون عنصر الوقت من الأمور الحاسمة في المواجهة الأمر الذي يحتاج إلى تكثيف خاص للجهود والخبرات والإمكانيات بشكل يصعب تحقيقه إلا بتضافر الجهود ولذلك لا بد من التعاون بين الدول[3].

الفرع الأول: ربط شبكات الاتصال والمعلومات

أولا: تعريف ربط الشبكات وأهميته

يشير مفهوم ربط شبكات الاتصال والمعلومات إلى عملية توصيل مجموعة من الحواسيب، والخوادم والأجهزة الذكية المختلفة ضمن شبكة واحدة، أو عبر شبكات متعددة، بهدف تسهيل تبادل البيانات والمعلومات وتوفير موارد تقنية مشتركة. وتكمن أهمية هذا الربط في كونه أحد الأعمدة الأساسية للبنية التحتية الرقمية في

[1] هدى حامد قشقوش، الجريمة المنظمة القواعد الموضوعية والإجرائية والتعاون الدولي، دار النهضة العربية، القاهرة، 2002 ص 83.

[2] أمينة سلام، "مكافحة الجريمة المعلوماتية في إطار القانون الدولي"، مذكرة لنيل شهادة ماستر، كلية الحقوق و العلوم السياسية، جامعة محمد خيضر، بسكرة، 2020، ص 26.

[3] مذكرة مكافحة الجريمة ص 30.

المؤسسات، حيث يتيح تحسين الإنتاجية، وتيسير سير العمل، وتسريع الوصول إلى المعلومات، فضلاً عن تعزيز القدرة على اتخاذ القرار المبني على بيانات لحظية.

يُعد هذا الربط أحد المتطلبات الجوهرية للتحول الرقمي، إذ لا يمكن تحقيق فاعلية أنظمة المعلومات ولا التطبيقات السحابية دون وجود شبكات اتصال قوية وموثوقة، كما أنه يمثل قاعدة الانطلاق نحو تطبيق مفاهيم حديثة مثل المدن الذكية، والحكومة الإلكترونية، والتعليم عن بُعد، والرعاية الصحية الذكية[1].

يقصد بربط شبكات الاتصال والمعلومات دمج مجموعة من الحواسيب والأجهزة الرقمية الأخرى ضمن منظومة واحدة تسمح بتبادل البيانات والموارد والمعلومات بسرعة وكفاءة عالية، سواء داخل المؤسسة نفسها أو بينها وبين مؤسسات أخرى.

ثانيا: مكونات البنية التحتية لربط الشبكات

تتطلب عملية ربط شبكات الاتصال والمعلومات بنية تحتية تقنية متكاملة، تتضمن العناصر التالية:

- الأجهزة المادية :(Hardware) مثل أجهزة التوجيه(Routers) ، والمبدلات(Switches) ، ونقاط الوصول اللاسلكي(Access Points) ، وكابلات الألياف البصرية، وخوادم التخزين.
- البرمجيات :(Software) وتشمل أنظمة تشغيل الشبكات، وبرمجيات إدارة الشبكة (مثل Cisco Network Assistant)، وأنظمة الأمن والحماية مثل الجدران النارية وأنظمة كشف التسلل.
- البروتوكولات :وهي القواعد التي تنظم عمليات الاتصال وتبادل البيانات، وأشهرها بروتوكول TCP/IP، وبروتوكولات التوجيه مثل OSPF و BGP
- البنية السحابية والافتراضية: حيث أصبح الاعتماد على خدمات الحوسبة السحابية أحد أسس ربط الشبكات الحديثة، ما يسمح باستخدام موارد موزعة جغرافيًا بشكل موحد وفعال[2].

أ- أنواع الشبكات المستخدمة في الربط

تنقسم شبكات الاتصال حسب نطاقها الجغرافي واستخدامها إلى:

- الشبكة المحلية :(LAN) وتربط أجهزة داخل نطاق جغرافي صغير كالمكتب أو المدرسة.
- الشبكة الواسعة :(WAN) تمتد عبر مساحات كبيرة، مثل شبكات المؤسسات الحكومية أو الربط بين فروع البنوك.
- شبكة الإنترنت :وهي أكبر شبكة عامة، وتُعد مثالًا على الربط بين ملايين الشبكات المحلية والعالمية.

[1] محمد عبد العال، "شبكات الحاسوب: المفاهيم الأساسية والتطبيقات العملية"، دار الفكر العربي، القاهرة، 2019. ص 76

[2] أحمد سعيد، أساسيات الشبكات والاتصالات، مكتبة الأنجلو المصرية، القاهرة، 2021. ص 54

- الشبكات الافتراضية :(VPN) وهي شبكات تتيح الاتصال الآمن عبر الإنترنت، وتستخدم بكثرة في ربط المؤسسات المتفرعة جغرافيًا[1].

ب- **فوائد ربط الشبكات في المؤسسات**

تُحقق عملية الربط فوائد إستراتيجية تشمل:

- توفير الموارد :عبر مشاركة الطابعات، قواعد البيانات، ووسائط التخزين.
- رفع الكفاءة :إذ يتم تقليص الزمن اللازم لإنجاز المعاملات، وزيادة موثوقية الخدمات المقدمة.
- تعزيز أمن البيانات :عبر إنشاء نقاط مراقبة مركزية، وأنظمة نسخ احتياطي منتظمة.
- تمكين الإدارة المركزية :إذ يمكن للإدارة العليا متابعة وتنسيق الأنشطة بشكل لحظي.
- دعم العمل التشاركي: من خلال تمكين الفرق المختلفة من التعاون على نفس البيانات والمشاريع[2].

ج- التحديات المرتبطة بربط الشبكات

رغم المزايا الكبيرة، إلا أن عملية الربط تواجه تحديات أبرزها:

- أمن الشبكة :فكلما زادت نقاط الاتصال زادت معها احتمالات الاختراق.
- ارتفاع تكاليف التأسيس والصيانة :خاصة في المؤسسات الكبيرة والمتوزعة جغرافيًا.
- الحاجة إلى كفاءات بشرية :تتطلب شبكات الاتصال الحديثة مهندسين وتقنيين ذوي خبرة في إدارة الشبكات وتأمينها.
- مشاكل التوافقية :قد تحدث عند ربط أنظمة تشغيل أو أجهزة من علامات تجارية مختلفة[3].

د- **استخدامات ربط الشبكات في القطاعات المختلفة**

- القطاع التعليمي: مثل الجامعات التي تربط بين أقسامها ومكتباتها الرقمية وأنظمة التعليم الإلكتروني.
- القطاع الصحي :حيث يتم ربط المستشفيات ومراكز الأشعة والمختبرات لتبادل سجلات المرضى.
- القطاع الحكومي: من خلال ربط الإدارات في إطار الحكومة الإلكترونية وتسهيل المعاملات الإدارية.
- القطاع الأمني والعسكري: لربط مراكز القيادة والتحكم وتبادل المعلومات الاستخباراتية في الزمن الحقيق[4]

---

1 عبد الرحمن عطا، الشبكات الحاسوبية وتقنيات الاتصال الحديثة، دار صفاء للنشر والتوزيع، عمّان، 2020، **ص 68 .**

2 يوسف محمود، المجلد15، "دور شبكات الاتصال في تطوير المؤسسات الحديثة"، **ع 2، مجلة العلوم والتقنية**، جامعة الملك سعود ، القاهرة ، 2022. **ص 93.**

3 سامي الزهراني، الأمن السيبراني وشبكات المعلومات، مكتبة جرير، الرياض، 2022، ص38.

4 عبد الله أبو السعود، مقدمة في البنية التحتية الرقمية، دار الراية للنشر، عمّان، 2021، ص28.

الفرع الثاني: القيام ببعض العمليات الشرطية والأمنية المشتركة

إنّ تزايد التهديدات الأمنية وتطور أساليب الجريمة، خصوصًا الجرائم المنظمة والعابرة للحدود، فرض على الدول تجاوز المقاربات الأمنية التقليدية، والانخراط في عمليات شرطية وأمنية مشتركة. وتُعتبر هذه العمليات إحدى الركائز الأساسية في التعاون الأمني الدولي والإقليمي، لما توفره من فرص لتبادل الخبرات والمعلومات، وتحقيق تدخل فعّال وسريع، لا يمكن إنجازه من طرف دولة بمفردها.

تشمل العمليات الشرطية والأمنية المشتركة عدة أوجه، من أبرزها:

أولا: الدوريات الأمنية المشتركة

تقوم بها قوات شرطية تابعة لدول متجاورة، خصوصًا في المناطق الحدودية التي تشهد تحركات غير قانونية مثل التهريب والهجرة السرية. وتُعتبر هذه الدوريات أداة فعالة لضبط الحدود، حيث تتبادل الأطراف المهام الأمنية والمراقبة[1].

ثانيا: تنفيذ عمليات مداهمة منسقة

تتم من خلال التنسيق بين وحدات خاصة في أكثر من دولة، بهدف تفكيك شبكات إجرامية تعمل في عدة بلدان، لا سيما شبكات الاتجار بالبشر والمخدرات، يتطلب ذلك توفر قواعد بيانات مشتركة، وتفاهم مسبق حول الإجراءات القضائية المرتبطة بالتسليم والتوقيف[2].

ثالثا: إجراء تدريبات وتمارين ميدانية مشتركة

بهدف تحسين الجاهزية وتوحيد أساليب التدخل، مثل ما تقوم به الدول الأوروبية في إطار "مبادرات التدريب المشتركة لمكافحة الإرهاب"، أو التدريبات السنوية التي تنظمها الجزائر مع عدد من دول الساحل ضمن إطار مكافحة الجماعات المسلحة.

رابعا: مراكز التنسيق الأمني

هي منصات تكنولوجية أو هيكلية تُنشأ بين الدول لتبادل البيانات والإنذارات المبكرة، مثل "مركز التنسيق الأمني الجزائري–النيجري–النيجيري–المالي"، الذي يُعد نموذجًا للتنسيق الإقليمي لمكافحة الجماعات المسلحة[3].

خامسا: التعاون في إطار المنظمات الدولية

مثل منظمة الإنتربول، التي تُعد بمثابة منصة عالمية لتنسيق العمليات الأمنية من خلال نشرات الإيقاف الدولية (النشرة الحمراء)، والعمليات المشتركة الواسعة مثل "عملية ليبيك (Lyon–Beijing Cooperation) " لمكافحة تهريب الأسلحة.

---

[1] سعيد، محمد. "التعاون الأمني الدولي ودوره في مكافحة الإرهاب"، **ع 12، مجلة البحوث القانونية والسياسية، جامعة غير محددة، بلد غير محدد،** 2021 **ص 84.**

[2] منصوري، عبد القادر "الأمن الإقليمي والتحديات الأمنية المشتركة في منطقة الساحل والمغرب العربي"، ع 45، مجلة السياسة الدولية، جامعة غير محددة، بلد غير محدد، 2020، ص 66.

[3] الأمّانة العامة لمجلس وزراء الداخلية العرب، "دليل التعاون الأمني العربي"، تونس، 2019، ص23.

هذا النوع من العمليات لا يمكن أنّ يكون فعالًا دون إطار قانوني وتنظيمي يحدد المسؤوليات، ويكفل احترام سيادة الدول، ويحمي الحقوق والحريات الأساسية. وهنا يبرز دور الاتفاقيات الثنائية والمتعددة الأطراف وكذلك المواثيق الدولية التي تُرسي قواعد تبادل المعلومات والتعاون القضائي، كاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية (اتفاقية باليرمو 2000)[1].

رغم النجاحات التي تحققت، تبقى هناك تحديات قائمة، أهمها تفاوت القدرات الأمنية بين الدول، وعدم تطابق الإطار القانوني، وضعف الثقة أحيانًا بين الشركاء، مما يعرقل تبادل المعلومات الحيوية، كما أنّ بعض الدول تتردد في الانخراط العميق في هذه العمليات، خشية التأثير على سيادتها الوطنية أو لأسباب سياسية.

إنّ تعزيز فعالية العمليات الشرطية والأمنية المشتركة يتطلب مأسسة التعاون الأمني من خلال بناء ثقة متبادلة، وتحديث التشريعات بما يسمح بسرعة التدخل، واعتماد تكنولوجيا حديثة تسهّل التنسيق الميداني والتحليل الاستباقي للبيانات.

المطلب الثالث: جهود الإنتربول والمنظمة الدولية للشرطة الجنائية ضد الجرائم المعلوماتية

حتى يسهل لكل دولة الاستمرار والعيش مع غيرها من الدول فإنها تحتاج إلى قدر من الأمن والنظام.

تشكل الجريمة إحدى القضايا الرئيسية في الكثير من دول العالم، وتشغل بال الحكومات والمختصين والأفراد على حد سواء، ولقد أثبت الواقع العملي أن الدولة – أي دولة – لا تستطيع بجهودها المنفردة القضاء على الجريمة مع هذا التطور الملموس والمذهل في كافة ميادين الحياة، فنتيجة للتطور الملموس والمذهل في الاتصالات وتكنولوجيا المعلومات وظهور الإنترنت والانتشار الواسع والسريع لها أدى إلى ظهور أشكال وأنماط جديدة من الجرائم منها الجرائم المتعلقة بشبكة الإنترنت وهي نوع من الجرائم المعلوماتية، التي باتت تشكل خطرا لا على سرية النظم الحاسوبية أو سلامتها أو توافرها فحسب، بل تعدت إلى أمن البنى الأساسية الحرجة.

لذلك أصبحت الحاجة ماسة إلى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة وتتعاون من خلاله أجهزة الشرطة في الدول المختلفة، خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنة بالإضافة إلى تعقب المجرمين الفارين من وجه العادلة[2].

فيما يلي سنتعرف على أهم أهداف الإنتربول وإستراتيجية المنظمة في مكافحة الجرائم المعلوماتية.

الفرع الأول: أهداف الانتربول

أولا: تعريف الإنتربول

الإنتربول هو أكبر منظمة شرطية دولية، أنشأت عام 1923، ومقرها الرئيسي في مدينة ليون بفرنسا،

[1] الإنتربول "تقارير التعاون الشرطي الدولي : آليات وتحديات التنفيذ"، 2020، ص04.

[2] تدابير مكافحة الجرائم المتصلة بالحواسيب، مؤتمر الأمم المتحدة الحادي عشر، لمنع الجريمة والعدالة الجنائية المنعقد في بانكوك في الفترة 18، 2005/04/25، وثيقة رقم A/CONF203/14، ص51.

وكما هو معروف من دستور الإنتربول الدولي فهي تتكون من الجمعية العامة اللجنة التنفيذية، الأمانة العامة المكاتب المركزية الوطنية، المستشارون لجنة ضبط ملفات الإنتربول وكانت تسمى هذه المنظمة باللجنة الدولية للشرطة الجنائية وتضم في عضويتها 195 دولة.

تقوم آلية العمل داخل منظمة الشرطة الدولية (الإنتربول) على تبادل المعلومات بين أعضائها بشأن المجرمين الدوليين، مما يُسهم في تنسيق الجهود لمكافحة مختلف أشكال الجريمة العابرة للحدود، كجرائم التهريب، والاتجار غير المشروع بالأسلحة، والجرائم السيبرانية. وفي السنوات الأخيرة، أولى الإنتربول اهتماما متزايدًا بالجريمة المنظمة، لاسيما الأنشطة المرتبطة بها مثل عمليات غسل الأموال.

ويحتفظ أفراد المنظمة بسجلات الجرائم الدولية وقد أنشأت المنظمة وحدة تحليل المعلومات الجنائية، التي تقضي باستخلاص المعلومات الهامة عن المنظمات الإجرامية وتبويبها، بهدف وضع تلك المعلومات في متناول هيئة الشرطة، أو الدول الأعضاء في الإنتربول.

مهمة الانتربول تتجلى في توفير الأمانة العامة للبلدان الأعضاء مجموعة من الخبرات والخدمات فالإنتربول تتدبر 19 قاعدة بيانات شرطية، تحتوي على معلومات عن الجرائم والمجرمين (كالأسماء وبصمات الأصابع وجوازات السفر المسروقة)، والتي يمكن للبلدان الاستفادة منها بشكل آني، كما تقدم أيضا الدعم في التحقيقات عن طريق تحليل الأدلة الجنائية، و المساعدة في تحديد مكان الفارين من العدالة في جميع أنحاء العالم؛ يعد التدريب جزءا بارزا من العمل في الكثير من المجالات حتى يصبح الموظفين ملمين بكيفية الاستفادة من خدمات الإنتربول بشكل فعال.

تخصص خبرات هذا الجهاز لدعم الجهود الوطنية في مكافحة الجرائم في ثالثة مجالات عالمية، التي تعتبر أكثر إلحاحا اليوم، وهي الإرهاب، والجريمة السيبيرية، والجريمة المنظمة. يتولى الموظفون العاملون في كل من مجالات الجريمة المتخصصة هذه، إدارة مجموعة غنية من مختلف الأنشطة مع البلدان الأعضاء، منها إسناد التحقيقات، والعمليات الميدانية والتدريب، والأهم من ذلك استشراف المستقبل من خلال البحث في الجرائم الدولية واتجاهاتها ومتابعة آخر المستجدات المتصلة بها[1].

ثانيا: جهود ومهام المنظمة الدولية للشرطة الجنائية الإنتربول

تهدف المنظمة إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف وعلى نحو فعال في مكافحة الجريمة. من تجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة، وذلك عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنضمة إليها وتتبادلها فيما بينها، إضافة إلى التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف، ومدها بالمعلومات المتوفرة لديها على إقليمها وخاصة بالنسبة للجرائم المتشعبة في عدة دول ومنها جرائم الإنترنت، و من الأمثلة على دور الإنتربول في ما يتعلق بالجرائم المتعلقة بالإنترنت ما حصل في الجمهورية اللبنانية عندما تم توقيف أحد الطلبة الجامعين من

[1] عشماني رضوان، "مكافحة جرائم المعلوماتية في القانون الجزائري والدولي"، أطروحة لنيل شهادة دكتوراه في العلوم تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة وهران 2 محمد بن أحمد، 2024، ص 192.

قبل القضاء اللبناني بتهمة إرسال صور إباحية لقاصرة دون العشرة أعوام من موقعه على شبكة الإنترنت، و ذلك إثر تلقي النيابة اللبنانية برقية من الإنتربول في ألمانيا بهذا الخصوص[1].

أمّا في مجال الجرائم المعلوماتية، فقد أنشأت المنظمة الدولية للشرطة الجنائية " الإنتربول" خلال عام 2004 وحدة خاصة لمكافحة جرائم التكنولوجيا ، كما قامت المنظمة بالتعاون مع مجموعة الدول الثمانية الكبرى (G8) بوضع استراتيجيات المواجهة هذا النوع من الجرائم، من خلال إنشاء مركز اتصالات أمني عبر الشبكة، يعمل على مدار 24 ساعة و 7 أيام في الأسبوع على مستوى مصالح الشرطة في الدول الأطراف واستخدام وسائل حديثة في تلك المكافحة كاستخدام قاعدة البيانات المركزية للصور الإباحية المحولة من قبل الدول الاطراف من خلال استخدام برنامج للتحليل والمقارنة لتلك الصور، وتزويد شرطة الدول الأطراف بكتيبات إرشادية حول الجرائم المعلوماتية وكيفية التدريب على مكافحتها والتحقيق فيها.

ومن بين الإنجازات التي حققتها الإنتربول في ظل مواجهة الجرائم المعلوماتية، تلك العملية التي قامت بها المباحث الفيدرالية الأمريكية بالاشتراك مع الإنتربول والمتعلقة بملاحقة الشخص الذي قام بنشر دودة الحب عبر الانترنت في الفلبين، وكذا العملية التي قامت بها شرطة الإنتربول، بالاشتراك مع المباحث الفيدرالية وكذا الشرطة الإنجليزية عام 1998 والتي أحرزت فيها إنجازات كبيرة، من خلال تفكيك منشور عليه أكثر من 75000 صورة سلبية لدعارة الأطفال، والقبض على 107 أشخاص في 12 دولة، وكذا عملية القبض على شاب ألماني، بتهمة توزيع أحد الفيروسات، وذلك بالتنسيق بين الإنتربول والمباحث الفيدرالية الأمريكية والشرطة الألمانية، وتفكيك موقع منشور للصور الإباحية في 02/05/2005، بالتنسيق مع الأوروبول.

على غرار هذه المنظمة، أنشأ المجلس الأوربي عام 1991م في لكسمبورج، شرطة أوربية لتكون همزة وصل بين أجهزة الشرطة الوطنية في الدول الأطراف، لملاحقة الجناة في الجرائم العابرة للحدود ومنها بطبيعة الحال الجرائم المتعلقة بالأنترنت.

أمّا على المستوى العربي، فقد أنشأ المكتب العربي للشرطة الجنائية من قبل مجلس وزراء الداخلية والعدل العرب في سنة 2010، بهدف تأمين وتنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة وملاحقة المجرمين في حدود القوانين والأنظمة المعمول بها في كل دولة، بالإضافة إلى تقديم المعونة في مجال دعم وتطوير أجهزة الشرطة في الدول الأعضاء[2].

[1] فاروق خلف، استاذ محاضر "ا"، " الآليات القانونية لمكافحة الجريمة المعلوماتية"، مجلة الحقوق والحريات، كلية الحقوق جامعة حمة لخضر، الوادي، ع 2، 2015، ص 12.

[2] فريد ناشف، "آليات التعاون الدولي في مكافحة الجرائم الإلكترونية"، المجلد8، ع1، مجلة البحوث في الحقوق والعلوم السياسية جامعة البليدة 2، الجزائر 2022، ص ص 438، 439.

الفرع الثاني: استراتيجية الإنتربول في مكافحة الجرائم المعلوماتية

مع التطور التكنولوجي الهائل في العقود الأخيرة، برزت الجرائم المعلوماتية كأحد أكبر التهديدات الأمنية على الصعيدين الوطني والدولي. حيث لم تعد تقتصر على الاحتيال أو الاختراق، بل باتت تشمل التجسس السيبراني، تخريب البنية التحتية الحيوية، واستغلال الفضاء الإلكتروني لتمويل الإرهاب وغسل الأموال اختراق الأنظمة، وسرقة البيانات، والاحتيال الإلكتروني؛ في ظل الطابع العابر للحدود لهذه الجرائم برز دور منظمة الشرطة الجنائية الدولية (الإنتربول) أحد أبرز الفاعلين في التصدي لهذا النوع من الجريمة من خلال استراتيجية شاملة تقوم على الوقاية، الرصد، التدخل، والتعاون الدولي.

أولًا: البنية المؤسسية المتخصصة لمكافحة الجريمة السيبرانية

أدرك الإنتربول مبكرًا خطورة التهديدات الرقمية، فأنشأ في عام 2015 المركز العالمي للابتكار (IGCI) في سنغافورة، ليكون بمثابة مركز قيادة عالمي لمواجهة الجريمة السيبرانية، ويتضمن هذا المركز:

- ✓ وحدة تحليل التهديدات الرقمية :التي ترصد الهجمات السيبرانية العالمية وتحدد اتجاهاتها.
- ✓ وحدة تحقيقات إلكترونية: متخصصة في تعقب مرتكبي الجرائم الإلكترونية عبر الحدود.
- ✓ مختبر الأدلة الرقمية: لتحليل البرمجيات الخبيثة وتطوير أدوات كشف الهجمات.

يُستخدم هذا المركز كنقطة تنسيق دولية بين الدول الأعضاء في المنظمة (أكثر من 195 دولة)، لتبادل البيانات الحساسة في إطار آمن وموثوق[1].

ثانيًا: نهج "الردع الذكي" عبر التكنولوجيا والشراكات

تعتمد استراتيجية الإنتربول على "الردع الذكي(Smart Deterrence) "، أي استخدام أحدث الوسائل التقنية لتعقّب الجريمة الإلكترونية وتعطيلها قبل وقوعها، من ذلك:

إطلاق أنظمة للإنذار المبكر، مثل Cyber Fusion Centre، الذي يوفر تحليلات فورية للهجمات المحتملة.

شراكات مع شركات تكنولوجيا عالمية (مثل Kaspersky و Trend Microو Microsoft) لتحديث قواعد البيانات الخاصة بالبرمجيات الضارة، واستغلال الذكاء الاصطناعي لتتبع سلوك المهاجمين.

تنسيق حملات عالمية، مثل عملية "Operation Africa Cyber Surge"، التي تم خلالها كشف شبكات احتيال إلكتروني في غرب إفريقيا[2].

ثالثًا: تطوير القدرات الوطنية للدول الأعضاء

يُدرك الإنتربول أنّ العديد من الدول، خصوصًا في إفريقيا وآسيا، تفتقر إلى الإمكانيات البشرية والتقنية لمواجهة التهديدات الرقمية، لذلك تستند استراتيجيته إلى:

---

[1] الإنتربول"مكافحة الجريمة السيبرانية – دور المركز العالمي للابتكار" www.interpol.int، بتاريخ 30 ماي 2025 على الساعة: 16:15.

[2] عبد الله ناصر،ع 7، "دور الشرطة الدولية في مكافحة الجريمة المعلوماتية"، مجلة القانون الرقمي جامعة جيلالي اليابس،بلعباس، 2022، ص74.

- ✓ تنظيم دورات تدريبية وورش عمل ميدانية حول تحليل الأدلة الرقمية، والتحقيق في جرائم العملات المشفّرة.
- ✓ دعم إنشاء فرق استجابة وطنية للحوادث السيبرانية .(CERTs)
- ✓ تقديم أدوات مجانية ومفتوحة المصدر للدول النامية لاستخدامها في المراقبة والتحليل.

وقد أطلقت المنظمة في هذا السياق برنامجًا عالميًا بعنوان Cybercrime Capacity Building Programme لرفع الجاهزية الوطنية للدول الأعضاء[1].

رابعًا: التعاون القضائي والقانوني في الجرائم المعلوماتية

إحدى ركائز الاستراتيجية تتمثل في دعم الإطار القانوني الدولي لمواجهة الجرائم الإلكترونية لأن معظم التشريعات الوطنية لا تواكب سرعة تطور الجريمة السيبرانية. ولهذا يسعى الإنتربول إلى:

تسهيل إصدار مذكرات توقيف دولية إلكترونية (النشرة الحمراء) في قضايا الجرائم المعلوماتية.

تقديم الدعم الفني في قضايا التحقيق الرقمي عبر الحدود.

تشجيع الدول على الانضمام إلى اتفاقية بودابست لمكافحة الجرائم المعلوماتية.

خامسًا: أمثلة عملية لنجاح الاستراتيجية

1. **عملية: "HAECHI ":**

عملية عالمية أُطلقت بالشراكة بين الإنتربول وهيئات إنفاذ القانون الآسيوية في 2021، استهدفت شبكات الجريمة الإلكترونية المتخصصة في الاحتيال المالي. النتيجة كانت توقيف أكثر من 1000 مشتبه به واسترجاع ملايين الدولارات من الأموال المسروقة.

2. **عملية:(2022) "Africa Cyber Surge":**

بمشاركة 25 دولة إفريقية، قاد الإنتربول تحقيقًا موسعًا في جرائم التصيد الاحتيالي والاحتيال البنكي عبر الإنترنت، تم خلاله توقيف مجرمين وضبط بنية تحتية رقمية تُستخدم في الاختراقات[2].

سادسًا: التحديات التي تواجه تنفيذ الاستراتيجية

رغم ما تحققه من نجاحات، فإنّ استراتيجية الإنتربول تواجه عدة تحديات، منها:

–تفاوت القدرات التقنية بين الدول الأعضاء، مما يجعل بعض الدول مرتعًا آمنًا للمجرمين الرقميين.

–صعوبة تتبع العملات الرقمية المستخدمة في الابتزاز وغسل الأموال.

