جامعة محمد بوضياف المسيلة

كلية الحقوق والعلوم السياسية

قسم الحقوق

محاضرات في مقياس

الوقاية من الجرائم الالكترونية

السنة الثانية ماستر تخصص (إدارة الكترونية وخدمات رقمية)

اعداد الدكتور: بوعون نضال

السنة الجامعية 2024-2025

مقدمة:

اعتمد الإنسان منذ القدم على وسائل متنوعة لنقل المعلومة وحفظها، من الرسومات البدائية والكتابة على الأحجار وجلود الحيوانات إلى الورق والمخطوطات، لتخزينها وتسهيل استرجاعها حين الحاجة إلى حل مشكلة مستعصية. غيرت ثورة تكنولوجيا المعلوماتية، التي بدأت منذ السبعينيات واستمر تطورها بشدة في العقد الأخير، مفهوم المعلومة راديكاليا، حيث أصبحت الحواسيب وشبكة الإنترنت – بمكتبتها الواسعة – World Wide Web أدوات أساسية لنقلها، تخزينها، استرجاعها، بل وتنبؤها باستخدام الذكاء الاصطناعي. وساهم انتشارها المعمق في كل مجال – إداري، اقتصادي، تجاري، تربوي – في تطوير نمط الحياة البشرية وتسهيل التعاملات بين الدول والمؤسسات والأفراد، محولة العالم إلى قرية صغيرة.

إلا أن هذه القدرة التكنولوجية الفائقة ولدت وجها مظلما يمثل في جرائم المعلوماتية، وهي الأفعال المنصوص عليها قانونا تستهدف الأنظمة الحاسوبية والشبكات للاطلاع على المعلومات المحمية، سرقتها، تخريبها، أو تعطيلها. يمارسها مجرمو المعلوماتية، فئة جديدة مميزة بالذكاء والمعرفة التكنولوجية العالية، بهدف مكاسب مادية أو معنوية، باستخدام هجمات إلكترونية سرية.

يهدف هذا العمل – الموجه لطلبة القانون في الجامعات – إلى دراسة الإطار التشريعي الجزائري لمكافحة هذه الظاهرة الإجرامية المستحدثة، لتطلعهم على الأدوات القانونية المتاحة، تحليل فجواتِها، واقتراح حلول لتطويرِها.

1- الإطار المفاهيمي للجريمة المعلوماتية:

تستهدف الجريمة، باعتبارها فعلاً محظورًا بنصوص القانون العقابي، في الغالب حقوق الغير، فترد أحيانًا على المال وأحيانًا على الشخص في ذاته، سواء في بعده **المادي** أو المعنوي. في ظل التحولات الاجتماعية التي كرّست مفاهيم الحداثة والتطور التكنولوجي، والتي أحدثت نقلة نوعية في نمط عيش الإنسان بفضل ما وفرته التقنيات التكنولوجية من وسائل اتصال ومعالجة للمعلومات، برز نمط مستحدث من الجرائم يعتدي على المال والنفس عبر الفضاء الرقمي الإلكتروني، ويُعد هذا النمط نتيجة مباشرة لانتشار تقنية المعلوماتية التي أضحت تمثل عصب الحياة المعاصرة وعنصر قوة في مسار التقدم الحضاري لأي دولة، بحيث لا يمكن لأي دولة مواكبة ركب المجتمع الدولي وتحقيق التنمية المنشودة دون توظيفها الفعال، وقد أصبح تداول المعلومات ومعالجتها في أقصر زمن وبأعلى قدر من الكفاءة محور اهتمام المتخصصين في هذا المجال، غير أن هذا الاهتمام جذب في المقابل فئة إجرامية تمتهن الاعتداء على الأنظمة المعلوماتية لأغراض غير مشروعة ومتباينة، وهي الظاهرة التي اصطلح على تسميتها بـ الجريمة المعلوماتية أو"La Cyber-crim" ، والتي غدت تشكل انشغالاً متزايدًا لدى القانونيين والمشرعين والخبراء الفنيين في مجال النظم المعلوماتية.

1-1 تعريف النظام المعلوماتي:

تُعدّ المعلومات المحلّ الرئيس للجريمة المعلوماتية، إذ تستهدف هذه الأخيرة البيانات والمعطيات التي لا يمكن النفاذ إليها إلا عبر منفذ واحد هو النظام المعلوماتي بوصفه الوعاء

المنطقي لتخزينها ومعالجتها[1]، ويشكّل هذا النظام بيئة تقنية أُنشئت خصيصًا لتداول المعلومات وفق آليات للمعالجة الآلية تتحكم فيها الحواسيب، منفردة أو متصلة عبر شبكات الاتصالات، بما يتيح تداولها ومعالجتها بأفضل وأسرع الأساليب خدمةً لترقية الأداء المؤسساتي لأجهزة الدولة ومصالحها الحيوية كالدفاع والصحة والتعليم والإعلام وغيرها[2]، إضافة إلى تيسير المعاملات بين الأفراد من خلال خدمات إلكترونية كالبيع والشراء والدفع الإلكتروني وخدمات البريد الإلكتروني وما في حكمها، مما يقتضي في الغالب الإدلاء ببيانات شخصية ذات طابع سري، ويجعل من هذه النظم هدفا مغريا لهواة ومحترفي الجريمة المعلوماتية على حد سواء[3].

وقد أولت بعض التشريعات المقارنة عناية خاصة بتعريف المعلومات، إذ عرّف المشرّع الفرنسي المعلومات في القانون رقم 82-652 المؤرخ في 26 جويلية 1982 المتعلق بتنظيم الاتصالات السمعية البصرية بأنها رنين الصور والوثائق والبيانات والرسائل أيًا كانت طبيعتها[4]، في حين تبنّى المشرّع الأمريكي بموجب قانون سنة 1999 المنظم للمعاملات التجارية الإلكترونية مفهومًا تكنولوجيًا موسّعًا، حين اعتبر المعلومات كل البيانات والكلمات والصور والأصوات والوسائط وبرامج الحاسوب والبرامج المضغوطة سواء كانت مخزنة على أقراص مرنة أو على قواعد بيانات أو غيرها، وهو النهج الذي حذا حذوه كل من المشرّعين البحريني والإماراتي في قوانينهما لسنة 2002 بشأن تنظيم المعاملات الإلكترونية، حيث عُرّفت المعلومات بأنها كل بيانات ذات خصائص إلكترونية في شكل نصوص أو رموز أو أصوات أو رسومات أو صور أو

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الحلبي الحقوقي، بيروت، 2009، ص، 45.

[2] محمد بن صالح الجمال، الجريمة المعلوماتية في التشريع الجزائري، منشورات الجمعية الجزائرية للبحث القانوني، الجزائر، 2015، ص،112.

[3] عبد الرحمن عثماني، جرائم تقنية المعلومات في ظل الاتفاقية العربية، رسالة ماجستير، جامعة ورقلة، 2022، ص. 78

[4] محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، مصر ،2004، ص39

برامج حاسوب أو غيرها من قواعد البيانات[1]، أما المشرّع الجزائري، فقد عرّف المعطيات المعلوماتية في الفقرة "ج" من المادة 02 من القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بأنها كل عرض للوقائع أو المعلومات أو المفاهيم في شكل معدّ للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج التي تمكّن هذه المنظومة من أداء وظيفتها، غير أن هذا التعريف يتسم بقدر من العمومية يخرجه عن الدقة المطلوبة في ضبط مدلول "المعلومة" تحديدًا ويميّزه عن غيره من المفاهيم التقنية المتداخلة[2].

ومن ثمّ تبرز الحاجة إلى إعادة صياغة تعريف أكثر تحديدًا للمعلومة في المجال المعلوماتي، بما يضمن الفصل بين مفهوم المعلومة ومفاهيم المعطيات والبرامج وقواعد البيانات، اتساقًا مع خصوصية ميدان تكنولوجيات المعلومات الذي لا يحتمل الخلط في المصطلحات والمفاهيم.

1-1-1) أنواع المعلومة: تقسم المعلومات الى

- **المعلومات الاسمية:** وهي البيانات المتعلقة بشخص معين، مثل اسمه وموطنه وحالته الاجتماعية، وتُعدّ من البيانات ذات الطابع الشخصي السري التي لا يجوز الاطلاع عليها أو معالجتها إلا بموافقته أو وفق ترخيص صريح من القانون.

[1] عبد العال الدريبي، الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والأنترنت، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2012، ص 44.

[2] القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 55، الجمهورية الجزائرية الديمقراطية الشعبية، 2009، الصادرة بتاريخ 16 أوت 2009

– **المعلومات المتعلقة بالمصنفات الفكرية:** وتشمل المعطيات ذات الطبيعة الإبداعية أو التقنية، كالمصنفات الأدبية والفنية، والاختراعات، والتسجيلات الفنية، وتخضع لحماية خاصة بموجب قوانين الملكية الفكرية وحقوق المؤلف والحقوق المجاورة.

– **المعلومات المتاحة:** وهي المعلومات الموجهة بطبيعتها إلى الجمهور، أو التي تُتاح للكافة دون قيد، مثل النشرات الجوية والتقارير الرسمية، ما لم تُقرّر الأنظمة القانونية إخضاع بعض فئاتها لقيود خاصة متعلقة بالسرية أو بالأمن الاقتصادي[1]

ويجب توافر جملة من الشروط الجوهرية من اجل الحماية القانونية لها، ولعل من أهمها:

1-1-2) تحديد المعلومات: أي أن تُحصر في نطاق معيّن يَصدُق عليه وصف التعيين أو القابلية للتعيين، وألا تندرج في إطار المعطيات الشائعة أو المتداولة على نطاق عام، وأن تنطوي على قدر من الأصالة أو الجِدة يميزها عن المعرفة العامة، وهو ما ينسجم مع الاتجاه الفقهي الذي يقرّر أن المعلومة تعبير مُصاغ لنقل رسالة بواسطة رموز أو إشارات مختارة[2]

1-1-3) السرية: إذ يُشترط ألا تكون المعلومة معروفة أو متاحة بوجه عام للغير، وأن يكون صاحبها قد اتخذ تدابير معقولة للمحافظة على سريتها، سواء استمدت هذه السرية من طبيعة موضوعها (مهنية، تجارية، تقنية...) أو من إرادة صاحبها عبر إجراءات الحجب كاستخدام كلمات

[1] عبد العال الدريبي، مرجع سابق، ص 45.

[2] محمد علي العريان، مرجع سابق، ص 38.

المرور أو آليات التشفير، وهي ذات الشروط التي تقررها الأنظمة الحديثة لحماية الأسرار التجارية والمعلومات غير المفصح عنها[1]

1-2) تعريف تقنية المعلوماتية:

تحتل المعلومات في العصر الحديث مكانة محورية في مسار التطور الحضاري، بعد أن أصبحت في صلب عمل النظم التقنية التي تُنشأ على أوسع نطاق وبأعلى قدر من السرعة والكفاءة، بهدف تخزينها وتداولها وضمان فاعليتها في مجالات استراتيجية كالدفاع والصحة والتعليم والقضاء، وهو ما أفرز ما يُعرف بتقنية المعلوماتية كنظام متكامل لمعالجة المعطيات رقميا.

وقد حرصت الاتفاقيات الدولية والإقليمية، إلى جانب التشريعات الوطنية، على ضبط تعريف دقيق للنظام المعلوماتي، إذ عرّفته اتفاقية بودابست لمكافحة الجرائم المعلوماتية في مادتها الأولى بأنه كل آلة، منفردة أو متصلة بغيرها، قادرة على تنفيذ معالجة آلية للمعطيات المعلوماتية وفق برنامج محدد، وتشمل هذه المعطيات كل تمثيل للوقائع أو المعلومات أو المفاهيم في أي شكل يُعدّ للمعالجة الآلية، بما في ذلك البرامج التي تمكّن الحاسوب من أداء مهامه[2].

كما أوضحت المذكرة التفسيرية للاتفاقية أن المقصود بالنظام المعلوماتي هو جهاز يتكوّن من مكونات مادية ومنطقية، مخصص للمعالجة الآلية للبيانات الرقمية، يشتمل على وسائل

[1] عبد العال الدريبي، مرجع سابق، ص 45.

[2] محمد بن صالح الجمال، الجريمة المعلوماتية في التشريع الجزائري، منشورات الجمعية الجزائرية للبحث القانوني، الجزائر، 2015، ص. 89.
انظر أيضًا: اتفاقية بودابست بشأن الجرائم الإلكترونية، المادة 1، مجلس أوروبا، 2001، النص العربي الرسمي، ص، 12.

الإدخال والإخراج والتخزين، وقد يعمل بشكل منفرد أو في إطار شبكة تضم عدة أجهزة مماثلة، على أن تتم هذه المعالجة بصورة آلية دون تدخل بشري مباشر في مراحلها الجوهرية[1].

وعلى صعيد التشريعات الوطنية المقارنة، عرّف نظام مكافحة الجرائم المعلوماتية السعودي النظام المعلوماتي بأنه مجموعة البرامج والأدوات المعدّة لمعالجة البيانات وإدارتها، بما في ذلك الحاسبات الآلية[2]، في حين اعتبر المشرّع الأردني في قانون المعاملات الإلكترونية رقم 85 لسنة 2001 أن نظم معالجة المعلومات هي الأنظمة الإلكترونية المستعملة لإنشاء رسائل المعلومات أو إرسالها أو تسلّمها أو معالجتها أو تخزينها أو تجهيزها بأي وسيلة أخرى[3]، أما المشرّع الجزائري، فقد قرّر في تشريعه المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال أن النظام المعلوماتي هو كل نظام منفصل أو مجموعة أنظمة متصلة أو مرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذًا لبرنامج معيّن، وهو تعريف ينسجم في جوهره مع الاتجاه الدولي في التركيز على عنصر المعالجة الآلية للبيانات كمعيار فني وقانوني مميز للنظام المعلوماتي[4].

[1] نفس المرجع، ص 92.

أنظر كذلك: التقرير التفسيري لاتفاقية بودابست بشأن الجرائم الإلكترونية، مجلس أوروبا، 8 نوفمبر 2001، الدورة رقم 109، ص 15

[2] نظام مكافحة الجرائم المعلوماتية السعودي، المادة 1، الجريدة الرسمية، المملكة العربية السعودية، 1428 هـ/2007 م، ص، 5.

انظر أيضًا: عبد الرحمن بن محمد الشيخ، الجرائم المعلوماتية في التشريع السعودي، دار المعرفة، الرياض، 2012، ص، 67.

[3] أحمد محمد الزعبي، المعاملات الإلكترونية في التشريع الأردني، دار الثقافة للنشر، عمان، 2005، ص، 34.

انظر كذلك: قانون المعاملات الإلكترونية الأردني رقم 85 لسنة 2001، المادة 2، الجريدة الرسمية، المملكة الأردنية الهاشمية، ص، 3.

[4] محمد بن صالح الجمال، الجريمة المعلوماتية في التشريع الجزائري، منشورات الجمعية الجزائرية للبحث القانوني، الجزائر، 2015، ص 95.

انظر كذلك: المادة 02 من قانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنلوجيا الاعلام والاتصال ومكافحتها، مرجع سابق.

1-2-1) شبكات الاتصال:

يشكّل النظام المعلوماتي بنية متكاملة تتكوّن من مكوّنات مادية وبرمجية مرتبطة غالبًا بشبكات اتصال، بحيث تنصب الجريمة المعلوماتية في الغالب على استغلال هذه العناصر (الحواسيب، وسائط التخزين، شبكات الاتصال) باعتبارها الوسيلة الرئيسة للوصول إلى المعلومات المخزنة أو المتداولة والاعتداء عليها.

1- مفهوم شبكة الاتصال: تُعدّ شبكة الاتصال في مجال النظم المعلوماتية وسيلة ربط بين حاسوبين أو أكثر، ويتم هذا الربط عبر وسائل مادية كسلك النحاس والألياف البصرية والكابلات، أو بوسائل لاسلكية كالموجات الراديوية والأشعة تحت الحمراء والاتصالات عبر الأقمار الصناعية. وتُصنَّف الشبكات، بحسب نطاقها الجغرافي، إلى شبكة محلية تغطي حيزًا محدودًا، وشبكة واسعة النطاق تمتد عبر مسافات كبيرة، وقد تكون هذه الشبكات متصلة ببعضها البعض بصورة بينية، وتُعد شبكة الإنترنت نموذجًا للشبكة العالمية التي تتكوّن من عدد لا حصر له من الشبكات المترابطة، وتستخدم بروتوكولات ونظمًا موحدة لنقل البيانات، بحيث تتصل النظم المعلوماتية بها كنقاط نهائية أو نقاط عبور أو كوسيلة لتسهيل نقل المعلومات[1].

2- تعريف شبكة الأنترنت: تُعتبر شبكة الإنترنت أكبر شبكة حواسيب موسَّعة على مستوى العالم[2]، إذ تربط بين الحواسيب الشخصية والشبكات المحلية والعامة، وتمكّن أي مستخدم، من أي مكان تقريبًا، من النفاذ إلى كمٍّ هائل من المعلومات عبر تجهيز بسيط يتمثل في حاسوب مكتبي

[1] هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة الجرائم المعلوماتية معلقا عليها، الطبعة الأولى، دار النهضة العربية، مصر، 2008، ص18.

[2] علي بن عبد الله غسيري، الأثار الأمنية لاستخدام الشباب للأنترنت، الطبعة الأولى، جامعة نايف للعلوم الأمنية، الرياض، السعودية، 2004، ص 38.

أو محمول ووسيلة نفاذ ملائمة[1]، وتؤدي الإنترنت وظيفة الوسيط الناقل للمعلومات بين الأجهزة المتصلة بها من خلال أنظمة للتحكم في البيانات وبروتوكولات وعناوين خاصة مثل، حيث يتم الاتصال عادة عبر خط هاتفي أو وسيلة نفاذ أخرى متصل بجهاز المودم الذي يتولى تحويل الإشارات الرقمية وتيسير انتقال الرسائل بين المرسِل والمرسَل إليه مرورًا بالخادم[2].

وتُعدّ شبكات الاتصال عنصرا جوهريا في تكوين النظام المعلوماتي، إذ لا يتحقق المفهوم الفني والقانوني للنظام المعلوماتي بمجرد وجود حاسوب معزول عن أي شبكة، ما دام هذا الحاسوب عاجزًا عن التفاعل مع غيره من الأنظمة وعن إرسال أو استقبال المعلومات[3]، في وقت باتت فيه شبكة الإنترنت أكبر منظومة معلوماتية عرفها العالم، بما توفره من خدمات كالتبادل الفوري للمعلومات، والبريد الإلكتروني، والتجارة الإلكترونية، والتعاقد عن بُعد وغيرها من الخدمات التي أضحت ملازمة للحياة اليومية[4]، وإن كانت في الوقت ذاته تشكل منفذًا مفضلاً لمجرمي المعلوماتية لارتكاب اعتداءات إلكترونية تطال مختلف الأهداف المرتبطة بها[5].

وقد تحوّلت هذه الشبكات ذاتها إلى مسرح للجريمة تُمارس في إطاره إجراءات قانونية خاصة بالبحث والتحري والتحقيق بغرض كشف ملابسات الجرائم المعلوماتية وضبط مرتكبيها، عبر آليات وإجراءات مستحدثة لم تكن معروفة في إطار أنماط الإجرام التقليدي[6].

---

[1] Don Parker, Fighting Computer Crime, New York : Wiley Computer Publications, 1983, p, 156

[2] Andrew Charlesworth, Information Technology Law, London: Butterworths, 1999, p, 245.

[3] محمد بن صالح الجمال، الجريمة المعلوماتية في التشريع الجزائري، منشورات الجمعية الجزائرية للبحث القانوني، الجزائر، 2015، ص، 134.

[4] Nahla Abdul Qader Al-Mumeni, Cybercrimes : Their Nature and Characteristics, Dar Al-Halabi Legal Publications, Beirut, 2009, p, 201.

[5] عبد الرحمن عثماني، جرائم تقنية المعلومات في ظل الاتفاقية العربية، رسالة ماجستير، جامعة ورقلة، 2022، ص، 156.

[6] Grabosky, Peter. Cybercrime: The Challenge of Trans-national Crime. Sydney: Federation Press, 2001, p, 89

وبذلك تُعدّ النظم المعلوماتية عصب الحياة في مجتمع المعلومات المعاصر بما تتيحه من وسائل وتقنيات متقدمة للتعامل مع المعلومة عن طريق الحواسيب وشبكات الاتصال، وقد أفضت مزاياها إلى اعتماد الحكومات والشعوب عليها بشكل شبه كلي لتعزيز قدراتها الأدائية وتطوير خدماتها[1]، غير أن هذا التطور المتسارع ولد في المقابل شعورًا متزايدًا بخطر التهديد الأمني نتيجة الاعتداءات الإلكترونية التي تستهدف هذه النظم بما تختزنه من معلومات شخصية ومالية وسرّية، الأمر الذي أفضى إلى بروز فرع علمي وتطبيقي مستقل يُعرف بـ الأمن المعلوماتي بوصفه الإطار المعني بحماية النظم المعلوماتية ومحتوياتها من المخاطر والتهديدات[2].

3- الأمن المعلوماتي: الامن المعلوماتي هو فرض ضوابط صارمة على سبل واساليب الوصول الى المعلومات، بهدف اضفاء الشرعية على حدود الصلاحيات واستخداماتها، كما يُعرَّف ايضا باتخاذ الاحتياطات والتنظيمات اللازمة للمحافظة على سلامة المعلومات المخزنة في الحواسيب من الاعطال والحوادث او الجرائم المتعمدة، وتتفق تعاريف الامن المعلوماتي على الحفاظ على المكونات المادية للحواسيب والاجزاء المرتبطة بها، كذلك ضمان سلامة المعلومات وسِرّيتها وملكيّتها والاستفادة الفعّالة منها، منع تداخل استخدامها او تخريبها او استبدالها ببيانات مضلِّلة او تحرُّفها او اساءة تفسيرها او الغائها او سرقتها او الفشل في استثمارها، ومعالجة جميع الخروقات المتعلقة بالسلامة والسِرِّيَّة والملكية لصالح صاحب المعلومة.

[1] Loader, Brian D., and Don Tapscott, eds. The Governance of Cyberspace. London : Routledge, 1998, p, 145

[2] Wall, David S. Cybercrime: The Transformation of Crime in the Information Age. Cambridge : Polity Press, 2007, p. 203.

ويلخص ذلك في أن الامن المعلوماتي بانه العلم الذي يعمل استراتيجيات الحماية للمعلومات من المخاطر المهددة لها وانشطة الاعتداء عليها، بما يشمل الوقاية والكشف والاستجابة للتهديدات[1].

ويتمتع مجال الامن المعلوماتي بأهمية بالغة نظرا لارتفاع قيمة المعلومات ودورها الحساس، خاصة بالنسبة للدول في المجالات الامنية والعسكرية والاقتصادية ذات الطابع الاستراتيجي، اذ يرتبط عنصر السرية ارتباطا وثيقا بما قد يفضي اليه فقدانها من خسائر فادحة [2].

كما ان تقنية المعلوماتية افضت، على صعيد الحياة الشخصية، الى تحديات جديدة تتمثل في زيادة كمية البيانات المجتمعة والمعالجة، باعتبارها مصدرا غنيا بمعلومات تعود الى عادات الافراد وهوياتهم وسلوكياتهم وآرائهم واتجاهاتهم، حيث تتدفق هذه المعلومات عبر الحدود دون معنى للحدود الجغرافية او السياسية، معرضة لجهات داخلية وخارجية او غير معروفة، مما ينجر اساءة استخدامها في دول لا تتصف بمستويات حماية قانونية كافية للمعلومات[3].

4- الجريمة المعلوماتية: لقد اجتذب مفهوم الجريمة المعلوماتية اهتمام الفقهاء والقانونيين والمختصين في مجال المعلوماتية، بهدف وضع تعريف شامل ومتوازن لهذا السلوك الاجرامي حاول كل منهم، وفق اختصاصه، صياغة تعريف ملائم، فمنهم من اكتفى بتعريف ضيق يقتصر

[1] عمر بن محمد العتبى، الأمن المعلوماتي ومدى توافقه مع المعايير المحلية والدولية، رسالة مقدمة لأجل نيل شهادة الدكتوراه، قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، السعودية، 2010، ص 15.

[2] Soltan, Khaled. Cybersecurity and Cyberwarfare: An Introduction. Hoboken: Wiley, 2017, p, 112

[3] Schneier, Bruce. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W.W. Norton & Company, 2015, p, 189

على الجرائم المرتبطة بالحاسوب والتي تشكل انتهاكا للقانون الجنائي، ومنهم من تبنى تعريفا واسعا يشمل كل جريمة يستخدم فيها الحاسوب[1]، وهو ما يفتقر الى الدقة والتحديد.

فيجب الرجوع الى أصله اللغوي بالفرنسي (La Cybercriminalité)، حيث يعود جذورها الى الكلمة اليونانية (Kubernan) بمعنى التحكم والتسيير، وفي سياق المعلوماتية يشير الى المعالجة الآلية للمعطيات، وقد امتد استعمال هذا المصطلح ليشمل كافة اشكال الاجرام الرقمي كالغش المعلوماتي والارهاب المعلوماتي[2].

اما من الناحية القانونية، فلا يوجد مصطلح موحد دوليا للدلالة على الجرائم الناشئة عن سوء استغلال النظم المعلوماتية او اساءة استخدامها، بل تختلف التسميات، فبعض الفقهاء يصفها بـ جريمة الغش المعلوماتي، واخرون بـ جريمة الاختلاس المعلوماتي، وآخرون يصفونها بـ جرائم الاحتيال المعلوماتي، غير ان المصطلح الاكثر شيوعا وانتشارا يبقى الجريمة المعلوماتية[3].

وقد تعددت التعاريف الواردة بشأن الجريمة المعلوماتية مع تعداد النظم القانونية والتشريعات والتوجهات الفقهية، مما يعكس التحدي في ضبط مفهوم موحد يتناسب مع خصوصيات هذا النوع الجديد من الاجرام الرقمي.

- **التعريف الاصطلاحي:** عرفت منظمة التعاون الاقتصادي والتنمية (O.E.C.D) سنة 1983 الجريمة المعلوماتية بأنها كل فعل او عمل غير مشروع او مخالف للأنظمة وغير مرخص،

[1] عمر بن محمد العتبي، مرجع سابق، ص 21.

[2] Myriam Quéméner, Yves Charpenel, La Cybercriminalité, Edition Economica, Paris, France-2010, p 07

[3] محمد بن صالح الجمال، مرجع سابق ص 23.

يستهدف انظمة المعالجة الآلية للمعلومات او تبادلها او نقلها، وتشمل بهذا المفهوم كل الجرائم التي تقع او تمس بشبكات الاتصال بصفة عامة، وشبكة الانترنت بصفة خاصة[1].

كما ورد تعريف الجريمة المعلوماتية في مؤتمر الامم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين الذي عقد بفينا سنة 2000 بأنها كل جريمة يمكن ارتكابها بواسطة نظام حاسوبي او شبكة حاسوبية او داخل نظام الحاسوب، وتشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية[2].

- التعاريف الفقهي:

يزعم أنصار الاتجاه الفقهي الأول عن طريق الفقيه (ميروي) الذي عرفها بأنها ذلك الفعل غير المشروع الذي يتورط في ارتكابه الحاسب، كما عرفها (روزبلات) بأنها نشاط غير مشروع موجّه لنسخ او تغيير او حذف او الوصول الى المعلومات المخزنة داخل الحاسوب او التي تحول عن طريقه، واكتفى (سولريز) بأنها اية نمط من الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات[3]

هذا وقد حاول الاتجاه الثاني المعاكس تفادي نقص التعاريف السابقة فعرفت بأنها كل فعل او امتناع عمدي ينشأ عن الاستخدام غير المشروع للتقنية المعلوماتية بهدف الاعتداء على

[1] OECD, Computer Crime : An International Perspective, Paris : Organisation for Economic Co-operation and Development, 1983, p12

[2] United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 10th Congress, Vienna, 2000, Report, p 45.

[3] محمد سيد سلطان، قضايا قانونية في امن المعلومات وحماية البيئة الإلكترونية، دار ناشري للنشر الإلكتروني، الكويت، سنة 2012، ص 62.

الاموال المادية او المعنوية، كما عرفت بأنها كل سلوك سلبي كان ام إيجابي يتم بموجبه الاعتداء على البرامج او المعلومات للاستفادة منها بأية صورة كانت[1].

ورأى (ميشال وكريدو) ان سوء استخدام الحاسوب يشمل استخدامه كأداة لارتكاب الجريمة، بالإضافة الى الولوج غير المصرح به لحاسوب المجني عليه او بياناته، ويمتد الى الاعتداءات المادية على الحاسوب او المعدات المتصلة به، والاستخدام غير المشروع لبطاقات الائتمان، وتزييف مكوناته المادية والمعنوية، بل وسرقة الجهاز نفسه او مكون من مكوناته[2]

- التعريف القانوني

عرف المشرع الجزائري الجريمة المعلوماتية في المادة 02 الفقرة (ا) من القانون رقم 09-04 المؤرخ في 05 اوت 2009 المتضمن قواعد الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها بأن الجرائم المتصلة بتكنولوجيات الاعلام والاتصال هي تلك الجرائم التي تمس بأنظمتها المعالجة الآلية للمعطيات المحددة في قانون العقوبات، او اية جريمة اخرى ترتكب او يسهل ارتكابها عن طريق منظومة معلوماتية او نظام للاتصالات الالكترونية[3].

1-2-1) شبكات الاتصال في النظام المعلوماتي:

يتكوّن النظام المعلوماتي، من مكوِّنات مترابطة تشمل العناصر المادية والبرمجية للحواسيب، إلى جانب شبكات الاتصال كقنوات ربط أساسية بينها والمدعومة بالأنترنت، مما يجعل

[1] نهلا عبد القادر المومني، مرجع سابق، ص 89

[2] محمد بن صالح الجمال، مرجع سابق، ص 112.

[3] المادة 02 فقرة أ، القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

الجريمة المعلوماتية تستغل هذه المكوّنات كوسائل رئيسية للوصول غير المشروع إلى المعلومات المخزنة أو المتداولة.

1-2-2) شبكة الاتصالات:

شبكة الاتصال في مجال النظم المعلوماتية، من الناحية التشريعية والفنية، هي تلك البنية التقنية التي تُنشئ ارتباطا وظيفيا بين حاسوبين أو أكثر لتبادل البيانات، سواء عبر وسائل سلكية كالكابلات والأسلاك الأرضية، أو لاسلكية كالموجات الراديوية أو الأشعة تحت الحمراء أو الأقمار الصناعية، حيث تصنّف الشبكة محلية (Local Network) اذا تم تقييد نطاقها جغرافيًا، أو واسعة النطاق (Wide Area Network) إذا امتدت على مساحة أوسع، وقد تترابط هذه الشبكات لتشكِّل بنى مترابطة، كما في حال شبكة الإنترنت التي تُمثل نموذجا عالميا لتكامل شبكات متعددة تعمل ببروتوكولات موحدة، والتي من شأنها أن تعزز دور النظم المعلوماتية كنقاط نهائية أو منافذ عبور أو وسائل لتسهيل نقل المعلومات، مما يُبرِز أهميتها في الإطار القانوني لمكافحة الجرائم المعلوماتية وضمان الأمن الرقمي[1].

1-2-3) تعريف الأنترنت:

يمثل الإنترنت أكبر شبكة حواسيب واسعة النطاق عالميا، تربط الحواسيب الشخصية بالشبكات المحلية والعامة، متاحا لأي فرد الانضمام إليه من منزله أو مكتبه أو أي مكان آخر عبر حاسوب مكتبي أو محمول مدعوم بتقنية المودم، للوصول إلى كم هائل من المعلومات[2]،

[1] هلالي عبد اللاه أحمد، مرجع سابق، ص 23.

[2] Andrew Murray, Information Technology Law: The Law and Society, 5th ed, (Oxford: Oxford University Press, 2023), PP 45-47.

وتعرف تقنيا بأنها وسيط ناقل للبيانات بين الأجهزة المتصلة، عبر أنظمة التحكم وبروتوكولات والعناوين الخاصة، حيث يتم الاتصال عبر خطوط هاتفية مرتبطة بمحول الإشارات الذي يحول الإشارات الرقمية وينقل الرسائل مرورا بالخادم[1].

وتشكل شبكات الأنترنت عنصرا أساسيا في تكوين النظام المعلوماتي، إذ لا يتحقق مفهومه الفني والقانوني بحاسوب معزل عن الشبكة، ما دام عاجزا عن التواصل مع غيره وإرسال أو استقبال المعلومات[2]، فشبكة الإنترنت تبين أكبر منظومة معلوماتية عالمية، تقدم خدمات حيوية كتبادل المعلومات والبريد الإلكتروني والتجارة الإلكترونية والتعاقد عن بعد، أضحت لازمة للحياة اليومية بتذليلها الصعوبات، غير أنها صارت ممرا مفضلا لمجرمي المعلوماتية لتحقيق أهدافهم الإجرامية، ومسرحا لجرائم تتخذ فيها إجراءات قضائية مخصصة للبحث والتحقيق والقبض على المرتكبين[3].

حيث أصبحت الحكومات والشعوب تعتمد على تقنية المعلوماتية بشكل كامل لتعزيز قدراتها الأدائية، مع السعي الدوري لتطويرها وزيادة فعاليتها وقدراتها، غير أن هذا التطور اللامتناهي لها وأثره على نمط الحياة أحدث شعوراً بالتهديد الأمني جراء الاعتداءات الإلكترونية التي تستهدف النظم المعلوماتية وما تحويه من معلومات شخصية ومالية وسرية، مما استدعى ظهور فرع علمي جديد يُعرف بمجال الأمن المعلوماتي.

[1] National Academies of Sciences, Engineering, and Medicine, Cybercrime Classification and Measurement (Washington, DC: The National Academies Press, 2025),P 23.

[2] Alex Alexandrou, Cybercrime and Information Technology, Theory and Practice (London: Routledge, 2021), P 112.

[3] United Nations Office on Drugs and Crime (UNODC), "What to Know about Cybercrime in 2025," October 25, 2025, https://www.unodc.org/unodc/frontpage/2025/October/what-to-know-about-cybercrime-in-2025.html... See 25/10/2025...21.00h

1-3) الأمن المعلوماتي:

يعد تنامي استخدامات تقنية المعلوماتية وتَوْلُد مفاهيم جديدة كالحكومة الإلكترونية والإدارة الرقمية والعقود الإلكترونية، مع انتشار مواقع التواصل الاجتماعي عبر شبكة الإنترنت واعتماد الأفراد لها يوميا، مصدرا لمخاطر أمنية تتجلى في الاعتداءات على المعطيات الرقمية، والتي تفضي إلى آثار سلبية للجرائم المعلوماتية؛ ومن منظور تحليلي، أدَّى هذا الانتشار إلى بزوغ مجال الأمن المعلوماتي كإطار موازٍ لتطور التقنية، يهدف إلى مواجهة التهديدات وحماية البيانات الشخصية والحساسة.

1-3-1) تعريف الأمن المعلوماتي:

الأمن المعلوماتي فرض ضوابط وقيود صارمة على سبل أو طرق الولوج الى المعلومات، بهدف اضفاء الشرعية على حدود وصلاحية استخدامها، كما يعرف باتخاذ الاحتياطات والتنظيمات التي تهدف الى محافظة المعلومات في الحاسوب مأمونا من الاعطال والحوادث او الجرائم المتعمدة، وتتفق غالبية التعاريف فيه على المحافظة على المكونات المادية للحاسوب و المعلومات وسلامتها وسريتها وملكيتها والاستفادة منها وحمايتها من التداخل واستخدامها غير اللائق او تخريبها، او استخدام معلومات مضللة، او تحريفها واستبدالها، او سوء تفسيرها وإلغائها او فشل استخدامها او سرقتها ومعالجة جميع الخروقات المتعلقة بالسلامة والسرية والملكية لصاحب المعلومة.

ويمكن اختصار تعريف موجز في أن الأمن المعلوماتي هو ذلك العلم الذي يبحث في استراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها وأنشطة الاعتداء عليها[1].

ويتمتع مجال الأمن المعلوماتي بأهمية بالغة نظرا لازدياد قيمة المعلومات ودورها الحساس، خاصة للدول في المجالات الأمنية والعسكرية والاقتصادية ذات الطابع الاستراتيجي، حيث ارتبط عنصر السرية بما يترتب على فقدانها من خسائر ، كما احدثت على الصعيد الشخصي تحديات وتهديدات جديدة، إذ تزيد من كمية البيانات المجمعة والمعالجة كمصدر غني بالمعلومات الشخصية المتعلقة بالعادات والهويات والسلوكيات والآراء والاتجاهات، وتتدفق عبر الحدود دون اعتبار للحدود الجغرافية أو السياسية، معرضة لجهات داخلية وخارجية أو غير معروفة، مما ينجر عنه إساءة استخدامها في دول لا تتصف بمستويات حماية عالية سواء كانت علمية أو تشريعية[2].

1-3-2) اهداف الأمن المعلوماتي:

تتجسد الأهداف الأساسية لاعتماد استراتيجيات الأمن المعلوماتي في أي منظومة معلوماتية في الحفاظ على سلامة المعلومة من حيث ثلاثة مبادئ جوهرية الإتاحة، والتكامل (النزاهة)، والسرية، وذلك بما يضمن حمايتها من التهديدات الرقمية المتنوعة، كما يُعرف بنموذج CIA Triad[3].

[1] عمر بن محمد العتبي، الأمن المعلوماتي ومدى توافقه مع المعايير المحلية والدولية، رسالة مقدمة لأجل نيل شهادة الدكتوراه، قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، السعودية، 2010، ص15 وما يليها.

[2] Jamal Awwad Alkharman et al, Cyber Attacks and its Implication to National Security, Pakistan Journal of Criminology 16, no. 3 (2024), PP 853- 861.

[3] أعمدة أمن المعلومات والأمن السيبراني :(CIA Triad) الدليل الكامل، Professor Technology، 10 أكتوبر 2024، https://www.professor-technology.com/2024/10/cia-triad.html... تاريخ الاطلاع 2024/02/12 ...12.00د.

– **مبدأ الإتاحة:** يشير مبدأ الإتاحة (Availability) إلى ضمان توافر المعلومة في صورتها الأصلية، في أي مكان ووقت مطلوب، مع منع أي أشكال من التخريب أو الخلط الذي يؤدي إلى تلويثها أو تعطيل استخدامها[1].

– **مبدأ التكامل:** يُقصد بمبدأ التكامل أو النزاهة (Integrity) الحفاظ على وحدة محتوى المعلومة المعالجة آليًا وعدم تجزئتها، حيث يُعد الأمن المعلوماتي الضمانة لسلامتها الكاملة منذ بداية المعالجة وحتى نهايتها، من خلال منع التلاعب الجزئي أو الكلي بها[2].

– **مبدأ السرية:** يتمثل مبدأ السرية (Confidentiality) في ضمان حفظ المعلومات المخزنة أو المنقولة عبر الشبكات، وعدم الاطلاع عليها أو استخدامها إلا بموجب إذن صريح، مع تحديد حدود الصلاحيات سواء كانت كلية أو جزئية، بما في ذلك الحقوق المتعلقة بالقراءة، أو الحذف، أو التعديل[3].

