وزارة التعليم العالي والبحث العلمي

جامعة عباس لغرور – خنشلة -

كلية الحقوق والعلوم السياسية

تخصص: قانون جنائي

# الاستراتيجية الوطنية والدولية في مكافحة الجرائم المعلوماتية

بحث مقدم لاستكمال مقاييس شهادة الماستر في الحقوق

تخصص: قانون جنائي

من اعداد :

- **نوار دعـــاء**
- **جمبية حنين ملاك**

تحت اشراف الدكتور:

**- أ.د. خلاف بدرالدين**

**لجنة المناقشة:**

| اسم ولقب الأستاذ | الرتبة العلمية | الجامعة الأصلية | الصفة |
|---|---|---|---|
| عبابسة محمد | أستاذ التعليم العالي | جامعة عباس لغرور خنشلة | رئيسا |
| خلاف بدرالدين | أستاذ التعليم العالي | جامعة عباس لغرور خنشلة | مشرفا ومقررا |
| معمري عبد الرشيد | أستاذ محاضر – أ - | جامعة عباس لغرور خنشلة | عضوا ممتحنا |

**السنة الجامعية**

**2024/2025**

# الاهداء

الحمد لله وكفى والصلاة على الحبيب المصطفى وأهله ومن وفى أما بعد:

إلى من غرست في روحي حب الكفاح،

إلى أمي ...نبع الحنان، وسِرّ الصبر الجميل،

وإلى أبي ...معلمي الأول، وعنوان العزّة والبساطة والشهامة.

إلى إخوتي وأخواتي،

سندي الحقيقي في لحظات الانكسار،

ورفاق حلمي في كل المراحل.

إلى كل أستاذ آمن بي،

وإلى كل صديق وقف إلى جانبي في صمت أو في صوت.

إلى نفسي ...التي قاومت، وصبرت، وتجاوزت،

أهدي هذا العمل المتواضع عربون وفاء واعتراف بالجميل.

**دعاء / حنين ملاك**

# شكروعرفان

أتقدّم بأسمى آيات الشكر والعرفان إلى:

والديّ الحبيبين، اللذين كان دعمهما اللامحدود وتضحياتهما الملهمة خير دافعٍ لي في مواصلة هذا المسار البحثي.

أساتذتي الأفاضل في كلية الحقوق، اللذين لم يبخلوا عليّ بعلمهم وإرشادهم الثمين طوال مراحل إعداد هذه الدراسة.

زملائي وأصدقائي، الذين شاركوني الأفكار والآراء، ووقفوا إلى جانبي في لحظات التحدي، فكانوا خير سند وعون.

زميلتي في البحث، الذي تشاركت معها لحظات العمل والإنجاز، فغنّى روح التعاون المثمر بيننا.

وإلى كل من لم تذكر إسماً هنا، لكنه كان له أثرٌ إيجابي في تقديم الدعم النفسي أو المعلوماتي أو التقني، أخصّ بالشكر كل من ساندني بعطائه وصدقه.

هذا العرفان منا لكم أقل ما يمكن أن نقدّمه تعبيرًا عن امتناني ودعمي المتواصل.

# مقدمة

## تمهيد:

شهد العالم في العقود الأخيرة تطورًا هائلًا في مجال تكنولوجيا المعلومات والاتصالات، مما أدى إلى تحول جذري في مختلف مجالات الحياة، سواء الاقتصادية أو الاجتماعية أو السياسية. ومع هذا التطور، ظهرت تحديات جديدة تهدد أمن الأفراد والمؤسسات والدول، من بينها الجرائم المعلوماتية التي باتت تشكل خطرًا متزايدًا في العصر الرقمي.

تُعرف الجرائم المعلوماتية بأنها تلك الأفعال الإجرامية التي تُرتكب باستخدام التكنولوجيا الرقمية، وتشمل مجموعة واسعة من الجرائم مثل الاحتيال الإلكتروني، سرقة البيانات، الاختراقات الأمنية، نشر البرمجيات الخبيثة، والتجسس الإلكتروني. وما يميز هذه الجرائم عن الجرائم التقليدية هو طبيعتها غير المادية، سرعة انتشارها، وصعوبة تتبع مرتكبيها، مما يجعل مكافحتها تحديًا معقدًا يتطلب استراتيجيات متطورة وآليات قانونية حديثة.

وفي ظل تزايد التهديدات السيبرانية، تسعى الدول إلى وضع أطراف قانونية فعالة لمكافحة هذه الجرائم بالإضافة إلى تعزيز التعاون الدولي لمواجهتها بشكل أكثر كفاءة. وتعد الجزائر من بين الدول التي أدركت خطورة الجرائم المعلوماتية، فقامت بوضع تشريعات تهدف إلى مكافحتها والحد من آثارها السلبية على المجتمع والاقتصاد الوطني.

إن تنامي هذه الجرائم استدعى الحاجة إلى تطوير استراتيجيات فعّالة لمكافحتها، سواء على الصعيدين الوطني أو الدولي. وقد ظهرت العديد من المبادرات القانونية والتقنية لمواجهة هذا التحدي، لكن تظل هناك العديد من العقبات القانونية والتقنية التي تعيق جهود المكافحة، مما يفرض ضرورة البحث في هذا المجال وتطوير حلول مبتكرة لمواكبة التحديات المستجدة.

هذه الدراسة تهدف إلى تسليط الضوء على الأسس القانونية والتشريعية لمكافحة الجرائم المعلوماتية، مع التركيز على استراتيجيات الدول الغربية والعربية في التصدي لهذه الظاهرة. سنستعرض كذلك التحديات التي تواجه هذه الاستراتيجيات وسبل تعزيز التعاون الدولي لمكافحة الجرائم الرقمية بفعالية.

تهدف هذه الدراسة إلى تسليط الضوء على الجرائم المعلوماتية من خلال تناول إطارها النظري والقانوني واستعراض الاستراتيجيات والممارسات الفعالة لمواجهتها على المستويين الوطني والدولي. كما سيتناول البحث التحديات التي تواجه الجهود المبذولة في مكافحة هذه الجرائم، مع تقديم مقترحات لتعزيز الحماية السيبرانية وتحقيق أمن المعلومات في العصر الرقمي كما نأمل أن نتمكن من تقديم رؤى حول سُبل تعزيز

الجهود الدولية والوطنية لمكافحة الجرائم المعلوماتية، مما يساعد على بناء مجتمع رقمي آمن، قادر على حماية البيانات والمعلومات من التهديدات المتزايدة في عصر تكنولوجيا المعلومات.

- **أهمية البحث:**

تنبع أهمية موضوع الجرائم المعلوماتية من التحول الجذري الذي شهده العالم في العقود الأخيرة حيث أصبحت التكنولوجيا الرقمية جزءًا لا يتجزأ من الحياة اليومية، بل ومرتكزًا أساسياً في الأنشطة الاقتصادية، الاجتماعية، والإدارية. هذا التطور الهائل في استخدام تكنولوجيا المعلومات والاتصال، رغم ما يحمله من مزايا، أفرز في المقابل نمطاً جديداً من الجرائم يتميز بالتعقيد، والسرعة، وصعوبة التتبع.

إن الجرائم المعلوماتية لا تقتصر على مجرد أفعال احتيالية بسيطة، بل تشمل اختراق أنظمة الدولة، سرقة البيانات الحساسة، نشر المعلومات الكاذبة، وانتهاك الخصوصية، مما يجعلها تهديداً حقيقياً للأمن القومي والاستقرار الاقتصادي والاجتماعي .كما أن الطبيعة العابرة للحدود لهذه الجرائم تجعل من مكافحتها تحدياً يتطلب تعاوناً وطنياً ودولياً محكماً، فضلاً عن إطار قانوني وتشريعي متجدد ومتكيف مع المستجدات التقنية.

ومن هذا المنطلق، تبرز الحاجة إلى دراسة الجوانب القانونية، التقنية، والمؤسساتية المرتبطة بمكافحة هذه الظاهرة، من أجل اقتراح حلول فعالة واستراتيجيات متقدمة تساهم في تعزيز الأمن الرقمي وحماية الحقوق والحريات في البيئة الإلكترونية.

- **أهداف البحث:**

- تحليل الإطار المفاهيمي والقانوني للجريمة المعلوماتية، وتحديد خصائصها التي تميزها عن الجرائم التقليدية.
- رصد الاستراتيجيات الدولية المعتمدة من قبل المنظمات الدولية والدول الكبرى لمكافحة الجرائم المعلوماتية، ومدى فعاليتها.
- تسليط الضوء على الجهود الوطنية والإقليمية في مكافحة هذه الجرائم، ومدى مواءمتها للمعايير الدولية.
- تقييم آليات التعاون الدولي سواء القضائي أو الأمني أو التقني في مجال مكافحة الجرائم الإلكترونية مع إبراز التحديات التي تواجهه.
- دراسة بعض التجارب المقارنة في مجال مكافحة الجرائم المعلوماتية، لاستخلاص الدروس والاستفادة من الممارسات الجيدة.

- **أسباب اختيار البحث:**

**1. الأسباب الذاتية:**

- الاهتمام الشخصي وذلك يعود إلى اهتمامي الخاص بالمجال الرقمي والتكنولوجي، وما يطرحه من تحديات قانونية معاصرة تستحق الدراسة والتحليل.

- الرغبة في التخصص حيث يمثل مجال مكافحة الجرائم المعلوماتية أحد أكثر ميادين القانون تطوراً في العصر الحديث، ما يجعله مجالاً خصباً للبحث، ويفتح آفاقاً مستقبلية لمزيد من التعمق الأكاديمي والمهني.

**2. الأسباب الموضوعية:**

- حداثة الموضوع وأهميته حيث أن الجريمة المعلوماتية تُعد من الجرائم المستحدثة التي تطورت بتطور وسائل التكنولوجيا، ما يستوجب تحليلاً قانونياً حديثاً ومتجدداً لمواجهتها.
- القصور التشريعي والعملي ما زالت أغلب التشريعات، خصوصاً في الدول النامية، تعاني من نقص أو تأخر في مجاراة هذا النوع من الجرائم، سواء من حيث النصوص القانونية أو الإمكانيات التقنية والمؤسسية.

➢ **الدراسات السابقة:**

**أولا: الدراسات العربية**

تطرقت العديد من الدراسات العربية موضوع الجرائم المعلوماتية من زوايا متعددة، حيث شكّلت مرجعًا مهمًا لفهم السياقات القانونية والأمنية في المنطقة. من بين أبرز هذه الدراسات، نذكر دراسة عبد العزيز الفاضلي الموسومة بـ"الجرائم الإلكترونية في التشريع المقارن" (2015)، والتي اعتمدت المنهج التحليلي المقارن، وقارنت بين تشريعات الدول العربية (كالجزائر، مصر، والسعودية) وبعض الدول الغربية، مبيّنة أن معظم التشريعات العربية رغم وجودها، تعاني من ضعف في التعريفات القانونية الدقيقة وصلاحيات الجهات المختصة وآليات الإثبات، ما يجعلها مرجعًا مهمًا لتوجيه الإصلاحات القانونية.

**ثانيًا: الدراسات الأجنبية**

على الصعيد الدولي، تناولت مجموعة من الدراسات الأجنبية قضية الجرائم المعلوماتية بمنظور استراتيجي وتقني شامل، ما يُعد مرجعًا مهمًا للمقارنة مع التجارب العربية. من أبرز هذه الدراسات كتاب "Cybercriminalité : Défi mondial"الصادر عن مجموعة من الباحثين الفرنسيين، والذي اعتمد المنهج التحليلي المقارن، وركّز على استعراض التحديات العالمية المرتبطة بالجرائم السيبرانية، خاصة من حيث تنامي القدرات التقنية للمجرمين مقابل تباطؤ الاستجابة القانونية والتقنية، مشددًا على ضرورة التعاون الدولي وتوحيد الجهود عبر اتفاقيات ملزمة. كما جاءت دراسة "Cybercrime and Digital Forensics"لـ Thomas J. Holt وAdam M. Bossler وKathryn C. Seigfried-Spellar لتتناول من منظور أمريكي العلاقة بين الجريمة الإلكترونية وأدوات التحليل الجنائي الرقمي، مبينةً أهمية بناء قدرات تقنية متقدمة في صفوف المحققين والقضاة للتعامل مع هذا النوع من الجرائم.

**ثالثا: محل دراستنا من الدراسات السابقة**

من خلال استعراضنا للدراسات السابقة، سواء العربية أو الأجنبية، يتّضح أن غالبية الأدبيات ركّزت على الجانب القانوني أو الأمني المتعلق بالجرائم المعلوماتية كلٌّ على حدة، مع اهتمام جزئي بتحليل فعالية الاستراتيجيات المتبعة في مختلف الدول. إلا أن دراستنا الحالية تميّزت بمحاولة الجمع بين البعد القانوني، المؤسساتي، والتطبيقي، من خلال مقارنة الاستراتيجيات الجزائرية مع نظيراتها العربية والدولية، مع التركيز على مدى فاعليتها وتحديات تنفيذها. كما أن هذه الدراسة سعت إلى تجاوز الطابع الوصفي لبعض الدراسات السابقة عبر اعتماد منهج تحليلي نقدي يُبرز نقاط القوة والقصور، ويطرح توصيات واقعية قابلة للتطبيق في السياق الجزائري والعربي. وبهذا، تكتسب دراستنا راهنيتها وأهميتها من كونها تندرج ضمن الجهود البحثية القليلة التي تقارب الموضوع من زاوية تكاملية، تربط بين الإطار التشريعي، الواقع الميداني، والأبعاد الجيو–استراتيجية لمكافحة الجريمة المعلوماتية في ظل التطورات التكنولوجية المتسارعة.

- **صعوبات الدراسة:**

واجهت هذه الدراسة جملة من الصعوبات، سواء على الصعيد المنهجي أو العملي، من أبرزها:

- قلة المراجع المتخصصة باللغة العربية التي تناولت موضوع الاستراتيجية الدولية لمكافحة الجرائم المعلوماتية بشكل معمق، الأمر الذي تطلّب العودة إلى مراجع أجنبية وترجمتها وتحليلها.
- تشتّت النصوص القانونية ذات الصلة، حيث إن الإطار التشريعي المتعلق بالجرائم المعلوماتية متوزع بين قوانين مختلفة، (الجنائية، المدنية، قوانين الإعلام والاتصال) مما صعّب من عملية الإحاطة الشاملة بكل الجوانب القانونية.
- الطابع المتطور والديناميكي للجريمة المعلوماتية، والذي يفرض تحديًا مستمرًا للباحث في متابعة المستجدات التقنية والقانونية، خاصة في ظل التحولات الرقمية المتسارعة.
- ندرة الدراسات المقارنة الميدانية التي توثق تجارب الدول في الاستجابة لهذه الجرائم بشكل تطبيقي وهو ما حد من إمكانية التحليل الواقعي لبعض النماذج.

ورغم هذه التحديات، سعت الدراسة إلى تجاوزها بالاعتماد على مصادر متنوعة وتحليل معمّق لتحقيق الأهداف المرجوة.

- **الاشكالية:**

رغم الجهود الوطنية والدولية المبذولة في سبيل التصدي للجرائم المعلوماتية، سواء من خلال سنّ التشريعات أو إبرام الاتفاقيات أو إنشاء أجهزة متخصصة، إلا أن هذه الظاهرة ما تزال تتوسع وتتعقد بتطور التكنولوجيا، مما يثير تساؤلات قانونية وقضائية عميقة حول مدى كفاية الإطار التشريعي والمؤسساتي الحالي لمجابهتها.

كما تطرح هذه الجرائم تحديات من نوع خاص، سواء فيما يتعلق بإثباتها والتحقيق فيها، أو بتكييفها قانونياً، أو من حيث التعاون الدولي في تعقب مرتكبيها وجمع الأدلة الرقمية. هذا إلى جانب وجود تباين كبير بين التشريعات الوطنية وعدم توافقها أحياناً مع المعايير الدولية.

من هنا، تتمحور إشكالية هذه الدراسة في السؤال الرئيسي التالي:

**إلى أي مدى تمكن المشرع الجزائري من تبني استراتيجية وطنية فعالة في مواجهة الجرائم المعلوماتية بما يتماشى مع الاستراتيجيات الدولية في اطار ذلك؟**

وتتفرع عن هذه الإشكالية مجموعة من التساؤلات الفرعية، أبرزها:

- كيف عرف المشرع الجزائري الجريمة المعلوماتية؟
- كيف واجه المشرع الجزائري الجريمة المعلوماتية؟
- ما هي تجارب الدول الرائدة في مكافحة الجرائم المعلوماتية؟
- إلى أي مدى تمكنت بعض الدول من تبني استراتيجيات فعالة لكبح انتشار هذه الجرائم؟

- **المنهج المعتمد:**

اعتمدت هذه الدراسة في تناولها لموضوع "الاستراتيجية الدولية في مكافحة الجرائم المعلوماتية " على المنهج الوصفي التحليلي، وذلك من خلال تحليل النصوص القانونية الدولية والوطنية ذات الصلة ودراسة الآليات المؤسسية والاتفاقيات الدولية التي تؤطر التعاون في هذا المجال .كما تم الاستعانة بالمنهج المقارن لمقارنة التجارب الغربية والعربية في مكافحة هذه الجرائم، بهدف الوقوف على أهم أوجه التشابه والاختلاف، واستجلاء النماذج الناجحة منها، مع الاعتماد على المنهج التقريري المقارن من خلال وصف القوانين وأهم التشريعات والتعديلات و تحليل المعطيات، وباعتباره الأنسب لتحليل أوجه التشابه والاختلاف بين الاستراتيجيات الوطنية والدولية في مكافحة الجرائم المعلوماتية".

ولتحقيق أهداف الدراسة، تم تقسيم البحث إلى مجموعة من الفصول والمباحث التي تناولت الجريمة المعلوماتية من الناحية القانونية والتنظيمية، ثم الاستراتيجيات المتبعة دوليًا، وأخيرًا استعراض دراسات مقارنة لتجارب بعض الدول.

تعالج هذه الدراسة موضوع "الاستراتيجية الوطنية و الدولية في مكافحة الجرائم المعلوماتية" من خلال عرض شامل ومنظم عبر فصلين رئيسيين، في الفصل الأول، يتم استعراض الإطار المفاهيمي والقانوني للجرائم المعلوماتية، حيث يتم التطرق إلى تعريف الجريمة المعلوماتية، خصائصها، وأنواعها إضافة إلى دراسة الهيئات الوطنية المكلفة بمكافحتها .كما سيتم التطرق إلى الإطار الدولي لهذه الجرائم من خلال استعراض الاتفاقيات الدولية والهيئات المعنية على مستوى العالم.

أما في الفصل الثاني، فتركز الدراسة على الاستراتيجيات والممارسات الفعالة في مكافحة الجرائم المعلوماتية. سيتم التطرق إلى الركائز الأساسية لهذه الاستراتيجيات، بالإضافة إلى استعراض الاستراتيجية الدولية لمكافحة الجرائم المعلوماتية، والتعاون الدولي في هذا المجال. وفي المبحث الأخير، سيتم مقارنة استراتيجيات بعض الدول الغربية والعربية في مكافحة الجرائم المعلوماتية، وتحليل أفضل الممارسات المتبعة.

# الفصل الأول:

# الإطار النظري

# للجرائم المعلوماتية

**تمهيد:**

مع الانفجار الرقمي الذي يشهده العالم في العقود الأخيرة، أصبحت التكنولوجيا جزءاً لا يتجزأ من مختلف جوانب الحياة اليومية، سواء على المستوى الشخصي أو المؤسسي أو الحكومي. فقد ساهم هذا التحول الرقمي في تطوير الخدمات، وتيسير المعاملات، وتعزيز التواصل، إلا أنه في المقابل أوجد بيئة خصبة لنشوء نوع جديد من الجرائم ذات الطابع غير التقليدي، يُطلق عليها "الجرائم المعلوماتية" أو "الجرائم السيبرانية". وتكمن خطورة هذه الجرائم في أنها لا ترتبط بمكان جغرافي محدد، ولا تُقيدها حدود زمنية، كما أن مرتكبيها غالباً ما يكونون مجهولي الهوية ويستخدمون تقنيات متطورة تُعقّد من مسألة تتبعهم أو إثبات إدانتهم.

وعليه، سيتناول هذا الفصل الإطار النظري المتعلق بالجرائم المعلوماتية، من خلال الوقوف على تعريفها، وتصنيفاتها المختلفة بحسب الأهداف والوسائل المستخدمة، والخصائص التي تميزها عن الجرائم التقليدية. كما سيتم تسليط الضوء على أهم التقنيات التي يستغلها المجرمون في تنفيذ هذا النوع من الجرائم، مع تقديم لمحة تحليلية عن الإطار القانوني الوطني والدولي المُعتمد لمكافحتها، وذلك بهدف رسم صورة شاملة تساعد في فهم أعمق لجوهر المشكلة وتُسهم في بناء حلول فعّالة على المستويين التشريعي والتنفيذي.

سنتطرق خلال هذا الفصل الى:

- **المبحث الاول:** مفهوم الجرائم المعلوماتية
- **المبحث الثاني:** الاطار القانوني لمكافحة الجرائم المعلوماتية
- **المبحث الثالث:** الاطار الدولي لمكافحة الجرائم المعلوماتية

## المبحث الاول: مفهوم الجرائم المعلوماتية

ادى التطور السريع في مجال التكنولوجيا والاتصالات الى ظهور شكل جديد من الجرائم يختلف في طبيعته ووسائله عن الجرائم التقليدية، وهو مايعرف بالجرائم المعلوماتية فقد أصبحت الوسائط الرقمية، من حواسيب وهواتف ذكية وشبكات الإنترنت، أدوات تُستخدم ليس فقط في تبادل المعلومات بل أيضًا في ارتكاب أفعال غير مشروعة تمس الأفراد والمؤسسات والدول.

ومع تزايد الاعتماد على التكنولوجيا في مختلف مناحي الحياة، اتسعت رقعة هذه الجرائم وتنوعت أساليبها، الأمر الذي أوجد تحديات قانونية وأمنية كبيرة وفرض على الأنظمة القانونية ضرورة تطوير مفاهيمها ومناهجها لمواكبة هذا النوع المستحدث من الجرائم.

### المطلب الاول: ماهية الجريمة المعلوماتية

يقصد بالجرائم المعلوماتية تلك الأفعال غير المشروعة التي تُرتكب باستخدام نظم المعلومات أو الشبكات الإلكترونية، سواء باستهدافها أو باستخدامها كوسيلة. في هذا المطلب، سيتم تناول مفهوم الجرائم المعلوماتية بشكل مباشر، من خلال عرض أبرز التعريفات وبيان نطاقها القانوني.

#### الفرع الأول: تعريف عام للجريمة المعلوماتية

**1. التعريف الفقهي:**

لقد تعددت التعريفات عند الدراسين والفقهاء فيما يخص الجريمة المعلوماتية والتي تتميز وتتباين من موضع الى اخروقد جمعنا مجموعة من التعاريف وضعت في هذا الحقل.

فمن التعريفات التي تستند إلى موضوع الجريمة، نجد تعريف ROSENBALT بأنه نشاط غير مشروع موجه لنسخ أو تغير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقة.[1] أو هي كما عرفها الفقيه سوال روز: أي نمط من أنماط

[1] سمير شعبان، "**الجريمة الالكترونية، مقارنة تحليلية لتحديد مفهوم الجريمة والمجرم**"، جامعة باتنة، الجزائر، ص 115.

الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات، ومن هذه التعريفات:

تعريف الأستاذ "جون فورستر" فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية ويعرفها "تادمان" بأنها كل أشكال السلوك غير المشروع الذي يرتكب بواسطة الحاسب".

