الجريمة المعلوماتية والآليات الدولية لحماية الأمن المعلوماتي

Cybercrime and International Mechanisms for the Protection of Information Security

الأستاذ هشام دوليم . Hicham DOULIM

أستاذ باحث في سلك الدكتوراه كلية العلوم القانونية والاقتصادية والاجتماعية المحمدية

جامعة الحسن الثاني الدار البيضاء

الملخص :

إن الجريمة المعلوماتية تمثل ظاهرة مركبة تتداخل فيها الأبعاد التقنية والقانونية والأمنية، الأمر الذي يفرض مقاربة متعددة المستويات تجمع بين تطوير التشريعات الوطنية، وتعزيز التعاون الدولي، وتحديث وسائل البحث الجنائي، وتأهيل الموارد البشرية القادرة على مواجهة التحديات الرقمية. كما أكدت الدراسة أن الآليات الدولية والإقليمية المعتمدة، رغم تطورها، ما تزال تحتاج إلى مزيد من التوحيد والفعالية لمواكبة سرعة انتشار الجرائم الإلكترونية وتعقيد أساليب ارتكابها.

Abstract :

Cybercrime constitutes a complex phenomenon in which technical, legal, and security dimensions intersect, requiring a multilayered approach that combines the development of national legislation, the enhancement of international cooperation, the modernization of criminal investigation tools, and the training of qualified human resources capable of confronting digital challenges. The study also emphasizes that, despite their progress, the current international and regional mechanisms still require further harmonization and effectiveness to keep pace with the rapid spread of cybercrimes and the increasing sophistication of their methods

مقدمة:

أفرز التطور التكنولوجي المتسارع تحولا عميقا في البنية الاجتماعية والاقتصادية والقانونية للمجتمعات الحديثة، مما أدى إلى ظهور أنماط جديدة من الإجرام لم تعد تستوعبها القواعد التقليدية.

وفي مقدمة هذه الأنماط تبرز الجريمة المعلوماتية باعتبارها ظاهرة إجرامية حديثة تتخذ من الوسائط الرقمية والفضاء الإلكتروني مجالا لارتكاب أفعال تمس الأفراد والمؤسسات والدول، وهو ما جعلها تشكل أحد أهم التحديات التي تواجه النظم القانونية على مستوى التجريم والعقاب والإثبات والاختصاص القضائي.

وأمام الطبيعة العابرة للحدود لهذه الجرائم، وتعقيدات اكتشافها وملاحقة مرتكبيها، أصبح من الضروري الوقوف على الإطار المفاهيمي للجريمة المعلوماتية، وخصائصها، وأنماطها، ثم البحث في الآليات القانونية والمؤسساتية الدولية التي تم اعتمادها لحماية الأمن المعلوماتي، بغية بناء رؤية شمولية تسمح بفهم الظاهرة وتحليل مقومات مواجهتها.

المطلب الأول: الطبيعة النظرية للجريمة المعلوماتية

عرفت الجريمة المعلوماتية تطورا ملحوظا نتيجة الاعتماد المتزايد على الوسائل التقنية في تدبير مختلف الأنشطة الاقتصادية والاجتماعية، مما أدى إلى بروز نمط إجرامي قائم على المعطيات الرقمية والبرمجيات والأنظمة المعلوماتية.

وقد أصبح هذا النوع من الجرائم يشكل تحديا حقيقيا للقانون الجنائي التقليدي، سواء على مستوى التعريف أو تحديد طبيعة الاعتداء أو ضبط العناصر المكونة للجريمة، نظرا لحداثة الوسائل المستعملة وارتباطها بفضاء افتراضي لا يخضع للحدود الجغرافية المعتادة.

وفي هذا الإطار يستعرض هذا المطلب الأسس النظرية للجريمة المعلوماتية من خلال بيان ماهيتها، وخصوصياتها، وأنماطها، وما تطرحه من إشكالات قانونية تستوجب مقاربة دقيقة تستوعب التغيرات التكنولوجية المتسارعة.

الفقرة الأولى: ماهية الجريمة المعلوماتية

تمثل الجريمة المعلوماتية أحد أبرز أنماط الإجرام الحديث، وذلك بالنظر إلى الأهداف التي تسعى إلى تحقيقها والوسائل التقنية المتطورة التي تتوسل بها، فهي جريمة تنشأ في فضاء افتراضي وتستعمل أدوات غير تقليدية، الأمر الذي يجعلها تختلف جذريا عن الجريمة التقليدية.

ويعتمد الجاني في هذا النوع من الجرائم على آليات تقنية متقدمة تسمح له بتنفيذ أفعاله عن بعد دون حضور مادي، مما يفرز نمطا إجراميا جديدا ذا خصائص مميزة.

وقد اتجه الفقه الجنائي إلى ربط تعريف الجريمة المعلوماتية مباشرة باستخدام الحاسب الآلي أو الأنظمة المعلوماتية باعتبارها الوسيلة الأساسية لارتكاب الفعل الإجرامي، ومن جهة أخرى، نجد أن المشرع – كما هو مستقر في علم القانون الجنائي – لا يضع تعريفا للجريمة، تاركا ذلك للفقه والقضاء.

وفي الإطار الدولي، اعتبرت اتفاقية بودابست لسنة 2001 المتعلقة بمكافحة الجريمة السيبرانية أن جرائم الأنترنت تشمل أي نشاط غير قانوني يتم عبر أجهزة أو شبكات المعلومات[1].

ويتضح من العودة إلى اللغة أن كلمة "الجريمة" تحيل إلى الذنب أو الفعل المحظور، ومن مشتقاتها جرم وأجرم واجترم، أما الجرم بالكسر فهو الجسد، ويقال تجرم عليه بمعنى نسب إليه ذنبا لم يرتكبه.

في حين أن لفظ "المعلوماتية" مشتق من الفعل "علم"، الدال على المعرفة والإعلام، كما ورد استخدام كلمة "معلومات" في القرآن الكريم في سياق التوقيت والبيان، أما اصطلاحا، فيمكن تعريف الجريمة المعلوماتية بأنها كل تصرف غير مصرح به أو تجاوز لما أذن به القانون، يتم باستخدام تقنيات المعلومات ويقع على الأنظمة أو المواقع الإلكترونية ويتسبب في ضرر، سواء حقق الجاني مكسبا أم لم يحقق[2].