– **مبدأ الضرورة:** في ظل الاعتماد المتزايد على النظم المعلوماتية، برزت الحاجة الماسة إلى تعزيز استراتيجيات وتقنيات الأمن المعلوماتي، نتيجة انتشار الإجرام المعلوماتي المرتبط بانتشار التقنيات اليومية وتغلغلها في الحياة اليومية؛ إذ يُشكل أي تهاون أو فراغ تشريعي منفذًا للمجرمين الرقميين، مما يهدد المصالح الأساسية للدولة، لا سيما الدفاعية العسكرية والمالية والصحية،

[1] الضوابط الأساسية للأمن السيبراني"، ega.ee، 2019، https://ega.ee/wp-content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf. ...تاريخ الاطلاع 2024/02/12 ...10.12د

[2] الثلاثية الأساسية لأمن المعلومات"CIA Triad ، root-x.dev، https://root-x.dev/blog/article/CIA-Triad. تاريخ الاطلاع 2024/02/12 ...12.45د

[3] أعمدة أمن المعلومات والأمن السيبراني :(CIA Triad) الدليل الكامل، مرجع سابق.

إضافة إلى المصالح الشخصية للأفراد في الفضاء الرقمي المتوسع، خاصة مع تحويل التكنولوجيا المعلوماتية إلى أجهزة محمولة ذكية متاحة على الدوام[1].

- **مبدأ التقنين:** استجابت التشريعات الوطنية والدولية، رغم اختلاف تعريفاتها للجريمة المعلوماتية، بتطوير استراتيجيات أمنية حديثة تهدف إلى مكافحتها وملاحقة مرتكبيها، الذين يتميزون بخصائص فريدة تجعل محاسبتهم أمرًا معقدًا نظرًا لخصوصيات جرائمهم وأساليب التمويه التي يلجؤون إليها[2].

1-4) الجريمة المعلوماتية:

لقد أثار مفهوم الجريمة المعلوماتية اهتمام الفقهاء القانونيين والمختصين في مجال تكنولوجيا المعلومات، بهدف صياغة تعريف شامل ومتوافق لهذا النوع من الجرائم، حيث سعى كل منهم إلى تقديم تعريف يتناسب مع اختصاصه؛ فبعضهم تبنى تعريفًا ضيقًا يقصرها على "الجرائم المرتبطة بالحاسوب والتي تشكل انتهاكًا للقانون الجنائي"[3]، بينما اعتمد آخرون تعريفا واسعا يشمل "كل جريمة يُستخدم فيها الحاسوب"، مما يفتقر إلى الدقة والتمييز[4]

ولصياغة تعريف متكامل لهذا السلوك الإجرامي، ينبغي الرجوع أولاً إلى المدلول اللغوي للمصطلح، ففي اللغة الفرنسية La Cybercriminalité ، يعود أصل كلمة Cyber إلى الكلمة

[1] عناصر الأمن السيبراني"، rmg-sa.com، 19 فبراير 2025، https://www.rmg-sa.com تاريخ الاطلاع 2024/02/20 ...09.00د

[2] أحمد محمد براك، شرح قانون الجرائم الإلكترونية، الإطار المفاهيمي، المواجهة الموضوعية- المواجهة الإجرائية في ضوء القانون رقم 17 لسنة 2023، دراسة تحليلية تأصيلية مقارنة، دار الثقافة للنشر والتوزيع، عمان، 2024، ص 112.

[3] الحلبي محمد، الجريمة المعلوماتية، التحديات القانونية، دار الحلبي الحقوقية، بيروت، 2019، ص 78.

[4] احمد شريف، الجرائم الإلكترونية، دراسة مقارنة، دار النهضة العربية، مصر، 2020، ص 56.

انظر كذلك: عمر بن محمد العتبي، مرجع سابق، ص 21

اليونانية Kubernan بمعنى التحكم والتسيير، وفي سياق المعلوماتية يشير إلى المعالجة الآلية للبيانات، وقد امتد استخدامه ليشمل جميع أشكال الإجرام الرقمي كالغش المعلوماتي والإرهاب المعلوماتي[1].

ومن الناحية القانونية، لا يوجد مصطلح موحد يشمل الجرائم الناتجة عن إساءة استغلال أو سوء استخدام النظم المعلوماتية، فبعض الفقهاء يصفونها بـ "جرائم الغش المعلوماتي"، وآخرون بـ "جرائم الاختلاس المعلوماتي"، أو "جرائم الاحتيال المعلوماتي"، إلا أن المصطلح الأكثر شيوعا واستخداما في الأدبيات القانونية يبقى "الجريمة المعلوماتية"[2]

1-4-1) تعريف الجريمة المعلوماتية:

الجريمة المعلوماتية هي كل سلوك إجرامي غير مشروع يرتكب باستخدام الحاسب الآلي أو الشبكات المعلوماتية أو أي تقنية اتصال حديثة، سواء كان الحاسوب أداة في الجريمة أو هدفا لها، بهدف تحقيق مكاسب مادية أو معنوية غير مشروعة مع إلحاق الضرر بالضحايا، هذا وقد تعددت التعاريف الواردة بشأنها بتعدد النظم والتشريعات والاتجاهات الفقهية فعرفت بأنها:

1-4-2) التعريف الاصطلاحي:

عرّفت منظمة التعاون الاقتصادي والتنمية (OECD) الجريمة المعلوماتية في عام 1983 بأنها "كل فعل أو عمل غير مشروع، أو مخالف للأنظمة والتشريعات، أو غير مرخص، يستهدف

[1] دوارعلي، قانون الأمن السيبراني، دار الغرب الإسلامي، الجزائر، 2022، ص 45.

[2] بن عيسى، فاطمة، الإجرام الرقمي في التشريعات العربية، منشورات الجامعة التونسية، تونس، 2023، ص123

أنظمة المعالجة الآلية للمعلومات أو تبادلها أو نقلها[1]"، وتشمل الجريمة المعلوماتية بهذا المفهوم " كل الجرائم التي يمكن أن تقع أو تمس بشبكات الاتصال بصفة عامة، وشبكة الأنترنت بصفة خاصة[2].

كما قدّم مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين، المنعقد في فيينا عام 2000، تعريفا للجريمة المعلوماتية يعد الأوسع نطاقا، حيث وصفها بأنها "كل جريمة يمكن ارتكابها بوساطة نظام حاسوبي أو شبكة حاسوبية، أو داخل بيئة النظام الحاسوبي ذاته، مما يشمل مبدئيًا جميع الأفعال الإجرامية المحتملة في الفضاء الإلكتروني، أما الخبير الأمريكي دونالد باركر (Parker) ، فقد وسّع المفهوم ليحيط بكافة أشكال التعسّف في استخدام النظم المعلوماتية، إذ عرفها بأنها "كل فعل إجرامي متعمّد، بغض النظر عن طبيعة صلته بالتكنولوجيا المعلوماتية، يُحدث خسارة مادية أو معنوية للمجني عليه، أو يكسب للفاعل مكاسب غير مشروعة[3].

1-4-3) التعريف الفقهي:

- **التعريف الضيق:** تزعّم هذا الاتجاه الفقهي الفقيه ديفيد فان دير ميرْوِه (Merwe) من خلال تعريفه الموجز والمضمون، حيث وصف الجريمة المعلوماتية بأنها "الفعل غير المشروع الذي يتورّط في ارتكابه الحاسوب كأداة أو وسيط أساسي[4]، أما روزبلات (Rosblat) بأنها "نشاط غير مشروع يهدف إلى نسخ أو تعديل أو حذف أو الوصول غير المصرّح به إلى المعلومات المخزنة

[1] منظمة التعاون الاقتصادي والتنمية(OECD) ، تقرير حول الجرائم المعلوماتية، باريس، 1983، ص 23

[2] Myriam Quéméner- Yves Charpenel - La Cybercriminalité – op,cit,p 08.

[3] تركي بن عبد الرحمان المويشير، مرجع سابق، ص ص15- 16.

[4] محمد أمين الشوابكة، جرائم الحاسوب والأنترنت (الجريمة المعلوماتية)، دار الثقافة للنشر والتوزيع، عمان الأردن،2009، ص 08.

داخل الحاسوب أو المنقولة عبره"، أما سولريز (Solerez) ، فقد اعتمد تعريفًا توسّعيًا يشمل "أي نمط من أنماط الجرائم التقليدية المنصوص عليها في قانون العقوبات، شريطة ارتباطها بتقنيات المعلومات"[1].

– **التعريف الموسع:** سعى هذا الاتجاه الفقهي إلى تقديم تعريف موسع للجريمة المعلوماتية، بهدف سد الثغرات الظاهرة في التعاريف السابقة، حيث عُرّفت بأنها "كل فعل أو امتناع متعمّد يترتب على الاستخدام غير المشروع للتقنيات المعلوماتية، بهدف الاعتداء على الأموال المادية أو المعنوية"، أو هي كل سلوك إجرامي، سواء كان إيجابيا أو سلبيا، يُرتكب بموجبه اعتداء على البرامج الحاسوبية أو المعلومات المُخزَّنة، بهدف الاستفادة منها بأي شكل كان[2].

كما تبنا الفقيهان ميشال وكريدو (Michel & Credo) في رؤية شمولية لمفهوم سوء استخدام الحاسوب، حيث يشمل ذلك استخدامه كأداة لارتكاب الجريمة الجنائية، بالإضافة إلى حالات الولوج غير المصرح به إلى أجهزة الحاسوب الخاصة بالمجني عليه أو البيانات المخزنة لديه، وتمتد صلاحية هذا التعريف لتشمل الاعتداءات المادية المباشرة على الجهاز الحاسوبي ذاته أو المعدات الملحقة به، وكذلك الاستخدام غير المشروع لأرقام وبطاقات الائتمان، وتزييف المكونات المادية والبرمجية للحاسوب، بل ويصل الأمر إلى سرقة الجهاز الحاسوبي ككل أو أي مكوّن أساسي من مكوّناته[3]

[1] محمد سيد سلطان، قضايا قانونية في امن المعلومات وحماية البيئة الإلكترونية، دار ناشري للنشر الإلكتروني، الكويت، 2012، ص 62.

[2] محمد سيد سلطان، مرجع متوفر على الموقع الرسمي لدار ناشري للنشر الإلكتروني، تاريخ التصفح2024/02/20، الرابط الإلكتروني:
https://www.nashiri.net/latest/books-mags-news/5051-2012-01-27-22-05-28-v15-5051.htm

[3] محمد أمين الشوابكة، مرجع سابق، ص ص 45-46

1-4-4) التعريف التشريعي:

عرف المشرع الجزائري الجريمة المعلوماتية في نص المادة 02- الفقرة -أ- من القانون رقم 09-04 المؤرخ في 05 أوت 2009 والمتضمن لقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات لإعلام والاتصال ومكافحتها بالقول بأن " الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هي تلك جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات أو أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية"[(62)]، كما يعرفها القانون الأمريكي بأن الجريمة هي عملية الولوج المتعمّد إلى جهاز حاسوبي محمي (protected computer) دون تصريح أو متجاوزًا التصريح الممنوح، بهدف الحصول على معلومات، الاحتيال، إلحاق الضرر، أو الابتزاز[1].

أما بالنسبة لاتفاقية بودابست بشأن الجرائم الإلكترونية فهي لا تحتوي على تعريف عام موحد لـ «الجريمة المعلوماتية"، بل تعتمد نهجًا عمليًا يُلزم الدول الأطراف بتجريم تسع جرائم المحددة في المواد 02 الى المادة 10 وهي

1. الولوج غير المشروع إلى أنظمة الحاسوب.
2. التنصُّت غير المشروع على البيانات.
3. تعديل البيانات/البرامج غير المصرح به.
4. إعاقة النظام (تعطيل الخدمة).

[1] نفس المرجع، ص ص 72-73

5. إنتاج/توزيع أدوات الجريمة (برمجيات خبيثة).

6. الاحتيال الحاسوبي.

7. تزوير البيانات الحاسوبية.

8. الإضرار بالبيانات.

9. الإضرار بالنظام.

كما تُشِير الديباجة إلى "الأفعال الموجهة ضد سرية، سلامة، وإتاحة أنظمة الحاسوب والبيانات "كمحور الاتفاقية، مع التركيز على التعاون الدولي السريع في التحقيق والتسليم[1].

1-5) خصائص ومميزات الجريمة المعلوماتية:

تميز مفهوم الجريمة المعلوماتية، كما تم التطرق إليه سابقًا، بأنه نشاط إجرامي مترابط ارتباطًا وثيقًا مع استخدام تقنيات الحاسوب وشبكات الاتصال، مما يُضفي عليها طابعًا خاصًا يميزها عن المفاهيم التقليدية للجريمة المادية، وتختلف اختلافا جذريًا عن السلوكيات الإجرامية التقليدية، التي ترتبط عادةً بأفعال مادية تترك أثرًا ملموسا في العالم الخارجي، حيث يتحول العالم الافتراضي إلى ملاذ آمن لها، مما يجعل السلوكيات الإجرامية غالبًا غير مرئية أو صعبة الإدراك المباشر، وهذا ما يميز هذا النوع من الجرائم عن باقيه من الجرائم الأخرى.

[1] المادة 02- الفقرة -أ- من القانون رقم 09-04 المؤرخ في 05 أوت 2009 والمتضمن لقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات لإعلام والاتصال ومكافحتها

1-5-1) انها جريمة عابرة للدول والقارات:

لقد أدّى ارتباط دول العالم كافة بشبكة الاتصالات الدولية عبر الأقمار الصناعية وشبكة الإنترنت إلى تحقيق عولمة الجريمة المعلوماتية كظاهرة ممكنة ومنتشرة، فأصبحت هذه الجرائم تتجاوز مفهوم الحدود الإقليمية للدول، مكتسحة الساحة العالمية بأكملها، حيث يمكن ارتكابها من أي نقطة جغرافية دون قيود، مما يستدعي تعاونًا دوليًا مكثفا في مكافحتها، كما تعقد هذه الطبيعة العابرة للحدود عمليات الملاحقة القضائية والتسليم الدولي، إذ تتطلّب تطوير أطر قانونية موحّدة كاتفاقية بودابست لضمان فعالية الاستجابة الأمنية[1].

حيث تثير الطبيعة العابرة للحدود التي تتميز بها الجريمة المعلوماتية تحديات قانونية جوهرية تتعلق بتحديد الدولة صاحبة الاختصاص القضائي، وتطبيق القانون الواجب العمل به، إلى جانب الإشكاليات المرتبطة بإجراءات الملاحقة والتحقيق القضائي، مما يجعل استغلال المجرمون المعلوماتيون الفراغات التشريعية في الدول التي تفتقر إلى قوانين مكافحة الجرائم السيبرانية، مختارين إياها كملاذ آمن لارتكاب أفعالهم الإجرامية، بينما تتجسّد آثارُ هذه الأفعالِ في أرجاء العالم، مما يعقد بشكل بالغ إجراءاتَ التحقيقِ والمحاكمة والتسليم الدولي[2]، مما تستدعي هذه الطبيعة المركبة تطوير آليات تعاون قضائي موحدة كالاتفاقية الدولية، لضمانِ تكاملِ وتوحيد المعاييرِ التشريعية لمواجهة الإجرام السيبراني العابر للحدود[3].

[1] ART 1030 sec (a) Computer Fraud and Abuse Act (18 U.S.C. § 1030), 1986, It was modified in 2008

[2] اتفاقية مجلس أوروبا رقم 185 بشأن الجرائم الإلكترونية، بودابست، 23 نوفمبر2001

[3] عبد العال الدريبي، مرجع سابق، ص 55

لقد دفعت التحديات الناجمة عن الجريمة المعلوماتية دول العالم إلى تكثيف الجهود الدولية والإقليمية لمكافحتها، حيث تُبرز اتفاقية مجلس أوروبا بشأن الجرائم الإلكترونية (بودابست، 23 نوفمبر 2001) كأهم إطار قانوني عالمي في هذا المجال، والتي فُتحت للتوقيع للدول غير الأوروبية، وانضمت إليها الولايات المتحدة في 22 سبتمبر 2006، مؤكدة أهميتها في توحيد آليات التعاون القضائي والتسليم[1].

كما اعتمد مجلسا وزراء الداخلية والعدل العرب في القاهرة بتاريخ 21 ديسمبر 2010 الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في الجلسة ذاتها، مُعبرين عن التزامهم بتنسيق الجهود الإقليمية لمواجهة التحولات الرقمية الناجمة عن انتشار تقنيات الاتصالات والنظم المعلوماتية[2].

حيث يُكْمِلُ الإطاران بعضهما الأول يوفر الإطار الشامل عالميا، والثاني يركُّ على الخصوصيات التشريعية العربية لاستجابة فعالة للإجرام السيبراني العابر للحدود.

1-5-2) صعوبة الاثبات والكشف عنها:

تتصف الجرائم المعلوماتية بخصائص تميزها عن الجرائم التقليدية للإجرام أبرزها طابع الخفاء وعدم الضهور الذي يهيمن على غالبية حالاتها حيث يمكن للضحية ان يبقى في حالة جهل تام بوجود الجريمة ضده وحتى لو تم تنفيذها اثناء اتصاله المباشر بالشبكة الالكترونية، ويتمتع المجرم المعلوماتي فيها بمهارات فنية رقمية متقدمة ومتخصصة تمكنه من تنفيذ الفعل

[1] Svantesson, Dan Jerker B. "Jurisdiction in Cyberspace: Towards 'Core Principles'." Tilburg Law Review 21, no. 1 (2015): pp. 46-56.

[2] المادة 01، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، هي وثيقة تكاملية اعتمدتها مجلسا وزراء الداخلية والعدل العرب في القاهرة بتاريخ 21 ديسمبر 2010، وتعد الإطار القانوني الإقليمي الرئيسي لمكافحة الإجرام السيبراني في العالم العربي

الاجرامي بدقة فائقة ودون ترك اثار واضحة كإرسال البرمجيات الضارة malware التي تعمل في الخلفية دون اشعار، التجسس الرقمي على البيانات المخزنة او المنقولة، والولوج غير المشروع للأنظمة باستخدام ثغرات امنية غير مرئية، وما يزيد من خصوصية صعوبة اكتشافها هي:

1- سرعة التنفيذ الميداني: تتميز الجريمة المعلوماتية بسرعة تنفيذ استثنائية، حيث لا يتجاوز الفعل التنفيذي ضغطة لوحة مفاتيح أو لمسة شاشة، مع الاستعداد التقني المسبق الذي يشمل توفير الأجهزة والبرمجيات المتخصصة.[1]

2- التنفيذ عن بعد (Remote Execution) :لا تتطلب معظم الجرائم المعلوماتية – باستثناء سرقة المعدات المادية– وجود الجاني في موقع الجريمة، إذ يمكن ارتكابها من أي مكان جغرافي أو دولة أخرى، كالاختراق الشبكي، اعتراض التحويلات المالية، تخريب البيانات، أو الاعتداء على حقوق الغير[2].

3- إخفاء المعالم الإجرامية :تكتسب هذه الجرائم طابعا خفيا جوهريا، فلا تُكتشف آثارها إلا بعد تحليل فني متخصص في الطب الشرعي الرقمي، مما يعيق عمليات الإثبات القضائي والملاحقة الجنائية[3].

---

[1] أحمد محمد الشريف، الجريمة المعلوماتية: الخصائص والتحديات القانونية، الجزائر، دار الفكر، 2024، ص ص 78-80.

[2] Samira Bin Issa, "Cybercrimes Across Borders: Issues of Judicial Jurisdiction," Journal of Law and Technology 12, no 3, 2025, 145-150.

[3] هشام رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي، مجلة الأمن والقانون، الامرات المتحدة، دبي، العدد الثاني، 1999، ص 11.

ولعل عملية "ماريبوسا(Mariposa) كانت أكبر دليل على محاولة الكشف والصعوبة التي تتميز فيها هذه الجريمة كانت تقريراً رسمياً للشرطة الإسبانية يركز على تفكيك أكبر شبكة بوت نت (botnet) في التاريخ، والتي كانت تتحكم بأكثر من 13 مليون حاسوب في 190 دولة لسرقة البيانات المالية وتوزيع البرمجيات الضارة.

موضوع التقرير بالتفصيل

يهدف التقرير إلى توثيق التعاون الدولي بين الشرطة الإسبانية ومعهدPanda Security ، مع التركيز على:

كما أن الجريمة المعلوماتية تتخذ من البيئة الرقمية للحاسوب والإنترنت ملاذا آمنا لها، إذ تتجسّد في حزمة من البيانات الإلكترونية غير المرئية التي تتدفّق عبر النظم المعلوماتية، مما يُتيح لمرتكب الجريمة طمس الأدلّة ومحوها بالكامل بسهولة فائقة، وهنا تعجز الوسائل التقليدية للبحث والتحقيق أمام هذه الجرائم، نظراً لتخصّصها في مسارح الجرائم التقليدية التي تعتمد على المعاينة المادّية والاحتفاظ بالآثار الملموسة، بينما يتضاءل دور مسرح الجريمة المعلوماتية في الإفصاح عن الأدلّة للأسباب التالية[1]:

- **عدم وجود آثار مادية** لا تترك الجريمة المعلوماتية أثرا ملموسا، مع صعوبة بالغة في الاحتفاظ بأي آثار رقمية إن وُجِدَتْ

- **الاعتماد على الذكاء التقني** تعتمد على أعلى مستويات الخبرة الرقمية في الارتكاب، مما يعجز المحقق التقليدي عن التعامل معها لنقص التكوين المعلوماتي والتقنيات المناسبة

- **نقص الخبراء المتخصّصين** للكشف عن الحقيقة والاستعانة بخبراء فائقين التخصّص، وهو أمر يصعب تحقيقه لقلة عددهم وانشغالهم بقضايا أخرى[2]

تفكيك البنية التحتية :إغلاق أكثر من 500 خادم C&C في 9 دول.

اعتقال الجناة :القبض على ثلاثة مشتبه بهم رئيسيين في إسبانيا.

التأثير العالمي :حماية ملايين المستخدمين من سرقة الهويات والبيانات المصرفية

أنظر: هيئة مكافحة الجريمة الإلكترونية الدولية، "عملية ماريبوسا: تفكيك أكبر شبكة بوت نت في التاريخ"، تقرير رسمي ،مدريد الشرطة الإسبانية، 2010

[1] حمد خليفة الملط، الجرائم المعلوماتية: دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2005، ص ص 89-92

[2] عبد العال الدريبي، مرجع سابق، ص 57.

1-5-3) جريمة هادئة:

تميز الجرائم التقليدية، مثل جرائم المخدرات والإرهاب والسرقة والسطو المسلح الى غير ذلك من الجرائم، باستخدام أدوات ووسائل مادية ملموسة، غالبًا ما ترتبط بالعنف المباشر، بينما الجرائم المعلوماتية، فتُصنف كجرائم "ناعمة أو هادئة" بطبيعتها، إذ لا تحتاج إلى عنف جسدي أو مواجهة مباشرة، حيث يتم نقل البيانات عبر الحواسيب أو سرقة الأرصدة المصرفية دون الحاجة إلى تبادل إطلاق النار مثلا، بينما الجرائم التقليدية تعتمد على تفاعل مادي يتضمن أدوات قابلة للرؤية والعنصر البشري المباشر، مما يجعلها عرضة للكشف عبر الشهود أو الأدلة الملموسة، وفي المقابل، تتسم الجرائم المعلوماتية باللامادية، إذ تحدث في الفضاء الرقمي من خلال نقل البيانات أو التلاعب الإلكتروني، دون الحاجة إلى عنف أو مواجهة وتشمل هذه الجرائم أفعالاً مثل الاختراق غير المصرح به أو سرقة الهوية الرقمية، والتي تتميز بالسرية والانفاذية عبر الحدود، مما يتطلب إطارا قانونيا متخصصا يركز على الحماية الرقمية بدلا من مكافحة العنف التقليدي. هذا التمييز يبرز الحاجة إلى تشريعات حديثة تتناسب مع طبيعة التهديدات السيبرانية[1].

1-6) الطبيعة القانونية للجريمة المعلوماتية:

تشمل الجريمة المعلوماتية أفعالًا مثل الاختراق غير المشروع، سرقة البيانات، أو التلاعب الرقمي، حيث يُعتبر موضوعها الأساسي المعلومة الرقمية كما هو منصوص عليه في قوانين مثل القانون الجزائري رقم 20-20، والتي تتسم بمعيار ثلاثي وسيلة الارتكاب (النظام الإلكتروني)،

[1] عبد العال الدريبي، مرجع سابق، ص 57.

انظر كذلك: تركي بن عبد الرحمان المويشير، مرجع سابق ، ص 24 وما يلها

موضوع الاعتداء (المعطيات الآلية)، والركن الشرعي المستمد من قانون العقوبات، وتتميز الجريمة المعلوماتية العابرة للحدود، السرية، والصعوبة في الإثبات، مما يتطلب تشريعات متخصصة تتجاوز الإطار التقليدي للعقوبات، هي جريمة "مستحدثة" تعكس تطور الذكاء الإجرامي في استحداثها وتطورها، وتحتاج إلى حماية قانونية.

1-6-1) أنها ذو طبيعة خاصة:

يرى الفقه القانوني أن الجريمة المعلوماتية، بوصفها جريمة تستهدف المعلومات كمجموعة مستحدثة من القيم القابلة للاستحواذ عليها منفصلة عن دعامتها المادية، يمكن تقييمها سعريا وفقا لسوقها في حال عدم حظرها تجاريا، مع ارتباطها بمؤلفها بعلاقة ملكية فكري، ويدعم هذا التوجه الأستاذ فيفانتي(Vivanti) ، الذي يرى أن "فكرة الشيء أو قيمته تتجسد في صورة معنوية، وأن نوع الحق يمكن أن ينتمي إلى قيمة معنوية ذات طابع اقتصادي، مما يجعلها جديرة بحماية القانون الجنائي" ويضيف أنه إذا كانت المعلومات والبرامج المعالجة آليا ذات قيمة اقتصادية، فإنه يتعين التعامل معها معاملة المال المادي، كما يبرز هذا الاتجاه ضرورة حماية المعلومة كأصل رقمي مستقل، قابل للاحتيال والسرقة، مما يستدعي تطبيق عقوبات جنائية مماثلة لتلك المتعلقة بالمال، مع التركيز على قيمتها السوقية والملكية الفكرية كأساس للركن المادي للجريمة[1].

[1] محمد علي العريان، مرجع سابق، ص51.

1-6-2) هي جريمة مستحدثة:

الجريمة المعلوماتية تتجاوز الإطار التقليدي للجرائم المادية لتصبح تهديدا لا ماديا يستهدف البيانات والأنظمة الإلكترونية، والتي تتميز بطبيعتها السيبرانية التي تتطلب أدوات تقنية حديثة مثل الاختراق والفيروسات الرقمية... الخ من التقنيات المستخدمة فيها، مما يجعلها تختلف جذريا عن الجرائم التقليدية في الوسيلة والمكان والإثبات، والتي نشأت مع انتشار الإنترنت وأنظمة المعلومات، مستدعية تشريعات جديدة لمواكبة سرعة تطورها، وتواجه الجريمة المعلوماتية صعوبات في التجريم بسبب عابريتها للحدود وعدم ملموسيتها، مما يستلزم قوانين متخصصة تركز على حماية المعلومة كقيمة اقتصادية وفكرية، كما في التشريعات الجزائرية والدولية، ويؤكد الفقه القانوني، كرأي الأستاذ فيفانتي، على معاملة المعلومات معاملة المال، معتبرًا إياها أصلًا مستقلًا يستحق الحماية الجنائية لقيمتها السوقية والمعنوية[1].

وقد سعى المشرع الجزائري إلى مواكبة التطورات القانونية المتعلقة بالجرائم المعلوماتية عبر تتابع تشريعات متخصصة، أبرزها التعديل الوارد في القانون رقم 04-15 المؤرخ 10 نوفمبر 2004 على قانون العقوبات، الذي أضاف فئة جديدة من الجرائم بعنوان "المساس بأنظمة المعالجة الآلية للمعطيات" في المواد 394 مكرر إلى 394 مكرر 07[2].

[1] Thomas J. Holt, Adam M. Bossler, and Kathryn C. Cybercrime and Digital Forensics ,Seigfried-Spellar ,3rd Edition, Routledge, 2022, new york, usa.PP 36-45.

[2] القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 عدّل وكمّل بقانون العقوبات (الأمر رقم 156/66)، وأبرز تعديلاته كانت في إدخال جرائم معلوماتية وجرائم اقتصادية لأول مرة، مثل تجريم تبييض الأموال (المواد 389 مكرر وما يليها) وتجريم الاعتداء على أنظمة المعالجة الآلية للمعطيات (المواد 394 مكرر وما يليها)، مما أظهر مواجهة تشريعية حديثة لجرائم العصر الرقمي والجريمة المالية المنظمة .

وقد كان أسس هذا التعديل مبدأ حماية "المال المنقول" الرقمي، مستمدًا من قانون الملكية الفكرية وحقوق المؤلف رقم 03-05 المؤرخ 19 يوليو 2003، وتبعه تعديل القانون المدني برئاسة القانون رقم 05-10 المؤرخ 30 جوان 2005 الذي حدد أشكال العقد الإلكتروني، إلى جانب تعديل قانون التأمينات الاجتماعية رقم 83-11 عبر القانون رقم 08-01 المؤرخ 23 جانفي 2008 الذي نظم معاملات البطاقات الإلكترونية والفوترة الرقمية[1].

وتُوّجت هذه السلسلة من التطورات التشريعية بالقانون رقم 09-04 المؤرخ 5 أوت 2009 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الذي سد الثغرات في القانون 04-05 ووضع الإجراءات اللازمة لملاحقة الجناة وعقابهم، مع الإشارة إلى الخصوصيات الاستثنائية لهؤلاء الجناة المعلوماتيين التي تعيق تتبعهم بفعل مهاراتهم الفائقة وبراعتهم في التملص من العقاب، وستكون موضوع المطلب اللاحق[2].

1-7) الجاني والمجني عليه أو (الضحية) في الجرائم المعلوماتية:

يُطلَق وصف المجرم في الفقه الجنائي على كل شخص يتعمد، بإرادة حرة واعية، بالقيام بفعل أو انتهاك منظومة القواعد القانونية ذات الطابع الجزائي التي تُنظِّم سلوك الأفراد، والتي تستهدف حماية المصالح العامة والخاصة في المجتمع على حد سواء، وقد درجت التشريعات الوطنية والأنظمة الجنائية المقارنة على سنّ نصوص عقابية وإجرائية لمواجهة هذه الأفعال الإجرامية وتعقّب مرتكبيها، بما يحقق الردع العام والخاص ويحافظ على النظام العام.

[1] https://www.mjustice.dz/wp-content/uploads/pdf/18012022.pdf.

[2] https://www.joradp.dz/ftp/jo-arabe/2015/a2015053.pdf

ورغم تعدد فئات المجرمين وتنوع أنماط السلوك الإجرامي، لم تكن مسألة ملاحقة الجناة في مرحلة الجريمة التقليدية تثير إشكالات بنيوية عميقة، بحكم الطابع المادي المحسوس لمعظم الجرائم، الأمر الذي كان ييسر تصنيفها وفق طبيعتها وتحديد فئات مرتكبيها ودوافعهم وغاياتهم الإجرامية، فضلاً عن اتخاذ تدابير وقائية ملائمة في مواجهتهم في ضوء درجة خطورتهم الإجرامية وتشابه أنماط السلوك داخل الفئة الإجرامية الواحدة.

غير أنّ ظهور تقنيات المعلومات والاتصال وما صاحبها من اعتماد واسع للمنظومات المعلوماتية في مختلف مجالات الحياة، أدى إلى بروز أنماط مستحدثة من الإجرام تختلف من حيث البنية والآثار عن الجرائم التقليدية، سواء من حيث طبيعة الفعل المجرّم أو خصائص الجناة أو وسائل التنفيذ أو حتى نوعية الضحايا، فتحوّلت جرائم الاحتيال التقليدي إلى جرائم احتيال إلكتروني، وجرائم السرقة إلى سرقة للمعطيات والمعلومات، كما اتخذت أفعال السب والقذف والاعتداء على الاعتبار والشخصية صوراً جديدة تمس بالبيانات الشخصية والمعطيات ذات الطابع السري في الفضاء المعلوماتي.

وتُظهر هذه التحولات في مجموعها أنّ الظاهرة الإجرامية قد شهدت انتقالاً نوعياً من النطاق المادي المحض إلى النطاق الرقمي والافتراضي، بما يستتبع إعادة النظر في المفاهيم التقليدية للجريمة والمجرم، ويفرض على المشرّع المعاصر إعادة تكييف نصوص التجريم والعقاب، واستحداث آليات إجرائية وتقنية ملائمة لمواجهة خطورة الجريمة المعلوماتية وتعقيداتها العابرة للحدود، إن كل هذه التطورات إن دلت على شيء فإنها تدل على تحول جذري في مجال الجريمة

والمجرم والمفاهيم المتعلقة بعلم الإجرام خصوصا في طريقة الجاني وتبعات الجريمة على المجني عليه.

1-7-1) المجرم المعلوماتي:

يرى الأستاذ (باركر- Parker) أن المجرم المعلوماتي وإن كان يتميز ببعض السمات الخاصة إلا أنه في النهاية لا يخرج عن كونه مرتكبا لفعل إجرامي يتطلب توقيع العقاب عليه[1].

- **المجرم المعلوماتي ذو طبع اجتماعي:** يتسم المجرم المعلوماتي – في الغالب – بكونه شخصاً ذا تكوين اجتماعي سليم ظاهريا، يتمتع بقدرة مرتفعة على التكيّف داخل محيطه الاجتماعي والمهني، بحيث ينجح في بناء صورة إيجابية عن ذاته لدى الآخرين، ويُنظر إليه بوصفه محل ثقة واعتماد، ولا سيما في بيئات العمل المتصلة بالأنظمة المعلوماتية وقواعد البيانات ذات الحساسية الخاصة، ويُفضي هذا الوضع إلى أنّ الجاني المعلوماتي لا يظهر في حالة تعارض أو خصومة ظاهرة مع المجتمع الذي ينتمي إليه، بل يتعمّد إظهار قدر كبير من الاندماج والتوافق معه، الأمر الذي يضاعف من خطورته الإجرامية متى اقترن هذا التكيّف الاجتماعي بميول إجرامية مستقرة. فإحساسه بأنه موضع ثقة وخارج نطاق الشبهات يعزّز جرأته على الاسترسال في نشاطه غير المشروع، لاسيما وأن الأفعال الإجرامية المعلوماتية غالباً ما تُرتكب في سرّية تامة وفي فضاء

[1] عبد العال الدريبي، مرجع سابق، ص 58

غير منظور، بما يجعل اكتشافها متعذّراً في كثير من الحالات أو متأخراً إلى مرحلة تصبح معها آثارها الضارة قائمة ويصعب تداركها[1].

ويُعدّ الخوف المستمر من انكشاف الفعل الإجرامي من أبرز المظاهر الاجتماعية الملازِمة لشخصية المجرم المعلوماتي، إذ يعيش هذا الأخير – في الغالب – في ظل توجس دائم من احتمال تعقّب نشاطه غير المشروع وظهور حقيقته أمام محيطه المهني والاجتماعي. ويزداد هذا الشعور حدّة لدى مرتكبي الجرائم المعلوماتية مقارنة بغيرهم من الجناة، نظراً لما يمكن أن يترتب على كشف أمرهم من آثار مالية سلبية وخسائر مادية معتبرة، إلى جانب ما يستتبع ذلك عادة من زوال المركز الوظيفي وتقويض المكانة المهنية التي يتمتعون بها. كما يجد هذا المعطى تفسيره في انتماء غالبية هؤلاء إلى فئات اجتماعية ذات مستوى عالٍ من التأهيل العلمي والرأسمال المعرفي، ويشغلون في الغالب وظائف تقنية أو تخصصية مرموقة، وهو ما يجعل النتائج الاجتماعية والمهنية المترتبة على افتضاح سلوكهم الإجرامي أشد وقعاً على سمعتهم ومركزهم الاعتباري[2].

– **المجرم المعلوماتي ذكي ومحترف:** يتسم المجرم المعلوماتي – في الغالب – بدرجة عالية من الذكاء والاحتراف المهني، حيث يمتلك رصيداً معتبراً من المعارف التقنية والمهارات المتخصصة في مجالات الحاسوب، ونظم المعلومات، والشبكات، وقواعد البيانات، وهي مهارات تمكّنه من استغلال الثغرات التقنية في البنى المعلوماتية واستعمال أدوات معقدة في الاختراق، والتشفير، وإخفاء الآثار الرقمية، بما يجعله متقدماً – من الناحية الفنية – على المستخدم العادي،

[1] أحمد بن علي، الجريمة المعلوماتية في القانون الجنائي المعاصر، دار النهضة العربية، 2000، القاهرة، ص 145.

[2] Michael L. Rich, Cybercrime and Social Profiles of Offenders , Oxford, Oxford University Press, 2020,P 97.

وغالباً أيضاً على ضحاياه[1]، وُيصنَّف هذا النمط من الجناة، في عدد من الكتابات الفقهية، ضمن فئة «المجرم المتخصص» أو «المجرم المحترف»، لما يتسم به من قدرة على توظيف خبرته التقنية في تنفيذ جرائم ذات طابع معلوماتي محض، مثل اختراق الأنظمة، أو الاستيلاء غير المشروع على البيانات، أو التلاعب بالمعاملات الإلكترونية، مع ما يميّزه من قدرة على تطوير أساليبه باستمرار لمواكبة تطور الوسائل التكنولوجية ووسائل الحماية التقنية، كما يُشار إلى أن الجريمة المعلوماتية ذاتها تُعد «إجرام ذكاء»، إذ تفترض في مرتكبها مستوى معيناً من القدرات العقلية والمهارات التحليلية، من حيث فهم بنية الأنظمة المعلوماتية وكيفية عملها، والقدرة على تجاوز آليات الحماية والرقابة، والتخطيط المسبق لمراحل تنفيذ الفعل الإجرامي بما يقلل من فرص اكتشافه أو ملاحقته[2].

يتميز المجرم المعلوماتي بقدرته على انتهاج أسلوب الهدوء والعمل غير المرئي لتحقيق أغراضه غير المشروعة مع الحرص على طمس الآثار الرقمية قدر الإمكان، ومن ثمّ يُنعت الإجرام المعلوماتي في الفقه الجنائي المعاصر بأنّه «إجرام الأذكياء»، باعتبار أنّ المجرم المعلوماتي يسعى بشغف دائم إلى اكتشاف أساليب جديدة لا يحيط بها غيره، تمكّنه من اختراق الحواجز والوسائط الأمنية في البيئة الإلكترونية والوصول إلى أهدافه في سرية ودقة عالية[3].

– **المجرم المعلوماتي يتميز بقوة التحمل والصبر:** يتطلّب النشاط الإجرامي المعلوماتي من مرتكبه قدراً مرتفعاً من الصبر وقوة الاحتمال، بالنظر إلى ما تستغرقه عمليات الاختراق أو تنفيذ التحويلات المالية غير المشروعة من وقت قد يمتد لساعات طويلة، بل لأيام متتالية في بعض الحالات قبل الوصول إلى النتيجة المتوخاة، كما تُعدّ المثابرة والاستمرار في المحاولة من الخصائص الرئيسة التي تعزّز فاعلية المجرم المعلوماتي وتنمّي مهاراته التقنية، ذلك أنّ تعدد

[1] الجازولي بن أحمد، خصوصية المجرم المعلوماتي ودوافعه، مجلة دراسات قانونية، العدد 2، 2021، ص 115

[2] David S. Wall, Cybercrime,The Transformation of Crime in the Information Age ,Cambridge, Polity Press, 2007, P 64

[3] عبد القادر حمدي، الجريمة المعلوماتية: دراسة في الطبيعة القانونية وخصائص المجرم المعلوماتي، دار الثقافة للنشر والتوزيع، 2020، عمان، ص 89.

المحاولات وتجاوز الإخفاقات المتكررة يقتضي استثماراً زمنياً ملحوظاً، يفرض عليه التحلي بقدر عالٍ من الصبر والمواظبة في إطار عمل غير مرئي إلى أن تتحقق غايته الإجرامية[1].