ونشير أيضا إلى أن جانبا من الفقه و المؤسسات ذات العلاقة بهذا الموضوع وضعت عددا من التعريفات التي تقوم على أساس سمات شخصية لدى مرتكب الفعل تعرف وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث و تبنتها الوزارة في دليلها لعام 1979 حيث عرفت الجريمة المعلوماتية على أنها أي جريمة لفاعلها معرفة فنية بالحاسبات تمكن من ارتكابها[1] .

كما عرفها الأستاذ دافيد "تومسن" أي جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها المعرفة بتقنية الحاسب الآلي[2].

**2. التعريف القانوني:**

عـرف المشـرع الجزائـري الجريمة المعلومـاتية فـي نص المـادة 02 –الفقرة أ – من القانون رقم 09–04 المؤرخ في 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها بالقول بأن الجرائم المتصلة بتكنولوجيات الاعلام والاتصال هي: جرائم المساس بأنظمة المعالجة الالية للمعطيات المحددة في قانون العقوبات أو أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية.

إذن وعملا بالتعاريف المقترحة للجريمة المعلوماتية، فإنه يمكننا اقتراح تعريف خاص يشمل كافة الجوانب "المتعلقة بالجريمة المعلوماتية فنعرفها بأنها كل السلوكات المجرمة التي يعتمد

[1] سمير شعبان، مرجع سابق، ص 116.

[2] عبد المؤمن بن صغير، "**الطبيعة الخاصة بالجريمة المرتكبة عبر الانترنت في التشريع الجزائري**"، الملتقى الوطني حول المعلوماتية بين الوقاية والمكافحة، المنعقد بجامعة بسكرة، 2015، ص 6.

مرتكبوها على الحاسوب وشبكات الاتصال، أي هي تلك الجرائم التي تقع على مستوى البيئة الرقمية.[1]

**الفرع الثاني: الفرق بين الجريمة التقليدية والجريمة المعلوماتية**

في ظل التطور التكنولوجي المتسارع، برزت الجرائم المعلوماتية كنوع جديد من الجرائم التي تعتمد على الوسائل الرقمية والأنظمة الإلكترونية، مما جعلها تختلف جذريًا عن الجرائم التقليدية التي تعتمد على الأساليب المادية. ورغم أن الهدف الأساسي لكلا النوعين هو الإضرار بالأفراد أو المؤسسات أو الدول إلا أن هناك فروقًا جوهرية بينهما من حيث الوسيلة، والمكان، وطريقة التنفيذ، والأثر، وآليات المكافحة.

**1. الاختلاف من حيث الوسيلة المستخدمة:**

- **الجرائم التقليدية:** ترتكب باستخدام أدوات ملموسة مثل الأسلحة، الأدوات الحادة المتفجرات، أو حتى الأيدي العارية.
- **الجرائم المعلوماتية:** ترتكب باستخدام الأجهزة الإلكترونية مثل الحواسيب، الهواتف الذكية، أو الشبكات الرقمية، مع الاعتماد على البرمجيات الخبيثة والتقنيات المتطورة.

**2. الاختلاف من حيث مكان ارتكاب الجريمة**

- **الجرائم التقليدية:** تحدث في أماكن مادية محددة مثل الشوارع، المنازل، البنوك، المتاجر وغيرها.
- **الجرائم المعلوماتية:** تُرتكب في الفضاء الإلكتروني دون الحاجة إلى تواجد المجرم في نفس موقع الضحية، مما يعقد مسألة تعقب الجاني[2].

**3. الاختلاف من حيث طبيعة الجاني**

- **الجرائم التقليدية:** غالبًا ما يكون الجاني معروفًا أو يمكن تحديد هويته بسهولة من خلال شهود العيان أو الأدلة المادية.

[1] سمير شعبان، مرجع سابق، ص 116.

[2] حكيم سياب، **"السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية"**، جامعة 20 أوت 1955، سكيكدة، ص 220.

- **الجرائم المعلوماتية:** يمكن أن يكون المجرم مجهول الهوية تمامًا، حيث يستخدم وسائل إخفاء الهوية مثل الشبكات الخاصة الافتراضية VPN، وتطبيقات تشفير البيانات والشبكات المظلمة Dark Web.

**4. الاختلاف من حيث الأدلة الجنائية**

- **الجرائم التقليدية:** تعتمد على الأدلة المادية مثل بصمات الأصابع، تسجيلات المراقبة شهود العيان والأسلحة المستخدمة.
- **الجرائم المعلوماتية:** تعتمد على الأدلة الرقمية مثل سجلات الدخول، عناوينIP، تحليل البيانات المخزنة على الأجهزة، وتتبع النشاط الإلكتروني للمجرم.

**5. الاختلاف من حيث نوع الضحايا**

- **الجرائم التقليدية:** تستهدف الأفراد أو الممتلكات بشكل مباشر، مثل جرائم القتل السرقة النصب، أو الاعتداءات الجسدية.
- **الجرائم المعلوماتية:** قد تستهدف أفرادًا، أو مؤسسات، أو حتى حكومات بأكملها، مثل الهجمات الإلكترونية التي تعطل أنظمة البنوك أو المؤسسات الأمنية.

**6. الاختلاف من حيث الأثر المترتب على الجريمة[1]**

- **الجرائم التقليدية:** ينتج عنها أضرار جسدية أو مادية واضحة مثل الإصابات، القتل، أو الخسائر المالية الفورية.
- **الجرائم المعلوماتية:** قد لا يكون لها أثر مادي مباشر، لكنها قد تؤدي إلى سرقة البيانات الشخصية وخسائر مالية ضخمة بسبب الاحتيال الإلكتروني، أو اختراق أنظمة حساسة تسبب أضرارًا اقتصادية وأمنية جسيمة.

**7. الاختلاف من حيث المكافحة القانونية والأمنية**

- **الجرائم التقليدية:** يتم التعامل معها من خلال القوانين الجنائية التقليدية وجهود أجهزة الشرطة والقضاء.

[1] حكيم سياب، مرجع سابق، ص 220.

- **الجرائم المعلوماتية:** تحتاج إلى قوانين متخصصة تشمل الأمن السيبراني، وتعاونًا دوليًا وتقنيات حديثة لتعقب الجناة وإثبات الجرائم، مثل استخدام الذكاء الاصطناعي في تحليل البيانات الجنائية الرقمية.[1]

- **نماذج عن الفرق بين الجريمتين:**[2]

إن الجريمة المعلوماتية تمثل تطورًا نوعيًا للجريمة التقليدية، إذ أصبحت تُمارس عبر الفضاء الرقمي بوسائل وأساليب تقنية متقدمة، مع الحفاظ في كثير من الأحيان على البنية الإجرامية ذاتها. فعلى سبيل المثال، إذا كانت السرقة في شكلها التقليدي تتمثل في سرقة سيارة من موقف سيارات، فإن نظيرها المعلوماتي قد يتمثل في اختراق حساب بنكي وسرقة الأموال إلكترونيًا، وهو ما يوضح انتقال الفعل الجرمي من الحيز المادي إلى الفضاء السيبراني. وبالمثل، فإن الاحتيال الذي كان يُمارس من خلال التلاعب في عقود العمل أو العقارات، بات يُرتكب اليوم عبر منصات التجارة الإلكترونية أو البريد الإلكتروني من خلال أساليب مثل التصيد الاحتيالي. أما الابتزاز، فقد تطور من مجرد تهديد بنشر صور خاصة للحصول على المال، إلى شكل جديد أكثر خطورة، يتمثل في استخدام برمجيات الفدية Ransomware التي تُخترق بها بيانات الضحية ويُطلب منها دفع فدية لاسترجاعها. ولم تَسلم حتى الجرائم الإرهابية من هذا التحول، إذ أصبح بالإمكان تنفيذ هجمات سيبرانية لتعطيل أنظمة حيوية مثل الأمن أو الطاقة الكهربائية في دول مستهدفة، بدلاً من تنفيذ تفجيرات مادية أو هجمات مسلحة كما كان يحدث سابقًا. وعليه، فإن الجريمة المعلوماتية ليست مجرد امتداد للجريمة التقليدية، بل تمثل تحولًا جوهريًا في أدوات وبيئة ارتكاب الجريمة.

[1] حكيم سياب، مرجع سابق، ص 220.

[2] Marc Watin-Augouard,"**La cybercriminalité : défi mondial**", CNRS éditions, Paris, 2016, P 178.

## المطلب الثاني: أنواع الجرائم المعلوماتية

تتنوع الجرائم المعلوماتية بشكل واسع نظرًا للتطور التكنولوجي المستمر وازدياد استخدام الإنترنت في مختلف مجالات الحياة. يمكن تصنيف الجرائم المعلوماتية وفقًا للجهة المستهدفة أو لطبيعة الجريمة نفسها. وفيما يلي أبرز أنواعها:

### الفرع الأول: الجرائم التي تستهدف الأفراد

تشمل الجرائم التي يكون ضحاياها أشخاصًا طبيعيين، حيث تُستغل بياناتهم أو تُنتهك خصوصيتهم أو يتم الإضرار بهم نفسيًا أو ماليًا، ومنها[1]:

1. **جرائم الاحتيال الإلكتروني**
   - سرقة بيانات الحسابات البنكية واستخدامها دون إذن.
   - الاحتيال عبر التسوق الإلكتروني من خلال مواقع وهمية.
   - التصيد الاحتيالي Phishing لخداع المستخدمين وسرقة بياناتهم الشخصية.
2. **جرائم الابتزاز الإلكتروني**
   - تهديد الأفراد بنشر معلومات حساسة أو صور خاصة للحصول على المال أو خدمات معينة.
   - اختراق الحسابات الشخصية وطلب فدية لاستعادتها.
3. **التشهير وانتهاك الخصوصية**
   - نشر معلومات شخصية دون إذن بغرض الإساءة أو التشهير.
   - تسجيل المكالمات أو تصوير الأفراد دون علمهم ونشر المحتوى على الإنترنت.
4. **الجرائم الأخلاقية التحرش الإلكتروني**
   - التحرش عبر وسائل التواصل الاجتماعي أو البريد الإلكتروني.
   - إرسال محتوى غير لائق بقصد الإزعاج أو الإساءة.

[1] الطاهر ياكر، "**مكافحة الجرائم المعلوماتية بين التشريعات الوطنية والاتفاقيات الدولية**"، كلية الحقوق والعلوم السياسية بخميس مليانة، الجزائر، 2022، ص 6.

**5. جريمة انتحال الشخصية:**

- اخفاء الشخصية والتصرف بحرية تحت اسم مستعار.
- أخذ البيانات الشخصية كالعنوان وتاريخ الميلاد ورقم الضمان الاجتماعي وما شابهها من أجل الحصول على البطاقات الائتمانية وغيره.

**الفرع الثاني: الجرائم التي تستهدف المؤسسات والدول**

تطورت الجرائم المعلوماتية بشكل كبير لتشمل استهداف المؤسسات والدول، مما يشكل تهديدًا للأمن الاقتصادي والسياسي والاجتماعي. تستخدم هذه الجرائم تقنيات متقدمة لاختراق الأنظمة، سرقة البيانات وتعطيل الخدمات، والتجسس الإلكتروني، مما يجعلها واحدة من أخطر التهديدات في العصر الرقمي[1].

**1. أشكال الجرائم المعلوماتية ضد المؤسسات والدول:**

- **الهجمات السيبرانية Cyber Attacks**

تشمل محاولات اختراق شبكات المؤسسات والدول لسرقة البيانات أو تعطيل الأنظمة. ومن أشهر أنواعها:

- هجمات الاختراق Hacking يتم فيها الدخول غير المصرح به إلى أنظمة الشركات أو المؤسسات الحكومية.
- هجمات حجب الخدمة DDoS Attacks تستهدف تعطيل الخوادم والأنظمة عبر إغراقها بحجم هائل من الطلبات.

- **التجسس الإلكترونيCyber Espionage** تتمثل في محاولات سرقة المعلومات السرية من المؤسسات أو الحكومات لاستخدامها في التجسس السياسي أو الصناعي.
  - تستخدمها الدول في الحروب السيبرانية للحصول على معلومات استخباراتية.
  - تُستهدف بها الشركات الكبرى للحصول على أسرار تجارية وتقنية.

[1] الطاهر ياكر، مرجع سابق، ص 6.

- **الجرائم المالية الإلكترونية**

تشمل الاحتيال البنكي، تزوير الحسابات، واختراق أنظمة الدفع الإلكترونية، مما يؤدي إلى خسائر مالية ضخمة للمؤسسات المصرفية والشركات.

- **الهجمات على البنية التحتية الحيوية**

- تستهدف منشآت الطاقة، المياه، المستشفيات، والمواصلات بهدف تعطيل الخدمات الأساسية.
- قد تؤدي إلى كوارث اقتصادية وسياسية إذا استهدفت محطات الطاقة أو الأنظمة الصحية.

- **نشر البرمجيات الخبيثة Malware Attacks**

يتم استخدام فيروسات، برامج الفدية Ransomware، وأحصنة طروادة لاختراق أجهزة الحواسيب وسرقة البيانات أو تشفيرها مقابل فدية مالية.

- **نشر المعلومات المضللة والحروب السيبرانية**

يتم استخدام الإنترنت ووسائل التواصل الاجتماعي لنشر أخبار مزيفة تهدف إلى التأثير على الرأي العام وزعزعة استقرار الحكومات[1].

**2. دوافع الجرائم المعلوماتية ضد المؤسسات والدول**

- تحقيق مكاسب مالية من خلال سرقة الأموال أو الابتزاز الإلكتروني؛
- التجسس وسرقة الأسرار للحصول على معلومات سياسية، اقتصادية، أو عسكرية؛
- الإضرار بالاقتصاد الوطني من خلال تعطيل البنوك أو الشركات الكبرى؛
- الحروب السيبرانية تستخدمها بعض الدول لاستهداف دول أخرى دون اللجوء إلى المواجهة العسكرية المباشرة.

**ثالثًا: آثار الجرائم المعلوماتية على المؤسسات والدول**

- **الخسائر المالية الضخمة** :تؤدي هذه الجرائم إلى خسارة ملايين الدولارات بسبب الاحتيال الإلكتروني أو الهجمات على الأنظمة المصرفية.

[1] سمير قط، "**أثر الجرائم المعلوماتية على أمن واستقرار الدول: قرصنة الموقع الالكتروني لوكالة الأنباء القطرية نموذجا**"، جمعة محمد خيضر ببسكرة، الجزائر، مجلة الناقد للدراسات السياسية، العدد 3، 2018، ص 133، ص 163.

- **تعطل الخدمات الحيوية** :قد تؤدي الهجمات إلى تعطيل الكهرباء، الاتصالات، والخدمات الصحية مما يشلّ الحياة اليومية.
- **فقدان الثقة في المؤسسات** :تؤثر هذه الجرائم على سمعة الشركات والحكومات، مما يقلل من ثقة الجمهور بها.
- **المخاطر الأمنية** :يمكن أن تؤدي الهجمات الإلكترونية إلى تسريب معلومات استخباراتية حساسة تعرض الأمن القومي للخطر[1].

**رابعًا: طرق مكافحة الجرائم المعلوماتية ضد المؤسسات والدول**

- **تعزيز الأمن السيبراني:** من خلال تحديث الأنظمة، استخدام جدران الحماية القوية وتطبيق التشفير المتقدم.
- **إنشاء فرق متخصصة في الأمن السيبراني:** تعمل على التصدي للهجمات الإلكترونية والاستجابة السريعة عند الاختراقات.
- **التعاون الدولي:** من خلال تبادل المعلومات بين الدول والمنظمات الأمنية مثل الإنتربول لمواجهة التهديدات السيبرانية.
- **التشريعات والقوانين الصارمة:** فرض عقوبات رادعة على مرتكبي الجرائم الإلكترونية وتعزيز الإطار القانوني لمكافحتها.
- **التوعية والتدريب:** نشر ثقافة الأمن السيبراني بين الموظفين والمواطنين لتقليل المخاطر المحتملة[2].

**المطلب الثالث: أساليب ارتكاب الجرائم المعلوماتية**

تشكل الجرائم المعلوماتية تهديدًا خطيرًا للمؤسسات والدول، مما يستدعي استراتيجيات قوية لمكافحتها. يعتمد الحد من هذه الجرائم على تطوير التقنيات الأمنية، سنّ القوانين

[1] سمحية بلقاسم، حميد بوشوشة، "**الجريمة الالكترونية بعد جديد للاجرام في الجزائر**"، جامعة قسنطينة، الجزائر، مجلة العلوم الانسانية، المجلد 10، العدد 1، 2023، ص 229.

[2] جمال الدهشان، "**الجرئم الالكترونية: دراسة قانونية مقارنة**"، دار النهضة العربية، القاهرة، مصر، 2019، ص 266.

الصارمة، وتعزيز التعاون الدولي كلما زاد التطور التكنولوجي، زادت الحاجة إلى جهود مكثفة لضمان أمن المعلومات وحماية الاقتصاد والأمن القومي.

**الفرع الأول: خصائص الجرائم المعلوماتية**

- **الطابع غير المادي للجريمة:** ترتكب الجرائم المعلوماتية في الفضاء الإلكتروني دون الحاجة إلى تفاعل مادي مباشر، حيث يتم استهداف البيانات والأنظمة بدلاً من الممتلكات الملموسة.
- **صعوبة تحديد الجاني:** يمكن للمجرمين إخفاء هويتهم عبر شبكاتVPN ، استخدام البرمجيات المشفرة، أو توجيه هجماتهم من عدة دول، مما يجعل تعقبهم أمرًا معقدًا.
- **سرعة التنفيذ والانتشار:** تحدث الجرائم المعلوماتية في غضون ثوانٍ أو دقائق، كما يمكن أن تنتشر البرمجيات الضارة بسرعة فائقة عبر الإنترنت؛
- **الأثر العابر للحدود:** لا تعترف هذه الجرائم بالحدود الجغرافية، حيث يمكن لمجرم في دولة ما استهداف ضحية في دولة أخرى دون أي تواجد مادي هناك؛
- **التطور المستمر في أساليب الهجوم:** تعمل الجريمة المعلوماتية في بيئة تقنية تتطور باستمرار، مما يجعل أساليبها دائمة التغيير والتحديث لمواكبة تقنيات الحماية؛
- **إمكانية استهداف أعداد كبيرة من الضحايا:** يمكن لمجرم واحد استهداف آلاف الأشخاص أو الشركات بضغطة زر، مثلما يحدث في عمليات الاحتيال الجماعي أو الهجمات السيبرانية الضخمة؛[1]
- **جرائم هادئة:** إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها كالقتل والسرقة وغيرها من الجرائم، فالجرائم الالكترونية لا تحتاج أدنى مجهود عضلي بل تعتمد على الدراسة الذهنية، والتفكير العلمي المدروس القائم عن تقنية الكمبيوتر وذلك يعود لكون هذا النوع من الجرائم عبارة عن معطيات وبيانات تتغير أو تعدل أو تمحى من السجلات المخزنة في ذاكرة الحاسبات إلا أن البعض يشبهها بجرائم

[1] سعاد مقدم، "**الجرائم المعلوماتية والجهود المبذولة لمكافحتها**"، جامعة الطارف، مجلة الدراسات في سيكولوجية الانحراف، المجلد 7، العدد 3، 2022، ص 183.

العنف مثل ما ذهب إليه مكتب التحقيقات الفيدرالي بالولايات المتحدة الأمريكى FBI نظرا لتماثل دوافع المعتدين على نظم الحاسب الآلي.

**الفرع الثاني: أركان الجريمة المعلوماتية**

تتشكل الجريمة المعلوماتية هي أيضا من الأركان الثلاثة المعروفة لدى الجريمة الكلاسية، حيث تتميز بخصوصيات تجعلها تختلف عن هذه الأخيرة، وهذا ما سنبينه في الأركان الثلاثة التالية:

**1. الركن الشرعي:**

انطلاقا من مبدا الشرعية ووفقا لاحكام المادة الأولى من قانون العقوبات الجزائري التي تنص على أن: "لا جريمة ولا عقوبة او تدابير امن بغير قانون" جرم القانون رقم 04-15 بعض صور الجريمة المعلوماتية ونص على العقوبات المقررة لمرتكبيها في القسم السابع مكرر تحت عنوان " المساس بأنظمة المعالجة الالية للمعطيات" من الفصل الثالث المعنون " الجنايات والجنح ضد الأموال من الباب الثاني المتعلق "بالجنايات والجنح ضد الأفراد وذلك في المواد من 394 مكرر الى 394 مكرر 08 من قانون العقوبات المعدل والمتمم.

في حين جاء القانون 09-04 متضمنا للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها كجانب وقائي يحد من وقوع الجرائم المعلوماتية من خلال وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتسجيل وتجميع محتواها في حينها والقيام بإجراءات التفتيش.

ولجوء المشرع الى تقنين او النص على مثل هذه الجرائم وجعلها في نطاق مبدأ الشرعية يمنع القاضي من اللجوء الى القياس، بمعنى عدم جواز لجوء القاضي الجنائي الى قياس فعل لم يرد نص على تحريمه على فعل ورد نص بتجريمه، فيقرر القاضي الجنائي للأول عقوبة الثاني بسبب التشابه بين الفعلين.[1]

[1] بوضياف اسمهان، "**الجريمة الالكترونية والاجراءات التشريعية لمواجهتها في الجزائر**"، جامعة بوضياف المسيلة الجزائر، مقال، العدد 11، 2018، ص 353.

**2. الركن المادي:**

يعتبر الركن المادي للجريمة هو المظهر الخارجي لها وكيانها المادي الظاهر، وهو الماديات المحسوسة في العالم الخارجي كما حددتها نصوص التجريم، فالقاعدة انه "لا جريمة دون ركن مادي" أو " لا جريمة ولا عقوبة الا بنص "، الا ان الركن المادي للجريمة المعلوماتية يختلف نوعا ما عن الجرائم التقليدية كون انه يقوم على صور في فعل الاعتداء والمتمثلة في:

**أولا: الدخول او البقاء غير المشروع:**

الدخول أو القاء غير المشروع في نظام المعالجة الالية للمعطيات او الشروع في ذلك نصت المادة 394 مكرر في قانون العقوبات على ان الدخول او الدخول والبقاء غير المشروع في نظام المعالجة الالية للمعطيات او الشروع في ذلك يشكل فعلا إجراميا ولهذا الفعل حسب المادة المذكورة صورتين كالتالي:[1]

أ. **الصورة البسيطة:** يتمثل النشاط الاجرامي في هذه الصورة في الافعال الاتية:

- **فعل الدخول:** يتحقق فعل الدخول بمجرد الوصول الى المعلومات المخزنة داخل النظام ودون علم ورضا صاحبه، لان هذا النظام لا يسمح للدخول فيه إلا لأشخاص معينين او يسمح بالدخول لكن مقابل نفقات.
- **البقاء:** معنى البقاء هو التواجد داخل نظام المعالجة الالية للمعطيات ضد ارادة من له الحق في السيطرة على هذا النظام، او بتجاوز المدة المسموح له بالبقاء فيها او عدم الانسحاب فورا وقطع وجوده في نظام البيانات او يطبع معلومات حين يسمح له بالرؤية فقط.

**ب. الصورة المشددة:**

نصت المادة 394 مكرر في الفقرتين الثانية والثالثة من قانون العقوبات على ظروف تشديد عقوبة فعل الدخول والبقاء غير المشروع عندما ينتج عن هذين الفعلين اما محو او تحويل

[1] سعاد مقدم، مرجع سابق، ص 185.

المعطيات التي يحتويها النظام، وإما عدم صلاحية النظام لأداء وظائفه من خلال تخريب نظام اشتعال المنطمة.