وقد تعددت التعريفات الفقهية للجريمة المعلوماتية تبعا لاختلاف زاوية المعالجة، فالأستاذ Sieber يرى أنها كل سلوك غير مشروع يتعلق بالمعالجة الآلية للمعطيات أو إرسالها، بينما تعتبر عند البعض أنها فعل غير مشروع يستلزم قدرا عاليا من المعرفة بتكنولوجيا الحاسوب لارتكابه أو ملاحقته[3].

أما Masse فيربط الجريمة بنتيجتها، معتبرا أنها اعتداءات ترتكب بواسطة المعلوماتية بغرض تحقيق ربح غير مشروع، ويذهب Tiedemann إلى أن الجريمة المعلوماتية تشمل كل أشكال السلوك غير المشروع الذي يتم باستخدام الحاسب، وتظهر هذه التعريفات أن الفقه ما زال منقسما بين التركيز على وسيلة ارتكاب الجريمة، أو على طبيعة الاعتداء، أو على الجاني نفسه[4].

---

[1] الاتفاقية الأوروبية بشأن الجريمة السيبرانية (اتفاقية بودابست)، 23 نونبر 2001. فتح التوقيع في بودابست، دخول حيز التنفيذ 1 يوليوز 2004. رقم المعاهدة ETS N°185.

[2] ابن منظور، لسان العرب، القاهرة، دار المعارف، ج4، ص112.

الراغب الأصفهاني، مفردات ألفاظ القرآن، بيروت، دار القلم، ط4، 1997، ص215.

[3] Sieber Ulrich. Computer Crime – International Approaches. Munich, C.H. Beck, 1998, p. 41.

قورة نائلة، جرائم الكمبيوتر: دراسة قانونية، القاهرة، دار النهضة العربية، ط2، 2005، ص13.

[4] Masse Philippe. La criminalité informatique, Paris, Litec, 1991, p.25.

وتختلف جرائم الحاسوب عن جرائم الأنترنت في كون الأولى يمكن ارتكابها دون اتصال بالشبكة، إذ يكفي توفر جهاز الحاسب للتلاعب بالبيانات المخزنة داخله، بينما تتطلب جرائم الأنترنت اتصال جهازين أو أكثر بالشبكة العالمية، مما يجعل شبكة الأنترنت شرطا أساسيا لقيام هذا النوع من الجرائم[5].

ومع ذلك، يلاحظ أن التعريفات الفقهية لجرائم الأنترنت غالبا ما تكون قاصرة، فهي إما تركز على موضوع الجريمة أو على الوسيلة أو على الفاعل، دون أن تستوعب الظاهرة ككل.

وقد ظهر اتجاه فقهي حديث يسعى إلى تجاوز قصور التعريفات التقليدية، معتبرا أن الجريمة المعلوماتية تشمل كل فعل أو امتناع يضر بمكونات الحاسب أو شبكات الاتصال بوصفها مصالح يحميها القانون الجنائي[6].

ويرى اتجاه آخر أنها كل فعل عمدي ينتج عن استعمال غير مشروع للتقنية بهدف الاعتداء على الأموال المادية أو المعنوية، وبالنظر إلى العناصر المادية والمعنوية للجريمة، فإنها تشترك مع الجريمة التقليدية من حيث كونها فعلا مجرما، لكنها تختلف عنها من حيث أدوات التنفيذ وطبيعة الفضاء المعلوماتي.

بالاضافة إلى ذلك، عمد مؤتمر الأمم المتحدة لمنع الجريمة ومعاقبة المجرمين إلى تعريف جرائم الأنترنت بأنها كل سلوك غير مشروع يمكن ارتكابه بواسطة نظام أو شبكة حاسوبية أو داخل نظام معلوماتي.

ويتميز هذا التعريف بشموليته للجوانب المادية والمعنوية، كما ينسجم مع ما تبنته منظمة التعاون الاقتصادي والتنمية التي اعتبرت الجريمة المعلوماتية كل فعل أو امتناع يمس الأموال المادية أو المعنوية بطريقة مباشرة أو غير مباشرة باستعمال التقنية، وتؤكد كل هذه التعريفات تطور الظاهرة وتعقدها، خاصة في ظل الارتفاع الكبير لجرائم الاختراق والاحتيال الإلكتروني على الصعيد الدولي إلى حدود سنة 2025[7].

ويتضح من مجمل الاتجاهات أن الظاهرة تتجاوز أي تعريف ضيق، لذلك يمكن القول إن الجريمة المعلوماتية هي كل نشاط إجرامي يستخدم النظام المعلوماتي أو الشبكات المعلوماتية كوسيلة أو كهدف، ويتم عبر أدوات تكنولوجية حديثة بقصد إلحاق ضرر مادي أو معنوي بالأفراد أو الهيئات، سواء تعلق الأمر بالمساس بالمعطيات المعلوماتية أو الاعتداء على الخصوصية أو الاحتيال باستعمال بطاقات الائتمان أو نشر المحتويات الإباحية أو التحريضية أو الإرهابية.[8]

Tiedemann Klaus. Wirtschaftsstrafrecht und Computerkriminalität, Freiburg, Verlag Herder, 1993, p.77

[5] محمد عبد الوهاب بدوي، الجريمة المعلوماتية: دراسة قانونية مقارنة، بيروت، الحلبي الحقوقية، ط1، 2012، ص47.

[6] عبد الغني بسي، الجرائم السيبرانية، الجزائر، ديوان المطبوعات الجامعية، ط3، 2019، ص56.

[7] United Nations, Report of the UN Congress on Crime Prevention, Cairo, A/CONF.169/15, 1995. OECD, Computer-Related Crimes, Paris, 1986

[8] عبد الرزاق بن زاهر، الجرائم الإلكترونية: المفهوم والخصائص، الرباط، مطبعة الأمنية، ط1، 2018، ص33.