– **المجرم المعلوماتي له السلطة:** يميل المجرم المعلوماتي في كثير من الحالات إلى الاستفادة من نوع من السلطة لا تقتصر على السلطة الوظيفية أو الإدارية فحسب، بل تمتد لتشمل السلطة التقنية والمعرفية التي تمنحه تفوقاً واضحاً على غيره داخل بيئته المهنية والرقمية، إذ غالباً ما يشغل هذا الصنف من الجناة مناصب أو مواقع عمل تسمح له بنفاذ مشروع إلى الأنظمة المعلوماتية أو قواعد البيانات أو البنى التحتية الرقمية الحساسة، أو يمتلك خبرة فنية متقدمة تمكّنه من التحكم في تلك الأنظمة والتصرف في مواردها على نحو قد يُسيء استخدامه لتحقيق أغراض غير مشروعة. كما تؤدي هذه السلطة – التنظيمية أو التقنية – إلى خلق اختلال في موازين القوة بينه وبين الضحايا، وتزيد من قابليته لاستغلال الصلاحيات الممنوحة له أو ثقة الجهة المشغّلة أو العملاء، بما يسهّل تنفيذ الفعل الإجرامي ويقلل من احتمالات اكتشافه في المراحل الأولى من مباشرته عمله الاجرامي[2].

إذا من خلال هذا يمكن سرد والاتفاق على مجموعة خصائص مكررة لدى هذه الفئة من المجرمين، من أهمها:

- ارتفاع مستوى الذكاء والقدرة على حل المشكلات التقنية المعقدة بسرعة.
- التخصص والمهارة الفنية العالية في مجالات الحاسوب، الشبكات، ونظم المعلومات.
- امتلاك قدر كبير من المعرفة ببنية الأنظمة الأمنية وكيفية تجاوزها أو استغلال ثغراتها.
- الميل إلى الإخفاء والتخفي والقدرة على التواري عن الأنظار وإخفاء الأدلة الرقمية.
- عدم الميل إلى العنف المادي، والاعتماد على الحيلة والخداع والتلاعب بالبيانات بدلا من القوة الجسدية.

[1] Thomas J. Holt, Cybercrime and Digital Forensics, An Introduction, New York, Routledge, 2018, P 122.

[2] Ahmed K. Hassan, Cybercrime Offenders and their Organizational Power ,London,Routledge, 2019, P 73.

- في كثير من الحالات يكون اجتماعيا وقادرا على التكيف، مما يساعده على استغلال ثقة الضحايا أو بيئة العمل في تسهيل ارتكاب الجريمة.

1-7-2) تقسيم فئات مجرمي المعلوماتية:

يتم تقسيم مجرمو المعلوماتية إلى عدة أقسام أو أصناف وذلك حسب درجة الخطورة التي يتميزون بها أو يشكلونها في مواجهة أمن نظم المعلومات، وكذلك بالنظر إلى حجم رغباتهم ودوافعهم الإجرامية وعادةً حسب نواياهم وطريقة عملهم، ولعل من أشهر التصنيفات لهم هو "ألوان القبعات" في عالم الاختراق ويمكن تصنيفهم كما يلي:

- **التصنيف حسب ألوان القبعات:**

1- قراصنة القبعة السوداء: هم مخترقون ذوو مهارات عالية يستهدفون الأنظمة والشبكات بهدف السرقة أو التخريب أو التجسس، مثل سرقة أرقام البطاقات البنكية أو ابتزاز الشركات.

2- قراصنة القبعة البيضاء: يسمون أيضًا القراصنة الأخلاقيين، يعملون بإذن الجهات المالكة للأنظمة لاختبار الاختراق واكتشاف الثغرات ثم المساعدة في إصلاحها والذين يكون عملهم في:

- **الهندسة الاجتماعية:** وهو من الشائع أن يستخدم قراصنة القبعة البيضاء الهندسة الاجتماعية ("اختراق الأشخاص") لاكتشاف نقاط الضعف في الدفاعات "البشرية" للشركات والمؤسسات؟ تدور الهندسة الاجتماعية حول خداع الضحايا والتلاعب بهم من أجل فعل شيء يجب ألا يفعلونه (مثل تحويل أموال أو مشاركة بيانات الدخول لحساباتهم، وما إلى ذلك).

- **اختبار الاختراق:** اختبارات الاختراق تهدف إلى الكشف عن الثغرات الأمنية ونقاط الضعف في دفاعات أي مؤسسة ونقاط النهاية حتى يمكن تصحيحها.

– **الاستكشاف والأبحاث:** يتضمن هذا البحث في المؤسسة وعنها لاكتشاف الثغرات الأمنية في بنيتها التحتية الفعلية والتكنولوجية. الهدف هو تجميع معلومات كافية لتحديد طرق تجاوز الضوابط الأمنية والآليات بشكل قانوني دون إتلاف أو كسر أي شيء.

– **البرمجة:** يعمل قراصنة القبعة البيضاء على إنشاء **هوني بوت** (أو مصائد مخترقي الشبكات) والتي تعمل كمصائد تغري المجرمين الإلكترونيين وتجذبهم وتشتتهم، أو تساعد قراصنة القبعة البيضاء في تجميع معلومات قيمة عن المهاجمين.

– **استخدام مجموعة من الأدوات الرقمية والحقيقية:** يشمل هذا العتاد والأجهزة التي تسمح لمختبري الاختراق بتثبيت بوتات وبرمجيات أخرى، والوصول إلى الشبكة أو الخوادم.

بالنسبة لبعض قراصنة القبعة البيضاء، تتركز العملية في شكل برامج مكافآت اكتشاف الثغرات، أي منافسات تمنح المخترقين جوائز نقدية على اكتشاف أي ثغرات أمنية. يوجد حتى دورات تدريبية وفعاليات وشهادات مخصصة للقرصنة الأخلاقية.

3– قراصنة القبعة الرمادية: يخترقون الأنظمة غالبًا دون إذن، بهدف استعراض المهارات أو تنبيه الشركة للثغرات، وقد يطلب بعضهم مقابلًا ماليًا، لذلك يُعدّ سلوكهم من الناحية القانونية غير مشروع رغم ادّعاء نية حسنة[1].

[1] https://me.kaspersky.com/resource-center/definitions/hacker-hat-types... See 12-4-2024...21.00m

1-7-3) الضحية في الجرائم المعلوماتية:

تبرز الإقرار بأهمية النظم المعلوماتية والنجاح البارز الذي حققته، أنّ لذلك ثمنا يتمثل في تأثيرها السلبي المحتمل على ضمانات الحق في الحياة الخاصة، فاعتماد معظم المؤسسات الحكومية والخاصة على تقنيات المعالجة المعلوماتية، بما تمتلكه من قدرة كبيرة على جمع وتخزين ومعالجة واسترجاع ومقارنة كم هائل من البيانات المتعلقة بأفراد المجتمع في مختلف قطاعاته، يثير تحديات حقيقية على صعيد حماية المعطيات الشخصية، ويزداد القلق حدة عند إساءة استخدام هذه المعلومات ذات الطبيعة السرية المخزنة إلكترونيا، إذ إن الربط بينها وتوظيفها على نحو غير مشروع يمكن أن يكشف عن جوانب من حياة الأفراد قد يؤدي إفشاؤها إلى الإضرار بالمصالح العامة والخصوصية الشخصية للمعنيين بها[1].

اذ أنّ تحديد ضحايا الإجرام المعلوماتي بدقة يعد أمرا إشكاليا، لأن غالبية هؤلاء لا يدركون تعرّضهم للاعتداء إلا بعد وقوعه فعليًا، وفي مثل هذه الحالات يميل الكثير منهم إلى الامتناع عن الإبلاغ، ظنًا منهم أنّ السكوت أجدى، فضلًا عن تحرج عدد منهم من الاعتراف بأن نظامهم المعلوماتي كان محلّ اعتداء، وخوفا من أن يشكل هذا الإقرار حافزًا للجناة على الاستمرار في اعتداءاتهم أو استهدافهم مجددًا[2].

[1] نهلا عبد القادر المومني، مرجع سابق، ص ص 86-87

[2] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011، ص 37

خصائص الضحية في الجريمة المعلوماتية:

- **من خصائص الضحية في هذا النوع من الجرائم:** صعوبة اكتشاف الاعتداء إلا بعد فوات الأوان، والخجل أو التردد في الإبلاغ بسبب السمعة أو الخوف من فقدان الثقة، وهو ما ينتج ما يُعرف بـ"الإخفاء الإحصائي" لعدد كبير من القضايا[1]

- **الضحية يتعرض غالبًا لآثار مركبة:** ضرر مالي (خسارة أموال أو بيانات)، وضرر معنوي ونفسي (قلق، خوف، اضطراب ما بعد الصدمة)، وضرر اجتماعي أو مهني (فقدان السمعة أو الوظيفة)، وقد أظهرت دراسة ميدانية بولاية باتنة وجود اضطرابات نفسية وسلوكية ملحوظة لدى ضحايا الجريمة المعلوماتية في الجزائر[2].

1-8) صور الجريمة المعلوماتية:

الجرائم المعلوماتية هي تلك الأفعال غير المشروعة التي تُرتكب باستخدام الحاسوب أو شبكات الاتصالات، كما قد تُوجَّه مباشرة إلى النُّظم المعلوماتية ذاتها ومكوّناتها التقنية والبرمجية، وتلتقي الجريمة المعلوماتية مع الجريمة التقليدية في الجوهر، من حيث كون كلتيهما تمثّل اعتداءً على مصالح عامة أو خاصة يحميها القانون، غير أنّهما تختلفان في العديد من الجوانب، لاسيما على مستوى الركن المادي والركن المعنوي لكل منهما، ففي حين تعد الأفعال المتمثلة في سرقة المعدات المادية للحاسوب أو إتلافها، مثل الشاشة أو الوحدة المركزية أو وسائل الاتصال بالشبكة كالكابلات، من قبيل الجرائم التقليدية لما تنطوي عليه من مساس بأموال ذات طبيعة مادية قابلة

1 منشور وزارة العدل، التحري والتحقيق في الجرائم الإلكترونية في القانون الجزائري، الجزائر، وزارة العدل، 2021، ص 90–92

2 دليلة جلول، ضحايا الجريمة المعلوماتية في الجزائر، أطروحة دكتوراه، جامعة باتنة 1، 2024، ص 145 وما يليها.

للحيازة، فإنّ الاعتداءات الموجَّهة إلى المكوّنات المنطقية للحاسوب تُصنَّف ضمن الجرائم المعلوماتية، متى انصبت على البرمجيات أو المعطيات المخزّنة أو المتداولة عبر شبكة الإنترنت، حيث يغدو الحاسوب في هذه الحالة أداة لارتكاب الجريمة لا محلا ماديا لها.

حيث تتعدد صور الجريمة المعلوماتية بتعدد محل الاعتداء والغاية منه، لكنها تشترك في اعتمادها على الحاسوب أو الشبكات وسيلة أو محلاً للفعل الإجرامي، ويمكن عرض أهم الصور في نقاط رئيسية كما يلي:

1-8-1) جرائم التعدي التي تستهدف النظم المعلوماتية:

يقصَد بالنظام المعلوماتي كل نظام مستقل، أو مجموعة من الأنظمة المترابطة أو المتصلة فيما بينها، يتولى واحد منها أو أكثر إجراء معالجة آلية للمعطيات تنفيذًا لبرنامج مُحدد[1]، وقد عرفها المشرع الجزائري بأنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في أو أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية[2].

- **جرائم التعدي على النظم المعلوماتية:** لقد كرّس المشرّع الجزائري قسما خاصا لجرائم المساس بأنظمة المعالجة الآلية للمعطيات ضمن قانون العقوبات، من المادة 394 مكرر إلى المادة 394 مكرر 7 وفق التعديلات المتعاقبة، حيث نصّ على تجريم أفعال الدخول والبقاء غير المشروع، والإتلاف والتخريب، وحيازة أو إفشاء أو استعمال المعطيات المتحصل عليها بطريق غير مشروع،

[1] https://www.secprint.sa/how-to-face-hacking/... See 13/04/2024...11.30m

[2] المادة 02، الفقرة (أ)، القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، مرجع سابق

وكذا مسؤولية الشخص المعنوي والشروع والاتفاق الجنائي[1]، ويُلاحظ انسجام هذا التوجّه مع الاتجاهات الدولية التي تميّز بين الجرائم "المعتمدة على التكنولوجيا (Cyber-dependent) " التي يكون موضوعها النظام أو البيانات نفسها، والجرائم "المُمكَّنة بالتكنولوجيا " (Cyber-enabled)التي تُستعمل فيها النظم المعلوماتية لتوسيع نطاق جرائم تقليدية[2]

حيث قرر المشرّع لهذه الأفعال عقوبة الحبس من ثلاثة أشهر إلى سنة، وغرامة مالية تتراوح بين 50.000 دج و100.000 دج، مع تشديد العقوبة إلى الضعف إذا نجم عن الفعل حذف أو تغيير في المعطيات المعلوماتية، وهي الحالة التي فصّلها بشكل أدق في المادة 394 مكرر 01 من القانون رقم 04-05 المعدِّل والمتمم لقانون العقوبات[3]

ويستفاد من ذلك أنّ السياسة التجريمية للمشرّع الجزائري في مجال حماية النظم المعلوماتية تبدو شاملة وواضحة من حيث تجريم الأفعال، غير أنّ الإشكال يظل قائمًا في عدم ضبط عناصر الركن المادي والركن المعنوي بدقة، بما قد يفضي إلى استغلال الثغرات القانونية للإفلات من العقاب، الأمر الذي يستدعي التوقف عند تحليل وبيان صور جرائم التعدي على النظم المعلوماتية بمزيد من التفصيل والتي تتضح فيما يلي:

- **جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي:** تتجسّد جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي في إقدام الجاني على الولوج، أو محاولة الولوج، بأساليب

[1] عبد القادر بوطالب، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مجلة الدراسات القانونية 5، عدد 1 2017، ص ص 120-123

[2] UNODC, "Cybercrime Legislation and Offences," Global Programme on Cybercrime ,Vienna, UNODC, 2016, PP,8-10

[3] قانون العقوبات، رقم 04-05 المعدِّل والمتمم، مرجع سابق

احتيالية إلى كل أو جزء من منظومة المعالجة الآلية للمعطيات، أو الاستمرار في التواجد داخلها دون سند قانوني، ويُرتّب المشرّع على هذا السلوك عقوبات سالبة للحرية ومالية، مع تشديد الجزاء إذا أسفر الفعل عن حذف أو تعديل للمعطيات أو عن الإخلال بسير المنظومة[1] وتُعتبر هذه الجريمة اعتداءً مباشرًا على سرية وسلامة النظام المعلوماتي، وقد أقرّتها الصكوك الدولية ضمن الجرائم الأساسية التي يتعيّن إدراجها في التشريعات الوطنية[2].

- **جريمة إتلاف أو تعطيل نظام المعالجة الآلية للمعطيات:** تكون هذه الجريمة في إلحاق ضرر جسيم بتشغيل النظام المعلوماتي، سواء عن طريق إدخال معطيات خبيثة كالبرمجيات الضارة، أو حذف أو تعديل البيانات، أو إغراق النظام بطلبات عن طريق هجمات حجب الخدمة مثلا، مما يؤدي إلى تعطيل كلي أو جزئي لوظائفه[3]، ويُعد هذا الفعل مساسًا بـ سلامة وتوافر البيانات والأنظمة، ويُقارن بما تسميه الاتفاقيات الدولية "التدخل غير المشروع في البيانات أو النظام[4].

- **جريمة إدخال أو تعديل المعطيات بطريق غير شرعية:** ينصرف هذا الفعل إلى إدخال بيانات في النظام أو تعديل أو محو ما يتضمنه من معطيات، على نحو يُغيّر الحقيقة الرقمية أو يؤثر في النتائج التي يقدّمها النظام، مما قد يفضي إلى إلحاق أضرار مالية أو قانونية بالغير مثل تعديل أرصدة، تغيير سجلات، أو تلاعب بنتائج أو وثائق رقمية[5]، وتُعد هذه الصورة قريبة من جرائم

[1] عمّار حشمان، الجريمة المعلوماتية في التشريع الجزائري، أطروحة ماجستير، جامعة ورقلة، 2017، ص ص 120-121.

[2] UNODC, Cybercrime Module 2, Offences against the Confidentiality, Integrity and Availability of Computer Data and Systems , Vienna: UNODC, 2018, PP 3–5

[3] عبد القادر بوطالب، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مجلة الدراسات القانونية، 5، عدد 1 ،2017، ص 120

[4] Council of Europe, Convention on Cybercrime (Budapest Convention), ETS No 185 (Budapest, 2001), arts, PP 4–5

[5] عمّار حشمان، مرجع سابق، ص 123

التزوير، إلا أنها تتخذ شكلًا إلكترونيًا يستهدف البيانات في بنيتها المنطقية داخل النظام المعلوماتي[1].

- **حيازة أو إفشاء أو استعمال المعطيات المتحصل عليها بطريق غير مشروع:** يعاقب المشرّع على الأفعال اللاحقة للاعتداء الأصلي على النظام، كحيازة أو إفشاء أو نشر أو استعمال المعطيات التي تم الحصول عليها من إحدى الجرائم المعلوماتية السابقة، باعتبارها تشكل اعتداءً مستقلًا على حق صاحب البيانات في السرية والتحكم في معطياته[2]، وهذه الصورة تواكب ما تُقرّه الاتفاقيات الدولية من تجريم لاستغلال البيانات المقرصنة ولو لم يشارك الفاعل في فعل الاختراق ذاته[3].

- **مسؤولية الشخص المعنوي، الاتفاق الجنائي، والشروع:** اعترف المشرّع بمسؤولية الشخص المعنوي عن جرائم المساس بالنظم المعلوماتية، ورتّب في حقه غرامات مشددة وتدابير إضافية (كوقف النشاط أو الحل) متى ارتُكبت الجريمة باسمه أو لحسابه[4] كما جرّم الاشتراك في مجموعة أو اتفاق يهدف إلى التحضير لجريمة أو أكثر من الجرائم المعلوماتية، واعتبر الشروع فيها معاقبًا عليه بنفس عقوبة الجريمة التامة، تبعًا لخطورة الإعداد التقني اللازم لوقوع الاعتداء[5]

1-9) أبرز الجرائم المعلوماتية من الناحية الواقعية:

1-9-1) الجرائم الواقعة على الأموال:

[1] وائل شعيب، الجرائم المعلوماتية، أنواعها وأحكامها في الفقه والقانون، دار الفكر الجامعي، 2019، القاهرة، ص 101 ومايليها.

[2] عبد القادر بوطالب، مرجع سابق، ص ص 128-129.

[3] https://unctad.org/system/files/official-document/Cybercrime%20Nayelly%20Loya%20(UNODC).pdf, PP 11-12

[4] عبد القادر بوطالب، مرجع سابق، ص 131

[5] عمّار حشمان، مرجع سابق، ص 135 وما يليها.

لقد أفضى الانتشار الواسع لتقنيات المعلومات وتغلغلها في مختلف مناحي الحياة اليومية، ولا سيما في مجال المعاملات المالية والتجارية، إلى بروز ما يُعرف بجرائم الاحتيال المعلوماتي بوصفها نمطًا مستحدثًا من السلوك الإجرامي المرتبط بالبيئة الرقمية، وقد تعددت التعاريف الفقهية لهذا السلوك، حيث عرّفه الأستاذ الأمريكي Squires بأنّه " إساءة استخدام نظام الحاسوب على نحو ينطوي، في سلوكه، على حيلة أو خدعة مضلِّلة"، وتُعدّ الجرائم المعلوماتية ذات الطابع الاحتيالي من صور السلوك الإجرامي غير المشروع الذي يُرتكب باستخدام وسائل تقنية، لا سيما الحاسوب وشبكة الإنترنت، بقصد تمكين الجاني من تحقيق مصلحة مالية أو الحصول على كسب مادي غير مشروع، وذلك من خلال استهداف الأنظمة المعلوماتية، والتلاعب بمعطياتها، وتحويل الأموال أو نقلها إلى حساباته أو لمصلحته الخاصة بما يشكّل اعتداءً على الذمة المالية للغير التي يحميها القانون الجزائي[1].

ويرجع الانتشار المتزايد لهذه الجرائم إلى التوسع الملحوظ في استخدام تقنيات المعاملات المالية الإلكترونية خلال السنوات العشر الأخيرة، نتيجة لما باتت توفره البنوك والمؤسسات المالية لزبائنها من خدمات رقمية متقدمة، مثل التوقيع الإلكتروني، والاطلاع على الأرصدة عن بعد، وتبادل وتحويل الأموال عبر الشبكات والأنظمة المعلوماتية، وقد أسهمت هذه البيئة الرقمية في استقطاب اهتمام محترفي الجريمة المعلوماتية، الذين انصبت جهودهم على ابتكار أساليب

[1] عبد الرحمن، سامي .الجرائم الإلكترونية وأحكامها في القانون الجزائري، دار هومة للنشر، الجزائر، 2021، ص 145.

للحصول على الأرقام السرية للزبائن وبيانات الدخول إلى أنظمة البنوك والمؤسسات المالية، بقصد تحويل الأموال بطرق غير مشروعة إلى حساباتهم الخاصة[1].

ولعل اهم الأمثلة التي كانت:

تفاصيل	التاريخ	القضية
توقيف 197 شخصاً في مختلف الولايات، خسائر تجاوزت 4 ملايين دولار لـ 500 ضحية، بما في ذلك شبكة دولية مع دولة آسيوية، باستخدام التصيد الإلكتروني والهندسة الاجتماعية .	ديسمبر 2025	تفكيك 32 شبكة نصب إلكتروني
المتهمون: «ع، ر» (رئيس مصلحة، 7 سنوات سجن)، «ع، ا» (موظف، 5 سنوات)، «ق، ع» (عون شباك، 2 سنوات)؛ اختلاس 15 مليار سنتيم (149 مليون دج) عبر تزوير 73 توقيعاً وإتلاف وثائق دون تسجيلها في النظام الآلي.	وقائع: 2002–2013، حكم: يونيو 2016	اختلاس في بنك وطني جزائري (شيغيفارا)
رعية تركي (5 سنوات حبس + مليون دج غرامة)، شريكه (3 سنوات)؛ تحويل أموال من 4 بنوك جزائرية إلى حسابات وهمية	حكم: 2025 (محكمة الشرقة)	نصب على 4 بنوك بـ200 مليون يورو
عصابة سرقت 70 مليون دج من تاجر باستخدام فيديو فيسبوك للاستدراج، أدى الفيديو إلى القبض عليهم؛ تم تداول التفاصيل على وسائل التواصل،	نوفمبر 2020	سرقة 70 مليون دج «عصابة آلو ماما»
حكم بـ6 سنوات سجن + 133 ألف دينار غرامة لاستيلاء على أموال زبائن عبر الحسابات البنكية .	نوفمبر 2025 (حكم المحكمة	إطار بنكي سابق في تونس[2]

[1] Joël Rivière et Didier Lucas – « Criminalité et internet une arnaque à bon March » – Article publier dans la revus de la sécurité Globale- numéro 06- année 2008- p 69-70. Disponible sur site www.cairn.info – Fonds documentaire (S.N.D.L) Système national de documentation en ligne – Algérie –Date de consultation 28/03/2014.

[2] خسائر ضحايا الاحتيال الإلكتروني تتجاوز 4 ملايين دولار في الجزائر، يوتيوب، 18 ديسمبر 2025، https://www.youtube.com/watch?v=3Lmk35OBVmU؛» موظفون بالبنك الجزائري يختلسون أموال الزبائن»، الشروق أونلاين، 19 يونيو 2016، https://www.echoroukonline.com؛ 5 سنوات حبساً لرعية تركي و3 سنوات لشريكه، فيسبوك (الجزائرية ون)، 1 أكتوبر 2025، https://www.facebook.com/Eldjazairiaone/posts؛» قصة 'سرقة 70 مليون' في الجزائر»، يوتيوب، 29 نوفمبر 2020، https://www.youtube.com/watch?v=U7mfvUp4CMA؛ شخص محكوم عليه بـ4 سنوات بالسجن»، إنستغرام، 30 نوفمبر 2025، https://www.instagram.com/reel/DRaLAUPjLxo/.

تفاصيل	التاريخ	القضية
	الابتدائية)	

أما المشرع الجزائري، فلقد اكتفى بالإشارة العامة الى جرائم الاحتيال الالكتروني ضمن نطاق المادة 394 مكرر 02 من قانون العقوبات 04-05، دون وضع نص تشريعي خاص محدد ومفصل لمختلف صورها، مع التركيز على مفهوم الاتجار بالمعطيات المعلوماتية عبر النظم المعلوماتية بقصد جني ارباح مالية غير مشروعة الى جانب الاستناد الى نصوص خاصة، كتلك الواردة في القانون رقم 83-11 المعدل بالقانون 08-01 مؤرخ 23 جانفي 2008 المتعلق بالتأمينات الاجتماعية، الذي يجرّم استعمال بطاقات الدفع بالغش من قبل غير التابع لهيئة الضمان الاجتماعي. ويعزى غياب الإطار التشريعي الخاص الكفيل بحماية المعاملات المالية الالكترونية الى ضعف الاعتماد على هذه الاساس في المجال المالي بالجزائر، نتيجة انفصال عامل الثقة بين المتعاملين والتقنية، وحجم المخاطر التي تهددها[1].

العقوبة	الجريمة	المادة
حبس 3 أشهر إلى سنة، غرامة 50,000-100,000 دج .	الدخول أو البقاء غير المشروع في نظام معلوماتي (بطريق الغش)	314 مكرر
حبس 6 أشهر إلى 3 سنوات، غرامة 500,000-2,000,000 دج	إدخال، إزالة، تعديل معطيات بغش في نظام آلي	394مكرر (1)
حبس 2 أشهر إلى 3 سنوات، غرامة 1,000,000-	التلاعب أو الإتلاف المتعمد للمعطيات أو النظام	394مكرر

[1] قانون العقوبات 04-05، مرجع سابق

العقوبة	الجريمة	المادة
5,000,000 دج .		(2)
عقوبات مشددة تشمل المسؤولية الجنائية للشخص المعنوي .	جرائم المعلوماتية على الأشخاص المعنويين (مؤسسات)	394مكرر (4)
حبس 1–5 سنوات، غرامة 500–20,000 دج (مشددة إلى 10 سنوات)	الاحتيال التقليدي (يُطبق على الإلكتروني)	372 معدلة
عقوبات خاصة بالتحويل أو التمويه .	تبييض الأموال الناتجة عن جرائم معلوماتية	389 مكرر

من خلال هذا تبرز لنا عدة صور للجرائم الواقعة على الأموال والتي نعدها كما يلي:

– **التحويل غير المشروع للأموال باستعمال التحايل الكتروني:** يعرف النصب أو الاحتيال في القانون الجزائري بأنه جريمة اعتداء على الملكية المالية لمال منقول، حيث يلجأ الجاني باستخدام إحدى وسائل الغش المعينة قانونا إلى حمل المجني عليه على تسليم المال المنقول، وقد وصفه بعض الفقهاء بأنه الاستيلاء العمدي على الحيازة الكاملة لمال مملوك للغير باستخدام الحيلة أو الخداع[1]، حيث نصّ المشرع الجزائري على تعريف جريمة النصب في المادة 372 من قانون العقوبات الجزائري، والتي تقابل المادة 313–1 من قانون العقوبات الفرنسي أنه كل من توصل الى استقبال او تلقي اموال او منقولات او سندات او تصرفات او اوراق مالية او وعود او مخالصات او ابراء من الالتزامات او الى الحصول على احدها او شرع في ذلك، وكان ذلك بالاحتيال لسلب كل ثروة الغير او بعضها او الشروع فيه اما باستعمال اسماء او صفات كاذبة او سلطة خيالية او اعتماد مالي خيالي او بإخلاد امل في الفوز باي شيء او في وقوع حادث او اية

[1] محمد علي العريان، مرجع سابق، ص 123

واقعة اخرى وهمية او الخشية من وقوع شيء منها يعاقب بالحبس من سنة 01 على الاقل الى خمس 05 سنوات على الأكثر وبغرامة من 500 الى 20.000 دج[1]

حيث يستقيم الركن المادي لجريمة الاحتيال على فعل التظاهر والإيحاء، وهو الفعل الصالح لإيقاع المجني عليه في الغلط، بما يؤدي الى اقتناعه المباشر بالمظهر الخارجي المادي، فالمجني عليه في هذه الجريمة هو من ينخدع بهذه المظاهر ويسلم ماله للغير[2].

ويمتد الاحتيال ليشمل ليس الشخص الطبيعي فحسب، بل الشخص المعنوي أيضاً، إذ تعتبر الشركات والمؤسسات العامة والخاصة أشخاصاً اعتبارية في نظر القانون. وبما أن الحاسوب وشبكات الاتصال الداخلية والخارجية تُعدّ من فروع ومكونات الشركة أو المؤسسة، فإنها صالحة لوقوع فعل الخداع والتحايل عليها، وقد اعتبر الفقه ممارسة أفعال الاحتيال عبر التلاعب بالبرامج والبيانات، وما يترتب على ذلك من إيهام للمجني عليه بصحتها، من أساليب الاحتيال الحديثة، حيث يُصبح الحاسوب في هذا السياق مجرد وسيلة للتحايل. أما الفقه الفرنسي، فعدّ غش الأنظمة المعلوماتية بهدف الاستيلاء على الأموال تحقيقاً لجريمة الاحتيال[3].

ويشترط ليتحقق الركن المادي لجريمة الاحتيال تحقق الأفعال التالية:

[1] قانون العقوبات الجزائري، مرجع سابق.

[2] تقرير مجموعة العمل الحكومية المشتركة الفرنسية 2014، تحت عنوان – حماية مستعملي شبكة الأنترنت- فيفري 2014- ص 20- متوفر على الموقع الرسمي لوزارة العدل الفرنسية، الرابط الإلكتروني:

http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf

[3] محمد أمين الشوابكة، مرجع سابق، ص 185

– لابد من تنفيذ فعل التلاعب بمدخلات النظام المعلوماتي أي تغذيته ببيانات غير صحيحة، أو من خلال التلاعب ببرامجه، إضافة إلى فعل الإدخال والإتلاف والمحو والطمس التي سبق وتفصيل معناها[1]

– يستعين مرتكبو جرائم الاحتيال المعلوماتي بشبكة الإنترنت كأداة رئيسية لتحقيق أغراضهم الإجرامية، من خلال اعتماد أساليب التصيد الإلكتروني (Phishing) والهندسة الاجتماعية، حيث يتم إرسال رسائل بريد إلكتروني مزيفة تتظاهر بأنها صادرة عن مؤسسات مالية أو رسمية موثوقة، تطلب فيها من الضحايا المحتملين تقديم بياناتهم الشخصية الحساسة مثل أرقام الحسابات البنكية وكلمات المرور، ويسمح هذا الإيقاع بالمجني عليه بالاستيلاء غير المشروع على أمواله أو أرصدته، كما يلجأون إلى تقنيات متقدمة كإرسال روابط لمواقع إلكترونية مزورة تدعو الضحية لزيارتها، مما يؤدي إلى إصابة أجهزته الحاسوبية ببرمجيات خبيثة (Malware) تتيح تسريب كافة المعلومات الخاصة به. ومن أحدث صور هذا الاحتيال نموذج "الاحتيال النيجيري Nigerian Scamأو Scam419 ، الذي يعتمد على رسائل بريد إلكتروني تدّعي طلب مساعدة لتحويل ملايين الدولارات مقابل نسبة تتراوح بين 10–15% من المبلغ، بشرط إيداع مبلغ أولي لتغطية رسوم إدارية أو فتح حساب مصرفي، مدعين تعرض المرسل لمشكلات سياسية تحول دون التصرف في أمواله[2].

[1] هلالي عبد اللاه أحمد، مرجع سابق ، ص 102

[2] Myriam Quéméner, Yves Charpenel, La cybercriminalité, op cit, p 135.

كما يتخذ الركن المعنوي فيها صورة القصد الجنائي الخاص كما نص عليه المشرع الجزائري في المادة 372 من قانون العقوبات، والذي يستلزم انصراف نية الجاني إلى تملك المال بطريق الغش، اين يتكون القصد العام في هذه الجريمة من اجتماع عنصري العلم والإرادة، فعلم الجاني بأن فعله ينطوي على الاستيلاء غير المشروع على مال الغير، مع الإرادة الجادة لتحقيق ذلك، ويفترض أن تتحقق الجريمة بدون وجه حق، وأن تكون المنفعة محققة بطريق غير مشروع، فليست من جريمة النصب المعاملات التجارية الإلكترونية الشرعية الهادفة إلى ربح استثماري مشروع، كالمنافسة التجارية التي تولد ضرراً اقتصادياً لشخص بينما تحقق منفعة لآخر، وليس بنية الغش كاستخدام برامج جمع المعلومات المتعلقة بالمنافس التجاري على شبكة الإنترنت بواسطة صائد المعلومات"Bot" ، مما يستبعد الجرائم المبنية على الغلط أو المنافسة المشروعة[1].

- **الاستخدام غير المشروع لأدوات الدفع الإلكتروني:** تُعدّ تقنية الدفع الإلكتروني للأموال من أبرز التطبيقات الحديثة لتكنولوجيا المعلومات، إذ كسّرت حاجز التعامل بالنقود المادية وعوائق المبادلات المالية التقليدية، فأصبحت تتم بسهولة وسيولة عالية في غضون لحظات غير أنها، وبقدر ما تؤكّد المؤسسات المالية أمنها، تظلّ الهدف الأوّلي لمرتكبي الجرائم المعلوماتية.

وبانتشار التجارة الإلكترونية بشكل واسع كتطبيق حديث لتكنولوجيا المعلومات، إذ أتاحت لرجال الأعمال تجنب مشقة السفر والتنقل بين الدول للقاء شركائهم وعملائهم، مما يوفر الوقت والجهد والتكاليف المالية، كما أصبح بإمكان المستهلك الحصول على السلع والخدمات المطلوبة دون الحاجة إلى التنقل أو الدفع النقدي التقليدي، حيث يكفي توفر جهاز حاسوب متصل بشبكة

[1] هلالي عبد اللاه أحمد، مرجع سابق ، ص 105

الإنترنت. ويمكن تشبيه التجارة الإلكترونية بسوق رقمي افتراضي يجتمع فيه البائعون والموردون والزبائن، حيث تُقدَّم الخدمات بشكل إلكتروني ويتم الدفع مقابلها عبر وسائل نقدية إلكترونية[1]

تشير الإحصائيات الحديثة إلى نمو هائل في حجم المعاملات المالية عبر شبكة الإنترنت، حيث بلغت قيمة عمليات البيع والشراء الإلكترونية في المملكة المتحدة يوم 8 ديسمبر 2007 حوالي 320 مليون جنيه إسترليني، مع توقعات بوصول مبادلات الربع الأخير من عام 2008 إلى 13.5 مليار جنيه إسترلينيوفي الوقت الحاضر، تُظهر بيانات 2025 ارتفاعاً مذهلاً لهذه الأرقام، إذ تجاوز حجم التجارة الإلكترونية العالمية 6.3 تريليون دولار أمريكي، بينما سجّلت المملكة المتحدة وحدها مبيعات إلكترونية بقيمة 221 مليار جنيه إسترليني في 2024، مع توقعات ببلوغ 260 مليار جنيه بحلول نهاية 2026[2].

وتمكّن بطاقات الدفع الإلكتروني من إجراء المعاملات المالية بشكل رقمي بالكامل دون الحاجة الى نقل مادي للأموال، مما وسّع نطاق التجارة الإلكترونية عالمياً من خلال تبسيط عمليات التبادل التجاري، وتتعدّد أشكال هذه البطاقات وأنواعها كبطاقات الائتمان ذات الحد الائتماني المرن، بطاقات الخصم المباشر المرتبطة بالرصيد المتاح، المحافظ الرقمية (Digital Wallets)، وبطاقات الدفع المقدّم(Prepaid Cards) ، وذلك نتيجة الانتشار الواسع والاعتماد المتزايد عليها في النظم الإلكترونية للدفع.

[1] قانون رقم 18-05 المؤرخ في 10 ماي 2018 المتعلق بالتجارة الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، ع 28، 16 ماي 2018، ص 12

[2] Statista ،"E-commerce worldwide - statistics & facts"،... see on https://www.statista.com/topics/871/online-shopping/?srsltid=AfmBOopXZvNy-iqDNh6ai37XRBJ_-D7F6QFexiOJvYz3yx3SQL-lfpGV

See UK Office for National Statistics ،"Internet Retail Sales"2024, p 15

وتمثل جرائم الاستخدام الغير شرعي لبطاقات الدفع الإلكتروني من ابرز اشكال الاعتداء على الاموال المتداولة عبر النظم المعلوماتية، خاصة مع الانتشار المتسارع للتجارة الالكترونية[1] ويتجسد هذا الاستعمال التعسفي – الذي يشكل جريمة – في الاستخدام غير المشروع للبطاقة من قبل غير حاملها، اذ يصنف الاستعمال المباشر من قبل حامل البطاقة عادة كجريمة خيانة امانة[2] ويقصد بهذه الجرائم التي يرتكبها الغير، تلك التي يقدم عليها متخصصون في مجال المعلوماتية ويستهدفون امن النظم ومرتادیها، في تركيز جهدهم على القرصنة والقبض على البيانات المالية الشخصية للأفراد والمؤسسات البنكية، بقصد اعيائها بطريق غير مشروع لاقتناء سلع وخدمات وتحميل الغير مسؤولية دفع ثمنها[3].

1-9-2) جرائم الاعتداء على حقوق الملكية الفكرية :

مع تسارع وتيرة الثورة المعلوماتية برزت تحديات جديدة موازية لهذا التطور، من أهمها الإشكالات المرتبطة بنمط مستحدث من أنماط الملكية الفكرية يمكن وصفه بـ الملكية الرقمية، وهي تلك التي تَرِدُ على برامج الحاسوب وبياناته والمصنفات الرقمية المنشورة عبر شبكة الإنترنت، والتي بُذل في إعدادها وجمعها وتنظيمها جهد فكري وإبداعي يقتضي توفير حماية قانونية ملائمة لها بوصفها حقوق ملكية فردية أو جماعية تعود لمؤلفيها وأصحابها، وفي سياق الانتقال إلى مجتمع المعلومات، يقتضي الأمر التوفيق بين ضمان نفاذ الأفراد إلى هذه الموارد المعلوماتية وبين

[1] حشمان، عمّار، الجريمة المعلوماتية في التشريع الجزائري، 2020، الجزائر، ص 167

[2] بن سعادة نادية، الجريمة الإلكترونية، دلالة المفهوم وفعالية المعالجة القانونية، مجلة العلوم القانونية والسياسية، عدد 14، سنة (2021)، ص 134.

[3] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (N. UNODC2013 ،) PP 92-98

كفالة حماية حقوق المؤلفين وذوي الحقوق المجاورة، من خلال تبني آليات حديثة لصون الملكية الرقمية ضمن منظومة حماية الملكية الفكرية[1].

وقد أشار المشرع الجزائري إلى مفهوم المصنفات الرقمية في الأمر 03-08 المؤرخ في 19-07-2003 في نصوص المواد 02-03-04-05 المتضمن لقانون حماية الدوائر الشكلية والمتكاملة، إضافة إلى نص المادة 03 والمادة 27 من الأمر 03-05 المؤرخ في 19-07-2003 المتضمن قانون حماية المصنفات وحقوق المؤلف، واشترط المشرع لا تكون هذه المصنفات محل حماية قانونية توفر شرطين هما:

إفراغ الإنتاج الذهني في صورة مادية وإصباغ صفة الابتكار على المصنف[2].