–ضعف التعاون القضائي الدولي أحيانًا بسبب غياب اتفاقيات تسليم مجرمين أو التباين في تعريف الجريمة المعلوماتية.

[1] الأمم المتحد "اتفاقية بودابست لمكافحة الجريمة المعلوماتية"، 2001، ص10.

2 تقرير المركز العربي للأمن السيبراني، "التهديدات الرقمية في إفريقيا: دور الإنتربول في المواجهة"، 2023،ص59.

–الخصوصية وحماية البيانات، حيث تواجه المنظمة انتقادات أحيانًا بسبب المخاوف المتعلقة بحرية استخدام الإنترنت[1].

يتضح أنّ استراتيجية الإنتربول في مكافحة الجرائم المعلوماتية تقوم على رؤية متكاملة تجمع بين التكنولوجيا، التدريب، الشراكات، والتنسيق القضائي، وتُعد نموذجًا عالميًا في مواجهة التهديدات السيبرانية. ومع التطور المستمر لأساليب الجريمة الرقمية، ستظل الحاجة ماسة إلى تحديث الإستراتيجية، وتوسيع نطاق التعاون، خاصة مع القطاع الخاص والمجتمع المدني، من أجل بناء بيئة رقمية آمنة للجميع.

1 Europol & INTERPOL"Cybercrime Strategies and Operational Guidelines", 2022,p88.

خلاصة الفصل

يتّضح من خلال هذا الفصل أنّ الجريمة المعلوماتية تمثل تحديًا قانونيًا وأمنيًا متناميًا، نتيجة لارتباطها الوثيق بالتطور التكنولوجي المتسارع، مما جعل منها أحد أبرز أشكال الإجرام المستحدث الذي يستغل البنية الرقمية لتحقيق أغراض غير مشروعة. وقد حاولنا في المبحث الأول الإحاطة بالمفاهيم الأساسية المرتبطة بهذه الظاهرة، من خلال التعرف على ماهيتها، أنواعها، وخصائصها التي تميزها عن الجرائم التقليدية لا سيما من حيث الوسائل، طبيعة الفضاء الذي تُرتكب فيه، والآثار المترتبة عليها.

أمّا في المبحث الثاني، فقد تطرقنا إلى أبرز آليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية، مركزين على المقاربة الجزائرية في هذا السياق، وكذلك على الدور المحوري الذي تلعبه المنظمات الدولية، وفي مقدمتها الإنتربول، في دعم جهود الدول وتنسيقها من أجل مواجهة هذه التهديدات العابرة للحدود.

إنّ التصدي الفعّال للجريمة المعلوماتية يقتضي تطويرًا مستمرًا للترسانة القانونية الوطنية، إلى جانب تعزيز التعاون الدولي في مجالات التشريع، التحقيق، وتبادل المعلومات، باعتبار أن التحديات التي تفرضه هذه الجرائم لم تعد محصورة في نطاق محلي، بل باتت تهدد الأمن الرقمي العالمي بأسره.

الفصل الثاني :

الاليات القضائية لمكافحة الجريمة المعلوماتية

تمهيد

في ظل التطور السريع للتكنولوجيا، أصبحت الجرائم المعلوماتية من أكبر التحديات التي تواجه الأنظمة القانونية الحديثة، حيث تتطلب أساليب جديدة للتصدي لها تتجاوز الحدود الجغرافية التقليدية، نظرًا للطبيعة العابرة لهذه الجرائم، فإن التعاون القضائي الدولي بات ضرورة ملحة لضمان تحقيق العدالة ومنع الإفلات من العقاب.

من أجل ذلك، يعتمد النظام القانوني على مجموعة من الآليات القضائية التي تهدف إلى تعزيز التعاون بين الدول، من بينها تسليم المجرمين والمساعدة القضائية، حيث يُمكن للدول تبادل المعلومات القانونية اللازمة، تنفيذ الأحكام، ونقل الإجراءات القضائية لضمان فاعلية التحقيقات والمتابعات الجنائية، ومع ذلك تواجه هذه الآليات تحديات عدة، تتعلق باختلاف القوانين بين الدول، القيود الدستورية التي تمنع بعض الدول من تسليم مواطنيها، إضافة إلى التأخير الذي قد ينتج عن الإجراءات الإدارية المعقدة.

إلى جانب ذلك، تُعد المساعدة القضائية إحدى الركائز الأساسية في مكافحة الجرائم المعلوماتية، حيث تشمل استجواب المتهمين، تبادل الأدلة الرقمية، والإنابة القضائية التي تتيح تنفيذ إجراءات قانونية بين الدول وفق إطار قانوني مشترك، غير أنّ نجاح هذه العملية يعتمد بشكل كبير على مدى التنسيق بين الدول ومدى توافق أنظمتها القانونية.

لمواجهة هذه التحديات، بات من الضروري تحديث التشريعات الوطنية بما يتماشى مع المعايير الدولية وتعزيز التعاون بين المؤسسات القضائية لضمان استجابة قانونية سريعة ودقيقة، كما أنّ تحسين البنية التحتية الرقمية للأدلة الجنائية يسهم في توفير وسائل فعالة للتعامل مع الجرائم السيبرانية، مما يضمن تحقيق العدالة بفعالية أكبر.

وعلى المستوى الدولي، يُعد توسيع نطاق الاتفاقيات الدولية لمكافحة الجرائم السيبرانية أحد الحلول الرئيسية، بالإضافة إلى إنشاء منصات إلكترونية آمنة لتبادل المعلومات القضائية بين الدول، كما أنّ تعزيز برامج التدريب المشترك بين الأنظمة القانونية المختلفة يسهم في توحيد الجهود، مما يسهل التعاون القضائي ويوفر استجابة أكثر كفاءة لتطورات الجريمة المعلوماتية.

إنّ تطوير هذه الآليات القانونية يُعد خطوة حاسمة نحو توفير نظام قضائي أكثر تكاملًا، قادر على التصدي للتهديدات الرقمية المتزايدة، وضمان تحقيق العدالة في بيئة قانونية متجددة تتماشى مع تطورات العصر الرقمي.

يرمي هذا الفصل إلى تسليط الضوء على أهمية التعاون القضائي الدولي في مواجهة الجرائم المعلوماتية التي أصبحت تمثل تهديدًا عالميًا يستدعي استجابة قانونية منسّقة بين الدول، ويعالج هذا الفصل من خلال المبحث الأول الآليات القانونية الأساسية لهذا التعاون، لا سيما آلية تسليم المجرمين والمساعدة القضائية باعتبارهما أداتين محوريتين في ملاحقة المجرمين وتبادل المعلومات والأدلة الجنائية الرقمية.

كما يتناول المبحث الثاني أبرز الآليات المقترحة للتغلب على التحديات التي تعيق هذا التعاون، سواء كانت قانونية أو تقنية أو مؤسساتية، ويقترح جملة من الحلول، منها تحديث التشريعات الوطنية، توسيع نطاق

الاتفاقيات الدولية، اعتماد منصات رقمية آمنة للتبادل القضائي، وتعزيز التكوين والتنسيق بين الأنظمة القضائية.

ويهدف هذا الفصل إلى إبراز مدى ارتباط فعالية التعاون الدولي بمدى تقارب الأنظمة القانونية وقدرتها على التكيّف مع متطلبات العصر الرقمي.

المبحث الاول : الية تسليم المجرمين و الية المساعدة القضائية

يعد تسليم المجرمين من أهم آليات التعاون القضائي الدولي، حيث يسمح للدول بتسليم الأشخاص المطلوبين لمحاكمتهم أو تنفيذ العقوبات الصادرة بحقهم، وفقًا لاتفاقيات دولية وثنائية، يشمل هذا النظام مجموعة من الجرائم التي يجوز فيها التسليم، مثل الجرائم الخطيرة كالإرهاب والجرائم المنظمة، بينما تستثني بعض الجرائم، مثل الجرائم السياسية والجرائم ذات الطابع العسكري، لضمان عدم استغلال التسليم لأغراض غير قانونية.

ورغم أهمية هذه الآلية، إلا أنها تواجه تحديات قانونية، أبرزها التجريم المزدوج، الذي يشترط أن تكون الجريمة معاقبًا عليها في كل من الدولة الطالبة والدولة المطلوب منها التسليم، مما قد يعيق تنفيذ الطلبات، كما أنّ التزاحم في طلبيات التسليم يمثل تحديًا آخر، حيث قد تتلقى الدولة أكثر من طلب لتسليم نفس الشخص من دول مختلفة، مما يستوجب معايير واضحة لتحديد الأولوية وفقًا لطبيعة الجريمة والعلاقات الدولية.

المطلب الاول : نظام تسليم المجرمين و التحديات الخاصة بتسليمهم

يُعتبر تسليم المجرمين من القضايا القانونية التي تثير جدلًا واسعًا بين الفقهاء، حيث تتباين الآراء حول طبيعته القانونية بين كونه عملًا سياديًا، إجراءً للتعاون الدولي، أو عملًا قضائيًا، يرى بعض الفقهاء أنّ إجراءات تسليم المجرمين تُعد من أعمال السيادة التي تمارسها الدولة بإرادتها المنفردة، دون تدخل من أي دولة أخرى أو منظمة دولية، ومع ذلك، فإن هذا الحق ليس مطلقًا، بل تحكمه مصادر قانونية واتفاقيات دولية تحدد أصوله، عند النظر في طلب التسليم، لا تقتصر الدولة المطلوب منها التسليم على تطبيق القواعد القانونية فقط، بل تأخذ بعين الاعتبار الاعتبارات السياسية التي قد تؤثر على قرارها.

وتبرز الصفة السياسية لهذا الإجراء عندما يكون اختصاص البت في الطلب بيد الحكومة أو إحدى الجهات التنفيذية، حيث يتم التسليم غالبًا عبر القنوات الدبلوماسية. كما أنّ حرية الدولة في قبول أو رفض طلب التسليم، حتى لو توافرت شروطه القانونية، تؤكد على طبيعته السيادية، إلا إذا كانت الدولة ملتزمة باتفاقية دولية تلزمها بتنفيذ التسليم.

على الجانب الآخر، يرى بعض الفقهاء أنّ نظام تسليم المجرمين يُعد أداة للتعاون الدولي في مجال العدالة الجنائية، حيث يُسهم في مكافحة الجرائم العابرة للحدود، عندما تقوم دولة بتسليم شخص مطلوب لدولة أخرى، فإنها بذلك تساعدها في تطبيق قوانينها الجنائية على مرتكب الجريمة. ومن المهم الإشارة إلى أنّ التسليم في حد ذاته لا يُعتبر عقوبة، كما أنّ الدولة التي تقوم به لا تمارس حقها في العقاب، بل تتيح للدولة الطالبة فرصة التحقيق والمحاكمة وفقًا لقوانينها. ومع تزايد الجرائم المنظمة وجرائم غسل الأموال، أصبح تسليم المجرمين ضرورة لضمان الأمن والاستقرار العالمي.

كما يُعد هذا النظام تطبيقًا عمليًا للتضامن الدولي في مكافحة الإجرام، ويتم غالبًا بناءً على اتفاقيات ثنائية أو متعددة الأطراف.

هناك اتجاه ثالث يرى أنّ نظام تسليم المجرمين ذو طبيعة قضائية، حيث تُناط مهمة البت في طلبات التسليم بالسلطة القضائية في بعض الدول، ومع ذلك، فإن الفصل بين الأعمال القضائية والسيادية يُعد أمرًا معقدًا، إذ

لا يمكن اعتبار قرار التسليم بمثابة محاكمة، بل هو إجراء يستند إلى قواعد السيادة الدولية فالسلطة القضائية لا تتعامل مع طلب التسليم باعتباره قضية جنائية بحتة، بل وفقًا للضوابط القانونية والسياسية التي تحكم العلاقات الدولية.

يتضح أنّ نظام تسليم المجرمين يجمع بين الطابع السيادي، التعاون الدولي، والطبيعة القضائية، حيث يعتمد تصنيفه على الإطار القانوني لكل دولة والجهة المختصة بالنظر في طلبات التسليم، ومع التطورات المتسارعة في الجرائم العابرة للحدود، أصبح من الضروري تعزيز التعاون الدولي لضمان تحقيق العدالة الجنائية ومنع إفلات المجرمين من العقاب[1].

الفرع الاول : الجرائم التي يجوز فيها تسليم المجرمين

يجوز تسليم المجرمين وفقًا لشروط قانونية محددة، والتي تختلف من دولة لأخرى حسب الاتفاقيات الدولية والتشريعات الوطنية، عمومًا، يتم التسليم في الحالات التالية[2]:

– وجود اتفاقية دولية أو ثنائية بين الدولة الطالبة والدولة المطلوب منها التسليم، تحدد الإجراءات والشروط القانونية.

– التجريم المزدوج، أي أن تكون الجريمة معاقبًا عليها في كل من الدولة الطالبة والدولة المطلوب منها التسليم.

– خطورة الجريمة، حيث يتم التسليم عادة في الجرائم الخطيرة مثل الإرهاب، الجرائم المنظمة، الاتجار بالبشر، وغسيل الأموال.

– عدم وجود موانع قانونية، مثل كون الشخص المطلوب من رعايا الدولة المطلوب منها التسليم، أو أن يكون هناك خطر على حقوقه وحرياته الأساسية.

– عدم انقضاء الدعوى العمومية أو العقوبة بالتقادم، حيث لا يجوز تسليم شخص إذا كانت الجريمة قد سقطت بالتقادم وفقًا للقوانين الوطنية.

– ضمانات المحاكمة العادلة، حيث يجب أن تضمن الدولة الطالبة عدم تعرض الشخص للتعذيب أو المحاكمة غير العادلة.

الفرع الثاني: الجرائم التي لا يجوز فيها تسليم المجرمين

يُعد مبدأ تسليم المجرمين من الوسائل القانونية التي تهدف إلى تعزيز التعاون الدولي في مكافحة الجريم غير أنّ المشرّع الجزائري وضع له قيودًا حمايةً لسيادة الدولة وضمانًا لحقوق الأفراد، فقد نصّت المادة 698 من قانون الإجراءات الجزائية على حالات لا يجوز فيها التسليم، من أبرزها: الجرائم ذات الطابع السياسي

[1] لعوارم وهيبة، نظام تسليم المجرمين دراسة تحليلية مقارنة بين المواثيق الدولية التشريع الجزائري و التشريعات المقارنة، كلية الحقوق و العلوم السياسية، مجلة البيبان للدراسات القانونية و السياسية، جامعة محمد البشير الابراهيمي برج بوعريريج، العدد الأول، 2016، ص112-113.

[2] العنيد محمد زيد، شروط تسليم المجرمين في النظام القانوني الجزائري، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، المجلد 13 العدد 01، 2021، ص629.

والجرائم العسكرية البحتة، إضافة إلى الجرائم التي ارتُكبت داخل الإقليم الجزائري أو تلك التي صدر بشأنها حكم نهائي من القضاء الوطني، كما يُرفض التسليم إذا كان من شأنه تعريض الشخص المطلوب لخطر على حياته أو معاملته بشكل غير إنساني في الدولة الطالبة.[1].

ورغم إمكانية توافر الشروط القانونية اللازمة لإعمال آلية تسليم المجرمين، إلا أنّ هناك موانع قانونية قد تحول دون تنفيذ هذا الإجراء، وتستند هذه الموانع إلى اعتبارات متعددة، منها ما هو ذاتي يتعلق بشخص المطلوب تسليمه، كأن يكون من رعايا الدولة المطلوب منها التسليم، مما يمنحها الحق في رفض الطلب حفاظًا على سيادتها، كما قد يكون الشخص أجنبيًا، لكن الدولة ترفض تسليمه حمايةً لحقوقه وحرياته الأساسية، خاصة إذا كان هناك خطر يهدد سلامته أو يخشى تعرضه لمحاكمة غير عادلة[2].

إلى جانب ذلك، هناك موانع إجرائية ترتبط بمخالفة تسليم الشخص للمبادئ القانونية، سواء تلك المتعلقة بمشروعية ملاحقته الجنائية أو تلك الخاصة بحق الدفاع، حيث يُشترط أن تكون الإجراءات القانونية المتبعة في الدولة الطالبة للتسليم متوافقة مع المعايير الدولية لضمان محاكمة عادلة، كما أنّ بعض الاعتبارات الأخرى تستند إلى قواعد الاختصاص الجنائي الدولي، حيث قد يكون للدولة المطلوب منها التسليم اختصاص قانوني يمنعها من تنفيذ الطلب.

وفي كافة الأحوال، فإن موانع التسليم تستند إلى مبادئ النظام القانوني الداخلي، والتي تقضي مثلًا بعدم جواز محاكمة الشخص عن ذات الفعل مرتين، أو انقضاء الدعوى العمومية أو الحكم الصادر بالعقوبة بالتقادم، حيث يُعتبر ذلك من القواعد الأساسية التي تحمي حقوق الأفراد وتضمن عدم تعرضهم لإجراءات قانونية غير عادلة.

وبذلك، تُشكل موانع التسليم ضمانة قانونية للشخص المطلوب تسليمه، سواء كان ذلك بهدف محاكمته باعتباره متهمًا، أو لتنفيذ الحكم الصادر بحقه باعتباره مدانًا، وتُسهم هذه الموانع في تحقيق التوازن بين مقتضيات التعاون الدولي في مكافحة الجريمة، وبين حماية الحقوق الأساسية للأفراد وفقًا للمعايير القانونية والإنسانية المتعارف عليها دوليًا[3].

الفرع الثالث : تحديات تسليم المجرمين

يواجه نظام تسليم المجرمين العديد من التحديات التي تعيق تنفيذه بفعالية، خاصة في الجرائم العابرة للحدود، من أبرز هذه التحديات التجريم المزدوج، حيث يشترط أن تكون الجريمة معاقبًا عليها في كل من الدولة الطالبة والدولة المطلوب منها التسليم، مما قد يؤدي إلى رفض الطلب إذا لم يكن هناك توافق قانوني بين الدولتين،

[1] المادة 698 من قانون الإجراءات الجزائية الجزائري، التي تنص على حالات رفض التسليم، الجريدة الرسمية للجمهورية الجزائرية.

[2] ذيب محمد، ومروان عثماني، شروط تسليم المجرمين في النظام القانوني الجزائري، مجلة الباحث القضائي, جامعة محمد خيضر بسكرة، المجلد 13، العدد 1، 2021، ص 630.

[3] الخزاري وفاء، الموانع القانونية لنظام تسليم المجرمين، مجلة المنارة للدراسات القانونية و الادارية، 13/05/2020 https://revuealmanara.com/الموانع-القانونية-لنظام-تسليم-المجرمين/ ، 2025/05/15 ، 10:13.

كما أنّ السيادة الوطنية تلعب دورًا رئيسيًا، حيث ترفض بعض الدول تسليم مواطنيها استنادًا إلى مبدأ السيادة، معتبرة أنّ محاكمة مواطنيها يجب أن تتم داخل أراضيها.

إضافة إلى ذلك، تؤثر الاعتبارات السياسية على قرارات التسليم، حيث يمكن أن ترفض دولة تسليم شخص لأسباب دبلوماسية أو سياسية، حتى لو كان هناك اتفاق قانوني يسمح بذلك، كما أنّ خطر المحاكمة غير العادلة يمثل تحديًا آخر، حيث ترفض بعض الدول التسليم إذا كان هناك احتمال أن يتعرض الشخص لانتهاكات حقوق الإنسان أو لمحاكمة غير عادلة في الدولة الطالبة.

من التحديات الأخرى التزاحم في طلبات التسليم، حيث قد تتلقى الدولة المطلوب منها التسليم طلبات متعددة من دول مختلفة لتسليم نفس الشخص، مما يخلق تعقيدات قانونية في تحديد الأولوية، كما أن بعض الجرائم، مثل الجرائم السياسية والعسكرية، غالبًا ما تكون مستثناة من نطاق التسليم وفقًا للاتفاقيات الدولية مما يحد من إمكانية ملاحقة مرتكبيها عبر الحدود[1].

الفرع الرابع: التجريم المزدوج

يعتبر التجريم المزدوج من أهم الشروط الخاصة بنظام تسليم المجرمين فهو منصوص عليه في أغلب التشريعات الوطنية والصكوك الدولية المعنية بتسليم المجرمين ويجد أساسه الفلسفي في أنّ التسليم إجراء يتضمن مساسا بالحرية الشخصية يستند إلى قضاء أجنبي، الأمر الذي يوجب أن يكون لهذا الإجراء ما يبرره في النظام القانوني الوطني، و أن يكون الفعل– مبنى الطلب– مجرما في القانون الوطني حتى لا تصطدم مشاعر الجماعة بالقبض على شخص أو اعتقاله لارتكابه فعلا تعتبره تلك الجماعة مباحا ومشروع[2].

وبالرغم من أهمية هذا الشرط إلا أنه غالبا ما يكون عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم المعلوماتية، لاسيما و أنّ بعض الدول لا تجرم هذه الجرائم، بالإضافة إلى أنه من الصعوبة تحديد ما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تنطبق على الجرائم المتعلقة بشبكة الإنترنت أم لا، يضاف إلى ذلك أنّ الدول قد تفسر بتوسع شرط ازدواج التجريم الأمر الذي يعوق تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين، ويحول بالتالي دون جمع الأدلة ومحاكمة مرتكبي الجرائم المعلوماتية[3].

---

[1] تدريست مريم، معوقات نظام تسليم المجرمين كآلية للتعاون القضائي الدولي لمكافحة الجريمة المنظمة عبر الوطنية، المجلة النقدية للعلوم القانونية والسياسية، كلية الحقوق و العلوم السياسية، جامعة مولود معمري تيزي وزو، العدد 30، 2016 الصفحات 30–51.

[2] سليمان ابو نمر و يوسف بوكشريدة، مكافحة الجريمة المعلوماتية في إطار القانون الدولي، مذكرة مقدمة من أجل نيل شهادة ماستر أكاديمي، كلية الحقوق و العلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، 2021، ص46.

[3] سليمان ابو نمر و يوسف بوكشريدة، مرجع سابق، ص47.

الفرع الخامس: خطر المحاكمة غير العادلة

المحاكمة غير العادلة تُعد من أخطر التحديات التي تواجه العدالة الجنائية، حيث تؤثر بشكل مباشر على حقوق الأفراد وضمانات المحاكمة العادلة، يمكن أن تنشأ هذه المخاطر نتيجة لعدة عوامل، مثل التدخل السياسي في القضاء، عدم استقلالية المحاكم، التمييز ضد المتهمين، أو انتهاك حقوق الدفاع، في بعض الحالات، يتم استخدام المحاكمات كأداة لقمع المعارضين السياسيين أو المدافعين عن حقوق الإنسان، حيث يُحرم المتهمون من الحق في محاكمة عادلة وشفافة، كما قد يُمنعون من الوصول إلى الأدلة أو الاستعانة بمحامين مستقلين[1].

وفقًا للقانون الدولي، فإن الحق في محاكمة عادلة منصوص عليه في الإعلان العالمي لحقوق الإنسان والعهد الدولي الخاص بالحقوق المدنية والسياسية، حيث يُشترط أن تكون المحاكم مستقلة ونزيهة لضمان تحقيق العدالة، علاوة على ذلك، فإن المحاكمات غير العادلة قد تتضمن إجراءات سرية، اعترافات منتزعة تحت التعذيب، أو عدم السماح للمتهم بالطعن في الحكم، مما يؤدي إلى إصدار أحكام جائرة بحق الأفراد دون مراعاة حقوقهم الأساسية، هذه الانتهاكات تُشكل تهديدًا خطيرًا لسيادة القانون، وتؤثر على مصداقية الأنظمة القضائية في الدول التي تُمارس فيها مثل هذه المحاكمات.

لذلك، فإن ضمان الشفافية القضائية، استقلالية القضاء، واحترام حقوق الدفاع يُعد أمرًا ضروريًا لحماية الأفراد من مخاطر المحاكمة غير العادلة، وضمان تحقيق العدالة وفقًا للمعايير الدولية[2].

الفرع السادس : التزاحم في طلبيات التسليم

يقصد بالتزاحم في طلبات التسليم أو تنازع الطلبات:" تلك الحالة التي يصل فيها إلى الدول المطلوب منها التسليم أكثر من طلب تسليم من عدة دول تطلب ذات الشخص، سواء كان الطلب متعلق بنفس الجريمة أو بجرائم أخرى المضرورة إلى الدولة المطلوب إليها، وللقول بوجود تزاحم في طلبات التسليم ينبغي أن تقدم الدولة الطالبة لأدلة التي تثبت قيام الشخص المطلوب بارتكاب الجريمة المعلوماتية وليس مجرد الادعاء وكذلك إرسال طلبها بالفعل، حيث لا تكفي التصريحات الشفوية أو إبداء الرغبة في استلام الشخص.

ولا يشترط في تزاحم الطلبات أن تتعاصر في وصولها إلى الدولة وسبب تعلق هذه الصعوبة بالجرائم المعلوماتية أنّ الشخص المطلوب تسليمه قد يرتكب جريمة أو أكثر من الجرائم المعلوماتية تمس في نفس الوقت بمصالح أساسية لأكثر من دولة، ففي هذه الحالة قد تتزاحم طلبات التسليم المقدمة من الدول المطلوب

---

[1] سلطان بن قايد و ناصر بن غيث و أحمد منصور و عبد السلام المرزوقي، محاكمة غير عادلة وأحكام جائرة: إدانة مدافعين حقوقيين ومعارضين سياسيين ظلما، مِنَا لحقوق الانسان، 2024/07/11، https://menarights.org/ar/articles/mhakmt-ghyr-adlt-wahkam-jayrt-adant-mdafyn-hqwqyyn-wmardyn-syasyyn-zlma ، 2025/05/15 ، 11:26.

[2] بلباي إكرام، ضمانات المحاكمة العادلة في المعايير الدولية، مجلة القانون الدستوري و المؤسسات السياسية، جامعة عبد الحميد بن باديس، المجلد 06، العدد 01، 2022، ص161-166.

إليها، بل يكفي أن تتوالى إلى الدولة المطلوب إليها، طالما أنّ الشخص المطلوب ما زال متواجدة على إقليمها، ولم يتم تسليمه إلى أي من الدول التي تطالب بتسليمه[1].

المطلب الثاني : الية المساعدة القضائية

تُعتبر المساعدة القضائية من أهم الضمانات القانونية التي تتيح للأفراد غير القادرين ماليًا الحق في اللجوء إلى القضاء دون تحمل المصاريف القضائية، مما يساهم في تحقيق مبدأ المساواة أمام القانون، تهدف هذه الآلية إلى إزالة العوائق المالية التي قد تمنع بعض الفئات من ممارسة حقوقهم القانونية، وتُطبق وفق إجراءات محددة لضمان منحها للأشخاص المستحقين.

في إطار تعريف المساعدة القضائية، يُمكن اعتبارها نظامًا قانونيًا يهدف إلى إعفاء المعوزين من التكاليف المرتبطة بالتقاضي مثل رسوم رفع الدعوى، أتعاب المحاماة، وأجور الخبراء والشهود، مما يُمكّنهم من الدفاع عن حقوقهم أمام القضاء، أمّا بالنسبة إلى خطوات المساعدة القضائية، فهي تتضمن تقديم طلب رسمي إلى الجهة المختصة، مرفقًا بوثائق تثبت عدم القدرة المالية، ثم دراسة الطلب من قبل الجهات القضائية، واتخاذ قرار بشأن قبوله أو رفضه، ليتم بعد ذلك تنفيذ إجراءات التقاضي دون تحمل الأعباء المالية المعتادة[2].