الفقرة الثانية: خصوصية الاجرام المعلوماتي

تتميز جرائم الأنترنيت بمجموعة من الخصائص من أبرزها أنها تطال معطيات الحاسوب، وهي تلك المتعلقة بفن الحاسوب كسرقة برامجه وتدميرها أو العبث ببياناته أو المعلومات المخزنة فيه، وهذه المعطيات ليست ذات طبيعة مادية ملموسة بل هي أقرب إلى الكيانات الذهنية أو المعنوية التي يتم إدخالها إلى النظام المعلوماتي[9].

وتتسم هذه الجرائم بصعوبة اكتشافها وإثباتها لأنها لا تترك أثرا خارجيا، وغالبا ما يتم اكتشافها بالمصادفة، ويعود ذلك إلى تطور الوسائل التقنية وانتشار مواقع متخصصة في السطو وبيع المعطيات، فضلا عن إمكانية الاستعانة بقراصنة محترفين مقابل مبالغ مالية، والاعتماد على أجهزة وشبكات غير شخصية لإخفاء الهوية[10].

وتعتبر الجريمة المعلوماتية جريمة عابرة للحدود، إذ أدى الربط العالمي لشبكة الأنترنيت إلى تجاوز الحدود الجغرافية وظهور مجتمع إلكتروني منفتح عبر شبكات تخترق الزمان والمكان، مما يطرح مشاكل قانونية وقضائية متعددة كما ظهر في قضية فيروس "حصان طروادة" المتعلقة بمرض نقص المناعة المكتسبة سنة 1989 وما نتج عنها من مطالبة المملكة المتحدة بتسليم الجاني من الولايات المتحدة[11].

ويستوجب ارتكاب الجرائم المعلوماتية وجود حاسوب ومعرفة تقنية به، إذ يستخدم الحاسوب كوسيلة لمعالجة المعلومات المقرصنة أو نسخ بطائق الائتمان عبر أجهزة تسجيل البيانات، ويتطلب هذا النوع من الجرائم إلماما واسعا بالمهارات الفنية لأن أغلب مرتكبيها متخصصون في المجال المعلوماتي[12].

ويميز الفقه بين الوضع الذي يكون فيه النظام المعلوماتي موضوعا للجريمة وبين الوضع الذي يكون فيه أداة لارتكابها؛ فقد يقع الاعتداء على المكونات المادية للنظام كإتلاف الحاسوب أو سرقة وسائط التخزين، أو الاعتداء على المكونات المعنوية كالبرامج والبيانات الإلكترونية عبر الحذف أو التغيير أو التزوير[13].

ويمكن أن يستعمل النظام المعلوماتي كأداة لارتكاب الجرائم التقليدية كالسرقة أو النصب أو حتى الجرائم الإرهابية، ورغم أن أصل الفعل تقليدي فإن المشرع يعتمد قواعد خاصة بالنظر لخطورته وطبيعته التقنية[14].

---

[9] محمد عبد الوهاب بدوي، الجريمة المعلوماتية: دراسة قانونية مقارنة، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت، 2012، ص 47.

[10] قورة نائلة، جرائم الكمبيوتر: دراسة قانونية، دار النهضة العربية، القاهرة، الطبعة الثانية، 2005، ص 13

[11] Ulrich Sieber, Computer Crime – International Approaches, C.H. Beck, Munich, 1998, p. 41

[12] Philippe Masse, La criminalité informatique, Éditions Litec, Paris, 1991, p. 25

[13] عبد الرزاق بن زاهر، الجرائم الإلكترونية: المفهوم والخصائص، مطبعة الأمنية، الرباط، الطبعة الأولى، 2018، ص 33.

[14] Klaus Tiedemann, Wirtschaftsstrafrecht und Computerkriminalität, Verlag Herder, Freiburg, 1993, p. 77

وتتميز الجرائم المعلوماتية بكونها لا تحتاج إلى القوة أو العنف، بل إلى مهارات تقنية في التعامل مع الحاسوب، وغالبا ما ترتكب بتعاون بين عدة أشخاص، سواء عبر تقديم مساعدة فنية أو لوجستية، أو من خلال التستر والصمت من طرف من يعلم بوقوع الجريمة[15].

ويتميز مرتكبو الجرائم المعلوماتية بالذكاء والقدرة على اختراق الأنظمة والتعديل في البرامج، إضافة إلى الخبرة والمهارة المكتسبة عبر التعلم والممارسة، وهو ما يجعلهم غالبا متخصصين في مجال المعلوماتية[16].

ويميل العديد من مرتكبي الجرائم المعلوماتية إلى ارتكاب هذه الجرائم بدافع اللهو أو إثبات التفوق أو التفاخر بقدراتهم، وتتشكل بينهم روابط اجتماعية تتجاوز الحدود الجغرافية، وتشكل مجموعات شبابية من نوابغ المعلوماتية[17].

الفقرة الثالثة: أنماط الجريمة المعلوماتية

تختلف أنماط الجرائم الإلكترونية حسب النوع والهدف من ارتكابها، وذلك بغية تحقيق أكبر ضرر ممكن عبر استخدام كافة الوسائل الإلكترونية المتاحة، وتشمل هذه الجرائم الطابع السياسي والعسكري والفردي والشبكات المعلوماتية، مما يعطيها تكييفات قانونية مختلفة[18].

وفي الجرائم الإلكترونية يحدد نمط الجريمة مدى تعلقها بالحاسوب، فقد يكون الحاسوب العنصر الرئيسي في تنفيذ الجريمة أو يتضاءل دوره ليصبح ثانويا، وقد لا تقوم الجريمة من دون الحاسوب، وقد يكون الحاسوب نفسه هو محل النشاط الإجرامي[19].

إن الحاسوب قد يكون الأداة الرئيسية لارتكاب الجريمة، حيث يحتوي على معلومات وأصول أساسية، مثل التحويل غير المشروع للأرصدة البنكية أو استخدامه لتزوير الأوراق المالية، بحيث يتحول من مجرد وسيلة إلى الباعث على ارتكاب الجريمة[20].

وفي حالات أخرى، يكون الحاسوب محل النشاط الإجرامي، حيث يستهدف مباشرة من خلال التخريب أو الإتلاف أو الفيروسات الإلكترونية، مثل إصابة الأقراص الصلبة أو حذف بيانات المخزن فيها[21].