1-9-3) جرائم المعلوماتية الماسة بالآداب العامة :

تتمثل هذه الجرائم بوجه عام في جملة من السلوكات التي تمس بالمنظومة الأخلاقية السائدة في المجتمع، غير أن تناولها قانونياً يطرح صعوبة خاصة بسبب تباين القيم والمعايير الاجتماعية بين مجتمع وآخر، بل وأحياناً داخل المجتمع الواحد بين طبقاته وفئاته المختلفة؛ إذ قد يُعدّ فعل معين مظهراً من مظاهر الانحلال الخلقي في بيئة اجتماعية معينة، بينما لا يُنظر إليه بالوصف نفسه في بيئة أخرى، وتُعرَّف جرائم الأخلاق في الإطار القانوني والاجتماعي، بأنها

[1] عبد الكريم عبد الله عبد الله، الحماية القانونية للملكية الفكرية على شبكة الأنترنت، دار الجامعة الجديدة، سنة 2008، مصر، ص 249.

[2] Ordonnance n° 03-05 du 19 Joumada El Oula 1424 correspondant au 19 juillet 2003 relative aux droits d'auteur et aux droits voisins, n° 44

الأفعال التي تنطوي على اعتداء على القيم الأخلاقية والاجتماعية المستقرة والمتعارف عليها في النظام الاجتماعي القائم[1].

ويُشترط في الغالب للقول بوجود جريمة معلوماتية ماسة بالآداب العامة أن تستوفي جملة من الشروط الأساسية، وهي العلنية، أي أن تترتب عليها نتائج يعترف بها القانون ويرتب عليها الآثار القانونية المتوقعة، والعرض على العامة، أي التوفر للجمهور بشكل يتاح له الوصول إليه[2].

أما المشرع الجزائري فقد تعرض لمفهوم هذه الجرائم في بعض نصوص قانون العقوبات دون تحديد نطاقها المتصل بتقنية المعلوماتية، إلا أنه يمكن إعمال هذه النصوص على جرائم المعلوماتية بالقياس على عموميتها وشموليتها[3] فنجد نص المادة 333 من قانون العقوبات الجزائري يجرم كل شخص ارتكب فعلا مخلا بالحياء بصفة علنية، ويعاقب عليه بالحبس من شهرين إلى سنتين وغرامة من 500 إلى 2000 دينار جزائري[4]، وتكملها المادة 333 مكرر بعقوبة مثلاها في حق من صنع أو حاز أو استورد أو سعى إلى ذلك، أو وزّع أو أجر أو ألصق أو أقام معارض أو عرض أو شرع في ذلك، أو باع أو شرع في البيع أو وزّع أو شرع في ذلك، كل مطبوع أو محرر أو رسم أو إعلان أو صورة أو لوحة زيتية أو صورة فوتوغرافية أو أنتج أي شيء مخل بالحياء[5].

[1] عبد العال الدريبي، مرجع سابق، ص 235.

[2] بن سعادة، نادية، الجريمة الإلكترونية، دلالة المفهوم وفعالية المعالجة القانونية، مجلة العلوم القانونية والسياسية، عدد 14 ،2021، ص 145.

[3] حشمان، عمّار، الجريمة المعلوماتية في التشريع الجزائري، جامعة ورقلة، 2020، ص 189.

[4] قانون العقوبات الجزائري، مرجع سابق

[5] نفس المرجع

1-9-4) الجرائم المعلوماتية الماسة بالنظام العام :

يثير تحديد طبيعة هذه الجرائم – التي تستخدم الجريمة المعلوماتية كوسيلة ارتكاب أساسية – إشكالية بالغة الصعوبة، نظرا للاعتماد على معيار الخطورة ومدى تهديدها للمصالح العامة للأفراد والمجتمع، غير أن أغلب التشريعات أقامت ترسانة قانونية عقابية لمواجهة كل ما يمس أمن وسلامة مواطنيها ومؤسساتها الحيوية، من خلال ما ورد في المادتين 15 و16 من الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتية والمتعلقة بالأعمال الإرهابية التي تكون بواسطة الأنظمة الكترونية و الجرائم المتعلقة بالجريمة المنضمة المرتكبة بواسطة النظم المعلوماتية، التي حصرت نوعها في نشر أفكار و مبادئ الجماعات الإرهابية و الدعوة لها، تمويل العمليات الإرهابية و التدريب عليها و تسهيل الاتصالات بين المنظمات الإرهابية، نشر طرق صناعة المتفجرات، نشر النعرات و الفتن و الاعتداء على الأديان و المعتقدات، القيام بعمليات غسل الأموال أو نشر طرق غسل الأموال، الترويج للمخدرات و المؤثرات العقلية، الاتجار بالأشخاص و الاتجار بالأعضاء البشرية[1].

حيث تشكل الجرائم المعلوماتية الماسة بالنظام العام في التشريع الجزائري تهديداً جوهرياً لأمن الدولة واستقرار المؤسسات الحيوية، إذ تُعرَّف بأنها الأفعال الإجرامية غير المشروعة التي تُرتكب بوساطة أنظمة المعالجة الآلية للمعطيات أو شبكات الاتصال الإلكترونية بقصد الإضرار بالدفاع الوطني أو السلامة العامة أو المصالح الاستراتيجية، وتُنظَم تشريعياً في المواد 394 مكرر إلى 394 مكرر 07 من قانون العقوبات، إلى جانب قانون 09-04 المؤرخ في 5 أوت 2009

[1] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المبرمة بالقاهرة بتاريخ 21 ديسمبر 2010.

المتعلق بمكافحة جرائم تكنولوجيا الإعلام والاتصال؛ حيث تُجرم الدخول أو البقاء غير المشروع في هذه الأنظمة بالحبس من ستة أشهر إلى ثلاث سنوات وغرامة تتراوح بين 500,000 و2,000,000 دينار جزائري مع تشديد العقوبة في حال الإتلاف أو التهديد المباشر للنظام العام، مع تجريم الإفشاء غير المشروع للبيانات الشخصية المادة 68 والجمع بالتدليس في نص المادة 59، شريطة توافر العلنية والخطورة الفعلية على المصالح العامة، مما يُبرِّر توسيع نطاق المسؤولية الجنائية لتشمل الشخص المعنوي وتفعيل إجراءات المراقبة الإلكترونية الخاصة[1]

1-9-5) جرائم الاعتداء على خصوصية الأفراد :

يُعدّ الحق في احترام الحياة الخاصة، بما يجسّده من مبدأ الخصوصية للأفراد، من الحقوق اللصيقة بالشخصية الإنسانية التي تُقرّر للإنسان لمجرد كونه إنسانًا، ويُصنَّف ضمن أهم حقوقه الأساسية لارتباطه الوثيق بحرية الفرد واستقلاله الذاتي. غير أنّ تطوّر تكنولوجيا المعلومات وما أفرزته من نظم معلوماتية متقدمة، قوامها الحواسيب وشبكات الاتصال على اختلاف أنواعها، الدولية منها والوطنية، بما تمتلكه من قدرات فائقة على جمع البيانات ذات الطابع الشخصي، واستثمارها عبر التخزين والاسترجاع والتصنيف والتحليل والمعالجة، ثم تداولها ونقلها دون عوائق تقنية تُذكر، أضحى يشكّل مساسًا جديًا وخطرًا حقيقيًا بحق الأفراد في احترام حياتهم الخاصة، لاسيما مع ظهور ما يُعرف بقواعد أو بنوك المعلومات، الأمر الذي استتبع ضرورة إقرار آليات

[1] بن سعادة نادية، مرجع سابق، ص 145 وما يليها.

انظر كذلك: حشمان عمار، الجريمة المعلوماتية في التشريع الجزائري، جامعة ورقلة، 2020، ص 189 وما يليها

قانونية فعّالة للتصدي للإجرام المعلوماتي الذي صار يُمثّل تهديدًا صريحًا لحقوق الإنسان، وفي مقدمتها الحق في الحياة الخاصة[1].

ويُقصَد بالحياة الخاصة في مجال الجرائم المعلوماتية ذلك النطاق السري من حياة الشخص، المادي منها والمعنوي، وما يرتبط به من بيانات ومعلومات ذات طابع شخصي تُعرّفه أو تجعل التعرف عليه ممكنًا، التي تُجمع أو تخزن أو تعالَج أو تُتداوَل عبر النظم أو الشبكات المعلوماتية، على نحو لا يجيز القانون التعرض لها بالاطلاع أو الاستخدام أو الإفشاء أو الربط ببيانات أخرى أو إتاحتها للغير إلا بناءً على رضا صريح من صاحبها أو استنادًا إلى سند قانوني مشروع، ويُعد كل مساس غير مبرّر بهذا النطاق، بالوسائط الإلكترونية أو الرقمية، اعتداءً على حرمة الحياة الخاصة في صورتها المعلوماتية[2].

وتشكل جرائم الاعتداء على حرمة الحياة الخاصة للأفراد جزءا مهما من النشاط الإجرامي المعلوماتي ويمكن حصر صورها في الأوصاف التالية:

- **جريمة القذف والتشهير عبر وسائل الأنترنت:** يُعرَّف القذف قانونًا بأنه إسناد واقعة معيّنة لو كانت صحيحة لأوجبت على من أُسندت إليه عقابًا أو احتقارًا عند أهل وطنه، مثل الرمي بالزنا أو الفساد أو السرقة، وهو يختلف عن السب الذي يتمثّل في عبارات غير محدِّدة تمس الشرف

[1] محمد مثال، حماية الحياة الخاصة في مواجهة تكنولوجيا المعلومات، دار الجامعة الجديدة، الإسكندرية، 2022، ص 45.

[2] نغم عبد الكريم مهدي، مفهوم الحق في حرمة الحياة الخاصة وأثر وسائل تقنية المعلومات الحديثة عليه، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كربلاء، المجلد 12، العدد 2، 2023، ص 210–212.

عمومًا[1] أما التشهير فيشمل نشر أو إذاعة أي عبارات أو صور أو فيديوهات من شأنها الحطُّ من قدر الشخص أو النيل من سمعته لدى الغير، سواء في حياته الخاصة أو المهنية[2].

ويُقصد بالقذف والتشهير عبر الإنترنت استخدام الوسائط الرقمية مثل فيسبوك، تويتر، إنستغرام، تيك توك، أو المنتديات الإلكترونية لنشر محتوى يحمل صفات القذف أو التشهير، مع تحقُّق شرط العلانية الذي يتميَّز بسرعة الانتشار واتساع الجمهور[3] ويُميِّز هذا النوع الخطورة بسبب الديمومة، إذ يبقى المحتوى متاحًا للعامة إلا إذا حُذِفَ أو حُجِبَ[4]

أركان الجريمة: يقوم الركن الشرعي من نصوص قوانين العقوبات المتعلقة بالقذف والسب، بالإضافة إلى قوانين الجرائم المعلوماتية التي تجرِّم النشر الإلكتروني للمحتوى المهين، مع اعتبار الإنترنت صورة حديثة من العلانية[5]

أما الركن المادي لها فيشمل الفعل نشر عبارة أو صورة أو فيديو يحمل واقعة قذف أو عبارة تشهيرية، مع توافر العلانية التي تتحقَّق بنشر المحتوى على صفحات عامة أو مجموعات واسعة، بخلاف الرسائل الخاصة المحدودة، ويُضاف إليه الاستمرارية إذا بقيَ المحتوى متاحًا[6].

بالنسبة للركن المعنوي فيتطلَّب علم الجاني بمضمون العبارات وأنها تمسُّ الشرف، مع إرادة النشر لإلحاق الضرر، وهو قصد جنائي خاص يُثْبَتُ من سياق المنشورات أو تاريخ الجاني[7].

---

[1] الشافعي محمد زكي، التكييف القانوني لجريمة القذف عبر مواقع التواصل الاجتماعي، مجلة البحوث القانونية رقم 5،2020، ص 125 وما يلها

[2] بركات يمان، جرائم السب والقذف التقليدية والإلكترونية- دراسة مقارنة- رسالة ماجستير، كلية القانون، جامعة الشارقة، 2019، ص 82.

[3] الشافعي محمد زكي، مرجع سابق، ص 50

[4] هزيل أمال، خليفي وردة، الجرائم الماسة بالسمعة والشرف عبر الإنترنت، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، مجلد 9، رقم 2، ص 155

[5] عبد السلام عليلي، جريمة القذف عبر وسائل التواصل الاجتماعي، مجلة الدراسات القانونية والاقتصادية، المركز الجامعي سي الحواس بريكة، المجلد 5، العدد 02، 2022، ص 577 وما يلها.

[6] المرجع نفسه، ص 578

وتتميَّز هذه الجريمة بسرعة الانتشار الذي يُضاعِفُ الضرر المعنوي، وصعوبة الإثبات بسبب الحسابات المجهولة، مما يستدعي خبراء تقنيين لتتبُّع العناوين IP أو السجلات الرقمية، كما تثير مشكلات الاختصاص القضائي عند عبور الحدود، حيث يُعتمَدُ مبدأ المكان أو الضرر[1].

- **جرائم التعدي على البيانات الشخصية:** تُعتبر الحياة الخاصة مقوِّمًا جوهريًا من مقوِّمات كيان الإنسان، لا يجوز المساس به أو نزعه عنه، ويُعد احترامها من المبادئ الدستورية الراسخة التي تقرّرها الدساتير الحديثة في صلب أحكامها، حيث تقضي بأن لحياة المواطنين الخاصة حرمة مصونة يحميها القانون، وبأن لكل شخص الحق في أن تظل أسرار حياته الخاصة بعيدة عن دائرة العلنية، ومحمية من كل صور تدخل الغير أو اطلاعهم عليها بغير سند مشروع[2].

وتشكل الجريمة المعلوماتية مظهرا حديثا، يهدد بخطر محدق البيانات الشخصية للأفراد من عدة زوايا نوجزها فيما يلي:

جمع وتخزين المعطيات بطرقة غير شرعية: يتمثل فعل انتهاك الحق في الحياة الخاصة للأفراد في عملية جمع البيانات الشخصية الدقيقة وتخزينها، وإن كانت صحيحة، على نحو غير مشروع، وتستمد هذه الصفة غير المشروعة إما من أساليب الحصول على هذه البيانات، أو من طبيعتها الخاصة التي تجعل معالجتها مساسا بحرمة الفرد[3].

---

[7] عبد السلام عليلي، مرجع سابق، ص 580

[1] لوسي موسى، التكييف القانوني لجريمة القذف عبر مواقع التواصل الاجتماعي في التشريع الجزائري، مجلة الدراسات السياسية والقانونية، جامعة عمار ثليجان الأغواط، المجلد 5، عدد 1، 2019، ص 291.

[2] Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." Harvard Law Review 4, no. 5 (1890),P 193

[3] IPID, P 198

من جهة الأساليب ان تكون غير المشروعية: يعتمد الجاني غالبا على وسائل تجسس تقنية متطورة، مثل استخدام معدات لترجمة ارتجاجات الجدران إلى كلمات وعبارات عبر برامج حاسوبية مخصصة، أو اعتراض الرسائل الإلكترونية، أو اختراق النظم المعلوماتية الخاصة بالمجني عليه، ما يعد تعديا صارخا على حرمة الحياة الخاصة[1]

غير مشروعية طبيعة البيانات: تتمثل في حرمة جمع وتخزين ومعالجة البيانات الشخصية الاسمية من قبل الغير دون إذن، كما في المعلومات المتعلقة بالسجل القضائي التي لا يجوز لغير السلطة القضائية التحكم بها حفاظا على سمعة الأشخاص وكرامتهم[2].

– **إساءة استعمال البيانات و المعلومات الاسمية:** تستند جريمة انتحال الشخصية الى مبدا الاعتداء على البيانات الشخصية التعريفية الخاصة بالغير، بهدف التمويه والافلات من المساءلة القانونية، حيث يقوم الجاني باستغلال هوية شخص آخر لتحقيق مكاسب غير مشروعة – غالبا ذات طابع مادي – دون تحمل تبعات الملاحقة القضائية، وقد سجلت الاحصائيات الفرنسية لعام 2009 نحو 210,000 حالة ضحايا لهذا النوع من الجرائم عبر الانترنت، بنمو سنوي يقدر بـ40% في الدول الغربية، مما يصنفها ضمن مكونات جرائم الاحتيال الالكتروني الأساسية، ويعزو زيادة التعرض لهذه المخاطر الى الاعتماد المتسارع على تكنولوجيا المعلومات وشبكة الانترنت، حيث تفرض آليات التحقق الرقمي – كاسم المستخدم وكلمة السر والعنوان الرقمي ورقم البطاقة المصرفية – كادوات اكثر عرضة للاستغلال مقارنة بالبيانات التقليدية (الاسم واللقب

[1] Solove, Daniel J. Understanding Privacy. Cambridge, MA: Harvard University Press, 2008, pp. 102–105.

[2] Westin, Alan F. Privacy and Freedom. New York: Atheneum, 1967, p. 346.

والصورة)، حيث شهدت هذه الجرائم توسعا غير مسبوق مع انتشار التكنولوجيا، حيث اشار الخبير القانوني اوليفي ايتانو الى ان "نحن قد دخلنا مرحلة الهوية المستهلكة"، اي الهوية القابلة للاستبدال والتنفيس بعد استخدامها للمرة الاولى[1].

إفشاء البيانات الاسمية (سرية البيانات للعلن): إن هذا النوع من السلوكات الإجرامية، قد يكون نتيجة حتمية للجرائم السالف ذكرها، بأن البيانات الخاصة قد انتقلت من السر إلى العلانية، بمجرد تخزينها بعد تجميعها على نحو غير مشروع أو حتى بصفة مشروعة، وبالتالي فإنها تكون عرضة للاطلاع عليها من قبل عدد غير محدد العدد من الأشخاص في حال عرضها على شبكة الأنترنت أو على الأقل من قبل عدد محدد متمثل في الأشخاص العاملين في فضاء المعلوماتية[2].

- **جرائم الاستغلال القصر عبر الأنترنت:** لم تشهد البشرية منذ وجودها تقاربا بين الافراد والحضارات كالذي تشهده اليوم، مجادلة بفعل توفر تكنولوجيا المعلوماتية وشبكة الانترنت، الا ان هذه الاخرة قد اصبحت مصدر خطر وتهديد لاعتبارات جدلية تتمثل اساسا في كونها شبكة تواصل بدون حدود جغرافية او ادارية، وبدون مركز موحد للإدارة القانونية، مما اتاح لفئة من المستخدمين استغلالها بشكل مخالف للهدف الاساسي من انشائها وهو تبادل المعارف والعلوم، فأصبحت وسيلة مفضلة لارتكاب جرائمهم الناشئة عن ميولاتهم الاجرامية وغاياتهم الدنياوية، وذلك

[1] Myriam Quéméner, Yves Charpenel, La cybercriminalité - op.cit -p 89-90.

[2] Solove, Daniel J. Understanding Privacy, Opcit, pp. 110-115.

- Cf. Algerian Law No. 18-07 of June 10, 2018, Art. 4 (regulating the conditions for lawful processing and storage of personal data to prevent unauthorized disclosure).

من خلال نشرهم وتبادلهم نصوصا ومقاطع فيديو تتعلق باستغلال الاطفال جنسيا بشكل مواد اباحية طفلية[1].

وتعد هذه الجرائم ناتجة مباشرة عن نطاق العالمية الذي تتمتع به شبكة الانترنت، والذي يتاح بواسطته نشر الاعمال المخلة بالآداب العامة والاخلاق الحامية، والتي يتباين مفهومها من بلد لآخر بسبب اختلاف التشريعات والقيم الثقافية. فاستخدام التكنولوجيا المعلوماتية في نشر المواد الاباحية الموجهة اصلًا لشريحة البالغين، قد لا يستثني شريحة الاطفال الذين يمكن ان يكونوا عرضة إما لتعرضهم لهذه المواد المضرة، او حتى محل انتاجها، مما يشكل اعتداء مادي ومعنوي صارخ على حقوق الاطفال وكرامتهم[2].

ومما يزيد من مخاطر الأنترنت على الأطفال هو اعتبارهم الفئة الأكثر انجذابا لهذه التقنية، والأكثر تصفحا للإنترنيت فقد قدمت وكالة كاليستو لاتحاد صوت الطفل– Calysto pour la fédération de la voix de l’enfant إحصائيات تفيد بأن 12% من هذه الفئة تقضي أكثر من 03 ساعات يوميا في تفقد الرسائل الإلكترونية، وأن أكثر من 87% منهم قد تفاجأوا بمضامين اغرائية فاضحة، وبالتالي فان الأطفال هم الفريسة الأسهل على شبكة الأنترنت[3].

[1] احمد بن محمد الشريف، الجرائم المعلوماتية وحماية الاطفال، الجزائر، دار الجامعة الجديدة، 2022، ص 156 وما يليها.

- انظر كذلك القانون رقم 18-07 المؤرخ في 10 جوان 2018 المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المادة 52 التي تجرم نشر المواد الاباحية الطفلية.

[2] احمد بن محمد الشريف، مرجع سابق، ص 157 وما يليها

[3] Myriam Quéméner, Yves Charpenel, Opcit, P 103

أنواع الجرائم المتعلقة بها:

نشر وتبادل المواد الإباحيّة الطفليّة: إنتاج، تخزين، أو توزيع صور ومقاطع فيديو تُظْهِرُ أطفالاً في أوضاع جنسيّة صريحة عبر مواقع الويب، تطبيقات التراسل، أو المنتديات المظللة (Dark Web).

التحرُّش الجنسيِ عبر الإنترنت :محادثات جنسيّة مُبَاشِرَةٌ مع قاصرين عبر وسائل التواصل الاجتماعيٍ أو غرف الدردشة، غالبًا باستخدام هويّات مزيَّفة.

الإغراء الجنسيٍ :(Grooming) بناء علاقة ثقة مع طفل عبر الإنترنت لاستدراجه إلى لقاء فعليٍ ينتهي بالاستغلال الجنسيٍ[1].

- التحديات القانونيّة والإجراءات الوقائية لمكافحة هذه الجريمة:

تواجه السلطات القضائية تحديات جمة في مواجهة جرائم الاستغلال الجنسي للقصر عبر الإنترنت تتراوح بين صعوبة إثبات الركن المادي للجريمة نتيجة استخدام تقنيات التشفير المتقدمة كـ VPNوشبكةTor ، وإشكالية الاختصاص القضائي العابر للحدود حيث يقع الجاني أو الخادم أو الضحية خارج الإقليم الوطني مما يستلزم تنازع قوانين واتفاقيات تسليم مجرمين غير مبرمة مع كثير من الدول. كما يثير تحدي الإثبات التقني حاجة ماسة الى خبراء متخصصين قادرين على تتبع العناوين الرقمية (IP addresses) واسترجاع السجلات اللوغية (logs) دون انتهاك خصوصية الأبرياء، إضافة الى ضمان سرية هويةِ الطفل الضحية أثناء التحقيقات لتفادي

[1] المادة 333 مكرَّر من قانون العقوبات الجزائريّ، المعدَّل بالقانون 15-05.

تعريضه للضرر النفسي الإضافي، وهو ما يفرض توازنا دقيقا بين مطلب العدالة وحماية حقوق الإنسان[1].

أما على صعيد التشريع الجزائري فقد جاء تجريم هذا النوع من السلوكيات متأخرا جدا من خلال القانون رقم 14-04 المؤرخ في 04 فيفري 2014 الذي استحدث نص المادة 333 مكرر 1 ضمن قانون العقوبات الجزائري والتي نصت على ان "يعاقب بالحبس من 5 سنوات الى 10 سنوات وبغرامة من 500 الف الى 1 مليون دج كل من صور قاصرا لم يكمل 18 سنة بأي وسيلة كانت وهو يمارس انشطة جنسية بصفة مبينة حقيقية او غير حقيقية، او صور الاعضاء الجنسية للقاصر جنسية اساسا، او قام بإنتاج او توزيع او نشر او ترويج او استيراد او تصدير او عرض او بيع او حيازة مواد اباحية متعلقة بالقصر، وفي حال الادانة تأمر الجهة القضائية بمصادرة الوسائل المستعملة لارتكاب الجريمة والاموال المتحصل عليها مع مراعاة حقوق الغير حسن النية."

وبذلك وسع المشرع الجزائري من مظاهر الحماية الجنائية التي كانت محصورة في النصوص التقليدية كالمادة 333 مكرر والمواد 335 ق من قانون العقوبات المتعلقة بفعل المخل بالحياء، ونصوص المواد من 342 الى 349 المتعلقة بجريمة البغاء وجرائم التحرش الجنسي المقررة بموجب المادة 341 مكرر، مسايرا بهذا النسق الدولي التشريعي في مجال حماية الاطفال ضد مخاطر تكنولوجيا المعلومات.

[1] بلقاسم بن محمد، الحماية الجزائية للطفل من جرائم الاستغلال الجنسي عبر شبكة الإنترنت، مجلة البحوث القانونية، العدد 12، سنة 2020، ص 78 وما يليها.

- انظر كذلك المادة 52 من القانون رقم 18-07 المؤرخ في 10 جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

غير ان النص الجديد لا يخلو من القصور الواضح، فقد سهى المشرع عن تجريم فعل الاغراء الجنسي (grooming) عبر شبكات الاتصال، وركز مجال التجريم على افعال التصوير وتصميم الصور الخاصة بالممارسة الجنسية ونشرها وحيازتها دون الالتفات الى الطبيعة التحضيرية لجريمة الاستدراج الالكتروني الذي يشكل مدخلا للاستغلال الفعلي، ولذلك يجب على المشرع الجزائري اعادة صياغة النص بما يتناسب مع واقع الجريمة المعلوماتية المعاصرة لا مع التصور القانوني التقليدي فقط، من خلال:

تجريم الاغراء الجنسي عبر الوسائل الالكترونية كركن تحضيري مستقل مع توسيع نطاق العقوبة لتشمل منصات التواصل الاجتماعي المسؤولة، كذلك اشتراط التعاون الدولي في التحقيقات عابرة الحدود[1].

2- آليات مكافحة الجرائم المعلوماتية:

أضحت الجريمة المعلوماتية قابلة للارتكاب من أي نقطة في العالم بالقدر نفسه من السهولة التي يمكن ارتكابها من أقرب مكان، نظرا لما تتيحه شبكات الاتصال الحديثة من تجاوز للحواجز المكانية والحدودية، إذ قد تشكل رسالة إلكترونية واحدة أداةً لارتكاب جريمة معلوماتية ممتدة عبر عدة دول، لكل منها نظام قانوني وإجرائي مغاير، بما يثير إشكالات جدية على مستوى تحديد الاختصاص القضائي وتطبيق القانون الأنسب، ويزداد الأمر تعقيدا بالنظر إلى الطبيعة المتطايرة والسريعة الزوال للأدلة والآثار الرقمية الواجب تتبعها للكشف عن هوية الجاني وملاحقته، الأمر الذي يستلزم اتخاذ إجراءات فورية وفعالة للحفاظ على هذه الأدلة واستجلابها قبل

[1] القانون رقم 14-04 المؤرخ في 04 فيفري 2014 المعدل لقانون العقوبات، المادة 333 مكرر 1 وما يليها.

اندثارها، غير أن بطئ الآليات والإجراءات الرسمية التقليدية قد يؤدي عملياً إلى ضياع تلك الأدلة أو تعذر الاستفادة منها، لاسيما عندما تكون عدة دول ضحيةً للجريمة ذاتها، بما يجعل من تتبع سلسلة الأدلة الرقمية وحفظها والمحافظة على سلامتها تحدياً كبيراً على الصعيد العملي، بل إن بعض الجرائم المعلوماتية ذات المظهر المحلي قد تنطوي على بعد دولي خفي، فيقتضي التحقيق فيها طلب المساعدة القضائية من جميع الدول التي مرّ عبر أقاليمها أو بنيتها التحتية نشاط الجريمة، أو التي يوجد على إقليمها مزودو الخدمات أو الخوادم أو غيرها من مصادر الأدلة الرقمية، وعليه فإن تفعيل إجراءات وآليات في مواجهة الجريمة المعلوماتية يفرض بالضرورة تعبئة وتنسيق جهود السلطات المختصة في دولة مصدر الجريمة، وفي دول الضحايا، وكذلك في الدول التي عبرت من خلالها الأفعال الإجرامية أو يحتمل وجود أدلة الجريمة في إقليمها، تحقيقاً لفعالية المتابعة الجزائية وضماناً لعدم إفلات الجناة من العقاب[1].

2-1 الجهود الدولية والإقليمية في مكافحة الجريمة المعلوماتية:

إن التطرق إلى جملة الجهود الدولية الموجهة لدعم سبل مكافحة الجريمة المعلوماتية، بما في ذلك أعمال البحث والتحقيق المتعلقة بها، يُعدّ إجراءً يتصادم مباشرةً مع الطابع العابر للحدود لهذه الجرائم، مما يؤدي غالباً إلى تعطيلها نتيجة مبدأ إقليمية القوانين الجنائية ومفهوم سيادة الدول على إقليمها، ويمكن تلخيص هذه الجهود في مجموعة من المبادرات التي ترعاها الأمم المتحدة، مثل اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية (اعتمدت في ديسمبر 2024)، إلى جانب

[1] يوسف حسن يوسف، الجرائم الدولية للإنترنت، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة،2011،ص 141.

مبادرات دولية أخرى كاتفاقية بودابست بشأن الجريمة المعلوماتية (2001) التي أسست قواعد التعاون في تبادل الأدلة الرقمية والمساعدة القانونية المتبادلة.

2-1-1) جهود هيئة الأمم المتحدة في دعم مكافحة الجريمة المعلوماتية (الالكترونية)

تبذل الأمم المتحدة جهوداً لافتة ومتواصلة في مجال التصدي للجريمة المعلوماتية، وتؤكد على ضرورة تعزيز العمل المشترك بين الدول الأعضاء من أجل التعاون على الحد من انتشارها والحد من تصاعد آثارها المدمّرة، ومن خلال تتبع المؤتمرات الدولية الخمسية التي تعقدها الأمم المتحدة بشأن منع الجريمة والعدالة الجنائية (UN Congress on Crime Prevention and Criminal Justice)، نجد أن جرائم الحاسب الآلي والجرائم المعلوماتية قد حظيت باهتمام واسع ومتزايد[1]، فقد كان المؤتمر العاشر المنعقد في فيينا عام 2000 من أوائل المؤتمرات التي تناولت الجرائم المتصلة بشبكات الحاسوب (Crimes relating to the computer network) ، واعتمد إعلان فيينا بشأن الجريمة والعدالة في مواجهة تحديات القرن الحادي والعشرين[2].

كما أن المؤتمر الرابع عشر المنعقد في كيوتو عام 2021 تناول تحت عنوانه العريض «الجرائم الحالية والتطورات الأخيرة والحلول الناشئة، ولا سيما التكنولوجيات الجديدة كوسائل للجريمة وأدوات ضدها»، مما يعكس التطور المستمر للنقاش الدولي حول هذه الظاهرة[3].

وتُوّجت هذه الجهود في ديسمبر 2024 باعتماد الجمعية العامة للأمم المتحدة «اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية»، بعد مفاوضات استمرت خمس سنوات منذ صدور

[1] United Nations Congresses on Crime Prevention and Criminal Justice ،UNODC, 2021, PP 2-5
[2] Vienna Declaration on Crime and Justice ،UN Doc. A/CONF.187/42000 , P 7
[3] Kyoto Declaration ،UN Doc. A/CONF.234/L.6/Rev.12021 , PP 2-10

القرار 247/74 في نوفمبر 2019، والتي تُعدّ أول اتفاقية عالمية شاملة في هذا المجال، وتهدف إلى تعزيز التعاون الدولي في منع ومكافحة الجرائم الإلكترونية، وتسهيل تبادل الأدلة الإلكترونية، وحماية حقوق الضحايا، ودعم بناء القدرات خصوصاً في الدول النامية[1].

وبالموازاة مع هذه المؤتمرات والاتفاقيات، أطلق مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC) عام 2013 «البرنامج العالمي لمكافحة الجريمة السيبرانية (Global Programme on Cybercrime) لتقديم الدعم الفني وبناء القدرات للدول الأعضاء في مواجهة هذه الجرائم، وفقاً لقرار الجمعية العامة 230/65 لعام 2011[2].

من خلال هذه الجهود الدولية التي عملت على إرساء مبادئ واسس لمواجهة هذا النوع من الجرائم المتصف بتطوره خلصت الى طرق ووسائل والتي نجيزها في:

– **تبادل المعلومات:** وهو إجراء يشمل تقديم المعلومات والبيانات والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية وهي بصدد النظر في جريمة ما، عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم، وقد يشمل التبادل السوابق القضائية للجناة ولهذا الإجراء سند قانوني حسب ما جاء في الفقرة الثانية من المادة 01 من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية.

– **نقل الإجراءات:** وهو قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جزائية بصدد جريمة ارتكبت في إقليم دولة أخرى لمصلحتها، إذا توافرت شروط معينة أهمها التجريم المزدوج بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها، بمعنى أن تكون مقررة في قانون الدولة

[1] United Nations Convention against Cybercrime ،UN Doc. A/RES/79/XXX2024.
[2] UNODC Global Programme on Cybercrime2013 ،https://www.globalcoalition.us/node/228... See 12/10/2024…21.00m

المطلوب منها اتخاذها إضافة إلى كونها إجراءات جوهرية في كشف الحقيقة، وهو الإجراء المنصوص عليه في معاهدة الأمم المتحدة لنقل الإجراءات في المسائل الجنائية، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة 2000.

– **الإنابة القضائية الدولية:** يقصد بها طلب اتخاذ إجراء قضائي من أجل إجراءات الدعوى الجنائية تتقدم به دولة طالبة إلى دولة مطلوب منها، لضرورة الفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة تعذر عليها القيام به بنفسها، ويهدف هذا الإجراء إلى تسهيل المتابعة القضائية والتغلب على عقبات مبدأ الإقليمية[1].

2-1-2) الجهود الاقليمية مكافحة الجريمة الالكترونية

– **دور المجلس الأوربي:** يلعب المجلس الأوروبي دوراً محورياً في مواجهة الجرائم المعلوماتية من خلال إقراره لسلسلة من التوصيات والمعاهدات الدولية الرامية إلى حماية البيانات الشخصية من الاستخدام السيئ، وضمان تدفق آمن للمعلومات عبر الأنظمة الإلكترونية. وفي هذا السياق، وقّع المجلس بتاريخ 28 يناير 1981 الاتفاقية رقم 108 بشأن حماية الأفراد في مواجهة المعالجة الآلية لبيانات الطبيعة الشخصية (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data)، والتي تمثّل أول اتفاقية دولية ملزمة في مجال حماية البيانات، وقد صَدَقَتْ عليها حتى الآن سبع عشرة دولة أوروبية[2].

[1] يوسف حسن يوسف، مرجع سابق، ص ص 150-153

[2] European Treaty Series - No. 108 ،Council of Europe ،Strasbourg… https://www.europarl.europa.eu/about-parliament/en... See 12/10/2024…21.45m

غير أن الحدث الأبرز في هذا الإطار يتمثّل في تتويج جهود المجلس الأوروبي بإقرار اتفاقية بودابست بشأن الجريمة الإلكترونية (Convention on Cybercrime) بتاريخ 23 نوفمبر 2001 تحت رقم 185 من سلسلة المعاهدات الأوروبية (European Treaty Series – ETS No. 185)، والتي تهدف إلى تحديث التشريعات الداخلية لتتوافق مع متطلّبات عالم الرقّم والتكنولوجيا الرقمية المتسارعة. وقد تناولت الاتفاقية بشمولية جميع القضايا المتعلقة بالجريمة المعلوماتية، بما في ذلك تجريم الأفعال الرقمية المحدّدة، والإجراءات التحقيقية الخاصّة، وآليات التعاون الدولي، مما يجعلها الإطار القانوني الدولي الأوّل والأكثر شمولاً في هذا المجال. ودخلت الاتفاقية حيز التنفيذ بتاريخ 1 يوليو 2004، وتظلّ إلى اليوم أداةً أساسيّةً تساهم بشكلٍ دائمٍ ومستمرٍ في دعم الجهود العالميّة لمكافحة الجرائم المعلوماتيّة من خلال توحيد المعايير القانونيّة وتيسير المساعدة القضائيّة المتبادلّة[1].

تسعى الاتفاقية إلى تثبيت مبادئ جنائية معاصرة تتوافق مع التطورات التكنولوجية المتسارعة والتحولات الجوهرية الناتجة عن انتشار الأنظمة الرقمية، حيث تضمّنت (48) مادّة موزّعة على ثلاثة فصول رئيسية، هي:

- **الفصل الأوّل** :المتعلّق بالعناصر الموضوعيّة للجرائم المعلوماتيّة، بما في ذلك تعريف المصطلحات التقنيّة ذات الصلة، وتحديد الأركان القانونيّة والمفاهيم الأساسيّة لأشكالها المتنوّعة.

[1] Myriam Quéméner, Yves Charpenel, La Cybercriminalité, op.cit,P 228.

- **الفصل الثاني** :الخاصّ بالضوابط الإجرائيّة المتّصلة بآليات التحقيق والبحث في شأن الجرائم المعلوماتيّة.
- **الفصل الثالث** :المُعْنَى بالأحكام القانونيّة الخاصّة بالجرائم المعلوماتيّة العابرة للحدود السياديّة.

كما اعتمدت الاتفاقية على مذكّرة تفسيريّة أصدرتها لجنة وزراء المجلس الأوروبي بتاريخ 8 نوفمبر 2001 في دورته رقم 109، بالإضافة إلى البروتوكول الإضافيّ الخاصّ بتجريم الأفعال المساسة بكرامة الإنسان والمُحَرِّضَة على العنف والكراهيّة والتمييز العنصريّ بوساطة الأنظمة المعلوماتيّة (رقم 189)، والذي اعتُمِدَ في ستراسبورغ بتاريخ 28 يناير 2003، وقد صَدَّقَتْ عليه 20 دولة ووقَّعَتْه 18 دولةً أُخْرَى، ودخل حيّزَ النفاذ بتاريخ 1 مارس 2006[1].

إضافةً إلى ما تقدّم، وضع المجلس الأوروبي في أبريل 2008 خطوطاً توجيهيّة تهدف إلى دعم وتعزيز عمل الجهات المختصّة بمكافحة الجرائم المعلوماتيّة، كأجهزة الشرطة المتخصّصة والسلطات القضائيّة، وهو ما أكدته توصيات ورشة عمل المجلس الأوروبي المنعقدة عام 2010، والتي شدّدت على ضرورة:

- دعم الطابع الدوليّ لاتفاقيّة بودابست.
- تكوين رجال قضاء متخصّصين في مجال مكافحة الجرائم المعلوماتيّة.
- إعداد مخطّط وخارطة طريق لعمل أجهزة مكافحة الجرائم المعلوماتيّة.

[1] La situation de la Convention sur la Cybercriminalité, Traité de Budapest, Disponible sur le site officiel du Conseil de l'Europe, Date de consultation : 13/10/2024 lien direct :
http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=20/07/2014&CL=FRE

- تكثيف الجهود لردع الجرائم المتعلّقة بالاستغلال الجنسيّ للأطفال عبر شبكة الإنترنت

– **دور الاتّحاد الأوروبي:** يلعب الاتّحاد الأوروبيّ دوراً فعّالاً في دعم الجهود التشريعيّة على المستوى الإقليميّ الأوروبيّ لمكافحة الجرائم المعلوماتيّة، من خلال مبادرات اللجنّة الأوروبيّة، والتي يمكن إيجازها في:

- **القرار رقم 68/2004** :المتعلّق بمكافحة الاستغلال الجنسيّ للأطفال عبر شبكة الإنترنت.
- **القرار رقم 222/2005** :بشأن تحديد الإجراءات الفعّالة لمكافحة الهجمات الإلكترونيّة ضدّ الأنظمة المعلوماتيّة.
- **التقرير الصادر بتاريخ 22 مايو 2007:** بعنوان «سياسة عامّة في مجال مكافحة الجرائم المعلوماتيّة»، والذي تضمّن مجموعة من الإجراءات الموجّهة لتطوير ودعم سبل التعاون بين الجهات المختصّة على المستويين الأوروبيّ والدولي[1].