الفرع الاول : المساعدة القضائية

المساعدة القضائية هي نظام قانوني يهدف إلى توفير الدعم القانوني للأفراد غير القادرين ماليًا على تحمل نفقات التقاضي، مما يتيح لهم اللجوء إلى العدالة دون قيود مالية، تُقدَّم هذه المساعدة للأشخاص الذين يستوفون شروطًا معينة، مثل الدخل المحدود أو التعرض لقضايا ذات طابع خاص كحقوق الإنسان، النزاعات العمالية، أو القضايا الأسرية[3].

تشمل المساعدة القضائية الإعفاء من الرسوم القضائية وأتعاب المحاماة، بالإضافة إلى تغطية تكاليف الخبرة القانونية والترجمة عند الحاجة، يتم منحها بعد تقديم طلب رسمي إلى الجهات المختصة، حيث يتم فحص الوضع المالي للطالب ومدى جدية القضية المطروحة أمام القضاء[4].

تهدف هذه الآلية إلى تحقيق العدالة والمساواة في الوصول إلى القضاء، وضمان عدم حرمان أي فرد من حقه في الدفاع عن نفسه بسبب ضيق ذات اليد، تُعتبر المساعدة القضائية أحد الركائز الأساسية لتعزيز الثقة في النظام القضائي، حيث تضمن حماية الحقوق الأساسية للجميع بغض النظر عن وضعهم الاقتصادي.

---

[1] سليمان ابو نمر و يوسف بوكشريدة، مرجع سابق، ص46-47.

[2] وزارة العدل الجزائرية، المساعدة القضائية، www.mjustice.dz/ar/المساعدة-القضائية/، 2025/05/15، 11:58.

[3] الأمر رقم 71-57 المؤرخ في 5 أوت 1971 والمتعلق بالمساعدة القضائية، المعدل والمتمم بالقانون رقم 09-02 المؤرخ في 25 فبراير 2009، الجريدة الرسمية للجمهورية الجزائرية.

[4] وزارة العدل الجزائرية، المساعدة القضائية، www.mjustice.dz/ar/المساعدة-القضائية/، 2025/05/15، 12:20.

المساعدة القضائية في الجزائر تستند إلى مجموعة من النصوص القانونية التي تحدد شروطها وإجراءاتها من بين القوانين الأساسية التي تنظم هذا النظام[1]:

1. الأمر رقم 71-57[2] المؤرخ في 5 أغسطس 1971 والمتعلق بالمساعدة القضائية، والذي تم تعديله وتحديثه لاحقًا.
2. القانون رقم 09-02[3] المؤرخ في 25 فبراير 2009، الذي يحدد شروط الاستفادة من المساعدة القضائية، بما في ذلك الأشخاص الطبيعيون والمعنويون الذين لا تسمح لهم مواردهم بالمطالبة بحقوقهم أمام القضاء.
3. القانون رقم 01-06[4] المؤرخ في 22 مايو 2001، الذي يحدد المساهمات المالية المخصصة للمساعدة القضائية.
4. يمكن للأفراد الذين يستوفون الشروط تقديم طلب إلى مكاتب المساعدة القضائية الموجودة في المحاكم والمجالس القضائية، حيث يتم فحص وضعهم المالي ومدى جدية القضية قبل منح المساعدة.

الفرع الثاني : خطوات المساعدة القضائية

المساعدة القضائية هي نظام قانوني يهدف إلى تمكين الأفراد غير القادرين ماليًا من ممارسة حقوقهم أمام القضاء دون تحمل المصاريف القضائية، للحصول على هذه المساعدة، يجب اتباع مجموعة من الخطوات القانونية والإجرائية لضمان استيفاء الشروط المطلوبة[5].

أولا : تقديم طلب رسمي

يجب على الشخص الراغب في الاستفادة من المساعدة القضائية تقديم طلب مكتوب إلى الجهة المختصة يتضمن ملخصًا لموضوع الدعوى أو الإجراء القضائي المطلوب.

ثانيا: إرفاق الوثائق المطلوبة

يجب أن يكون الطلب مرفقًا بعدد من الوثائق التي تثبت عدم قدرة مقدم الطلب على تحمل المصاريف القضائية، وتشمل:

1. نسخة من مستخرج جدول الضرائب أو شهادة عدم فرض الضريبة.

---

[1] وزارة العدل الجزائرية، المساعدة القضائية، www.mjustice.dz/ar/المساعدة-القضائية/، 2025/05/15، 12:37.

[2] الأمر رقم 71-57 المؤرخ في 5 أوت 1971 والمتعلق بالمساعدة القضائية، المعدل والمتمم، الجريدة الرسمية للجمهورية الجزائرية، العدد 64.

[3] القانون رقم 09-02 المؤرخ في 25 فبراير 2009، المعدل والمتمم للأمر رقم 71-57 المتعلق بالمساعدة القضائية، الجريدة الرسمية للجمهورية الجزائرية، العدد 15.

[4] القانون رقم 01-06 المؤرخ في 22 مايو 2001، المعدل والمتمم للأمر رقم 71-57 المتعلق بالمساعدة القضائية، الجريدة الرسمية للجمهورية الجزائرية، العدد 29.

[5] وزارة العدل الجزائرية، المساعدة القضائية، www.mjustice.dz/ar/المساعدة-القضائية/، 2025/05/15، 13:28.

2. تصريح شرفي يثبت فيه مقدم الطلب أنّ موارده المالية غير كافية، مصادق عليه من رئيس المجلس الشعبي البلدي لمقر سكنه.
3. كشف الراتب للأشهر الثلاثة الأخيرة، إن وجد.

ثالثا : تقديم الطلب إلى الجهة المختصة

يتم تقديم الطلب إلى مكاتب المساعدة القضائية الموجودة لدى الجهات القضائية وفقًا للحالات التالية[1]:

1. إلى وكيل الجمهورية إذا كانت الدعوى أمام المحكمة.
2. إلى النائب العام لدى المجلس القضائي إذا كانت القضية من اختصاص المجلس القضائي.
3. إلى النائب العام لدى المحكمة العليا أو محافظ الدولة لدى مجلس الدولة في القضايا التي تكون من اختصاصهما.

رابعا: دراسة الطلب واتخاذ القرار

بعد تقديم الطلب، تقوم الجهة المختصة بمراجعته والتحقق من استيفاء الشروط القانونية، يتم اتخاذ القرار بناءً على[2]:

1. مدى جدية الدعوى وأهميتها القانونية.
2. الوضع المالي لمقدم الطلب ومدى استحقاقه للمساعدة القضائية.

خامسا : منح المساعدة القضائية

منح المساعدة القضائية وآثارها[3]، والمتمثلة في:

1. أن يكون طالب المساعدة في حالة عسر مالي مثبت.
2. أن تكون الدعوى المراد رفعها أو الدفاع فيها غير تعسفية أو كيدية.
3. إمكانية استفادة الأجانب المقيمين بصفة قانونية من هذه المساعدة.
4. منحها استثنائيًا في حالات خاصة تستدعيها العدالة حتى لو لم تتوفر الشروط المالية.
5. الإعفاء من دفع الرسوم القضائية.
6. تعيين محامٍ على نفقة الدولة.
7. شمولها للإجراءات التنفيذية المتعلقة بالأحكام الصادرة.

سادسا : تنفيذ الإجراءات القضائية

[1] وزارة العدل الجزائرية، المساعدة القضائية، www.mjustice.dz/ar/المساعدة-القضائية/، 2025/05/15، 14:32.

[2] وزارة العدل الجزائرية، المساعدة القضائية، www.mjustice.dz/ar/المساعدة-القضائية/، 2025/05/15، 14:49.

[3] الأمر رقم 71-57 المؤرخ في 5 أوت 1971 والمتعلق بالمساعدة القضائية، المعدل والمتمم بالقانون رقم 09-02 المؤرخ في 25 فبراير 2009، الجريدة الرسمية للجمهورية الجزائرية.

بعد الحصول على المساعدة القضائية، يمكن للشخص متابعة دعواه أمام القضاء دون تحمل أي تكاليف مالية، حيث يتم تعيين محامٍ للدفاع عنه إذا لزم الأمر[1].

الفرع الثالث: صور المساعدة القضائية

تُعد المساعدة القضائية أحد أبرز أوجه التعاون القضائي الدولي، إذ تُمكّن الدول من تبادل المعلومات والإجراءات القانونية بهدف الوصول إلى العدالة ومنع الإفلات من العقاب. من بين أهم ملامح هذه المساعدة : تبادل المعلومات، ونقل الإجراءات، والإنابة القضائية[2].

ففيما يخص تبادل المعلومات، يُعد أحد الركائز الأساسية للتعاون القضائي الدولي، حيث يسمح للدول بتبادل بيانات قضائية حساسة تتعلق بالمطلوبين، مثل أسمائهم، سوابقهم الجنائية، وأماكن تواجدهم، يتم ذلك عبر قنوات متعددة مثل الإنتربول، أو من خلال اتفاقيات ثنائية ومتعددة الأطراف، هذا التبادل يُسهم في تسريع التحقيقات، تفادي تضارب الاختصاصات، وتعزيز فعالية مكافحة الجرائم العابرة للحدود، مثل الإرهاب وغسيل الأموال، كما أوصت الأمم المتحدة بإنشاء قواعد بيانات دولية لتيسير هذا التعاون[3].

يُقصد بنقل الإجراءات في إطار المساعدة القضائية استمرار استفادة الشخص المعوز من الإعفاءات والتسهيلات القانونية عند انتقال الدعوى أو الأعمال القضائية من جهة إلى أخرى، سواء تعلق الأمر بتنفيذ حكم أو مباشرة دعوى جديدة مرتبطة بالنزاع الأصلي، هذا النقل لا يُسقط الحق في المساعدة، بل يُراعى فيه وضع المستفيد وظروفه الاجتماعية، ويُقرر المكتب المختص ما إذا كانت المساعدة تستمر أو تُعدل حسب الحالة، وفقًا لما نص عليه القانون رقم 01-04 المؤرخ في 20 أوت 2001 المتعلق بالمساعدة القضائية[4].

أما الإنابة القضائية، فهي صورة راقية من صور المساعدة القضائية، تُستخدم عندما تطلب سلطة قضائية من دولة أخرى تنفيذ إجراء قضائي معين، مثل استجواب شاهد، أو إجراء تفتيش، أو حجز ممتلكات، يُنفذ هذا الطلب وفقًا لضوابط قانونية تضمن احترام الأنظمة المحلية للدولة المتلقية، وغالبًا ما يتم بناءً على اتفاقيات واضحة تحدد النطاق والحدود، الإنابة القضائية تُعد تجسيدًا للتعاون والثقة بين الأنظمة القضائية المختلفة، وتعكس التزامًا دوليًا بمكافحة الجريمة وتعزيز العدالة الجنائية[5].

---

[1] وزارة العدل الجزائرية، المساعدة القضائية، www.mjustice.dz/ar/المساعدة-القضائية/، 2025/05/15 ، 15:04.

[2] ايمان بن عثمان و ليلى بن بغيلة، التعاون القضائي الدولي ركيزة أساسية لتحقيق العدالة الجنائية الدولية، كلية العلوم الاسلامية، جامعة الوادي، مجلة الشهاب، المجلد 11، العدد 01، 2025، ص 482-485.

[3] فايق مينا، "التعاون القضائي الدولي: تبادل المعلومات والمساعدة القانونية"، مينا فايق للاستشارات القانونية، 2023، www.menafayq.com/international-judicial-cooperation-information-exchange-legal-assistance/ ، 2025/09/25 ، 9:51.

[4] القانون رقم 01-04 المؤرخ في 20 أوت 2001 المتعلق بالمساعدة القضائية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 46، سنة 2001.

[5] ايمان بن عثمان و ليلى بن بغيلة، نفس المرجع.

الفرع الرابع: تبادل المعلومات

يشير تبادل المعلومات إلى عملية مشاركة البيانات أو المعرفة بين الأفراد أو المؤسسات أو الدول بهدف تعزيز التعاون وتحقيق الأهداف المشتركة. يمكن أن يتم تبادل المعلومات في مختلف المجالات، مثل القانون، التكنولوجيا، الاقتصاد، والبحث العلمي، حيث يساعد في تحسين اتخاذ القرارات، تعزيز الابتكار وزيادة الكفاءة التشغيلية.

في السياق القانوني، يُعتبر تبادل المعلومات عنصرًا أساسيًا في المساعدة القضائية الدولية، حيث يسمح للجهات القضائية بتبادل الأدلة والمعلومات القانونية لدعم التحقيقات الجنائية أو تنفيذ الأحكام القضائية عبر الحدود، يتم ذلك من خلال الاتفاقيات الدولية التي تحدد آليات تبادل المعلومات بين الدول، مما يساعد على تسريع الإجراءات القانونية وضمان تحقيق العدالة.

أما في المجال التنظيمي، فإن تبادل المعلومات داخل المؤسسات يُسهم في تحسين الإنتاجية وتعزيز الابتكار، حيث يتم مشاركة المعرفة والخبرات بين الموظفين والأقسام المختلفة، كما إنّ تبادل المعرفة داخل المنظمات يساعد في تحسين عملية اتخاذ القرار، تعزيز الابتكار، وزيادة الكفاءة التشغيلية[1].

أولا: تعريف تبادل المعلومات

تبادل المعلومات في آلية المساعدة القضائية هو عملية تواصل رسمي ومنظم بين السلطات القضائية أو الجهات المركزية في الدول المختلفة، بهدف تبادل بيانات أو مستندات أو أدلة قانونية لازمة للتحقيق أو المحاكمة أو تنفيذ الأحكام، ويُعدّ هذا التبادل أحد الركائز الأساسية للتعاون القضائي الدولي، خاصة في القضايا ذات الطابع العابر للحدود مثل الإرهاب، غسل الأموال، الجريمة المنظمة، وتهريب المخدرات[2].

ثانيا: أهمية تبادل المعلومات[3]

1. تحسين عملية اتخاذ القرار :يساعد تبادل المعلومات في توفير بيانات دقيقة وموثوقة، مما يُمكّن الأفراد والمؤسسات من اتخاذ قرارات أكثر استنارة.
2. تعزيز الابتكار والتطوير :يُساهم في مشاركة الأفكار والخبرات، مما يُحفّز الإبداع ويساعد في تطوير حلول جديدة.
3. زيادة الكفاءة والإنتاجية :يُقلل من التكرار ويسمح بالاستفادة من المعرفة المتاحة، مما يُحسّن الأداء العام.

---

[1] Oyetunji, Damilola، "ما هو تبادل المعرفة ولماذا هو مهم؟" Klutch, 2024، https://klutch.app/ar/blog/what-is-knowledge-sharing-and-why-is-it-important/ ، 2025/05/20 ، 17:24.

[2] مجموعة أدوات الأمم المتحدة بشأن المخدرات الاصطناعية، المساعدة القانونية المتبادلة، Mutual Legal Assistance ، 2025/09/25 ، 18:19.

[3] مينا فيرال، "نماذج التواصل: فهم آليات تبادل المعلومات"، 2024، نماذج التواصل: فهم آليات تبادل المعلومات – MENAVIRAL | مينا فيرال ، 2025/05/20 ، 19:15.

4. تعزيز التعاون الدولي :يُساعد في تنسيق الجهود بين الدول في المجالات القانونية، الاقتصادية والعلمية، مما يُسهم في تحقيق أهداف مشتركة.

ثالثا: آليات تبادل المعلومات[1]

1. التبادل القانوني للمعلومات

في المجال القانوني، يُعتبر تبادل المعلومات عنصرًا أساسيًا في المساعدة القضائية الدولية، حيث يسمح للجهات القضائية بتبادل الأدلة والمعلومات القانونية لدعم التحقيقات الجنائية أو تنفيذ الأحكام القضائية عبر الحدود، يتم ذلك من خلال:

أ. الاتفاقيات الدولية التي تحدد آليات تبادل المعلومات بين الدول.

ب. المنصات الإلكترونية المشتركة التي تتيح تبادل البيانات القضائية بسرعة وكفاءة.

ج. التعاون بين أجهزة إنفاذ القانون لضمان الحصول على المعلومات اللازمة للتحقيقات الجنائية.

2. التبادل الإلكتروني للبيانات

يُشير التبادل الإلكتروني للبيانات إلى نقل المعلومات بين الأنظمة الرقمية دون تدخل بشري، مما يُساعد في تحسين سرعة وكفاءة العمليات التجارية والإدارية، يتم ذلك عبر:

أ. أنظمة إدارة البيانات التي تُتيح مشاركة المعلومات بين المؤسسات.

ب. تقنيات التشفير لضمان حماية البيانات أثناء نقلها.

ج. البروتوكولات الآمنة مثل EDIالتي تُستخدم في تبادل المستندات التجارية بين الشركات.

3. تبادل المعرفة داخل المؤسسات

في السياق التنظيمي، يُعد تبادل المعرفة عنصرًا أساسيًا في إدارة المعرفة، حيث يُساعد في تحسين الإنتاجية وتعزيز الابتكار. يتم ذلك عبر:

أ. الاجتماعات وورش العمل التي تُتيح مشاركة الأفكار والخبرات.

ب. المنصات الرقمية الداخلية التي تُستخدم لتوثيق ونشر المعرفة داخل المؤسسات.

ج. برامج التدريب والتطوير التي تُساعد في نقل المعرفة بين الموظفين.

[1] مينا فيرال، "نماذج التواصل: فهم آليات تبادل المعلومات"، 2024، نماذج التواصل: فهم آليات تبادل المعلومات – MENAVIRAL | مينا فيرال ، 2025/05/20 ، 21:03.

رابعا : التحديات التي تواجه تبادل المعلومات

يواجه تبادل المعلومات عدة تحديات[1]، منها:

1. ضعف البنية التحتية الرقمية
2. نقص الموارد البشرية المؤهلة
3. الثغرات القانونية
4. البيروقراطية وضعف التنسيق المؤسسي
5. مخاطر الأمن السيبراني

خامسا: الحلول المقترحة لتعزيز تبادل المعلومات

لضمان فاعلية تبادل المعلومات، يجب اتخاذ عدة تدابير[2]، منها:

1. تطوير أنظمة إدارة البيانات لضمان دقة وسرعة نقل المعلومات.
2. تعزيز التعاون الدولي من خلال اتفاقيات تُحدد آليات تبادل المعلومات القانونية والتجارية.
3. تحسين البنية التحتية الرقمية لضمان سرعة وكفاءة نقل البيانات.
4. تطبيق تقنيات التشفير لحماية المعلومات أثناء تبادلها.

الفرع الخامس : نقل الاجراءات

المعاهدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية، التي اعتمدتها الأمم المتحدة عام 1990 تهدف إلى تعزيز التعاون الدولي في العدالة الجنائية على أساس احترام السيادة وعدم التدخل، وذلك من خلال تمكين دولة من طلب نقل الإجراءات الجنائية إلى دولة أخرى إذا كان ذلك يخدم العدالة بصورة أفضل تشترط المعاهدة أن يكون الفعل مجرَّمًا في كلا الدولتين (التجريم المزدوج)، وأن يُقدَّم الطلب مكتوبًا ومصحوبًا بالوثائق اللازمة مثل هوية المشتبه فيه ووصف الجريمة والنصوص القانونية ذات الصلة.

كما تحدد أسبابًا للرفض مثل الطابع السياسي أو الضريبي للجريمة أو عدم انتماء المشتبه فيه للدولة المطالبة، وتكفل المعاهدة حقوق المشتبه فيه في إبداء الرأي وحقوق الضحية في التعويض، وتلزم الدولة الطالبة بوقف ملاحقاتها بعد قبول الطلب، بينما تتولى الدولة المطالبة الإجراءات وفق قانونها مع عدم فرض عقوبة أشد من تلك المنصوص عليها في قانون الدولة الطالبة.

---

[1] محمد الزعارة، واقع التحول الرقمي وسبل تحقيق النجاعة القضائية، 2025/02/15 https://www.droitetentreprise.com/واقع-التحول-الرقمي-وسبل-تحقيق-النجاعة/ ، 2025/09/25 ، 10:43.

[2] مينا فيرال، "نماذج التواصل: فهم آليات تبادل المعلومات"، 2024، نماذج التواصل: فهم آليات تبادل المعلومات – MENAVIRAL | مينا فيرال ، 2025/05/20 ، 11:27.

كما تجيز اتخاذ تدابير مؤقتة مثل التوقيف أو الحجز على الممتلكات، وتدعو إلى التشاور في حال تعدد الدعاوى لتحديد الدولة الأنسب لمتابعة القضية، مع تحمل كل دولة تكاليفها، وبذلك توفر المعاهدة إطارًا قانونيًا يضمن تجنب الازدواجية في الملاحقات، حماية حقوق الأطراف، وتفعيل التعاون القضائي الدولي[1].

أولا : تعريف نقل الإجراءات القضائية

نقل الإجراءات القضائية هو آلية للتعاون الدولي في القضايا الجنائية، تتيح لدولة أن تطلب من أخرى مباشرة الملاحقة أو المحاكمة إذا اقتضت ذلك مصلحة العدالة، يتم الطلب كتابيًا عبر القنوات الرسمية، ويشمل بيانات المشتبه فيه والوقائع القانونية، لا يُقبل الطلب إلا إذا كان الفعل مجرَّمًا في قانون الدولة المطلوب إليها (ازدواجية التجريم)، مع إمكانية رفضه إذا كان ذا طابع سياسي أو مخالفًا للنظام العام.

عند القبول، توقف الدولة الطالبة إجراءاتها، وتخضع القضية لقانون الدولة المستقبِلة مع ضمان حقوق الضحايا والمتهم، وبهذا يُسهم النقل في تفادي الازدواجية القضائية وتوحيد الجهود لتحقيق عدالة أكثر فعالية في القضايا العابرة للحدود. [2].

ثانيا : أهمية نقل الإجراءات القضائية[3]

1. تعزيز مكافحة الجرائم العابرة للحدود مثل الإرهاب، الاتجار بالبشر، والجرائم المالية.
2. ضمان تنفيذ الأحكام القضائية في الدول المختلفة، مما يمنع المجرمين من الإفلات من العقاب.
3. تسهيل تبادل الأدلة والمعلومات القانونية بين الدول، مما يساعد في تسريع التحقيقات الجنائية.
4. تحقيق العدالة الدولية من خلال توفير إطار قانوني مشترك لتنفيذ الإجراءات القضائية.

ثالثا : آليات نقل الإجراءات القضائية

تُعد آليات نقل الإجراءات القضائية من الركائز الأساسية في بناء تعاون دولي فعال لمكافحة الجرائم التي تتجاوز الحدود الوطنية، حيث تُمكّن الدول من تبادل المعلومات، تنفيذ الأحكام، وملاحقة الجناة عبر أنظمة قانونية مختلفة[4]. وتتمثل هذه الآليات في ستة عناصر رئيسية:

---

[1] جامعة منيسوتا، مكتبة حقوق الإنسان، نقل الإجراءات في المسائل الجنائية https://hrlibrary.umn.edu/arab/b051.html ، اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة 118/45 المؤرخ في 14 كانون الأول/ديسمبر 1990، 2025/09/25 ، 12:12.

[2] جامعة منيسوتا، مكتبة حقوق الإنسان، نقل الإجراءات في المسائل الجنائية، https://hrlibrary.umn.edu/arab/b051.html ، اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة 118/45 المؤرخ في 14 كانون الأول/ديسمبر 1990، 2025/09/25 ، 12:39.

[3] United Nations Office on Drugs and Crime, "Transfer of Criminal Proceedings", Education for Justice – UNODC, 2025, https://sherloc.unodc.org/cld/ar/education/tertiary/organized-crime/module-11/key-issues/transfer-of-criminal-proceedings.html , 25/05/2025 ,10:34 .

[4] فايق مينا، "الجرائم العابرة للحدود: آليات التعاون القضائي"، 2025/07/22، https://www.menafayq.com/transnational-crimes-judicial-cooperation-mechanisms ، 2025/09/25 ، 15:11.

1. المساعدة القانونية المتبادلة وهي وسيلة رسمية لتبادل الأدلة وتنفيذ الإجراءات القضائية بين الدول مثل استجواب الشهود أو تفتيش الأماكن، وتتم غالبًا بموجب اتفاقيات ثنائية أو متعددة الأطراف.
2. تسليم المجرمين إجراء قانوني تُسلّم بموجبه دولة شخصًا مطلوبًا لدولة أخرى لمحاكمته أو تنفيذ العقوبة، ويخضع لشروط مثل ازدواجية التجريم وعدم المساس بالسيادة أو الأمن القومي.
3. نقل المحكوم عليهم يُتيح للمحكوم عليهم قضاء عقوبتهم في دولتهم الأصلية، مما يُسهم في إعادة تأهيلهم ويُخفف العبء عن الدولة التي أصدرت الحكم.
4. الاعتراف بالأحكام القضائية الأجنبية يُمكّن الدول من الاعتراف وتنفيذ الأحكام الصادرة عن محاكم دول أخرى، سواء كانت جنائية أو مدنية، وفقًا لشروط قانونية محددة واتفاقيات دولية.
5. الفرق المشتركة للتحقيق (JITs) فرق ميدانية مكوّنة من ممثلين قضائيين وأمنيين من عدة دول، تُشكّل للتحقيق في قضية واحدة ذات طابع دولي، وتُسهّل تبادل الأدلة وتجاوز العقبات الإجرائية.
6. التعاون الشرطي والاستخباراتي يشمل تبادل المعلومات الأمنية، التنسيق في عمليات القبض، وتطوير القدرات التحقيقية، وتلعب فيه منظمات مثل الإنتربول ويوروبول دورًا محوريًا.

رابعا : التحديات التي تواجه نقل الإجراءات القضائية

رغم أهميته، يواجه نقل الإجراءات القضائية عدة تحديات[1]، منها:

1. التأخير في تنفيذ الطلبات القضائية بسبب الإجراءات البيروقراطية.
2. عدم توافق القوانين بين الدول، مما يؤدي إلى رفض بعض الطلبات القضائية.
3. القيود المتعلقة بحماية البيانات، حيث تفرض بعض الدول قيودًا على تبادل المعلومات القانونية.
4. غياب إطار قانوني موحد لتنظيم التعاون القضائي بين الدول المختلفة.

خامسا : الحلول المقترحة لتعزيز نقل الإجراءات القضائية

لضمان فاعلية نقل الإجراءات القضائية، يجب اتخاذ عدة تدابير[2]، منها:

1. تطوير اتفاقيات دولية تحدد إجراءات قانونية موحدة لتسهيل التعاون القضائي.
2. إنشاء منصات إلكترونية لتبادل المعلومات القضائية بسرعة وكفاءة.
3. تعزيز التعاون بين الدول من خلال برامج تدريبية مشتركة للقضاة والمحققين.
4. تحديث القوانين الوطنية لضمان توافقها مع المعايير الدولية لنقل الإجراءات القضائية.

[1] United Nations Office on Drugs and Crime, "Transfer of Criminal Proceedings", Education for Justice – UNODC, 2025, https://sherloc.unodc.org/cld/ar/education/tertiary/organized-crime/module-11/key-issues/transfer-of-criminal-proceedings.html , 25/05/2025 , 11:28.

[2] United Nations Office on Drugs and Crime, "Transfer of Criminal Proceedings", Education for Justice – UNODC, 2025, https://sherloc.unodc.org/cld/ar/education/tertiary/organized-crime/module-11/key-issues/transfer-of-criminal-proceedings.html , 25/05/2025 , 12:30.

الفرع السادس : الانابة القضائية

الإنابة القضائية[1] هي إجراء قانوني يتيح للجهات القضائية تفويض سلطة قضائية أخرى لتنفيذ إجراءات قانونية معينة، مثل جمع الأدلة، استجواب الشهود، أو تنفيذ الأحكام القضائية، تُستخدم هذه الآلية عندما يكون تنفيذ الإجراء المطلوب خارج نطاق اختصاص المحكمة أو القاضي الذي ينظر القضية، سواء داخل الدولة أو على المستوى الدولي.