---

[15] عبد الغني بسي، الجرائم السيبرانية، ديوان المطبوعات الجامعية، الجزائر، الطبعة الثالثة، 2019، ص 56.

[16] قورة، جرائم الكمبيوتر: دراسة قانونية، مرجع سابق، ص 44.

[17] David S. Wall, Cybercrime and the Internet, Oxford University Press, 2010, p. 22

[18] قورة نائلة، الجرائم المعلوماتية: دراسة قانونية مقارنة، دار النهضة العربية، القاهرة، الطبعة الثالثة، 2023، ص 15–17.

[19] محمد عبد الوهاب بدوي، الجريمة المعلوماتية: دراسة قانونية مقارنة، منشورات الحلبي الحقوقية، بيروت، الطبعة الثانية، 2022، ص 62.

[20] Philippe Masse, La criminalité informatique, Éditions Litec, Paris, 1991,

وهناك جرائم تتم بواسطة وسائل إلكترونية بحيث يكون الحاسوب عاملا ثانويا، وتكون الجريمة قابلة للتنفيذ بأدوات أخرى أهم من الحاسوب، مثل السب والقذف أو الخيانة الزوجية الإلكترونية، حيث يسهل الحاسوب ارتكاب الجريمة لكنه ليس العنصر الأساسي فيها[22].

ومن تم فإن الإشكالات القانونية تنشأ من تداخل الجرائم التقليدية مع الإلكترونية، مثل تطبيق الفصل 493 من القانون الجنائي المغربي على الخيانة الزوجية الإلكترونية، حيث اختلف الفقه بين الاتجاه الضيق الذي يقتصر على المواقعة التقليدية، والاتجاه الواسع الذي يشمل كل ممارسة جنسية عبر الوسائل الإلكترونية.

والقضاء المغربي اعتمد في عدة أحكام على الرسائل الإلكترونية والمكالمات الصوتية والفيديوهات كأدلة لإثبات الخيانة الزوجية، معتبرا أن صدور الرسائل من المتهم يكفي لإثبات الركن المادي للجريمة دون اشتراط المواقعة[23].

وتعد الجرائم الإلكترونية إما واقعة على الأموال مثل السطو الإلكتروني والتحويل غير المشروع للأموال وقرصنة البطاقات، أو على الأشخاص مثل التهديد والمضايقة والملاحقة وانتحال الشخصية، أو على أمن الدولة مثل الإرهاب الرقمي والتجسس[24].

وجريمة التهديد والمضايقة والملاحقة تتم عبر البريد الإلكتروني أو برامج المحادثة دون اتصال مادي بين الجاني والمجني عليه، بينما جريمة انتحال الشخصية تستهدف اغتيال السمعة أو الاحتيال المالي، بما يشمل القاصرين، وغالبا عبر تقديم صورة وهمية لتحقيق أهداف إجرامية[25].

أما السب والقذف فتعد أكثر الجرائم الإلكترونية شيوعا، ويمكن ارتكابها عبر أي وسيلة اتصال مكتوبة أو سمعية أو بصرية، وقد أقرت المحكمة الابتدائية بالرباط ثبوت جنحة القذف عبر النشر الإلكتروني استنادا للفصل 38 من قانون الصحافة والنشر[26].

---

[21] Tiedemann Klaus, Wirtschaftsstrafrecht und Computerkriminalität, Verlag Herder, Freiburg, 1993

[22] David S. Wall, Cybercrime and the Internet, Oxford University Press, London, 2010

[23] مجموعة الأحكام القضائية المغربية، قضايا الطلاق والتعويض بالاستناد إلى وسائل الاتصال الإلكترونية، الرباط، 2022، ص 45–50.

[24] عبد الغني بسي، الجرائم السيبرانية وأمن المعلومات، ديوان المطبوعات الجامعية، الجزائر، الطبعة الرابعة، 2020، ص 68–72.

[25] قورة نائلة، الجرائم المعلوماتية: دراسة قانونية مقارنة، مرجع سابق، ص 55–60.

[26] مجموعة الأحكام القضائية المغربية، القذف الإلكتروني والجرائم ضد الشرف، الرباط، 2021، ص 22–26.

وفي ما يتعلق بالجرائم الواقعة على أمن الدولة فتشمل الإرهاب الرقمي ونشر معلومات مضللة على المواقع الإرهابية، كما تشمل التجسس على المؤسسات الوطنية والدولية للحصول على الأسرار، مما يفرض تحديث الإجراءات الوقائية وحماية الشبكات الداخلية.[27]

المطلب الثاني: الاليات القانونية والمؤسساتية الدولية لحماية الأمن المعلوماتي

أمام الارتفاع المتزايد للجرائم المعلوماتية واتساع نطاقها العابر للحدود، بات من اللازم تطوير منظومة دولية قادرة على ضمان الأمن المعلوماتي وتعزيز سبل التعاون بين الدول لمكافحة هذا الشكل من الإجرام المعقد.

وقد ساهم المنتظم الدولي، عبر مجموعة من الاتفاقيات والهيئات الإقليمية والعالمية، في وضع قواعد مشتركة تتعلق بضبط الأفعال المجرمة، وتوحيد آليات البحث والتتبع، وتنظيم التعاون القضائي والأمني لحماية الفضاء الإلكتروني.

ويهدف هذا المطلب إلى تحليل أهم الآليات القانونية والمؤسساتية الدولية والإقليمية التي أحدثت لمواجهة الجريمة المعلوماتية، سواء من خلال الاتفاقيات متعددة الأطراف أو عبر المنظمات الدولية المتخصصة، بما يعكس التطور المستمر في الجهود العالمية الرامية إلى حماية الأمن المعلوماتي.

الفقرة الأولى: الاتفاقيات الدولية للحماية من مخاطر الجريمة المعلوماتية

تواجه الجريمة المعلوماتية تحديات متعددة تعيق مكافحتها، ولم تعد الصعوبات مقتصرة على اكتشافها وإثباتها، بل امتدت إلى إشكالات أعقد تتعلق بتحديد القانون الواجب التطبيق وبالجهة القضائية المختصة، خاصة وأن الطبيعة العابرة للحدود تجعل كل دولة تعتبر نفسها معنية بملاحقة مرتكبي هذا النوع من الجرائم.