**ثانيا: ادخال المعطيات بطريق الغش**

يقصد بفعل الادخال حسب المادة 394 مكرر 01 من قانون العقوبات اضافة معطيات جديدة الى نظام المعالجة الالية او التعديل من معلومات داخله كان يتضمنه مسبقا فغير فيها، ومثال ذلك حالة الاستخدام التعسفي لبطاقات السحب والائتمان سواء من صاحبها الشرعي أو عن غيره كحالة السرقة والتزوير.[1]

**ج. الركن المعنوي للجريمة المعلوماتية**

يتخذ الركن المعنوي في اغلب الجرائم بصفة عامة صورة القصد الجنائي، والذي يتحقق بتوافر ارادة بعمل غير شرعي لدى الجاني مع علمه بان القانون يجرمه، ونفس الامر ينطبق على الجريمة المعلوماتية التي يقوم ركنها المعنوي على توافر الارادة الجرمية لدى الفاعل، وهذا ما يظهر من خلال استعمال المشرع الجزائي لعبارة " الغش" و" العمد" و"الاعداد الجريمة"، في المواد 394 مكرر و 394 مكرر 1 و 394 مكرر2، وفي الاخير 394 مكرر 5 من قانون العقوبات وهذا ان دل فإنما يدل على ان الجريمة المعلوماتية جريمة عمدية بامتياز ولا يفترض فيها عنصر الخطأ.

هذا ويختلف الركن المعنوي في الجرائم المعلوماتية من جريمة الى أخرى فجريمة الدخول غير المصرح به الى نظام الحاسب الالي تتطلب قصدا جنائيا يتمثل في علم الجاني بعناصر الركن المادي للجريمة، اي العلم بان الولوج الى داخل النظام بشكل غير مصرح يغد جريمة باعتبار حماية المشرع لمحل الحق وهو الحاسب الالي لما يتضمنه من برامج ومعلومات.

وفي جريمة الاحتيال الالكتروني التي بدورها تعد جريمة عمدية يتطلب لقيامها توافر القصد الجنائي لقيام مسؤولية الجاني، والقصد الجنائي المشترط هو القصد الجنائي بنوعيه العام

[1] سعاد مقدم، مرجع سابق، ص 185.

والخاص، فالمجرم يعلم بأنه يخالف القانون بسلوكه مع اتجاه نيته الى تحقيق ربح غير مشروع له او للغير او تجريد شخص آخر من ممتلكاته على نحو غير مشروع.[1]

[1] سعاد مقدم، مرجع سابق، ص 186.

## المبحث الثاني: الإطار القانوني لمكافحة الجرائم المعلوماتية في الجزائر

مع التطور السريع في مجال التكنولوجيا والاتصالات، ظهرت الجرائم المعلوماتية كتهديد متزايد يطال الأفراد، المؤسسات، وحتى الدول. وقد أدركت الجزائر خطورة هذه الظاهرة، مما دفعها إلى تطوير إطار قانوني وتنظيمي لمكافحتها.

يهدف هذا المبحث إلى استعراض التشريعات الوطنية التي تم وضعها لمواجهة الجرائم المعلوماتية بالإضافة إلى الهيئات المكلفة بتطبيق هذه القوانين. كما يناقش التحديات التي تعيق تنفيذ القوانين بفعالية مثل التطور المستمر للتقنيات وضعف التنسيق بين الجهات المعنية. من خلال هذا الإطار القانوني تسعى الجزائر إلى تعزيز الأمن السيبراني وحماية الأفراد والمؤسسات من مخاطر الجرائم الإلكترونية.

### المطلب الأول: التشريعات الوطنية لمكافحة الجرائم المعلوماتية

حرصت الجزائر على وضع إطار قانوني لمكافحة الجرائم المعلوماتية بهدف التصدي للتهديدات السيبرانية المتزايدة، وحماية الأفراد والمؤسسات من مخاطر الاعتداءات الإلكترونية. وقد تبلورت هذه الجهود من خلال سنّ مجموعة من القوانين والتشريعات التي تحدد الجرائم الإلكترونية وعقوباتها، إضافة إلى التعديلات التي طالت القوانين التقليدية لمواكبة التطورات التكنولوجية.

#### الفرع الأول: القوانين الجزائرية المتعلقة بالجريمة المعلوماتية

شهد النظام القانوني الجزائري تطورًا لمواجهة الجرائم المعلوماتية، حيث تم إدراج نصوص قانونية خاصة بهذا النوع من الجرائم، ومن أبرزها:[1]

- قانون العقوبات: قامت الجزائر بتعديل قانون العقوبات بموجب القانون رقم 04 -15 المؤرخ في 10 نوفمبر 2004، والذي ادخل عليه تعديل في 20 ديسمبر 2006.

[1] فاروق خلف، "**الاليات القانونية لمكافحة الجريمة المعلوماتية**"، كلية الحقوق والعلوم السياسية الوادي، الجزائر، مجلة الحقوق والحريات، العدد 2، 2015، ص 15.

ويتضمن قانون العقوبات الجزائري القسم السابع تحت عنوان" المساس بأنظمة المعالجة الآلية للمعطيات " ضمن المواد من 394 إلى 394 مكرر6، و التي تناولت أنواع الجرائم الالكترونية و عقوبتها.[1]

- قانون رقم 09-04 المؤرخ في 2009/8/16: و هو القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها، صدر هذا القانون في الجريدة الرسمية رقم 47 الصادرة بتاريخ 16/8/2009يحتوي على 6 فصول تناولت التعريف بالجريمة، مراقبة الاتصالات الالكترونية، القواعد الإجرائية والهيئة الوطنية للوقاية من الجرائم المعلوماتية و الاختصاص القضائي و هذا في 19 مادة.

## الفرع الثاني: التعديلات والتحديثات على القوانين الجزائرية لمكافحة الجرائم المعلوماتية[2]

نظرًا لتطور الجريمة المعلوماتية وتعقيد أساليبها، قامت الجزائر بتعديل وتحديث منظومتها القانونية بشكل مستمر لمواكبة المستجدات التكنولوجية وضمان حماية الأفراد والمؤسسات من التهديدات الإلكترونية. ومن أبرز هذه التعديلات والتحديثات:

### 1. تعزيز العقوبات على الجرائم المعلوماتية

مع تزايد خطورة الجرائم الإلكترونية، شددت السلطات الجزائرية العقوبات المفروضة على مرتكبيها، حيث تم إدراج عقوبات أشد على الأفعال التالية:

- **الاختراق غير المشروع للأنظمة الإلكترونية** :رفع العقوبات على عمليات القرصنة والاختراق غير المصرح به لأنظمة المعلومات الخاصة والعامة؛
- **الاحتيال الإلكتروني** :تشديد العقوبات على عمليات النصب عبر الإنترنت، بما في ذلك الاحتيال المصرفي وسرقة البيانات البنكية؛

[1] فاروق خلف، مرجع سابق، ص 15.

[2] مهدي رضا، **الجرائم السبيرانية واليات مكافحتها في التشريع الجزائري**، مجلة اليليزا للبحوث والدراسات، جامعة محمد بوضياف، المسيلة، الجزائر، المجلد 06، العدد 02، 2021، ص 116، ص 117.

- **التشهير الإلكتروني والابتزاز عبر الإنترنت** :فرض عقوبات أكثر صرامة على الجرائم المتعلقة بالمساس بسمعة الأفراد عبر الوسائل الرقمية، مع التركيز على الابتزاز الإلكتروني ونشر المعلومات الشخصية بدون إذن.

2. **تحديث القوانين المتعلقة بحماية البيانات الشخصية**

استجابةً للتطورات الرقمية وحماية حقوق الأفراد، قامت الجزائر بإدراج قوانين جديدة تحمي البيانات الشخصية، وألزمت المؤسسات العامة والخاصة بما يلي:

- الالتزام بحماية المعلومات الشخصية وتخزينها وفقًا لمعايير أمنية مشددة؛
- فرض عقوبات على الجهات التي تفشل في تأمين بيانات المستخدمين أو تستغلها لأغراض غير مشروعة؛
- إنشاء هيئات رقابية لضمان الامتثال للقوانين الخاصة بحماية البيانات الشخصية.

3. **قوانين مكافحة الإرهاب السيبراني والتجسس الإلكتروني**

مع تنامي التهديدات الإرهابية في الفضاء الإلكتروني، قامت الجزائر بإدراج مواد قانونية جديدة تهدف إلى[1]:

- تجريم استخدام الإنترنت لأغراض إرهابية، مثل تجنيد الأفراد، الترويج للأفكار المتطرفة أو تمويل العمليات الإرهابية عبر الشبكات الرقمية؛
- تعزيز المراقبة القانونية للاتصالات الإلكترونية، مع ضمان احترام الحقوق الأساسية للمواطنين؛
- التعاون مع الدول والمنظمات الدولية لتعقب الجرائم السيبرانية ذات الطابع الإرهابي أو الاستخباراتي.

4. **إدراج قوانين جديدة لحماية المعاملات الإلكترونية والتجارة الرقمية**

- تعزيز القوانين الخاصة بالتجارة الإلكترونية لضمان حقوق المستهلك وحمايته من عمليات الاحتيال الإلكتروني؛
- تنظيم الدفع الإلكتروني لمنع عمليات غسيل الأموال وتمويل الأنشطة غير القانونية عبر المنصات الرقمية؛

[1] عقباش بريزة، عقباش حنان، "**اليات مواجهة الجريمة الالكترونية في التشريع الجزائري**"، مذكرة لنيل شهادة الماستر جامعة محمد البشير الابراهيمي، الجزائر، 2022، ص 41.

- فرض قيود على الشركات التي تجمع بيانات المستخدمين دون تصريح، مع إلزامها بتوضيح كيفية استخدام تلك البيانات[1].

**5. تطوير التشريعات الخاصة بالأدلة الرقمية**

أصبحت الأدلة الرقمية جزءًا أساسيًا في التحقيقات الجنائية، ولهذا تم إدراج قوانين جديدة تهدف إلى:

- الاعتراف بالأدلة الرقمية في المحاكم ومعاملتها بنفس أهمية الأدلة التقليدية؛
- إلزام مزودي خدمات الإنترنت بحفظ سجلات البيانات لفترة معينة، للمساعدة في التحقيقات المتعلقة بالجرائم الإلكترونية؛
- وضع معايير قانونية صارمة لاستخدام البيانات الرقمية في التحقيقات، مع مراعاة حماية خصوصية الأفراد.

**المطلب الثاني: الهيئات المعنية لمكافحة الجرائم المعلوماتية في الجزائر**

نظرًا لخطورة الجرائم المعلوماتية وتأثيرها على الأفراد والمؤسسات، أنشأت الجزائر عدة هيئات رسمية تهدف إلى مكافحتها، كل منها يتمتع بمهام محددة تهدف إلى تعزيز الأمن السيبراني، حماية البيانات وتطبيق القوانين ذات الصلة.

**الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال**

أنشئت هذه الهيئة بموجب القانون رقم 09-04 المؤرخ في 5 أوت 2009 و الذي حددت المادة 14 منه مهام الهيئة و المتمثلة في:

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحته؛
- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام و الاتصال في ذلك تميع المعلومات و انجاز الخبرات القضائية؛

[1] عقباش بريزة، مرجع سابق، ص 42.

- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال وتحديد مكان تواجدهم[1].

**الفرع الثاني: الهيئة القضائية الجزائية المتخصصة**

والتي تم إنشاؤها بموجب القانون 14/04 المؤرخ في 10 نوفمبر 2004 المعدل للقانون الإجراءات الجزائية و أن اختصاصها إقليمي موسع طبقا للمرسوم التنفيذي رقم 348/06 المؤرخ في 2006/1/5.

**الفرع الثالث: المعهد الوطني للأدلة الجنائية و علم الإجرام**

لقد جاء في القانون رقم 04-09 مجموعة من التدابير الوقائية التي يتم اتخاذها مسبقا من طرف مصالح معينة لتفادي وقوع جرائم معلوماتية أو الكشف عنها و عن مرتكبيها في وقت مبكر وهي كالتالي:

**1. مراقبة الاتصالات الالكترونية:**

لقد نصت المادة 1 على أربع حالات التي يجوز فيها لسلطات الأمن القيام بمراقبة المرسلات و الاتصالات الالكترونية، وذلك بالنظر إلى خطورة التهديدات المحتملة وأهمية المصلحة المحتملة وهي :

- للوقاية من الأفعال التي تحمل وصف جرائم الإرهاب والتخريب و جرائم امن الدولة.
- عندما تتوفر معلومات عن احتمال وقوع اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام؛
- لضرورة التحقيقات و المعلومات القضائية حينما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية؛
- في إطار تنفيذ طلبات المساعدات القضائية الدولية المتبادلة.

**2. إقحام مزودي خدمات الاتصالات الالكترونية في مسار الوقاية من الجرائم المعلوماتية**

وذلك من خلال فرض عليهم مجموعة من الالتزامات مذكورة في المواد التالية 10 ، 11 و 12 :

[1] مهداوي حنان، مرجع سابق، ص 1072.

- الالتزام بالتعاون مع مصالح الأمن المكلف بالتحقيق القضائي عن طريق جمع أو تسجيل المعطيات المتعلقة بالاتصالات والمراسلات و وضعها تحت تصرفها مع مراعاة سرية هذه الإجراءات و التحقيق؛
- الالتزام بحفظ المعطيات المتعلقة بحركة السير و كل المعلومات التي من شانها أن تساهم في الكشف عن الجرائم و مرتكبيها، وهذين الالتزامين موجهين لكل مقدمي خدمات الاتصالات الالكترونية دون استثناء؛
- الالتزام بالتدخل الفوري لسحب المحتويات التي يسمح لهم الاطلاع عليها بمجرد العلم طريقة مباشرة أو غير مباشرة بمخالفتها للقانون، و تخزينها أو جعل الوصول إليها غير ممكن؛
- الالتزام بوضع ترتيبات تقنية للحد من إمكانية الدخول إلى الموزعات التي تحتوي على معلومات متنافية مع النظام العام والآداب العامة مع إخطار المشتركين لديهم بوجودها و ننشير إلى أن هذين الالتزامين يخصان فقط مقدمي الدخول إلى الانترنت[1].

**المطلب الثالث: الاشكالات المتعلقة بتطبيق القوانين**

رغم الجهود المبذولة من قبل الدولة الجزائرية لمكافحة الجرائم المعلوماتية عبر سن التشريعات وإنشاء الهيئات المختصة، إلا أن هناك العديد من التحديات التي تعيق التطبيق الفعلي والفعال لهذه القوانين. هذه التحديات تتنوع بين مشكلات تقنية، قانونية، وإدارية، مما يستوجب إيجاد حلول فعالة لمواجهتها.

**الفرع الأول: صعوبات مواجهة الجريمة المعلوماتية في الجزائر**

- صعوبة تحصيل الاثباتات والادلة: أي تتخلل عملية التحريات والتحقيقات القضائية في القضايا الماسة بأمن المعلومات صعوبات جمة، من أبرزها صعوبة تحصيل المعطيات المتعلقة بمزودي الخدمة لتمركزها أساسا بالجزائر العاصمة فقط، وعليه فهي تأخذ وقت طويل لتحصيلها؛

[1] بوضياف اسمهان، مرجع سابق، ص 370.

- يضاف الى ذلك صعوبة أخرى تتمثل في صعوبة تحصيل الادلة في هذا النوع من الجرائم، كون الجناة فيها ليسو أشخاص عاديين بل يتميزون بالذكاء و الخبرة الكبيرة في اتقان العمل بالحاسب الالي وأنظمته وبرامجه، وعليه يتمكنون من اخفاء أفعالهم الاجرامية بسهولة كبيرة، من خلال استخدام التلاعب غير المرئي بما يعرف بالنبضات أو الذبذبات الاكترونية التي يتم تسجيل البيانات والمعطيات عن طريقها؛
- كما أن الاثبات أو الدليل في مثل هكذا قضايا صعب جدا سواء ما تعلق منها بأدلة مباشرة تتمثل في اعتراف الجاني، والخبرة ومعاينة مسرح الجرم، الذي يصعب تحديده هو الاخر، أو الادلة غير المباشرة التي يتحصل عليها القاضي عن طريق الاستقراء والاستنتاج. وإن كان أمر تحصيل الادلة صعب بالنسبة لهذه الجرائم الواقعة داخل الوطن غير أن تحصيل الادلة أصعب لما تكون واقعة في الجزائر وآثارها امتدت للخارج؛[1]
- صعوبات فنية و تقنية: فالجرائم المعلوماتية جرائم من نوع خاص تتطلب أدوات عمل خاصة في اكتشافها وتتبع حيثياتها والتوصل الى مرتكبيها الحقيقيين، فلا الادلة ولا مكان الجرم معلومين، و لا أدوات تنفيذها ووقت وقوعها معروفين، بل كل ذلك يتسم بالضبابية والصعوبة في التحديد، بسبب ما تتسم به الجريمة المعلوماتية من خصوصية تميزها عن الجريمة التقليدية، الا ان العمل على اكتشافها ممكن الى حد كبير اذا ما قيست صعوبتها بالصعوبات التي تواجه محاربي الجرائم المعلوماتية؛
- نقص الخبرة الفنية والتقنية: والمعرفة اللازمة بالباحث الالي وأنظمته لدى المكلفين بعملية مكافحة هذه الجرائم، وهذه الأخيرة تتطلب اطلاعا واسعا بعالم التقنيات وأدواته سواء كانوا قضاة أو أو رجال أمن أو أعضاء بالهيئات المتخصصة بذلك قصد التمكن من فهمها واكتشافها ومحاربتها، خاصة وأن مجال هذه الجرائم يتسم بالتغير والتحول السريعين؛
- الامتناع عن التبليغ عن المجنى عليهم: أو التبليغ بعد فوات الأوان وهذا أم ناتج عن اما عن جهل الضحايا بالقانون أو عن تخوفهم من ما قد يترتب عن القيام بذلك، فكثير من المؤسسات المالية كالبنوك مثلا تحجم عن الابلاغ عن ذلك بحجة أنه سيكون سببا في تعريض ثقة المتعاملين معها للاهتزاز.

[1] فتيحة حيمر، "**الجرائم المعلوماتية في الجزائر: المواجهة والتحدي**"، مجلة الحقوق والعلوم السياسية، جامعة خنشلة المجلد 12، العدد1 ، 2025، ص 281.

- صعوبة وضخامة كم البيانات والملفات الالكترونية، المتواجدة في تلك البيئة الالكترونية لتلك الجرائم وبالتالي فالأمر يصعب من امكانية تحديد وفصل البريء منها من ماهو غير ذلك، ولهذا فالتحري والتحقيق يطول.[1]

**الفرع الثاني: تفعيل مكافحة الجرائم المعلوماتية في الجزائر**

من منطلق تلك الصعوبات واستقراء للواقع الالكتروني والمعلوماتي والبنية التحية الخاصة بكل ذلك ببلادنا، يتضح جليا أن مهمة محاربة هذه الجرائم في غاية الصعوبة، و ينبغي على الجزائر بذل المزيد من الجهود لايجاد سبل فعالة للتصدي لها، و منها نذكر:

- في إطار زرع الثقافة المعلوماتية في المجتمع، يجب توعية الأولياء بخطورة هذه الجرائم وبدورهم كمراقب أول في العملية، إضافة الى الدور الهام لمختلف المؤسسات التعليمية في بث الوعي بمخاطر الاستغلال السيئ لتكنولوجيا الاعلام والاتصال، ناهيك عن الدورالذي يمكن أن تلعبه تنظيمات المجتمع المدني في هذا الاطارلما تملكه من امكانيات الولوج في مفاصل المجتمع والقيام بالتحسيس والتوعية؛
- تحيين البرامج التعليمية وتكييفها حسب متطلبات العصر بإدراج مواد أو على الأقل دروس ضمن برامجها تبرز من خلالها المخاطر الناتجة عن الاستغلال السيئ لتكنولوجيا الاعلام والاتصال من جهة، وعن عدم توفير نظم لحماية المعلومات الالكترونية من جهة أخرى؛
- فتح المجال أمام وسائل الاعلام السمعية والبصرية لنشر التوعية أيضا بمخاطر الجرائم المعلوماتية والطرق المتبعة من قبل المجرمين لاصطياد ضحاياهم؛
- اشراك المواطن في عملية محاربة هذه الجرائم، و تشجيعه على التعاون مع مختلف أجهزة الدولة و التبليغ الفوري عن الجريمة التي تمس بجهازه ومعلوماته، دون تردد أو خوف؛
- عقد المزيد من المؤتمرات التي تتدارس الموضوع، وتبحث في طرق المواجهة قصد الخروج بتوصيات من شأنها المساعدة في التقليل من آثار هذه الجرائم؛

[1] فتيحة حيمر، مرجع سابق، ص 282.

- أما على المستوى الدولي فلابد من الانضمام لمختلف الأجهزة والهيئات الدولية المختصة في المجال قصد تبادل الخبرات وتسهيل الاجراءات القضائية المتعلقة بتسليم المجرمين وكذا مباشرة الانابات القضائية الدولية ونشر أوامر القبض للمبحوث عنهم دوليا[1].

تمثل التحديات في تطبيق القوانين الخاصة بالجرائم المعلوماتية عائقًا كبيرًا أمام تحقيق بيئة إلكترونية آمنة في الجزائر. ومن الضروري العمل على تحديث التشريعات، تعزيز التنسيق بين الجهات المختصة، وزيادة الوعي المجتمعي لمكافحة هذه الجرائم بشكل فعال.

[1] فتيحة حيمر، مرجع سابق، ص 282.

## المبحث الثالث: الإطار الدولي لمكافحة الجرائم المعلوماتية

يعد الإطار الدولي لمكافحة الجرائم المعلوماتية من المواضيع الحيوية في ظل تزايد التهديدات الإلكترونية العابرة للحدود. نظراً للطبيعة العالمية للفضاء السيبراني، أصبحت الجهود الوطنية غير كافية لمواجهة التحديات التي تفرضها الجرائم المعلوماتية، مما استدعى ضرورة التعاون الدولي عبر سن تشريعات موحدة، وإبرام اتفاقيات دولية، وتنسيق الجهود بين مختلف الدول والمنظمات المختصة.

يتناول هذا المبحث الجهود الدولية لمكافحة الجرائم المعلوماتية من خلال الاتفاقيات الدولية وأدوار المنظمات العالمية مثل الأمم المتحدة والإنتربول، إضافة إلى دراسة التحديات التي تواجه التعاون الدولي سواء من حيث الفروقات القانونية بين الدول أو من حيث التوازن بين مكافحة الجريمة وحماية حقوق الأفراد في الفضاء الرقمي.

### المطلب الاول: الاتفاقيات الدولية لمكافحة الجرائم المعلوماتية

يشكل التعاون الدولي أحد الركائز الأساسية في مكافحة الجرائم المعلوماتية، نظراً لطبيعتها العابرة للحدود وصعوبة تعقب مرتكبيها ضمن نطاق دولة واحدة. ولهذا السبب، تم إبرام عدد من الاتفاقيات الدولية التي تهدف إلى توحيد الجهود بين الدول، وتعزيز التنسيق القانوني والتقني لمواجهة التهديدات السيبرانية.

#### الفرع الأول: اتفاقية بودابست حول الجرائم المعلوماتية[1]

شكلت اتفاقية بودابست لمكافحة الجريمة السيبرانية، كخطة رائدة على مستوى التعاون بين الدول، وهي الوحيدة حتى اليوم، من حيث الدول المنظمة اليها، وترتكز أهمية هذه الاتفاقية بفعالياتها على اقرارها لاجراءات عملية، تلتزم الدول المنظمة بادراجها في قوانينها الوطنية

[1] بوقرين عبد الحليم، قطاف سليمان، "**الاليات القانونية الموضوعية لمكافحة الجرائم السبرانية في ظل اتفاقية بودابست والتشريع الجزائري**"، كلية الحقوق والعلوم السياسية، الأغواط، الجزائر، المجلة الأكاديمية للبحوث القانونية والسياسية، مجلد 6، العدد 1، 2022، ص 339.