أولا: أهمية الإنابة القضائية[2]

1. تُعدّ ركيزة أساسية لضمان سير العدالة بكفاءة، خاصة في القضايا التي تتجاوز حدود الاختصاص المكاني.
2. تسمح للمحاكم بطلب مساعدة جهات قضائية أخرى داخل الدولة أو خارجها لتنفيذ أعمال مثل سماع الشهود أو جمع الأدلة أو إجراء المعاينات.
3. تضمن استمرار سير الدعوى دون الحاجة لنقل أطرافها أو المحكمة إلى مكان الإجراء.
4. تُعتبر أداة مرنة تخدم مبدأ التكامل بين الجهات القضائية وتُسرّع من وتيرة التقاضي.
5. تُخفف العبء عن المحاكم الأصلية وتمنع تعطيل إجراءات جمع الأدلة الهامة، مما يعزز من فاعلية النظام القضائي ككل.

ثانيا: أنواع الإنابة القضائية

1. الإنابة القضائية الداخلية: تتم داخل الدولة عندما يكون هناك حاجة إلى تنفيذ إجراء قضائي في منطقة خارج اختصاص المحكمة الأصلية. تشمل هذه الإنابة[3]:
   أ. تفويض قاضي آخر أو ضابط شرطة قضائية لجمع الأدلة أو استجواب الشهود.
   ب. إجراء معاينات ميدانية في مناطق خارج نطاق المحكمة الأصلية.
2. الإنابة القضائية الدولية: تتم بين الدول عندما يكون تنفيذ الإجراء القضائي مطلوبًا في دولة أخرى. تشمل هذه الإنابة:
   أ. طلب تنفيذ إجراءات قضائية في دولة أخرى وفقًا للاتفاقيات الدولية.
   ب. تبادل المعلومات القانونية بين الدول لضمان تحقيق العدالة.
   ج. تنفيذ الأحكام القضائية الصادرة في دولة أخرى وفقًا للإطار القانوني المتفق عليه.

---

[1] بوشليق كمال، "النظام القانوني للإنابة القضائية في التشريع الجزائري"، مجلة دراسات و ابحاث المجلة العربية للأبحاث و الدراسات في العلوم الإنسانية و الاجتماعية، جامعة باتنة 1، المجلد 12، العدد 3، 2020، الصفحات 571-575.

[2] مينا فايق، "أحكام الإنابة القضائية وجمع الأدلة في القضايا"، موقع مينا فايق للاستشارات القانونية، 2025/09/19، https://www.menafayq.com/judicial-delegation-evidence-collection-cases/ ، 2025/09/25، 16:19.

[3] بوشليق كمال، مرجع سابق، ص 576-578.

ثالثا : التحديات التي تواجه الإنابة القضائية

رغم أهميتها، تواجه الإنابة القضائية عدة تحديات، منها[1]:

1. البطء في الإجراءات إذ تتسم طلبات الإنابة القضائية بالتعقيد وكثرة المراحل الشكلية، مما يؤدي إلى تأخير تنفيذها.
2. الاختلاف بين النظم القانونية تباين القوانين الوطنية والإجراءات الجنائية بين الدول يعرقل أحيانًا قبول الطلبات أو تنفيذها.
3. القيود المتعلقة بالسيادة الوطنية بعض الدول تتحفظ على تنفيذ الإنابات إذا رأت أنها تمس بسيادتها أو نظامها العام.
4. ضعف الثقة المتبادلة غياب الثقة بين السلطات القضائية في بعض الدول يؤدي إلى التردد في تبادل المعلومات أو تنفيذ الطلبات.
5. القصور في الاتفاقيات الدولية عدم وجود اتفاقيات ثنائية أو متعددة الأطراف شاملة يحد من فعالية الإنابة القضائية.
6. الاعتبارات السياسية قد تتأثر بعض الطلبات بعوامل سياسية أو دبلوماسية، مما يعيق التعاون القضائي.

رابعا: الحلول المقترحة لتعزيز الإنابة القضائية[2]

لضمان فاعلية الإنابة القضائية، يجب اتخاذ عدة تدابير، منها:

1. تطوير اتفاقيات دولية تحدد إجراءات قانونية موحدة لتسهيل التعاون القضائي.
2. إنشاء منصات إلكترونية لتبادل المعلومات القضائية بسرعة وكفاءة.
3. تعزيز التعاون بين الدول من خلال برامج تدريبية مشتركة للقضاة والمحققين.
4. تحديث القوانين الوطنية لضمان توافقها مع المعايير الدولية للإنابة القضائية.

المبحث الثاني : اليات مواجهة تحديات التعاون الدولي في مكافحة الجرائم المعلوماتية

يُعد التعاون الدولي في مكافحة الجرائم المعلوماتية ضرورة ملحة في ظل تزايد التهديدات السيبرانية التي تتجاوز الحدود التقليدية للدول، على المستوى الوطني الجزائري، يتم العمل على تحديث التشريعات لمواكبة التطورات الرقمية، وتعزيز الأمن السيبراني من خلال إنشاء وحدات متخصصة لمكافحة الجرائم الإلكترونية إضافة إلى تطوير آليات التحقيق الرقمي وتبادل المعلومات بين الجهات المختصة.

---

[1] فايق مينا، "الجرائم العابرة للحدود: آليات التعاون القضائي"، 2025/09/22، https://www.menafayq.com/transnational-crimes-judicial-cooperation-mechanisms، 2025/09/25 ، 17:07.

[2] بوشليق كمال، مرجع سابق، ص 578-580.

أمّا على المستوى الدولي، فتتمثل الجهود في توسيع نطاق الاتفاقيات الثنائية ومتعددة الأطراف، وتعزيز التعاون التقني والقضائي بين الدول، إلى جانب تطوير منصات مشتركة لتبادل البيانات حول الجرائم السيبرانية، هذه الآليات تهدف إلى تحسين التنسيق بين الدول وضمان استجابة فعالة لمواجهة الجرائم المعلوماتية.

المطلب الاول : آليات مواجهة تحديات التعاون الدولي في مكافحة الجرائم المعلوماتية على المستوى الوطني

تلعب القوانين والتشريعات الجزائرية دورًا أساسيًا في مكافحة الجريمة الإلكترونية، حيث عمل المشرع الجزائري على وضع إطار قانوني شامل لمواجهة هذه الجرائم التي تهدد الأمن السيبراني والاقتصاد الوطني من أبرز القوانين التي تم سنّها في هذا المجال القانون رقم 04/09[1] المؤرخ في 5 أغسطس 2009، الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، يهدف هذا القانون إلى تجريم الأفعال الإلكترونية غير المشروعة، مثل الاختراق الإلكتروني، الاحتيال عبر الإنترنت وانتهاك البيانات الشخصية، مع فرض عقوبات رادعة لضمان الحد من انتشار هذه الجرائم[2].

أمّا التدابير الإجرائية فهي تتجلى في إنشاء وحدات متخصصة داخل الأجهزة الأمنية والقضائية، تُعنى بجمع وتحليل الأدلة الرقمية باستخدام أحدث تقنيات الطب الشرعي الإلكتروني، تُقام ورش عمل ودورات تدريبية مُكثفة للقضاة والمحققين والعاملين في المجال الأمني، بهدف تعزيز قدراتهم الفنية على التعامل مع الجرائم السيبرانية وضمان تطبيق الإجراءات القانونية بالشكل الصحيح، كما يُعزز التعاون بين الجهات المختصة على المستوى الوطني من خلال آليات تنسيق وتبادل معلومات، بالإضافة إلى إقامة شراكات مع جهات دولية تسهم في متابعة المجرمين والتصدي للجرائم العابرة للحدود.

تشكل هذه الجهود، سواء على الصعيد الموضوعي من خلال التشريعات الواضحة أو على الصعيد الإجرائي عبر الوحدات المتخصصة والتدريب والتعاون المتعدد الأطراف، ركيزة أساسية لتحقيق بيئة رقمية آمنة داخل الوطن الجزائري ومواجهة التحديات التي تفرضها الجرائم الإلكترونية في العصر الحديث.[3]

الفرع الاول : التدابير الموضوعية

تبنى المشرع الجزائري موقفًا واضحًا تجاه الجرائم الإلكترونية، حيث عمل على وضع إطار قانوني شامل لمكافحتها من خلال قانون العقوبات وقانون الإجراءات الجزائية، إضافة إلى القواعد الإجرائية التي تساعد على كشف ملابسات هذه الجرائم، في هذا السياق، تم تعديل قانون العقوبات ليشمل الجرائم السيبرانية، حيث تم إدراج عقوبات مشددة على الجرائم المتعلقة بالاحتيال الإلكتروني، التزوير الرقمي، والاعتداء على الأنظمة

[1] قانون رقم 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها، ج.ر، العدد 47.

[2] خاليدة بن بعلاش و علي عثماني، الأحكام الموضوعية و الإجرائية لمكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة أبحاث قانونية و سياسية، المجلد 06 العدد 02، 2021، ص699.

[3] خاليدة بن بعلاش و علي عثماني، مرجع سابق، ص 700.

المعلوماتية، كما نص قانون الإجراءات الجزائية على آليات التحقيق الرقمي، مثل اعتراض المراسلات الإلكترونية والتفتيش الرقمي، مما يسهم في جمع الأدلة الرقمية وملاحقة الجناة.

كما أنشئت هياكل أمنية وقضائية متخصصة، مثل خلايا مكافحة الجريمة المعلوماتية على مستوى الأمن الوطني والدرك الوطني، تضم كوادر مؤهلة في مجالات تحليل الأدلة الرقمية ومتابعة النشاطات الإلكترونية المشبوهة، إلى جانب ذلك، تم وضع القواعد الإجرائية التي تساعد على كشف ملابسات الجرائم المعلوماتية مثل تحليل بيانات المرور الإلكتروني، الحفظ العاجل للمعطيات الرقمية، واعتراض الاتصالات المشبوهة وفقًا لضوابط قانونية محددة.

كما تم إلزام مقدمي الخدمات الرقمية بالحفاظ على البيانات الإلكترونية لفترة محددة وتقديمها للجهات القضائية عند الحاجة، مما يسهم في تعزيز الأمن السيبراني ومكافحة الجرائم الإلكترونية بفعالية[1].

وعلى صعيد التنسيق المؤسساتي، تعزز التعاون بين وزارات العدل، الداخلية، الدفاع الوطني، ومؤسسات تنظيم الاتصالات، لضمان توحيد الجهود والاستجابة بشكل فعّال للتهديدات الإلكترونية، هذه الإجراءات مكّنت الجزائر من بناء قاعدة قانونية ومؤسساتية تُمكّنها من الانخراط بفعالية في الجهود الدولية الرامية إلى مكافحة الجريمة المعلوماتية[2].

أولا : موقف المشرع الجزائري من الجريمة الالكترونية

اتخذ المشرع الجزائري موقفًا واضحًا تجاه الجريمة الإلكترونية، حيث سعى إلى وضع إطار قانوني شامل لمكافحتها والحد من آثارها السلبية على الأفراد والمؤسسات، وقد تجسد هذا الموقف في إصدار القانون رقم 04/09 المؤرخ في 5 أغسطس 2009، الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، يهدف هذا القانون إلى تجريم الأفعال الإلكترونية غير المشروعة مثل الاختراق غير المصرح به، الاحتيال الإلكتروني، وانتهاك البيانات الشخصية، مع فرض عقوبات رادعة لضمان الحد من انتشار هذه الجرائم[3].

إلى جانب ذلك، قام المشرع الجزائري بتعديل بعض مواد قانون العقوبات لتشمل الجرائم السيبرانية، حيث تم إدراج عقوبات مشددة على الجرائم المتعلقة بالتزوير الرقمي، الاعتداء على الأنظمة المعلوماتية، والتشهير

[1] لرقط عزيزة، "التعاون الدولي في مكافحة الجرائم المعلوماتية (إشكالاته وآليات التغلب عليها)"، مجلة التواصل في الاقتصاد وإدارة القانون، كلية الحقوق و العلوم السياسية، جامعة باجي مختار عنابة، المجلد 25، العدد 04، 2019.

[2] شرف الدين وردة، بلجراف سامية، "الجوانب الموضوعية والإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري"، مجلة المنار للدراسات والبحوث القانونية والسياسية، كلية الحقوق و العلوم السياسية، جامعة يحيى فارس المدية، المجلد 1، العدد 3، 2017، الصفحات 31-58.

[3] مطماطي راويـــة، الجريمة الإلكترونية في التشريع الجزائري، مجلة القانون و الأعمال الدولية، 2019/04/17، الجريمة الإلكترونية في التشريع الجزائري ، 2025/05/15 ، 16:14.

الإلكتروني، كما تم تعزيز الإجراءات التحقيقية من خلال منح الضبطية القضائية صلاحيات موسعة في جمع الأدلة الرقمية واعتراض الاتصالات المشبوهة، مما يسهم في تحسين الاستجابة لهذه الجرائم[1].

ثانيا : قانون العقوبات

لقد تعرض المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي في قانون العقوبات بموجب القانون 15/04[2] المؤرخ في 10 نوفمبر 2004 بعنوان: "المساس بأنظمة المعالجة الآلية للمعطيات" ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى 394 مكرر 8.

وفي عام 2006 أدرج المشرع تعديل آخر على قانون العقوبات بموجب القانون 23/06[3] حيث مس هذا التعديل القسم السابع مكرر الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تم تشديد العقوبة المقررة لهذه الأفعال.

ويرجع سبب هذا التعديل إلى ازدياد الوعي بخطورة هذا النوع المستحدث من الإجرام باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى.

أمّا بالنسبة لأنواع الجرائم الإلكترونية المنصوص عليها في قانون العقوبات والتي يمكن تصنيفها إلى ما يلي:

1. الغش أو الشروع فيه، في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات.
2. حذف أو تغيير لمعطيات المنظمة.
3. إدخال أو تعديل في نظام المعطيات.
4. تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار.
5. حيازة أو إفشاء أو نشر أو استعمال المعطيات.
6. تكوين جمعية الأشرار.

وعليه، يمكن تكييف هذه الأفعال الإجرامية بأنها جرائم ضد أموال الغير والمضرة بالمجتمع، وتجدر الإشارة إلى أنّ المشرع قد قام بتعديل قانون العقوبات في سنة 2016، مستحدثا بذلك نصا جديدا وهو المادة 87 مكرر 12 والتي أحدثت لنا جريمة جديدة وهي جناية تجنيد الأشخاص لصالح إرهابي أو منظومة إرهابية باستخدام وسائل تكنولوجيا الإعلام والاتصال[4].

ثالثا : قانون الإجراءات الجزائية

---

1 شاين نوال ، الجريمة الإلكترونية في التشريع الجزائري –ماهيتها، موضوعها، خصائصها، ومظاهر تحدياتها، مجلة سوسيولوجيا، المجلد 06 العدد 02، 2020، ص59.

2 المادة 394 من القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004، المتعلق بقوانين العقوبات." الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، 2004، العدد 71.

3 القانون رقم 23/06 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون العقوبات، ج.ر.عدد 84.

4 المادة 87 من القانون رقم 02/16 المؤرخ في 19 ماي 2016 المعدل والمتمم لقانون العقوبات، ج. ر. عدد 37.

فيما يتعلق بمتابعة الجريمة الإلكترونية فهي تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية كالتفتيش والمعاينة، واستجواب المتهم والضبط والتسرب والشهادة والخبرة، غير أنّ المشرع الجزائري فقد نص على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية[1].

كما نص على التفتيش في المادة 45 الفقرة 7 من نفس القانون[2] المعدلة حيث اعتبر أنّ التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه في القواعد العامة من حيث الشروط الشكلية والموضوعية.

ونص كذلك المشرع على التوقيف للنظر في جريمة المساس بأنظمة المعالجة في المادة 51 الفقرة 6 وكذلك على اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

أمّا بالنسبة لباقي الإجراءات من تحقيق ومحاكمة فإنه تطبق عليه نفس إجراءات الجريمة التقليدية.

– القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها :

يهدف هذا القانون[3] إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. وقد تبنى هذا القانون تعريف الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وكل ما يتعلق بالمنظومة المعلوماتية وكذا معطيات المعلومات ومقدمو الخدمات[4].

وقد خول هذا القانون بعض الإجراءات التي تطبق على الجرائم الإلكترونية من:

أ. مراقبة الاتصالات الإلكترونية[5].

ب. تفتيش المنظومة المعلوماتية[6].

ج. حجز المعطيات المعلوماتية[7].

---

[1] المادة 37 من القانون رقم 07/17 المؤرخ في 27 مارس 2017 المعدل والمتمم لقانون الإجرات الجزائية ،ج.ر .عدد20.

[2] المادة 45 الفقرة الثانية من القانون رقم 07/17 المؤرخ في 27 مارس 2017 المعدل والمتمم لقانون الإجرات الجزائية، القانون السابق.

[3] القانون رقم 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها ، القانون السابق.

[4] المادة 2 من القانون 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها ، القانون السابق.

[5] المادة 4 من القانون 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها ، القانون السابق.

[6] المادة 5 من القانون 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها ، القانون السابق.

[7] المادة 6 من القانون 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها ، القانون السابق.

وقد أنشأ بموجب هذا القانون هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال[1] والتي من مهامها:

أ. تفعيل التعاون القضائي والأمني و إدارة و تنسيق العمليات الوقائية.

ب. تبادل المعلومات مع الجهات الأجنبية من أجل تفعيل الحماية على المنظومة المعلوماتية من كل خطر يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني.

رابعا: القواعد الإجرائية التي تساعد على كشف ملابسات الجريمة المعلوماتية

ونص الفصل الثالث على القواعد الإجرائية التي تساعد على كشف ملابسات هذا النوع من الجرائم، وذلك من حيث تفتيش للمنظومة المعلوماتية وحجز المعطيات المعلوماتية.

1. تفتيش المنظومة المعلوماتية:

أجاز هذا القانون للسلطات القضائية المختصة، وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية، وفي إطار هذا القانون الدخول بغرض التفتيش ولو عن بعد إلى:

أ- منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها.

ب- منظومة تخزين معلوماتية.

كما انه إذا كان هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، و أنّ هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها، بعد إعلام السلطة القضائية المختصة مسبقا بذلك، أمّا إذا كان تبين بأنها مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة، طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبادئ المعاملة بالمثل[2].

التفتيش يأخذ مجالين في الوضعيات المشار إليها، إمّا أن يكون في مجال أعمال التحقيق تقوم به السلطات القضائية المختصة، و إمّا أن يكون في مجال أعمال الاستدلال يقوم به ضباط الشرطة القضائية بناء على أمر تصدره السلطات المختصة، وفي كلتا الحالتين يكون جهاز الحاسوب هو المستهدف بمختلف ما يتكون منه[3].

---

[1] المادتين 13 و 14 من القانون 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها ، القانون السابق.

[2] المادة 5 من القانون رقم 04/09، المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها ، القانون السابق.

[3] عثماني رضوان، مرجع سابق، ص105.

كما أنه يمكن للسلطات المكلفة بالتفتيش، تسخير كل شخص لديه دراية بعمل المنظومة المعلوماتية محل البحث، أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها[1].

2. حجز المعطيات المعلوماتية: عندما يتم اكتشاف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها، ويتبين للسلطة التي تباشر التفتيش أنه ليس من الضروري حجز كل المنظومة، يتم في هذه الحالة نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز.

وعلى هذه السلطات السهر على المحافظة على هذه المعطيات في كل الأحوال، حتى ولو جاز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق[2].

ويتعين على السلطة التي تقوم بالتفتيش، استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة إذا استحالة إجراء الحجز لأسباب تقنية تبعا لما جاءت به المادة 06 من هذا لقانون[3].

أمّا فيما يتعلق "بالمعطيات المحجوزة ذات المحتوى المجرم"، يمكن للسلطة التي تباشر التفتيش أن تآمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة[4].

خامسا: التزامات مقدمي الخدمات

أمّا الفصل الرابع من هذا القانون 09- 04 تطرق ل "التزامات مقدمي الخدمات"، وقبل التطرق لهذه الالتزامات لابد علينا معرفة من هم مقدمي الخدمات.

1. مقدمي الخدمة: حسب المادة 02 من القانون 09-04 هم أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات، وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها.

---

[1] الفقرة الأخيرة من المادة 5 من القانون رقم 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها ، القانون السابق.

[2] المادة 06 من القانون رقم 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها ، القانون السابق.

[3] المادة 07 من القانون رقم 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها ، القانون السابق.

[4] المادة 08 من القانون رقم 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها ، القانون السابق.

وهذا ما نصت عليه اتفاقية بودابست* الموقعة في 23 نوفمبر 2001 المتعلقة بالإجرام الالكتروني في المادة الأولى، معتبرة مقدم الخدمة fournisseur de service كل جهة عامة أو خاصة تقدم لمستخدمي خدماتها إمكانية الاتصال عن طريق النظام المعلوماتي، وكل جهة أخرى تعالج أو تخزن البيانات المعلوماتية بدلا من خدمة الاتصال أو نيابة عن مستخدمي هذه الخدمة.

في إطار هذا القانون، يتعين على مقدمي الخدمات، تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، وبوضع المعطيات التي يتعين عليهم حفظها تحت تصرف هذه السلطات، كما يتعين على مقدمي الخدمات كتمان سرية

العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها، وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق[1].

2. التزامات مقدمي الخدمة:

أ. حفظ المعطيات المتعلقة بحركة السير: وذلك بحفظ:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.
- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.
- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال، وكذا عناوين المواقع المطلع عليها.

أمّا بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه.

ب. و بالنسبة للالتزامات الخاصة بمقدمي خدمة الإنترنت: يتعين عليهم التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن، كما يتعين عليهم وضع ترتيبات تقنية تسمح بحصر إمكانيات الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وأخبار المشتركين لديهم بوجودها[2].

---

* هي أول معاهدة دولية تهدف إلى مكافحة الجرائم المعلوماتية من خلال تنسيق التشريعات الوطنية، وتعزيز تقنيات التحقيق وتسهيل التعاون الدولي بين الدول، تم التوقيع عليها في بودابست، المجر، بتاريخ 23 نوفمبر 2001، ودخلت حيز التنفيذ في 1 يوليو 2004.

[1] عثماني رضوان، مرجع سابق، ص107.

[2] المادة 12 من القانون رقم 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها ، القانون السابق.

الفرع الثاني: التدابير الإجرائية

أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

وفقًا للمرسوم الرئاسي الصادر في 6 يونيو 2019، فإن الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال تعتبر مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية، ذات ركيزة أساسية في حماية الأمن السيبراني في الجزائر، حيث تعمل على التصدي للتهديدات الرقمية المتزايدة، وتعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، وضمان بيئة رقمية آمنة للمواطنين والمؤسسات[1].

يترأس الهيئة وزير الدفاع الوطني أو ممثله، و تتشكل من ممثلين عن وزارات الداخلية، العدل والمواصلات السلكية واللاسلكية، وتوضع تحت سلطة وزارة الدفاع الوطني، قد تم تأسيسها استجابةً لتزايد الجرائم الإلكترونية وتأثيرها على الأمن الوطني، في البداية، كانت الهيئة تتمتع بصفة السلطة الإدارية المستقلة، مما منحها صلاحيات واسعة في مجال مكافحة الجرائم الإلكترونية، ومع ذلك، وبسبب ظروف سياسية، تم تعديل وضعها الإداري لتصبح هيئة موضوعة تحت سلطة وزارة الدفاع الوطني، مما يعكس الأهمية الأمنية لهذه الجرائم وتأثيرها على استقرار الدولة[2].

دور الهيئة في حماية الأمن السيبراني ومكافحة الجرائم الإلكترونية: حيث تقوم بوظيفتين أساسيتين[3]:

أ. الدور الوقائي : يركز على الجرائم الإرهابية أو التخريبية التي تهدد أمن الدولة، مثل الهجمات السيبرانية التي تستهدف البنية التحتية الحيوية أو المؤسسات الحكومية.

ب. الدور المكافح: يشمل التصدي للجرائم الإلكترونية الأخرى، مثل الاحتيال الإلكتروني الاختراقات، والجرائم المالية الرقمية، بالإضافة إلى تقديم الدعم للهيئات القضائية بعد وقوع الجريمة.

1. الأهداف التي تسعى الهيئة لتحقيقها[4]:

أ. مراقبة الجرائم الإلكترونية : عبر استخدام تقنيات متقدمة لرصد الأنشطة المشبوهة على الإنترنت وتحليل البيانات المتعلقة بالجرائم السيبرانية.

---

[1] بداوي حميدة و بن سالم فطيمة، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها مذكرة مكملة لنيل شهادة ماستر تخصص إعلام آلي و أنترنت، جامعة البشير الإبراهيمي برج بوعريريج، الجزائر، 2023، ص14،4.

[2] بداوي حميدة و بن سالم فطيمة، مرجع سابق.

[3] حابت أمل، "دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، المجلة الدولية للبحوث القانونية و السياسية، كلية الحقوق و العلوم السياسية، جامعة تيزي وزو، المجلد 05، العدد 03، 2021، ص 473–475.

[4] المرسوم الرئاسي رقم 21–439 المؤرخ في 7 نوفمبر 2021، المتضمن تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وسيرها، الجريدة الرسمية، الجمهورية الجزائرية الديمقراطية الشعبية، 10 نوفمبر 2021، العدد 89، الصفحات 6–8.

ب. التعاون مع الجهات القضائية: من خلال تقديم الأدلة الرقمية والمعلومات اللازمة للتحقيقات، مما يساعد في تحديد هوية مرتكبي الجرائم الإلكترونية.

ج. تنظيم حملات توعية : تهدف إلى تعزيز الأمن السيبراني لدى المواطنين والمؤسسات، من خلال نشر ثقافة الحماية الرقمية وتقديم إرشادات حول كيفية تجنب الوقوع ضحية للجرائم الإلكترونية.

د. اقتراح تعديلات قانونية: لضمان مواكبة التشريعات للتطورات التكنولوجية، حيث تعمل الهيئة على تقديم توصيات بشأن تحديث القوانين المتعلقة بالجرائم الإلكترونية لضمان فاعلية المكافحة القانونية لهذه الجرائم.

2. مهامها[1]:

أ. التداول حول الاستراتيجية الوطنية للوقاية من الجرائم الإلكترونية.

ب. تقييم حالة التهديدات السيبرانية بشكل دوري لتحديد أولويات عمليات المراقبة.

ج. دراسة التقرير السنوي لنشاطات الهيئة والمصادقة عليه.

3. كما تتولى المديرية العامة للهيئة مسؤولية:

أ. إعداد وتنفيذ برنامج عمل الهيئة.

ب. إدارة الميزانية وضمان حسن سير العمليات المالية.

ج. تبادل المعلومات مع الهيئات الأجنبية لتحديد مكان مرتكبي الجرائم الإلكترونية والتعرف عليهم.

د. إجراء الخبرات القضائية لمساعدة السلطات القضائية في التحقيقات المتعلقة بالجرائم السيبرانية.

ثانيا: الوحدات التابعة لسلك الأمن الوطني

تلعب الوحدات الأمنية التابعة لسلك الأمن الوطني دورًا محوريًا في مكافحة الجرائم المعلوماتية والتحقيق فيها، وذلك من خلال مهامها المتخصصة التي تشمل رصد الأنشطة الرقمية غير المشروعة، وجمع الأدلة الإلكترونية، وتحليلها بواسطة أحدث التقنيات المتاحة. وتتنوع هذه الوحدات بحسب اختصاصاتها، حيث تضم فرقًا متخصصة في التحريات الجنائية الرقمية، وأخرى تُعنى بالمراقبة الإلكترونية وتتبع الأنشطة المشبوهة على شبكة الإنترنت[2].