– **دور الدول العربية:** تقيم الجهود العربية في مجال تعزيز التعاون الاقليمي لمواجهة الجرائم المعلوماتية على انها محتشمة نسبيا مقارنة بالجهود الاوروبية المتقدمة، حيث تركزت البدايات الاولى على دعم الاجراءات الامنية الموجهة ضد الاعتداءات الماسة بحقوق المؤلف، نظرا لعدم انتشار هذه الجرائم بعد في الدول العربية. ويعّد القرار رقم 229 لسنة 1996 الصادر عن اجتماع مجلس وزراء العدل العرب اول مقترح تشريعي عربي موجّه لمكافحة الجرائم المعلوماتية.

[1] Myriam Quéméner, Yves Charpenel, La Cybercriminalité, op.cit,PP 229-230

غير ان أبرز هذه الجهود يتمثل في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، التي انبثقت عن اجتماع مشترك لمجلسي الوزراء الداخليين والعدل العرب في مقر الامانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 21 ديسمبر 2010، وقد وقّعتها 23 دولة عربية بما فيها الجزائر في اليوم ذاته، وتتكون الاتفاقية من خمسة فصول أو محاور رئيسية وهي:

الفصل الاول :الاحكام العامة، بما في ذلك تعريف المصطلحات الأساسية.

الفصل الثاني :الاحكام المتصلة بالتجريم المباشر لجرائم تقنية المعلومات.

الفصل الثالث :الاحكام الإجرائية الخاصة بآليات البحث والتفتيش والحفاظ على الادلة الرقمية.

الفصل الرابع :الاحكام المتعلقة بالتعاون القضائي المتبادل ومبادئ الاختصاص القضائي العابر للحدود.

الفصل الخامس :الاحكام الختامية والتنفيذية.

وتعّد هذه الاتفاقية نموذجا عربيا يحاكي الى حد كبير اتفاقية بودابست الاوروبية، من خلال تفصيلها الدقيق لإجراءات البحث والتحقيق المعلوماتي، مما يعزز التنسيق القانوني والقضائي بين الدول الاطراف لمواجهة الطبيعة العابرة لهذه الجرائم[1].

2-2) الجهود الوطنية (التشريع الجزائري):

في إطار الجهود الدولية والإقليمية الرامية إلى تعزيز ودعم سياسات مكافحة الجريمة المعلوماتية، بما في ذلك تيسير وإدارة عمليات البحث والتحري ذات الصلة، حرص المشرّع

[1] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، مرجع سابق

الجزائري على مواكبة التطورات التشريعية العالمية في هذا المجال، سعيًا منه إلى تبنّي أحدث الأدوات القانونية لمواجهة هذا النمط المتغير من الجرائم.

وقد جاء هذا التوجّه استجابة للتحولات التقنية التي تشهدها الجزائر خلال السنوات الأخيرة، لاسيما مع تعميم خدمات الاتصال بشبكة الإنترنت، وتوسيع استخدام تقنيات المعلوماتية ضمن مختلف المؤسسات الحكومية، الأمر الذي أسفر عن ارتفاع ملحوظ في معدلات الجريمة المعلوماتية.

وأمام هذه المعطيات، تدخّل المشرّع الجزائري لوضع الأطر القانونية والمخططات العملية الكفيلة بتنفيذ سياسة شاملة ذات بعد وقائي وردعي في مواجهة هذه الجرائم. وتمثل أول تدخل تشريعي نوعي في هذا المجال في صدور القانون رقم 04-05 المؤرخ في 10 نوفمبر 2004، المعدِّل والمتمِّم لقانون العقوبات الجزائري، حيث تضمّن استحداث قسم خاص بعنوان جرائم المساس بأنظمة المعالجة الآلية للمعطيات. وقد نص هذا القسم على مجموعة من المواد تتراوح من المادة 394 مكرر إلى المادة 394 مكرر 07، التي عالجت مختلف صور الجريمة المعلوماتية، بدءًا من الدخول غير المشروع إلى الأنظمة المعلوماتية، وصولًا إلى الأفعال الماسة بأمن وسلامة النظم المعلوماتية العامة والخاصة، مع تحديد العقوبات المقررة لكل منها بما يتناسب مع طبيعتها وخطورتها.

غير أن هذه الجهود الأولية لم تكن كافية لتفعيل سياسة فعالة لمكافحة الجرائم المعلوماتية، إذ أسفر تعارض أحكام قانون العقوبات مع قانون الإجراءات الجزائية –لا سيما في مسائل الاختصاص النوعي والإقليمي– عن عقبات جمّة أعاقت تطبيق النصوص العقابية.

استدعى ذلك تدخّل المشرّع الجزائري بموجب القانون رقم 06–22 المؤرّخ 20 ديسمبر 2006، المعدِّل والمتمِّم لقانون الإجراءات الجزائية، الذي حدّث نصوص المواد 45 إلى 47 ليحدّد قواعد الاختصاص النوعي والمحلّي، ومواعيد إجراء التفتيش المتّصل بالجرائم المعلوماتية.

التشريع الخاص: القانون 09–04 نموذجًا متكاملاً

وفي هذا السياق، يُعدّ القانون رقم 09–04 المؤرّخ 5 أغسطس 2009 المتضمّن للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتّصال ومكافحتها، أبرز التشريعات الخاصّة بهذا المجال، إذ يُشكّل إطارًا قانونيًّا نموذجيًّا يتضمّن 19 مادّة موزّعة على ستّة فصول:

- **الفصل الأوّل** :الأحكام العامّة، بما في ذلك الأهداف (الوقاية من الجرائم المعلوماتية)، تعريفات المصطلحات المفتاحيّة، ومجال التطبيق.
- **الفصل الثاني** :مفهوم المراقبة الإلكترونيّة.
- **الفصل الثالث** :الإجراءات الخاصّة بالتفتيش الإلكترونيّ وحجز الأدلّة الرقميّة.
- **الفصل الرابع** :التزامات مقدمي خدمات الإنترنت في مساعدة السلطات التحقيقيّة.
- **الفصل الخامس** :مهام الهيئة الوطنيّة للوقاية من الجرائم المعلوماتيّة.
- **الفصل السادس** :قواعد الاختصاص القضائيّ في التعاون الدوليّ لأعمال البحث والتحقيق.

يتميّز هذا القانون بتكامل نصوصه ووضوح مبادئه في تنظيم مكافحة الجرائم المعلوماتية وتسيير التحقيقات، غير أنّ عيبَه الأبرز يكمن في الجمود التشريعيّ منذ صدوره، إذ لم يُحدّث رغم التطوّر المتسارع لتكنولوجيا المعلوماتيّة واستغلالها في الإجرام. لذا، يتعذّر على المشرّع الجزائري الاكتفاء بالنصوص الحاليّة، بل يجب تحديثها لضمان فعاليّة المكافحة[1].

التكميل التنفيذيّ: المرسوم الرئاسيّ 15-261

أمّا آخر الجهود التشريعيّة، فيتمثّل في المرسوم الرئاسيّ رقم 15-261 المؤرّخ 8 أكتوبر 2015، المتضمّن إنشاء الهيئة الوطنيّة المكلّفة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتّصال ومكافحتها. تُشرف هذه الهيئة على عمليّات البحث والتحقيق، مدعومة تقنيًّا بـ"مديريّة المراقبة الوقائية واليقظة الإلكترونية" التابعة لـ «مركز العمليّات التقنيّة"، مع ملحقات جهويّة لتذليل العقبات التحقيقيّة، يتكوّن إطارها القانونيّ من 43 مادّة، مكمّلاً لقانون 09-04، غير أنّ تأخّر صدوره (من 2009 إلى 2015) أوجد فراغًا تشريعيًّا أعاق التحقيقات طيلة تلك الفترة[2].

2-3) الهيئات المتخصصة في مكافحة الجرائم الالكترونية:

يرى جانب معتبر من الفقه أن الطابع الدولي للجريمة المعلوماتية يمثل من الناحية القانونية إحدى أخطر الإشكاليات التي تفرزها البيئة الرقمية المعاصرة، ذلك أن هذا النمط من الإجرام لا يعترف بالحدود الإقليمية للدول، بحكم طبيعته اللامادية واعتماده على شبكة إنترنت عابرة للحدود الجغرافية، بحيث يمكن أن يقع الفعل الإجرامي في إقليم دولة بينما تتحقق نتائجه في إقليم دولة

[1] قانون العقوبات الجزائري، القسم السابع مكرّر، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مرجع سابق

[2] المرسوم الرئاسيّ رقم 15-261 المؤرّخ 8 أكتوبر 2015، المتضمّن إنشاء الهيئة الوطنيّة المكلّفة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتّصال ومكافحتها، الجريدة الرسمية العدد 53، الصادرة في 2015/10/08 ، الجمهورية الجزائرية الديمقراطية الشعبية.

أخرى وتأسيساً على ذلك، أفضت الطبيعة العابرة للحدود للجريمة المعلوماتية إلى خلق تهديد معلوماتي دولي مركب، يتيح لمرتكب الجريمة تنفيذ نشاطه الإجرامي في فضاء افتراضي قد يبعد آلاف الكيلومترات عن موطن الضحية أو عن الإقليم الذي ترتبت فيه الآثار الضارة، الأمر الذي أفرز إشكالات عملية ونظرية تتعلق بتحديد الاختصاص القضائي، واحترام سيادة الدول، وآليات التعاون القضائي الدولي في مجال مكافحة هذا النمط من الإجرام، إن كل هذه التهديدات و الاعتداءات الإلكترونية، دفعت بالدول إلى استحداث هيئات ووحدات وأقسام خاصة بمكافحة الجرائم المعلوماتية، و العمل على تطويرها بشكل يسمح لها بالتحكم في هذه الظاهرة، على كافة الأصعدة بما فيها الإجرائية خصوصا وذلك على المستوى الدولي، وتعتبر الهيئات الأوروبية رائدة في هذا المجال بالنظر إلى قدرتها على التعامل مع هذه المسائل من خلال استحداث هيئات دولية وداخلية تعمل جنب الى جنب في التصدي الأول لهذا النوع من الجرائم الخطيرة[1].

2-3-1) الهيئات الدولية المتخصصة:

- **الإنتربول:** بدأت فكرة منظمة الانتربول منذ مطلع القرن العشرين، وبالتحديد في عام 1914 عندما عقد أول اجتماع دولي للقانون الجنائي، عقدته الجمعية الدولية للقانون الجنائي، في مدينة (موناكو) الفرنسية، وضم الاجتماع عددا من ضباط الشرطة والمحامين والأساتذة من أربعة عشر بلداً، وتمت مناقشة العديد من المواضيع المتعلقة بالتعاون الأمني بين الدول، ومن بينها كيفية تبادل المعلومات وتوثيقها وملاحقة المجرمين وتعقبهم وإلقاء القبض عليهم، وتسليم المجرمين،

[1] Feverier Rémy-Management de la sécurité des systèmes d'information : les collectivités territoriales face au risque numérique, Thèse de Doctorat, Ecole Doctoral de science Economique et de gestion, université Paris 02, France , Avril 2012,PP 89-92

وبحث الاجتماع أيضا إمكانية إنشاء مركز دولي لتبادل المعلومات الجنائية المتعلقة بالجريمة والمجرمين بين الدول، لكن لم يسفر على أي نتائج عملية وهذا بسبب الحرب العالمية الأولى[1].

وخلال سنة 1923 دفعت الظروف التي كانت سائدة في أوروبا بقائد شرطة فيينا (جوهان شوبير) – (Johann Shubert) إلى دعوة عقد مؤتمر ثان للشرطة مابين 3 و10 سبتمبر 1923، لذات الأسباب التي عقد من أجلها المؤتمر الأول، حيث شارك فيه حوالي 138 مندوبا يمثلون 20 دولة وإقليما، واتفق المجتمعون خلاله على إنشاء ما يسمى باللجنة الدولية للشرطة الجنائية بحيث تكون فيينا مقرا لها، والتي عملت بدورها على التنسيق بين مختلف أجهزة الشرطة لمكافحة الجريمة، و قد اقتصر على الدول الأوروبية فحسب، غير أن نشاطه توقف بسبب تأثره بالأحداث السياسية بعد نشوب الحرب العالمية الثانية، و بعد انتهائها دعا (المستر لوفاج) المفتش العام للشرطة البلجيكية إلى عقد مؤتمر دولي بإحياء اللجنة الدولية للشرطة الجنائية، ونقل مقرها إلى باريس حيث تمت تعديلات هامة في نظامها، فأنشئ فيها منصب الرئاسة، ولجنة تنفيذية، و منصب للأمين العام، و أطلق على هذه اللجنة اسم(اللجنة الدولية للشرطة الجنائية) وذلك تعبيرا عن الإرادة المتجهة إلى تسليط الضوء على استمرارية المؤسسة[2].

وضع القانون الأساسي للمنظمة الدولية للشرطة الجنائية الإنتربول من طرف الجمعية العامة في الدورة الخامسة والعشرين والمنعقدة في فيينا في الفترة ما بين 6 و13 جوان 1956، وهو بمثابة الميثاق والدستور المنظم للمنظمة، وقد راسل وزارات الخارجية للدول الأعضاء فيها لإبداء ما تراه

[1] الموقع الرسمي للأنتربول
https://www.interpol.int/ar 12/12/2024....14:15m معلومات عن الأنتربول /لمحة عامة/

[2] حليمة خراز، المنظمة الدولية للشرطة الجنائية ودورها في مكافحة الإرهاب، مقال منشور في كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم.
https://www.asjp.cerist.dz/en/downArticle/141/2/1/6805.....12/12/2024..15:00m

من تعديلات واعتراضات خلال مدة لا تتجاوز 6 أشهر وأصبح نافذا في 13 جوان 1956، حيث وصل عدد الدول فيها غلى 126 دولة في سنة 1977 وارتفع إلى 177 دولة في سنة 1998 أما حاليا فيقدر عدد الدول الأعضاء بـ 192 دولة[1]

- **الطبيعة القانونية للإنتربول:** يتحدد الشكل القانوني للمنظمة الدولية للشرطة الجنائية (الإنتربول) في ضوء التطور التاريخي الذي عرفته هذه المنظمة، إذ ثار في البداية جدل فقهي حول تبعيتها لأشخاص القانون الخاص، استناداً إلى القرار الصادر عن المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة سنة 1949، الذي منحها مركز المنظمة غير الحكومية ذات الطابع الاستشاري، مع حصر اختصاصها في المجال الجنائي دون امتداد ولايتها إلى المسائل السياسية أو العسكرية أو الدينية أو العرقية التي تظل من صميم اختصاصات الدول وحكوماتها، وقد تعزز هذا الاتجاه أيضاً بطبيعة الإطار الاتفاقي الذي تأسست في نطاقه، حيث جاء الارتباط القانوني في بادئ الأمر بين المنظمة وسلطات الشرطة في الدول الأعضاء، لا مع حكومات هذه الدول مباشرة، بما أوحى بأن المنظمة أقرب إلى تجمع مهني شرطي دولي منها إلى منظمة دولية حكومية بالمعنى الدقيق[2]، ويتجلى تمتع المنظمة الدولية للشرطة الجنائية بشخصية قانونية دولية مستقلة من خلال توافر مقومات الكيان الدائم والمعلوم، وهو ما كرسته إعادة تسميتها من "اللجنة الدولية للشرطة الجنائية" إلى "المنظمة الدولية للشرطة الجنائية"، بما يضعها في مصاف المنظمات الدولية الحكومية الأخرى من حيث البنية والصفة القانونية، ويُستفاد من ذلك أن لهذه

[1] اليوم في الإنتربول، لديها عضوية عالمية تضم 192 بلدا، ويحتفظ كل بلد بمكتب مركزي وطني، يعمل به موظفون وطنيون لإنفاذ القوانين وهو يشكل حلقة الوصل مع الشبكة العالمية للإنتربول، مما يمكن البلدان الأعضاء من العمل معا على إجراء تحقيقات عبر الحدود الوطنية، وتشارك المكاتب المركزية الوطنية بصورة متزايدة في تشكيل اتجاه المنظمة...القانون الأساسي للمنظمة العالمية الدولية الجنائية (الإنتربول)، وثيقة رقم [I/CONS/GA/1956 (2017)]

[2] حليمة خراز، مرجع سابق، ص 153.

المنظمة إرادة ذاتية متميزة عن إرادات الدول الأعضاء، تُمارَس في ميدان العلاقات الدولية، من خلال إبرامها لاتفاقات تعاون مستقلة، من بينها اتفاق التعاون المبرم مع منظمة الأمم المتحدة بشأن دراسة مشكلات الجريمة وتعزيز التعاون في مكافحتها، والذي صدر بشأنه القرار رقم 4961 بتاريخ 8 مارس 1971، متضمناً الإقرار الصريح بكون المنظمة الدولية للشرطة الجنائية منظمة دولية حكومية، ويُضاف إلى ذلك أن الفقه يستند في تدعيم هذا التكييف إلى ما استقر عليه القضاء الدولي، إذ أقرت محكمة العدل الدولية في رأيها الاستشاري الصادر في 11 أبريل 1949 مبدأ تمتع المنظمات الدولية الحكومية بالشخصية القانونية الدولية اللازمة لتحقيق أهدافها المنوطة بها، بما يعني قدرتها على اكتساب الحقوق وتحمل الالتزامات على الصعيد الدولي، وهو ما ينطبق على الإنتربول في ضوء ما سبق بيانه من عناصر تنظيمية ووظيفية[1].

كما أنّ لها بناء هيكلها وتنظيمها يتكون من جمعية عامة ولجنة تنفيذية، والكاتبة المركزية الوطنية، ومستشارين ولجنة الرقابة على المحفوظات[2]، كذلك الأمانة العامة والتي يرأسها الأمين العام للمنظمة والتي تنقسم بدورها إلى إدارات تابعة لها والتي تتمثل في قسم الإدارة العامة وقسم التعاون الشرطي وقسم البحوث والدراسات وقسم المجلة الدولية للشرطة الجنائية[3].

- **عمل الإنتربول في مجال مكافحة الجرائم الالكترونية:** تباشر المنظمة الدولية للشرطة الجنائية (الإنتربول) وظيفتين رئيستين في مجال مكافحة الجريمة ذات البعد العابر للحدود، تتمثل أولاهما

[1] القانون الأساسي للمنظمة العالمية الدولية الجنائية (الإنتربول)، المادة الأولى وما يليها
انظر كذلك: دليل الممارسات، في تطبيق المادة 3 من القانون الأساسي للإنتربول، في سياق معاملة المعلومات عبر قنوات الإنتربول، الطبعة الثانية، فبراير2013.... 2024/12/12... 15.20 د article 3-arabic-february 2013vb CD.pdf
[2] المادة 5، القانون الأساسي للمنظمة العالمية الدولية الجنائية (الأنتربول)، مرجع سابق
[3] المواد 25-27-28-30، نفس المرجع

في تجميع وحفظ وتحليل مختلف البيانات والمعلومات المتعلقة بالجريمة والمجرمين، وذلك عن طريق ما تنشئه الدول الأعضاء من مكاتب مركزية وطنية للشرطة الجنائية الدولية داخل إقليم كل دولة، بما يتيح تيسير تبادل المعلومات وتدعيم جهود التحري والتحقيق، أما الوظيفة الثانية فتتجسد في تيسير التعاون الدولي في ملاحقة المجرمين الفارين والمطلوبين للعدالة، من خلال دعم إجراءات تعقبهم وإلقاء القبض عليهم وتنسيق تسليمهم إلى الدول الطالبة، وفقاً للآليات القانونية والاتفاقيات الثنائية والمتعددة الأطراف ذات الصلة، وبذلك تتخصص المنظمة في مكافحة الجرائم ذات الطابع الدولي، وعلى وجه الخصوص الجرائم الخطيرة مثل جرائم الاستغلال الجنسي للأطفال عبر شبكة الإنترنت، وفي هذا السياق برزت عدة دعوات صريحة لتعزيز التعاون الدولي في مواجهة الإجرام المعلوماتي، إذ دعت الأمينة العامة للمنظمة آنذاك " رايموند كندال" في مؤتمر جرائم الإنترنت المنعقد في لندن بتاريخ 09 أكتوبر 2000، إلى ضرورة إقامة إطار فعال للتعاون الدولي لمكافحة هذا النمط المستحدث من الإجرام، بالنظر إلى خطورته وتعقيد آلياته التقنية، وقد أكد هذا التوجه المدير التنفيذي للخدمات الشرطية في الإنتربول " ليبوتان" خلال المؤتمر الدولي السادس بشأن الجرائم المعلوماتية المنعقد بالقاهرة في أفريل 2005، مشدداً على أهمية التنسيق العملياتي بين أجهزة إنفاذ القانون عبر الدول.

كما ذهب المدير العام لمركز بحوث الشرطة الأسترالية إلى الدعوة لاعتماد منهجية تحقيق متزامنة على الصعيد العالمي في الجرائم المعلوماتية، بما يضمن عدم إفلات مرتكبي هذه الجرائم

من الملاحقة بفعل تشتت الأدلة وتوزعها بين عدة ولايات قضائية، ويعكس في الوقت ذاته الوعي المتزايد بالطابع الكوني لهذا النوع من الإجرام[1].

وتظهر الجهود العملية للمنظمة الدولية للشرطة الجنائية (الإنتربول) في مكافحة الإجرام المعلوماتي من خلال مبادرات مؤسسية متخصصة، من أبرزها تنظيمها في شهر فيفري سنة 2005 للمؤتمر الثاني للتنسيق بشأن جرائم الاحتيال المعلوماتي، وذلك على خلفية قضية احتيال إلكتروني طال ضحايا بلغ عددهم حوالي 2000 شخص من 60 دولة مختلفة، قُدّرت خسائرهم المالية بحوالي 166 مليون أورو، وقد تُوّجت هذه الجهود بتوقيف المتهمين الرئيسيين في هذه القضية في إسبانيا خلال شهر ديسمبر 2004، بناءً على طلب المساعدة القضائية الدولية الذي تقدم به النائب العام الألماني عبر قنوات الإنتربول، بما يعكس الدور المحوري للمنظمة في تفعيل التعاون العملياتي بين سلطات الادعاء وأجهزة إنفاذ القانون في الدول الأعضاء.

واستمراراً لهذا المسار، وسعياً إلى مأسسة مكافحة الجرائم المعلوماتية وتدعيم القدرات الوطنية في هذا المجال، بادر الإنتربول في شهر سبتمبر 2005 إلى تنظيم المؤتمر الدولي الأول لتكوين المحققين في الجرائم المعلوماتية بمدينة ليون الفرنسية، حيث شاركت في أعماله ثلاثون دولة أرسلت خبراءها ومتخصصيها للاستفادة من برامج التكوين والتأهيل التي طُرحت خلاله، والذي يُعد هذا المؤتمر خطوة متقدمة في اتجاه إرساء مقاربة دولية منسقة للتحقيق في الجرائم المعلوماتية، ترتكز على تكوين كفاءات بشرية متخصصة قادرة على التعامل مع التعقيدات التقنية

[1] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي- الإسكندرية، 2007، ص ص 151-152

لهذا النوع من الإجرام، وعلى توحيد الخطط الإجرائية والتقنية بين مختلف الدول بما يحد من الثغرات التي يمكن أن يستغلها المجرمون في الفضاء السيبراني[1]

- **وسائل الإنتربول في مكافحة الجرائم الالكترونية:** تُعَدُّ المنظمة الدولية للشرطة الجنائية (الإنتربول) أداةً محورية في مكافحة الجرائم المعلوماتية من خلال وسائل متكاملة ترتكز على التعاون الدولي والدعم التقني، ويمكن إجمالها على النحو الآتي:

قواعد البيانات والأنظمة المعلوماتية: تشغل الإنتربول قواعد بيانات متخصصة مثل (ICSE) قاعدة بيانات الجرائم السيبرانية و(FIDINT) الاستخبارات المالية الدولية، بالإضافة إلى مركز (Cyber Fusion Centre) الذي يتيح تبادل المؤشرات الرقمية (IOCs) بين الدول الأعضاء في الوقت الفعلي، مما يدعم عمليات التحقيق والاستجابة للهجمات السيبرانية[2]

في شبكات الاتصال الآمنة: تعتمد على نظام I-24/7 الآمن لتبادل المعلومات بين المكاتب المركزية الوطنية (NCBs) ، إلى جانب منصات Cybercrime Collaboration Services المخصصة للمحققين في الجرائم الرقمية، مما يضمن السرعة والسرية في التواصل العملياتي[3]

---

[1] Mohamed Chawki, Combattre la cybercriminalité, Edition de saint Amans, Paris, France,Mai 2009, PP 343-344

[2] Interpol. "Cybercrime." Accessed February 23, 2024 https://www.interpol.int/Crimes/Cybercrime.
See : Interpol. "Our 19 databases." Accessed February 23, 2024. https://www.interpol.int/How-we-work/Databases/Our-databases... 13/12/2024…10.30m

[3] Interpol. "INTERPOL | The International Criminal Police Organization." Accessed February 23, 2024. https://www.interpol.int. interpol
Interpol. "Cybercrime Collaboration Services." Accessed February 23, 2024. https://www.interpol.int/Crimes/Cybercrime/Cybercrime-Collaboration-Services... 13/12/2024…10.50m

في خلق عمليات مشتركة ودعم فني: تنسق عمليات دولية مشتركة مثل **Operation HAECHI** و**Operation First Light**، وتقدم دعماً فنياً ميدانياً يشمل تحليل الأدلة الرقمية، تتبع العملات المشفرة، وفك تشفير الاتصالات المحمية، كما في قضايا الاحتيال عبر الإنترنت والجرائم المالية[1]

اعمال برامج التكوين وبناء قدرات بشرية: وذلك في تنظيم دورات تدريبية متقدمة في Virtual Academy وورش عمل حول التحقيق الجنائي الرقمي، مع إصدار دليل Cybercrime Manual لتوحيد الممارسات التحقيقية بين الدول، مما يعزز الكفاءة الوطنية في مواجهة الإجرام السيبراني[2].

بناء شراكات الاستراتيجية مع المؤسسات التكنلوجية: وهذا في خلق تعاون مع شركات التكنولوجيا الكبرى في إطار Private Sector Innovation Programme، ومع المنظمات الدولية مثل Europolو UNODC، لتطوير معايير مشتركة وتبادل الاستخبارات حول التهديدات الناشئة كالـ ransomware والاستغلال الجنسي للأطفال عبر الإنترنت[3].

[1] Interpol. "Cybercrime – our response." Accessed February 23,2024. https://www.interpol.int/Crimes/Cybercrime/Cybercrime-our-response.interpol
See : Interpol. "Cybercrime – our response (English)." Accessed February 23,2024. https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-our-response. 13/12/2024…11.20m
[2] Interpol. "CYBERCRIME." Accessed February 23,2024 https://www.interpol.int/content/download/5267/file/Cybercrime.pdf. 13/12/2024…11.45m
[3] Interpol's Statement - The United Nations Convention. Accessed February 23,2024…https://hanoiconvention.org/statement/interpols-statement/.hanoiconvention
See : Interpol. "Public-private partnerships." Accessed February 23,2024 https://www.interpol.int/Crimes/Cybercrime/Partners. 13/12/2024…12.00 m

حيث من شأنها أن تتيح هذه الوسائل المتعددة للإنتربول أداء دور تنسيقي فعال في مواجهة الطبيعة العابرة للحدود للجرائم المعلوماتية، وتجمع بين الدعم التقني والعملياتي والقانوني لتدعيم الجهود الوطنية.

- **منظمة اليوروبول:** يعد يوروبول (Europol)، أو وكالة الشرطة الأوروبية، كياناً مؤسسياً أوروبيا حكوميا يهدف إلى تعزيز الأمن الداخلي للاتحاد الأوروبي من خلال تقديم الدعم التشغيلي والتحليلي لأجهزة إنفاذ القانون في الدول الأعضاء، في مواجهة الجرائم المنظمة عابرة الحدود والإرهاب، وفقاً لما نص عليه البروتوكول الإضافي إلى الاتفاقية الأوروبية بشأن مكافحة الجريمة المنظمة الدولية (1995) وتالياً قرار المجلس JHA 371/2009/الذي أسس الوكالة بصفتها بشكل نهائي.

ويقع المقر الرئيسي ليوروبول في مدينة لاهاي بهولندا، ويضم أكثر من 900 موظف متخصص، من بينهم 137 ضابط شرطة وصل (Police Attachés) منتدَبين من الدول الأعضاء والشريكة، أين يعين المدير التنفيذي من قبل مجلس الاتحاد الأوروبي بوصفه الممثل القانوني للوكالة، بينما يضطلع مجلس الإدارة – المكوَّن من ممثل رفيع المستوى عن كل دولة عضو بالإضافة إلى ممثل عن المفوضية الأوروبية – بإعطاء التوجيهات الاستراتيجية والإشراف على تنفيذ المهام، مع مراعاة مبدأ التناسب والشفافية في اتخاذ القرارات.

كما أنه لا تتمتع أجهزة يوروبول بصلاحيات تنفيذية مباشرة لإلقاء القبض أو الاعتقال في أي إقليم، إذ يظل ذلك من اختصاص السلطات الوطنية، لكنها تؤدي دوراً مسانداً حاسماً يشمل جمع المعلومات الاستخباراتية، تحليلها الجنائي المتقدم، توزيعها عبر قنوات آمنة، وتنسيق

المهمات المشتركة (Joint Investigation Teams – JITs) بين الدول الأعضاء، كما تقدم خدمات استباقية للوقاية من الجرائم، والتحقيق فيها، وتتبع مرتكبيها، مع الاستفادة من خبرات موظفيها المتنوعة القادمين من عدة أجهزة.

وتعمل يوروبول بشراكة وثيقة مع أجهزة الأمن في دول الاتحاد الأوروبي (27 دولة عضو)، بالإضافة إلى دول شريكة خارج الاتحاد مثل النرويج، أستراليا، كندا، والولايات المتحدة الأمريكية، مما يعزز فعالية التعاون عبر الحدود في قضايا الجريمة المنظمة الدولية، وتُشَكِّل هذه المقاربة المتكاملة نموذجاً للتنسيق الأوروبي في مواجهة التهديدات الأمنية المعاصرة، مع الحفاظ على احترام الاختصاصات الوطنية وسيادة القوانين الداخلية لكل دولة[1].

وقد شهد الأوروبول سنة 2008 طفرة نوعية في وسائل عمله وصلاحياته فبتاريخ 24 أكتوبر 2008 تقرر بلكسومبورغ إنشاء قاعدة بيانات أوروبية مشتركة بميزانية أولية قدرها ثلاثمائة ألف يوروا تخضع لتسيير منظمة الأوروبول، وتضمن التنسيق بين عمل جهات الشرطة للدول الأعضاء من خلال إحصاء وجمع كافة القضايا الإجرامية التي لها علاقة بالمعلوماتية وذلك لأجل التنسيق بين عمل الجهات الأمنية[2].

وتطبيقاً لهذا الإطار، فقد اعتمد مجلس الاتحاد الأوروبي، في جلسته المنعقدة بمدينة بروكسل (بلجيكا) بتاريخ 22 نوفمبر 2000، في سياق مناقشة ملف الاتصالات الإلكترونية

---

[1] تمت الموافقة على تأسيس اليوروبول في معاهدة ماسترخت عام1992، وباشرت الوكالة بالقيام بعمليات محدودة بتاريخ 3 يناير عام1994 ، وفي عام 1998 تمت مراجعة طبيعة عمل اليوروبول من قبل دول الاتحاد الأوربي وبدأت الوكالة بالقيام بمهامها كاملة بتاريخ 1 يوليو سنة 1999

https://www.europol.europa.eu/fr/about-europol.... 13/12/2024...14.00 m

[2] Myriam Quéméner – Joël Ferry– Cybercriminalité Défi mondial– op.cit– p 238.

(Paquet Télécom)، مبدأ توسيع اختصاصات يوروبول لتشمل ملاحقة ومتابعة مرتكبي الجرائم المعلوماتية، وذلك من خلال إضفاء صلاحية تنظيميّة عليها لتنسيق الدوريات الإلكترونية عبر الفضاء السيبراني[1].

وفي هذا الصدد، يُستشف من القرار الإطاري للمجلس JHA 383/2000/بشأن مكافحة الجريمة المنظمة أهمية تجميع المعلومات الاستخباراتية المتعلقة بالجرائم الرقمية من مصادر متعددة، بما في ذلك البيانات التي يوفرها مزودو خدمات الإنترنت (ISPs) وأجهزة الشرطة الوطنية في الدول الأعضاء، وفقاً لمبادئ التناسب والضرورة في معالجة البيانات الشخصية بما يتوافق مع توجيه حماية البيانات CE 46/95/وقرار إطاري JHA. 383/2000/ومن الناحية القانونية، يُعد هذا التوجه خطوة تأسيسية نحو إقامة نظام تنسيقي أوروبي موحِّد لمواجهة التهديدات المعلوماتية العابرة للحدود، مع التمسُّك بمبدأ عدم امتداد صلاحيات يوروبول إلى التدخُّل التنفيذي المباشر في الإقليم الوطني للدول الأعضاء، بل الاقتصار على الدعم التحليلي والتشغيلي[2].

- منظمة اليورو جيست:

يُعد الأوروجست (Eurojust) أحد أهم الأجهزة القضائية التابعة للاتحاد الأوروبي، إذ أُنشئ بموجب قرار مجلس الاتحاد الأوروبي المؤرخ في 22 فبراير 2002، في إطار مسعى مؤسسي يروم تدعيم الفضاء الأوروبي القائم على الأمن والحرية والعدالة[3]، ويعكس تأسيس هذه الهيئة

[1] Céline Renard Castétes- op.cit-p 564.

[2] Council Framework Decision 2000/383/JHA of 29 May 2000 on the approximation of the laws and regulations of the Member States in the field of combating organized crime. Official Journal L 139, 24/05/2000, PP 1-4.

[3] Council of the European Union, Council Decision of 28 February 2002 setting up Eurojust, Official Journal of the European Communities, L 63/1, 2002, p. 3.

الإرادة السياسية للدول الأعضاء في مواجهة تحديات الجريمة المنظمة، ولا سيما الجرائم ذات البعد العابر للحدود على غرار الجرائم المعلوماتية، التي تفرض بطبيعتها تعاونًا قضائيًا يتجاوز الحدود الوطنية للأنظمة القانونية[1]

ويتمثل الدور الجوهري للأوروجست في تعزيز التنسيق القضائي بين السلطات الوطنية المختصة، من خلال تجميع وتبادل المعلومات ذات الصلة بالقضايا الجنائية، وتنظيم الدعم القانوني والفني لجهات الادعاء العام عبر الاتحاد الأوروبي[2]، كما تُسهم الهيئة في تحسين فعالية التحقيقات والملاحقات القضائية من خلال وضع آليات مؤسسية لتجاوز التعارض القانوني في الاختصاص أو النزاع حول السيادة القضائية بين الدول الأعضاء[3].

وفي مجال مكافحة الجريمة المعلوماتية، يضطلع الأوروجست بوظيفة محورية تتمثل في تهيئة مناخ التعاون بين الأجهزة القضائية والشرطية المختصة، من خلال توفير التحليلات القانونية والاستراتيجية التي تمكّن من تحديد أنماط السلوك الإجرامي الإلكتروني، وتنسيق الجهود بين مختلف السلطات الوطنية المعنية[4]، كما يشكل الأوروجست حلقة وصل أساسية مع اليوروبول (Europol)، الذي يتولى الجانب التحقيقي العملياتي، بينما يتولى الأوروجست الجانب القضائي التحليلي الداعم لهذه التحقيقات[5].

أما من حيث بنيته التنظيمية، فيتألف الأوروجست من نواب عامين، ومستشارين قضائيين، وضباط شرطة قضائية من الدول الأعضاء، يتم انتدابهم وفق مقتضيات القوانين الوطنية لكل

[1] Mitsilegas, V., *EU Criminal Law after Lisbon*, Hart Publishing, 2016, p. 112.
[2] European Commission, *Eurojust Annual Report 2019*, Luxembourg, 2020, p. 21
[3] Peers, S., *EU Justice and Home Affairs Law*, Oxford University Press, 2021, p. 345
[4] Eurojust, *Report on Cybercrime Cooperation*, The Hague, 2019, p. 9
[5] Europol & Eurojust, *Joint Report on Cooperation Mechanisms*, 2020, p. 15

دولة، بما يضمن الجمع بين المعرفة التقنية بالأنظمة القانونية الوطنية والخبرة العملية في مجال التعاون القضائي الأوروبي[1]، وبهذا يشكل الأوروجست نموذجًا متقدمًا للتكامل القضائي في الاتحاد الأوروبي، يعكس تطور مفهوم السيادة القضائية المشتركة في مواجهة الجريمة المعلوماتية العابرة للحدود[2].

ويحكم عمل الأروجست في مجال متابعة الجرائم الكترونية ثلاث (03) أهداف هي:

1- تطوير وتحسين وسائل التنسيق في مجال المتابعة وذلك بين السلطات المختصة للدول الأعضاء

2- تسهيل التعاون بين الجهات القضائية في مجال المتابعات من خلال تنفيذ أوامر المساعدة القضائية الدولية، والاستجابة لطلبات الإبعاد.

3- دعم السلطات الوطنية من أجل ضمان فعالية المتابعة الجزائية[3].

يتّضح من خلالها أنّ الأجهزة الدولية المكلّفة بإجراءات البحث والتحقيق في الجرائم المعلوماتية تشكّل في معظمها امتدادًا لمبادرات أوروبية متقدّمة في مجال بناء الأطر المؤسسية للتعاون القضائي والأمني في الفضاء الرقمي، وهو ما تجسّده بوجه خاص آليات مجلس أوروبا واتفاقية بودابست بشأن الجريمة المعلوماتية وما انبثق عنها من هياكل فنية متخصّصة، غير أنّ نشاط هذه الآليات يتركّز أساسًا ضمن المجال الأوروبي، مع امتدادات باتجاه أمريكا الشمالية

[1] Fletcher, M., *Judicial Cooperation in the EU: Principles and Practice*, Routledge, 2018, p. 78.
[2] Chalmers, D., Davies, G., & Monti, G., *European Union Law: Text and Materials*, Cambridge University Press, 2020, p. 589.
[3] Myriam Quéméner – Joël Ferry– Cybercriminalité Défi mondial - op.cit- p 239.

وبعض مناطق شرق آسيا، في حين يظل التنسيق المؤسسي المماثل في المحيطين العربي والإفريقي محدودا من حيث النطاق والفعالية، رغم ما تبذله بعض المنظمات الدولية والإقليمية من جهود لبناء القدرات في هذا المجال، وتبعًا لذلك، يبرز من منظور السياسة الجنائية الدولية والحكامة الأمنية في الفضاء السيبراني، مطلبُ استحداث أو تعزيز أطر إقليمية عربية وإفريقية متخصّصة في مكافحة الإجرام المعلوماتي، بما يضمن توحيد المقاربات التشريعية، وتدعيم قدرات سلطات التحقيق والمتابعة، وتيسير آليات المساعدة القضائية المتبادلة على المستوى الإقليمي.

2-3-2) الهيئات الوطنية في التشريعات المقارنة:

أسست أغلب الدول سواء المتقدمة تكنلوجيا أو الدول النامية منها خصوصا وحدات خاصة بمكافحة الجرائم المعلوماتية، كما تتولى في نفس الوقت مسائل البحث والتحقيق بشأنها نذكر منها ما هو عليه الحال في:

- التشريع الجزائري:

صدر في العدد الأخير من الجريدة الرسمية المرسوم الرئاسي المؤرخ في 06 جويلية 2019 الذي يحدّد تشكيلة "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها" وتنظيمها وكيفيات سيرها، بصياغة قانونية على النحو الآتي:

تنشأ هيئة وطنية تسمى "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها"، تتمتع بالشخصية المعنوية والاستقلالية المالية، وتعدّ مؤسسة عمومية ذات طابع إداري توضع تحت سلطة وزير الدفاع الوطني. يحدد مقر الهيئة بمدينة الجزائر، ويمكن نقله إلى أي مكان آخر من التراب الوطني بقرار من وزير الدفاع الوطني.