مثل تلك الخاصة بجمع بيانات الاتصال وحفظها، مما يتيح تحديد مصدرها، وصلاحية الجهات القضائية المعنية، والمساعدة المتبادلة وتسليم المجرمين.

والمشرع الجزائري على غرار هذه الدول رغم عدم المصادقة عليها، الا انه نهج نهجها والتزم بشريعتها خاصة بالجانب الموضوعي لمواجهة الجريمة السيبرانية، وهذا ما نلمسه في المادة 04-15 المتعلق بقانون العقوبات والنصوص القانونية الخاصة المتعلقة بالجرائم السيبرانية.

**1. مضمون الاتفاقية:**

تكونت هذه الاتفاقية من 48 مادة في ميدان محاربة الجرائم السيبرانية، لقد ركزت هذه الأخيرة على ثلاثة عناصر:

- العنصر الأول: يتمثل في أهمية التدابير التشريعية الموضوعية أي نصوص التجريم الموضوعية؛
- العنصر الثاني: يتمثل في أهمية التدابير التشريعية الاجرائية المتلائمة مع طبية الجريمة الالكترونية.
- العنصر الثالث: أهمية تدابير التعاون الدولي والاقليمي في هذا المجال، وكان ذلك في مواد الاتفاقية الموزعة على أربعة فصول:

- الفصل الأول: تضمن تعريفا للمصطلحات الأساسية المادة 1؛
- الفصل الثاني: وجاء تحت عنوان الخطوات التي يجب اتخاذها على الصعيد الوطني وهو مؤلف من ثلاثة أقسام: الأول: يضم المواد من 2 الى 13 والتي تعالج النصوص الموضوعية لجرائم الحاسوب. الثاني: يضم المواد من 14 الى 21 والتي تتعلق بالقواعد الاجرائية؛[1]

  والثالث: يضم المادة 22 ويتعلق بالاختصاص.
- الفصل الثالث: وجاء تحت عنوان التعاون الدولي، وهو من المادة 23 حتى المادة 35.

[1] ليندة شرابشة،"**السياسة الدولية والاقليمية في مجال مكافحة الجريمة الالكترونية، الاتجاهات الدولية في مجال مكافحة الجريمة الالكترونية**"، المركز الجامعي سوق أهراس، الجزائر، ص 247.

- الفصل الرابع: ويتضمن الأحكام الختامية من المادة 36 الى 148، كما حددت اتفاقية بودابست الجرائم المعلوماتية وصنفتها في خمسة عنوانين في القسم الأول من الاتفاقية كالتالي:

العنوان الأول: ويضم جوهر جرائم الحاسب أو الجرائم المعلوماتية، وهي تلك الجرائم التي تعرف بالجرائم ضد سرية البيانات وسلامتها وسلامة النظم واتاحة البيانات والنظم؛

العنوان الثاني: ويضم الانتهاكات الممارسة بواسطة الحاسب الالي: والتي تمس المصالح القانونية والتي تحميها قوانين العقوبات، وتضم أيضا جرائم الغش المعلوماتي والتزوير المعلوماتي؛

العنوان الثالث: ويشمل الانتهاكات والجرائم المرتبطة بالمحتوى والتي تخص الانتاج والنشر غير المشروع للمواد الاباحية الطفولية عبر النظم المعلوماتية، في المادة التاسعة من الاتفاقية.

العنوان الرابع: ويشمل الجرائم المتعلقة بالاعتداء على الملكية الفكرية والحقوق المرتبطة بها في نص المادة 10 من الاتفاقية.

- العنوان الخامس: وهو يشتمل على أحكام اضافية بخصوص المشروع والاشتراك طبقا للمعايير الدولية الحديثة بالنسبة لمسؤولية الأشخاص وأيضا الجزاءات والتدابير المعنوية.[1]

**2. القواعد الموضوعية للجرائم السيبرانية في الاتفاقية:**

وزعت الاتفاقية الجرائم التي ترتكب بواسطة الانترنت على أربع مجموعات كبرى تضم الأولى الجرائم التي تتعرض لخصوصية وسلامة الأنظمة والبيانات، مثل النفاذ غير الشرعي، والاعتراض غير الشرعي وتشويه البيانات وسلامة النظام، وتضم المجموعة الثانية جرائم التزوير والاحتيال، بينما تندرج في الثالثة الجرائم المتصلة بالمحتوى مثل انتاج وتوزيع وحيازة مواد اباحية يستخدم فيها الأطفال، وفي المجموعة الرابعة جرائم الاعتداء على الملكية الفكرية، والحقوق المجاورة، ونصت في توصيتها رقم: 87/15 على تنظيم ومراقبة استخدام

[1] ليندة شرابشة، مرجع سابق، ص 247.

البيانات الشخصية في المجال الشرطي، وفي التوصية رقم: 04/90 على حماية البيانات الشخصية المنزلة في المجال الإلكتروني المعلوماتي، ونصت في مادتها الثانية على أن الاعتراض الغير قانوني للبيانات الشخصية و المتداولة بين الحواسيب يعد جريمة معلوماتية وسأفصل ذلك لاحقا، واستنادا الى المواد 2-13 فان الاتفاقية تلزم الدول الاعضاء فيها باتخاذ الاجراءات والتدابير التشريعية الملائمة لتجريم تسع جرائم في الميدان المعلوماتي وهي: [1]

- الدخول غير القانوني المتعمد وقد استخدمت الاتفاقية هذا المصطلح في حين أن غالبية إن لم يكن جميع التشريعات الوطنية تستخدم تعبر الدخول غير المصرح به، وذلك بالدخول المتعمد إلى أي نظام كمبيوتر أو جزء منه دون حق أو إذن سواء أكان بنية انتهاك وسائل الأمن أو بنية الحصول على معطيات الكمبيوتر أو لأية نية غير مشروعة المادة 2.
- الاعتراض غير القانوني المتعمد ودون حق بواسطة وسائل تكنولوجية للبيانات المرسلة غير العامة إلى أو من نظام كمبيوتر وكذلك اعتراض الإشعاعات الكهرومغناطيسية المنبعثة من أي نظام كمبيوتر تحمل مثل هذه المعطيات المادة 3.
- التدخل المتعمد أو الإرادي في المعطيات بالتدمير أو الحذف أو التشويه والإفساد أو تبديلها أو تغييرها أو تعديلها أو تعطيلها أو كبتها أو إخمادها، وقد ذهبت لجنة الخبراء إلى أن تعديل البيانات يشمل خلطها الغش أما تعطيل أو إخماد أو كبت البيانات فيتعلق بإجراءات منع وصولها إلى العنوان المرسلة إليه كحذف جزء منها على نحو لا يتيح وصولها إلى الموضع الفيزيائي المطلوب أو تصبح غير قادرة على ذلك أو منع الغير من الوصول إليها، وذهب بعض الخبراء إلى وجوب اشتراط حصول الضرر جراء التدخل في البيانات كعنصر من عناصر التجريم إلا أن النص لم يشر لهذا العنصر فجرم كل تدخل في المعطيات على أن يكون مقصودا المادة 4.
- التدخل المتعمد في الأنظمة وهنا نقوم ببث وإرسال المادة 5 ذات الأفعال المشار إليها في المادة 4 وذلك المتعلقة بالتدخل في المعطيات بغية تعطيل بإدخال أو تعديل أو

[1] ليندة شرابشة، مرجع سابق، ص 247.

حذف أو إخفاء بيانات أداء وعمل الأنظمة بالتدمير والحذف الكمبيوتر على نحو يظهر بيانات غير والتعديل والتعطيل.

- إساءة استخدام الأجهزة تصف ديباجة اتفاقية بودابست نيتها على السياسة الجنائية التي تهدف إلى حماية المجتمع من الجرائم الإلكترونية ، وتعتزم على وجه التحديد ردع الإجراءات الموجهة ضد السرية والنزاهة، وتوافر أنظمة الكمبيوتر والشبكات وبيانات الكمبيوتر بالإضافة إلى إساءة استخدام هذا النظام والشبكات والبيانات من خلال النص على تجريم مثل هذا السلوك، سبق وسميت هذه الجريمة في المسودات الأولى للاتفاقية السابقة الأدوات غير القانونية وإن كان بعض يرى أن هذا العنوان أكثر دقة، وتحتوي هذه الجريمة على نوعين من الأفعال الأولى المنصوص عليها في الفقرة أ من المادة 6 وتشمل الإنتاج المتعمد أو بيع أو شراء أو استخدام أو استيراد أو توزيع أو غير ذلك من أدوات ووسائل توفير الأجهزة بما فيها برامج الكمبيوتر بهدف ارتكاب أي فعل إجرامي من الأفعال المنصوص عليها في المواد 25 المشار إليها سابقا وكذلك كلمات السر ورموز الدخول أو أية برامج مشابهة بحيث تتيح اختراق نظام الكمبيوتر أو الدخول إليه أو إلى أي جزء منه بنية ارتكاب أي فعل من الأفعال المنصوص عليها في المواد 2-5 كما تشمل هذه الجريمة وفق الفقرة 2 من المادة 6 الحيازة والتملك لأي عنصر أو أداة مما ورد ذكره في الفقرة 1 أعلاه بنية ارتكاب أي من الأفعال المشار إليها في المواد 2-5 من الاتفاقية.
- التزوير المتعمد باستخدام جهاز الكمبيوتر وذلك بإدخال أو تعديل أو حذف أو إخفاء بيانات الكمبيوتر على نحو يظهر بيانات غير أصلية لتكون مقبولة قانونا وكأنها بيانات أصلية وبغض النظر عما إذا كانت هذه البيانات مقروءة أو غير مقروءة ويحق للدولة أن تشترك نية أو قصد الغش لقيام المسؤولية الجنائية المادة 7.
- الاحتيال المتعمد باستخدام الكمبيوتر بدون حق وعلى نحو يسبب خسارة الغير لممتلكاته بيانات الكمبيوتر أو من خلال التدخل بعمليات نظام الكمبيوتر أو برامجه بنية الحصول على منفعة اقتصادية لنفسه أو لغيره مادة 8.[1]

[1] ليندة شرابشة، مرجع سابق، ص 250.

- الجرائم المرتبطة بدعارة الأطفال وهنا يلاحظ أولا أن هناك جرائم كثيرة في المحتوى إلا أن الاتفاقية نصت عليها صراحة، إلا أن مشرعي الاتفاقية اقتصروا في جرائم المحتوى على هذه الجريمة فقط فقضت في المادة التاسعة منها بوجوب اتخاذ الدولة المنظمة للاتفاقية التدابير التشريعية لتجريم قيام أية شخص وبشكل قصدي عرض أو توزيع أو نقل أو غير ذلك من الأفعال التي من شأنها أن توفر أو تتيح توفير المواد الإباحية المتعلقة بالأطفال من خلال نظام كمبيوتر وتجريم إنتاج مواد دعارة الأطفال بغرض توزيع عبر نظام الكمبيوتر، ولا شك أن تفسير تلك الجريمة يؤدي إلى أن عرض المواد الإباحية يتضمن كذلك إعطاء معلومات حول وسائل العرض والاتصال هذه المواد وكذلك ربط المواقع بمداخل إلى مواقع إباحية تعرض هذه المواد، أما فيما يتعلق بالجدل حول مفهوم المواد الإباحية المتعلقة بالأطفال وما تشمله فمثلما هو الحال في المفاوضات الدولية حينما تختلف الثقافات وتتنوع و تصل لحد عدم الاتفاق يتم ترك ذلك للنظم الوطنية حسب قواعد النظام والآداب العامة لكن تم الاتفاق أنها تشمل كل مادة جنسية تتعلق بالاتصال الجنسي بالأطفال وفي ضوء الخلاف حول المحتوى ونطاقه، جرى الاتفاق على معايير الحد الأدنى التي نص عليها في الفقرتين الثانية والثالثة من ذات المادة، فقضت الفقرة الثانية من المادة 9 على أن مواد دعارة الأطفال تشمل أية مواد تظهر بشكل مرئي قيام القاصر بتصرفات جنسية أو ظهور أي شخص باتصال أو تصرف جنسي مع قاصر وكذلك الصور الواقعية التي تمثل أو تظهر قاصرا يتدخل بتصرف جنسي، أما الفقرة الثالثة فقد قررت أن المقصود بالقاصر يحدد تبعا للقانون الداخلي للدول الأعضاء على أن يتضمن في جميع الأحوال الأطفال الأشخاص دون سن 18 وإتاحة الفرصة لكل دولة لتحديد السن على أن يكون حده الأدنى وفقا لما تقدم المادة 9 بفقراتها الثلاث.[1]
- الجرائم المرتبطة بحق المؤلف أوجبت الاتفاقية في المادة 10 بفقرتيها الأولى: والتي تخص حق المؤلف، والثانية: تختص بالحقوق المجاورة، وجوب اتخاذ الدول المنظمة تدابير تشريعية تجرم الإخلال أو الاعتداء على حق المؤلف أو الحقوق المجاورة وفقا لما

[1] ليندة شرابسة، مرجع سابق، ص 250.

تحدده القوانين الوطنية للدول الأعضاء الموافقة مع اتفاقية بيرن لحماية المصنفات الأدبية والفنية واتفاقية تربس TRIPS، واتفاقية الوايبو – WIPO لحق المؤلف.[1]

**الفرع الثاني: دور الأمم المتحدة في مواجهة الجرائم المعلوماتية**

تعد الأمم المتحدة من أبرز الفاعلين الدوليين في مجال تنظيم ومكافحة الجرائم المعلوماتية نظراً لدورها الشامل في تنسيق الجهود بين الدول وتعزيز إطار قانوني دولي مشترك يُعالج التحديات المرتبطة بالفضاء السيبراني. ومع تسارع تطور التكنولوجيا الرقمية، ازدادت الحاجة إلى تدخل الأمم المتحدة لضمان الأمن السيبراني على الصعيد العالمي[2].

**1. مؤتمرات الأمم المتحدة لمنع الجريمة ومعاملة لمجرمين:**

وتعقد مؤتمرات دورية كل خمس سنوات وذلك لتعزيز وتبادل المعارف والخبرات بين الإخصائيين من مختلف الدول من أجل تدعيم التعاون الدولي والإقليمي في مجال مكافحة الجريمة، ونعرض بإيجاز بعض هذه المؤتمرات:

- **المؤتمر الخامس جينيف 1975:** وقد ناقش هذا المؤتمر:
  - التغيرات فى أشكال واتجاهات الجريمة وطنيا ودوليا.
  - دور التشريعات الجنائية واجراءات التقاضي ودور الشرطة فى منع الجريمة.
  - معاملة المجرميين داخل السجون .
  - الآثار الاقتصادية والاجتماعية للجريمة.
- **المؤتمر الدولى السادس بكركاس فنزويلا فى عام 1980:** وقد ناش هذا المؤتمر عدة نقاط وهي:
  - المعدلات الجديدة للجريمة واستيراتيجيات مكافحتها.
  - قضاء الأحداث.
  - إساءة استعمال السلطة.
  - بعض المسائل الإصلاحية ومعايير حقوق الإنسان.
  - قواعد الأمم المتحدة ومبادؤها التوجيهية فى القضاء الجنائي.

[1] ليندة شرابسة، مرجع سابق، ص 250.

[2] فتيحة حيمر، مرجع سابق، ص 273.

وأوصى مؤتمر الأمم المتحدة السادس لمنع الجريمة ومعاملة المجرمين بتطوير التبادل المنهج للمعلومات بوصفه عنصرا رئيسيا من عناصر خطة العمل الدوليه لمنع الجريمة ومكافحتها.

- **مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين:** تم إنعقاده فى مدينه ميلانو بإيطاليا في 26 أغسطس – 6 سبتمبر سنة 1985 م والذي انبثق عن هذا المؤتمر مجموعة من القواعد التوجيهية والتي توجت بالمصادقة على هذه المبادئ في هافانا بكوبا عام 1990 م .وقد أكد هذا المؤتمر على وجوب تطبيق التطورات الجديدة في مجال العلم والتكنولوجيا في كل مكان لصالح الجمهور لمنع الجريمة على نحو فعال كما أكد على أن التكنولوجيا بما أنها قد تولد أشكالا جديدة من الجريمة فإنه ينبغي اتخاذ تدابير ملائمة ضد حالات إساءة الاستعمال لهذه التكنولوجيا، وأشاروا إلى مسألة الخصوصية التي يمكن أن تخترق عن طريق الإطلاع على البيانات الشخصية المخزنة داخل نظم الحسابات الآلية والتي تشكل إنتهاكا و اعتداء على حرمة الحياة الخاصة لحقوق الإنسان. وأكد المؤتمر أيضا على وجوب إعتماد ضمانات ملائمة لصون السرية كذلك أكد المؤتمر عبر قواعده التوجيهية على ضرورة تشجيع التشريعات الحديثة التي تجرم وتتناول جرائم الحاسب الآلي باعتبارها نمطا من أنماط الجريمة المنظمة كغسيل الأموال والإحتيال المنظم وفتح حسابات وتشغيلها بأسماء وهمية.
- وقد أسفر المؤتمر الثامن لمنع الجريمة ومعاملة المجرميين: عن عدة توصيات تم عرضها على الجمعية العامة والتى أقرتها وأصدرتها فى ثلاثه صكوك دولية هي:

- المعاهدة النموذجية لتسليم المجرميين.
- المعاهدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية.
- المعاهدة النموذجية لتبادل المساعدة في المسائل الجنائية[1].

**2. قرارت الأمم المتحدة:**

أما عن قرارات الأمم المتحدة في هذا المجال فهي:

[1] فتيحة حيمر، مرجع سابق، ص 273.

- القرار121/54 عام 1990، وكذلك نشر دليل منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها في العام 1994.
- القرار 53/70 في 4 ديسمبر 1998، القرار 49/54 في ديسمبر 1991.
- القرار 55/28 في 20 نوفمبر 2000، القرار 19/56 في 29 نوفمبر 2001.
- القرار 59/57 في 22 نوفمبر 2002، القرار 32/58 في 18 ديسمبر 2003 حول موضوع التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي.
- القرار 55/63 في 4 ديسمبر، القرار 121/56 في 19 ديسمبر 2003 بشأن مكافحة إستخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات، ويدعو هذا القرار الدول الأعضاء عند وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات على أن تأخذ فى الإعتبار عمل لجنة منع الجريمة والعدالة الجنائية.
- قرار الجمعية العامة 239/57 في 31 جانفي 2003، القرار 199/58 في 30 جانفي 2004 بشأن إنشاء ثقافة عالمية للأمن السيبراني»، والذي يدعو الدول الأعضاء إلى التعاون وتعزيز ثقافة الأمن السيبراني[1].

تدعو الجمعية العامة في قراراتها والتي غالبا ما تكون مماثلة لقرارات الإتحاد الدولي للاتصالات الدول الأعضاء، عند وضع القوانين الوطنية والسياسات العامة لمكافحة إساءة إستعمال تكنولوجيا المعلومات وأن تأخذ في الاعتبار أعمال لجنة منع الجريمة ولجنة العدالة الجنائية وغيرها من المنظمات الدولية والإقليمية.

وقد عقدت كذلك منظمة الأمم المتحدة المؤتمر الثاني عشر لمنع الجريمة والعدالة فى الفتره من 12-19 أفريل 2010، حيث ناقشت فيه الدول الأعضاء بلجنة منع الجريمة والعدالة الجنائية وذلك بالبرازيل مختلف التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة بما في ذلك الجرائم الحاسوبية، حيث إحتل هذا النوع من الجرائم موقعا بارزا في جدول أعمال المؤتمر وذلك تأكيدا على خطورتها والتحديات التي تطرحها.

[1] فتيحة حيمر، مرجع سابق، ص 273.

إن التعاون الدولي في مكافحة الجرائم المعلوماتية يُعد أساسًا رئيسيًا لمواجهة التحديات الرقمية المعقدة حيث تسهم المنظمات الدولية والدول في تعزيز التنسيق الأمني، وتبادل المعلومات، والتعاون القضائي. إلا أن هذا التعاون يواجه بعض التحديات المتعلقة بتنسيق القوانين الوطنية، ومعايير الأمن السيبراني، مما يستدعي المزيد من التنسيق والابتكار في آليات التعاون لمواجهة تهديدات الفضاء السيبراني بفعالية أكبر. [1]

## المطلب الثاني: التعاون الدولي في مكافحة الجرائم المعلوماتية

يعد التعاون الدولي أحد العناصر الأساسية لمكافحة الجرائم المعلوماتية، وذلك نظرًا للطبيعة العابرة للحدود لهذه الجرائم. إذ يمكن أن يرتكب الجاني جريمة معلوماتية من مكان معين، بينما تكون الضحية في دولة أخرى. لذا، تتطلب مواجهة هذه الجرائم تنسيقًا فعالًا بين الدول ومنظمات الأمن الدولية بالإضافة إلى التفاعل بين الجهات المعنية بمكافحة الجرائم الإلكترونية.

### الفرع الأول: التعاون الأمني الدولي لمكافحة الجرائم المعلوماتية

بالنظر إلي التعاون الأمني الدولي بمفهومه الواسع نجد انه يشمل مجالات مختلفة، كالمجال الشرطي والمجال القانوني و المجال القضائي، و مراد ذلك أن تحقيق الأمن يتطلب تنفيذ إجراءات تتعلق بتلك المجالات المجتمعة. و التعاون الأمني الدولي لا يقتصر على إجراءات ملاحقة الأشخاص المطلوبين بل يتعدى الأمر ذلك ليشمل مكافحة الجريمة بشقيها الوقائي والقمعي بما يشمل العناية بحقوق المتهمين و الضحايا، و مراعاة حقوق الدول و سيادتها للعدالة.

[1] بيدي أمال، "**جهود الأمم المتحدة في مكافحة الجرائم السيبرانية**"، مجلة البحوث في كلية العلوم القانونية والسياسية" جامعة الجلفة، المجلد 8، العدد 1، 2022، ص 306.

## 1. مفهوم التعاون الأمني الدولي

يعرف التعاون الأمني الدولي بأنه تبادل العون و المساعدة و تضافر الجهود المشتركة بين طرفين دوليين أو أكثر لتحقيق نفع أو خدمة أو مصلحة مشتركة في مجال التصدي لمخاطر الإجرام. وما يرتبط به من مجالات أخرى، مثل مجال العدالة الجنائية، و مجال الأمن، أو لتخطي مشكلة الحدود و السيادة التي قد تعترض الجهود الوطنية لملاحقة المجرمين وتعقب مصادر التهديد، سواء كانت المساعدة المتبادلة قانونية أو قضائية أو شرطية، و سواء اقتصرت على دولتين فقط أو امتددت اقلميا أو عالميا.

ويعد التعاون الدولي ثمرة تطور العلاقات الدولية، ونتيجة حتمية لما تشهده الجريمة من تطور متلاحق يكاد يقفز في أرقامه من عام الى اخر، حتى أصبح تطور الجريمة المعلوماتية في حد ذاته ظاهرة دولية. [1]

## 2. صور التعاون الأمني الدولي لمكافحة الجرائم المعلوماتية

- **ربط شبكات الاتصال و المعلومات:** تحتاج الاتصالات الشرطية إلي وسائل للاتصال تحقق السرعة الملائمة لتتمكن أجهزة العدالة الجنائية من التواصل بين السلطات تحقيق و الملاحقة المختلفة، لذا عمدت الدول و المنظمات الدولية تطوير الاتصال وتبادل المعلومات في ما بينها.
- **القيام ببعض العمليات الشرطية و الأمنية المشتركة:** تعقب المجرم المعلوماتي و تعقب الأدلة الرقمية و ضبطها ، و قيام بعملية تفتيش العابر للحدود لمكونات الحاسب الآلي والأنظمة المعلوماتية و شبكات الاتصال بحثا عما قد تحويه من أدلة وبراهين على ارتكاب الجريمة المعلوماتية ، كلها أمور تستدعي القيام ببعض العمليات الشرطية والأمنية المشتركة، واشتراك الدول في ما بينها للقيام بعمليات شرطية و أمنية يؤدي إلى صقل مهارات و خبرات القائمين على مكافحة تلك الجرائم و بتالي وضع حد لها.[2]

---

[1] سامح أحمد موسى، "**الجوانب الاجرائية للحماية الجنائية لشبكة الانترنت**"، رسالة دكتوراه، كلية الحقوق الاسكندرية مصر، 2010، ص 523.