أهم اختصاصات الوحدات التابعة لسلك الأمن الوطني في مكافحة الجرائم المعلوماتية[3]:

1. المراقبة والرصد الإلكتروني:

---

[1] المرسوم الرئاسي رقم 21-439 المؤرخ في 7 نوفمبر 2021، المتضمن تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وسيرها، نفس المرجع.

[2] عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة مقدمة لاستكمال متطلبات شهادة الماستر المهني الطور الثاني، كلية العلوم الاقتصادية و العلوم التجارية و علوم التسيير، جامعة قاصدي مرباح ورقلة، الجزائر، 2019، ص40،37.

[3] مبرك عز الدين، ومحمد أمين مهري، "الآليات القانونية لحماية البيانات الرقمية"، الشعب أونلاين، 10 أبريل 2023، https://www.echaab.dz/2023/04/10/الآليات-القانونية-لحماية-البيانات-ال ، 2025/05/25 ، 17:46.

أ. تعتمد هذه الوحدات على أنظمة متطورة لرصد الاتصالات المشبوهة والمواقع الإلكترونية التي قد تكون متورطة في أنشطة غير قانونية.

ب. تستخدم تقنيات الذكاء الاصطناعي وتحليل البيانات الضخمة لتحديد الأنماط السلوكية التي تشير إلى أنشطة إجرامية محتملة.

2. التحقيق في الجرائم السيبرانية :

أ. تشمل التحقيقات تحليل الأدلة الرقمية مثل سجلات الدخول والخروج من الأنظمة، والاتصالات المشفرة، والمعاملات المالية الإلكترونية المشبوهة.

ب. تتعاون هذه الوحدات مع المؤسسات القضائية لضمان جمع الأدلة وفقًا للمعايير القانونية التي تحمي حقوق الأفراد خلال عمليات التحقيق.

3. التنسيق مع الأجهزة الأمنية والمؤسسات الدولية:

أ. نظرًا للطابع العابر للحدود للجرائم المعلوماتية، تعمل هذه الوحدات بالتنسيق مع وكالات دولية لمكافحة الجرائم السيبرانية.

ب. يتم تبادل المعلومات مع الجهات الأمنية الخارجية من خلال الاتفاقيات الدولية التي تهدف إلى تعقب الجناة وضبطهم.

4. التوعية والتدريب:

أ. تقوم هذه الوحدات بحملات توعية تهدف إلى تثقيف المواطنين حول مخاطر الجرائم المعلوماتية وكيفية حماية بياناتهم الشخصية.

ب. تقدم برامج تدريبية متخصصة لموظفي الأمن حول تقنيات التحقيق الرقمي وأساليب مكافحة الجرائم الإلكترونية.

5. التطوير المستمر للمعدات والتقنيات:

أ. يتم تحديث الأدوات المستخدمة في التحقيقات بشكل دوري، بما يشمل البرمجيات الخاصة بتحليل البيانات وتقنيات فك التشفير.

ب. تعتمد هذه الوحدات على الأنظمة الحديثة لمكافحة الاختراقات والهجمات السيبرانية التي تستهدف البنية التحتية الرقمية.

هذه المهام تجعل الوحدات التابعة لسلك الأمن الوطني ذات أهمية حيوية في مواجهة الجرائم المعلوماتية، إذ تساهم في تعزيز الأمن السيبراني وحماية الأفراد والمؤسسات من المخاطر الإلكترونية المتزايدة.

ثالثا : الوحدات التابعة للدرك الوطني

يلعب الدرك الوطني دورًا رئيسيًا في مكافحة الجرائم الإلكترونية، حيث يعتمد على وحدات متخصصة وتقنيات حديثة لرصد الأنشطة الإجرامية الرقمية والتحقيق فيها، وفقًا للمصادر المتاحة، فإن الدرك الوطني يتبع نهجًا شاملاً يشمل الوقاية، التحقيق، والتعاون الدولي لضبط الجرائم السيبرانية، تتولى هته الوحدات ايضا

مسؤولية تنفيذ مهام متعددة تتعلق بالأمن العام، التحقيقات الجنائية، كما تعمل وفق تنظيم دقيق يضمن التنسيق الفعّال بين مختلف الفرق المتخصصة[1].

أهم الوحدات التابعة للدرك الوطني[2] :

1. الوحدات الإقليمية:
   أ. مسؤولة عن حفظ النظام العام ومراقبة المناطق الريفية والحضرية.
   ب. تتولى التحقيق في الجرائم المحلية والتنسيق مع السلطات القضائية.
2. الوحدات المتخصصة:
   أ. تشمل فرق مكافحة الجرائم السيبرانية، التي تعمل على كشف الجرائم الرقمية وتتبع مرتكبيها.
   ب. فرق مكافحة الإرهاب، التي تتعاون مع الأجهزة الأمنية الأخرى لضمان الأمن الوطني.
3. وحدات الإسناد:
   أ. توفر الدعم اللوجستي والتقني للوحدات الأخرى، بما في ذلك المعدات الحديثة للتحقيقات.
   ب. تشمل فرق التدخل السريع التي تتعامل مع الحالات الطارئة.
4. المصالح والمراكز العلمية والتقنية:
   أ. تضم مختبرات الأدلة الجنائية الرقمية، حيث يتم تحليل البيانات الإلكترونية المرتبطة بالجرائم.
   ب. توفر التدريب والتطوير المستمر لأفراد الدرك في مجال التحقيقات الرقمية.
5. المفرزة الخاصة للتدخل :
   أ. وحدة متخصصة في التعامل مع الحالات الأمنية الحرجة، مثل احتجاز الرهائن أو العمليات الخاصة.
   ب. تعمل وفق بروتوكولات دقيقة لضمان تنفيذ المهام بكفاءة وسرعة.

هذه الوحدات تلعب دورًا أساسيًا في تعزيز الأمن الوطني، سواء من خلال التحقيقات الجنائية التقليدية أو عبر مكافحة الجرائم السيبرانية الحديثة.

المطلب الثاني : آليات مواجهة تحديات التعاون الدولي في مكافحة الجرائم المعلوماتية على المستوى الدولي

أضحت الجرائم المعلوماتية في ظل الثورة الرقمية من أخطر صور الإجرام المعاصر، لما تتسم به من طبيعة عابرة للحدود وصعوبة في الكشف والإثبات، وقد أفرز هذا الواقع تحديات جمة أمام التعاون الدولي في المجال الجنائي، لعل أبرزها التباين التشريعي بين الدول في تعريف الجريمة المعلوماتية وتكييفها القانوني،

[1] عمار حشمان، مرجع سابق، ص44-45.

[2] وزارة الدفاع الوطني الجزائرية، الدرك الوطني – التنظيم والمهام، https://www.mdn.dz/site_cgn/sommaire/presentation/org_missions/org_missions_ar.php ، 2025/05/25، 18:57.

وتضارب الاختصاص القضائي بشأن ملاحقة مرتكبيها، فضلاً عن تمسك بعض الدول بمبدأ السيادة الوطنية بما يحدّ من فعالية تبادل المعلومات والأدلة.

كما أن بطء آليات المساعدة القضائية التقليدية لا ينسجم مع السرعة الفائقة التي تُرتكب بها هذه الجرائم إضافة إلى ما تطرحه من صعوبات تقنية متعلقة بالتشفير وإخفاء الهوية، وتفاوت القدرات بين الدول المتقدمة والنامية في مجال التحقيق الرقمي[1].

يُشكّل اختلاف الأنظمة القانونية والإجرائية بين الدول عائقًا بارزًا أمام فعالية مكافحة الجرائم الإلكترونية إذ إن اعتماد كل دولة لنهج خاص في التعامل مع هذه القضايا يؤدي إلى صعوبات في تنسيق التحقيقات وتنفيذ الأحكام، ومن هنا تبرز الحاجة إلى وضع معايير قانونية موحّدة تنظم آليات التحقيق، إلى جانب تطوير منصات مشتركة لتبادل الأدلة الرقمية بسهولة وسرعة، مع إبرام اتفاقيات دولية تحدد إجراءات معيارية واضحة تعزز التعاون بين السلطات القضائية وتزيد من فاعلية الإجراءات القانونية.

وفي السياق ذاته، يُعد تنازع الاختصاص القضائي من أبرز الإشكاليات نظرًا للطبيعة العابرة للحدود للجرائم المعلوماتية وما تثيره من تساؤلات حول الجهة المخوّلة بالمحاكمة، الأمر الذي يستدعي اعتماد مبادئ قانونية دقيقة تحدد صلاحيات الدول في التحقيق والملاحقة، مع إمكانية إنشاء هيئات قضائية دولية متخصصة، إضافةً إلى تعزيز التنسيق بين أجهزة إنفاذ القانون عبر منصات تعاون دولية للحد من النزاعات القضائية وتسهيل اتخاذ الإجراءات المناسبة[2].

ومن الجوانب المهمة أيضًا، نقص التدريب المتخصص في مجال الجرائم المعلوماتية، إذ تحتاج التحقيقات في هذا النوع من الجرائم إلى مهارات دقيقة في تحليل الأدلة الرقمية وفهم الأساليب المستخدمة من قبل المجرمين السيبرانيين، لمواجهة هذا التحدي، ينبغي توفير برامج تدريبية مستمرة لمتخصصي إنفاذ القانون، بالإضافة إلى تشجيع التعاون بين المؤسسات الأكاديمية والهيئات القضائية لتطوير المعرفة القانونية والتقنية في هذا المجال، تبادل الخبرات بين الدول يعد عاملاً جوهريًا لتعزيز كفاءة العاملين في مكافحة الجرائم الإلكترونية[3].

ولمواجهة هذه الإشكالات، برزت عدة آليات قانونية ومؤسساتية، من أهمها السعي إلى توحيد التشريعات الوطنية عبر الانضمام إلى الاتفاقيات الدولية ذات الصلة، وفي مقدمتها اتفاقية بودابست* لسنة 2001 بشأن

---

[1] ناشف فريد، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 8، العدد ، 2022، ص436،442.

[2] وريدة جندلي، التعاون الدولي لمكافحة الجريمة المعلوماتية : الفاعلية و التحديات، مجلة القانون و العلوم السياسية، المجلد 10 العدد 02، 2024، ص323،327.

[3] وريدة جندلي، مرجع سابق، ص328-331.

* اتفاقية بودابست (اتفاقية مجلس أوروبا بشأن الجرائم المعلوماتية) هي أول وأهم صك دولي ملزم في مجال مكافحة الجرائم الإلكترونية، تم اعتمادها في 23 نوفمبر 2001 بمدينة بودابست (المجر)، ودخلت حيّز النفاذ في 1 يوليو 2004.

الجرائم المعلوماتية، وتبسيط إجراءات المساعدة القانونية المتبادلة بما يضمن سرعة وفعالية التعاون، كما تم اعتماد شبكات اتصال دائمة (7/24) لتبادل المعلومات التقنية بصورة عاجلة، وتعزيز الثقة المتبادلة من خلال إبرام اتفاقيات ثنائية ومتعددة الأطراف تكفل سرية البيانات المتبادلة.

وإلى جانب ذلك، يبرز دور برامج التدريب وبناء القدرات للدول الأقل تجهيزاً، وتشكيل فرق تحقيق مشتركة لملاحقة الجرائم العابرة للحدود، فضلاً عن تحديث آليات تسليم المجرمين لتشمل الجرائم المعلوماتية صراحة مع إشراك القطاع الخاص، ولا سيما مزوّدي خدمات الإنترنت وشركات التكنولوجيا، في جهود الكشف والتبليغ[1]، وعليه، فإن معالجة التحديات التي تعترض التعاون الدولي في مكافحة الجرائم المعلوماتية تقتضي تكاملاً بين الجهود التشريعية والمؤسساتية والتقنية، بما يحقق التوازن بين مقتضيات السيادة الوطنية ومتطلبات العدالة الجنائية الدولية، ويضمن حماية فعّالة للأمن الرقمي العالمي.

الفرع الاول : آلية مواجهة تحدي القصور التشريعي للدول والتعارض بين مصالحها

أولا: القصور التشريعي

يرى الفقه الدستوري أنّ من واجب القاضي الدستوري مراجعة قصور المشرع في تنظيم بعض القضايا التي يفرض الدستور تنظيمها، باعتبار أنّ النص الدستوري يسمو على باقي التشريعات، لا تقتصر رقابة القاضي الدستوري على مطابقة القوانين لأحكام الدستور فحسب، بل تمتد إلى فحص السلوك التشريعي الإيجابي حيث يؤدي تقاعس المشرع عن سنّ قوانين ضرورية إلى خلق فراغ قانوني قد تستغله السلطة التنفيذية، مما يؤدي إلى تداخل الاختصاصات[2].

يقصد بالقصور التشريعي عدم كفاية النص القانوني لمعالجة المسألة التي ينظمها، سواء من حيث الشمولية أو الفاعلية، إذ قد يضع المشرع قانونًا لكنه يعالجه بصورة سطحية دون التعمق في كافة جوانبه، في مثل هذه الحالات، يلجأ القاضي إلى استخدام أدوات قانونية أخرى، مثل القياس والمبادئ العامة للقانون لضمان تحقيق العدالة وإكمال التنظيم القانوني.

يعرَّف القصور التشريعي بأنه وجود ثغرات في النظام القانوني تعيق تطبيق القانون بالشكل المطلوب، إمّا بسبب عدم وجود قاعدة قانونية تحكم قضية معينة، أو نتيجة لعدم امتثال المشرع لالتزام دستوري صريح يفرض عليه التدخل لتفعيل النصوص الدستورية، لهذا، يُعد استنفاذ المشرع لاختصاصه التشريعي أمرًا ضروريًا، إذ يجب عليه التدخل كلما اقتضت المصلحة العامة ذلك، مع مراعاة عدم تفويض اختصاصاته للسلطة التنفيذية إلا وفق ما يحدده الدستور .

عندما يكون القصور التشريعي جزئيًا، أي أنّ القانون يعالج القضية لكن بصورة غير كافية، فقد يكون بالإمكان الطعن في دستورية النص القانوني بسبب عدم استيفائه لمتطلبات التشريع المنسجم مع الدستور وهذا

[1] ناشف فريد، مرجع سابق، ص442،447.

[2] محمد نجم محسن، دور القاضي الدستوري في إصلاح القصور التشريعي، المجلة القانونية(مجلة متخصصة في الدراسات و البحوث القانونية)، المجلد 03 العدد 09، 2021، ص921،922.

ينطبق سواء كان القصور ناتجًا عن إغفال مقصود من المشرع أو عن خطأ في التقدير، إذ أنّ المشكلة ليست في نية المشرع، بل في عدم شمولية القانون لجميع الجوانب اللازمة لتنظيم المسألة المطروحة .

يتفق بعض الفقهاء الدستوريين على أنّ القصور التشريعي يتمثل في عدم قيام المشرع بتنظيم بعض الجوانب التي كفلها الدستور، سواء بسبب الإهمال أو سوء تقدير المسألة المطروحة، يميز بعض الفقهاء بين إساءة استعمال السلطة التشريعية، وهو تصرف مقصود يتعارض مع المصلحة العامة، وبين أخطاء التشريع الناتجة عن سوء فهم الواقع القانوني، والتي تؤدي إلى فراغ تشريعي غير متعمد[1].

يُعد دور القاضي الدستوري في معالجة الفراغ التشريعي جوهريًا، حيث يتحتم عليه إعلان وجود مخالفة دستورية تستوجب تدخل المشرع لسدّ الفجوة القانونية، القاضي، بصفته حاميًا للدستور، يضطلع بمهمة تفسير النصوص الدستورية وتقييم مدى التزام المشرع بأحكامها، بحيث يختار الحل القانوني الذي يحافظ على المشروعية الدستورية ويضمن حماية المجتمع من الأزمات القانونية الناتجة عن نقص التشريع.

في ظل هذه التطورات، أصبح القضاء لا يقتصر دوره على مراقبة القوانين، بل بات يساهم في تصحيح العمل التشريعي، حيث يتدخل لإلزام المشرع بسنّ قوانين ضرورية لاستكمال التنظيم القانوني للحقوق، هذا التحول يعكس تطورًا في وظيفة القضاء، حيث أصبح يمارس دورًا فعالًا في ضمان اتساق التشريعات مع الدستور، مما يعزز التوازن بين السلطات ويحد من المشكلات القانونية التي قد تنشأ بسبب قصور التشريع[2].

ثانيا: آلية مواجهة تحدي القصور التشريعي للدول والتعارض بين مصالحها

لمواجهة القصور التشريعي الذي تعاني منه بعض الدول في مجال مكافحة الجرائم الإلكترونية، لا بد من إيجاد حلول فعالة تقلل من الفجوات القانونية وتتيح تنسيقًا أفضل بين الأنظمة التشريعية المختلفة، بالنظر إلى تعارض المصالح بين الدول، يصبح من الضروري اعتماد إجراءات قانونية موحدة أو على الأقل متقاربة لضمان عدم استغلال الفروقات التشريعية من قبل المجرمين السيبرانيين الذين يلجؤون إلى الدول ذات القوانين الأكثر تساهلًا للإفلات من العقاب[3].

1. توحيد النظم القانونية عبر الاتفاقيات الدولية

يُعد توحيد النظم القانونية للدول في مجال الجرائم الإلكترونية من الحلول المثالية، إلا أنه يصطدم بصعوبات كبيرة بسبب اختلاف التشريعات الداخلية لكل دولة، لذا، فإن إبرام الاتفاقيات الدولية والإقليمية يُعد البديل الأكثر

[1] محمد نجم محسن، مرجع سابق، ص923.

[2] محمد نجم محسن، مرجع سابق، ص 923-924.

[3] فيروز العوض الكريم صالح، دور التعاون الدولي في مكافحة الجريمة الإلكترونية، مجلة جامعة شندي للبحوث و الدراسات الشرعية و القانونية، العدد التاسع، 2023، ص117-118.

واقعية، حيث توفر هذه الاتفاقيات إطارًا قانونيًا مشتركًا يُسهل التعاون بين الدول ويساعد على التغلب على العراقيل القانونية، مما يؤدي إلى تعزيز فعالية مكافحة هذه الجرائم وتوحيد الجهود الدولية[1].

2. تقليل الفوارق بين الأنظمة الجنائية الداخلية

يرتكز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية على تقليص الفوارق بين الأنظمة الجنائية، حيث يبحث المجرمون السيبرانيون عن الثغرات القانونية التي تسمح لهم بممارسة أنشطتهم دون مواجهة عواقب قانونية لذلك، فإن تقارب الأنظمة التشريعية بين الدول يساعد على الحد من هذه الظاهرة، ويمنع مرتكبي الجرائم من التنقل بين الدول بحثًا عن قوانين أكثر تساهلًا، هذا التقارب يساهم أيضًا في رفع مستوى الحماية القانونية ضد الجرائم الإلكترونية ويضمن تطبيق العدالة على الصعيد الدولي[2].

3. تدويل القانون الجنائي وتوحيد الإجراءات القضائية

إنّ التعاون الدولي في مجال مكافحة الجرائم الإلكترونية يمثل خطوة نحو تدويل القانون الجنائي، من خلال وضع قواعد موضوعية وإجرائية موحدة تُسهل تنفيذ التشريعات عبر الحدود، تُعد هذه الخطوة من التدابير الأساسية لمنع الجريمة، إذ تعمل على إحاطة المتهمين بسياج قانوني دولي يحول دون إفلاتهم من المسؤولية الجنائية والعقوبات المترتبة على أفعالهم غير المشروعة[3].

4. التنسيق بين التشريعات لضمان ملاحقة المجرمين

تعتبر مواءمة القوانين الوطنية أحد المحاور الأساسية لتفعيل التعاون الدولي في مكافحة الجرائم الإلكترونية حيث يجب أن تكون التشريعات متسقة بحيث لا يكون الفعل معاقبًا عليه في دولة ومباحًا في دولة أخرى يتطلب هذا التنسيق أن تقوم الدول بتحديث قوانينها الوطنية بما يضمن الحد الأدنى من التوافق مع المعايير الدولية، مما يساعد على سد الفجوات القانونية وتحقيق ملاحقة فعالة للمجرمين السيبرانيين أينما وجدوا.

5. إصلاح التشريعات الإجرائية لمواكبة التطورات التقنية

نظرًا لتنوع النظم الإجرائية بين الدول، بدأت العديد من الحكومات في إصلاح قوانينها الجنائية لتتماشى مع تطورات الجرائم الإلكترونية، وذلك عبر دمج التطبيقات الرقمية الحديثة في مجال الإجراءات القضائية، مما يتيح إمكانية تتبع الجرائم الإلكترونية بشكل أكثر كفاءة ودقة، هذا الإصلاح يشمل تعديل القوانين المتعلقة

---

[1] ياكر الطاهر، "مكافحة الجرائم الإلكترونية بين التشريعات الوطنية والاتفاقيات الدولية"، مجلة الصدى للدراسات القانونية والسياسية، كلية الحقوق و العلوم السياسية، جامعة الجيلالي بونعامة خميس مليانة، المجلد 4، العدد 4، 2022، الصفحات 20-24.

[2] مراد ماشوش، "الجهود الدولية لمكافحة الإجرام السيبراني"، مجلة القانون والأعمال الدولية، 22 مايو 2018 https://www.droitetentreprise.com/الجهود-الدولية-لمكافحة-الإجرام-السيب/ ، 2025/05/25 ، 20:16.

[3] مراد ماشوش، "الجهود الدولية لمكافحة الإجرام السيبراني"، مجلة القانون والأعمال الدولية، 22 مايو 2018 https://www.droitetentreprise.com/الجهود-الدولية-لمكافحة-الإجرام-السيب/ ، 2025/05/25 ، 20:48.

بالتحقيقات الجنائية، بحيث تكون قادرة على التعامل مع الجرائم السيبرانية بفعالية، من خلال السماح باستخدام الأدلة الرقمية وتقنيات التحري الحديثة التي تتيح تتبع النشاط الإجرامي عبر الإنترنت[1].

6. استخدام الاتفاقيات الدولية لتنسيق الإجراءات القانونية

لقد أبرمت العديد من الدول اتفاقيات دولية تهدف إلى التقريب بين القوانين الجنائية الوطنية لمكافحة الجرائم العابرة للحدود، يُعد هذا التعاون أحد أكثر الحلول العملية لمواجهة التناقض بين التشريعات، حيث يسمح للدول بتبادل المعلومات وإجراء التحقيقات المشتركة، مما يعزز مكافحة الجرائم الإلكترونية بشكل أكثر كفاءة. يتجلى هذا التقارب القانوني في قبول تفويض الاختصاص في إجراءات التحري وجمع الأدلة، مما يساعد سلطات التحقيق على تجاوز العقبات المرتبطة بالحدود القانونية بين الدول[2].

7. التوصيات الأوروبية بشأن تطوير الإجراءات الجنائية

بسبب التطور السريع في مجال تكنولوجيا المعلومات، أدركت العديد من الدول الأوروبية ضرورة مراجعة الإجراءات الجنائية لتتماشى مع تطورات العصر الرقمي، وقد أصدر المجلس الأوروبي التوصية رقم 95/13 لعام 1995، التي تهدف إلى توجيه الدول نحو تعديل قوانينها الإجرائية الوطنية لمواكبة تطورات الجرائم الإلكترونية. تضمنت هذه التوصية مجموعة من التدابير المهمة، منها[3]:

أ. تحديد إجراءات تفتيش أجهزة الحاسوب وضبط المعلومات المخزنة فيها وفقًا للقواعد القانونية.

ب. السماح بضبط البرامج والمعلومات الرقمية بنفس القواعد المتبعة في عمليات التفتيش التقليدية، مع إخطار الجهات المسؤولة.

ج. تمكين جهات التحقيق من توسيع نطاق التفتيش ليشمل الأجهزة المرتبطة بالنظام محل التفتيش شريطة إثبات الضرورة القانونية لذلك.

د. إقرار إجراءات مراقبة وتسجيل إلكتروني للتحري، مع إلزام المؤسسات الحكومية بالتعاون مع سلطات التحقيق.

هـ. منح سلطات التحري صلاحية توجيه أوامر للجهات المالكة للمعلومات للسماح بالاطلاع على البيانات المخزنة ضمن الأنظمة المعلوماتية.

و. توحيد أنظمة التعاون مع الأدلة الإلكترونية لضمان الاعتراف بها بين الدول المختلفة.

ز. إنشاء وحدات خاصة لمكافحة الجرائم الإلكترونية، مع تطوير الكوادر البشرية في المجال الرقمي.

---

[1] بن فرحات نور الدين، وعمري عبد القادر، "الطابع العابر للحدود للجرائم الإلكترونية وأثره على عمليات التحقيق الجنائي" مجلة الباحث السياسي والقانوني، جامعة يحيى فارس المدية، المجلد 9، العدد 9، 2024، الصفحات 666–671.

[2] وزارة العدل الجزائرية، المعاهدات والاتفاقيات الدولية، https://www.mjustice.dz/ar/conventions-internationaux-2-2/ ، 2025/05/26 ، 9:28.

[3] **Council of Europe.** *Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology*. Adopted 11 September 1995, https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-no-r-95-13 , 26/05/2025 , 10:21.

ح. إقرار آليات تتيح توسيع نطاق التحقيقات الرقمية لتشمل أنظمة كمبيوتر في دول أخرى، وفقًا لاتفاقيات دولية تحدد كيفية تنفيذ هذا الإجراء.

8. التحقيق الرقمي العابر للحدود وأهميته في مكافحة الجرائم الإلكترونية

نظرًا للطبيعة العابرة للحدود للجرائم الإلكترونية، أصبح من الضروري وضع إطار قانوني مشترك يسمح للدول بتبادل المعلومات الإلكترونية وإجراء التحقيقات الجنائية بطريقة سلسة وفعالة. هذه الآليات تساعد في تعزيز التعاون القضائي بين الدول، وتتيح ملاحقة المجرمين السيبرانيين دون التعرض لعوائق قانونية، إنّ تطوير التعاون الدولي في مجال التحقيقات الرقمية لا يسهم فقط في تحقيق العدالة الجنائية، بل يعزز أيضًا قدرة الدول على مكافحة الجرائم الإلكترونية بفاعلية أكبر، مما يجعل البيئة الرقمية أكثر أمنًا واستقرارًا.

بهذه الحلول، يمكن الحد من القصور التشريعي بين الدول وضمان استجابة أكثر كفاءة في التحقيقات الجنائية الرقمية، مما يعزز التعاون الدولي في مواجهة التحديات القانونية المرتبطة بالجرائم الإلكترونية[1].

الفرع الثاني: آلية مواجهة تحدي تنوع واختلاف النظم القانونية الإجرائية

أولا: تنوع واختلاف النظم القانونية الإجرائية

يرجع إلى عدة عوامل رئيسية تؤثر على كيفية تطبيق القوانين وتنفيذ الأحكام القضائية بين الدول المختلفة[2].

أحد الأسباب الأساسية لهذا التنوع هو اختلاف التقاليد القانونية، حيث يعتمد بعض الدول على النظام القانوني الأنجلوسكسوني الذي يقوم على السوابق القضائية، بينما تتبنى دول أخرى النظام القانوني اللاتيني الذي يعتمد على التشريعات المكتوبة كأساس للقرارات القضائية، هذا الاختلاف ينعكس مباشرة على كيفية إدارة القضايا القانونية، إذ أنّ بعض الدول تعتمد على تفسير القضاة للنصوص القانونية وفقًا للسوابق، بينما تعتمد دول أخرى على تطبيق القوانين وفقًا لنصوص محددة مسبقًا.