تتكوّن الهيئة من مجلس توجيه ومديرية عامة. يرأس مجلس التوجيه وزير الدفاع الوطني أو ممثله، ويضم في عضويته ممثلين عن القطاعات المكلفة بالداخلية والجماعات المحلية، والعدل، والاتصالات السلكية واللاسلكية والتكنولوجيات والرقمنة، وكل مؤسسة أو هيئة وطنية أخرى معنية يحددها التنظيم، يتولى مجلس التوجيه بوجه خاص:

1. التداول في الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، كما هي محددة في هذا المرسوم والنصوص ذات الصلة.
2. التداول في مسائل تطوير الهيئة وتعزيز وسائلها، وكذا في ميكانيزمات التعاون مع المؤسسات والهيئات الوطنية المختصة؛
3. التقييم الدوري لحالة التهديد في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. قصد تحديد مضامين عمليات المراقبة الواجب القيام بها، والأهداف المراد بلوغها بدقة.
4. إعداد نظامه الداخلي والمصادقة عليه.
5. دراسة التقرير السنوي لنشاطات الهيئة والمصادقة عليه.

يجتمع مجلس التوجيه في دورة عادية مرتين (2) في السنة، بناء على استدعاء من رئيسه، ويمكنه أن يجتمع في دورة غير عادية كلما اقتضت الضرورة ذلك، بناء على استدعاء من رئيسه أو بطلب من أحد أعضائه أو من المدير العام للهيئة.

تتولى المديرية العامة قيادة الهيئة والتسيير اليومي لنشاطاتها، وتمارس على وجه الخصوص المهام الآتية:

1. السهر على حسن سير مختلف هياكل الهيئة وضمان انسجام أعمالها.

2. إعداد مشروع ميزانية الهيئة وتقديمه وفقاً للتشريع والتنظيم المعمول بهما.

3. إعداد برنامج عمل الهيئة وتنفيذه بعد المصادقة عليه من الجهات المختصة.

4. تنظيم وتنسيق تبادل المعلومات مع الهيئات النظيرة الأجنبية، بغرض تجميع وتحليل المعطيات الضرورية لتحديد مكان مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرّف عليهم

5. السهر على تنفيذ القرارات والتوجيهات الصادرة عن مجلس التوجيه.

يعدّ المدير العام الآمر بالصرف لميزانية الهيئة، ويُعيَّن وفقاً للتنظيم المعمول به في وزارة الدفاع الوطني، يعيَّن مستخدمو الهيئة وفق الأنظمة المطبَّقة في وزارة الدفاع الوطني، ويُعاد إدماج القضاة والمستخدمين التابعين للقطاعات الوزارية الأخرى العاملين في الهيئة في هياكلهم الأصلية عند إنهاء مهامهم بها، طبقاً للتشريع والتنظيم المعمول بهما.

تضم المديرية العامة على الخصوص:

1. **مديرية تقنية:** تكلف بمهام المراقبة الوقائية للاتصالات الإلكترونية في إطار الوقاية من الأفعال الإرهابية والتخريبية والاعتداءات التي تستهدف أمن الدولة، وتقديم المساعدة التقنية للسلطات القضائية ولمصالح الشرطة القضائية، بما في ذلك في مجال الخبرة القضائية، في إطار مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم التي تستوجب اللجوء إلى أساليب التحري الخاصة المسندة للهيئة.

2. **مديرية الإدارة والوسائل:** تكلف بتسيير الموارد البشرية والوسائل المالية الخاصة بالهيئة، وضمان الإسناد التمويني والتقني، وصيانة العتاد والوسائل والمنشآت القاعدية، وإعداد احتياجات الهيئة في إطار تحضير تقديرات الميزانية.

تحدد الأحكام المالية المتعلقة بالهيئة، لا سيما ما يخص مواردها ونفقاتها، على النحو الآتي:

- تتكوّن موارد الهيئة من الإعانات التي تمنحها الدولة، وعائدات النشاطات المرتبطة بموضوعها، وكل الموارد الأخرى التي يجيزها التشريع والتنظيم المعمول بهما.
- تشمل نفقات الهيئة نفقات التسيير ونفقات التجهيز المرتبطة بتنفيذ مهامها، وتُصرف وفقاً لأحكام قانون المالية والنصوص التطبيقية ذات الصلة[1].

- التشريع الفرنسي:

تتميّز فرنسا بإرساء بنية مؤسساتية متخصّصة في مكافحة الجرائم المعلوماتية، في مقدمتها مركز مكافحة الجرائم الرقمية Centre de lutte contre les criminalités numériques (C3N)، باعتباره مصلحة تابعة للدرك الوطني ذات اختصاص قضائي وطني، يضطلع بتجميع مختلف الوحدات التابعة للقطب القضائي للدرك الوطني التي تعالج بصورة مباشرة قضايا الجريمة المرتبطة بالفضاء الرقمي وتحليلها، ويتولى في الوقت ذاته قيادة وتنسيق نشاط شبكة المحققين الرقميين عبر التراب الوطني، ولا سيما داخل شبكة "Cybergend" المكوّنة من آلاف المحققين المتخصصين، مع اضطلاعه بمهمات التحقيق في قضايا الجرائم السيبرانية واسعة

[1] المرسوم الرئاسي رقم 19-172 المؤرخ في 06 شوال عام 1440 الموافق لـ 09 يونيو عام 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، الجريدة الرسمية، الجمهورية الجزائرية الديمقراطية الشعبية، العدد 37، لسنة 2019

النطاق، وتوفير الخبرة التقنية والدعم العملياتي لوحدات الدرك الإقليمية، إلى جانب دوره في رصد الظواهر الإجرامية المستجدّة عبر الإنترنت وتحليل أنماطها تمهيدا لصياغة استجابة عملياتية ملائمة[1].

وعلى مستوى أعلى من التنسيق، أنشِئت الوحدة الوطنية للجرائم السيبرانية Unité nationale cyber بموجب قرار وزاري، باعتبارها وحدة وطنية متخصّصة تابعة للدرك الوطني، تتولّى قيادة، وتسيير، وتنشيط جهاز مكافحة التهديدات السيبرانية على مستوى الدرك، وتمارس اختصاصاً وطنياً في مجال الوقاية من الأشكال المتخصّصة والمنظمة وعابرة الحدود من الجرائم السيبرانية وقمعها، كما تختص كذلك بمكافحة استخدام شبكات الاتصالات الإلكترونية والتكنولوجيات الرقمية لتسهيل ارتكاب الجرائم، مع سهرها على تنسيق عمل مختلف الهوائيات الجهوية والمراكز التابعة لمركز مكافحة الجرائم الرقمية C3N، وتوجيه أنشطة التحسيس والوقاية لصالح مختلف فئات المستعملين، فضلا عن دورها في تجميع المعلومات الإستراتيجية المتعلقة بحالة التهديد في الفضاء السيبراني لفائدة السلطات المختصة بوضع وتنفيذ السياسة الوطنية في مجال مكافحة الجريمة السيبرانية[2].

[1] Sophie Bernard, Gendarmerie nationale, « Centre de lutte contre les criminalités numériques (C3N) », Pôle judiciaire de la gendarmerie nationale, Publié le 28 janvier 2020.
https://www.gendarmerie.interieur.gouv.fr/gendinfo/actualites/2020/la-montee-en-puissance-de-l-investigation-cyber-en-gendarmerie.
Voir : Philippe Guisnel, « Organisation de l'État français en gestion de crise cybernétique », Cahiers de la sécurité et de la justice, no 54, 2021.

[2] Arrêté du 23 novembre 2023 relatif à la création de l'unité nationale cyber, Journal officiel de la République française, France ,2023.
Voir : Gendarmerie nationale, « Unité nationale cyber (UNC) », *UNPJ – Gendarmerie nationale*, https://www.gendarmerie.interieur.gouv.fr/unpj/l-unpj/unite-nationale-cyber

- الولايات المتحدة الأمريكية:

يعد مكتب التحقيقات الفيدرالي FBI الجهة الرئيسية الفيدرالية المسؤولة عن التحقيق والملاحقة القضائية في الجرائم السيبرانية، بموجب اختصاصاته الواسعة المنصوص عليها في القانونين الفيدراليين الأساسيين، قانون مكافحة الاحتيال الحاسوبي والإساءة Computer Fraud) and Abuse Act – CFAA، 18 U.S.C. § 1030) وقانون الجرائم الإلكترونية والحماية Electronic Communications Privacy Act – ECPA)، 18–2510 §§ U.S.C. (2522، حيث تشكّل شعبة الجرائم السيبرانية Cyber Division)أو CyD) الوحدة التنفيذية الرئيسية لهذه المهمّات منذ تأسيسها في عام 2002، وتتولّى قيادة الجهود الوطنية المنسَّقة للتحقيق والملاحقة في جرائم الإنترنت، بما في ذلك الإرهاب الإلكتروني، التجسُّس السيبراني، الاختراقات الحاسوبية، الاحتيال الإلكتروني الكبير، سرقة الهوية، سرقة الملكية الفكرية، واستغلال الأطفال جنسيّاً عبر الإنترنت، مع التركيز على التهديدات الأمنية الوطنية والاقتصادية الناجمة عن الخصوم الأجانب أو الجماعات الإجرامية المنظّمة، حيث أدَّت تحقيقاتها منذ 2008 إلى أكثر من 1600 إدانة، 78.6 مليون دولار تعويضات، و4.6 مليار دولار استردادات مالية[1].

كما تُنشَأ فرق الجرائم السيبرانية الميدانية (Cyber Squads) في كلٍّ من المكاتب الـ56 التابعة لـ FBIعبر الولايات المتحدة، وتضمُّ عملاء تحقيق ميدانيِّين (agents) ومحلّلين تقنيِّين (analysts) مدرَّبين خصيصاً على التحقيقات السيبرانية، حيث تُعَالِجُ هذه الفرق التهديدات المحلِّية والإقليميَّة مثل الاختراقات الحاسوبية، سرقة الملكية الفكرية، استغلال الأطفال عبر

[1] Federal Bureau of Investigation. "FBI Cyber Division." https://www.fbi.gov/investigate/cyber. Accessed March 22, 2025 …13.30m

الإنترنت، والاحتيال الإلكتروني، وتُشَكِّلُ الركيزة العمليَّة لشعبة CyD من خلال فرق الاستجابة السريعة (Cyber Action Teams) التي تُنْشَرُ دوليَّاً لدعم التحقيقات عابرة الحدود، وتعمل جميع هذه الفرق ضمن الإطار التنسيقيَّ الوطنيَّ لـالمركز الوطنيَّ المشترك للتحقيق في الجرائم السيبرانيَّة (National Cyber Investigative Joint Task Force – NCIJTF)، الذي أُسِّسَ في 2008 كمركزٍ مُتعدَّدِ الوكالات يضمُّ أكثر من 30 جهة حكوميَّة أمريكيَّة مثلCIA ، وزارة الدفاعDOD ، وزارة الأمن الداخليَّDHS ، ووكالة الأمن القوميَّ NSA، بالإضافة إلى شركاء دوليِّين، لمشاركة المعلومات الاستخباراتيَّة، تنسيق التحقيقات في التهديدات الكبرى، وتطوير استراتيجيَّات مشتركة لمكافحة الخصوم السيبرانيِّين، مما يُعَزِّزُ الاستجابة المتكاملة للتهديدات الوطنيَّة والدوليَّة[1].

ويحدد أولويات شعبة CyD بترتيب هرمي يعطي الأولوية الأولى للاختراقات السيبرانية ذات الطابع الأمني الوطني(national security cyber intrusions) ، تليها استغلال الأطفال جنسياً، حقوق الملكية الفكرية، والاحتيال عبر الإنترنت، مع الاعتماد على مركز شكاوى الجرائم الإلكترونية (Internet Crime Complaint Center – IC3) كمصدر رئيسي للقضايا، حيث تلقى أكثر من 75,000 شكوى في 2002 وحدها، وقد ساهمت في تفكيك شبكات إجرامية كبرى[2].

[1] https://www.american.edu/spa/life-on-an-fbi-cyber-squad.cfm. Accessed March 22, 2025 …14.20m
[2] FBI Cyber Division: Cyber Crime stories, Opcit.

- في الامرات العربية المتحدة:

تشكِّل إدارة مكافحة الجرائم الإلكترونية (Cyber Crime Unit) الوحدة المتخصِّصة الرئيسية في شرطة دبي لمكافحة الجرائم المعلوماتية والإلكترونية، وتضمّ إدارة الأدلة الرقمية Digital Forensics Department التي تطوَّرت من وحدة صغيرة مُؤَسَّسَةٍ قبل نحو 24 عاماً (حوالي 2001) إلى قسم تقليديٍّ عالي التقدُّم يضم 7 وحدات متخصِّصة و70 خبيراً، ويتعامل مع 80–100 قضيَّة شهريَّاً، مع نظام فحص يشمل استرداد البيانات، فكّ الشِّفْرَة، وتحليلها باستخدام تقنيَّات متقدِّمة مثل تحليل الصَّوْتِ وكشف العواطف من الصُّوَرِ الحيَّةِ(deepfakes) ، وتحقيقات دوليَّة مُنْسَقَةٌ مع وكالات أمن أجنبيَّة لتعقُّبِ المجرمين المقيمين خارج الإمارات، وقد حصلت إدارة الأدلة على جائزة الجمعيَّة الدَّوْلِيَّةِ لِرُؤَسَاءِ الشُّرْطَةِ (IACP Award) لتفوُّقِها العالميّ في مجال الأدلة الرَّقْمِيَّةِ[1].

- في السعودية:

تشكِّل إدارة مكافحة الجرائم المعلوماتية التابعة للمديرية العامة للأمن العام في المملكة العربية السعودية الوحدة الرئيسية لمكافحة الجرائم الإلكترونية، وتضمّ وحدات متخصصة في الطب الشرعي الرقمي (Digital Forensics) ضمن الإدارة العامة للأدلة الجنائية، والتي طوّرَتْ معالم مثل معمل جنائي رقمي في جدة منذ 2014 لفحص الجرائم المعلوماتية بتقنيات متقدِّمة[2]، والتي تتعامل الإدارة مع بلاغات الجرائم عبر الرقم الموحَّد 1909 أو تطبيق "كلنا أمن"، وتشمل فحص

[1] سعود علي اللوغاني، المواجهة الإجرائية الدولية في مكافحة الجريمة الالكترونية- في ضوء التشريعات الوطنية والاتفاقيات الدولية، دار الحافظ، 1443-2022،دبي، ص ص 50-52

[2] https://www.pv.gov.sa/Eservices/Pages/CybercrimesService.aspx... Accessed March 23, 2025 …14.00m

الأدلة الرقمية مثل استرداد البيانات، تحليل الهجمات السيبرانية (النصب، الاحتيال، السرقة المالية)، والتعاون مع النيابة العامة لإعداد تقارير فنية. تركز على جرائم الإنترنت والتجسس، مع تدريب كوادر في التحقيق الجنائي الرقمي لمواكبة رؤية 2030[1]، حيث تدعم الجهود تشريعات مثل نظام مكافحة جرائم المعلوماتية (2007) ونظام الإثبات الجديد (1443هـ) الذي يعزز حجية الدليل الرقمي، مع فعاليات مثل قمة العلوم الطبية الشرعية 2025 لتعزيز الابتكار في الأدلة الرقمية[2].

[1] https://www.secprint.sa/cybercrime-reporting-number-ksa/... Accessed March 23, 2025 …14.40m

[2] نظام مكافحة جرائم المعلوماتية السعودي، الصادر بموجب المرسوم الملكي رقم (م/17) بتاريخ 8 ربيع الأول 1428هـ (26 مارس 2007)، يهدف إلى الحد من الجرائم الإلكترونية عبر معاقبة الدخول غير المشروع، التنصت، الاحتيال، التشهير، والاعتداء على البيانات الشخصية، بعقوبات تشمل السجن والغرامة، ضماناً للأمن المعلوماتي وحماية الاقتصاد الوطني.

الخاتمة:

لم تعد تكنولوجيا المعلوماتية امتيازًا محتكرًا للدول المتقدمة فحسب، بل أصبحت منذ السبعينيات، وخاصة خلال العقد الأخير، أحد أركان الحياة الحديثة الأساسية للدول والمجتمعات على حد سواء. فقد انتشرت في كل المجالات الحياتية، حيث تحولت الحواسيب وشبكة الإنترنت إلى أدوات يومية يمتلكها الفرد العادي وتعتمد عليها المؤسسات والحكومات، مساهمة في تطوير الفكر البشري، تحسين نمط الحياة، وتعزيز التواصل العالمي والابتكار الاقتصادي. غير أن هذا الانتشار الواسع أنتج في الوقت ذاته تحديًا خطيرًا، وهو الجرائم المعلوماتية أو الإلكترونية، التي تستهدف الأنظمة الحاسوبية والشبكات بهدف الاطلاع على المعلومات السرية، سرقتها، تخريبها، أو تعطيلها، مما يهدد الأمن الوطني والخصوصية الشخصية.

وتتميز هذه الجرائم بطابعها المتقدم والمعقد، إذ ينفذها مجرمون متخصصون ذوو معرفة تقنية عالية من خلال هجمات إلكترونية سرية وغير مرئية، مثل الاختراقات السيبرانية، البرمجيات الضارة، والاحتيال عبر الإنترنت، بهدف تحقيق مكاسب مادية فورية (كالسرقة المالية) أو معنوية طويلة الأمد (كالتجسس الصناعي أو السياسي). ولم تقتصر مخاطرها على الجانب المادي، بل امتدت إلى استهداف الفئات الهشة مثل القصر والأطفال عبر استدراجهم في المنصات الرقمية لغايات نفسية وجنسيّة، مما يفاقم من تعقيد الظاهرة ويستدعي تدخلاً وقائيًا وتربويًا.

وفي مواجهة هذه التحديات، وضع القانون الجزائي إطارًا تشريعيًا فعالًا وحديثًا يجرم الاعتداءات على أنظمة المعلومات، يحمي الفئات الضعيفة، ويعزز التعاون الدولي. ومع ذلك،

يظل النجاح في مكافحة الجرائم الإلكترونية مرهونًا بتوعية المجتمع، تطوير الكفاءات التقنية، وتعزيز الشراكات بين الدول، لضمان بيئة رقمية آمنة تحقق التوازن بين الابتكار والأمن.

وتمثل مكافحة الجرائم الإلكترونية ضرورة ملحّة للحفاظ على إنجازات الثورة الرقمية، حيث تتطلب جهودًا مشتركة تجمع بين التشريعات القوية، التقنيات المتقدِّمة كالتحقيق الرقمي والذكاء الاصطناعي، والتثقيف المستمر لتحويل الإنترنت من سلاح محتمل إلى أداة تنمية مستدامة، بهذا النهج الشامل يمكن للمجتمعات أن تواجه التهديدات الرقمية بثقة، محافظةً على أمنها وازدهارها في عصر التحول الرقمي.

قائمة المراجع

المعاهدات الدولية والقوانين:

- اتفاقية بودابست بشأن الجرائم الإلكترونية، مجلس أوروبا، 23 نوفمبر 2001.
- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، القاهرة بتاريخ 21ديسمبر 2010.
- القانون رقم 18-07 المؤرخ في 10 جوان 2018 المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.
- قانون رقم 18-05 المؤرخ في 10 ماي 2018 المتعلق بالتجارة الإلكترونية، الجمهورية الجزائرية الديمقراطية الشعبية.
- القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجمهورية الجزائرية الديمقراطية الشعبية.
- قانون نظام مكافحة الجرائم المعلوماتية، المملكة العربية السعودية، 1428هـ/2007 م.
- القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم بقانون العقوبات (الأمر رقم 156/66)، الجمهورية الجزائرية الديمقراطية الشعبية.
- قانون المعاملات الإلكترونية الأردني رقم 85 لسنة 2001

الكتب والمؤلفات:

- أحمد بن علي، الجريمة المعلوماتية في القانون الجنائي المعاصر، دار النهضة العربية، 2000، القاهرة.

- احمد بن محمد الشريف، الجرائم المعلوماتية وحماية الاطفال، الجزائر، دار الجامعة الجديدة، 2022.

- احمد شريف، الجرائم الإلكترونية، دراسة مقارنة، دار النهضة العربية، مصر، 2020.

- أحمد محمد الزعبي، المعاملات الإلكترونية في التشريع الأردني، دار الثقافة للنشر، عمان، 2005.

- أحمد محمد الشريف، الجريمة المعلوماتية: الخصائص والتحديات القانونية، الجزائر، دار الفكر، 2024.

- أحمد محمد براك، شرح قانون الجرائم الإلكترونية، الإطار المفاهيمي، المواجهة الموضوعية- المواجهة الإجرائية في ضوء القانون رقم 17 لسنة 2023، دراسة تحليلية تأصيلية مقارنة، دار الثقافة للنشر والتوزيع، عمان، 2024.

- الحلبي محمد، الجريمة المعلوماتية، التحديات القانونية، دار الحلبي الحقوقية، بيروت، 2019،.

- بن عيسى، فاطمة، الإجرام الرقمي في التشريعات العربية، منشورات الجامعة التونسية، تونس، 2023.

- حشمان عمّار، الجريمة المعلوماتية في التشريع الجزائري، 2020، الجزائر.

- حمد خليفة الملط، الجرائم المعلوماتية: دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2005.

- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011.

- دوار علي، قانون الأمن السيبراني، دار الغرب الإسلامي، الجزائر، 2022.

- عبد الرحمن بن محمد الشيخ، الجرائم المعلوماتية في التشريع السعودي، دار المعرفة، الرياض، 2012.

- عبد الرحمن سامي، الجرائم الإلكترونية وأحكامها في القانون الجزائري، دار هومة للنشر، الجزائر، 2021.

- عبد العال الدريبي، الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والأنترنت، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2012.

- عبد القادر حمدي، الجريمة المعلوماتية: دراسة في الطبيعة القانونية وخصائص المجرم المعلوماتي، دار الثقافة للنشر والتوزيع، 2020، عمان.

- عبد الكريم عبد الله عبد الله، الحماية القانونية للملكية الفكرية على شبكة الأنترنت، دار الجامعة الجديدة، سنة 2008، مصر،

- علي بن عبد الله غسيري، الأثار الأمنية لاستخدام الشباب للأنترنت، الطبعة الأولى، جامعة نايف للعلوم الأمنية، الرياض، السعودية، 2004.

- محمد أمين الشوابكة، جرائم الحاسوب والأنترنت (الجريمة المعلوماتية)، دار الثقافة للنشر والتوزيع، عمان الأردن،2009.

– محمد بن صالح الجمال، الجريمة المعلوماتية في التشريع الجزائري، منشورات الجمعية الجزائرية للبحث القانوني، الجزائر، 2015.

– محمد بن صالح الجمال، الجريمة المعلوماتية في التشريع الجزائري، منشورات الجمعية الجزائرية للبحث القانوني، الجزائر، 2015.

– محمد بن صالح الجمال، الجريمة المعلوماتية في التشريع الجزائري، منشورات الجمعية الجزائرية للبحث القانوني، الجزائر، 2015.

– محمد سيد سلطان، قضايا قانونية في امن المعلومات وحماية البيئة الإلكترونية، دار ناشري للنشر الإلكتروني، الكويت، سنة 2012.

– محمد سيد سلطان، قضايا قانونية في امن المعلومات وحماية البيئة الإلكترونية، دار ناشري للنشر الإلكتروني، الكويت، 2012.

– محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، مصر ،2004.

– محمد مثال، حماية الحياة الخاصة في مواجهة تكنولوجيا المعلومات، دار الجامعة الجديدة، الإسكندرية، 2022.

– نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الحلبي الحقوقي، بيروت، 2009.

– هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة الجرائم المعلوماتية معلقا عليها، الطبعة الأولى، دار النهضة العربية، مصر، 2008.

– وائل شعيب، الجرائم المعلوماتية، أنواعها وأحكامها في الفقه والقانون، دار الفكر الجامعي، 2019، القاهرة.

رسائل الدكتوراه والماجيستير:

- دليلة جلول، ضحايا الجريمة المعلوماتية في الجزائر، أطروحة دكتوراه، جامعة باتنة 1، 2024.

- عمر بن محمد العتبى، الأمن المعلوماتي ومدى توافقه مع المعايير المحلية والدولية، رسالة مقدمة لأجل نيل شهادة الدكتوراه، قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، السعودية، 2010.

- عمر بن محمد العتبي، الأمن المعلوماتي ومدى توافقه مع المعايير المحلية والدولية، رسالة مقدمة لأجل نيل شهادة الدكتوراه، قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، السعودية، 2010.

- عبد الرحمن عثماني، جرائم تقنية المعلومات في ظل الاتفاقية العربية، رسالة ماجستير، جامعة ورقلة، 2022.

- بركات يمان، جرائم السب والقذف التقليدية والإلكترونية- دراسة مقارنة- رسالة ماجستير، كلية القانون، جامعة الشارقة، 2019.

- عمّار حشمان، الجريمة المعلوماتية في التشريع الجزائري، أطروحة ماجستير، جامعة ورقلة، 2017.

المجلات والدوريات:

- الجازولي بن أحمد، خصوصية المجرم المعلوماتي ودوافعه، مجلة دراسات قانونية، العدد 2، 2021.

- الشافعي محمد زكي، التكييف القانوني لجريمة القذف عبر مواقع التواصل الاجتماعي، مجلة البحوث القانونية رقم 5،2020.

- بلقاسم بن محمد، الحماية الجزائية للطفل من جرائم الاستغلال الجنسي عبر شبكة الإنترنت، مجلة البحوث القانونية، العدد 12، سنة 2020.

- بن سعادة نادية، الجريمة الإلكترونية، دلالة المفهوم وفعالية المعالجة القانونية، مجلة العلوم القانونية والسياسية، عدد 14 ،2021،

- بن سعادة نادية، الجريمة الإلكترونية، دلالة المفهوم وفعالية المعالجة القانونية، مجلة العلوم القانونية والسياسية، عدد 14، سنة (2021).

- عبد السلام عليلي، جريمة القذف عبر وسائل التواصل الاجتماعي، مجلة الدراسات القانونية والاقتصادية، المركز الجامعي سي الحواس بريكة، المجلد 5، العدد 02، 2022.

- عبد القادر بوطالب، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مجلة الدراسات القانونية، 5، عدد 1 ،2017.

- عبد القادر بوطالب، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مجلة الدراسات القانونية 5، عدد 1 2017.

– لوسي موسى، التكييف القانوني لجريمة القذف عبر مواقع التواصل الاجتماعي في التشريع الجزائري، مجلة الدراسات السياسية والقانونية، جامعة عمار ثليجان الأغواط، الملد 5، عدد 1، 2019.

– نغم عبد الكريم مهدي، مفهوم الحق في حرمة الحياة الخاصة وأثر وسائل تقنية المعلومات الحديثة عليه، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كربلاء، المجلد 12، العدد 2، 2023.

– هزيل أمال، خليفي وردة، الجرائم الماسة بالسمعة والشرف عبر الإنترنت، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، مجلد 9، رقم 2، 2019.

– هشام رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي، مجلة الأمن والقانون، الامرات المتحدة، دبي، العدد الثاني، 1999.

تقارير ومناشير:

التقرير التفسيري لاتفاقية بودابست بشأن الجرائم الإلكترونية، مجلس أوروبا، 8 نوفمبر 2001، الدورة رقم 109.

تقرير مجموعة العمل الحكومية المشتركة الفرنسية 2014، تحت عنوان – حماية مستعملي شبكة الأنترنت– فيفري 2014– ص 20– متوفر على الموقع الرسمي لوزارة العدل الفرنسية، الرابط

منشور وزارة العدل، التحري والتحقيق في الجرائم الإلكترونية في القانون الجزائري، الجزائر، وزارة العدل، 2021.

منظمة التعاون الاقتصادي والتنمية(OECD) ، تقرير حول الجرائم المعلوماتية، باريس، 1983.

الهيئة لمكافحة الجريمة الإلكترونية الدولية، "عملية ماريبوسا: تفكيك أكبر شبكة بوت نت في التاريخ"، تقرير رسمي ،مدريد الشرطة الإسبانية، 2010

مراجع الكترونية:

- أعمدة أمن المعلومات والأمن السيبراني :(CIA Triad) الدليل الكامل، Professor Technology، 10 أكتوبر 2024، https://www.professor-technology.com/2024/10/cia-triad.html... تاريخ الاطلاع 2024/02/12 12.00...د

- الضوابط الأساسية للأمن السيبراني"، ega.ee، 2019، https://ega.ee/wp-content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf... تاريخ الاطلاع 2024/02/12 ...10.12د

- الثلاثية الأساسية لأمن المعلومات"CIA Triad ، root-x.dev، https://root-x.dev/blog/article/CIA-Triad... تاريخ الاطلاع 2024/02/12 ...12.45د

- عناصر الأمن السيبراني"، rmg-sa.com، 19 فبراير 2025، https://www.rmg-sa.com تاريخ الاطلاع 2024/02/20 ...09.00د

- محمد سيد سلطان، مرجع متوفر على الموقع الرسمي لدار ناشري للنشر الإلكتروني، تاريخ التصفح2024/02/20، الرابط الإلكتروني:

https://www.nashiri.net/latest/books-mags-news/5051-2012-01-27-22-05-28-v15-5051.htm

مراجع باللغة الأجنبية:

Books :

- Ahmed K. Hassan, Cybercrime Offenders and their Organizational Power ,London,Routledge, 2019.
- Alex Alexandrou, Cybercrime and Information Technology, Theory and Practice (London: Routledge, 2021), P 112.
- Andrew Charlesworth, Information Technology Law, London: Butterworths, 1999.
- Andrew Murray, Information Technology Law: The Law and Society, 5th ed, (Oxford: Oxford University Press, 2023).
- Council of Europe, Convention on Cybercrime (Budapest Convention), ETS No 185 (Budapest, 2001),
- David S. Wall, Cybercrime,The Transformation of Crime in the Information Age ,Cambridge, Polity Press, 2007.
- Don Parker, Fighting Computer Crime, New York : Wiley Computer Publications, 1983.
- Grabosky, Peter. Cybercrime: The Challenge of Trans-national Crime. Sydney: Federation Press, 2001.
- Jamal Awwad Alkharman et al, Cyber Attacks and its Implication to National Security, Pakistan Journal of Criminology 16, no. 3 (2024).
- Loader, Brian D., and Don Tapscott, eds. The Governance of Cyberspace. London : Routledge, 1998.
- Michael L. Rich, Cybercrime and Social Profiles of Offenders , Oxford, Oxford University Press, 2020.

- Myriam Quéméner, Yves Charpenel, La Cybercriminalité, Edition Economica, Paris, France-2010.
- Nahla Abdul Qader Al-Mumeni, Cybercrimes : Their Nature and Characteristics, Dar Al-Halabi Legal Publications, Beirut, 2009.
- National Academies of Sciences, Engineering, and Medicine, Cybercrime Classification and Measurement (Washington, DC: The National Academies Press, 2025).
- OECD, Computer Crime : An International Perspective, Paris : Organisation for Economic Co-operation and Development, 1983.
- Samira Bin Issa, "Cybercrimes Across Borders: Issues of Judicial Jurisdiction," Journal of Law and Technology 12, no 3, 2025.
- Schneier, Bruce. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W.W. Norton & Company, 2015.
- Soltan, Khaled. Cybersecurity and Cyberwarfare: An Introduction. Hoboken: Wiley, 2017.
- Svantesson, Dan Jerker B. "Jurisdiction in Cyberspace: Towards 'Core Principles'." Tilburg Law Review 21, no. 1 (2015).
- Thomas J. Holt, Adam M. Bossler, and Kathryn C. Cybercrime and Digital Forensics ,Seigfried-Spellar ,3rd Edition, Routledge, 2022, new york, usa.
- Thomas J. Holt, Cybercrime and Digital Forensics, An Introduction, New York, Routledge, 2018.
- UNODC, "Cybercrime Legislation and Offences," Global Programme on Cybercrime ,Vienna, UNODC, 2016.

- UNODC, Cybercrime Module 2, Offences against the Confidentiality, Integrity and Availability of Computer Data and Systems , Vienna: UNODC, 2018.

- Wall, David S. Cybercrime: The Transformation of Crime in the Information Age. Cambridge : Polity Press, 2007.

- Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." Harvard Law Review 4, no. 5 (1890).

Solove, Daniel J. Understanding Privacy. Cambridge, MA: Harvard University Press, 2008.

United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 10th Congress, Vienna, 2000, Report.

Westin, Alan F. Privacy and Freedom. New York: Atheneum, 1967.

Other diverse references in foreign languages :

- United Nations Office on Drugs and Crime (UNODC), "What to Know about Cybercrime in 2025," October 25, 2025, https://www.unodc.org/unodc/frontpage/2025/October/what-to-know-about-cybercrime-in-2025.html... See 25/10/2025…21.00h

- ART 1030 sec (a) Computer Fraud and Abuse Act (18 U.S.C. § 1030), 1986, It was modified in 2008

- https://www.mjustice.dz/wp-content/uploads/pdf/18012022.pdf.

- https://www.joradp.dz/ftp/jo-arabe/2015/a2015053.pdf

- https://me.kaspersky.com/resource-center/definitions/hacker-hat-types... See 12-4-2024…21.00m

- https://www.secprint.sa/how-to-face-hacking/... See 13/04/2024…11.30m

https://unctad.org/system/files/officialdocument/Cybercrime%20Nayelly%20Loya%20(UNODC).pdf.

- Joël Rivière et Didier Lucas – « Criminalité et internet une arnaque à bon March » – Article publier dans la revus de la sécurité Globale- numéro 06- année 2008, Disponible sur site www.cairn.info – Fonds documentaire (S.N.D.L) Système national de documentation en ligne – Algérie –Date de consultation 28/03/2014.

- Ordonnance n° 03-05 du 19 Joumada El Oula 1424 correspondant au 19 juillet 2003 relative aux droits d'auteur et aux droits voisins, n° 44

Cf. Algerian Law No. 18-07 of June 10, 2018, Art. 4 (regulating the conditions for lawful processing and storage of personal data to prevent unauthorized disclosure).

فهرس المحتويات

مقدمة:

United Nations Convention against Cybercrime : Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes

اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية؛

تعزيز التعاون الدولي لمكافحة جرائم معينة مرتكبة بواسطة نظم تكنولوجيا المعلومات والاتصالات ولتبادل الأدلة في شكل إلكتروني على الجرائم الخطيرة

المصدر: موقع الأمم المتحدة

https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html

The States Parties to the present Convention,

Bearing in mind the purposes and principles of the Charter of the United Nations,

Noting that information and communications technologies, while having enormous potential for the development of societies, create new opportunities for perpetrators, may contribute to the increase in the rate and diversity of criminal activities, and may have an adverse impact on States, enterprises and the well-being of individuals and society as a whole,

Concerned that the use of information and communications technology systems can have a considerable impact on the scale, speed and scope of criminal offences, including offences related to terrorism and transnational organized crime, such as trafficking in persons, the smuggling of migrants, the illicit manufacturing of and trafficking in firearms, their parts, components and ammunition, drug trafficking and trafficking in cultural property,

Convinced of the need to pursue, as a matter of priority, a global criminal justice policy aimed at the protection of society against cybercrime by, inter alia, adopting appropriate legislation, establishing common offences and procedural powers and fostering international cooperation to prevent and combat such activities more effectively at the national, regional and international levels,

Determined to deny safe havens to those who engage in cybercrime by prosecuting these crimes wherever they occur,

Stressing the need to enhance coordination and cooperation among States by, inter alia, providing technical assistance and capacity-building, including the transfer of technology on mutually agreed terms, to countries, in particular developing countries, upon their request, to improve national legislation and frameworks and enhance the capacity of national authorities to deal with cybercrime in all its forms, including its prevention, detection, investigation and prosecution, and emphasizing in this context the role that the United Nations plays,

Recognizing the increasing number of victims of cybercrime, the importance of obtaining justice for those victims and the necessity to address the needs of persons in vulnerable situations in measures taken to prevent and combat the offences covered by this Convention,

Determined to prevent, detect and suppress more effectively international transfers of property obtained as a result of cybercrime and to strengthen international cooperation in the recovery and return of proceeds of the crimes established in accordance with this Convention,

Bearing in mind that preventing and combating cybercrime is a responsibility of all States and that they must cooperate with one another, with the support and involvement of relevant international and regional organizations, as well as non-governmental organizations, civil society organizations, academic institutions and private sector entities, if their efforts in this area are to be effective,

Recognizing the importance of mainstreaming a gender perspective in all relevant efforts to prevent and combat the offences covered by this Convention, in accordance with domestic law,

Mindful of the need to achieve law enforcement objectives and to ensure respect for human rights and fundamental freedoms as enshrined in applicable international and regional instruments,

Acknowledging the right to protection against arbitrary or unlawful interference with one's privacy, and the importance of protecting personal data,

Commending the work of the United Nations Office on Drugs and Crime and other international and regional organizations in preventing and combating cybercrime,

Recalling General Assembly resolutions 74/247 of 27 December 2019 and 75/282 of 26 May 2021,

Taking into account the existing international and regional conventions and treaties on cooperation in criminal matters, as well as similar treaties that exist between Member States of the United Nations,

Have agreed as follows:

Chapter I: General provisions

Article 1: Statement of purpose

The purposes of this Convention are to:

(a) Promote and strengthen measures to prevent and combat cybercrime more efficiently and effectively;

(b) Promote, facilitate and strengthen international cooperation in preventing and combating cybercrime; and

(c) Promote, facilitate and support technical assistance and capacity-building to prevent and combat cybercrime, in particular for the benefit of developing countries.

Article 2: Use of terms

For the purposes of this Convention:

(a) "Information and communications technology system" shall mean any device or group of interconnected or related devices, one or more of which, pursuant to a program, gathers, stores and performs automatic processing of electronic data;

(b) "Electronic data" shall mean any representation of facts, information or concepts in a form suitable for processing in an information and communications technology system, including a program suitable to cause an information and communications technology system to perform a function;

(c) “Traffic data” shall mean any electronic data relating to a communication by means of an information and communications technology system, generated by an information and communications technology system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration or type of underlying service;

(d) “Content data” shall mean any electronic data, other than subscriber information or traffic data, relating to the substance of the data transferred by an information and communications technology system, including, but not limited to, images, text messages, voice messages, audio recordings and video recordings;

(e) “Service provider” shall mean any public or private entity that:

(i) Provides to users of its service the ability to communicate by means of an information and communications technology system; or

(ii) Processes or stores electronic data on behalf of such a communications service or users of such a service;

(f) “Subscriber information” shall mean any information that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

(i) The type of communications service used, the technical provisions related thereto and the period of service;

(ii) The subscriber’s identity, postal or geographical address, telephone or other access number, billing or payment information, available on the basis of the service agreement or arrangement;

(iii) Any other information on the site of the installation of communications equipment, available on the basis of the service agreement or arrangement;

(g) “Personal data” shall mean any information relating to an identified or identifiable natural person;

(h) “Serious crime” shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty;

(i) “Property” shall mean assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, including virtual assets, and legal documents or instruments evidencing title to, or interest in, such assets;

(j) “Proceeds of crime” shall mean any property derived from or obtained, directly or indirectly, through the commission of an offence;

(k) “Freezing” or “seizure” shall mean temporarily prohibiting the transfer, conversion, disposition or movement of property or temporarily assuming custody or control of property on the basis of an order issued by a court or other competent authority;

(l) “Confiscation”, which includes forfeiture where applicable, shall mean the permanent deprivation of property by order of a court or other competent authority;

(m) “Predicate offence” shall mean any offence as a result of which proceeds have been generated that may become the subject of an offence as defined in article 17 of this Convention;

(n) “Regional economic integration organization” shall mean an organization constituted by sovereign States of a given region to which its member States have transferred competence in

respect of matters governed by this Convention and which has been duly authorized, in accordance with its internal procedures, to sign, ratify, accept, approve or accede to it; references to "States Parties" under this Convention shall apply to such organizations within the limits of their competence;

(o) "Emergency" shall mean a situation in which there is a significant and imminent risk to the life or safety of any natural person.