[2] قاضي خولة، جباس منال، "**التعاون الدولي في مكافحة الجريمة المعلوماتية**"، مذكرة لنيل شهادة ماستر، كلية الحقوق والعلوما السياسية بورقلة، الجزائر، ص 22.

### 3. التعاون الأمني و جهود منظمة الانتربول في مكافحة الجرائم المعلوماتية

الانتربول هو اكبر منظمة شرطية دولية، انشات عام 1923، و مقرها الرئيسي في مدينة ليون بفرنسا، وكما هو معروف من دستور الانتربول الدولي فهي تتكون من الجمعية العامة اللجنة التنفيذية الأمانة العامة، المكاتب المركزية الوطنية، المستشارون، لجنة ضبط ملفات الانتربول.

و طريقة العمل داخل المنظمة تتم بتبادل أعضاء الانتربول المعلومات عن المجرمين الدوليين، و يتعاونون فيما بينهم في مكافحة الجرائم الدولية، مثل جرائم التهريب، و عمليات البيع و الشراء غير المشروع للأسلحة، الجرائم الالكترونية، وقد ركز الانتربول في السنوات الأخيرة بصورة أساسية على الجريمة المنظمة و الأنشطة الإجرامية ذات الصلة بها، مثل غسل الأموال ويحتفظ أفراد المنظمة بسجلات الجرائم الدولية، وتهدف الى:

- جمع المعلومات المتعلقة بالجرائم و المجرمين، وذلك عن طريق المعلومات التي تتسلمها المنظمة المكتب الرئيسي في ليون من المكاتب المركزية الوطنية للشرطة الجنائية في الدول الأعضاء ويتم ذلك عبر شبكة اتصالات حديثة.
- التعاون مع دول الأعضاء في ضبط الهاربين والمطلوبين أيا كانت جنسياتهم و صدر ضدهم أحكام قضائية، أو أوامر بالضبط والإحضار لمثولهم أمام جهات التحقيق، وذلك من خلال اصدار النشرات الدولية المخصصة.
- دعم جهود الشرطة في مكافحة الإجرام العابر للحدود، وتقديم الخدمات في مجال الأدلة الجنائية كبصمات الأصابع، والحمض النووي.
- إنشاء وتنمية كافة المؤسسات القادرة على المساهمة الفعالة في الوقاية من جرائم القانون العامة.
- تامين وتنمية التعاون المتبادل على أوسع نطاق بين كافة سلطات الشرطة الجنائية في إطار القوانين القائمة في مختلف البلدان، وبروح الإعلان العالمي لحقوق الإنسان.[1]

[1] وريدة جندلي، "**التعاون الدولي لمكافحة الجريمة العلوماتية: الفاعلية والتحديات**"، مجلة القانون والعلوم السياسية، جامعة سكيكدة، المجلد 10، العدد 2، 2024، ص 324.

**الفرع الثاني: دوافع التعاون الدولي**

يمكن أخذ الاعتبارات التي من خلالها يمكن تبرير التعاون الدولي في مجال مكافحة الجرائم المعلوماتية، منها ما يلي:

**أولا:** أن أي دولة مهما بلغت درجة قوتها وصلابتها لا تستغني عن الدخول في علاقات تعاون متبادلة مع غيرها من الدول، خاصة وأن جهودها الداخلية في المكافحة أو الملاحقة للجرائم لم تعد بكافية لمنع الجريمة أو تقليص حجمها، وذلك بسبب التقدم التكنولوجي، مما ساعد على ظهور أنماط جديدة من الجريمة، وتفاقم حجمها على المستويات الوطنية والإقليمية والعالمية كالجريمة المنظمة، والإرهاب، وغسل الأموال، والجرائم المعلوماتية وتزييف العملة.

**ثانيا:** الجرائم المعلوماتية جرائم غير إقليمية في أغلب الأحيان، مما يؤدي إلى توزيع أركانها على عدة دول، كما أن أدلة إثباتها يسهل طمثها ومحوها مما يجعل هناك صعوبة قائمة ضد القوانين الوطنية التقليدية في مواجهة هذا النوع من الجرائم، وهذا ما جعل المجتمع الدولي يتجه نحو إنشاء أجهزة تعاونية تعمل على مستويات حكومية أو غير حكومية من أجل ضمان التنسيق والمتابعة فيما يتخذ من تدابير دولية وداخلية لوضع الالتزام الدولي بالتعاون موضع التنفيذ الإيجابي والمتكامل.

**ثالثا:** أن هذا التعاون يعتبر خطوة على طريق تدويل القانون الجنائي، ذلك أنه قمة قواعد موضوعية وإجرائية تهيمن على أذهان العديد من مقنني القرن العشرين، ومن شأن تشابه هذه القواعد أن يخلق نوعا من التقارب بين التشريعات الحالية، ويجعل الحديث عن توحيد أو تدويل القانون الجنائي أمرا قابلا للتحقيق، وبذلك نقف على أعتاب قانون جنائي دولي في سبيل مكافحة الجريمة المنظمة عابرة الحدود. [1]

**رابعا:** أنه يعتبر من قبيل التدابير المانعة من ارتكاب الجريمة، لأن المجرم سوف يجد نفسه محاطا بسياج مانعة من الإفلات من المسؤولية عن الجريمة التي ارتكبها، أو من العقوبة

[1] طارق ابراهيم الدسوقي، "**الأمن المعلوماتي النظام القانوني لحماية المعلوماتي**"، دار الجامعة الجديدة للنشر، الاسكندرية، 2009، ص 593.

التي حكم بها، فإذا ارتكب جريمة في دولة ما وتمكن من الهروب إلى دولة أخرى، فإنه سوف يكون عرضة للقبض عليه أو ترحيله إلى البلد الآخر، ومن شأن كل ذلك أن يجعل المجرم يعزف عن سلوك سبيل الجريمة، بما يحقق الردع الخاص للمجرم المعلوماتي، وعلى المستوى الأعم يتحقق الردع العام عندما تجد العقوبة سبيلها للتطبيق على الجريمة المعلوماتية المرتكبة.[1]

## المطلب الثالث: التحديات القانونية والأخلاقية في التعاون الدولي

يعد التعاون الدولي أمرًا ضروريًا لمكافحة الجرائم المعلوماتية، نظرًا لطبيعتها العابرة للحدود. غير أن هذا التعاون يصطدم بعدة تحديات قانونية وأخلاقية تعيق فعاليته، وتتطلب جهودًا متزايدة لتجاوزها وتحقيق توازن بين المكافحة الفعّالة للجريمة وحماية الحقوق والحريات الأساسية للأفراد.

### الفرع الأول: التحديات القانونية والأخلاقية في مكافحة الجرائم المعلوماتية على المستوى الوطني

يشكل التعاون الدولي في مكافحة الجرائم المعلوماتية ضرورة ملحة في ظل الطابع العابر للحدود لهذه الجرائم، إلا أن تفعيل هذا التعاون على المستوى الوطني يواجه عدة إشكاليات تحدّ من فعاليته، ويمكن تلخيص أبرزها فيما يلي:

#### 1. عدم كفاية وملاءمة القوانين القائمة:

التطور في المجال التكنولوجي سواء من ناحية الحياة العامة أو الخاصة واعتماد الجميع عليه في سائر شؤونهم، واستغلال الجناة لتلك التقنية في ارتكاب جرائمهم، هذا التطور في الحقيقة لا يقابل التطور بذات الدرجة في النصوص القانونية.

وبالتالي فإن الكثير من نصوص القوانين الجنائية الداخلية لبعض الدول لا تكفي بوضعها الحالي لمواجهة تلك الصور المستحدثة من الجرائم، لتطلب غالبية النصوص الصفة المادية

[1] طارق ابراهيم الدسوقي، مرجع سابق، ص 593.

في الشيء محل ارتكاب الجريمة، وهو ما يتنافى مع الطبيعة المعلوماتية، وبالتالي تخرج تلك الصور من طائلة التجريم والعقاب. [1]

وعلى الرغم من إصدار العديد من الدول للتشريعات المتعلقة بالجرائم المعلوماتية وانضمامها للعديد من الاتفاقيات الدولية التي تجرم الأفعال المخالفة للمعاهدات المنظمة لهذه الجرائم إلا أن هذه النصوص غير كافية لمعالجة سائر الجرائم المرتكبة في مجال الكمبيوتر والإنترنت الأمر الذي يؤدي لتقليل جهود رجال الشرطة عند ضبط الجرائم والكشف عن مرتكبيها، كما أن الكثير من التشريعات الداخلية للدول وإن كانت تحتوي على قواعد عامة يمكن تطبيقها على الجرائم التقليدية إلا أنه نظراً لاختلاف أركان وشروط الجرائم المعلوماتية عن أركان وشروط الجرائم التقليدية فإنه يترتب على ذلك عدم إمكان تطبيق هذه النصوص على هذه الجرائم، مما يصعب مهمة الأجهزة الشرطية والقضائية في ضبط هذه الجرائم وملاحقة مرتكبيها قضائيا.

**2. صعوبة إثبات الجرائم المعلوماتية والتحقيق فيها:**

من إشكاليات الجرائم المعلوماتية أنها تتميز في أكثر صورها بأنها مستترة وخفية لا يلحظها المجني عليه غالباً أو يدري حتى بوقوعها، فهي غالباً ما تكشف بمحض الصدفة ولذلك توصف بالجريمة غير المرئية، ومما يزيد الأمر تعقيداً هو أن الجريمة المعلوماتية ما تتم عن بعد، حيث لا يتواجد الفاعل على مسرح الجريمة ومن ثم تتباعد المسافات بين الفعل والنتيجة.

فالفعل الإجرامي في هذه الجرائم ليس له آثار مادية، فلا يوجد أدلة قولية أو مادية أو حالات تلبس يمكن إدراكها بالحواس، حيث إن الدليل في هذه الجرائم يكون في صورة نبضات إلكترونية غير محسوسة، مما يتطلب من المحقق أن تكون لديه دراية علمية كافية بأنظمة الحاسب وحقيقة تشغيلها، حتى يتسنى له التعامل معها للبحث عن الأدلة والمحافظة عليها.

[1] عزيزة لرقط، " **التعاون الدولي في مكافحة الجرائم المعلوماتية: اشكالاتها واليات التغلب عليها**"، مجلة التواصل كلية الحقوق والعلوم السياسية، عنابة، مجلد، 25، العدد 4، 2019، ص 3.

كما أن المجرم في هذه الجرائم يحاول قدر الإمكان إعاقة الوصول إلى الدليل بشتى الوسائل فهو بعد ارتكاب جريمته يقوم بدس برامج أو وضع كلمات سرية ورموز تعوق الوصول إلى الدليل، أو يلجأ إلى تشفير التعليمات مما يصعب الوصول إلى دليل يدينه، حيث إنه من السهل على المجرم في أغلب الجرائم المعلوماتية محو الدليل في زمن قياسي، ولا يستغرق ذلك سوى دقائق معدودة بالاستعانة بالبرامج المخصصة لذلك.[1]

وترجع صعوبة إثبات الجرائم المعلوماتية – فضلاً عما سبق – إلى الأسباب التالية:

- صعوبة الاحتفاظ الفني بآثارها إن وجدت.
- الحرفية الفنية العالية التي تتطلبها من أجل الكشف عنها نقض خبرة رجال الشرطة والتحقيق، وهذا ما يعرقل عمل المحقق الذي تعود على التعامل مع الجرائم التقليدية.
- اعتمادها على الخداع في ارتكابها، والتضليل في التعرف على مرتكبيها، والذين يعتمدون على التخفي عبر دروب الإنترنت تحت قناع فني.

**الفرع الثاني: اشكاليات التعاون الدولي في مجال مكافحة الجرائم المعلوماتية**

رغم الأهمية القصوى للتعاون الدولي في التصدي للجرائم المعلوماتية، إلا أن هذا التعاون يواجه تحديات وإشكاليات عديدة على المستوى الدولي، ترتبط أساسًا باختلاف النظم القانونية، وتضارب المصالح وصعوبة تنسيق الجهود في فضاء إلكتروني مفتوح وعابر للحدود. ومن أبرز هذه الإشكاليات:

**1. القصور التشريعي للدول والتعارض بين مصالحها:**

إن اختلاف الأنظمة القانونية للدول يعد عقبة كبيرة تعترض سبيل التعاون الدولي بين تلك الدول في مجال مكافحة الجرائم المعلوماتية، لما يترتب على ذلك الاختلاف من مشكلات تطبيق القانون، وما يثيره هذا الاختلاف من مشكلات في الواقع العملي، كما أن قصور غالبية النظم التشريعية للدول عن وضع مفهوم محدد للجرائم المعلوماتية، وكذلك قصورها في وضع نظام قانوني خاص لتلك الجرائم يجعل سبل التعاون الدولي أمراً صعباً.

[1] عزيز لرقط، مرجع سابق، ص 4.

وبنظرة متأنية للأنظمة القانونية القائمة في الكثير من الدول لمواجهة الجرائم المعلوماتية يمكن القول بعدم وجود اتفاق عام بين الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الإنترنت الواجب تجريمها أو بمعنى آخر عدم وجود نظام قانوني لدى الدول خاص بمكافحة الجرائم المعلوماتية، فما يكون مباحاً في أحد الأنظمة قد يكون مجرماً في نظام آخر، ويمكن إرجاع ذلك إلى عدة أسباب، منها اختلاف البيئات والعادات والتقاليد والديانات والثقافات من مجتمع لآخر، وبالتالي اختلاف السياسة التشريعية من مجتمع لآخر، وقد يتجلى سبب غياب هذا النموذج في كثرة التعاريف والمفاهيم القانونية التي تتعلق بهذا الأمر فكل دولة تضع تعريفات ومصطلحات حسب أنظمتها القانونية الجنائية، وتحديداً الناتجة أساساً عن التطور الذى يعرفه المجال المعلوماتي.

وهذا ما ينعكس سلباً على إجراءات التعاون الدولي، حيث إن عدم النص على جميع الجرائم المعلوماتية والتي تهدد أمن واقتصاديات الدول يؤثر ذلك على صانعي القرار في المجالات المختلفة، وخاصة المجالات السياسية والاقتصادية، مما يؤثر بالسلب على الاتجاه السياسي والفكرالقانوني والتجريم والعقاب في مختلف الدول.

كما أن القصور التشريعي الداخلي لمختلف الدول في وضع نظام قانوني خاص بالجرائم المعلوماتية يقف عائقا أمام التعاون الدولي في مواجهة هذه الجرائم، حيث إن ترك هذه الجرائم لتطبق عليها القواعد القانونية العامة لا يتلاءم مع طبيعتها التقنية، مما يؤدي إلى إفلات المجرمين من العدالة وإهدار الحقوق للإفراد المجني عليهم ، وعندما تتعارض مصالح الدول فإن ذلك يمثل عقبة كبيرة تعترض سبل التعاون الدولي، إذ تلجأ كل دولة إلى تغليب ما تقضيه مصالحها ولو تعارض مع مصلحة الدولة الأخرى، وتتوقف قدرة الدول على التعاون الدولي في مسائل العدالة الجنائية وتنفيذ القوانين إلى حد ما على العلاقات السياسية القائمة بينها.[1]

### 2. تنوع واختلاف النظم القانونية الإجرائية:

بسبب تنوع واختلاف النظم القانونية الإجرائية نجد أن طرق التحري والتحقيق والمحاكمة التي تثبت فاعليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى، أو قد لا يسمح بإجرائها

[1] عزيز لرقط، مرجع سابق، ص 5.

كما هو الحال بالنسبة للمراقبة الإلكترونية، والتسليم المراقب، والعمليات المستترة، وغيرها من الإجراءات المشابهة، فإذا ما اعتبرت طريقة ما من طرق جمع الاستدلالات أو التحقيق أنها قانونية في دولة معينة، قد تكون ذات الطريقة غير مشروعة في دولة أخرى، وبالتالي فإن الدولة الأولى سوف تشعر بخيبة أمل لعدم قدرة سلطات إنفاذ القانون في الدولة الأخرى على استخدام ما تعتبره هي أنه أداة فعالة، بالإضافة إلى أن السلطات القضائية لدى الدولة الثانية قد لا تسمح باستخدام أي دليل إثبات جرى جمعه بطرق ترى هذه الدولة أنها طرقاً غير مشروعة، حتى وإن كان هذا الدليل تم الحصول عليه في اختصاص قضائي وبشكل مشروع.

وهذا يعني عدكم وجود تنسيق بين الدول المختلفة فيما يتعلق بالاجراءات الجنائية المتبعة بشأن الجرائم المعلوماتية، سواء ما تعلق منها بأعمال الاستدلال أو التحقيق أو المحاكمة.

تُعد الإشكاليات الوطنية في التعاون الدولي لمكافحة الجرائم المعلوماتية من أبرز العوائق أمام التصدي الفعال لهذا النوع من الجرائم، حيث تعاني العديد من الدول من ضعف التشريعات، نقص البنية التحتية التقنية، وتداخل الصلاحيات بين الهيئات المعنية. كل ذلك يستدعي ضرورة تطوير الإطار القانوني، وتعزيز الكفاءات المتخصصة، ووضع سياسات واضحة لضمان مشاركة فعالة في التعاون الدولي[1].

[1] عزيز لرقط، مرجع سابق، ص 6.

## خلاصة الفصل

تطرق هذا الفصل الإطار النظري للجرائم المعلوماتية عبر دراسة مفهومها وتعريفها العام، مع إبراز الفروقات الجوهرية بينها وبين الجرائم التقليدية، سواء من حيث الوسائل أو طبيعة الضحايا أو نطاق ارتكابها. كما قمنا بتصنيف أنواع الجرائم المعلوماتية وفقًا للجهة المستهدفة، سواء كانت أفرادًا، مؤسسات أو دولًا، مع تحليل آليات ارتكاب هذه الجرائم عبر استعراض خصائصها وأركانها القانونية.

كما استعرضنا الإطار القانوني الجزائري لمكافحة الجرائم المعلوماتية، بالتركيز على القوانين الوطنية ذات الصلة، والتعديلات التشريعية التي حاولت مواكبة التطورات التقنية، بالإضافة إلى دور الهيئات الرسمية مثل وزارة الداخلية والدرك الوطني. ورغم هذه الجهود، كشف الفصل عن وجود تحديات حقيقية تتعلق بسرعة التطور التكنولوجي وضعف التنسيق بين المؤسسات.

وعلى المستوى الدولي، سلطنا الضوء على أبرز الاتفاقيات الدولية مثل اتفاقية بودابست ودور الأمم المتحدة في دعم الجهود العالمية لمكافحة هذه الجرائم، بالإضافة إلى أهمية التعاون الدولي، وما يصاحبه من إشكاليات قانونية وأخلاقية تتعلق باختلاف القوانين بين الدول وصعوبة تحقيق التوازن بين حماية الأمن واحترام الحقوق والحريات.

ما يمكن أن نصل اليه في نهاية هذا الفصل الى أن الجرائم المعلوماتية من بين أكثر الظواهر الإجرامية تعقيدًا وتسارعًا في التطور، ما يجعل مواجهتها أكثر صعوبة مقارنة بالجرائم التقليدية. فرغم ما شهدته التشريعات الوطنية من تطورات ملموسة في سبيل التصدي لهذه التهديدات، إلا أن هذه المنظومات القانونية لا تزال بحاجة إلى مراجعة وتحديث مستمرين لمواكبة الأساليب المتجددة التي يستخدمها مرتكبو الجرائم الإلكترونية. وفي هذا السياق، يُمثل التنسيق المؤسسي بين مختلف الجهات الوطنية، من أمنية وقضائية وتقنية أحد أهم عوامل النجاح في التصدي الفعّال لهذه الجرائم. وعلى الصعيد الدولي، أصبح التعاون بين الدول أمرًا لا غنى عنه في ظل الطبيعة العابرة للحدود للجرائم المعلوماتية، إلا أن اختلاف النظم القانونية والثقافية يشكل تحديًا حقيقيًا أمام بناء شراكات أمنية متماسكة وفعّالة.

لذا، فإن مكافحتها تتطلب استراتيجية وطنية ودولية شاملة، تقوم على محاور متكاملة تشمل تحديث التشريعات، نشر الوعي المجتمعي، تنمية القدرات التقنية للأجهزة المختصة، وتعزيز أطر التعاون الإقليمي والدولي. وعليه، فإن مكافحة هذا النوع من الجرائم لم تعد مسؤولية محلية حصرية، بل أضحت مسؤولية جماعية تستوجب تنسيقًا وتكاملًا بين مختلف الفاعلين على المستويين الوطني والدولي.

# الفصل الثاني:

## الاستراتيجيات المعتمدة في مكافحة الجرائم المعلوماتية

**تمهيد:**

شهد العالم خلال العقود الأخيرة طفرة هائلة في مجال تكنولوجيا المعلومات والاتصالات، أحدثت تحولاً جذريًا في مختلف مجالات الحياة، من الاقتصاد والتعليم إلى الأمن والعلاقات الاجتماعية. ومع هذا التطور المتسارع، ظهرت إلى السطح تحديات جديدة لم تكن مطروحة بهذه الحدة من قبل.

وبناءً على ما تم عرضه وتحليله في الفصل الأول، الذي تناول الإطار المفاهيمي للجرائم المعلوماتية، وتحدياتها القانونية والتنظيمية، تبرز الحاجة الملحة إلى تسليط الضوء على الاستجابات العملية لهذه الظاهرة، من خلال استعراض وتحليل الاستراتيجيات المعتمدة في مواجهتها على المستويين الوطني والدولي. ويأتي هذا الفصل ليُعنى بشكل خاص بدراسة هذه الاستراتيجيات، ليس فقط من خلال عرض الأطر النظرية والسياسات العامة، بل من خلال التركيز على التدابير الوقائية والأمنية والإجرائية المعتمدة، التي تمثل جوهر الاستجابة الفعالة لهذه الجرائم.

كما سيتم التطرق إلى نماذج من التعاون الدولي، الذي يعد عنصرًا حاسمًا في ضوء الطبيعة العابرة للحدود لهذه الجرائم، فضلًا عن استعراض التجارب الرائدة لبعض الدول والمنظمات الإقليمية والدولية التي وضعت استراتيجيات شاملة لمكافحة الجريمة الإلكترونية. ويهدف هذا الطرح إلى إبراز أفضل الممارسات التي يمكن الاستفادة منها وتكييفها مع خصوصيات السياقات الوطنية، مما يسهم في دعم بناء منظومة متكاملة وفعالة لمواجهة التحديات السيبرانية.

يخصص هذا الفصل لدراسة:

- **المبحث الاول:** الاستراتيجية الأمنية لمكافحة الجرائم المعلوماتية
- **المبحث الثاني:** الاستراتيجية الدولية لمكافحة الجرائم المعلوماتية
- **المبحث الثالث:** تجارب الدول في مكافحة الجرائم المعلوماتية

## المبحث الأول: الاستراتيجية الوطنية لمكافحة الجرائم المعلوماتية

نظراً لتزايد معدلات الجرائم المعلوماتية، ظهرت تحديات قانونية جديدة تتعلق بانتشار الجرائم المعلوماتية وضروة التصدي لها بفعالية، وقد عمل المشرع الجزائري على مواجهة هذه الظاهرة من خلال وضع تدابير وقائية و اثباتية تتلائم مع طبيعة البيئة الرقمية.