سبب آخر لهذا التنوع هو السيادة الوطنية، حيث تسعى كل دولة إلى الحفاظ على استقلالها القانوني، مما يؤدي إلى وضع إجراءات قضائية تتناسب مع سياساتها الداخلية، بما في ذلك القوانين المتعلقة بالتحقيقات المحاكمات، وتنفيذ الأحكام، بالإضافة إلى ذلك، يلعب التطور التشريعي دورًا مهمًا في اختلاف النظم القانونية الإجرائية، إذ أنّ بعض الدول تقوم بتحديث قوانينها بانتظام لمواكبة التغيرات التكنولوجية والاجتماعية، في حين أنّ دولًا أخرى لا تزال تعتمد على تشريعات قديمة قد لا تكون ملائمة للمتغيرات القانونية الحديثة.

---

[1] Free Tech ، "التعاون الدولي في مكافحة الجرائم السيبرانية: التحديات والفرص"، 2025، https://freetech.tech/information-security-essentials/التعاون-الدولي-في-مكافحة-الجرائم-السي/ ، 2025/05/26 ، 11:34.

[2] أنس المعولي، الفرق بين النظامين الانجلوساكسوني الانجليزي و النظام المدني اللاتيني، مجموعة نون العلمية، 2019/08/16، مجموعة نون العلمية – الفرق بين النظامين الأنجلوسكسوني/الانجليزي (Common Law) والنظام المدني/ اللاتيني (Civil Law) ، 2025/05/26 ، 13:37.

الاختلافات الثقافية والاجتماعية تؤثر أيضًا على كيفية صياغة القوانين الإجرائية في كل دولة، حيث تعكس القوانين القيم الأخلاقية والمعايير الاجتماعية السائدة، مما يؤدي إلى اختلاف في كيفية التعامل مع القضايا القانونية مثل الجرائم الإلكترونية أو القوانين التجارية، هذه الفروقات قد تسبب تحديات في التعاون القانوني الدولي، خاصة في القضايا العابرة للحدود التي تستلزم تنسيقًا بين الأنظمة القانونية المختلفة[1].

ثانيا: المشاكل والعوائق الناتجة عن اختلاف النظم القانونية الإجرائية[2]

1. التضارب في القوانين بين الدول

أ. كل دولة تضع تشريعاتها وفقًا لاحتياجاتها الداخلية، مما يؤدي إلى اختلاف الإجراءات القانونية خاصة في المسائل الجنائية مثل تسليم المجرمين أو التعامل مع الأدلة الرقمية.

ب. بعض الدول تعتبر أفعالًا معينة جرائم جنائية، بينما تكون نفس الأفعال قانونية في دول أخرى، مما يجعل ملاحقة المتهمين أمرًا معقدًا.

2. صعوبات تنفيذ الأحكام القضائية عبر الحدود

أ. تنفيذ الأحكام في دولة أخرى يتطلب توافقًا قانونيًا بين الأنظمة القضائية، وهو أمر غير متوفر دائمًا بسبب اختلاف القواعد الإجرائية.

ب. بعض الدول ترفض الاعتراف بالأحكام الصادرة من محاكم دول أخرى، خاصة عندما تكون هناك فروقات كبيرة في المعايير القانونية.

3. العوائق في التحقيقات الجنائية الدولية

أ. اختلاف إجراءات التحري وجمع الأدلة بين الدول يؤدي إلى تعقيد التحقيقات في القضايا التي تشمل أكثر من دولة.

ب. تقنيات التحقيق الحديثة، مثل مراقبة الاتصالات أو التحليل الرقمي للبيانات، قد تكون مسموحة في بعض الدول ومحظورة في أخرى، مما يعطل سير التحقيقات.

4. تحديات تبادل المعلومات القانونية بين الدول

أ. بعض الدول تفرض قيودًا مشددة على تبادل البيانات القضائية لحماية خصوصية الأفراد، مما يعيق التعاون الدولي في مكافحة الجرائم.

ب. قوانين حماية البيانات تختلف بين الدول، مما يجعل الوصول إلى الأدلة والمعلومات القانونية أمرًا معقدًا.

---

[1] أنس المعولي، الفرق بين النظامين الانجلوساكسوني الانجليزي و النظام المدني اللاتيني، مجموعة نون العلمية، 2019/08/16، مجموعة نون العلمية – الفرق بين النظامين الأنجلوسكسوني/الانجليزي (Common Law) والنظام المدني/ اللاتيني (Civil Law)، 2025/05/26 ، 14:52.

[2] منقور قويدر، العوائق الاجرامية امام إعمال الطرق البديلة لحل النزاعات في المادة الادارية، مجلة القانون، العدد 5، 2015، ص29،32.

5. ضعف التنسيق بين الأنظمة القانونية الإجرائية

أ. غياب إطار قانوني موحد لمعاملة القضايا الجنائية والمدنية يؤدي إلى صعوبات في تحقيق العدالة الدولية.

ب. بعض الدول تشترط موافقات قانونية معقدة لتنفيذ إجراءات قضائية داخل أراضيها، مما يبطئ تنفيذ القوانين الدولية.

الفرع الثالث: آلية مواجهة تحدي تنازع الاختصاص القضائي الدولي

أولا : تنازع الاختصاص القضائي الدولي

وهي مشكلة قانونية تنشأ عندما تتداخل اختصاصات المحاكم في أكثر من دولة نتيجة لوجود عنصر أجنبي في النزاع. هذا التداخل يثير صعوبات في تحديد المحكمة المختصة وفقاً للقوانين المختلفة لكل دولة إذ تعتمد كل منها معايير خاصة بها لتحديد الاختصاص القضائي، مثل معيار جنسية الأطراف أو مكان وقوع الفعل أو محل إقامة المدعى عليه[1].

يعود السبب الرئيسي وراء هذا التنازع إلى تعدد الأنظمة القانونية، حيث تطبق كل دولة نظاماً قانونياً مستقلاً يؤدي إلى اختلاف المعايير المعتمدة لتحديد المحكمة المختصة، كما أنّ وجود طرف أجنبي أو ارتباط النزاع بأكثر من دولة يزيد من تعقيد المسألة، كذلك، يساهم التطور الاقتصادي والتجاري الدولي في حدوث هذا التداخل، حيث يؤدي انتشار الاستثمارات والمعاملات التجارية عبر الحدود إلى خلق حالات قضائية ذات طابع دولي تستدعي تدخل أكثر من نظام قانوني لحلها.

علاوة على ذلك، تختلف الدول في تفسيرها للاتفاقيات الدولية المنظمة للاختصاص القضائي، مما يؤدي إلى تضارب الآراء حول المحكمة المختصة بالنظر في القضايا العابرة للحدود، تنازع الاختصاص القضائي الدولي لا يقتصر فقط على تحديد المحكمة المختصة، بل يمتد تأثيره إلى القانون الواجب التطبيق على النزاع، وغالباً ما يكون القاضي أمام تحدي اختيار القانون الأنسب لتحقيق العدالة والإنصاف للأطراف[2].

يلعب عنصر السيادة الوطنية دوراً مهماً في هذا الإطار، حيث تسعى كل دولة إلى تطبيق قوانينها الداخلية كلما أمكن ذلك، كما أنّ تحقيق العدالة بين الأطراف يُعد معياراً أساسياً في اختيار القانون المناسب حيث يفضل القاضي تطبيق القانون الذي يتماشى مع طبيعة النزاع ويضمن حقوق جميع الأطراف، كذلك يمكن اللجوء إلى الأعراف القانونية الدولية والقرارات القضائية السابقة كمصادر استرشادية لتحديد القانون الواجب التطبيق.

[1] عبد الله فاضل حامد و جلال حسين عنز و هقال صديق اسماعيل، أثر الاختصاص القضائي الدولي في تحديد القانون الواجب التطبيق على العلاقات الخاصة الدولية "دراسة تحليلية" ، مجلة العلوم السياسية والقانون، مجلد 9، عدد 2، 2020 ص125،123.

[2] عبد الله فاضل حامد و جلال حسين عنز و هقال صديق اسماعيل، المرجع نفسه، ص 128،125.

إنّ هذا التنازع القضائي الدولي يمثل تحدياً رئيسياً أمام أنظمة القانون الدولي الخاص، حيث يتطلب وضع حلول منهجية متكاملة تستند إلى الاتفاقيات الدولية والمبادئ القانونية الموحدة لضمان تحقيق العدالة القانونية والتقليل من حالات التنازع التي قد تؤثر على سير العدالة في القضايا ذات الطابع الدولي[1].

ثانيا: آلية مواجهة تحدي تنازع الاختصاص القضائي الدولي

1. الآليات القانونية لمعالجة هذه المشكلة :

أ. توحيد القواعد القانونية عبر الاتفاقيات الدولية الاتفاقيات الدولية تلعب دورًا رئيسيًا في الحد من تنازع الاختصاص القضائي، حيث تضع معايير موحدة لتحديد المحكمة المختصة، من أبرز هذه الاتفاقيات اتفاقية بروكسل واتفاقية لاهاي، التي تهدف إلى توحيد القواعد القانونية بين الدول وضمان تطبيق العدالة[2].

ب. مبدأ الاختصاص الحصري بعض القضايا تتطلب أن يتم الفصل فيها أمام محاكم معينة مثل القضايا المتعلقة بالممتلكات غير المنقولة أو النزاعات التجارية الدولية، هذا المبدأ يساعد في تقليل حالات التنازع ويوفر وضوحًا قانونيًا للأطراف.

ج. مبدأ إرادة الأطراف يمكن للأطراف المتنازعة الاتفاق مسبقًا على المحكمة المختصة في العقود التجارية أو الاتفاقيات القانونية، مما يساهم في تقليل حالات التنازع ويوفر وضوحًا قانونيًا للأطراف.

د. تطبيق القانون الأكثر ارتباطًا بالنزاع يسعى القاضي إلى اختيار القانون الذي يحقق العدالة ويعكس طبيعة النزاع بشكل أفضل، حيث يتم اختيار القانون الذي يتماشى مع معايير العدالة والإنصاف مع مراعاة السيادة الوطنية لكل دولة.

هـ. الاعتراف المتبادل بالأحكام القضائية الاعتراف المتبادل بالأحكام القضائية بين الدول يسهل تنفيذ الأحكام ويقلل من حالات التنازع، حيث يتم الاعتراف بالأحكام الصادرة عن المحاكم الأجنبية وتنفيذها وفقًا للقواعد القانونية المتفق عليها.

و. إنشاء محاكم دولية مختصة في بعض الحالات، يمكن إنشاء محاكم دولية مختصة للنظر في النزاعات ذات الطابع الدولي، مثل محكمة العدل الدولية والمحكمة الجنائية الدولية، التي توفر إطارًا قانونيًا لحل النزاعات بين الدول والأفراد.

ز. تعزيز التعاون القضائي بين الدول التعاون القضائي بين الدول يساعد في تبادل المعلومات القانونية وتسهيل تنفيذ الأحكام القضائية، مما يساهم في الحد من تنازع الاختصاص القضائي الدولي.

2. تأثير هذه الآليات على تحقيق العدالة

تطبيق هذه الآليات القانونية يساعد في تحقيق العدالة وضمان سير التقاضي بسلاسة، حيث يتم تحديد المحكمة المختصة وفقًا لمعايير قانونية واضحة، مما يقلل من حالات التنازع ويضمن حقوق الأطراف المتنازعة، كما

[1] عبد الله فاضل حامد و جلال حسين عنز و هقال صديق اسماعيل، مرجع سابق، ص129.

[2] عبد الله فاضل حامد و جلال حسين عنز و هقال صديق اسماعيل، مرجع سابق، ص130.

أنّ توحيد القواعد القانونية عبر الاتفاقيات الدولية يسهم في تعزيز الثقة بين الدول ويقلل من حالات التضارب القانوني[1].

الفرع الرابع: آلية مواجهة التحدي الخاص في مجال التدريب

يواجه مجال التدريب العديد من التحديات التي تؤثر على جودة البرامج التدريبية ومدى تحقيقها للأهداف المرجوة، هذه التحديات قد تكون تخطيطية، فنية، اجتماعية أو نفسية، مما يستدعي تطوير استراتيجيات فعالة للتعامل معها وضمان نجاح العملية التدريبية[2].

1. التحديات التخطيطية والتنظيمية

تعد تخطيط البرامج التدريبية وتنظيم الجداول الزمنية من أبرز العقبات التي تواجه المؤسسات التدريبية من بين هذه التحديات[3]:

أ. ضعف تحديد احتياجات المتدربين، مما يؤدي إلى عدم توافق المحتوى التدريبي مع متطلباتهم.

ب. التوازن بين المحتوى النظري والتطبيق العملي، حيث يجب أن يكون هناك انسجام بين الجانبين لضمان الفهم والتطبيق الفعلي.

ج. التغيرات في احتياجات سوق العمل، مما يتطلب تحديث البرامج التدريبية باستمرار لتلبية المتطلبات الحديثة.

د. تنسيق الجداول الزمنية، حيث يجب مراعاة ظروف المتدربين وضمان استقرار الجدول دون تعارضات أو إلغاءات غير متوقعة.

2. التحديات الفنية[4]

تشمل التحديات الفنية في التدريب تصميم المحتوى التدريبي واستخدام التكنولوجيا التعليمية، من بين هذه التحديات:

أ. ابتكار محتوى جذاب وسلس، بحيث يكون مفهوماً ومتوازناً بين المعلومات والتفاعل.

ب. ضمان وصول فعال للتقنيات التعليمية، حيث يجب توفير الأدوات الرقمية المناسبة لدعم العملية التدريبية.

---

[1] عبد الله فاضل حامد و جلال حسين عنز و هقال صديق اسماعيل، مرجع سابق، ص130.

[2] كريم هدى، "التعامل مع التحديات التدريبية"، الهيئة العربية للمدربين، 27 ديسمبر 2023، التعامل مع التحديات التدريبية – الهيئة العربية للمدربين ، 2025/05/26 ، 15:29.

[3] كريم هدى، "التعامل مع التحديات التدريبية"، الهيئة العربية للمدربين، 27 ديسمبر 2023، التعامل مع التحديات التدريبية – الهيئة العربية للمدربين ، 2025/05/26 ، 16:02.

[4] كريم هدى، "التعامل مع التحديات التدريبية"، الهيئة العربية للمدربين، 27 ديسمبر 2023، التعامل مع التحديات التدريبية – الهيئة العربية للمدربين ، 2025/05/26 ، 16:39.

ج. التعامل مع الأجهزة والبرامج المعقدة، حيث قد يواجه المدربون صعوبة في استخدام التكنولوجيا الحديثة بشكل فعال.

3. التحديات الاجتماعية

أ. التحديات الاجتماعية تتعلق بالتفاعل بين المدرب والمتدربين، وتشمل:

ب. صعوبة فهم احتياجات المتدربين، حيث تختلف مستويات الفهم والخلفيات الثقافية.

ج. التأثيرات الثقافية واللغوية، التي قد تؤثر على تفاعل المتدربين واستيعابهم للمحتوى.

د. تنوع المجموعة التدريبية، حيث يجب على المدرب تعديل أساليبه لضمان استفادة جميع المشاركين.

4. التحديات النفسية

أ. التحديات النفسية تؤثر على تحفيز المتدربين والتعامل مع التوتر، ومن أبرزها:

ب. ضعف الدافعية لدى المتدربين، حيث قد يكون لديهم نقص في الاهتمام أو عدم رؤية الفوائد المستقبلية للتدريب.

ج. التوتر والضغط النفسي، الذي قد ينجم عن القلق بشأن الأداء أو الضغط الزمني.

د. التعامل مع الإجهاد العام، حيث يجب على المدربين توفير بيئة تدريبية محفزة تقلل من التوتر.

5. استراتيجيات التعامل مع التحديات التدريبية

أ. للتغلب على هذه التحديات، يمكن اعتماد عدة استراتيجيات، منها:

ب. تقييم احتياجات المتدربين لضمان توافق البرامج التدريبية مع متطلباتهم.

ج. توظيف التقنيات الحديثة مثل منصات التعلم الإلكتروني والوسائط المتعددة.

د. تبادل الخبرات والدروس المستفادة بين المدربين لتحسين جودة التدريب.

هـ. استشارة الخبراء والمتخصصين للحصول على دعم وإرشاد في حل التحديات التدريبية.

الفرع الخامس : آلية مواجهة التحديات الخاصة بالإنابة القضائية الدولية

تعد الإنابة القضائية الدولية إحدى أهم الوسائل القانونية التي تتيح التعاون بين الدول في المجال القضائي، حيث تمكن السلطات القضائية في دولة معينة من طلب تنفيذ إجراءات قضائية في دولة أخرى ومع تزايد الجرائم العابرة للحدود، أصبح من الضروري تطوير آليات فعالة للتغلب على التحديات التي تواجه الإنابة القضائية الدولية، سواء من حيث الإجراءات القانونية أو التعاون بين الدول[1].

أولا : التحديات التي تواجه الإنابة القضائية الدولية

تواجه الإنابة القضائية الدولية عدة تحديات تعيق فعاليتها، ومن أبرزها[2]:

[1] بن عودة نبيل، درعي لعربي، "الإنابات القضائية الدولية في المجال الجزائي"، مجلة القانون الدولي والتنمية، المجلد 7، العدد 2، 2019، ص. 139-144.

[2] بن عودة نبيل، درعي لعربي، نفس المرجع، ص145-154.

1. التعقيدات القانونية والإجرائية :تختلف القوانين والإجراءات القضائية بين الدول، مما يؤدي إلى صعوبات في تنفيذ الإنابات القضائية.
2. مبدأ السيادة الوطنية :بعض الدول تتردد في تنفيذ الإنابات القضائية الصادرة عن دول أخرى بسبب اعتبارات السيادة.
3. التأخير في تنفيذ الإنابات القضائية :قد تستغرق الإجراءات القضائية وقتًا طويلاً بسبب البيروقراطية أو عدم توفر الموارد اللازمة.
4. عدم وجود اتفاقيات دولية موحدة :عدم وجود إطار قانوني موحد لتنظيم الإنابة القضائية يؤدي إلى تضارب في تنفيذها بين الدول المختلفة.
5. التحديات التقنية :تشمل صعوبة تبادل المعلومات إلكترونيًا بين السلطات القضائية المختلفة، مما يؤثر على سرعة تنفيذ الإنابات القضائية.

ثانيا : آليات مواجهة هذه التحديات

لضمان فعالية الإنابة القضائية الدولية، يمكن اعتماد مجموعة من الآليات، منها[1]:

1. تعزيز التعاون الدولي عبر الاتفاقيات القضائية
   أ. توقيع اتفاقيات ثنائية ومتعددة الأطراف لتنظيم الإنابة القضائية.
   ب. توحيد الإجراءات القانونية بين الدول لضمان تنفيذ الإنابات القضائية بسلاسة.
2. تطوير البنية التحتية القضائية والتقنية
   أ. استخدام التكنولوجيا الحديثة لتسهيل تبادل المعلومات بين الدول.
   ب. إنشاء منصات إلكترونية مشتركة لتقديم طلبات الإنابة القضائية ومتابعتها.
3. تسريع الإجراءات القضائية
   أ. وضع جداول زمنية محددة لتنفيذ الإنابات القضائية.
   ب. تقليل البيروقراطية من خلال تبسيط الإجراءات القانونية.
4. تعزيز الثقة بين الدول
   أ. تحسين العلاقات الدبلوماسية والقضائية بين الدول لضمان تنفيذ الإنابات القضائية.
   ب. تعزيز التعاون بين السلطات القضائية عبر تبادل الخبرات والتدريب المشترك.
5. إصلاح التشريعات الوطنية
   أ. تعديل القوانين الداخلية للدول لتسهيل تنفيذ الإنابات القضائية.
   ب. اعتماد معايير قانونية موحدة تتماشى مع الاتفاقيات الدولية.

[1] بن عودة نبيل، درعي لعربي، نفس المرجع، ص155-160.

خلاصة

يُعد التعاون القضائي الدولي ركيزة أساسية في مواجهة الجرائم المعلوماتية، حيث يعتمد على مجموعة من الآليات القانونية لضمان ملاحقة المجرمين ومحاسبتهم، بغض النظر عن الحدود الجغرافية التي تفصل الدول، من بين هذه الآليات، يُعتبر تسليم المجرمين أداة قانونية فعالة، لكنه يواجه تحديات متعددة، مثل اختلاف التشريعات بين الدول، رفض بعض الدول تسليم مواطنيها لأسباب دستورية، وصعوبات في الإجراءات القانونية التي تؤدي إلى تأخير تنفيذ عمليات التسليم.

إلى جانب ذلك، تلعب المساعدة القضائية دورًا بارزًا في تبادل المعلومات القانونية بين الدول، مما يسهم في جمع الأدلة الضرورية، نقل الإجراءات القضائية إلى دولة أخرى عند الحاجة، وتنفيذ الأحكام وفقًا للقوانين الدولية المتفق عليها. الإنابة القضائية، باعتبارها أحد جوانب المساعدة القضائية، تُساعد في تنفيذ الإجراءات القانونية مثل استجواب الشهود وجمع الأدلة في دولة أخرى، مما يسهم في تعزيز فاعلية التعاون القانوني الدولي.

لمواجهة تحديات التعاون الدولي في مكافحة الجرائم المعلوماتية، ينبغي العمل على تطوير التشريعات الوطنية بما يتماشى مع المعايير العالمية، وتعزيز التنسيق بين المؤسسات القضائية لضمان استجابة قانونية سريعة ودقيقة، كما أنّ تحسين البنية التحتية الرقمية للأدلة الجنائية سيسهم في توفير وسائل فعالة للتعامل مع الجرائم السيبرانية داخل الدول.

على المستوى الدولي، يُعد توسيع نطاق الاتفاقيات الدولية لمكافحة الجرائم السيبرانية أحد الحلول الرئيسية، بالإضافة إلى إنشاء منصات إلكترونية آمنة لتبادل المعلومات القضائية بين الدول، كما أنّ تعزيز برامج التدريب المشترك بين الأنظمة القانونية المختلفة يُساعد على توحيد الجهود، مما يسهل التعاون القضائي ويوفر استجابة أكثر كفاءة لتطورات الجريمة المعلوماتية.

يتطلب التصدي الفعّال للجرائم المعلوماتية نهجًا شاملاً يجمع بين تحديث القوانين، تعزيز التعاون بين الدول، والاستفادة من التكنولوجيا لضمان تنفيذ العدالة بشكل فعال، من خلال هذه التدابير، يمكن تحقيق نظام قانوني أكثر كفاءة في مواجهة الجرائم المعلوماتية المتزايدة.

خاتمة

خاتمة

تعدّ الجريمة المعلوماتية أحد أبرز التحديات الأمنية والقانونية في العصر الرقمي، فهي تتجاوز الأطر التقليدية للجريمة من حيث الوسيلة والمجال، بل وتفرض نفسها بقوة على أجندة السياسات الدولية. وقد بيّن هذا البحث من خلال فصليه الأول والثاني أبعاد هذه الظاهرة وتعقيداتها، وسلط الضوء على الجهود الوطنية والدولية المبذولة للتصدي لها، مع تحليل فعالية الآليات الدولية المختلفة المعتمدة في هذا المجال.

يمكن القول إن دراسة الجريمة المعلوماتية تكتسي أهمية كبيرة، باعتبارها تسهم في تسليط الضوء على نمط جديد من الجرائم بدأ في الظهور والانتشار في العديد من المجتمعات. وتكمن خصوصية هذا النوع من الجرائم في ارتباطه الوثيق بالتكنولوجيا الحديثة، ما جعله يختلف عن الجرائم التقليدية سواء من حيث التسمية أو طبيعة الأفعال التي يندرج ضمنها.

وفي ضوء ما سبق، يمكن استخلاص النتائج التالية:

- إنّ مكافحة الجريمة المعلوماتية لم تعد خيارًا بل أصبحت ضرورة أمنية وقانونية واقتصادية
- إنّ مكافحة الجريمة المعلوماتية مسؤولية مشتركة تتطلب تفعيل آليات التعاون الدولي بشقيها القضائي والأمني، وتحديث المنظومات القانونية بما يتلاءم مع تحولات الفضاء الرقمي.
- إنّ نجاح الجهود الدولية يبقى مرهونًا بمدى قدرة الدول على تجاوز تحديات السيادة، الفروقات التقنية، وتباين النظم القانونية، نحو بناء جبهة قانونية دولية موحدة في مواجهة التهديدات السيبرانية
- الجهود التشريعية الجزائرية تظل بحاجة إلى مواكبة دورية للتطورات العالمية.

وعليه نقترح ما يلي:

- على الدولة الجزائرية تعزيز الخبرات التقنية، ومراجعة الإطار القانوني بشكل دوري، خاصة وأن التهديدات تتطور بوتيرة أسرع من قدرة التشريعات الوطنية على ملاحقتها.

ومن خلال النتائج الأخيرة المتوصل إليها من خلالها هذه الدراسة نقترح ما يلي:

- **الانضمام النشط لاتفاقية بودابست** من طرف جميع الدول، خاصة العربية، مع مواءمة التشريعات الوطنية مع نصوصها، لتعزيز التعاون القضائي والتقني الدولي.
- **إنشاء هيئة دولية مستقلة للجرائم المعلوماتية** تحت مظلة الأمم المتحدة، تجمع بين الخبرات القانونية، التقنية، والأمنية، وتعمل كمنسق عالمي في مكافحة هذا النوع من الجرائم.
- **تحديث التشريعات الوطنية** بما يراعي التطورات التقنية ويضع آليات واضحة للتجريم والعقاب والإثبات، وتدريب القضاة والضباط على تطبيقها.
- **تعزيز الثقافة القانونية الرقمية** عبر برامج توعية وطنية تستهدف الأفراد والمؤسسات، لتمكينهم من الوقاية والإبلاغ عن الجرائم الإلكترونية.

- **تطوير أدوات التحقيق الرقمي** وإنشاء مختبرات جنائية إلكترونية متطورة على المستوى الإقليمي بما يسمح باستخراج الأدلة الرقمية وفق معايير دولية.
- **إنشاء شبكة عربية للتحقيق الرقمي** تعمل على تنسيق الجهود بين الدول العربية وتبادل الخبرات والمعلومات حول الهجمات الإلكترونية.
- **تفعيل التعاون بين القطاع العام والخاص** خاصة مع شركات التكنولوجيا ومزودي خدمات الإنترنت للمساعدة في تتبع الأنشطة المشبوهة ودعم التحقيقات الجنائية.

الملاحق

الملحق رقم 1 القانون رقم 04/09

25 شعبان عام 1430 هـ
16 غشت سنة 2009 م

الجريدة الرّسميّة للجمهوريّة الجزائريّة / العدد 47

5

قوانين

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

إن رئيس الجمهورية،

– بناء على الدستور، لا سيما المواد 119 و120 و122 – 7 و126 منه،

– وبمقتضى الأمر رقم 66 – 155 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 66 – 156 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 75 – 58 المؤرّخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمن القانون المدني، المعدّل والمتمّم،

– وبمقتضى القانون رقم 2000 – 03 المؤرّخ في 5 جمادى الأولى عام 1421 الموافق 5 غشت سنة 2000 الذي يحدّد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 03 – 05 المؤرّخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003 والمتعلق بحقوق المؤلف والحقوق المجاورة،

– وبمقتضى القانون رقم 08 – 09 المؤرّخ في 18 صفر عام 1429 الموافق 25 فبراير سنة 2008 والمتضمن قانون الإجراءات المدنية والإدارية،

– وبعد رأي مجلس الدولة،

– وبعد مصادقة البرلمان،

يصدر القانون الآتي نصه :

الفصل الأول

أحكام عامة

الهدف

المادّة الأولى : يهدف هذا القانون إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

المصطلحات

المادّة 2 : يقصد في مفهوم هذا القانون بما يأتي :

أ – الجرائم المتصلة بتكنولوجيات الإعلام والاتصال : جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية،

ب – منظومة معلوماتية : أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين،

ج – معطيات معلوماتية : أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها،

د – مقدمو الخدمات :

1 – أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات،

2 – وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها،

هـ – المعطيات المتعلقة بحركة السير: أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة،

و – الاتصالات الإلكترونية : أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.