Article 3: Scope of application

This Convention shall apply, except as otherwise stated herein, to:

(a) The prevention, investigation and prosecution of the criminal offences established in accordance with this Convention, including the freezing, seizure, confiscation and return of the proceeds from such offences;

(b) The collecting, obtaining, preserving and sharing of evidence in electronic form for the purpose of criminal investigations or proceedings, as provided for in articles 23 and 35 of this Convention.

Article 4: Offences established in accordance with other United Nations conventions and protocols

1. In giving effect to other applicable United Nations conventions and protocols to which they are Parties, States Parties shall ensure that criminal offences established in accordance with such conventions and protocols are also considered criminal offences under domestic law when committed through the use of information and communications technology systems.

2. Nothing in this article shall be interpreted as establishing criminal offences in accordance with this Convention.

Article 5: Protection of sovereignty

1. States Parties shall carry out their obligations under this Convention in a manner consistent with the principles of sovereign equality and territorial integrity of States and that of non-intervention in the domestic affairs of other States.

2. Nothing in this Convention shall entitle a State Party to undertake in the territory of another State the exercise of jurisdiction and performance of functions that are reserved exclusively for the authorities of that other State by its domestic law.

Article 6: Respect for human rights

1. States Parties shall ensure that the implementation of their obligations under this Convention is consistent with their obligations under international human rights law.

2. Nothing in this Convention shall be interpreted as permitting suppression of human rights or fundamental freedoms, including the rights related to the freedoms of expression, conscience, opinion, religion or belief, peaceful assembly and association, in accordance and in a manner consistent with applicable international human rights law.

Chapter II: Criminalization

Article 7: Illegal access

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence under its domestic law, when committed intentionally, the access to the whole or any part of an information and communications technology system without right.

2. A State Party may require that the offence be committed by infringing security measures, with the intent of obtaining electronic data or other dishonest or criminal intent or in relation to an information and communications technology system that is connected to another information and communications technology system.

Article 8: Illegal interception

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the interception, made by technical means, of non-public transmissions of electronic data to, from or within an information and communications technology system, including electromagnetic emissions from an information and communications technology system carrying such electronic data.

2. A State Party may require that the offence be committed with dishonest or criminal intent, or in relation to an information and communications technology system that is connected to another information and communications technology system.

Article 9: Interference with electronic data

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the damaging, deletion, deterioration, alteration or suppression of electronic data.

2. A State Party may require that the conduct described in paragraph 1 of this article result in serious harm.

Article 10: Interference with an information and communications technology system

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the serious hindering of the functioning of an information and communications technology system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing electronic data.

Article 11: Misuse of devices

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

(a) The obtaining, production, sale, procurement for use, import, distribution or otherwise making available of:

(i) A device, including a program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with articles 7 to 10 of this Convention; or

(ii) A password, access credentials, electronic signature or similar data by which the whole or any part of an information and communications technology system is capable of being accessed;

with the intent that the device, including a program, or the password, access credentials, electronic signature or similar data be used for the purpose of committing any of the offences established in accordance with articles 7 to 10 of this Convention; and

(b) The possession of an item referred to in paragraph 1 (a) (i) or (ii) of this article, with intent that it be used for the purpose of committing any of the offences established in accordance with articles 7 to 10 of this Convention.

2. This article shall not be interpreted as imposing criminal liability where the obtaining, production, sale, procurement for use, import, distribution or otherwise making available, or the possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with articles 7 to 10 of this Convention, such as for the authorized testing or protection of an information and communications technology system.

3. Each State Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 (a) (ii) of this article.

Article 12: Information and communications technology system-related forgery

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion or suppression of electronic data resulting in inauthentic data with the intent that they be considered or acted upon for legal purposes as if they were authentic, regardless of whether or not the data are directly readable and intelligible.

2. A State Party may require an intent to defraud, or a similar dishonest or criminal intent, before criminal liability attaches.

Article 13: Information and communications technology system-related theft or fraud

Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by means of:

(a) Any input, alteration, deletion or suppression of electronic data;

(b) Any interference with the functioning of an information and communications technology system;

(c) Any deception as to factual circumstances made through an information and communications technology system that causes a person to do or omit to do anything which that person would not otherwise do or omit to do;

with the fraudulent or dishonest intent of procuring for oneself or for another person, without right, a gain in money or other property.

Article 14: Offences related to online child sexual abuse or child sexual exploitation material

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

(a) Producing, offering, selling, distributing, transmitting, broadcasting, displaying, publishing or otherwise making available child sexual abuse or child sexual exploitation material through an information and communications technology system;

(b) Soliciting, procuring or accessing child sexual abuse or child sexual exploitation material through an information and communications technology system;

(c) Possessing or controlling child sexual abuse or child sexual exploitation material stored in an information and communications technology system or another storage medium;

(d) Financing the offences established in accordance with subparagraphs (a) to (c) of this paragraph, which States Parties may establish as a separate offence.

2. For the purposes of this article, the term "child sexual abuse or child sexual exploitation material" shall include visual material, and may include written or audio content, that depicts, describes or represents any person under 18 years of age:

(a) Engaging in real or simulated sexual activity;

(b) In the presence of a person engaging in any sexual activity;

(c) Whose sexual parts are displayed for primarily sexual purposes; or

(d) Subjected to torture or cruel, inhumane or degrading treatment or punishment and such material is sexual in nature.

3. A State Party may require that the material identified in paragraph 2 of this article be limited to material that:

(a) Depicts, describes or represents an existing person; or

(b) Visually depicts child sexual abuse or child sexual exploitation.

4. In accordance with their domestic law and consistent with applicable international obligations, States Parties may take steps to exclude the criminalization of:

(a) Conduct by children for self-generated material depicting them; or

(b) The consensual production, transmission, or possession of material described in paragraph 2 (a) to (c) of this article, where the underlying conduct depicted is legal as determined by domestic law, and where such material is maintained exclusively for the private and consensual use of the persons involved.

5. Nothing in this Convention shall affect any international obligations which are more conducive to the realization of the rights of the child.

Article 15: Solicitation or grooming for the purpose of committing a sexual offence against a child

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the act of intentionally communicating, soliciting, grooming, or making any arrangement through an information and communications technology system for the purpose of committing a sexual offence against a child, as defined in domestic law, including for the commission of any of the offences established in accordance with article 14 of this Convention.

2. A State Party may require an act in furtherance of the conduct described in paragraph 1 of this article.

3. A State Party may consider extending criminalization in accordance with paragraph 1 of this article in relation to a person believed to be a child.

4. States Parties may take steps to exclude the criminalization of conduct as described in paragraph 1 of this article when committed by children.

Article 16: Non-consensual dissemination of intimate images

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the selling, distributing, transmitting, publishing or otherwise making available of an intimate image of a person by means of an information and communications technology system, without the consent of the person depicted in the image.

2. For the purpose of paragraph 1 of this article, "intimate image" shall mean a visual recording of a person over the age of 18 years made by any means, including a photograph or video recording, that is sexual in nature, in which the person's sexual parts are exposed or the person is engaged in sexual activity, which was private at the time of the recording, and in respect of which the person or persons depicted maintained a reasonable expectation of privacy at the time of the offence.

3. A State Party may extend the definition of intimate images, as appropriate, to depictions of persons who are under the age of 18 years if they are of legal age to engage in sexual activity under domestic law and the image does not depict child abuse or exploitation.

4. For the purposes of this article, a person who is under the age of 18 years and depicted in an intimate image cannot consent to the dissemination of an intimate image that constitutes child sexual abuse or child sexual exploitation material under article 14 of this Convention.

5. A State Party may require the intent to cause harm before criminal liability attaches.

6. States Parties may take other measures concerning matters related to this article, in accordance with their domestic law and consistent with applicable international obligations.

Article 17: Laundering of proceeds of crime

1. Each State Party shall adopt, in accordance with fundamental principles of its domestic law, such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally:

(a)

(i) The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of that person's actions;

(ii) The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime;

(b) Subject to the basic concepts of its legal system:

(i) The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime;

(ii) Participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.

2. For purposes of implementing or applying paragraph 1 of this article:

(a) Each State Party shall establish as predicate offences relevant offences established in accordance with articles 7 to 16 of this Convention;

(b) In the case of States Parties whose legislation sets out a list of specific predicate offences, they shall, at a minimum, include in that list a comprehensive range of offences established in accordance with articles 7 to 16 of this Convention;

(c) For the purposes of subparagraph (b) of this paragraph, predicate offences shall include offences committed both within and outside the jurisdiction of the State Party in question. However, offences committed outside the jurisdiction of a State Party shall constitute predicate offences only when the relevant conduct is a criminal offence under the domestic law of the State where it is committed and would be a criminal offence under the domestic law of the State Party implementing or applying this article, had it been committed there;

(d) Each State Party shall furnish copies of its laws that give effect to this article and of any subsequent changes to such laws or a description thereof to the Secretary-General of the United Nations;

(e) If required by fundamental principles of the domestic law of a State Party, it may be provided that the offences set forth in paragraph 1 of this article do not apply to the persons who committed the predicate offence;

(f) Knowledge, intent or purpose required as an element of an offence set forth in paragraph 1 of this article may be inferred from objective factual circumstances.

Article 18: Liability of legal persons

1. Each State Party shall adopt such measures as may be necessary, consistent with its legal principles, to establish the liability of legal persons for participation in the offences established in accordance with this Convention.

2. Subject to the legal principles of the State Party, the liability of legal persons may be criminal, civil or administrative.

3. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offences.

4. Each State Party shall, in particular, ensure that legal persons held liable in accordance with this article are subject to effective, proportionate and dissuasive criminal or non-criminal sanctions, including monetary sanctions.

Article 19: Participation and attempt

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence, in accordance with its domestic law, when committed intentionally, the

participation in any capacity, such as that of an accomplice, assistant or instigator, in an offence established in accordance with this Convention.

2. Each State Party may adopt the necessary legislative and other measures to establish as a criminal offence, in accordance with its domestic law, when committed intentionally, any attempt to commit an offence established in accordance with this Convention.

3. Each State Party may adopt the necessary legislative and other measures to establish as a criminal offence, in accordance with its domestic law, when committed intentionally, the preparation for an offence established in accordance with this Convention.

Article 20: Statute of limitations

Each State Party shall, where appropriate, considering the gravity of the crime, establish under its domestic law a long statute of limitations period in which to commence proceedings for any offence established in accordance with this Convention and establish a longer statute of limitations period or provide for the suspension of the statute of limitations where the alleged offender has evaded the administration of justice.

Article 21: Prosecution, adjudication and sanctions

1. Each State Party shall make the commission of an offence established in accordance with this Convention liable to effective, proportionate and dissuasive sanctions that take into account the gravity of the offence.

2. Each State Party may adopt, in accordance with its domestic law, such legislative and other measures as may be necessary to establish aggravating circumstances in relation to the offences established in accordance with this Convention, including circumstances that affect critical information infrastructures.

3. Each State Party shall endeavour to ensure that any discretionary legal powers under its domestic law relating to the prosecution of persons for offences established in accordance with this Convention are exercised in order to maximize the effectiveness of law enforcement measures in respect of those offences and with due regard to the need to deter the commission of such offences.

4. Each State Party shall ensure that any person prosecuted for offences established in accordance with this Convention enjoys all rights and guarantees in conformity with domestic law and consistent with the applicable international obligations of the State Party, including the right to a fair trial and the rights of the defence.

5. In the case of offences established in accordance with this Convention, each State Party shall take appropriate measures, in accordance with its domestic law and with due regard to the rights of the defence, to seek to ensure that conditions imposed in connection with decisions on release pending trial or appeal take into consideration the need to ensure the presence of the defendant at subsequent criminal proceedings.

6. Each State Party shall take into account the gravity of the offences concerned when considering the eventuality of early release or parole of persons convicted of such offences.

7. States Parties shall ensure that appropriate measures are in place under domestic law to protect children who are accused of offences established in accordance with this Convention, consistent

with the obligations under the Convention on the Rights of the Child and the applicable Protocols thereto, as well as other applicable international or regional instruments.

8. Nothing contained in this Convention shall affect the principle that the description of the offences established in accordance with this Convention and of the applicable legal defences or other legal principles controlling the lawfulness of conduct is reserved to the domestic law of a State Party and that such offences shall be prosecuted and punished in accordance with that law.

Chapter III: Jurisdiction

Article 22: Jurisdiction

1. Each State Party shall adopt such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when:

(a) The offence is committed in the territory of that State Party; or

(b) The offence is committed on board a vessel that is flying the flag of that State Party or an aircraft that is registered under the laws of that State Party at the time when the offence is committed.

2. Subject to article 5of this Convention, a State Party may also establish its jurisdiction over any such offence when:

(a) The offence is committed against a national of that State Party; or

(b) The offence is committed by a national of that State Party or a stateless person with habitual residence in its territory; or

(c) The offence is one of those established in accordance with article 17, paragraph 1 (b) (ii), of this Convention and is committed outside its territory with a view to the commission of an offence established in accordance with article 17, paragraph 1 (a) (i) or (ii) or (b) (i), of this Convention within its territory; or

(d) The offence is committed against the State Party.

3. For the purposes of article 37, paragraph 11,of this Convention, each State Party shall take such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when the alleged offender is present in its territory and it does not extradite such person solely on the ground that the person is one of its nationals.

4. Each State Party may also adopt such measures as may be necessary to establish its jurisdiction over the offences established in accordance with this Convention when the alleged offender is present in its territory and it does not extradite the person.

5. If a State Party exercising its jurisdiction under paragraph 1 or 2 of this article has been notified, or has otherwise learned, that any other States Parties are conducting an investigation, prosecution or judicial proceeding in respect of the same conduct, the competent authorities of those States Parties shall, as appropriate, consult one another with a view to coordinating their actions.

6. Without prejudice to norms of general international law, this Convention shall not exclude the exercise of any criminal jurisdiction established by a State Party in accordance with its domestic law.

Chapter IV: Procedural measures and law enforcement

Article 23: Scope of procedural measures

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this chapter for the purpose of specific criminal investigations or proceedings.

2. Except as provided otherwise in this Convention, each State Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

(a) The criminal offences established in accordance with this Convention;

(b) Other criminal offences committed by means of an information and communications technology system; and

(c) The collection of evidence in electronic form of any criminal offence.

3. (a) Each State Party may reserve the right to apply the measures referred to in article 29 of this Convention only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in article 30 of this Convention. Each State Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in article 29;

(b) Where a State Party, owing to limitations in its legislation in force at the time of the adoption of this Convention, is not able to apply the measures referred to in articles 29 and 30 of this Convention to communications being transmitted within an information and communications technology system of a service provider which:

(i) Is being operated for the benefit of a closed group of users; and

(ii) Does not employ public communications networks and is not connected with another information and communications technology system, whether public or private;

that State Party may reserve the right not to apply these measures to such communications. Each State Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in articles 29 and 30 of this Convention.

Article 24: Conditions and safeguards

1. Each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this chapter are subject to conditions and safeguards provided for under its domestic law, which shall provide for the protection of human rights, in accordance with its obligations under international human rights law, and which shall incorporate the principle of proportionality.

2. In accordance with and pursuant to the domestic law of each State Party, such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, include, inter alia, judicial or other independent review, the right to an effective remedy, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3. To the extent that it is consistent with the public interest, in particular the proper administration of justice, each State Party shall consider the impact of the powers and procedures in this chapter upon the rights, responsibilities and legitimate interests of third parties.

4. The conditions and safeguards established in accordance with this article shall apply at the domestic level to the powers and procedures set forth in this chapter, both for the purpose of domestic criminal investigations and proceedings and for the purpose of rendering international cooperation by the requested State Party.

5. References to judicial or other independent review in paragraph 2 of this article are references to such review at the domestic level.

Article 25: Expedited preservation of stored electronic data

1. Each State Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified electronic data, including traffic data, content data and subscriber information, that have been stored by means of an information and communications technology system, in particular where there are grounds to believe that the electronic data are particularly vulnerable to loss or modification.

2. Where a State Party gives effect to paragraph 1 of this article by means of an order to a person to preserve specified stored electronic data in the person's possession or control, the State Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of those electronic data for a period of time as long as necessary, up to a maximum of 90 days, to enable the competent authorities to seek their disclosure. A State Party may provide for such an order to be subsequently renewed.

3. Each State Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the electronic data to keep confidential the undertaking of such procedures for the period of time provided for in its domestic legislation.

Article 26: Expedited preservation and partial disclosure of traffic data

Each State Party shall adopt, in respect of traffic data that are to be preserved under the provisions of article 25 of this Convention, such legislative and other measures as may be necessary to:

(a) Ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of a communication; and

(b) Ensure the expeditious disclosure to the State Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the State Party to identify the service providers and the path through which the communication or indicated information was transmitted.

Article 27: Production order

Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

(a) A person in its territory to submit specified electronic data in that person's possession or control that are stored in an information and communications technology system or an electronic data storage medium; and

(b) A service provider offering its services in the territory of the State Party to submit subscriber information relating to such services in that service provider's possession or control.

Article 28: Search and seizure of stored electronic data

1. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

(a) An information and communications technology system, part of it, and electronic data stored therein; and

(b) An electronic data storage medium in which the electronic data sought may be stored;

in the territory of that State Party.

2. Each State Party shall adopt such legislative and other measures as may be necessary to ensure that, where its authorities search or similarly access a specific information and communications technology system or part of it, pursuant to paragraph 1 (a) of this article, and have grounds to believe that the electronic data sought are stored in another information and communications technology system or part of it in its territory, and such data are lawfully accessible from or available to the initial system, such authorities shall be able to expeditiously conduct the search to obtain access to that other information and communications technology system.

3. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure electronic data in its territory accessed in accordance with paragraph 1 or 2 of this article. These measures shall include the power to:

(a) Seize or similarly secure an information and communications technology system or part of it, or an electronic data storage medium;

(b) Make and retain copies of those electronic data in electronic form;

(c) Maintain the integrity of the relevant stored electronic data;

(d) Render inaccessible or remove those electronic data in the accessed information and communications technology system.

4. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the information and communications technology system in question, the information and telecommunications network, or their component parts, or measures applied to protect the electronic data therein, to provide, as is reasonable, the necessary information to enable the undertaking of the measures referred to in paragraphs 1 to 3 of this article.

Article 29: Real-time collection of traffic data

1. Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

(a) Collect or record, through the application of technical means in the territory of that State Party; and

(b) Compel a service provider, within its existing technical capability:

(i) To collect or record, through the application of technical means in the territory of that State Party; or

(ii) To cooperate and assist the competent authorities in the collection or recording of;

traffic data, in real time, associated with specified communications in its territory transmitted by means of an information and communications technology system.

2. Where a State Party, owing to the principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a) of this article, it may instead adopt such legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means in that territory.

3. Each State Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this

Article 30: Interception of content data

1. Each State Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious criminal offences to be determined by domestic law, to empower its competent authorities to:

(a) Collect or record, through the application of technical means in the territory of that State Party; and

(b) Compel a service provider, within its existing technical capability:

(i) To collect or record, through the application of technical means in the territory of that State Party; or

(ii) To cooperate and assist the competent authorities in the collection or recording of;

content data, in real time, of specified communications in its territory transmitted by means of an information and communications technology system.

2. Where a State Party, owing to the principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1 (a) of this article, it may instead adopt such legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory, through the application of technical means in that territory.

3. Each State Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

Article 31: Freezing, seizure and confiscation of the proceeds of crime

1. Each State Party shall adopt, to the greatest extent possible within its domestic legal system, such measures as may be necessary to enable the confiscation of:

(a) Proceeds of crime derived from offences established in accordance with this Convention or property the value of which corresponds to that of such proceeds;

(b) Property, equipment or other instrumentalities used in or destined for use in offences established in accordance withthis Convention.

2. Each State Party shall adopt such measures as may be necessary to enable the identification, tracing, freezing or seizure of any item referred to in paragraph 1 of this article for the purpose of eventual confiscation.

3. Each State Party shall adopt, in accordance with its domestic law, such legislative and other measures as may be necessary to regulate the administration by the competent authorities of frozen, seized or confiscated property covered in paragraphs 1 and 2 of this article.

4. If proceeds of crime have been transformed or converted, in part or in full, into other property, such property shall be liable to the measures referred to in this article instead of the proceeds.

5. If proceeds of crime have been intermingled with property acquired from legitimate sources, such property shall, without prejudice to any powers relating to freezing or seizure, be liable to confiscation up to the assessed value of the intermingled proceeds.

6. Income or other benefits derived from proceeds of crime, from property into which proceeds of crime have been transformed or converted or from property with which proceeds of crime have been intermingled, shall also be liable to the measures referred to in this article, in the same manner and to the same extent as proceeds of crime.

7. For the purposes of this article and article 50 of this Convention, each State Party shall empower its courts or other competent authorities to order that bank, financial or commercial records be made available or be seized. A State Party shall not decline to act under the provisions of this paragraph on the ground of bank secrecy.

8. Each State Party may consider the possibility of requiring that an offender demonstrate the lawful origin of alleged proceeds of crime or other property liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law and with the nature of the judicial and other proceedings.

9. The provisions of this article shall not be construed as prejudicing the rights of bona fide third parties.

10. Nothing contained in this article shall affect the principle that the measures to which it refers shall be defined and implemented in accordance with the provisions of the domestic law of a State Party.

Article 32: Establishment of criminal record

Each State Party may adopt such legislative or other measures as may be necessary to take into consideration, under such terms as, and for the purpose that, it deems appropriate, any previous conviction in another State of an alleged offender for the purpose of using such information in criminal proceedings relating to an offence established in accordance with this Convention.

Article 33: Protection of witnesses

1. Each State Party shall take appropriate measures, in accordance with its domestic law and within its means, to provide effective protection from potential retaliation or intimidation for witnesses who give testimony or, in good faith and on reasonable grounds, provide information concerning offences established in accordance with this Convention or otherwise cooperate with investigative or judicial authorities and, as appropriate, for their relatives and other persons close to them.

2. The measures envisaged in paragraph 1 of this article may include, inter alia, without prejudice to the rights of the defendant, including the right to due process:

(a) Establishing procedures for the physical protection of such persons, such as, to the extent necessary and feasible, relocating them and permitting, where appropriate, non-disclosure or

limitations on the disclosure of information concerning the identity and whereabouts of such persons;

(b) Providing evidentiary rules to permit witness testimony to be given in a manner that ensures the safety of the witness, such as permitting testimony to be given through the use of communications technology such as video links or other adequate means.

3. States Parties shall consider entering into agreements or arrangements with other States for the relocation of persons referred to in paragraph 1 of this article.

4. The provisions of this article shall also apply to victims insofar as they are witnesses.

Article 34: Assistance to and protection of victims

1. Each State Party shall take appropriate measures within its means to provide assistance and protection to victims of offences established in accordance with this Convention, in particular in cases of threat of retaliation or intimidation.

2. Each State Party shall, subject to its domestic law, establish appropriate procedures to provide access to compensation and restitution for victims of offences established in accordance with this Convention.

3. Each State Party shall, subject to its domestic law, enable views and concerns of victims to be presented and considered at appropriate stages of criminal proceedings against offenders in a manner not prejudicial to the rights of the defence.

4. With respect to the offences established in accordance with articles 14 to 16 of this Convention, each State Party shall, subject to its domestic law, take measures to provide assistance to victims of such offences, including for their physical and psychological recovery, in cooperation with relevant international organizations, non-governmental organizations, and other elements of civil society.

5. In applying the provisions of paragraphs 2 to 4 of this article, each State Party shall take into account the age, gender and the particular circumstances and needs of victims, including the particular circumstances and needs of children.

6. Each State Party shall, to the extent consistent with its domestic legal framework, take effective steps to ensure compliance with requests to remove or render inaccessible the content described in articles 14 and 16 of this Convention.

Chapter V: International cooperation

Article 35: General principles of international cooperation

1. States Parties shall cooperate with each other in accordance with the provisions of this Convention, as well as other applicable international instruments on international cooperation in criminal matters, and domestic laws, for the purpose of:

(a) The investigation and prosecution of, and judicial proceedings in relation to, the criminal offences established in accordance with this Convention, including the freezing, seizure, confiscation and return of the proceeds from such offences;

(b) The collecting, obtaining, preserving and sharing of evidence in electronic form of criminal offences established in accordance with this Convention;

(c) The collecting, obtaining, preserving and sharing of evidence in electronic form of any serious crime, including serious crimes established in accordance with other applicable United Nations conventions and protocols in force at the time of the adoption of this Convention.

2. For the purpose of the collecting, obtaining, preserving and sharing of evidence in electronic form of offences as provided for in paragraph 1 (b) and (c) of this article, the relevant paragraphs of article 40, and articles 41 to 46 of this Convention shall apply.

3. In matters of international cooperation, whenever dual criminality is considered a requirement, it shall be deemed fulfilled irrespective of whether the laws of the requested State Party place the offence within the same category of offence or denominate the offence by the same terminology as the requesting State Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under the laws of both States Parties.

Article 36: Protection of personal data

1. (a) A State Party transferring personal data pursuant to this Convention shall do so in accordance with its domestic law and any obligations the transferring Party may have under applicable international law. States Parties shall not be required to transfer personal data in accordance with this Convention if the data cannot be provided in compliance with their applicable laws concerning the protection of personal data;

(b) Where the transfer of personal data would not be compliant with paragraph 1 (a) of this article, States Parties may seek to impose appropriate conditions, in accordance with such applicable laws, to achieve compliance in order to respond to a request for personal data;

(c) States Parties are encouraged to establish bilateral or multilateral arrangements to facilitate the transfer of personal data.

2. For personal data transferred in accordance with this Convention, States Parties shall ensure that the personal data received are subject to effective and appropriate safeguards in the respective legal frameworks of the States Parties.

3. In order to transfer personal data obtained in accordance with this Convention to a third country or an international organization, a State Party shall notify the original transferring State Party of its intention and request its authorization. The State Party shall transfer such personal data only with the authorization of the original transferring State Party, which may require that the authorization be provided in written form.

Article 37: Extradition

1. This article shall apply to the criminal offences established in accordance with this Convention where the person who is the subject of the request for extradition is present in the territory of the requested State Party, provided that the offence for which extradition is sought is punishable under the domestic law of both the requesting State Party and the requested State Party. When the extradition is sought for the purpose of serving a final sentence of imprisonment or another form of detention imposed in respect of an extraditable offence, the requested State Party may grant the extradition in accordance with domestic law.

2. Notwithstanding paragraph 1 of this article, a State Party whose law so permits may grant the extradition of a person for any of the criminal offences established in accordance with this Convention that are not punishable under its own domestic law.

3. If the request for extradition includes several separate criminal offences, at least one of which is extraditable under this article and some of which are not extraditable by reason of their period of imprisonment but are related to offences established in accordance with this Convention, the requested State Party may apply this article also in respect of those offences.

4. Each of the offences to which this article applies shall be deemed to be included as an extraditable offence in any extradition treaty existing between States Parties. States Parties undertake to include such offences as extraditable offences in every extradition treaty to be concluded between them.

5. If a State Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another State Party with which it has no extradition treaty, it may consider this Convention the legal basis for extradition in respect of any offence to which this article applies.

6. States Parties that make extradition conditional on the existence of a treaty shall:

(a) At the time of deposit of their instruments of ratification, acceptance or approval of or accession to this Convention, inform the Secretary-General of the United Nations whether they will take this Convention as the legal basis for cooperation in extradition with other States Parties to this Convention; and

(b) If they do not take this Convention as the legal basis for cooperation in extradition, seek, where appropriate, to conclude treaties on extradition with other States Parties to this Convention in order to implement this article.

7. States Parties that do not make extradition conditional on the existence of a treaty shall recognize offences to which this article applies as extraditable offences between themselves.

8. Extradition shall be subject to the conditions provided for by the domestic law of the requested State Party or by applicable extradition treaties, including, inter alia, conditions in relation to the minimum penalty requirement for extradition and the grounds upon which the requested State Party may refuse extradition.

9. States Parties shall, subject to their domestic law, endeavour to expedite extradition procedures and to simplify evidentiary requirements relating thereto in respect of any offence to which this article applies.

10. Subject to the provisions of its domestic law and its extradition treaties, the requested State Party may, upon being satisfied that the circumstances so warrant and are urgent, and at the request of the requesting State Party, including when the request is transmitted through existing channels of the International Criminal Police Organization, take a person whose extradition is sought and who is present in its territory into custody or take other appropriate measures to ensure the person’s presence at extradition proceedings.

11. A State Party in whose territory an alleged offender is found, if it does not extradite such person in respect of an offence to which this article applies solely on the ground that the person is one of its nationals, shall, at the request of the State Party seeking extradition, be obliged to submit the case without undue delay to its competent authorities for the purpose of prosecution. Those authorities shall take their decisions and conduct their proceedings in the same manner as in the case of any other offence of a comparable nature under the domestic law of that State Party. The States Parties

concerned shall cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecution.

12. Whenever a State Party is permitted under its domestic law to extradite or otherwise surrender one of its nationals only upon the condition that the person will be returned to that State Party to serve the sentence imposed as a result of the trial or proceedings for which the extradition or surrender of the person was sought and that State Party and the State Party seeking the extradition of the person agree with this option and other terms that they may deem appropriate, such conditional extradition or surrender shall be sufficient to discharge the obligation set forth in paragraph 11 of this article.

13. If extradition, sought for purposes of enforcing a sentence, is refused because the person sought is a national of the requested State Party, the requested State Party shall, if its domestic law so permits and in conformity with the requirements of such law, upon application of the requesting State Party, consider the enforcement of the sentence imposed under the domestic law of the requesting State Party or the remainder thereof.

14. Any person regarding whom proceedings are being carried out in connection with any of the offences to which this article applies shall be guaranteed fair treatment at all stages of the proceedings, including enjoyment of all the rights and guarantees provided by the domestic law of the State Party in the territory of which that person is present.

15. Nothing in this Convention shall be interpreted as imposing an obligation to extradite if the requested State Party has substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person’s sex, race, language, religion, nationality, ethnic origin or political opinions, or that compliance with the request would cause prejudice to that person’s position for any one of these reasons.

16. States Parties may not refuse a request for extradition on the sole ground that the offence is also considered to involve fiscal matters.

17. Before refusing extradition, the requested State Party shall, where appropriate, consult with the requesting State Party to provide it with ample opportunity to present its opinions and to provide information relevant to its allegation.

18. The requested State Party shall inform the requesting State Party of its decision with regard to the extradition. The requested State Party shall inform the requesting State Party of any reason for refusal of extradition unless the requested State Party is prevented from doing so by its domestic law or its international legal obligations.

19. Each State Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary-General of the United Nations the name and address of an authority responsible for making or receiving requests for extradition or provisional arrest. The Secretary-General shall set up and keep updated a register of authorities so designated by the States Parties. Each State Party shall ensure that the details held in the register are correct at all times.

20. States Parties shall seek to conclude bilateral and multilateral agreements or arrangements to carry out or to enhance the effectiveness of extradition.

Article 38: Transfer of sentenced persons

States Parties may, taking into consideration the rights of sentenced persons, consider entering into bilateral or multilateral agreements or arrangements on the transfer to their territory of persons sentenced to imprisonment or other forms of deprivation of liberty for offences established in accordance with this Convention, in order that they may complete their sentences there. States Parties may also take into account issues relating to consent, rehabilitation and reintegration.

Article 39: Transfer of criminal proceedings

1. States Parties shall consider the possibility of transferring to one another proceedings for the criminal prosecution of an offence established in accordance with this Convention where such a transfer is deemed to be in the interests of the proper administration of justice, particularly in cases where several jurisdictions are involved, with a view to concentrating the prosecution.

2. If a State Party that makes the transfer of criminal proceedings conditional on the existence of a treaty receives a request for transfer from another State Party with which it has no treaty in this matter, it may consider this Convention as the legal basis for the transfer of criminal proceedings in respect of any offence to which this article applies.

Article 40: General principles and procedures relating to mutual legal assistance

1. States Parties shall afford one another the widest measure of mutual legal assistance in investigations, prosecutions and judicial proceedings in relation to the offences established in accordance with this Convention, and for the purposes of the collection of evidence in electronic form of offences established in accordance with this Convention, as well as of serious crimes.

2. Mutual legal assistance shall be afforded to the fullest extent possible under relevant laws, treaties, agreements and arrangements of the requested State Party with respect to investigations, prosecutions and judicial proceedings in relation to the offences for which a legal person may be held liable in accordance with article 18 of this Convention in the requesting State Party.

3. Mutual legal assistance to be afforded in accordance with this article may be requested for any of the following purposes:

(a) Taking evidence or statements from persons;

(b) Effecting service of judicial documents;

(c) Executing searches and seizures, and freezing;

(d) Searching or similarly accessing, seizing or similarly securing, and disclosing electronic data stored by means of an information and communications technology system pursuant to article 44 of this Convention;

(e) Collecting traffic data in real time pursuant to article 45 of this Convention;

(f) Intercepting content data pursuant to article 46 of this Convention;

(g) Examining objects and sites;

(h) Providing information, evidence and expert evaluations;

(i) Providing originals or certified copies of relevant documents and records, including government, bank, financial, corporate or business records;

(j) Identifying or tracing proceeds of crime, property, instrumentalities or other things for evidentiary purposes;

(k) Facilitating the voluntary appearance of persons in the requesting State Party

(l) Recovering proceeds of crime;

(m) Any other type of assistance that is not contrary to the domestic law of the requested State Party.

4. Without prejudice to domestic law, the competent authorities of a State Party may, without prior request, transmit information relating to criminal matters to a competent authority in another State Party where they believe that such information could assist the authority in undertaking or successfully concluding inquiries and criminal proceedings or could result in a request formulated by the latter State Party pursuant to this Convention.

5. The transmission of information pursuant to paragraph 4 of this article shall be without prejudice to inquiries and criminal proceedings in the State of the competent authorities providing the information. The competent authorities receiving the information shall comply with a request that said information remain confidential, even temporarily, or with restrictions on its use. However, this shall not prevent the receiving State Party from disclosing in its proceedings information that is exculpatory to an accused person. In such a case, the receiving State Party shall notify the transmitting State Party prior to the disclosure and, if so requested, consult with the transmitting State Party. If, in an exceptional case, advance notice is not possible, the receiving State Party shall inform the transmitting State Party of the disclosure without delay.

6. The provisions of this article shall not affect obligations under any other treaty, bilateral or multilateral, that governs or will govern, in whole or in part, mutual legal assistance.

7. Paragraphs 8 to 31 of this article shall apply to requests made pursuant to this article if the States Parties in question are not bound by a treaty on mutual legal assistance. If those States Parties are bound by such a treaty, the corresponding provisions of that treaty shall apply unless the States Parties agree to apply paragraphs 8 to 31 of this article in lieu thereof. States Parties are strongly encouraged to apply the provisions of those paragraphs if they facilitate cooperation.

8. States Parties may decline to render assistance pursuant to this article on the ground of absence of dual criminality. However, the requested State Party may, when it deems appropriate, provide assistance, to the extent it decides at its discretion, irrespective of whether the conduct would constitute an offence under the domestic law of the requested State Party. Assistance may be refused when requests involve matters of a de minimis nature or matters for which the cooperation or assistance sought is available under other provisions of this Convention.

9. A person who is being detained or is serving a sentence in the territory of one State Party and whose presence in another State Party is requested for purposes of identification, testimony or otherwise providing assistance in obtaining evidence for investigations, prosecutions or judicial proceedings in relation to offences established in accordance with this Convention may be transferred if the following conditions are met:

(a) The person freely gives informed consent;

(b) The competent authorities of both States Parties agree, subject to such conditions as those States Parties may deem appropriate.

10. For the purposes of paragraph 9 of this article:

(a) The State Party to which the person is transferred shall have the authority and obligation to keep the person transferred in custody, unless otherwise requested or authorized by the State Party from which the person was transferred;

(b) The State Party to which the person is transferred shall, without delay, implement its obligation to return the person to the custody of the State Party from which the person was transferred as agreed beforehand, or as otherwise agreed, by the competent authorities of both States Parties;

(c) The State Party to which the person is transferred shall not require the State Party from which the person was transferred to initiate extradition proceedings for the return of the person;

(d) The person transferred shall receive credit for service of the sentence being served in the State from which the person was transferred for time spent in the custody of the State Party to which the person was transferred.

11. Unless the State Party from which a person is to be transferred in accordance with paragraphs 9 and 10 of this article so agrees, that person, regardless of the person's nationality, shall not be prosecuted, detained, punished or subjected to any other restriction of liberty in the territory of the State to which that person is transferred in respect of acts, omissions or convictions prior to the person's departure from the territory of the State from which the person was transferred.

12. (a) Each State Party shall designate a central authority or authorities that shall have the responsibility and power to receive requests for mutual legal assistance and either to execute them or to transmit them to the competent authorities for execution. Where a State Party has a special region or territory with a separate system of mutual legal assistance, it may designate a distinct central authority that shall have the same function for that region or territory;

(b) Central authorities shall ensure the speedy and proper execution or transmission of the requests received. Where the central authority transmits the request to a competent authority for execution, it shall encourage the speedy and proper execution of the request by the competent authority;

(c) The Secretary-General of the United Nations shall be notified of the central authority designated for this purpose at the time each State Party deposits its instrument of ratification, acceptance or approval of or accession to this Convention, and shall set up and keep updated a register of central authorities designated by the States Parties. Each State Party shall ensure that the details held in the register are correct at all times;

(d) Requests for mutual legal assistance and any communication related thereto shall be transmitted to the central authorities designated by the States Parties. This requirement shall be without prejudice to the right of a State Party to require that such requests and communications be addressed to it through diplomatic channels and, in urgent circumstances, where the States Parties agree, through the International Criminal Police Organization, if possible.

13. Requests shall be made in writing or, where possible, by any means capable of producing a written record, in a language acceptable to the requested State Party, under conditions allowing that State Party to establish authenticity. The Secretary-General of the United Nations shall be notified of the language or languages acceptable to each State Party at the time it deposits its instrument of ratification, acceptance or approval of or accession to this Convention. In urgent circumstances and

where agreed by the States Parties, requests may be made orally, but shall be confirmed in writing forthwith.

14. Where not prohibited by their respective laws, central authorities of States Parties are encouraged to transmit and receive requests for mutual legal assistance, and communications related thereto, as well as evidence, in electronic form under conditions allowing the requested State Party to establish authenticity and ensuring the security of communications.

15. A request for mutual legal assistance shall contain:

(a) The identity of the authority making the request;

(b) The subject matter and nature of the investigation, prosecution or judicial proceeding to which the request relates and the name and functions of the authority conducting the investigation, prosecution or judicial proceeding;

(c) A summary of the relevant facts, except in relation to requests for the purpose of service of judicial documents;

(d) A description of the assistance sought and details of any particular procedure that the requesting State Party wishes to be followed;

(e) Where possible and appropriate, the identity, location and nationality of any person concerned, as well as the country of origin, description and location of any item or accounts concerned;

(f) Where applicable, the time period for which the evidence, information or other assistance is sought; and

(g) The purpose for which the evidence, information or other assistance is sought.

16. The requested State Party may request additional information when it appears necessary for the execution of the request in accordance with its domestic law or when it can facilitate such execution.