يهدف هذا المبحث الى تسليط الضوء على الجوانب الاساسية لمكافحة الجريمة المعلوماتية في الجزائر من خلال عرض التدابير الوقائية والاجراءات المتبعة لاثبات الجريمة المعلوماتية اضافة الى النصوص القانونية التي تجرم الافعال المعلوماتية وفقا للنصوص القانونية المعمول بها في الجزائر.

### المطلب الأول: الاستراتيجيات الأمنية

تلعب الأجهزة الأمنية دوراً محورياً في التصدي للجرائم المعلوماتية، نظراً لطبيعتها التقنية المعقدة وخطورتها على الأمن العام، وقد اعتمدت الجزائر مجموعة من الاستراتيجيات الأمنية التي تهدف إلى تعزيز قدرة الدولة على الوقاية من هذه الجرائم وكشفها والتعامل معها بفعالية. [1]

#### الفرع الأول: التدابير الوقائية

**1. المراقبة الالكترونية:**

حيث سمح باللجوء لهذا الإجراء في حالات محددة حصرا المادة 04 من القانون 09-04 ص 06 و تكون بموجب إذن مكتوب من السلطات القضائية المختصة، للوقاية من الأفعال الإرهابية أو التخريبية أو الجرائم الماسة بأمن الدولة، أو في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، كما أنه لمقتضيات التحريات و التحقيقات القضائية عندما يكون

[1] مهدي رضا، مرجع سابق، ص 118.

من الصعب الوصول إلى نتيجة م الأبحاث الجارية دون اللجوء إلى هذا الإجراء، و يمكن الاستعانة بالمراقبة الالكترونية في إطار تنفيذ المساعدة القضائية الدولية المتبادلة.

**2. الاستعانة بمزودي الخدمات للوقاية من الجرائم السبيرانية:**

ويكون ذلك من خلال تقديم مزودي الخدمات المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات تحت تصرف السلطات وتشمل هذه المعطيات: المادة 11 من القانون 09-04 ، ص 07. [1]

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

ويشترط التزام مقدمي الخدمات بحفظ هذه المعطيات وأطلق عليها: المعطيات المتعلقة بحركة السير، ولم يغفل تعريفها بموجب المادة الأولى من هذا القانون بأنها: أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة الاتصالات وتوضع مصدر الاتصال والوجهة المرسل إليها والطريق الذي يسلكه ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة.

زيادة على ذلك أفرد المشرع الجزائري مجموعة التزامات خاصة بمقدمي خدمات الانترنت المادة 12 من القانون 09-04، ص 08 تشمل التدخل الفوري لسحب المحتويات المخالفة للقوانين وتخزينها أو حضر الدخول إليها، إضافة إلى الالتزام بموضع ترتيبات تقنية تحصر إمكانية الدخول إلى الموزعات التي تحتوي على معلومات مخالفة للنظام العام أو الآداب العامة.

[1] مهدي رضا، مرجع سابق، ص 119.

**الفرع الثاني: التدابير الاجرائية**

**1. تفتيش وحجز المنظومة المعلوماتية**

فلمقتضيات حماية النظام العام او لمستلزمات التحريات أو التحقيقات القضائية الجارية، تم وضع مجموعة ترتيبات تقنية لمراقبة الاتصالات الالكترونية، وتجميع وتسجيل محتواها في حينها، والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية المادة 03 من القانون 09-04 ، ص06. [1]

غير أن إجراء الحجز قد تصادفه عدة إشكالات لأسباب تقنية مما يتعين على السلطات التي تقوم بالتفتيش استعمال تقنيات مناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.المادة 07 من القانون 09-04، ص 07.

وجدير بالذكر أن هذا القانون أجاز اللجوء إلى التفتيش ولو عن بعد بسرعة الى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، كما يمكن التفتيش عن بعد في منظومة تخزين معلوماتية. ويمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدة وتزويدها بكل المعلومات ضرورية.

**2. تمديد الاختصاص بنظر الجرائم المعلوماتية**

حيث يؤول الاختصاص للمحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، في حالة ارتكاب الجريمة من أجنبي وكانت الجريمة تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.

**3. المساعدة القضائية الدولية:**

كما تناولنا سابقا يسمح المشرع الجزائري بإمكانية تبادل المساعدة القضائية الدولية لجمع الأدلة المتعلقة بالجريمة في شكلها الالكتروني، ومن الممكن الاستجابة لطلبات المساعدة

[1] مهدي رضا، مرجع سابق، ص 120.

الرامية إلى تبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية او وفقا لمبدأ المعاملة بالمثل.

الجرائم السيبرانية جرائم يصعب التحكم فيها و التصدى لها نظرا لخصوصيتها باعتبارها جرائم عابرة للجغرافيا، وأيضا باعتبار أن التطور المذهل في الجانب التكنولوجي والالكتروني والرقمي صعب هو الآخر من مهمة مكافحة هذه الجريمة.[1]

**المطلب الثاني: طرق اثبات الجريمة الالكترونية**

تعد الجريمة الإلكترونية جريمة تقنية تحتاج للدقة في التعامل معها سواء من ناحية الإجراءات المتبعة بشأنها أو من ناحية وسائل إثباتها والتي يجب مواكبتها وإعطاء خصوصيات لها، ويمكن حصر أهمها في الاستجواب والشهادة و الخبرة.

**الفرع الأول: الاستجواب الإلكتروني**

يعتبر الاستجواب الإلكتروني أحد إجراءات التحقيق في الجريمة الإلكترونية للكشف عن هوية المتهم وعلاقته بالجريمة، كما أنه محاط بجملة من الشروط والضمانات التي تكفل تحقيق عادل.

**1. مفهوم الاستجواب الإلكتروني**

يعتبر إجراء قضائي يقوم به قاضي التحقيق وهو على أربع مستويات استجواب عند الحضور الأول و استجواب في الموضوع و استجواب اجمالي و استجواب في حالة الإستعجال، حيث يقوم قاضي التحقيق من خلال الإستجواب الأولي من التأكد من هوية المتهم وإحاطته بالوقائع المجرمة المنسوبة إليه و تعيين محامي له إذا لم يختر المتهم محامي له بشرط أن يكون قد طلب ذلك و بالنسبة للإستجواب في الموضوع فإنه يؤخذ كقرينة ضد المتهم وهذا كله في ظل استيفاء الشروط القانونية و احترام الضمانات المقررة عند الإستجواب وهو ما نصت عليه المواد من 100 إلى 105 من قانون الإجراءات الجزائية المعدل والمتمم.

[1] مهدي رضا، مرجع سابق، ص 124.

### 2. قواعد استجواب المجرم الالكتروني

يقبع في ذلك أسلوب قبلي ويتمثل في تبادل المعلومات بين قاضي التحقيق والخبير الالكتروني حيث يقوم هذا الاخير بشرح كافة الأبعاد التقنية والمصطلحات الالكترونية لقاضي التحقيق والتي يمكن استخدامها أثناء الاستجواب وفي الأخير وضع خطة الاستجواب بناء على المعطيات السابقة وأسلوب بعدي أي عند بدء الاستجواب حيث يتم إتاحة الفرصة للخبير لحضور جلسة الاستجواب مع إمكانية توجيه أسئلة فرعية للمتهم و في حال الدول التي لا تسمح بذلك يستحب تكوين لجان تحقيق الحضور الخبير في عضويتها تفادي إضاعة الوقت في استجواب المتهم حول جريمة لا يمكن اكتشافها مع تحرير محضر الإستجواب بكل دقة ووضوح.[1]

## الفرع الثاني: الشهادة الإلكترونية

تعرف الشهادة عموما على أنها أقوال يدلي بها غير الخصوم أمام الجهات القضائية وإسنادها للمتهم بالنفي أو الإثبات وهي على أنواع شهادة مباشرة ونقصد بها كل شخص شهد وقوع الجريمة بحواسه أي شهادة سماعية حيث نقلها شخص لشخص آخر، و شهادة بالتسامع وهي التي سمعها شخص من ما يتداوله الناس من أقوال وتختلف القيمة الثبوتية لهذه الأنواع من الشهادة حسب تدرجها، نص المشرع الجزائري على مختلف أحكامها في المواد من 220 إلى 238 من قانون الإجراءات الجزائية المعدل والمتمم. [2]

### 1. تعريف الشاهد الإلكتروني

يقصد به صاحب الخبرة و التخصص في المجال الإلكتروني حيث تكون له معلومات عن شبكة الانترنت و شبكات الاتصال . حيث تشمل فئات الشهادة بهذا المفهوم عدة طوائف منها مستخدموا الحاسب الآلي وخبراء البرمجة والمحللون و مهندسو الصيانة و الخبراء التقنيين ومقدمي الخدمات الوسيطة.

---

[1] حاحة عبد العالي، قلات سمية، **"المكافحة الاجرائية للجرائم الالكترونية –دراسة حالة الجزائر-"**، كلية الحقوق و العلوم السياسية محمد خيضر ببسكرة، الجزائر، مجلة المفكر، المجلد 13، العدد 02، 2018، ص 233.

[2] المرجع نفسه، ص 234.

### 2. إلزام الشاهد بتقديم معلومات عن الجريمة الإلكترونية

بالرغم من اختلاف الفقه والقانون بخصوص هذا الشأن إلا أن موقف المشرع الجزائري محدد من خلال المادة 10 من القانون رقم 09/04 إذ ألزمت مقدمي الخدمات بالتعاون مع السلطات المكلفة بالتحريات القضائية من أجل تزويدهم بكافة المعطيات المتعلقة بمحتوى الإتصالات وفي هذا الإطار نجد أن المشرع الجزائري ألقى مجموعة من الالتزامات على عاتق مقدمي الخدمات منها حفظ المعطيات المتعلقة بحركة سير أي حمايتها ومنع إتلافها وقد تم تحديد أنواع هذه المعطيات وهذا كله في المادة 11 وكذلك ما نصت عليه المادة 12 من التدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين و تخزينها أو جعل الدخول إليها غير ممكن وكذا وضع الترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة و إخبار المشتركين لديهم بوجودها، من خلال هذا يحاول المشرع الجزائري حصر الجريمة الإلكترونية وتطويقها من مختلف الجوانب.

### 3. التزامات الشاهد في الجريمة الإلكترونية

نذكر منها طبع ملفات البيانات المخزنة وتسليمها للسلطات القضائية والإفصاح عن كلمات المرور و الكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج المختلفة .[1]

### الفرع الثالث: الخبرة الإلكترونية

عادة ما تعترض القاضي الجزائي أمور فنية تحتاج لذوي الاختصاص كل في مجاله منها الجريمة الإلكترونية، لذا تسند مهام الخبرة لرجال خارج القضاء في نطاق الشروط الواجب احترامها.

[1] حاحة عبد العالي، قلات سمية، مرجع سابق، ص 235.

## 1. مفهوم الخبرة الإلكترونية

يقصد بها عموما استخدام قدرات شخص الفنية أو العلمية والتي لا تتوافر لدى رجل القضاء أو المحقق من أجل الكشف عن دليل أو قرينة تفيد في معرفة الحقيقة بشأن وقوع الجريمة أو نسبتها إلى المتهم.

من خلال التعريف أعلاه نستنتج أن الخبرة وسيلة من وسائل الإثبات الفنية التي تتطلب الاستعانة بذوي التخصص من غير رجال القضاء وقد نظم المشرع مختلف أحكامها من اختيار الخبراء وواجباتهم منها حلف اليمين و خضوعهم للرقابة القضائية و قيامهم بأداء مهامهم بأنفسهم و إبداع التقارير في المدة المحددة، في المواد من 143 إلى 156 من قانون الإجراءات الجزائية المعدل والمتمم بالقانون رقم 06/22 ولقد أشار المشرع الجزائري للخبرة في مجال الجريمة الإلكترونية أيضا من خلال الفقرة الأخيرة من المادة 5 من القانون رقم 09/04 عندما نصت على أنه يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية قصد مساعدتها وتزويدها بكل المعلومات الضرورية وكذلك المادة 19 من المرسوم 15/261 السابق ذكره حيث سمحت للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الإستعانة بأي خبير قصد مساعدتها في أعمالها. [1]

## 2. القواعد الالكترونية التي تحكم الخبرة الإلكترونية

وتتجسد في خطوات ما قبل التشغيل نذكر منها التأكد من مطابقة محتويات أحراز المضبوطات لما هو مدون عليها وكذلك من صلاحية وحدات النظام للتشغيل وفي خطوات التشغيل و الفحص والتي تتجلى في استكمال تسجيل باقي معطيات الوحدات من خلال قراءات الجهاز وعمل نسخة من كل وسائط التخزين المضبوطة لإجراء الفحص المبدئي على هذه النسخة لحماية الأصل، تحديد أنواع وأسماء المجموعات البرامجية إظهار الملفات المخبأة، والقاعدة الثالثة تحديد مدى ترابط بين الدليل المادي والتقني وفي الأخير تدون النتائج وإعداد التقارير.

[1] حاحة عبد العالي، قلات سمية، مرجع سابق، ص 236.

## المطلب الثالث: تجريم الأفعال المعلوماتية في القانون الجزائري

في ظل التنامي السريع لاستخدام تكنولوجيات الإعلام والاتصال، وظهور أنماط جديدة من السلوك الإجرامي، وجدت الجزائر نفسها أمام ضرورة ملحّة لتأطير هذا المجال قانونياً. فالجريمة المعلوماتية لم تعد مجرد تهديد محتمل، بل أصبحت واقعاً ملموساً يمس الأفراد المؤسسات، والدولة على حدّ سواء .وقد سعى المشرّع الجزائري إلى مواجهة هذه الظاهرة من خلال سن تشريعات خاصة تجرم الأعمال المعلوماتية وتحدد طبيعتها وأركانها والعقوبات المقررة لها، سواء في قانون العقوبات أو في القوانين الخاصة ذات الصلة، وذلك في إطار التزامات الدولة بحماية أمن المعلومات وضمان الاستخدام الآمن للفضاء الرقمي.

### الفرع الأول: تجريم الأفعال الالكترونية في اجراءات القانون

لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل مما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتمم لأمر 66-156، حيث أضيف قسم بعنوان "المساس بأنظمة المعالجة الآلية للمعطيات ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى 394 مكرر ونصت هذه المواد على ما يلي :

نصت المادة 394 مكرر على جريمة الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات محاولة ذلك بنصها " يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 5000 دج إلى 100000 دج كل من يدخل أو يبقى عن طريق الغش في كل جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك . [1]

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير معطيات المنظومة. وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000دج.

[1] بولحية شهرزاد، خلوفي رشيد، "**تحديات الجريمة الالكترونية في الجزائر**"، جامعة الجزائر 1، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد 02، 2019، ص 1989.

نصت المادة 394 مكرر 1 على إدخال أو إزالة أو تعديل بطريق الغش معطيات في نظام المعالجة الآلية بنصها " يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500.000 دج إلى 2000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أوعدل الغش المعطيات التي يتضمنها".

نصت المادة نصت المادة 394 مكرر 2 على أن يعاقب بالحبس من شهرين الى ثلاث أشهر وبغرامة من 1000.0000 دج الى 5000.0000 دج كل من يقوم عمدا وعن طريق الغش بما يأتي:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

نصت المادة 394 مكرر3 على أنه: تضاعف العقوبة المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد.

نصت المادة 394 مكرر4 على أنه : يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات بالحد الأقصى للغرامة المقررة للشخص الطبيعي .[1]

نصت المادة 394 مكرر5 على فعل اشتراك في جريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم فإنه يعاقب بنفس عقوبة المقررة للجريمة في حد ذاتها وذلك بنصها: كل من شارك في مجموعة أو في اتفاق بغرض الإعداد الجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها.

[1] بولحية شهرزاد، خلوفي رشيد، مرجع سابق، ص 1990.

نصت المادة 394 مكرر6 على: مع الاحتفاظ بحقوق الغير حسن النية، بحكم مصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها.

نصت المادة 394 مكرر6 على: مع الاحتفاظ بالحقوق غير الحسنة ، بحكم مصادرة الأجهزة والبرامج المستخدمة في اغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفق لهذا القسم، علاوة على اغلاق المحل أو مكان الاستغلال اذا كانت الجريمة قد ارتكبت بعلم مالكها.

نصت المادة 394 مكرر7على أنه: يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المكررة للجنحة ذاتها.[1]

في عام 2006 أدخل المشرع الجزائري تعديلا آخرا على قانون العقوبات بموجب قانون رقم 06-2339 المؤرخ في 20 ديسمبر 2006 حيث مس ذلك التعديل القسم السابع مكرر والخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وقد تم تشديد العقوبة المقررة لهذه الأفعال فقط دون المساس بالنصوص التجريمية الواردة في هذا القسم من القانون 04-15 وربما يرجع سبب هذا التعديل إلى ازدياد الوعي بخطورة هذا النوع المستحدث عن الإجرام باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى وشيوع ارتكابه ليس فقط من الطبقة المثقفة بل من قبل الجميع بمختلف الأعمار ومستويات التعليم نتيجة تبسيط وسائل التكنولوجيا المعلومات وانتشار الأنترنت كوسيلة لنقل المعلومات.

**الفرع الثاني: تجريم الأفعال الإلكترونية في قانون الإجراءات الجزائية**

نجد أن المشرع نص على تمديد الاختصاص المحلي لوكيل الجمهورية في جرائم الإلكترونية في المادة 37 قانون الإجراءات الجزائية. ونص على التفتيش في المادة 45 الفقرة 7 وعلى توقيف النظر في جريمة المساس بأنظمة المعالجة في المادة 51 الفقرة 6 وعلى تراض المراسلات وتسجيل الأصوات والتقاط الصور من المادة 65 مكرر 5 إلى 65 مكرر 10.

[1] بولحية شهرزاد، خلوفي رشيد، مرجع سابق، ص 1990.

أما بالنسبة لنصوص إجراءات التحقيق والمحاكمة تطبق عليه نفس إجراءات الجريمة التقليدية.

ومع ذلك، فقد شهد قانون الإجراءات الجزائية الجزائري عدة تعديلات مهمة لمواكبة الجرائم الإلكترونية وخصوصاً من خلال إدراج وسائل التحقيق الخاصة التي تُستخدم عادة في كشف هذا النوع من الجرائم. إليك أبرز النقاط المتعلقة بتجريم وملاحقة الأعمال الإلكترونية في إطار الإجراءات الجزائية: [1]

- **التفتيش الإلكتروني والمصادرة الرقمية:**

من خلال التعديلات التي جاء بها القانون رقم 07-17المؤرخ في 27مارس 2017، تم السماح بالتفتيش في الأنظمة المعلوماتية، بما في ذلك:

- الدخول إلى الحواسيب والخوادم.
- نسخ البيانات أو حجزها.
- تحليل محتوى الوسائط الرقمية.

المادة 65 مكرر 5 الى المادة 65 مكرر15 تُنظم إجراءات التفتيش والمعاينة الإلكترونية.

- **التحقيق باستخدام وسائل خاصة:**

في إطار الجرائم الخطيرة مثل الجرائم المعلوماتية، أتاح القانون استعمال:

- التنصت على الاتصالات الإلكترونية.
- المراقبة عن بُعد للأشخاص والمواقع الإلكترونية.
- اختراق الحسابات بموافقة النيابة العامة أو قاضي التحقيق.

رغم أن قانون الإجراءات الجزائية لايُجرّم الجرائم الإلكترونية بشكل مباشر، فإنه يُعطي الأدوات القانونية اللازمة لملاحقتها وكشف مرتكبيها عبر آليات التفتيش الإلكتروني والمراقبة، في تكيّف واضح مع طبيعة الجرائم المعلوماتية التي تتطلب وسائل إثبات خاصة وفعالة.

[1] بولحية شهرزاد، خلوفي رشيد، مرجع سابق، ص 1991.

## المبحث الثاني: مظاهر التعاون الدولي في مكافحة الجرائم المعلوماتية

شهد العالم في العقود الأخيرة تطوراً تكنولوجياً هائلاً صاحبه تصاعد كبير في حجم وتعقيد الجرائم المعلوماتية، ما دفع المجتمع الدولي إلى التفكير في بلورة استراتيجيات موحدة أو منسقة لمواجهتها .ونظراً للطبيعة العابرة للحدود لهذه الجرائم، لم تعد الإجراءات الوطنية وحدها كافية، بل بات من الضروري اعتماد آليات دولية قانونية وتنظيمية لتعزيز التعاون بين الدول وتوحيد الجهود في مواجهة هذا التهديد المتنامي.

### المطلب الأول: التعاون الشرطي

يعد التعاون الأمني الدولي، و التعاون القضائي الدولي، و التعاون الدولي بشان تسليم المجرمين لمكافحة الجرائم المعلوماتية، من أهم صور و مظاهر التعاون الدولي في مجال مكافحة الجرائم المعلوماتية. وعليه سنحاول من خلال هذا المطلب أن نتطرق إلى مظاهر التعاون الدولي.[1]

- لا يمكن مكافحة الجرائم المعلوماتية إلا بوجود تعاون دولي بين أجهزة الشرطة في دول العالم المختلفة وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالحاسب الآلي والإنترنت وتعميمها.

فنتيجة للتطور الكبير في الاتصالات وتقنية المعلومات وظهور شبكة الإنترنت والانتشار الواسع والسريع لها وانتقال المجرمين من بلد لآخر، فقد أدركت دول العالم بأنه يستحيل على دولة ما بمفردها القضاء على الجرائم عابرة الحدود، وبالتالي تظهر الحاجة لوجود تعاون دولي على المستوى الإجرائي الجنائي بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة، ذلك أن الإجراءات العامة للشرطة في كل دولة لا تسمح لأجهزة الشرطة العاملة فيها بتعقب المجرمين ومتابعتهم متى ما تجاوزوا حدود الدولة، فمثلاً في جرائم الاختراق والإتلاف المعلوماتي قد يكون مرتكب الجريمة يحمل جنسية دولة ما ويرتكب جريمته من حاسبات آلية موجودة في دولة أخرى، وتقع الآثار المدمرة لهذا الهجوم في دولة ثالثة فمن الطبيعي أن تقف مشاكل الحدود والاختصاص القضائي عقبة أمام اكتشاف هذه

[1] العبيدي أسامة، مرجع سابق، ص 123.

الجرائم ومعاقبة مرتكبيها، ويبدو أن التعاون الدولي قد قطع شوطا كبيرا سواء على مستوى التعاون الثنائي أو الاقليمي وذلك من خلال:[1]

- **تطوير وسائل الاتصال والمعلومات بين أجهزة الشرطة في الدول المختلفة:**

يتم عادة استخدام القنوات الدبلوماسية Diplomatic Channels في إجراء الاتصال بين أجهزة العدالة الجنائية الوطنية بصفة عامة وأجهزة الشرطة بصفة خاصة وبين مثيلاتها في الدول الأخرى، وبما أن الاتصالات الشرطية تحتاج إلى اتصالات خاصة سريعة، لذا فقد حاولت الدول المختلفة والمنظمة الدولية للشرطة الجنائية الإنتربول تطوير نظم اتصال خاصة لتبادل المعلومات فيما بينها.

- **جهود جهاز الشرطة الأوروبية Europol:**

أنشئ جهاز الشرطة الأوروبية Europol في عام 1992م بناء على معاهدة ماسترخت Maastricht Treaty وبدأ الجهاز عمله في عام 1999م ويبلغ عدد موظفيه 625 موظفاً ويقع مقره في لاهاي بهولندا وينسق هذا الجهاز مع أجهزة الشرطة حول العالم ومع المنظمات الدولية ذات العلاقة كالشرطة الدولية الإنتربول. ويغطي عمل جهاز الشرطة الأوروبية الدول الـ 27 الأعضاء في الاتحاد الأوروبي European Union لمكافحة الجرائم العابرة للحدود ومنها جرائم الحاسب الآلي والإنترنت وأصبح هذا الجهاز وكالة أوروبية كاملة Full Eu Agency في عام 2010م مما أعطى هذا الجهاز صلاحيات واسعة في تجميع المعلومات والأدلة، ويقوم جهاز الشرطة الأوروبية بإقامة العديد من الدورات التدريبية المتعلقة بمكافحة الجريمة والتي يشارك فيها ممثلون عن الدول الأوروبية وغيرها.