مجال التطبيق

المادّة 3 : مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

الفصل الثاني

مراقبة الاتصالات الإلكترونية

الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية

المادّة 4 : يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 أعلاه في الحالات الآتية :

أ – للوقاية من الأفعال الموصوفة بجرائم الإرهاب أوالتخريب أوالجرائم الماسةبالأمن الدولة،

ب – في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني،

ج – لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية،

د – في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة.

عندما يتعلق الأمر بالحالة المنصوص عليها في الفقرة "أ" من هذه المادة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 أدناه، إذنا لمدة ستة (6) أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

تكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الفقرة "أ" من هذه المادة موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتهما، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

الفصل الثالث

القواعد الإجرائية

تفتيش المنظومات المعلوماتية

المادّة 5 : يجوز للسلطات القضائية المختصة وكذا ضبّاط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه، الدخول، بغرض التفتيش، ولو عن بعد، إلى :

أ – منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب – منظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة "أ" من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها، انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

حجز المعطيات المعلوماتية

المادّة 6 : عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة

تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنـ ـومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللا مة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحرا وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في الهـ ومة المعلوماتية التي تجري بها العملية.

غير أنه يجو لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

الحجز عن طريق منع الوصول إلى المعطيات

المادّة 7 : إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 6 أعلاه، لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنـ ومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخ لهم باستعمال هذه الهـ ومة.

المعطيات المحجوزة ذات المحتوى المجرم

المادّة 8 : يمكن السلطة التي تباشر التفتيش أن تلأمر باتخاذ الإجراءات اللا مة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة ، لا سيما عن طريق تكليف أي شخ مؤهل باستعمال الوسائل التقنية المناسبة لذلك.

حدود استعمال المعطيات المتحصل عليها

المادّة 9 : تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجو استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية.

الفصل الرابع

التزامات مقدمي الخدمات

مساعدة السلطات

المادّة 10 : في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفـ ها وفقا للمادة 11 أدناه، تحت تصرف السلطات المذكورة.

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من ا ققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.

حفظ المعطيات المتعلقة بحركة السير

المادّة 11 : مع مراعاة طبيعة ونوعية الخدمات، يلتزم مقدمو الخدمات بحفـ :

أ – المعطيات التي تسمح بالتعرف على مستعملي الخدمة،

ب – المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال،

ج – الخصائ التقنية وكذا تاريخ ووقت ومدة كل اتصال،

د – المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها،

هـ – المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفـ المعطيات المذكورة في الفقرة "أ" من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه.

تحدد مدة حفـ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل.

دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخ الطبيعي بالحبس من ستة (6) أشهر إلى خمس (5) سنوات وبغرامة من 50.000 دج إلى 500.000 دج.

يعاقب الشخ المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات.

تحدد كيفيات تطبيق الفقرات 1 و2 و3 من هذه المادة، عند الحاجة، عن طريق التنظيم.

الالتزامات الخاصة بمقدمي خدمة "الإنترنت"

المادّة 12 : زيادة على الالتزامات المنصوص عليها في المادة 11 أعلاه، يتعين على مقدمي خدمات "الإنترنت" ما يأتي :

أ – التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن،

ب – وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى المعطيات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.

الفصل الخامس

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته

إنشاء الهيئة

المادّة 13 : تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم.

مهام الهيئة

المادّة 14 : تتولى الهيئة المذكورة في المادة 13 أعلاه، خصوصا المهام الآتية :

أ – تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته،

ب – مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية،

ج – تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.

الفصل السادس

التعاون والمساعدة القضائية الدولية

الاختصاص القضائي

المادّة 15 : زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني.

المساعدة القضائية الدولية المتبادلة

المادّة 16 : في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني.

يمكن، في حالة الاستعجال، ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى أعلاه، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أوالبريد الإلكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها.

تبادل المعلومات واتخاذ الإجراءات التحفظية

المادّة 17 : تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقات الدولية الثنائية ومبدأ المعاملة بالمثل.

القيود الواردة على طلبات المساعدة القضائية الدولية

المادّة 18 : يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أوالنظام العام.

يمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب.

المادّة 19 : ينشر هذا القانون في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009.

عبد العزيز بوتفليقة

الملحق رقم 2 القانون رقم 06/01

" الجمهوريّة الجزائريّة الدّيمقراطية الشّعبيّة باسم الشّعب الجزائري".

وتنتهي بالصيغة الآتية :

" وبناء على ما تقدّم فإنّ الجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة تدعو وتأمر جميع أعوان التّنفيذ إذا طلب إليهم ذلك، تنفيذ هذا (القرار، الحكم...) وعلى النواب العامين ووكلاء الجمهورية لدى المحاكم مدّ يد المساعدة اللاّزمة لتنفيذه، وعلى جميع قادة وضباط القوّة العموميّة تقديم المساعدة اللاّزمة لتنفيذه بالقوّة عند الاقتضاء، إذا طلب إليهم ذلك بصفة قانونية،

وبناء عليه وقع هذا الحكم ".

وفي القضايا الإدارية تكون الصيغة التنفيذية على الوجه الآتي :

" الجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة تدعو وتأمر الوزير أو الوالي أو رئيس المجلس الشّعبي البلدي، كلّ فيما يخصّه، وتدعو وتأمر كلّ أعوان التّنفيذ المطلوب إليهم ذلك فيما يتعلّق بإجراءات القانون العام في مواجهة الأطراف الخصوصيّين أن يقوموا بتنفيذ هذا القرار".

" *المادّة 324* : جميع الأحكام والقرارات القضائية قابلة للتّنفيذ في كل أنحاء الأراضي الجزائرية.

ولأجل التّنفيذ الجبري للأحكام والقرارات يطلب قضاة النيابة العامّة مباشرة استعمال القوّة العموميّة، ويشعر الوالي بذلك.

وعندما يكون التّنفيذ من شأنه الإخلال بالنّظام العام إلى درجة الخطورة، يمكن الوالي وبطلب مسبّب يقدّمه في أجل ثلاثين (30) يوما من تاريخ إشعاره أن يلتمس التّوقيف المؤقّت لمدّة أقصاها ثلاثة (3) أشهر ".

المادّة 3 : ينشر هذا القانون في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 28 صفر عام 1422 الموافق 22 مايو سنة 2001.

عبد العزيز بوتفليقة

قانون رقم 01 - 06 مؤرّخ في 28 صفر عام 1422 الموافق 22 مايو سنة 2001، يعدّل ويتمّم الأمر رقم 71 - 57 المؤرّخ في 14 جمادى الثّانية عام 1391 الموافق 5 غشت سنة 1971 والمتعلّق بالمساعدة القضائيّة.

إنّ رئيس الجمهوريّة،

- بناء على الدّستور، لاسيّما المواد 119و120و122 و126 و151 منه،

- وبمقتضى الأمر رقم 65 - 278 المؤرّخ في 22 رجب عام 1385 الموافق 16 نوفمبر سنة 1965 والمتضمّن التّنظيم القضائي،

- وبمقتضى الأمر رقم 66 - 154 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966والمتضمّن قانون الإجراءات المدنيّة، المعدّل والمتمّم،

- وبمقتضى الأمر رقم 66 - 155 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمّن قانون الإجراءات الجزائيّة، المعدّل والمتمّم،

- وبمقتضى الأمر رقم 66 - 156 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمّن قانون العقوبات، المعدّل والمتمّم،

- وبمقتضى الأمر رقم 71 - 57 المؤرّخ في 14 جمادى الثانية عام 1391 الموافق 5 غشت سنة 1971 والمتعلّق بالمساعدة القضائية،

- وبمقتضى القانون رقم 84 - 17 المؤرّخ في 8 شوال عام 1404 الموافق 7 يوليو سنة 1984 والمتعلّق بقوانين المالية، المعدّل والمتمّم،

- وبمقتضى القانون رقم 91 - 04 المؤرّخ في 22 جمادى الثانية عام 1411 الموافق 8 يناير سنة 1991 والمتضمّن تنظيم مهنة المحاماة،

- وبعد مصادقة البرلمان،

يصدر القانون الآتي نصّه :

المادّة الأولى : يعدّل هذا القانون ويتمّم الأمر رقم 71 - 57 المؤرّخ في 14 جمادى الثانية عام 1391 الموافق 5 غشت سنة 1971 والمتعلّق بالمساعدة القضائية.

المادّة 2 : تعدّل المادّة 25 من الأمر رقم 71 - 57 المؤرّخ في 14 جمادى الثانية عام 1391 الموافق 5 غشت سنة 1971 والمذكور أعلاه، وتحرّر كما يأتي :

" *المادّة 25* : يتمّ تعيين محام مجانا في الحالات الآتية :

1 - لجميع القصّر الماثلين أمام قاضي الأحداث أو محكمة الأحداث أو أيّة جهة جزائية أخرى،

2 - للمتّهم الذي يطلبها أمام قاضي التّحقيق أو المحكمة التي تفصل في مواد الجنح،

3 - للطاعن بالنّقض إذا طلبها أمام الغرفة الجنائية بالمحكمة العليا عندما تتجاوز العقوبة المحكوم بها عليه خمس (5) سنوات سجنا نافذة،

4 - إذا كان المتّهم مصابا بعاهة من شأنها أن تؤثّر على دفاعه،

5 - للمتّهم الذي يطلبها أمام محكمة الجنايات مع مراعاة أحكام المادّة 29 مكرّر أدناه".

المادّة 3 : يتمّم الأمر رقم 71 - 57 المؤرّخ في 14 جمادى الثانية عام 1391 الموافق 5 غشت سنة 1971 والمذكور أعلاه ، بباب رابع مكرّر، يتضمّن المادّة 29 مكرّر، يحرّر كما يأتي :

" **الباب الرابع مكرّر**

المساهمات المالية المخصّصة للمساعدة القضائية

المادّة 29 مكرّر : يتقاضى المحامي المكلّف بالمساعدة القضائية في المواد المدنيّة ، وكذا في حالة التّعيين التلقائي أمام محكمة الجنايات مكافأة مالية تكون على عاتق خزينة الدّولة.

ويمكن أن تخفّض المكافأة إذا تعلّق الأمر بسلسلة من القضايا تعالج مسائل متشابهة.

تحدّد شروط وكيفيات تطبيق هذه المادّة عن طريق التّنظيم".

المادّة 4 : ينشر هذا القانون في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 28 صفر عام 1422 الموافق 22 مايو سنة 2001.

عبد العزيز بوتفليقة

قانون رقم 01 - 07 مؤرّخ في 28 صفر عام 1422 الموافق 22 مايو سنة 2001، يعدّل ويتمّم القانون رقم 91 - 10 المؤرّخ في 12 شوّال عام 1411 الموافق 27 أبريل سنة 1991 والمتعلّق بالأوقاف.

إنّ رئيس الجمهوريّة،

- بناء على الدّستور، لاسيّما المواد 2 و9 (الفقرة 3) و52 (الفقرة 3) و 119 و 120 و122 - 25 و126 منه،

- وبمقتضى الأمر رقم 66 - 154 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966والمتضمّن قانون الإجراءات المدنيّة، المعدّل والمتمّم،

- وبمقتضى الأمر رقم 66 - 155 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمّن قانون الإجراءات الجزائيّة، المعدّل والمتمّم،

- وبمقتضى الأمر رقم 66 - 156 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمّن قانون العقوبات، المعدّل والمتمّم،

- وبمقتضى الأمر رقم 75 - 58 المؤرّخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمّن القانون المدني، المعدّل والمتمّم،

الملحق رقم 3 القانون رقم 15/04

"المادة 620 مكرر: تنشأ لدى وزارة العدل مصلحة لنظام آلي وطني لصحيفة السوابق القضائية مرتبطة بالجهات القضائية يديرها قاض".

تحدد، عند الاقتضاء، كيفيات تطبيق هذه المادة عن طريق التنظيم".

"المادة 620 مكرر1 : يوجه طلب صحيفة السوابق القضائية إلى وكيل الجمهورية لدى المحكمة المرتبطة بالنظام الآلي الوطني لصحيفة السوابق القضائية".

يحرر ويوقع كاتب الضبط القسائم رقم 2 والقسائم رقم 3 المسلمة من طرف الجهات القضائية المرتبطة بالنظام الآلي الوطني لصحيفة السوابق القضائية، ويؤشر عليها وكيل الجمهورية.

المادة 12 : ينشر هذا القانون في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004.

عبد العزيز بوتفليقة

قانون رقم 04 – 15 مؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004، يعدل ويتمم الأمر رقم 66–156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات.

إن رئيس الجمهورية،

– بناء على الدستور، لاسيّما المواد 119 و120 و122–7 و 126 منه،

– وبمقتضى الأمر رقم 66–155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، المعدل والمتمم،

– وبمقتضى الأمر رقم 66–156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، المعدل والمتمم،

– وبعد مصادقة البرلمان،

يصدر القانون الآتي نصه :

المادّة الأولى : يعدل هذا القانون ويتمّم الأمر رقم 66–156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات.

المادّة 2 : يعدل ويتمم عنوان الباب الأول من الكتاب الأول من الأمر رقم 66– 156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمذكور أعلاه، ويحرر كما يأتي :

الباب الأول

العقوبات المطبقة على الأشخاص الطبيعية

المادّة 3 : تتمم الفقرة الأولى من المادة 5 من الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمذكور أعلاه، وتحرر كما يأتي :

"المادّة 5 : العقوبات الأصلية في مواد الجنايات :

1) (بدون تغيير)،

2) (بدون تغيير)،

3) (بدون تغيير).

إن عقوبات السجن لا تمنع تطبيق عقوبة الغرامة.

(الباقي بدون تغيير) " .

المادّة 4 : يتمم الكتاب الأول من الأمر رقم 66–156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمذكور أعلاه، بباب أول مكرر، عنوانه "العقوبات المطبقة على الأشخاص المعنوية"، يشمل مادتين 18 مكرر و18 مكرر 1، تحرران كما يأتي :

الباب الأول مكرر

العقوبات المطبقة على الأشخاص المعنوية

"المادّة 18 مكرّر : العقوبات التي تطبق على الشخص المعنوي في مواد الجنايات والجنح هي :

1– الغرامة التي تساوي من مرة (1) إلى خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.

2– واحدة أو أكثر من العقوبات الآتية :

– حل الشخص المعنوي،

– غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس (5) سنوات،

– الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس (5) سنوات،

– المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر، نهائيا أو لمدة لا تتجاوز خمس (5) سنوات،

– مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها،

– نشر وتعليق حكم الإدانة،

– الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس (5) سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته".

"*المادّة 18 مكرّر 1* : العقوبات التي تطبق على الشخص المعنوي في المخالفات هي :

الغرامة التي تساوي من مرة (1) إلى خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.

كما يمكن الحكم بمصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها".

المادّة 5 : يتمم الأمر رقم 66–156 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمذكور أعلاه بمادة 51 مكرر تحرر كما يأتي :

"*المادّة 51 مكرّر*: باستثناء الدولة والجماعات المحلية والأشخاص المعنوية الخاضعة للقانون العام، يكون الشخص المعنوي مسؤولا جزائيا عن الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه الشرعيين عندما ينص القانون على ذلك.

إن المسؤولية الجزائية للشخص المعنوي لا تمنع مساءلة الشخص الطبيعي كفاعل أصلي أو كشريك في نفس الأفعال".

المادّة 6 : تعدل وتتمم المادتان 176 و177 من الأمر رقم 66–156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمذكور أعلاه، وتحرران كما يأتي :

"*المادّة 176* : كل جمعية أو اتفاق مهما كانت مدته وعدد أعضائه تشكل أو تؤلف بغرض الإعداد لجناية أو أكثر، أو لجنحة أو أكثر، معاقب عليها بخمس (5) سنوات حبس على الأقل، ضد الأشخاص أو الأملاك تكوّن جمعية أشرار، وتقوم هذه الجريمة بمجرد التصميم المشترك على القيام بالفعل".

"*المادّة 177* : يعاقب على الاشتراك في جمعية الأشرار بالسجن المؤقت من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 500.000 دج إلى 1.000.000 دج، إذا تم الإعداد لارتكاب جنايات.

وتكون العقوبة الحبس من سنتين (2) إلى خمس (5) سنوات والغرامة من 100.000 دج إلى 500.000 دج، إذا تم الإعداد لارتكاب جنح.

ويعاقب منظم جمعية الأشرار أو من يباشر فيها أية قيادة كانت بالسجن المؤقت من عشر (10) سنوات إلى عشرين (20) سنة وبغرامة من 1.000.000 دج إلى 5.000.000 دج".

المادّة 7 : يتمم الأمر رقم 66–156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمذكور أعلاه بمادتين 177 مكرر و 177 مكرر 1 تحرران كما يأتي :

"*المادّة 177 مكرّر*: دون الإخلال بأحكام المادة 42 من هذا القانون، يعد اشتراكا في جمعية الأشرار المنصوص عليها في هذا القسم :

1– كل اتفاق بين شخصين أو أكثر لارتكاب إحدى الجرائم المنصوص عليها في المادة 176 من هذا القانون، بغرض الحصول على منفعة مالية أو مادية أخرى.

2 – قيام الشخص عن علم بهدف جمعية الأشرار أو بعزمها على ارتكاب جرائم معينة بدور فاعل في :

أ – نشاط جمعية الأشرار وفي أنشطة أخرى تضطلع بها هذه الجماعة مع علمه أن مشاركته ستساهم في تحقيق الهدف الإجرامي للجماعة.

ب – تنظيم ارتكاب جريمة من قبل جمعية الأشرار أو الإيعاز بارتكاب تلك الجريمة أو المساعدة أو التحريض عليه أو تيسيره أو إبداء المشورة بشأنه".

"*المادّة 177 مكرّر 1* : يكون الشخص المعنوي مسؤولا جزائيا وفقا للشروط المنصوص عليها في المادة 51 مكرر أعلاه، عن الجرائم المنصوص عليها في المادة 176 من هذا القانون، ويعاقب بالغرامة التي تساوي خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي المنصوص عليها في المادة 177 من هذا القانون.

ويتعرض أيضا لواحدة أو أكثر من العقوبات الآتية :

1 – مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها،

2 – المنع لمدة خمس (5) سنوات من مزاولة، بطريقة مباشرة أو غير مباشرة، النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته،

3 – الإقصاء من الصفقات العمومية لمدة خمس (5) سنوات،

4 – غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس (5) سنوات،

5 – حل الشخص المعنوي".

المادّة 8 : يعدل ويتمم العنوان رقم 1 من القسم الأول من الفصل الأول من الباب الثاني من الكتاب الثالث من الأمر رقم 66–156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمذكور أعلاه، ويحرر كما يأتي :

1 – القتل العمد والقتل مع سبق الإصرار والترصد وقتل الأصول والأطفال والتسميم والتعذيب.

المادّة 9 : يتمم الأمر رقم 66–156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمذكور أعلاه، بمواد 263 مكرر و263 مكرر 1 و263 مكرر 2 تحرر كما يأتي :

"*المادّة 263 مكرّر:* يقصد بالتعذيب كل عمل ينتج عنه عذاب أو ألم شديد جسديا كان أو عقليا يلحق عمدا بشخص ما، مهما كان سببه".

"*المادّة 263 مكرّر1 :* يعاقب بالسجن المؤقت من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 100.000 دج إلى 500.000 دج كل من يمارس أو يحرض أو يأمر بممارسة التعذيب على شخص.

يعاقب على التعذيب بالسجن المؤقت من عشر (10) سنوات إلى عشرين(20) سنة وبغرامة من 150.000 دج إلى 800.000 دج، إذا سبق أو صاحب أو تلى جناية غير القتل العمد".

"*المادّة 263 مكرّر2 :* يعاقب بالسجن المؤقت من عشر(10) سنوات إلى عشرين (20) سنة وبغرامة من 150.000 دج إلى 800.000 دج، كل موظف يمارس أو يحرض أو يأمر بممارسة التعذيب من أجل الحصول على اعترافات أو معلومات أو لأي سبب آخر.

وتكون العقوبة السجن المؤبد، إذا سبق التعذيب أو صاحب أو تلى جناية غير القتل العمد.

يعاقب بالسجن المؤقت من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 100.000 دج إلى 500.000 دج، كل موظف يوافق أو يسكت عن الأفعال المذكورة في المادة 263 مكرر من هذا القانون".

المادّة 10 : يتمم الأمر رقم 66–156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمذكور أعلاه، بمادة 341 مكرر تحرر كما يأتي :

"*المادّة 341 مكرّر:* يعد مرتكبا لجريمة التحرش الجنسي ويعاقب بالحبس من شهرين (2) إلى سنة (1) وبغرامة من 50.000 دج إلى 100.000 دج، كل شخص يستغل سلطة وظيفته أو مهنته عن طريق إصدار الأوامر للغير أو بالتهديد أو الإكراه أو بممارسة ضغوط عليه قصد إجباره على الاستجابة لرغباته الجنسية.

في حالة العود تضاعف العقوبة".

المادّة 11 : يتمم الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر رقم 66–156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمذكور أعلاه، بقسم سادس مكرر عنوانه : "تبييض الأموال" ويشمل المواد من 389 مكرر إلى 389 مكرر 7، تحرر كما يأتي :

القسم السادس مكرر

تبييض الأموال

"*المادّة 389 مكرّر:* يعتبر تبييضا للأموال:

أ – تحويل الممتلكات أو نقلها مع علم الفاعل بأنها عائدات إجرامية، بغرض إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات أو مساعدة أي شخص متورط في ارتكاب الجريمة الأصلية التي تأتّت منها هذه الممتلكات، على الإفلات من الآثار القانونية لفعلته.

ب – إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو الحقوق المتعلقة بها، مع علم الفاعل أنها عائدات إجرامية.

ج – اكتساب الممتلكات أو حيازتها أو استخدامها مع علم الشخص القائم بذلك وقت تلقيها، أنها تشكل عائدات إجرامية.

د – المشاركة في ارتكاب أي من الجرائم المقررة وفقا لهذه المادة، أو التواطؤ أو التآمر على ارتكابها ومحاولة ارتكابها والمساعدة والتحريض على ذلك وتسهيله وإسداء المشورة بشأنه".

"*المادّة 389 مكرّر1* : يعاقب كل من قام بتبييض الأموال بالحبس من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 1.000.000 دج إلى 3.000.000 دج" .

"*المادّة 389 مكرّر2* : يعاقب كل من يرتكب جريمة تبييض الأموال على سبيل الاعتياد أو باستعمال التسهيلات التي يمنحها نشاط مهني أو في إطار جماعة إجرامية، بالحبس من عشر (10) سنوات إلى خمس عشرة (15) سنة وبغرامة من 4.000.000 دج إلى 8.000.000 دج".

"*المادّة 389 مكرّر3* : يعاقب على المحاولة في ارتكاب الجرائم المنصوص عليها في هذا القسم بالعقوبات المقررة للجريمة التامة".

"*المادّة 389 مكرّر4* : تحكم الجهة القضائية المختصة بمصادرة الأملاك موضوع الجريمة المنصوص عليها في هذا القسم، بما فيها العائدات والفوائد الأخرى الناتجة عن ذلك، في أي يد كانت، إلا إذا أثبت مالكها أنه يحوزها بموجب سند شرعي، وأنه لم يكن يعلم بمصدرها غير المشروع.

يمكن الجهة القضائية المختصة الحكم بمصادرة الأموال محل الجريمة عندما يبقى مرتكب أو مرتكبو التبييض مجهولين.

إذا اندمجت عائدات جناية أو جنحة مع الأموال المتحصل عليها بطريقة شرعية، فإن مصادرة الأموال لا يمكن أن تكون إلا بمقدار هذه العائدات.

كما تنطق الجهة القضائية المختصة بمصادرة الوسائل والمعدات المستعملة في ارتكاب جريمة التبييض.

إذا تعذر تقديم أو حجز الممتلكات محل المصادرة، تقضي الجهة القضائية المختصة بعقوبة مالية تساوي قيمة هذه الممتلكات.

يجب أن يتضمن الحكم أو القرار القاضي بالمصادرة تعيين الممتلكات المعنية وتعريفها وكذا تحديد مكانها".

"*المادّة 389 مكرّر5* : يطبق على الشخص الطبيعي المحكوم عليه لارتكابه الجرائم المنصوص عليها في المادتين 389 مكرر1 و389 مكرر2 عقوبة واحدة أو أكثر من العقوبات التكميلية المنصوص عليها في المادة 9 من هذا القانون".

"*المادّة 389 مكرّر6* : يجوز الحكم بالمنع من الإقامة على الإقليم الوطني بصفة نهائية أو لمدة عشر (10) سنوات على الأكثر، على كل أجنبي مدان بإحدى الجرائم المنصوص عليها في المادتين 389 مكرر1 و389 مكرر2".

"*المادّة 389 مكرّر7* : يعاقب الشخص المعنوي الذي يرتكب الجريمة المنصوص عليها في المادتين 389 مكرر1 و389 مكرر2 بالعقوبات الآتية :

– غرامة لا يمكن أن تقل عن أربع (4) مرات الحد الأقصى للغرامة المنصوص عليها في المادتين 389 مكرر1 و389 مكرر2 من هذا القانون .

– مصادرة الممتلكات والعائدات التي تم تبييضها.

– مصادرة الوسائل والمعدات التي استعملت في ارتكاب الجريمة.

إذا تعذر تقديم أو حجز الممتلكات محل المصادرة، تحكم الجهة القضائية المختصة بعقوبة مالية تساوي قيمة هذه الممتلكات.

ويمكن الجهة القضائية أن تقضي بالإضافة إلى ذلك بإحدى العقوبتين الآتيتين :

أ – المنع من مزاولة نشاط مهني أو اجتماعي لمدة لا تتجاوز خمس (5) سنوات.

ب – حل الشخص المعنوي".

المادّة 12 : يتمم الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر رقم 66–156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمذكور أعلاه، بقسم سابع مكرر، عنوانه "المساس بأنظمة المعالجة الآلية للمعطيات" ويشمل المواد من 394 مكرر إلى 394 مكرر7، تحرر كما يأتي :

القسم السابع مكرر

المساس بأنظمة المعالجة الآلية للمعطيات

"*المادّة 394 مكرّر*: يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 150.000 دج".

"*المادّة 394 مكرّر 1* : يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

"*المادّة 394 مكرّر2* : يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمدا وعن طريق الغش بما يأتي :

1- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزّنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2 – حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

"*المادّة 394 مكرّر3* : تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد".

"*المادّة 394 مكرّر 4* : يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي".

"*المادّة 394 مكرّر5* : كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها".

"*المادّة 394 مكرّر6* : مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها".

"*المادّة 394 مكرّر 7* : يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها".

المادّة 13 : تلغى أحكام الفقرة 3 من المادة 110 مكرر من الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمذكور أعلاه.

المادّة 14 : ينشر هذا القانون في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004.