فقد أدى تجاوز هذه الجرائم للحدود الجغرافية إلى تضارب في القوانين الوطنية وإلى نقاش واسع حول ضوابط الاختصاص المكاني، رغم أن مبدأ الإقليمية ما يزال يشكل الأساس في تحديد مجال تطبيق التشريعات الجنائية داخليا ودوليا.

[27] OECD, Cybersecurity and the Protection of Critical Information Infrastructures, Paris, 2023

ولمواجهة هذه الإشكالات، ومع توسع المعاملات عبر شبكات الإنترنت والارتفاع المهول للجريمة المعلوماتية ذات الطابع العابر للحدود، ظهرت الحاجة إلى إطار دولي قادر على توحيد الجهود بعدما عجزت التشريعات الوطنية بمفردها عن التصدي لها.

وهكذا اتجه المنتظم الدولي إلى وضع اتفاقيات تهدف إلى التقريب بين القوانين الجنائية للدول وتوفير حماية فعالة لأمن الفضاء الرقمي.

وفي هذا السياق، شكل مؤتمر الأمم المتحدة العاشر لمنع الجريمة المنعقد بفيينا ما بين 10 و17 أبريل 2000، ثم المؤتمر الحادي عشر المنعقد ببانكوك ما بين 18 و25 أبريل 2005، محطة أساسية لتعريف الجريمة المعلوماتية بوصفها: «كل فعل جرمي يرتكب بواسطة نظام أو شبكة معلوماتية أو داخل بيئة إلكترونية»، وهو تعريف أصبح مرجعا دوليا إلى غاية اليوم.

ومن جهة أخرى، بادرت اللجنة الأوروبية المعنية بمشكلات الجريمة ولجنة الخبراء في جرائم الحاسوب إلى إعداد مشروع اتفاقية دولية لمكافحة هذا النوع من الإجرام، أعلن عنها في 27 أبريل 2000 من طرف مجلس أوروبا، وتم التوقيع عليها في بودابست بتاريخ 23 نونبر 2001، ودخلت حيز التنفيذ في فاتح يونيو 2004.[28]

وقد هدفت هذه الاتفاقية، المعروفة بـ"اتفاقية بودابست بشأن الجريمة المعلوماتية"، إلى التصدي للاعتداءات الإلكترونية الحديثة على المواقع التجارية وغير التجارية، وإلى تنبيه المجتمع الدولي لمخاطر التوسع غير المنضبط للشبكات المعلوماتية، مع مراعاة الطابع الكوني لهذه الجرائم.

كما أن أول استعمال لمصطلح "Internet Crime" كان في مؤتمر أستراليا سنة 1998، قبل أن يوصي مؤتمر القانون والإنترنت المنعقد بلشبونة بتاريخ 26 يناير 2001 بالاقتصار على استعمال مصطلح "Cyber Crime" نظرا لدقته وشموليته وارتباطه المباشر بالفضاء الرقمي، مع التأكيد على ضرورة التمييز بين الجرائم التي ترتكب عبر الإنترنت وتلك التي لا يتطلب ارتكابها استعمال الشبكة[29].

وتمثل اتفاقية بودابست لسنة 2001 الإطار الدولي الأكثر شمولية إلى سنة 2025، وقد انضمت إليها دول عديدة مثل الولايات المتحدة واليابان وكندا وفرنسا والمغرب، وتتميز هذه الاتفاقية بانفتاحها على جميع الدول الراغبة في مكافحة الجريمة المعلوماتية، وبإرسائها لسياسة جنائية موحدة وآليات تعاون دولي تمكن من تتبع

[28] Convention on Cybercrime (Budapest Convention) تاريخ الإعلان: 27 أبريل 2000، تاريخ التوقيع: 23 نونبر 2001 – بودابست، تاريخ دخول حيز التنفيذ: 1 يونيو 2004 ، الرقمETS No.18 .

[29] محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والإنترنت، منشاة المعارف، مصر، الإسكندرية، 2006، ص:120.

الجناة عبر الحدود، وتحقيق تنسيق تشريعي يسمح بملاحقة هذا النوع من الجرائم بفعالية أكبر، خصوصا في ظل توسع الاقتصاد الرقمي والخدمات السحابية.

ومع ذلك، لا يزال التعاون الدولي يعاني من قصور واضح مقارنة مع التطور التقني السريع للجرائم الإلكترونية، إذ ما تزال العديد من الدول تعتمد إجراءات تقليدية لا تساير الطبيعة المتغيرة للإجرام العابر للحدود.

كما أن مرور معظم الأفعال الإجرامية عبر الإنترنت يجعل مسألة تحديد الاختصاص القضائي وتطبيق القانون المناسب مسألة معقدة تتطلب تحديثا مستمرا للآليات القانونية.

وترتبط هذه الجهود أيضا باتفاقيات حماية المعطيات الشخصية، وعلى رأسها اتفاقية ستراسبورغ لسنة 1981، المبنية على مبادئ منظمة التعاون الاقتصادي والتنمية لسنة 1980، والدلائل المعتمدة من الأمم المتحدة سنة 1990، والدليل الأوروبي لسنة 1995، ثم مبادئ حماية الحياة الخاصة في الاتصالات الدولية لسنة 2002، والدليل الأوروبي CE. 66/97/وتقوم هذه الأدوات على مبادئ أساسية أهمها: الرقابة على أنظمة معالجة البيانات، والمشروعية، والطمأنينة، بهدف الحد من المخاطر المهددة للأمن المعلوماتي.

وبخصوص التصنيف الدولي للجرائم الإلكترونية، فقد تبنت التدابير التشريعية الأوروبية تقسيمها إلى: جرائم الهدف، وجرائم الوسيلة، وجرائم المحتوى، وهو التصنيف الذي اعتمدته اتفاقية بودابست 2001، والتي وضعت أربعة أصناف رئيسية[30]:

الطائفة الأولى: الجرائم المرتكبة ضد سرية وسلامة ومصداقية البيانات والنظم، وتشمل:

–الولوج غير المشروع،

–الاعتراض غير القانوني،

–الإضرار بالبيانات،

–الإضرار بالنظم،

–إساءة استخدام الأدوات المعلوماتية.