كما يوجد توجه داخل الاتحاد الأوروبي لإنشاء وحدة أوروبية لمكافحة الجرائم المعلوماتية تهدف إلى زيادة التعاون الدولي لحماية الدول الأوروبية ومواطنيها من الجرائم المعلوماتية.

[1] العبيدي أسامة، مرجع سابق، ص 123.

ففي اجتماع لوزراء الإتحاد الأوروبي الذي عقد في لوكسمبورغ في 27 ابريل 2011م تم طرح عدد من التصورات والإستراتيجيات لمكافحة جرائم الحاسب الآلي والإنترنت في الدول الأوروبية. وأكدت هذه التصورات على أهمية حماية الأنظمة المعلوماتية في دول الإتحاد الأوروبي European Union واتخاذ الإجراءات العاجلة والرد السريع في حالة حصول إنقطاعات Disruptions لشبكة الإنترنت أو هجوم إلكتروني. وأيد الوزراء الأوروبيون إنشاء وحدة دائمة تعمل كمنسق ونقطة اتصال Liaison ليتمكن عن طريقها مستخدمي شبكة الإنترنت وضحايا الجرائم المعلوماتية والقطاع الخاص عموماً من تقديم شكاواهم في حالة حدوث أية تجاوزات أو جرائم بحقهم. وتكون مهمة هذه الوحدة جمع وتحديث أفضل الطرق والمعايير في أساليب التحقيق الإلكتروني المتبعة في الشرطة والقضاء في الدول الأوروبية وتقييم أساليب التحقيق المتبعة من قبل أجهزة الشرطة والقضاء في دول الإتحاد الأوروبي.

- **التعاون عن طريق القيام بعمليات شرطية مشتركة:**

وتعد هذه الصورة من التعاون الأمني من أهم الصور في مجال مكافحة الجرائم المعلوماتية خاصة وأن أجهزة العدالة الجنائية ليست بنفس المستوى والإعداد في جميع الدول وإنما يوجد تفاوت فيما بينها فبعض الدول متقدمة تقنياً وبشرياً ولها باع كبير في مواجهة الجرائم المستحدثة ومنها الجرائم المعلوماتية والبعض الآخر تفتقد ذلك، كما أن تتبع مرتكبي الجرائم المعلوماتية والتنقيب عن الأدلة الرقمية وضبطها والقيام بالتفتيش العابر للحدود لمكونات الحاسب الآلي والأنظمة المعلوماتية وشبكات الاتصال بحثاً عما قد تحويه من أدلة على ارتكاب جريمة معلوماتية، كلها أمور تتطلب القيام ببعض العمليات الشرطية والأمنية والتقنية المشتركة، وهو من شأنه أن يؤدي إلى زيادة الخبرات والمهارات للقائمين على مكافحة تلك الجرائم.[1]

- **مركز الشكاوى الخاصة بجرائم الإنترنت في العالم:**

يعد مركز الشكاوى الخاصة بجرائم الإنترنت في العالم من أهم الأجهزة المخصصة لمكافحة جرائم الحاسب الآلي والإنترنت فالنظام المعروف باسم IC3 هو كناية عن نظام تبليغ وإحالة

[1] شحاتة علا الدين، "**التعاون الدولي لمكافحة الجريمة**"، ايتراك للنشر والتوزيع، القاهدرة، مصر، ص 635.

الشكاوى الأفراد في الولايات المتحدة الأمريكية والدول الأخرى في مكافحة جرائم الإنترنت ويخدم هذا المركز وعبر تقديم شكوى ترسل عن طريق الإنترنت الأفراد والمؤسسات والأجهزة المختصة بمكافحة جرائم الإنترنت سواء الموجودة في الولايات المتحدة أو في الدول الأخرى ويعمل في هذا المركز فريق من الموظفين والمحللين من المتخصصين في مجال الحاسب الآلي وشبكة الإنترنت. ويقوم هؤلاء بتلقي الشكاوى المتعلقة بجرائم الإنترنت من الأشخاص المجنى عليهم، ثم يقومون بالبحث في الشكاوى وإعداد ملفها وإحالتها إلى وكالات تطبيق القوانين الفيدرالية والمحلية الأمريكية وإلى أجهزة تطبيق القوانين الدولية كالإنتربول وغيرها من الوكالات التنظيمية وفرق العمل Task Forces التي تشارك فيها عدة وكالات للقيام بالتحقيق فيها. ويستطيع الأشخاص من كافة دول العالم تقديم شكاوى بواسطة موقع مركز الشكاوى الخاصة بجرائم الإنترنت، ويطلب الموقع اسم الشخص المجني عليه أو المبلغ وعنوانه البريدي ورقم هاتفه، إضافة إلى اسم وعنوان ورقم هاتف والعنوان الإلكتروني، إذا كان متوافراً للشخص أو الجهة المشتبه بقيامهما بنشاط إجرامي، إضافة إلى تفاصيل تتعلق بكيفية حدوث الجريمة حسب ما يورده مقدم الشكوى ووقت حدوثها اعتقاده بحدوثها، إضافة إلى أية معلومات أخرى تدعم الشكوى.

- **التعاون القضائي بين الدول**

يهدف التعاون القضائي بين الدول الى التنسيق بين السلطات القضائية، فيما يتعلق بالإجراءات الجنائية من حيث إجراءات التحقيق والمحاكمة إلى حين صدور الحكم على المحكوم عليه، وضمان عدم إفلاته من العقاب .[1]

وقد تعرضت اتفاقية الأمم المتحدة لمكافحة الجريمة إلى ضرورة تفعيل المساعدة القضائية المتبادلة بين الدول في مرحلة التحقيق أو المحاكمة والمتعلقة بالجرائم المنصوص عليها في هذه الاتفاقية، حيث نصت المادة 18 منه على أن تقدم الدول الأطراف لبعضها البعض أكبر قدر ممكن من المساعدة القانونية المتبادلة في التحقيقات والملاحقات والإجراءات القضائية فيما يتصل بالجرائم المشمولة بهذه الاتفاقية.

[1] سالم محمد سليمان الأوجلي، "**أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات**"، رسالة دكتوراه، كلية الحقوق عين شمس، مصر، ص 425.

وترتبط المساعدة القضائية، بما تقدمه دولة ما من اجراءات من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم، وتعتبر الاتفاقيات الدولية منبع الالتزامات بين الدول، على أن يظل ما ليس ملزما ممكنا، وفقا لما ينص عليه القانون الداخلي في كل من الدولتين، وقد أدرجه المشرع الجزائري ونص عليه في القانون رقم 09.04، في المادة 16 معتبراً أنه في إطار التحريات والتحقيقات القضائية الجارية لمعاينة الجرائم المعلوماتية يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة، في الشكل الكتروني، أما عن المساعدة القضائية الدولية فتتمثل فيما يلي:

- **تبادل المعلومات:** ويشمل تقديم المعلومات والوثائق التي تطلبها سلطة قضائية أو أمنية أجنبية، متى كانت بصدد جريمة ما عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم، وقد يشمل التبادل أيضا السوابق القضائية للجناة تتعرف من خلاله الجهات القضائية على الماضي الجنائي للفرد المحال إليها، لتقرير الأحكام الخاصة بالعود ووقف تنفيذ العقوبة وغيرها من الإجراءات.

وفي إطار الجرائم الإلكترونية أقرت الاتفاقية الأوربية حول الجريمة الافتراضية، تبادل المعلومات في المادة 23 منها، بنصها صراحة على وجوب توافر التعاون الدولي بين الدول الأطراف وتعميقه، وتقليل العوائق، بما يوفر أكبر قدر من السهولة والسرعة لتبادل المعلومات والأدلة بين الأطراف.[1]

كما نصت المادة الأولى من اتفاقية الرياض العربية للتعاون القضائي على هذا التبادل بنصها: تتبادل وزارات العدل لدى الأطراف المتعاقدة بصفة منتظمة نصوص التشريعات النافذة والمطبوعات والنشرات والبحوث القانونية والقضائية والمجلات التي تنشر فيها الأحكام القضائية، كما تتبادل لمعلومات المتعلقة بالتنظيم القضائي.

- **نقل الإجراءات:** أقرت هذه الصورة من صور المساعدة القضائية العديد من الاتفاقيات الدولية كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة غير الوطنية 2000، وفي المادة 21

[1] عبد الرحمان فتحي سمحان، "**الجوانب الاجرائية المتعلقة بالانترنت**"، دار النهضة العربية، مصر، 2012، ص 5.

منها، ومعاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي 1999و في المادة 9 منها، وكذا المادة 16من النموذج الاسترشادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي 2003م.

وتتجسد هذه الصورة في قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية بصدد جريمة ارتكبت في إقليم دولة أخرى، ولمصلحة هذه الأخيرة، وذلك بتوافر شروط معينة كالتجريم المزدوج، وأن تؤدي الاجراءات المطلوب اتخاذها دورا مهما في الوصول إلى الحقيقة.

- **الانابة القضائية الدولية:** تعبر الإنابة القضائية عن قيام دولة ما بمباشرة إجراء قضائي يتعلق بدعوى قيد النظر داخل الحدود الإقليمية لدولة أخرى نيابة عنها، وبناء على طلب تلك الدولة المناب عنها ووفقا لما تقرره بنود الاتفاقية الدولية بين الدولتين في هذا الشأن وتهدف الإنابة القضائية إلى تذليل العقبات التي تعترض سير الإجراءات الجنائية في ظل ما تشهده الظواهر الإجرامية من تطور.[1]

ومن شأن الإنابة القضائية تسهيل الاجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة، والتغلب على العقبة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى، كإجراء التفتيش والضبط والمعاينة. وتماشيا مع سرعة الجريمة الإلكترونية، وتجنبا لطول إجراءات طلب الإنابة القضائية الدولية، فقد أبرمت العديد من الاتفاقيات الجديدة التي ساهمت في اختصار الاجراءات عن طريق الاتصال المباشر بين السلطات المعنية بالتحقيق، كالاتفاقية الأميريكية الكندية، التي تنص على تبادل المعلومات شفهيا في حالة الاستعجال.[2]

- **التعاون الدولي في تسليم المجرمين** : يعرف تسليم المجرمين بأنه الإجراء الذي تسلم بموجبه دولة استنادا إلى معاهدة أو تأسيسا على المعاملة بالمثل عادة إلى دولة أخرى

[1] عبد الرحمان فتحي سمحان، مرجع سابق، ص 6.

[2] سليمان أبو نمر، يوسف بوكشريدة، "**مكافحة الجريمة المعلوماتية في اطار القانون الدولي**"، مذكرة ماستر، كلية الحقوق والعلوم السياسية محمد خضير بسكيكدة، الجزائر، 2021، ص 36.

شخصا تطلبه الدولة الأخيرة لاتهامه أو لأنه محكوم عليه لعقوبة جنائية وتشترط معظم الدول للتعليم التجريم المزدوج للسلوك الذي يطالب بالتسليم لأجله وأن يكون معاقبا عليه بموجب قوانين الدولة طالبة التسليم والدولة المطلوب إليها.

وتتلخص هذه الصورة من صور التعاون الدولي لمواجهة الجريمة عامة والمعلوماتية خاصة في قيام الدولة التي يتواجد على إقليمها المتهم بارتكاب إحدى الجرائم العابرة للحدود، كجرائم الأنترنت، بمحاكمة هذا المتهم إذا كان تشريعها يسمح بذلك، وإلا تسليمه لدولة اخرى مختصة من أجل محاكمته، والغرض من وراء ذلك، هو الحيلولة دون إفلات المتهم من العقاب متى كان القانون الداخلي للدولة المتواجد على إقليمها لا يسمح لها بمحاكمته. وقد كانت مسألة تسليم المجرمين في مجال مكافحة الجرائم الإلكترونية موضوع العديد من الاتفاقيات والمعاهدات الدولية، أهمها معاهدة بودابست لمكافحة جرائم الأنترنت، من خلال المواد 12 و 23 و 24 و 25 منها، وتوصيات المجلس المجلس الأوربي بشأن

مشاكل الإجراءات الجنائية المتعلقة بتكنولوجية المعلومات من خلال التوصية رقم 13/95 بتاريخ 11 سبتمبر 1995.[1]

**المطلب الثاني: جهود منظمة الانتربول في مكافحة الجرائم المعلوماتية**

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

[1] العبيدي أسامة بن غانم، مرجع سابق، ص 22.

## الفرع الأول: مفهوم الانتربول

### 1. تعريف الانتربول:

الإنتربول هو أكبر منظمة شرطية دولية، أنشأت عام 1929م، ومقرها الرئيسي في مدينة ليون بفرنسا، وكما هو معروف من دستور الإنتربول الدولي فهي تتكون من الجمعية العامة اللجنة التنفيذية، الأمانة العامة، المكاتب المركزية الوطنية، المستشارون لجنة ضبط ملفات الإنتربول، وكانت تسمى هذه المنظمة باللجنة الدولية للشرطة الجنائية وتضم في عضويتها 182 دولة. [1]

وطريقة العمل داخل المنظمة تتم بتبادل أعضاء الانتربول المعلومات عن المجرمين الدوليين، ويتعاونون فيما بينهم في مكافحة الجرائم الدولية، مثل جرائم التهريب، وعمليات البيع والشراء غير المشروع للأسلحة، والجرائم الإلكترونية، وقد ركز الإنتربول في السنوات الأخيرة بصورة أساسية على الجريمة المنظمة والأنشطة الإجرامية ذات الصلة بها، مثل غسل الأموال. ويحتفظ أفراد المنظمة بسجلات الجرائم الدولية وقد أنشأت المنظمة وحدة تحليل المعلومات الجنائية والتي تقضي باستخلاص المعلومات الهامة عن المنظمات الإجرامية وتبويبها، بهدف وضع تلك المعلومات في متناول هيئة الشرطة، أو الدول الأعضاء في الإنتربول.

### 2. أهداف الانتربول:

تستهدف هذه المنظمة تأكيد وتشجيع التعاون بين سلطات البوليس في الدول الأطراف وطبقا للمادة الثانية من ميثاق المنظمة تتمثل أهم أهداف هذه المنظمة في تحقيق الآتي:

- جمع المعلومات المتعلقة بالجرائم والمجرمين، وذلك عن طريق المعلومات التي تتسلمها المنظمة المكتب الرئيسي في اليون من المكاتب المركزية الوطنية للشرطة الجنائية في الدول الأعضاء، ويتم ذلك عبر شبكة اتصالات حديثة.

[1] العبيدي أسامة بن غانم، مرجع سابق، ص 22.

- التعاون مع الدول الأعضاء في ضبط الهاربين والمطلوبين – أيا كانت جنسياتهم والصادر ضدهم أحكام قضائية، أو أوامر بالضبط والإحضار لمثولهم أمام جهات التحقيق، وذلك من خلال إصدار النشرات الدولية المخصصة.
- دعم جهود الشرطة في مكافحة الإجرام العابر للحدود، وتقديم الخدمات في مجال الأدلة الجنائية كبصمات الأصابع، والحمض النووي.
- إنشاء وتنمية كافة المؤسسات القادرة على المساهمة الفعالة في الوقاية من جرائم القانون العام.
- تأمين وتنمية التعاون المتبادل على أوسع نطاق بين كافة سلطات الشرطة الجنائية في إطار القوانين القائمة في مختلف البلدان، وبروح الإعلان العالمي لحقوق الإنسان.[1]

**الفرع الثاني: استراتيجية الانتربول في مكافحة الجريمة المعلوماتية**

أنشأت المنظمة الدولية للشرطة الجنائية الإنتربول خلال عام 2004، وحدة خاصة لمكافحة جرائم التكنولوجيا ، كما قامت المنظمة بالتعاون مع مجموعة الدول الثمانية الكبرى 68 بوضع استراتيجيات لمواجهة هذا النوع من الجرائم، وذلك من خلال:

- إنشاء مركز اتصالات أمني عبر الشبكة يعمل على مدار 24 ساعة 7 أيام في الأسبوع على مستوى مصالح الشرطة في الدول الأطراف.
- استخدام وسائل حديثة في تلك المكافحة كاستخدام قاعدة البيانات المركزية للصور الإباحية المحولة من قبل الدول الأطراف والتي تستخدم برنامج Excalibur للتحليل والمقارنة الأوتوماتيكية لتلك الصور.
- تزويد شرطة الدول الأطراف بكتيبات ارشادية حول الجرائم المعلوماتية وكيفية التدريب على مكافحتها والتحقيق فيها.

وهكذا يتولى الإنتربول إقامة العلاقات بين الدول والمنظمة وتبادل المعلومات بين سلطات التحقيق فيما يتعلق بالجرائم المتشعبة في عدة دول كتلك المتعلقة بالجرائم المعلوماتية. وبهذا فإن شرطة الإنتربول تعد منظومة عالمية تختص بمكافحة الجرائم الدولية والعابرة للحدود

[1] العبيدي أسامة بن غانم، مرجع سابق، ص 23.

الوطنية للدول، بما فيها الجرائم المعلوماتية، وذلك ما أكدته نتائج الدورة رقم 77 للجمعية العامة المنظمة الإنتربول، حيث دعا الأمين العام للإنتربول السيد بونالد نوبل جميع الحكومات والدول لدعم وتطوير نظم تبادل المعلومات حول المشتبه بهم ومحاربة الإرهاب المتنامي في كل أنحاء العالم بكل صوره بما فيه الإرهاب المعلوماتي، وقد نجحت المنظمة الدولية للشرطة الجنائية. الإنتربول خلال الأعوام الأخيرة في جعل اسمها من أكثر الأسماء التي يخشاها المجرمون. وعلى المستوى العربي نجد أن مجلس وزراء الداخلية العرب أنشأ المكتب العربي للشرطة الجنائية بهدف تأمين وتنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة وملاحقة المجرمين في حدود القوانين والأنظمة المعمول بها في كل دولة بالإضافة إلى تقديم المعونة في مجال دعم وتطوير أجهزة الشرطة في الدول الأعضاء.[1]

## المطلب الثالث: التعاون الدولي في مجال التدريب لمكافحة الجرائم المعلوماتية

في ظل الطبيعة المتغيرة والديناميكية للجرائم المعلوماتية، أصبح من الضروري أن تواكب الجهات المكلفة بإنفاذ القانون التطورات التقنية المستمرة. ومن هنا برزت الحاجة إلى التعاون الدولي في مجال التدريب وبناء القدرات، باعتباره ركيزة أساسية في تعزيز جاهزية الدول لمواجهة هذه التهديدات العابرة للحدود.

### الفرع الأول: أهمية تأهيل القائمين على أجهزة مكافحة الجرائم المعلوماتية

بات التدريب في مجال مكافحة الجرائم المعلوماتية وسيلة للاستثمار الذي تلجأ إليه عادة المنظمات الإدارية لتحقيق أهدافها باعتباره عنصرا حيويا لابد منه لبناء الخبرات والمهارات المتجددة، والواقع أن التدريب أصبح يلعب دورا مهما في حياة الإنسانية المعاصرة، فقد زاد الاهتمام بالتدريب بمختلف جوانبه التقنية وأضحى من ضروريات الحياة لدى أغلب أفراد المجتمعات ، سواء أكان متدربا أم بالنسبة للمنظمة التي تقوم بعملية التدريب أيضا، وسواء أكانت منظمة مدنية أم عسكرية أم حكومية أم خاصة أم كانت تعمل في قطاع العدالة أم في غيره فهو أحد العناصر الأساسية لزيادة كفاءة الكادر البشري ويرفع إنتاجيته ويحقق التنمية

[1] العبيدي أسامة بن غانم، مرجع سابق، ص 23.

بمفهومها الشامل، والدافع من عملية التدريب هو إدخال وإحداث تعديلات جوهرية على سلوك المتدربين تبدو آثارها واضحة في سلوكهم لأداء الأعمال التي يكلفون بها كلا ومجاله بشكل أفضل بعد عملية التدريب ، كما أن التدريب يعد الوسيلة الفعلية والتطبيقية الناجحة والمؤثرة التي تكفل الاستفادة من مهارات وتجارب الآخرين من خلال أشخاص مؤهلين على ذلك، والمقصود بالتدريب هنا التدريب التقني وغير التقليدي الذي يكسب الأفراد خبرة فنية عالية في مجال الجريمة المعلوماتية. هذه الخبرة التقنية لا تتأتى دون تدريب تخصصي يراعى فيه القدرات الشخصية للمتدرب من حيث توافر الصلاحية العلمية والقدرات الذهنية لتلقي التدريب ، وهنا يكون من السهل تدريب متخصص في تكنولوجيا المعلومات وشبكات الاتصال بدلا من تدريب القائمين على تنفيذ القانون كرجال الشرطة أو ممثلي الادعاء ويذهب بعض الخبراء إلى أنه يجب أن تتوافر لدى المتدرب خبرة لا تقل عن خمس سنوات في المجالات التي لها علاقة بتكنولوجيا المعلومات كالبرمجة وتصميم النظم وتحليلها وإدارة الشبكات وعمليات الحاسب الآلي، ويجب أن يشمل المنهج التدريبي على بيان بالمخاطر والتهديدات ونقاط الضعف وأماكن الاختراقات لشبكة معلومات وأجهزة الحاسب الآلي وأيضا ذكر مفاهيم وتعريفات للصفات التي يتميز بها المجرم المعلوماتي والدوافع وراء ارتكاب الجرائم المعلوماتية ولابد أن يراعي في البرنامج التدريبي نوعه وصفته وما إذا كان رسميا من خلال حلقات دراسية أو حلقات نقاش ورش عمل حول هذه الجرائم المستحدثة، ويجب أن يكون هناك تفاعل مثمر بين المشاركين لتحليل الحالات الدراسية وتبادل الخبرة العلمية في كيفية التعامل مع الحاسب الآلي وكيفية استخدامها.[1]

وقد يكون التدريب فردية أو يتم ضم مجموعة من المتدربين للعمل معا كفريق ويتعين على الفرق أن تخوض تجارب عملية بحيث تعرض عليه عينة من الجرائم المعلوماتية التي تم التحقيق فيها على أن يراعي في هذه العينة التنويع لكي تؤدي دورها في إكساب المشاركين في البرنامج التدريبي الخبرة المطلوبة. وهذا يتطلب أن يقوم بالتدريب جهة مختصة ولها الخبرة الكافية في اختيار المتدربين ذوو الخبرة العلمية والفنية والصفات الشخصية المميزة.

[1] سليمان أبو نمر، يوسف بوكشريدة، مرجع سابق، ص 38.

ولابد لعملية التدريب أن تكون مستمرة؛ لأن الجرائم المعلوماتية في تطور مستمر وسريع ولابد أيضا أن تسعى الأجهزة الأمنية التي تكون مسؤولة عن التحقيق أن تستعين بالمختصين والخبراء في مجال الحاسوب ويمكن ذلك عن طريق استعانة كلية الشرطة مثلا وقبولها بتعيين دفعات من الجامعيين من خريجي كليات تكنولوجيا المعلومات تخرجهم ضباط مؤهلين قانونيا وتقنيا وعلى الكليات التي تدرس القانون أن تعنى بتدريس الحاسوب وعلومه وذلك يؤدي إلى أن تكون لدي خريجي هذه الكليات ثقافة قانونية وثقافة بالحاسوب[1].