17. A request shall be executed in accordance with the domestic law of the requested State Party and, to the extent not contrary to the domestic law of the requested State Party and where possible, in accordance with the procedures specified in the request.

18. Wherever possible and consistent with fundamental principles of domestic law, when an individual is in the territory of a State Party and has to be heard as a witness, victim or expert by the judicial authorities of another State Party, the first State Party may, at the request of the other, permit the hearing to take place by videoconference if it is not possible or desirable for the individual in question to appear in person in the territory of the requesting State Party. States Parties may agree that the hearing shall be conducted by a judicial authority of the requesting State Party and attended by a judicial authority of the requested State Party. If the requested State Party does not have access to the technical means necessary for holding a videoconference, such means may be provided by the requesting State Party, upon mutual agreement.

19. The requesting State Party shall not transmit or use information or evidence furnished by the requested State Party for investigations, prosecutions or judicial proceedings other than those stated in the request without the prior consent of the requested State Party. Nothing in this paragraph shall prevent the requesting State Party from disclosing in its proceedings information or evidence that is exculpatory to an accused person. In the latter case, the requesting State Party shall notify the

requested State Party prior to the disclosure and, if so requested, consult with the requested State Party. If, in an exceptional case, advance notice is not possible, the requesting State Party shall inform the requested State Party of the disclosure without delay.

20. The requesting State Party may require that the requested State Party keep confidential the fact and substance of the request, except to the extent necessary to execute the request. If the requested State Party cannot comply with the requirement of confidentiality, it shall promptly inform the requesting State Party.

21. Mutual legal assistance may be refused:

(a) If the request is not made in conformity with the provisions of this article;

(b) If the requested State Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests;

(c) If the authorities of the requested State Party would be prohibited by its domestic law from carrying out the action requested with regard to any similar offence, had it been subject to investigation, prosecution or judicial proceedings under their own jurisdiction;

(d) If it would be contrary to the legal system of the requested State Party relating to mutual legal assistance for the request to be granted.

22. Nothing in this Convention shall be interpreted as imposing an obligation to afford mutual legal assistance if the requested State Party has substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, language, religion, nationality, ethnic origin or political opinions, or that compliance with the request would cause prejudice to that person's position for any one of these reasons.

23. States Parties may not refuse a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.

24. States Parties shall not decline to render mutual legal assistance pursuant to this article on the ground of bank secrecy.

25. Reasons shall be given for any refusal of mutual legal assistance.

26. The requested State Party shall execute the request for mutual legal assistance as soon as possible and shall take as full account as possible of any deadlines suggested by the requesting State Party and for which reasons are given, preferably in the request. The requested State Party shall respond to reasonable requests by the requesting State Party on the status, and progress in its handling, of the request. The requesting State Party shall promptly inform the requested State Party when the assistance sought is no longer required.

27. Mutual legal assistance may be postponed by the requested State Party on the ground that it interferes with an ongoing investigation, prosecution or judicial proceeding.

28. Before refusing a request pursuant to paragraph 21 of this article or postponing its execution pursuant to paragraph 27 of this article, the requested State Party shall consult with the requesting State Party to consider whether assistance may be granted subject to such terms and conditions as it deems necessary. If the requesting State Party accepts assistance subject to those conditions, it shall comply with the conditions.

29. Without prejudice to the application of paragraph 11 of this article, a witness, expert or other person who, at the request of the requesting State Party, consents to give evidence in a proceeding or to assist in an investigation, prosecution or judicial proceeding in the territory of the requesting State Party shall not be prosecuted, detained, punished or subjected to any other restriction of the person's liberty in that territory in respect of acts, omissions or convictions prior to the person's departure from the territory of the requested State Party. Such safe conduct shall cease when the witness, expert or other person having had, for a period of 15 consecutive days or for any period agreed upon by the States Parties from the date on which the person has been officially informed that the presence of the person is no longer required by the judicial authorities, an opportunity of leaving, has nevertheless remained voluntarily in the territory of the requesting State Party or, having left it, has returned of the person's own free will.

30. The ordinary costs of executing a request shall be borne by the requested State Party, unless otherwise agreed by the States Parties concerned. If expenses of a substantial or extraordinary nature are or will be required to fulfil the request, the States Parties shall consult to determine the terms and conditions under which the request will be executed, as well as the manner in which the costs shall be borne.

31. The requested State Party:

(a) Shall provide to the requesting State Party copies of government records, documents or information in its possession that under its domestic law are available to the general public;

(b) May, at its discretion, provide to the requesting State Party, in whole, in part or subject to such conditions as it deems appropriate, copies of any government records, documents or information in its possession that under its domestic law are not available to the general public.

32. States Parties shall consider, as may be necessary, the possibility of concluding bilateral or multilateral agreements or arrangements that would serve the purposes of, give practical effect to or enhance the provisions of this article.

Article 41: 24/7 network

1. Each State Party shall designate a point of contact available 24 hours a day, 7 days a week, in order to ensure the provision of immediate assistance for the purpose of specific criminal investigations, prosecutions or judicial proceedings concerning offences established in accordance with this Convention, or for the collection, obtaining and preservation of evidence in electronic form for the purposes of paragraph 3 of this article and in relation to the offences established in accordance with this Convention, as well as to serious crime.

2. The Secretary-General of the United Nations shall be notified of such point of contact and keep an updated register of points of contact designated for the purposes of this article and shall annually circulate to the States Parties the updated list of contact points.

3. Such assistance shall include facilitating or, if permitted by the domestic law and practice of the requested State Party, directly carrying out the following measures:

(a) The provision of technical advice;

(b) The preservation of stored electronic data pursuant to articles 42 and 43 of this Convention, including, as appropriate, information about the location of the service provider, if known to the requested State Party, to assist the requesting State Party in making a request;

(c) The collection of evidence and the provision of legal information;

(d) The locating of suspects; or

(e) The provision of electronic data to avert an emergency.

4. A State Party's point of contact shall have the capacity to carry out communications with the point of contact of another State Party on an expedited basis. If the point of contact designated by a State Party is not part of that State Party's authority or authorities responsible for mutual legal assistance or extradition, the point of contact shall ensure that it is able to coordinate with that authority or those authorities on an expedited basis.

5. Each State Party shall ensure that trained and equipped personnel are available to ensure the operation of the 24/7 network.

6. States Parties may also use and strengthen existing authorized networks of points of contact, where applicable, and within the limits of their domestic laws, including the 24/7 networks for computer-related crime of the International Criminal Police Organization for prompt police-to-police cooperation and other methods of information exchange cooperation.

Article 42: International cooperation for the purpose of expedited preservation of stored electronic data

1. A State Party may request another State Party to order or otherwise obtain, in accordance with article 25 of this Convention, the expeditious preservation of electronic data stored by means of an information and communications technology system located within the territory of that other State Party, and in respect of which the requesting State Party intends to submit a request for mutual legal assistance in the search or similar access, seizure or similar securing, or disclosure of the electronic data.

2. The requesting State Party may use the 24/7 network provided for in article 41 of this Convention to seek information concerning the location of the electronic data stored by means of an information and communications technology system and, as appropriate, information about the location of the service provider.

3. A request for preservation made under paragraph 1 of this article shall specify:

(a) The authority seeking the preservation;

(b) The offence that is the subject of a criminal investigation, prosecution or judicial proceeding and a brief summary of the related facts;

(c) The stored electronic data to be preserved and their relationship to the offence;

(d) Any available information identifying the custodian of the stored electronic data or the location of the information and communications technology system;

(e) The necessity of the preservation;

(f) That the requesting State Party intends to submit a request for mutual legal assistance in the search or similar access, seizure or similar securing, or disclosure of the stored electronic data;

(g) As appropriate, the need to keep the request for preservation confidential and not to notify the user.

4. Upon receiving the request from another State Party, the requested State Party shall take all appropriate measures to preserve expeditiously the specified electronic data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition for providing such preservation.

5. A State Party that requires dual criminality as a condition for responding to a request for mutual legal assistance in the search or similar access, seizure or similar securing, or disclosure of stored electronic data may, in respect of offences other than those established in accordance with this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that, at the time of disclosure, the condition of dual criminality could not be fulfilled.

6. In addition, a request for preservation may be refused only on the basis of the grounds contained in article 40, paragraph 21 (b) and (c) and paragraph 22, of this Convention.

7. Where the requested State Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting State Party's investigation, it shall promptly so inform the requesting State Party, which shall then determine whether the request should nevertheless be executed.

8. Any preservation effected in response to a request made pursuant to paragraph 1 of this article shall be for a period of not less than 60 days, in order to enable the requesting State Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

9. Before the expiry of the preservation period in paragraph 8 of this article, the requesting State Party may request an extension of the period of preservation.

Article 43: International cooperation for the purpose of expedited disclosure of preserved traffic data

1. Where, in the course of the execution of a request made pursuant to article 42 of this Convention to preserve traffic data concerning a specific communication, the requested State Party discovers that a service provider in another State Party was involved in the transmission of the communication, the requested State Party shall expeditiously disclose to the requesting State Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2. Disclosure of traffic data under paragraph 1 of this article may be refused only on the basis of the grounds contained in article 40, paragraph 21 (b) and (c) and paragraph 22, of this Convention.

Article 44: Mutual legal assistance in accessing stored electronic data

1. A State Party may request another State Party to search or similarly access, seize or similarly secure, and disclose electronic data stored by means of an information and communications technology system located within the territory of the requested State Party, including electronic data that have been preserved pursuant to article 42 of this Convention.

2. The requested State Party shall respond to the request through the application of relevant international instruments and laws referred to in article 35 of this Convention, and in accordance with other relevant provisions of this chapter.

3. The request shall be responded to on an expedited basis where:

(a) There are grounds to believe that the relevant data are particularly vulnerable to loss or modification; or

(b) The instruments and laws referred to in paragraph 2 of this article otherwise provide for expedited cooperation.

Article 45: Mutual legal assistance in the real-time collection of traffic data

1. States Parties shall endeavour to provide mutual legal assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of an information and communications technology system. Subject to the provisions of paragraph 2 of this article, such assistance shall be governed by the conditions and procedures provided for under domestic law.

2. Each State Party shall endeavour to provide such assistance at least with respect to criminal offences for which the real-time collection of traffic data would be available in a similar domestic case.

3. A request made in accordance with paragraph 1 of this article shall specify:

(a) The name of the requesting authority;

(b) A summary of the main facts and the nature of the investigation, prosecution or judicial proceeding to which the request relates;

(c) The electronic data in relation to which the collection of the traffic data is required and their relationship to the offence;

(d) Any available data that identify the owner or user of the data or the location of the information and communications technology system;

(e) Justification for the need to collect the traffic data;

(f) The period for which traffic data are to be collected and a corresponding justification of its duration.

Article 46: Mutual legal assistance in the interception of content data

States Parties shall endeavour to provide mutual legal assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of an information and communications technology system, to the extent permitted under treaties applicable to them or under their domestic laws.

Article 47: Law enforcement cooperation

1. States Parties shall cooperate closely with one another, consistent with their respective domestic legal and administrative systems, to enhance the effectiveness of law enforcement action to combat the offences established in accordance with this Convention. States Parties shall, in particular, take effective measures:

(a) To enhance and, where necessary, to establish channels of communication between their competent authorities, agencies and services, taking into account existing channels, including those of the International Criminal Police Organization, in order to facilitate the secure and rapid exchange of information concerning all aspects of the offences established in accordance with this

Convention, including, if the States Parties concerned deem it appropriate, links with other criminal activities;

(b) To cooperate with other States Parties in conducting inquiries with respect to offences established in accordance with this Convention concerning:

(i) The identity, whereabouts and activities of persons suspected of involvement in such offences or the location of other persons concerned;

(ii) The movement of proceeds of crime or property derived from the commission of such offences;

(iii) The movement of property, equipment or other instrumentalities used or intended for use in the commission of such offences;

(c) To provide, where appropriate, necessary items or data for analytical or investigative purposes;

(d) To exchange, where appropriate, information with other States Parties concerning specific means and methods used to commit the offences established in accordance with this Convention, including the use of false identities, forged, altered or false documents and other means of concealing activities, as well as cybercrime tactics, techniques and procedures;

(e) To facilitate effective coordination between their competent authorities, agencies and services and to promote the exchange of personnel and other experts, including, subject to bilateral agreements or arrangements between the States Parties concerned, the posting of liaison officers;

(f) To exchange information and coordinate administrative and other measures taken, as appropriate, for the purpose of early identification of the offences established in accordance with this Convention.

2. With a view to giving effect to this Convention, States Parties shall consider entering into bilateral or multilateral agreements or arrangements on direct cooperation between their law enforcement agencies and, where such agreements or arrangements already exist, amending them. In the absence of such agreements or arrangements between the States Parties concerned, the States Parties may consider this Convention to be the basis for mutual law enforcement cooperation in respect of the offences established in accordance with this Convention. Whenever appropriate, States Parties shall make full use of agreements or arrangements, including international or regional organizations, to enhance the cooperation between their law enforcement agencies.

Article 48: Joint investigations

States Parties shall consider concluding bilateral or multilateral agreements or arrangements whereby, in relation to offences established in accordance with this Convention that are the subject of criminal investigations, prosecutions or judicial proceedings in one or more States, the competent authorities concerned may establish joint investigative bodies. In the absence of such agreements or arrangements, joint investigations may be undertaken by agreement on a case-by-case basis. The States Parties involved shall ensure that the sovereignty of the State Party in whose territory such investigations are to take place is fully respected.

Article 49: Mechanisms for the recovery of property through international cooperation in confiscation

1. Each State Party, in order to provide mutual legal assistance pursuant to article 50 of this Convention with respect to property acquired through or involved in the commission of an offence established in accordance with this Convention, shall, in accordance with its domestic law:

(a) Take such measures as may be necessary to permit its competent authorities to give effect to an order of confiscation issued by a court of another State Party;

(b) Take such measures as may be necessary to permit its competent authorities, where they have jurisdiction, to order the confiscation of such property of foreign origin by adjudication of an offence of money-laundering or such other offence as may be within its jurisdiction or by other procedures authorized under its domestic law; and

(c) Consider taking such measures as may be necessary to allow confiscation of such property without a criminal conviction in cases in which the offender cannot be prosecuted by reason of death, flight or absence or in other appropriate cases.

2. Each State Party, in order to provide mutual legal assistance upon a request made pursuant to article 50, paragraph 2, of this Convention, shall, in accordance with its domestic law:

(a) Take such measures as may be necessary to permit its competent authorities to freeze or seize property upon a freezing or seizure order issued by a court or competent authority of a requesting State Party that provides a reasonable basis for the requested State Party to believe that there are sufficient grounds for taking such actions and that the property would eventually be subject to an order of confiscation for the purposes of paragraph 1 (a) of this article;

(b) Take such measures as may be necessary to permit its competent authorities to freeze or seize property upon a request that provides a reasonable basis for the requested State Party to believe that there are sufficient grounds for taking such actions and that the property would eventually be subject to an order of confiscation for the purposes of paragraph 1 (a) of this article; and

(c) Consider taking additional measures to permit its competent authorities to preserve property for confiscation, such as on the basis of a foreign arrest or criminal charge related to the acquisition of such property.

Article 50: International cooperation for the purposes of confiscation

1. A State Party that has received a request from another State Party having jurisdiction over an offence established in accordance with this Convention for the confiscation of proceeds of crime, property, equipment or other instrumentalities referred to in article 31, paragraph 1, of this Convention situated in its territory shall, to the greatest extent possible within its domestic legal system:

(a) Submit the request to its competent authorities for the purpose of obtaining an order of confiscation and, if such an order is granted, give effect to it; or

(b) Submit to its competent authorities, with a view to giving effect to it to the extent requested, an order of confiscation issued by a court in the territory of the requesting State Party in accordance with article 31, paragraph 1, of this Convention insofar as it relates to proceeds of crime, property, equipment or other instrumentalities situated in the territory of the requested State Party.

2. Following a request made by another State Party having jurisdiction over an offence established in accordance with this Convention, the requested State Party shall take measures to identify, trace

and freeze or seize proceeds of crime, property, equipment or other instrumentalities referred to in article 31, paragraph 1, of this Convention for the purpose of eventual confiscation to be ordered either by the requesting State Party or, pursuant to a request under paragraph 1 of this article, by the requested State Party.

3. The provisions of article 40 of this Convention are applicable, mutatis mutandis, to this article. In addition to the information specified in article 40, paragraph 15, of this Convention, requests made pursuant to this article shall contain:

(a) In the case of a request pertaining to paragraph 1 (a) of this article, a description of the property to be confiscated, including, to the extent possible, the location, and where relevant, the estimated value of the property and a statement of the facts relied upon by the requesting State Party sufficient to enable the requested State Party to seek the order under its domestic law;

(b) In the case of a request pertaining to paragraph 1 (b) of this article, a legally admissible copy of an order of confiscation upon which the request is based issued by the requesting State Party, a statement of the facts and information as to the extent to which execution of the order is requested, a statement specifying the measures taken by the requesting State Party to provide adequate notification to bona fide third parties and to ensure due process, and a statement that the confiscation order is final;

(c) In the case of a request pertaining to paragraph 2 of this article, a statement of the facts relied upon by the requesting State Party and a description of the actions requested and, where available, a legally admissible copy of an order on which the request is based.

4. The decisions or actions provided for in paragraphs 1 and 2 of this article shall be taken by the requested State Party in accordance with and subject to the provisions of its domestic law and its procedural rules or any bilateral or multilateral treaty, agreement or arrangement to which it may be bound in relation to the requesting State Party.

5. Each State Party shall furnish copies of its laws and regulations that give effect to this article and of any subsequent changes to such laws and regulations or a description thereof to the Secretary-General of the United Nations.

6. If a State Party elects to make the taking of the measures referred to in paragraphs 1 and 2 of this article conditional on the existence of a relevant treaty, that State Party shall consider this Convention the necessary and sufficient treaty basis.

7. Cooperation under this article may also be refused or provisional measures may be lifted if the requested State Party does not receive sufficient and timely evidence or if the property is of a de minimis value.

8. Before lifting any provisional measure taken pursuant to this article, the requested State Party shall, wherever possible, give the requesting State Party an opportunity to present its reasons in favour of continuing the measure.

9. The provisions of this article shall not be construed as prejudicing the rights of bona fide third parties.

10. States Parties shall consider concluding bilateral or multilateral treaties, agreements or arrangements to enhance the effectiveness of international cooperation undertaken pursuant to this article.

Article 51: Special cooperation

Without prejudice to its domestic law, each State Party shall endeavour to take measures to permit it to forward, without prejudice to its own criminal investigations, prosecutions or judicial proceedings, information on proceeds of offences established in accordance with this Convention to another State Party without prior request, when it considers that the disclosure of such information might assist the receiving State Party in initiating or carrying out criminal investigations, prosecutions or judicial proceedings or might lead to a request by that State Party under article 50 of this Convention.

Article 52: Return and disposal of confiscated proceeds of crime or property

1. Proceeds of crime or property confiscated by a State Party pursuant to article 31 or 50 of this Convention shall be disposed of by that State Party in accordance with its domestic law and administrative procedures.

2. When acting on a request made by another State Party in accordance with article 50 of this Convention, States Parties shall, to the extent permitted by domestic law and if so requested, give priority consideration to returning the confiscated proceeds of crime or property to the requesting State Party so that it can give compensation to the victims of the crime or return such proceeds of crime or property to their prior legitimate owners.

3. When acting on a request made by another State Party in accordance with articles 31 and 50 of this Convention, a State Party may, after due consideration has been given to compensation of victims, give special consideration to concluding agreements or arrangements on:

(a) Contributing the value of such proceeds of crime or property or funds derived from the sale of such proceeds of crime or property or a part thereof to the account designated in accordance with article 56, paragraph 2 (c), of this Convention, and to intergovernmental bodies specializing in the fight against cybercrime;

(b) Sharing with other States Parties, on a regular or case-by-case basis, such proceeds of crime or property, or funds derived from the sale of such proceeds of crime or property, in accordance with its domestic law or administrative procedures.

4. Where appropriate, unless States Parties decide otherwise, the requested State Party may deduct reasonable expenses incurred in investigations, prosecutions or judicial proceedings leading to the return or disposition of confiscated property pursuant to this article.

Chapter VI: Preventive measures

Article 53: Preventive measures

1. Each State Party shall endeavour, in accordance with fundamental principles of its legal system, to develop and implement or maintain effective and coordinated policies and best practices to reduce existing or future opportunities for cybercrime through appropriate legislative, administrative or other measures.

2. Each State Party shall take appropriate measures, within its means and in accordance with fundamental principles of its domestic law, to promote the active participation of relevant individuals and entities outside the public sector, such as non-governmental organizations, civil

society organizations, academic institutions and private sector entities, as well as the general public, in the relevant aspects of prevention of the offences established in accordance with this Convention.

3. Preventive measures may include:

(a) Strengthening cooperation between law enforcement agencies or prosecutors and relevant individuals and entities outside the public sector, such as non-governmental organizations, civil society organizations, academic institutions and private sector entities for the purpose of addressing relevant aspects of preventing and combating the offences established in accordance with this Convention;

(b) Promoting public awareness regarding the existence, causes and gravity of the threat posed by the offences established in accordance with this Convention through public information activities, public education, media and information literacy programmes and curricula that promote public participation in preventing and combating such offences;

(c) Building and making efforts to increase the capacity of domestic criminal justice systems, including training and developing expertise among criminal justice practitioners, as part of national prevention strategies against the offences established in accordance with this Convention;

(d) Encouraging service providers to take effective measures, where feasible in the light of national circumstances and to the extent permitted by domestic law, to strengthen the security of the service providers' products, services and customers;

(e) Recognizing the contributions of the legitimate activities of security researchers when intended solely, and to the extent permitted and subject to the conditions prescribed by domestic law, to strengthen and improve the security of service providers' products, services and customers located within the territory of the State Party;

(f) Developing, facilitating and promoting programmes and activities in order to discourage those at risk of engaging in cybercrime from becoming offenders and to develop their skills in a lawful manner;

(g) Endeavouring to promote the reintegration into society of persons convicted of offences established in accordance with this Convention;

(h) Developing strategies and policies, in accordance with domestic law, to prevent and eradicate gender-based violence that occurs through the use of an information and communications technology system, as well as taking into consideration the special circumstances and needs of persons in vulnerable situations in developing preventive measures;

(i) Undertaking specific and tailored efforts to keep children safe online, including through education and training on and raising public awareness of child sexual abuse or child sexual exploitation online and through revising domestic legal frameworks and enhancing international cooperation aimed at its prevention, as well as making efforts to ensure the swift removal of child sexual abuse and child sexual exploitation material;

(j) Enhancing the transparency of and promoting the contribution of the public to decision-making processes and ensuring that the public has adequate access to information;

(k) Respecting, promoting and protecting the freedom to seek, receive and impart public information concerning cybercrime;

(l) Developing or strengthening support programmes for victims of the offences established in accordance with this Convention;

(m) Preventing and detecting transfers of proceeds of crime and property related to the offences established in accordance with this Convention.

4. Each State Party shall take appropriate measures to ensure that the relevant competent authority or authorities responsible for preventing and combating cybercrime are known and accessible to the public, where appropriate, for the reporting, including anonymously, of any incident that may be considered a criminal offence established in accordance with this Convention.

5. States Parties shall endeavour to periodically evaluate existing relevant national legal frameworks and administrative practices with a view to identifying gaps and vulnerabilities and ensuring their relevance in the face of changing threats posed by the offences established in accordance with this Convention.

6. States Parties may collaborate with each other and with relevant international and regional organizations in promoting and developing the measures referred to in this article. This includes participation in international projects aimed at the prevention of cybercrime.

7. Each State Party shall inform the Secretary-General of the United Nations of the name and address of the authority or authorities that may assist other States Parties in developing and implementing specific measures to prevent cybercrime.

Chapter VII: Technical assistance and information exchange

Article 54: Technical assistance and capacity-building

1. States Parties shall, according to their capacity, consider affording one another the widest measure of technical assistance and capacity-building, including training and other forms of assistance, the mutual exchange of relevant experience and specialized knowledge and the transfer of technology on mutually agreed terms, taking into particular consideration the interests and needs of developing States Parties, with a view to facilitating the prevention, detection, investigation and prosecution of the offences covered by this Convention.

2. States Parties shall, to the extent necessary, initiate, develop, implement or improve specific training programmes for their personnel responsible for the prevention, detection, investigation and prosecution of the offences covered by this Convention.

3. Activities referred to in paragraphs 1 and 2 of this article may deal, to the extent permitted by domestic law, with the following:

(a) Methods and techniques used in the prevention, detection, investigation and prosecution of the offences covered by this Convention;

(b) Building capacity in the development and planning of strategic policies and legislation to prevent and combat cybercrime;

(c) Building capacity in the collection, preservation and sharing of evidence, in particular in electronic form, including the maintenance of the chain of custody and forensic analysis;

(d) Modern law enforcement equipment and the use thereof;

(e) Training of competent authorities in the preparation of requests for mutual legal assistance and other means of cooperation that meet the requirements of this Convention, especially for the collection, preservation and sharing of evidence in electronic form;

(f) Prevention, detection and monitoring of the movements of proceeds deriving from the commission of the offences covered by this Convention, property, equipment or other instrumentalities and methods used for the transfer, concealment or disguise of such proceeds, property, equipment or other instrumentalities;

(g) Appropriate and efficient legal and administrative mechanisms and methods for facilitating the seizure, confiscation and return of proceeds of offences covered by this Convention;

(h) Methods used in the protection of victims and witnesses who cooperate with judicial authorities;

(i) Training in relevant substantive and procedural law, and law enforcement investigation powers, as well as in national and international regulations and in languages.

4. States Parties shall, subject to their domestic law, endeavour to leverage the expertise of and cooperate closely with other States Parties and relevant international and regional organizations, non-governmental organizations, civil society organizations, academic institutions and private sector entities, with a view to enhancing the effective implementation of this Convention.

5. States Parties shall assist one another in planning and implementing research and training programmes designed to share expertise in the areas referred to in paragraph 3 of this article, and to that end shall also, when appropriate, use regional and international conferences and seminars to promote cooperation and to stimulate discussion on problems of mutual concern.

6. States Parties shall consider assisting one another, upon request, in conducting evaluations, studies and research relating to the types, causes and effects of offences covered by this Convention committed in their respective territories, with a view to developing, with the participation of the competent authorities and relevant non-governmental organizations, civil society organizations, academic institutions and private sector entities, strategies and action plans to prevent and combat cybercrime.

7. States Parties shall promote training and technical assistance that facilitates timely extradition and mutual legal assistance. Such training and technical assistance may include language training, assistance with the drafting and handling of mutual legal assistance requests, and secondments and exchanges between personnel in central authorities or agencies with relevant responsibilities.

8. States Parties shall strengthen, to the extent necessary, efforts to maximize the effectiveness of technical assistance and capacity-building in international and regional organizations and in the framework of relevant bilateral and multilateral agreements or arrangements.

9. States Parties shall consider establishing voluntary mechanisms with a view to contributing financially to the efforts of developing countries to implement this Convention through technical assistance programmes and capacity-building projects.

10. Each State Party shall endeavour to make voluntary contributions to the United Nations Office on Drugs and Crime for the purpose of fostering, through the Office, programmes and projects with a view to implementing this Convention through technical assistance and capacity-building.

Article 55: Exchange of information

1. Each State Party shall consider analysing, as appropriate, in consultation with relevant experts, including from non-governmental organizations, civil society organizations, academic institutions and private sector entities, trends in its territory with respect to offences covered by this Convention, as well as the circumstances in which such offences are committed.

2. States Parties shall consider developing and sharing with each other and through international and regional organizations statistics, analytical expertise and information concerning cybercrime, with a view to developing, insofar as possible, common definitions, standards and methodologies, as well as best practices, to prevent and combat such crime.

3. Each State Party shall consider monitoring its policies and practical measures to prevent and combat offences covered by this Convention and making assessments of their effectiveness and efficiency.

4. States Parties shall consider exchanging information on legal, policy and technological developments related to cybercrime and the collection of evidence in electronic form.

Article 56: Implementation of the Convention through economic development and technical assistance

1. States Parties shall take measures conducive to the optimal implementation of this Convention to the extent possible, through international cooperation, taking into account the negative effects of the offences covered by this Convention on society in general and, in particular, on sustainable development.

2. States Parties are strongly encouraged to make concrete efforts, to the extent possible and in coordination with each other, as well as with international and regional organizations:

(a) To enhance their cooperation at various levels with other States Parties, in particular developing countries, with a view to strengthening their capacity to prevent and combat the offences covered by this Convention;

(b) To enhance financial and material assistance to support the efforts of other States Parties, in particular developing countries, in effectively preventing and combating the offences covered by this Convention and to help them to implement this Convention;

(c) To provide technical assistance to other States Parties, in particular developing countries, in support of meeting their needs regarding the implementation of this Convention. To that end, States Parties shall endeavour to make adequate and regular voluntary contributions to an account specifically designated for that purpose in a United Nations funding mechanism;

(d) To encourage, as appropriate, non-governmental organizations, civil society organizations, academic institutions and private sector entities, as well as financial institutions, to contribute to the efforts of States Parties, including in accordance with this article, in particular by providing more training programmes and modern equipment to developing countries in order to assist them in achieving the objectives of this Convention;

(e) To exchange best practices and information with regard to activities undertaken, with a view to improving transparency, avoiding duplication of effort and making best use of any lessons learned.

3. States Parties shall also consider using existing subregional, regional and international programmes, including conferences and seminars, to promote cooperation and technical assistance and to stimulate discussion on problems of mutual concern, including the special problems and needs of developing countries.

4. To the extent possible, States Parties shall ensure that resources and efforts are distributed and directed to support the harmonization of standards, skills, capacity, expertise and technical capabilities with the aim of establishing common minimum standards among States Parties to eradicate safe havens for the offences covered by this Convention and strengthen the fight against cybercrime.

5. To the extent possible, the measures taken under this article shall be without prejudice to existing foreign assistance commitments or to other financial cooperation arrangements at the bilateral, regional or international levels.

6. States Parties may conclude bilateral, regional or multilateral agreements or arrangements on material and logistical assistance, taking into consideration the financial arrangements necessary for the means of international cooperation provided for by this Convention to be effective and for the prevention, detection, investigation and prosecution of the offences covered by this Convention.

Chapter VIII: Mechanism of implementation

Article 57: Conference of the States Parties to the Convention

1. A Conference of the States Parties to the Convention is hereby established to improve the capacity of and cooperation between States Parties to achieve the objectives set forth in this Convention and to promote and review its implementation.

2. The Secretary-General of the United Nations shall convene the Conference of the States Parties not later than one year following the entry into force of this Convention. Thereafter, regular meetings of the Conference shall be held in accordance with the rules of procedure adopted by the Conference.

3. The Conference of the States Parties shall adopt rules of procedure and rules governing the activities set forth in this article, including rules concerning the admission and participation of observers, and the payment of expenses incurred in carrying out those activities. Such rules and related activities shall take into account principles such as effectiveness, inclusivity, transparency, efficiency and national ownership.

4. In establishing its regular meetings, the Conference of the States Parties shall take into account the time and location of the meetings of other relevant international and regional organizations and mechanisms in similar matters, including their subsidiary treaty bodies, consistent with the principles identified in paragraph 3 of this article.

5. The Conference of the States Parties shall agree upon activities, procedures and methods of work to achieve the objectives set forth in paragraph 1 of this article, including:

(a) Facilitating the effective use and implementation of this Convention, the identification of any problems thereof, as well as the activities carried out by States Parties under this Convention, including encouraging the mobilization of voluntary contributions;

(b) Facilitating the exchange of information on legal, policy and technological developments pertaining to the offences established in accordance with this Convention and the collection of evidence in electronic form among States Parties and relevant international and regional organizations, as well as non-governmental organizations, civil society organizations, academic institutions and private sector entities, in accordance with domestic law, as well as on patterns and trends in cybercrime and on successful practices for preventing and combating such offences;

(c) Cooperating with relevant international and regional organizations, as well as non-governmental organizations, civil society organizations, academic institutions and private sector entities;

(d) Making appropriate use of relevant information produced by other international and regional organizations and mechanisms for preventing and combating the offences established in accordance with this Convention, in order to avoid unnecessary duplication of work;

(e) Reviewing periodically the implementation of this Convention by its States Parties;

(f) Making recommendations to improve this Convention and its implementation as well as considering possible supplementation or amendment of the Convention;

(g) Elaborating and adopting supplementary protocols to this Convention on the basis of articles 61 and 62 of this Convention;

(h) Taking note of the technical assistance and capacity-building requirements of States Parties regarding the implementation of this Convention and recommending any action it may deem necessary in that respect.

6. Each State Party shall provide the Conference of the States Parties with information on legislative, administrative and other measures, as well as on its programmes, plans and practices, to implement this Convention, as required by the Conference. The Conference shall examine the most effective way of receiving and acting upon information, including, inter alia, information received from States Parties and from competent international and regional organizations. Inputs received from representatives of relevant non-governmental organizations, civil society organizations, academic institutions and private sector entities, duly accredited in accordance with procedures to be decided upon by the Conference, may also be considered.

7. For the purpose of paragraph 5 of this article, the Conference of the States Parties may establish and administer such review mechanisms as it considers necessary.

8. Pursuant to paragraphs 5 to 7 of this article, the Conference of the States Parties shall establish, if it deems necessary, any appropriate mechanisms or subsidiary bodies to assist in the effective implementation of the Convention.

Article 58: Secretariat

1. The Secretary-General of the United Nations shall provide the necessary secretariat services to the Conference of the States Parties to the Convention.

2. The secretariat shall:

(a) Assist the Conference of the States Parties in carrying out the activities set forth in this Convention and make arrangements and provide the necessary services for the sessions of the Conference as they pertain to this Convention;

(b) Upon request, assist States Parties in providing information to the Conference of the States Parties, as envisaged in this Convention; and

(c) Ensure the necessary coordination with the secretariats of relevant international and regional organizations.

Chapter IX: Final provisions

Article 59: Implementation of the Convention

1. Each State Party shall take the necessary measures, including legislative and administrative measures, in accordance with fundamental principles of its domestic law, to ensure the implementation of its obligations under this Convention.

2. Each State Party may adopt more strict or severe measures than those provided for by this Convention for preventing and combating the offences established in accordance with this Convention.

Article 60: Effects of the Convention

1. If two or more States Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly.

2. Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a State Party under international law.

Article 61: Relation with protocols

1. This Convention may be supplemented by one or more protocols.

2. In order to become a Party to a protocol, a State or a regional economic integration organization must also be a Party to this Convention.

3. A State Party to this Convention is not bound by a protocol unless it becomes a Party to the protocol in accordance with the provisions thereof.

4. Any protocol to this Convention shall be interpreted together with this Convention, taking into account the purpose of that protocol.

Article 62: Adoption of supplementary protocols

1. At least 60 States Parties shall be required before any supplementary protocol is considered for adoption by the Conference of the States Parties. The Conference shall make every effort to achieve consensus on any supplementary protocol. If all efforts at consensus have been exhausted and no agreement has been reached, the supplementary protocol shall, as a last resort, require for its adoption at least a two-thirds majority vote of the States Parties present and voting at the meeting of the Conference.

2. Regional economic integration organizations, in matters within their competence, shall exercise their right to vote under this article with a number of votes equal to the number of their member States that are Parties to this Convention. Such organizations shall not exercise their right to vote if their member States exercise theirs and vice versa.

Article 63: Settlement of disputes

1. States Parties shall endeavour to settle disputes concerning the interpretation or application of this Convention through negotiation or any other peaceful means of their own choice.

2. Any dispute between two or more States Parties concerning the interpretation or application of this Convention that cannot be settled through negotiation or other peaceful means within a reasonable time shall, at the request of one of those States Parties, be submitted to arbitration. If, six months after the date of the request for arbitration, those States Parties are unable to agree on the organization of the arbitration, any one of those States Parties may refer the dispute to the International Court of Justice by request in accordance with the Statute of the Court.

3. Each State Party may, at the time of signature, ratification, acceptance or approval of or accession to this Convention, declare that it does not consider itself bound by paragraph 2 of this article. The other States Parties shall not be bound by paragraph 2 of this article with respect to any State Party that has made such a reservation.

4. Any State Party that has made a reservation in accordance with paragraph 3 of this article may at any time withdraw that reservation by notification to the Secretary-General of the United Nations.

Article 64: Signature, ratification, acceptance, approval and accession

1. This Convention shall be open to all States for signature in Hanoi in 2025 and thereafter at United Nations Headquarters in New York until 31 December 2026.

2. This Convention shall also be open for signature by regional economic integration organizations, provided that at least one member State of such an organization has signed this Convention in accordance with paragraph 1 of this article.

3. This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary-General of the United Nations. A regional economic integration organization may deposit its instrument of ratification, acceptance or approval if at least one of its member States has done likewise. In that instrument of ratification, acceptance or approval, such organization shall declare the extent of its competence with respect to the matters governed by this Convention. Such organization shall also inform the depositary of any relevant modification in the extent of its competence.

4. This Convention is open for accession by any State or any regional economic integration organization of which at least one member State is a Party to this Convention. Instruments of accession shall be deposited with the Secretary-General of the United Nations. At the time of its accession, a regional economic integration organization shall declare the extent of its competence with respect to matters governed by this Convention. Such organization shall also inform the depositary of any relevant modification in the extent of its competence.

Article 65: Entry into force

1. This Convention shall enter into force on the ninetieth day after the date of deposit of the fortieth instrument of ratification, acceptance, approval or accession. For the purpose of this paragraph, any instrument deposited by a regional economic integration organization shall not be counted as additional to those deposited by member States of that organization.

2. For each State or regional economic integration organization ratifying, accepting, approving or acceding to this Convention after the deposit of the fortieth instrument of such action, this Convention shall enter into force on the thirtieth day after the date of deposit by such State or

organization of the relevant instrument or on the date on which this Convention enters into force pursuant to paragraph 1 of this article, whichever is later.

Article 66: Amendment

1. After the expiry of five years from the entry into force of this Convention, a State Party may propose an amendment and transmit it to the Secretary-General of the United Nations, who shall thereupon communicate the proposed amendment to the States Parties and to the Conference of the States Parties to the Convention for the purpose of considering and deciding on the proposal. The Conference shall make every effort to achieve consensus on each amendment. If all efforts at consensus have been exhausted and no agreement has been reached, the amendment shall, as a last resort, require for its adoption a two-thirds majority vote of the States Parties present and voting at the meeting of the Conference.

2. Regional economic integration organizations, in matters within their competence, shall exercise their right to vote under this article with a number of votes equal to the number of their member States that are Parties to this Convention. Such organizations shall not exercise their right to vote if their member States exercise theirs and vice versa.

3. An amendment adopted in accordance with paragraph 1 of this article is subject to ratification, acceptance or approval by States Parties.

4. An amendment adopted in accordance with paragraph 1 of this article shall enter into force in respect of a State Party 90 days after the date of the deposit with the Secretary-General of the United Nations of an instrument of ratification, acceptance or approval of such amendment.

5. When an amendment enters into force, it shall be binding on those States Parties that have expressed their consent to be bound by it. Other States Parties shall still be bound by the provisions of this Convention and any earlier amendments that they have ratified, accepted or approved.

Article 67: Denunciation

1. A State Party may denounce this Convention by written notification to the Secretary-General of the United Nations. Such denunciation shall become effective one year after the date of receipt of the notification by the Secretary-General.

2. A regional economic integration organization shall cease to be a Party to this Convention when all of its member States have denounced it.

3. Denunciation of this Convention in accordance with paragraph 1 of this article shall entail the denunciation of any protocols thereto.

Article 68: Depositary and languages

1. The Secretary-General of the United Nations is designated depositary of this Convention.

2. The original of this Convention, of which the Arabic, Chinese, English, French, Russian and Spanish texts are equally authentic, shall be deposited with the Secretary-General of the United Nations.