الطائفة الثانية: الجرائم المرتبطة بالحاسوب، مثل:

–التزوير المعلوماتي،

[30] عمر محمد يونس، المذكرة التفسيرية للاتفاقية الأوروبية حول الجريمة الافتراضية، دون ذكر الطبعة، 2005، ص:15.

–الاحتيال المعلوماتي.

الطائفة الثالثة: جرائم المحتوى، وعلى رأسها الجرائم الإباحية ودعارة الأطفال.

الطائفة الرابعة: الاعتداءات على حقوق المؤلف والحقوق المجاورة، وخصوصا قرصنة البرمجيات.

وهكذا يتضح أن حماية الأمن المعلوماتي على المستوى الدولي شهدت تباينا مفاهيميا نتيجة تشعب ظاهرة المعلوماتية وغموض حدودها، كما أن تطور الجريمة الإلكترونية فرض على المنظمات الدولية اعتماد اتفاقيات ومقاربات متجددة.

الفقرة الثانية: الاتفاقيات الإقليمية للحماية من الجريمة المعلوماتية

تعد مكافحة الجريمة المعلوماتية مجالا يتطلب استحضار القواعد القانونية التي وضعت لسد الفراغ التشريعي في هذا النوع من الإجرام المستحدث، وذلك ضمانا لاحترام مبدأ الشرعية الجنائية الذي يقضي بألا جريمة ولا عقوبة إلا بنص. وقد ساهمت الاتفاقيات الدولية والإقليمية إلى حد كبير في إرساء منظومة قانونية مشتركة لمواجهة الجرائم المعلوماتية، عبر وضع قواعد للتعاون القضائي والأمني وتبادل المعلومات وتحديد الاختصاص، بما يحد من ظاهرة الإفلات من العقاب الناتجة عن الطابع العابر للحدود لهذه الجرائم[31].

أولا: الاتفاقية العربية لمكافحة الجرائم المعلوماتية[32]

أصدرت جامعة الدول العربية بتاريخ 21 دجنبر 2010 اتفاقية عربية متخصصة في مكافحة الجرائم المعلوماتية، شكلت نقطة تحول في التعاون العربي لمواجهة هذا النوع من الإجرام، بالنظر لما تضمنته من توحيد للمفاهيم وتجريم للأفعال المستحدثة، فضلا عن إرساء قواعد للتعاون القضائي وتبادل المعلومات والخبرات، وإقرار مبادئ تسليم المجرمين والمساعدة القانونية المتبادلة.

وقد صادق المغرب على هذه الاتفاقية بموجب ظهير شريف رقم 1.13.46 الصادر في 13 مارس 2013 بتنفيذ القانون رقم 76.12، لتصبح جزءا من المنظومة القانونية الوطنية. وتتكون الاتفاقية من ديباجة وخمسة فصول تروم تعزيز التعاون العربي وتحصين الأمن المعلوماتي للدول العربية.

---

[31] اتفاقية بودابست، المجلس الأوروبي، إعلان 27 أبريل 2000، توقيع 23 نونبر 2001، دخول حيز التنفيذ 1 يونيو 2004، ETS No.185

[32] اتفاقية عربية لمكافحة جرائم تقنية المعلومات، جامعة الدول العربية، إعلان 21 دجنبر 2010، توقيع بالقاهرة، دخول حيز التنفيذ 2013 بالنسبة للمغرب بموجب ظهير 1.13.46، قانون 76.12

كما نصت الاتفاقية على التزام كل دولة طرف بتنفيذ أحكامها في إطار احترام سيادتها الإقليمية، وعدم التدخل في الشؤون الداخلية للدول الأخرى، مع التشديد على عدم جواز ممارسة أي ولاية قضائية فوق إقليم دولة أخرى دون سند قانوني.

ولتفعيل مقتضيات الحماية، دعت الاتفاقية إلى إنشاء آليات وطنية متخصصة لرصد الجرائم المعلوماتية وتتبع مرتكبيها، والتعاون مع الهيئات الإعلامية والرقمية لتوعية المواطنين بخطر هذه الجرائم، ومواكبة التطور التقني المستمر.

وفي الجانب الزجري، شملت الاتفاقية تجريم الدخول أو البقاء غير المشروع في النظم المعلوماتية، والاعتداء على سلامة البيانات، واعتراض الاتصالات، وإساءة استخدام الأدوات المعلوماتية، والتزوير والاحتيال المعلوماتي، إضافة إلى التجريم المتعلق بالإباحية الرقمية، خاصة تلك التي تستهدف الأطفال.

كما توسعت في تجريم الأفعال الإرهابية المرتكبة عبر الأنظمة المعلوماتية مثل نشر أفكار التنظيمات الإرهابية أو الدعوة إليها أو تمويلها أو تسهيل اتصالها أو نشر طرق تصنيع المتفجرات.

وتبرز أهمية هذا الإطار القانوني في كونه يقر بضرورة تكاثف الجهود الدولية، نظرا للتطور السريع للتقنيات مقارنة ببطء التشريعات، ولأن ملاحقة مرتكبي الجرائم المعلوماتية تستلزم إجراءات تتجاوز الحدود الوطنية، وقد خصصت الاتفاقية المواد 32 إلى 36 للتعاون القانوني والقضائي، بما في ذلك المساعدة القضائية المتبادلة بين الدول العربية.

ثانيا: الاتفاقية رقم 108 للاتحاد الأوروبي المتعلقة بحماية الأشخاص تجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي[33]

أولت الدول الأوروبية اهتماما كبيرا لحماية الخصوصية الرقمية، وتعد الاتفاقية رقم 108، المعروفة باتفاقية ستراسبورغ لسنة 1981، أول اتفاقية دولية ملزمة في مجال حماية المعطيات الشخصية.