عبد العزيز بوتفليقة

قانون رقم 04-05 مؤرّخ في 27 جمادى الثانية عام 1425 الموافق 14 غشت سنة 2004، يعدّل ويتمّم القانون رقم 90-29 المؤرّخ في 14 جمادى الأولى عام 1411 الموافق أوّل ديسمبر سنة 1990 والمتعلّق بالتهيئة والتعمير(استدراك).

الجريدة الرّسميّة – العدد 51 الصادر بتاريخ 28 جمادى الثانية عام 1425 الموافق 15 غشت سنة 2004.

الصفحة 5 – العمود الأوّل – المادّة 5 – السطر 7 منها.

– بدلا من : "ومهندس معتمدين، في إطار عقد تسيير المشروع".

– يقرأ : "ومهندس في الهندسة المدنية معتمدين، معا، في إطار عقد إدارة المشروع".

...(الباقي بدون تغيير)...

المراجع

قائمة المراجع

القرآن الكريم: سورة يونس، الآية: 75.

المراجع الفقهية :

باللغة العربية :

1. أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة، الجزائر، ط: 10، 2011.
2. أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط: 02، 2006.
3. أحمد سعيد، أساسيات الشبكات والاتصالات، مكتبة الأنجلو المصرية، القاهرة، 2021.
4. اسامة احمد المناعسة، جلال محمد الزغبي، جرائم تقنية نظم المعلومات الإلكترونية، ط3، دار الثقافة للنشر والتوزيع، عمان 2004.
5. الأمانة العامة لمجلس وزراء الداخلية العرب، "دليل التعاون الأمني العربي"، تونس، 2019.
6. الإنتربول "تقارير التعاون الشرطي الدولي : آليات وتحديات التنفيذ"، 2020.
7. بهاء المرى، شرح قانون مكافحة جرائم تقنية المعلومات وحجية الدليل الرقمي في الإثبات، العربية للنشر والتوزيع، أفنان للطباعة، مصر، 2019.
8. تقرير المركز العربي للأمن السيبراني، "التهديدات الرقمية في إفريقيا: دور الإنتربول في المواجهة"، 2023.
9. جميل عبد الباقي الصغير، الجوانب الإجرائية المتعلقة بالانترنت، دار النهضة العربية، القاهرة، 2001..
10. خالد ممدوح ابراهيم، التقاضي الالكتروني "الدعوى الالكترونية وإجراءاتها أمّام المحاكم"، دار الفكر الجامعي، الإسكندرية.
11. سامي الزهراني، الأمن السيبراني وشبكات المعلومات، مكتبة جرير، الرياض، 2022.
12. سميرة معاشي، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني، ع 07، جامعة محمد خيضر بسكرة، افريل 2010.
13. عادل يحي، السياسية الجنائية في مواجهة الجريمة المعلوماتية، ط 1، دار النهضة العربية، القاهر، 2014.
14. عبد الرحمن عطا، الشبكات الحاسوبية وتقنيات الاتصال الحديثة، دار صفاء للنشر والتوزيع، عمّان، 2020.
15. عبد الفتاح البيومي حجازي، مكافحة جرائم الأنترنت، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2006.
16. عبد الله أبو السعود، مقدمة في البنية التحتية الرقمية، دار الراية للنشر، عمّان، 2021.
17. علاء الدين شحاتة، التعاون الدولي لمكافحة الجريمة، القاهرة، 2020.

18. علي جبار الحسناوي، جرائم الحاسوب والأنترنت، دار اليازوري، الأردن 2009.
19. غانم مرضي الشمري، الجرائم المعلوماتية، ط 1، دار الثقافة، عمان، 2016.
20. فهد عبد الله العبيد العازمي، "الإجراءات الجنائية المعلوماتية"، كلية الحقوق، جامعة عين شمس، دار الجامعة الجديدة 2016.
21. فوزية عبد الستار، قانون العقوبات –القسم الخاص– دار النهضة العربية، القاهرة، 1990.
22. محمد أمين احمد الشوابكة، جرائم الحاسوب الأولى والإنترنت، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، 2004.
23. محمد عبد العال، "شبكات الحاسوب: المفاهيم الأساسية والتطبيقات العملية"، دار الفكر العربي، القاهرة، 2019.
24. ممدوح بحر، حماية الحياة الخاصة في القانون الجنائي، دار الثقافة للنشر، عمان، 1996.
25. منير محمد الجنبيهي ممدوح محمد الجنبيهي، جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية 2005.
26. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، 2005..
27. نهلة عبد القادر المومني، الجرائم المعلوماتية، ط1، دار الثقافة للنشر والتوزيع، عمان، 2008.
28. هدى حامد قشقوش، الجريمة المنظمة القواعد الموضوعية والإجرائية والتعاون الدولي، دار النهضة العربية، القاهرة، 2002.
29. هشام محمد فريد رستم، قانون العقوبات مخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، مصر، 1995.
30. ياسر سيد فهمي، المواجهة الموضوعية للجرائم الإلكترونية، دار النهضة العربية، القاهرة، مصـــر، 2023.
31. يزيد أبو حليط، الجرائم الالكترونية والوقاية منها في القانون الجزائري، في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، قانون العقوبات –قانون الإجراءات الجزائية– قوانين خاصة، د،ط، دار الجامعة الجديدة للنشر الإسكندرية 2019.
32. يوسف المصري، الجرائم المعلوماتية والرقمية للحاسوب والأنترنت، ط 1، دار العدالة، عمان، 2011.

باللغة الأجنبية :

1. Europol & INTERPOL"Cybercrime Strategies and Operational Guidelines", 2022.
2. Parker (Doun B3) Figding computer crime A new Framework for protecting information 1998.

المذكرات و الرسائل العلمية :

1. أمينة سلام، "مكافحة الجريمة المعلوماتية في إطار القانون الدولي"، مذكرة لنيل شهادة ماستر، كلية الحقوق و العلوم السياسية، جامعة محمد خيضر، بسكرة، 2020.
2. بداوي حميدة و بن سالم فطيمة، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها، مذكرة مكملة لنيل شهادة ماستر تخصص إعلام آلي و أنترنت، جامعة البشير الإبراهيمي برج بوعريريج، الجزائر، 2023.
3. بعرة سعيدة، الجريمة الالكترونية في التشريع الجزائري، دراسة مقارنة، مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق، كلية الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2016/2015.
4. خالد بن مبارك القحطاني، التعاون الأمني الدولي في مواجهة الجريمة المعلوماتية عبر الوطنية، أطروحة داكتورة، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، دار النهضة العربية الرياض، 2006.
5. سليمان ابو نمر و يوسف بوكشريدة، مكافحة الجريمة المعلوماتية في إطار القانون الدولي، مذكرة مقدمة من أجل نيل شهادة ماستر أكاديمي، كلية الحقوق و العلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، 2021.
6. سوير سفيان، "جرائم المعلوماتية"، مجلد مذكرة لنيل شهادة الماجستير في العلوم الجنائية و علم الإجرام، كلية الحقوق و العلوم السياسية، جامعة أبوبكر بلقايد، تلمسان، 2010.
7. عبد الكريم شيباني، الحماية الإجرائية والموضوعية للجريمة المعلوماتية، مذكرة لنيل شهادة ماستر، كلية الحقوق والعلوم السياسية، جامعة الطاهر موالي، سعيدة، 2015/2016.
8. عثماني رضوان، "مكافحة جرائم المعلوماتية في القانون الجزائري والدولي"، أطروحة لنيل شهادة دكتوراه في العلوم تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة وهران 2 محمد بن أحمد، 2024.
9. عثماني رضوان، مكافحة جرائم المعلوماتية في القانون الجزائري و الدولي،أطروحة مقدمة للحصول على شهادة دكتوراه في العلوم تخصص قانون جنائي، كلية الحقوق و العلوم السياسية جامعة محمد بن احمد 2 وهران، الجزائر، 2024.
10. عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة مقدمة لاستكمال متطلبات شهادة الماستر المهني الطور الثاني، كلية العلوم الاقتصادية و العلوم التجارية و علوم التسيير، جامعة قاصدي مرباح ورقلة، الجزائر، 2019.

11. معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة مكملة لنيل شهادة الماجستير وعلوم الجنائية، 2011-2012.
12. نداء نائل فايز المصري، خصوصية الجرائم المعلوماتية، مذكرة لنيل شهادة الماجستير، جامعة النجاح الوطنية فلسطين2017.

المقالات العلمية :

باللغة العربية :

1. ايمان بن عثمان و ليلى بن بغيلة، التعاون القضائي الدولي ركيزة أساسية لتحقيق العدالة الجنائية الدولية، كلية العلوم الاسلامية، جامعة الوادي، مجلة الشهاب، المجلد 11، العدد 01، 2025.
2. بلباي إكرام، ضمانات المحاكمة العادلة في المعايير الدولية، مجلة القانون الدستوري و المؤسسات السياسية، جامعة عبد الحميد بن باديس، المجلد 06، العدد 01، 2022.
3. بن عودة نبيل، درعي لعربي، *"الإنابات القضائية الدولية في المجال الجزائي"*، مجلة القانون الدولي والتنمية، المجلد 7، العدد 2، 2019.
4. بن فرحات نور الدين، وعمري عبد القادر، "الطابع العابر للحدود للجرائم الإلكترونية وأثره على عمليات التحقيق الجنائي"، مجلة الباحث السياسي والقانوني، جامعة يحيى فارس المدية، المجلد 9، العدد 9، 2024.
5. بوشليق كمال، "النظام القانوني للإنابة القضائية في التشريع الجزائري"، مجلة دراسات و ابحاث المجلة العربية للأبحاث و الدراسات في العلوم الإنسانية و الاجتماعية، جامعة باتنة 1، المجلد 12، العدد 3، 2020.
6. تدريست مريم، معوقات نظام تسليم المجرمين كآلية للتعاون القضائي الدولي لمكافحة الجريمة المنظمة عبر الوطنية، *المجلة النقدية للعلوم القانونية والسياسية*، كلية الحقوق و العلوم السياسية، جامعة مولود معمري تيزي وزو، العدد 30، 2016.
7. حابت أمل، "دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، المجلة الدولية للبحوث القانونية و السياسية، كلية الحقوق و العلوم السياسية، جامعة تيزي وزو، المجلد 05، العدد 03، 2021.
8. خاليدة بن بعلاش و علي عثماني، الأحكام الموضوعية و الإجرائية لمكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة أبحاث قانونية و سياسية، المجلد 06 العدد 02، 2021.
9. ذيب محمد، ومروان عثماني، شروط تسليم المجرمين في النظام القانوني الجزائري، مجلة الباحث القضائي, جامعة محمد خيضر بسكرة، المجلد 13، العدد 1، 2021.

10. سعيد، محمد. "التعاون الأمني الدولي ودوره في مكافحة الإرهاب"، ع 12، مجلة البحوث القانونية والسياسية، جامعة غير محددة، بلد غير محدد، 2021.
11. شاين نوال ، الجريمة الإلكترونية في التشريع الجزائري –ماهيتها، موضوعها، خصائصها، ومظاهر تحدياتها، مجلة سوسيولوجيا، المجلد 06 العدد 02، 2020.
12. شرف الدين وردة، بلجراف سامية، "الجوانب الموضوعية والإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري"، مجلة المنار للدراسات والبحوث القانونية والسياسية، كلية الحقوق و العلوم السياسية، جامعة يحيى فارس المدية، المجلد 1، العدد 3، 2017.
13. صورية بوربانة، التعاون الدولي في مكافحة الجرائم المعلوماتية، مجلة القانون الدولي للدراسات البحثية، ع 01، جامعة طاهري محمد، بشار 2019.
14. عبد الله فاضل حامد و جلال حسين عنز و هقال صديق اسماعيل، أثر الاختصاص القضائي الدولي في تحديد القانون الواجب التطبيق على العلاقات الخاصة الدولية "دراسة تحليلية" ، *مجلة العلوم السياسية والقانون*، مجلد 9، عدد 2، 2020.
15. عبد الله ناصر،ع 7، "دور الشرطة الدولية في مكافحة الجريمة المعلوماتية"، مجلة القانون الرقمي جامعة جيلالي اليابس،بلعباس، 2022.
16. العنيد محمد زيد، شروط تسليم المجرمين في النظام القانوني الجزائري، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، المجلد 13 العدد 01، 2021.
17. فاروق خلف، استاذ محاضر "ا"، " الآليات القانونية لمكافحة الجريمة المعلوماتية"، مجلة الحقوق والحريات، كلية الحقوق جامعة حمة لخضر، الوادي، ع 2، 2015.
18. فريد ناشف، "آليات التعاون الدولي في مكافحة الجرائم الإلكترونية"، المجلد8، ع1، مجلة البحوث في الحقوق والعلوم السياسية جامعة البليدة 2، الجزائر 2022.
19. فيروز العوض الكريم صالح، دور التعاون الدولي في مكافحة الجريمة الإلكترونية، مجلة جامعة شندي للبحوث و الدراسات الشرعية و القانونية، العدد التاسع، 2023.
20. لرقط عزيزة، "التعاون الدولي في مكافحة الجرائم المعلوماتية (إشكالاته وآليات التغلب عليها)"، مجلة التواصل في الاقتصاد وإدارة القانون، كلية الحقوق و العلوم السياسية، جامعة باجي مختار عنابة، المجلد 25، العدد 04، 2019.
21. لعوارم وهيبة، نظام تسليم المجرمين دراسة تحليلية مقارنة بين المواثيق الدولية التشريع الجزائري و التشريعات المقارنة، كلية الحقوق و العلوم السياسية، مجلة البيبان للدراسات القانونية و السياسية، جامعة محمد البشير الابراهيمي برج بوعريريج، العدد الأول، 2016.
22. لورنس سعيد الحوامدة، "الجرائم المعلوماتية أركانها وآلية مكافحتها" دراسة تحليلية مقارنة، مجلة ميزان للدراسات القانونية والشرعية، الأردن، 2016/08/13.

23. محمد نجم محسن، دور القاضي الدستوري في إصلاح القصور التشريعي، المجلة القانونية(مجلة متخصصة في الدراسات و البحوث القانونية)، المجلد 03 العدد 09، 2021.
24. منصوري، عبد القادر "الأمن الإقليمي والتحديات الأمنية المشتركة في منطقة الساحل والمغرب العربي"، ع 45، مجلة السياسة الدولية، جامعة غير محددة، بلد غير محدد، 2020.
25. منقور قويدر، العوائق الاجرامية امام إعمال الطرق البديلة لحل النزاعات في المادة الادارية، مجلة القانون، العدد 5، 2015.
26. وريدة جندلي، التعاون الدولي لمكافحة الجريمة المعلوماتية : الفاعلية و التحديات، مجلة القانون و العلوم السياسية، المجلد 10 العدد 02، 2024.
27. ياكر الطاهر، "مكافحة الجرائم الإلكترونية بين التشريعات الوطنية والاتفاقيات الدولية"، مجلة الصدى للدراسات القانونية والسياسية، كلية الحقوق و العلوم السياسية، جامعة الجيلالي بونعامة خميس مليانة، المجلد 4، العدد 4، 2022.
28. يوسف محمود، المجلد15، "دور شبكات الاتصال في تطوير المؤسسات الحديثة"، ع 2، مجلة العلوم والتقنية، جامعة الملك سعود ، القاهرة ، 2022.

باللغة الأجنبية :

1. Benson (Carl), Jablon (Andrew), Kaplan (Paul) & Resenthal (Mara), Computer Crimes, Americain C‹L‹Review, vol‹34, N°21,997.

المواقع الالكترونية

باللغة العربية :

1. Free Tech ، "التعاون الدولي في مكافحة الجرائم السيبرانية: التحديات والفرص"، 2025، . https://freetech.tech/information-security-essentials/التعاون-الدولي-في-مكافحة-الجرائم-السي/ ، 2025/05/26.
2. Oyetunji, Damilola، "ما هو تبادل المعرفة ولماذا هو مهم؟" Klutch, ,2024، https://klutch.app/ar/blog/what-is-knowledge-sharing-and-why-is-it-important/ ، 2025/05/20.
3. الإنتربول"مكافحة الجريمة السيبرانية – دور المركز العالمي للابتكار" www.interpol.int، بتاريخ 30 ماي 2025 على الساعة: 16:15.
4. أنس المعولي، الفرق بين النظامين الانجلوساكسوني الانجليزي و النظام المدني اللاتيني، مجموعة نون العلمية، 2019/08/16، مجموعة نون العلمية – الفرق بين النظامين الأنجلوسكسوني/الانجليزي (Common Law)والنظام المدني/ اللاتيني(Civil Law) ، 2025/05/26.

5. جامعة منيسوتا، مكتبة حقوق الإنسان، نقل الإجراءات في المسائل الجنائية، https://hrlibrary.umn.edu/arab/b051.html ، اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة 118/45 المؤرخ في 14 كانون الأول/ديسمبر 1990، 2025/09/25.
6. الخزاري وفاء، الموانع القانونية لنظام تسليم المجرمين، مجلة المنارة للدراسات القانونية و الادارية، 13/05/2020، https://revuealmanara.com/الموانع-القانونية-لنظام-تسليم-المجرمين/ ، 2025/05/15.
7. سلطان بن قايد و ناصر بن غيث و أحمد منصور و عبد السلام المرزوقي، محاكمة غير عادلة وأحكام جائرة: إدانة مدافعين حقوقيين ومعارضين سياسيين ظلما، مِنَا لحقوق الانسان، 2024/07/11، https://menarights.org/ar/articles/mhakmt-ghyr-adlt-wahkam-jayrt-adant-mdafyn-hqwqyyn-wmardyn-syasyyn-zlma
8. فايق مينا، "التعاون القضائي الدولي: تبادل المعلومات والمساعدة القانونية"، مينا فايق للاستشارات القانونية، 2023، www.menafayq.com/international-judicial-cooperation-information-exchange-legal-assistance/ ، 2025/09/25.
9. فايق مينا، "الجرائم العابرة للحدود: آليات التعاون القضائي"، 2025/07/22، https://www.menafayq.com/transnational-crimes-judicial-cooperation-mechanisms ، 2025/09/25.
10. كريم هدى، "التعامل مع التحديات التدريبية"، *الهيئة العربية للمدربين*، 27 ديسمبر 2023، التعامل مع التحديات التدريبية – الهيئة العربية للمدربين ، 2025/05/26
11. مبرك عز الدين، ومحمد أمين مهري، "الآليات القانونية لحماية البيانات الرقمية"، الشعب أونلاين، 10 أبريل 2023، https://www.echaab.dz/2023/04/10/الآليات-القانونية-لحماية-البيانات-ال ، 2025/05/25.
12. مجموعة أدوات الأمم المتحدة بشأن المخدرات الاصطناعية، المساعدة القانونية المتبادلة، Mutual Legal Assistance ، 2025/09/25.
13. محمد الزعارة، واقع التحول الرقمي وسبل تحقيق النجاعة القضائية، 2025/02/15 https://www.droitetentreprise.com/واقع-التحول-الرقمي-وسبل-تحقيق-النجاعة/ ، 2025/09/25.
14. مراد ماشوش، "الجهود الدولية لمكافحة الإجرام السيبراني"، مجلة القانون والأعمال الدولية، 22 مايو 2018، https://www.droitetentreprise.com/الجهود-الدولية-لمكافحة-الإجرام-السيب/ ، 2025/05/25.

15. مطماطي راويــة، الجريمة الإلكترونية في التشريع الجزائري، مجلة القانون و الأعمال الدولية، 2019/04/17، الجريمة الإلكترونية في التشريع الجزائري ، 2025/05/15.

16. مينا فايق، "أحكام الإنابة القضائية وجمع الأدلة في القضايا"، موقع مينا فايق للاستشارات القانونية، 2025/09/19، https://www.menafayq.com/judicial-delegation-evidence-collection-cases/ ، 2025/09/25.

17. مينا فيرال، "نماذج التواصل: فهم آليات تبادل المعلومات"، 2024، نماذج التواصل: فهم آليات تبادل المعلومات | MENAVIRAL – مينا فيرال ، 2025/05/20.

18. وزارة الدفاع الوطني الجزائرية، الدرك الوطني – التنظيم والمهام، https://www.mdn.dz/site_cgn/sommaire/presentation/org_missions/org_missions_ar.php ، 2025/05/25.

19. وزارة العدل الجزائرية، المساعدة القضائية، www.mjustice.dz/ar/المساعدة-القضائية/، 2025/05/15.

20. وزارة العدل الجزائرية، المعاهدات والاتفاقيات الدولية، https://www.mjustice.dz/ar/conventions-internationaux-2-2/، 2025/05/26.

باللغة الأجنبية :

1. **Council of Europe.** *Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology.* Adopted 11 September 1995, https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-no-r-95-13
2. United Nations Office on Drugs and Crime, "Transfer of Criminal Proceedings", Education for Justice – UNODC, 2025, https://sherloc.unodc.org/cld/ar/education/tertiary/organized-crime/module-11/key-issues/transfer-of-criminal-proceedings.html/

المؤتمرات العلمية :

1. بن غدفة شريفة والقص صليحة، الجريمة الإلكترونية الممارسة ضد المرأة على صفحات الأنترنت وطرق محاربتها أعمال الملتقى الوطني، "آليات مكافحة الجرائم الالكترونية في التشريع الجزائري، الجزائر، 29 مارس 2017.
2. تدابير مكافحة الجرائم المتصلة بالحواسيب، مؤتمر الأمم المتحدة الحادي عشر، لمنع الجريمة والعدالة الجنائية المنعقد في بانكوك في الفترة 18، 2005/04/25، وثيقة رقم A/CONF203/14.
3. فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر " الجرائم الإلكترونية "، طرابلس، بتاريخ 25-24 مارس 2017.

4. محمد عقاد، جريمة التزوير في المحررات للحاسب الآلي، دراسة مقارنة، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي،1993.

المعاهدات الدولية :

1. اتفاقية بودابست لمكافحة الجريمة المعلوماتية، تم اعتمادها من قبل لجنة وزراء مجلس أوروبا في دورته التاسعة بعد المائة بتاريخ 8 نوفمبر لعام 2001، وفتح باب التوقيع عليها في بودابست في 23 نوفمبر ودخلت حيز النفاذ في 1 يوليو لعام 2004.
2. الأمم المتحد "اتفاقية بودابست لمكافحة الجريمة المعلوماتية"، 2001.

النصوص التشريعية :

1. الأمر رقم 71-57 المؤرخ في 5 أوت 1971 والمتعلق بالمساعدة القضائية، المعدل والمتمم بالقانون رقم 09-02 المؤرخ في 25 فبراير 2009. الجريدة الرسمية للجمهورية الجزائرية.
2. الأمر رقم 71-57 المؤرخ في 5 أوت 1971 والمتعلق بالمساعدة القضائية، المعدل والمتمم، الجريدة الرسمية للجمهورية الجزائرية، العدد 64.
3. الأمر رقم 71-57 المؤرخ في 5 أوت 1971 والمتعلق بالمساعدة القضائية، المعدل والمتمم بالقانون رقم 09-02 المؤرخ في 25 فبراير 2009. الجريدة الرسمية للجمهورية الجزائرية.

القوانين و التشريعات و المراسيم :

1. القانون رقم 01-04 المؤرخ في 20 أوت 2001 المتعلق بالمساعدة القضائية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 46، سنة 2001.
2. القانون رقم 01-06 المؤرخ في 22 مايو 2001، المعدل والمتمم للأمر رقم 71-57 المتعلق بالمساعدة القضائية، الجريدة الرسمية للجمهورية الجزائرية، العدد 29.
3. القانون رقم 23/06 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون العقوبات، ج.ر.عدد 84.
4. قانون رقم 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها، ج.ر، العدد 47.
5. القانون رقم 09-02 المؤرخ في 25 فبراير 2009، المعدل والمتمم للأمر رقم 71-57 المتعلق بالمساعدة القضائية، الجريدة الرسمية للجمهورية الجزائرية، العدد 15.
6. المادة 01 في الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون العقوبات، المعدل والمتمم.

[7] المادة 07 من القانون رقم 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها ، ج.ر، العدد 47.

[8] المادة 08 من القانون رقم 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها ، ج.ر، العدد 47.

9. المادة 12 من القانون رقم 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها ، ج.ر، العدد 47.

[10] المادة 2 من القانون 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها ، ج.ر، العدد 47.

[11] المادة 37 من القانون رقم 07/17 المؤرخ في 27 مارس 2017 المعدل والمتمم لقانون الإجرات الجزائية ،ج.ر .عدد20.

[12] المادة 394 من القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004، المتعلق بقوانين العقوبات." الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، 2004، العدد 71.

[13] المادة 4 من القانون 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها ، ج.ر، العدد 47.

[14] المادة 5 من القانون 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها ، ج.ر، العدد 47.

[15] المادة 6 من القانون 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها ، ج.ر، العدد 47.

16. المادة 698 من قانون الإجراءات الجزائية الجزائري، التي تنص على حالات رفض التسليم، الجريدة الرسمية للجمهورية الجزائرية.

[17] المادة 87 من القانون رقم 02/16 المؤرخ في 19 ماي 2016 المعدل والمتمم لقانون العقوبات، ج. ر. عدد 37.

[18] المادتين 13 و 14 من القانون 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها ، ج.ر، العدد 47.

19. المرسوم الرئاسي رقم 21–439 المؤرخ في 7 نوفمبر 2021، المتضمن تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وسيرها، الجريدة الرسمية، الجمهورية الجزائرية الديمقراطية الشعبية، 10 نوفمبر 2021، العدد 89، الصفحات 6–8.

الفهرس

الفهرس

ملخص:

الجريمة المعلوماتية هي كل فعل غير مشروع يستهدف البيانات أو الأنظمة عبر الوسائل التقنية، وتتميز بخصائص أهمها الطابع العابر للحدود وصعوبة الإثبات. تصنَّف تبعًا لمحل الجريمة أو دور الحاسب فيها أو بحسب مساسها بالأشخاص والأموال. المجرم المعلوماتي غالبًا ذو مهارات تقنية عالية، بينما المجني عليه قد يكون فردًا أو مؤسسة أو دولة. ويُبرز البحث أهمية التعاون الأمني الدولي عبر تبادل المعلومات والعمليات المشتركة وجهود الإنتربول، إضافة إلى الآليات القضائية مثل تسليم المجرمين والمساعدة القضائية. وأخيرًا، يقترح البحث آليات وطنية ودولية للتغلب على التحديات، تشمل تحديث التشريعات، تجاوز اختلاف النظم القانونية، حل تنازع الاختصاص، وتعزيز التدريب والتأهيل.

الكلمات المفتاحية: الجريمة المعلوماتية – المجرم المعلوماتي – المجني عليه – التعاون الأمني الدولي – الإنتربول – تسليم المجرمين – المساعدة القضائية – الإنابة القضائية – التجريم المزدوج – تنازع الاختصاص – القصور التشريعي.

Abstract:

Cybercrime is any unlawful act targeting data or systems through technological means, characterized mainly by its cross-border nature and the difficulty of detection and proof. It is classified according to the object of the crime, the role of the computer (as a tool or target), or its impact on individuals and property. The cybercriminal is often highly skilled in technology, while the victim may be an individual, an institution, or even a state.

The study highlights the importance of international security cooperation through information exchange, joint operations, and the efforts of INTERPOL. It also addresses judicial mechanisms such as extradition of criminals and mutual legal assistance, including information exchange, transfer of procedures, and judicial delegation. Finally, it proposes national and international mechanisms to overcome challenges, including updating legislation, bridging differences in legal systems, resolving jurisdictional conflicts, and enhancing training and capacity building.

Keywords: Cybercrime – Cybercriminal – Victim – International security cooperation – INTERPOL – Extradition – Mutual legal assistance – Judicial delegation – Double criminality – Jurisdictional conflict – Legislative gaps.