وتهدف هذه الاتفاقية إلى وضع إطار قانوني موحد يضمن سلامة المعالجة الآلية للبيانات الشخصية، عبر تحديد المبادئ الأساسية المتعلقة بجمع البيانات ومعالجتها وتخزينها والحق في الولوج إليها وتصحيحها، مع إرساء قواعد المسؤولية والتجريم في حالة خرق الالتزامات القانونية.

[33] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data، إعلان 28 يناير 1981، توقيع 28 يناير 1981، دخول حيز التنفيذ 1 أكتوبر 1985، ETS No.108؛ البروتوكول الإضافي الموقع 8 نوفمبر 2001، ظهير 1.14.136 بتاريخ 31 يوليو 2014

وقد انضم المغرب إلى هذه الاتفاقية في 22 غشت 2014 بعد إصداره القانون رقم 09.08 سنة 2008 وإنشاء اللجنة الوطنية لحماية الحياة الخاصة، وهو ما أهله لاحقا للمصادقة على البروتوكول الإضافي للاتفاقية والمتعلق بسلطات المراقبة ونقل المعطيات عبر الحدود، بموجب ظهير شريف رقم 1.14.136 بتاريخ 31 يوليو 2014.

وتقوم الاتفاقية على مبادئ أساسية أهمها ضرورة جمع البيانات بطريقة مشروعة ودقيقة، وتحديد مدة حفظها وأغراض معالجتها، وحماية سريتها ومنع استعمالها لغير الأغراض المخصصة لها، وضمان حق الشخص في الاطلاع عليها وتصحيحها، وتوفير حماية أمنية مناسبة لها، مع تحديد الفئات المخول لها الولوج إليها.

وبالنظر إلى كثافة تدفق البيانات عبر الحدود، تمت مراجعة الاتفاقية عبر بروتوكول إضافي لتعزيز الحماية وضبط عمليات النقل الدولي للبيانات الشخصية.

الفقرة الثالثة: المنظمات الدولية للحماية من الجريمة المعلوماتية

تضطلع المنظمات الدولية بدور أساسي في تعزيز الأمن المعلوماتي ومواجهة التحديات المرتبطة بالجريمة السيبرانية، خصوصا مع التطور المتسارع للمعطيات الرقمية واعتماد الدول على التقنيات الحديثة في مختلف مناحي الحياة.

وقد شهدت المرحلة الممتدة إلى حدود سنة 2025 تطورا ملحوظا في انخراط المجتمع الدولي في وضع آليات وقواعد ملزمة لمكافحة الجرائم المعلوماتية، سواء عبر الاتفاقيات متعددة الأطراف، أو من خلال المنظمات المختصة التي توجه السياسات الدولية وتشرف على التنسيق الأمني، وتطوير المعايير المشتركة لحماية الأنظمة المعلوماتية.

أولا: منظمة الأمم المتحدة[34]

تعد منظمة الأمم المتحدة الإطار الدولي الأوسع لمكافحة الجريمة ذات البعد العابر للحدود، بما فيها الجريمة المعلوماتية، فإلى جانب مبادئها المؤطرة مثل المساواة في السيادة، وحل النزاعات سلميا، ومنع استخدام القوة، تساهم المنظمة عبر وكالاتها وبرامجها في تطوير منظومة حماية الأمن المعلوماتي عالميا.

ويبرز ذلك من خلال الاتفاقيات المرتبطة بالمصنفات الذهنية، ومنها الاتفاقية العالمية لحق المؤلف الصادرة سنة 1952 عن اليونسكو، والتي شكلت أحد الأسس الأولى لحماية الإنتاج الفكري، رغم أنها لم تتناول بشكل مباشر برامج الحاسوب أو الجرائم المعلوماتية.

كما اضطلعت الأمم المتحدة بدور محوري عبر مؤتمراتها الدولية لمنع الجريمة ومعاملة المجرمين، مثل مؤتمر ميلانو 1985 وما نجم عنه من قواعد توجيهية، ثم مؤتمر هافانا 1990 الذي أكد ضرورة تحديث القوانين الجنائية لمواجهة الجرائم المعلوماتية، وتعزيز الضمانات المتعلقة بحماية الخصوصية، وتطوير تدابير أمن الحاسوب، والتعاون الدولي.

وتواصل هذا المسار عبر المؤتمرات اللاحقة، ومنها مؤتمر القاهرة 1995، والذي أوصى بحماية الحياة الخاصة والملكية الفكرية في مواجهة مخاطر التكنولوجيا الحديثة. وحتى سنة 2025، تستمر الأمم المتحدة في دعم الجهود الأممية لمكافحة الجرائم العابرة للحدود من خلال مكتب الأمم المتحدة المعني بالمخدرات والجريمة، الذي يعمل على توفير قواعد نموذجية وتشجيع الدول على اعتماد تشريعات متقدمة في مجال مكافحة الجريمة السيبرانية.

[34] ميثاق الأمم المتحدة، سان فرانسيسكو، 26 يونيو 1945، دخل حيز التنفيذ في 24 أكتوبر 1945.
الاتفاقية العالمية لحق المؤلف، اليونسكو، جنيف، 6 شتنبر 1952، دخلت حيز التنفيذ في 1955.
مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين، ميلانو، 1985، واعتماد مبادئ هافانا 1990.
مؤتمر الأمم المتحدة التاسع لمنع الجريمة، القاهرة، أبريل 1995.
تقارير مكتب الأمم المتحدة المعني بالمخدرات والجريمة UNODC حول الجريمة السيبرانية، 2019–2024.

ثانيا: المنظمة العالمية للملكية الفكرية[35]

تعتبر المنظمة العالمية للملكية الفكرية إحدى الوكالات الدولية ذات الاختصاص المباشر بحماية المصنفات الفكرية، بما فيها البرامج المعلوماتية، وقد تأسست بموجب اتفاقية ستوكهولم في 14 يوليوز 1967، ودخلت حيز التنفيذ سنة 1970، ثم أصبحت وكالة متخصصة تابعة للأمم المتحدة منذ دجنبر 1974.

وتتمثل أهدافها في تعزيز حماية الملكية الفكرية عالميا، وضمان التعاون الإداري بين اتحادات الملكية الصناعية وحقوق المؤلف، إضافة إلى دعم قدرات البلدان النامية في مجال الملكية الصناعية ونقل التكنولوجيا.

ومن أبرز إسهامات المنظمة في مجال الجريمة المعلوماتية إعداد النصوص التشريعية النموذجية سنة 1978 لحماية برامج الحاسوب، والتي هدفت إلى توجيه الدول لاعتماد تشريعات ملائمة تتضمن حماية البرامج وملاحقها ومستنداتها، وتوحيد قواعد الحماية في إطار المعايير الدولية.

وقد أثبتت هذه النصوص أهميتها في مواجهة التحديات المتزايدة والمتصلة بتحديد محل الجريمة وتجاوز الحدود في نقل البيانات، ومع التطورات المستجدة إلى سنة 2025، واصلت المنظمة إصدار توصيات ومعايير تقنية وقانونية متقدمة، خصوصا في مجال الذكاء الاصطناعي، وحماية البيانات الناتجة عن الأنظمة المؤتمتة، والإبداعات الرقمية.

ثالثا: منظمة التجارة العالمية[36]

تؤدي منظمة التجارة العالمية دورا محوريا في حماية البرامج المعلوماتية من خلال اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (تريبس)، التي فرضت على الدول الأعضاء احترام الحماية الممنوحة لبرامج الحاسوب باعتبارها مصنفات أدبية.

كما أقرت حقوقا للمؤلفين مثل الحق في تأجير البرامج، وحماية النسخ القانونية منها. وتستهدف هذه الحماية الحد من القرصنة، وضمان احترام الحقوق المالية والمعنوية للمؤلفين والمبتكرين.

---

[35] اتفاقية إنشاء المنظمة العالمية للملكية الفكرية، ستوكهولم، 14 يوليوز 1967، دخلت حيز التنفيذ سنة 1970.

النصوص النموذجية لحماية برامج الحاسوب، المنظمة العالمية للملكية الفكرية، جنيف، 1978.

تقارير WIPO حول الابتكار والبيانات الرقمية، طبعات 2019–2024.

[36] اتفاقية مراكش المؤسسة لمنظمة التجارة العالمية، مراكش، 15 أبريل 1994، دخلت حيز التنفيذ سنة 1995.

اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (تريبس)، 1994.

تقارير منظمة التجارة العالمية حول التجارة الرقمية، 2020–2025.

إلا أن هذه الحماية ما تزال محل انتقادات، بالنظر إلى ثغرات تتعلق بآليات التزام الدول، وعدم تناول مسألة الفيروسات المعلوماتية بشكل صريح، رغم ما تشكله من مخاطر كبيرة على أمن الشبكات والأنظمة.

وقد دفعت هذه الإشكالات منظمة التجارة العالمية إلى تعزيز التعاون مع المنظمة العالمية للملكية الفكرية خلال الفترة 2018–2025 لإعداد خطط مشتركة لتطوير المعايير، في ظل تزايد تهديدات القرصنة والاختراق.

رابعا: الشرطة الجنائية الدولية (الإنتربول)[37]

تعد الإنتربول من أبرز المنظمات الدولية العاملة في مكافحة الجريمة المعلوماتية، خصوصا بعد تأسيسها بصيغتها الحديثة سنة 1946 إثر مؤتمر بروكسيل، وقد أصبحت اليوم تضم 195 دولة عضوا.

وتتمثل مهامها في دعم التعاون بين أجهزة الشرطة عبر المكاتب المركزية الوطنية، وتبادل المعلومات والبيانات المتعلقة بالمجرمين، وإصدار نشرات دولية، وتنفيذ عمليات ميدانية مشتركة لملاحقة مرتكبي الجرائم العابرة للحدود، بما فيها الجرائم السيبرانية.

وقد أنشأت الإنتربول عددا من المراكز الإقليمية للاتصالات في طوكيو، نيوزيلندا، نيروبي، أذربيجان، وبوينس آيرس، إضافة إلى مكتب إقليمي في بانكوك. كما تم تطوير أنظمة اتصالات آمنة تتيح تبادل المعلومات في الزمن الحقيقي، وتم تعزيز وحدات متخصصة في الجرائم الرقمية مثل وحدة الإنتربول للجرائم السيبرانية.

وتبرز فعالية الإنتربول في عدد من القضايا، مثل ضبط مرتكبي الجرائم المتعلقة بالاستغلال الجنسي للأطفال عبر الإنترنت، أو ملاحقة أفراد الشبكات الإجرامية العابرة للحدود.

ومع تطور التحديات الرقمية إلى سنة 2025، أطلقت الإنتربول عدة برامج متقدمة، من أبرزها مبادرة "Cybercrime Knowledge Exchange" ومنصة "Cyber Fusion Centre" لدمج التحليل الاستخباراتي بالعمل الأمني الدولي.

---

[37] مؤتمر بروكسيل لإحياء اللجنة الدولية للشرطة الجنائية، 9 يوليوز 1946.

النظام الأساسي للمنظمة الدولية للشرطة الجنائية (الإنتربول)، باريس، 1956، مع تعديلاته اللاحقة.

تقارير الإنتربول حول الجرائم السيبرانية، 2018–2025.

خاتمة:

يتضح مما سبق أن الجريمة المعلوماتية تمثل ظاهرة مركبة تتداخل فيها الأبعاد التقنية والقانونية والأمنية، الأمر الذي يفرض مقاربة متعددة المستويات تجمع بين تطوير التشريعات الوطنية، وتعزيز التعاون الدولي، وتحديث وسائل البحث الجنائي، وتأهيل الموارد البشرية القادرة على مواجهة التحديات الرقمية.

كما أكدت الدراسة أن الآليات الدولية والإقليمية المعتمدة، رغم تطورها، ما تزال تحتاج إلى مزيد من التوحيد والفعالية لمواكبة سرعة انتشار الجرائم الإلكترونية وتعقيد أساليب ارتكابها.

ولذلك يبقى تحقيق الأمن المعلوماتي رهينا بإرساء سياسات جنائية متجددة، وتعزيز التعاون العابر للحدود، وتكثيف الجهود التوعوية والتقنية لضمان حماية المعطيات والمصالح الحيوية للأفراد والدول في ظل التحول الرقمي المتسارع.