**الفرع الثاني: مظاهر التعاون الدولي في مجال تدريب رجال العدالة الجزائية**

أجهزة العدالة في الكثير من الدول ليست لديها الجاهزية لمواجهة جرائم الحاسب ومثيلاتها من الجرائم الحديثة ذات التطور المستمر، ومن هنا ولأننا نعلم أنه ما من دولة يمكنها النجاح في مواجهة هذه الأنماط المستحدثة بمفردها دون تعاون وتنسيق مع غيرها من الدول كانت الدعوة إلى ضرورة وجود تعاون دولي في هذه الناحية، أي في مجال المساعدات القضائية المتبادلة وفي مجال تسليم المجرمين وفي مجال تدريب رجال العدالة وهناك بعض الاتفاقيات الدولية والإقليمية التي دعت صراحة إلى ضرورة وجود تعاون بين الدول في مجال التدريب ونقل الخبرات فيما بينهما كما هو الحال في المادة 9 من مشروع الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود وقد يكون التعاون الدولي في مجال تدريب رجال العدالة على مواجهة الجرائم المتعلقة بشبكة الإنترنت بين الدول وأجهزة العدالة الجزائية لديها، ففي جمهورية مصر العربية نجد أن النيابة العامة تعقد الندوات والمؤتمرات وحلقات النقاش وتشارك فيها سواء عقدت أو خارجها، بالإضافة إلى أنه يتم إرسال أعضاء النيابة من مختلف الدرجات في برامج خارجية، وذلك بالتعاون مع أجهزة النيابة العامة الأخرى والهيئات الدولية بهدف الاطلاع على أحدث النظم في هذا في الدول المجال. وقد يتحقق من عقد تلك اللقاءات والندوات تبادل الآراء والخبرات بين المشاركين وتبادل الرأي وطرح الأفكار والتصورات وتشجيع التعاون بين الدول والأطراف أو المعاهدات من أجل مقاومة تلك الجرائم.

[1] سليمان أبو نمير، يوسف كشريدة، مرجع سابق، ص 38.

ومن فوائد تلك البرامج والندوات التدريبية التي تعود عليه أو المنظمات المشاركة أنها تمكنها من طرح ما تريد من موضوعات حيوية، كما أنها تعلن عن دورها الرائد لتزيد من ثقة الأطراف الأخرى في أدائها بما يشجع على إجراء المزيد من التعاون معها، ويمكن أيضا لهذه البرامج التدريبية أن تفيد متلقي التدريب عن طريق زيادة مهاراته وخبراته ومعلوماته وقدراته على التعامل مع الأجهزة الدولية الأخرى، الأمر الذي ينعكس على الجهة التي ينتمي إليها بالفائدة.

ومن أهم التجارب تجربة الولايات المتحدة الأمريكية في مجال مكافحة الجرائم المعلوماتية فالولايات المتحدة الأمريكية تحرص على توفير المساعدة التقنية والتدريب لرفع قدرات العدالة الجزائية لدى الحكومات الأخرى مساعدة من لديها أجهزة شرطة وادعاء عام وقضاة أيضا ليصبحوا أكثر فعالية في مكافحة الجريمة، فمثل هذه المساعدة لا تؤدي إلى تيسير بناء إطار للتعاون الدولي في مجال تطبيق القانون وحسب، ولكنها تعزز أيضا قدرة الحكومات الأجنبية المعنية على ضبط مشاكل الجريمة المعلوماتية لديها قبل أن يمتد ليتجاوز حدود بلدانها، وهناك مكتب للمساعدة والتدريب على تطوير أجهزة الادعاء العام في الخارج التابع لوزارة العدل الأمريكية، وهذا الجهاز مكلف بتوفير المساعدة اللازمة لتعزيز مؤسسات العدالة الجزائية في دول أخرى وتعزيز إدارة القضاء في الخارج، كما أن البرنامج الدولي للمساعدة والتدريب على التحقيق الجزائي الذي كثيرا ما يعمل على توفير مساعدات الأجهزة الشرطة في البلدان العالم الثالث في مختلف أنحاء العالم. وفي الوقت الحاضر تقدم وزارة العدل الأمريكية مساعدات للقضاء الدول في أفريقيا ودول أخرى في آسيا وأوروبا الشرقية والوسطى وغيرها. ونجد أيضا أن أجهزة تطبيق القانون الأمريكية توفر أيضا تدريبا لنظيراتها من الأجهزة في البلدان الأخرى داخل الولايات المتحدة الأمريكية أو خارجها عن طريق إنشاء معاهدة خاصة بالتدريب مثل كلا من المجر وتايلاند، وفي هذه المعاهدة يقوم خبراء أمريكيون في عمل أجهزة تطبيق القانون باطلاع المتدربين على أساليب وسبل مبتكرة للتحقيق، ويشجعون على تبادل الآراء مع نظرائهم في مختلف أنحاء العالم.[1]

[1] سليمان أبو نمر، يوسف بوكشريدة، مرجع سابق، ص 40.

إن التعاون الدولي في مجال التدريب لا يُعد رفاهية، بل ضرورة حتمية لضمان فعالية المواجهة المشتركة للجرائم الإلكترونية .فكلما زادت قدرة الدول على مواكبة التطورات التقنية كلما تقلصت فجوة الحماية بينها وبين المجرمين الرقميين الذين لا يعترفون بالحدود. التعاون في التدريب هو المفتاح لتكوين شبكة عالمية قوية قادرة على التصدي لهذا التهديد المتنامي[1].

[1] سليمان أبو نمر، يوسف بوكشريدة، مرجع سابق، ص 40.

## المبحث الثالث: تجارب الدول في مكافحة الجرائم المعلوماتية

يتباين تعامل الدول مع الجرائم المعلوماتية بحسب طبيعة نظمها القانونية والتقنية ومستوى تطورها الرقمي، ويسعى هذا المبحث إلى تسليط الضوء على نماذج من استراتيجيات الدول الغربية والعربية في مواجهة هذه الجرائم، بهدف الوقوف على نقاط القوة والقصور واستنتاج الدروس المستفادة التي يمكن أن تواجه الدول الأخرى ومنها الجزائر. نحو تطوير استجابة فعالة وشاملة.

### المطلب الأول: استراتيجية مكافحة الجرائم المعلوماتية في الدول الغربية

شهدت الدول الغربية منذ تسعينيات القرن الماضي تزايدًا ملحوظًا في التهديدات الإلكترونية، مما دفعها إلى تطوير استراتيجيات متكاملة لمكافحة الجرائم المعلوماتية، تجمع بين الأطر التشريعية، والهياكل المؤسسية المتخصصة، والتعاون الدولي والتقني. وتُعد هذه الدول من أوائل من تبنى قوانين خاصة بالجريمة السيبرانية، وأنشأ أجهزة متخصصة في التحقيق الرقمي والتدخل السريع.

ويهدف هذا المطلب إلى عرض وتحليل النماذج المعتمدة في بعض الدول الغربية الرائدة مثل فرنسا والولايات المتحدة الأمريكية، من حيث المنظومة القانونية، ودور الأجهزة الأمنية وكذلك الممارسات الفعالة على المستوى الوقائي والتنسيقي، بما يتيح إمكانية الاستفادة منها في تطوير السياسات الجزائرية في هذا المجال.

#### الفرع الأول: الإطار القانوني لمكافحة الجرائم المعلوماتية في فرنسا

تعد فرنسا من الدول الرائدة في مجال مكافحة الجريمة المعلوماتية، حيث أولت اهتماماً مبكراً بهذا النوع من الجرائم، نتيجة إدراكها لتزايد الاعتماد على الوسائط الرقمية في مختلف مجالات الحياة .وقد أسست ترسانة قانونية ومؤسساتية متكاملة تهدف إلى الوقاية، والكشف والمتابعة القضائية للجرائم السيبرانية[1].

[1] Weill Pierre-Alain. "**État de la législation et tendances de la jurisprudence relatives à la protection des données personnelles en droit pénal français**" Revue internationale de droit comparé. Vol. 39 N°3. Juillet-septembre. p. 655-675.

### 1. قانون غودفرين Loi Godfrain لعام 1988:

يعتبر هذا القانون أول حجر أساس في التشريع الفرنسي لمكافحة الجرائم المعلوماتية. تم بموجبه إدراج مواد جديدة في القانون الجنائي الفرنسي المواد 323-1 الى 323-7، تجرّم ما يلي:

- الدخول غير المصرح به إلى نظام معالجة آلية للبيانات.
- إعاقة أو تعطيل تشغيل النظام.
- تعديل أو حذف البيانات المخزنة فيه.
- الإضرار بمعطيات الغير أو اختراق الخصوصية.
- ويُلاحظ أن هذا القانون وضع أُسساً واضحة لفهم" الاعتداء الرقمي "حتى في مرحلة كان فيها استخدام الإنترنت محدودًا، مما يُظهر حنكة تشريعية استباقية.

### 2. قانون الثقة في الاقتصاد الرقمي LCEN لسنة 2004:

جاء هذا القانون في سياق التوسع في التجارة الإلكترونية والخدمات الرقمية، ليضبط النشاطات عبر الإنترنت .يتضمن القانون أحكامًا تنظم:

- مسؤولية مقدمي خدمات الإنترنت.
- إزالة المحتوى غير القانوني.
- التصدي للاحتيال الإلكتروني.phishing
- تنظيم البريد غير المرغوب فيه.spam

كما أعطى صلاحيات موسّعة للسلطات القضائية والأمنية في تتبع الأدلة الرقمية وإصدار أوامر الحجب[1].

### 3. قانون البرمجة العسكرية LPM للفترة 2014-2019 و 2024-2030:

في خطوة غير مسبوقة، ربط المشرّع الفرنسي الأمن السيبراني بالدفاع الوطني. هذا القانون:

- ألزم المؤسسات التي تدير بُنى تحتية ذات طابع حيوي OIV بتطبيق بروتوكولات أمنية صارمة.
- فرض إجراءات الإبلاغ الإجباري عن الحوادث الإلكترونية.

[1] **"La loi pour une République numérique est promulguée"**. economie.gouv.fr France. Le portail de l'Économie et des Financies. Retrievé 2016-12-01.

- منح الوكالة الوطنية لأمن نظم المعلومات ANSSI صلاحيات تفتيش وتدقيق إلكتروني.

ويُعدّ هذا التكامل بين الأمن الداخلي والدفاع الرقمي ميزة متقدمة للاستراتيجية الفرنسية[1].

**4. الإجراءات القضائية المرتبطة بالأدلة الرقمية:**

أصدر المشرّع الفرنسي عدة نصوص تتيح:

- تفتيش الأجهزة الرقمية بإذن قضائي.
- اعتراض الاتصالات الرقمية في إطار التحقيقات.
- تخزين البيانات المتعلقة بحركة المستخدمين.data retention

كل هذه التدابير تعكس محاولة التوفيق بين حماية الحريات الأساسية وضمان الفعالية في مكافحة الجريمة السيبرانية[2].

**5. الاطار المؤسساتي:**

أنشأت فرنسا عدداً من الهيئات المتخصصة أبرزها:

- الوكالة الوطنية لأمن نظم المعلومات ANSSI، وهي الجهة المركزية المسؤولة عن تعزيز الأمن السيبراني على المستوى الوطني[3].
- وحدة مكافحة الجريمة المعلوماتية في الشرطة الوطنية، والتي تعمل على التحقيق في قضايا القرصنة الابتزاز الإلكتروني، والاعتداء على الأنظمة المعلوماتية.
- النيابة العامة المختصة في قضايا الجرائم الرقمية، التي تمكّن من تسريع معالجة هذه القضايا وتوفير الخبرة اللازمة في التحقيق[4].

---

[1] JEAN francois auran, 10 May 2025, "**Examining the french military programming 2024-2030**", ESD, euro-sd.com/2024/01/articles/36190/examining-the-french-military-programming-act-2024-2030/

[2] Watin-Augouard, M. (2011). "**Cybercriminalité : Défi mondial**". Paris: L'Harmattan, 2012, P 95.

[3] "**Groupement interministériel de contrôle**". www.sgdsn.gouv.fr. 17 November 2022. Retrievé 2024-12-28.

[4] Jacques Massey."**Enquête : le casse-tête des écoutes judiciaires**". La Lettre de l'Expansion. 4 September 2017, P122-125.

يظهر الإطار القانوني الفرنسي تطورا تدريجيا يتماشى مع التحولات الرقمية، حيث انتقل من التجريم العام إلى مقاربات أكثر تخصصًا وتكاملًا .ويُعد هذا التطور أساسًا قانونيًا يُمكّن باقي أجهزة الدولة من تطبيق استراتيجية وطنية فعالة لمكافحة الجرائم المعلوماتية.

**الفرع الثاني: الاطار القانوني التشريعي للاستراتيجية الامريكية**

تعد الولايات المتحدة من أوائل الدول التي أولت أهمية كبرى للأمن السيبراني، نظراً لتطور بنيتها الرقمية واعتمادها الواسع على تكنولوجيا المعلومات في القطاعات الحكومية، العسكرية والاقتصادية.

**1. الإطار القانوني التشريعي:**

اعتمدت الولايات المتحدة مجموعة من القوانين التي تُشكل أساسًا لمكافحة الجرائم المعلوماتية، من أهمها:

- قانون الاحتيال وإساءة استخدام الحاسوب CFAA لسنة 1986ويُعتبر من أبرز النصوص القانونية التي تُجرم الاختراق غير المصرح به للأنظمة المعلوماتية.
- USA PATRIOT Act 2001: وسع صلاحيات التحقيق الإلكتروني، خاصة في الجرائم المتعلقة بالإرهاب السيبراني.
- Cybersecurity Information Sharing Act CISA 2015: يشجع المؤسسات الخاصة على تبادل المعلومات المتعلقة بالتهديدات الإلكترونية مع الحكومة[1].

**2. المؤسسات الفاعلة:**

- وزارة الأمن الداخليDHS، عبر ذراعها المختصة بالأمن السيبراني – CISA Cybersecurity and Infrastructure Security Agency، تشرف على التنسيق بين مختلف القطاعات لحماية البنية التحتية الرقمية.
- مكتب التحقيقات الفيدرالي FBI، وتحديدًا عبر وحدة الجرائم الإلكترونية، التي تقوم بتحقيقات متخصصة في الهجمات السيبرانية.
- القيادة السيبرانية الأمريكية USCYBERCOM، المسؤولة عن الردع والدفاع والهجوم الإلكتروني عند الضرورة.

[1] Clifford, R.D, 2015, "**Cybercrime : the investigation, Prosecution and defense of a computer-related crime**", P 233.

**3. الجهود الدولية:**

- تعد الولايات المتحدة فاعلًا محوريًا في التعاون الدولي عبر اتفاقيات ثنائية ومتعددة الأطراف، منها التعاون في إطار التحالف الاستخباراتي Five Eyes، وتعاونها مع الإنتربول واليوروبول.
- دعمت بقوة اتفاقية بودابست حول الجريمة السيبرانية2001، وكانت من أولى الدول الموقعة عليها.

**4. التوعيات والمبادرات:**

- أطلقت حملات وطنية مثل "Stop. Think. Connect."لتعزيز الوعي العام بالممارسات الآمنة على الإنترنت.
- تشجع مؤسسات التعليم العالي على إنشاء برامج جامعية متخصصة في الأمن السيبراني بدعم من NSA و DHS.

يتضح من خلال تحليل الاستراتيجية الأمريكية في مكافحة الجرائم المعلوماتية أن الولايات المتحدة قد تبنت نموذجاً شاملاً ومتكاملاً، يجمع بين الإطار التشريعي الصارم والتنسيق المؤسسي الفعال، فضلاً عن التعاون الدولي المكثف .فقد عملت على تطوير قوانين مرنة ومحدثة مثل قانون الاحتيال وإساءة استخدام الحاسوبCFAA، وأوجدت مؤسسات متخصصة كمكتب التحقيقات الفيدرالي FBI ووحدة الجرائم الإلكترونية في وزارة الأمن الداخلي .كما ركّزت الاستراتيجية الأمريكية على الجانب الوقائي والتدريبي إلى جانب تبني مقاربة استباقية عبر تعزيز الأمن السيبراني الوطني .ومع ذلك، تبقى التحديات قائمة خاصة في ظل التطور السريع لتقنيات الجريمة الرقمية، ما يستدعي جهداً مستمراً لتحديث الآليات ومضاعفة التنسيق مع الدول والمنظمات[1].

[1] علي عبد القادر القهوجي، "**الجرائم الالكترونية –دراسة مقارنة–**"، دار الجامعة الجديدة، الاسكندرية، 2019، ص 400.

## المطلب الثاني: استراتيجية مكافحة الجرائم المعلوماتية في الدول العربية

شهد العالم العربي خلال السنوات الأخيرة تزايدًا ملحوظًا في الاهتمام بمواجهة الجرائم المعلوماتية وذلك نتيجة للانتشار الواسع لاستخدام الإنترنت والتقنيات الرقمية في مختلف مناحي الحياة، مما أدى إلى بروز تحديات أمنية وقانونية تستوجب تحركًا فعّالًا من قبل الحكومات .وقد سارعت العديد من الدول العربية إلى تطوير أطر قانونية ومؤسساتية لمكافحة هذا النوع من الجرائم، من خلال سن تشريعات خاصة، وإنشاء هيئات متخصصة في الأمن السيبراني، بالإضافة إلى المشاركة في مبادرات إقليمية ودولية لتعزيز التعاون في هذا المجال.

تفاوتت الاستراتيجيات المعتمدة من دولة عربية إلى أخرى، وفقًا لمستوى التطور الرقمي والقدرات التقنية والإرادة السياسية، إلا أنها اتفقت في جملة من النقاط أبرزها :ضرورة إصدار تشريعات واضحة، وتكوين كوادر بشرية متخصصة، وتعزيز التعاون القضائي والأمني مع الدول الأخرى، إلى جانب إطلاق حملات توعية رقمية تستهدف المجتمع.

### الفرع الأول: الاستراتيجية المصرية في مكافحة الجرائم المعلوماتية

اعتمدت جمهورية مصر العربية خلال العقدين الأخيرين خطوات جادة في سبيل مكافحة الجرائم المعلوماتية، مدفوعة بتزايد الاعتماد على الوسائل الرقمية والاتصالات الإلكترونية في المجالات الاقتصادية والاجتماعية والأمنية، إلى جانب تزايد التهديدات الإلكترونية وتنوعها.

وقد تمثلت الركيزة الأساسية للاستراتيجية المصرية في إصدار القانون رقم 175 سنة 2018[1] بشأن مكافحة جرائم تقنية المعلومات، والذي يُعد أول تشريع متكامل في البلاد يتناول هذه الجرائم بشكل تفصيلي .ينظم هذا القانون الجرائم التي تُرتكب عبر الإنترنت، مثل اختراق الشبكات، الاعتداء على البيانات الشخصية، الاحتيال الإلكتروني، الجرائم المتعلقة بالأمن القومي، والتحريض على العنف والكراهية عبر الوسائط الرقمية.

[1] جمهورية مصر العربية، "**القانون رقم 175لسنة 2018بشأن مكافحة جرائم تقنية المعلومات**"، الجريدة الرسمية العدد 33 مكرر ب، 2018/08/14.

وقد نص القانون على مجموعة من العقوبات التي تراوحت بين الغرامات المالية والسجن وشمل أحكامًا تتعلق بالتحقيق وجمع الأدلة الرقمية، وحماية المعطيات الشخصية، وهو ما يعكس تطورًا في فهم طبيعة الجريمة المعلوماتية ومتطلبات مكافحتها.

- من الناحية المؤسسية: أنشأت مصر عدة كيانات تُعنى بمواجهة هذا النوع من الجرائم من أبرزها:

- إدارة مكافحة جرائم الحاسبات وشبكات المعلومات التابعة لوزارة الداخلية، وهي الجهة المختصة بتلقي بلاغات الجرائم المعلوماتية والتحقيق فيها.
- المركز المصري للاستجابة لطوارئ الحاسبات والشبكات EG-CERT التابع للجهاز القومي لتنظيم الاتصالات، والذي يعمل على تأمين البنية التحتية للمعلومات الحيوية ورصد التهديدات السيبرانية والتعامل معها.

كما تضمنت الاستراتيجية المصرية محورًا توعويًا وتدريبيًا، من خلال تنظيم حملات توعية إعلامية حول مخاطر الإنترنت، وإدراج مفاهيم الأمن السيبراني ضمن المناهج التعليمية وتدريب القضاة وأفراد الشرطة على كيفية التعامل مع هذا النوع المستحدث من الجرائم.

أما على المستوى الدولي، فقد عززت مصر تعاونها الإقليمي والدولي في هذا المجال من خلال عضويتها في المنظمة العربية لتكنولوجيا المعلومات والاتصالاتAICTO [1] ومشاركتها في عدة اتفاقيات ومؤتمرات دولية تهدف إلى تطوير إطار تشريعي وأمني متكامل لمواجهة التهديدات السيبرانية[2].

- **أصول المحاكمات الجنائية:**

تدعم المنظمات الموقعة أدناه الدعوات التي أطلقتها عدة دول خلال الاستعراض الدوري الشامل الرابع لمصر الذي عُقد في مجلس حقوق الإنسان التابع للأمم المتحدة في 28 يناير 2025، لحث الحكومة المصرية على ضمان امتثال مشروع قانون الإجراءات الجنائية المقترح مؤخرا لالتزاماتها الدولية في مجال حقوق الإنسان. يُشكّل مشروع القانون الذي يناقشه البرلمان المصري حاليًا، ويهدف إلى استبدال قانون الإجراءات الجنائية

[1] AICTO نسخة محفوظة 14 مارس 2012، https://web.archive.org/.

[2] عبد العزيز الفاضلي، "**الجرائم الإلكترونية في التشريع المقارن**"، دار النشر للجامعات، مصر، الطبعة 1، 2019، ص 151.

المصري لعام 1950، تهديدًا خطيرًا للحق في الخصوصية، حيث يمنح المسؤولين عن إنفاذ القانون سلطات واسعة وتعسفية لمراقبة واعتراض اتصالات الأشخاص وأنشطتهم عبر الإنترنت. ونحث البرلمان المصري على رفض المسودة المقترحة وسن قانون جديد للإجراءات الجنائية يدعم الحقوق المنصوص عليها في الدستور المصري ويتماشى مع المعايير الدولية لحقوق الإنسان.

تهدد عدة أحكام في مشروع القانون الحق في الخصوصية في مصر بشكل خطير، وتضفي الشرعية على المراقبة التعسفية وغير القانونية التي تقوم بها الدولة، لا سيما تجاه المدافعين عن حقوق الإنسان والصحفيين والمعارضين. على سبيل المثال، تمنح المادتان 79 و 80 من مشروع القانون سلطات تقديرية غامضة وواسعة لقضاة التحقيق لإصدار أمر لمدة لا تتجاوز 30 يوما يمكن تجديده إلى أجل غير مسمى بزيادات قدرها 30 يوما يسمح للسلطات بضبط الخطابات والرسائل والبرقيات والصحف والمطبوعات والطرود، ومراقبة الاتصالات السلكية واللاسلكية للأفراد وحساباتهم على وسائل التواصل الاجتماعي، بما في ذلك المحتوى الخاص. وكذلك رسائل البريد الإلكتروني والرسائل المخزنة على الهواتف والأجهزة "متى كان لذلك فائدة في كشف الحقيقة في جناية أو جنحة يعاقب عليها بالسجن لأكثر من ثلاثة أشهر.

وبموجب مشروع القانون المقترح، يمكن للقضاة أيضًا أن يأمروا بمصادرة الهواتف أو الأجهزة المحمولة أو المواقع الإلكترونية أو أي وسيلة تكنولوجية أخرى، و"تسجيل المحادثات الخاصة إذا لزم الأمر لصالح التحقيقات"، أو وضع الأجهزة والحسابات تحت مراقبة الدولة إذا كانت الأفعال متعلقة بالجرائم المذكورة في المادة 116 مكرر التي تتعلق بالإضرار المتعمد للممتلكات العامة أو المصالح الموكلة إلى الموظفين العموميين، وكذلك الجرائم المذكورة في المادة 308 مكرر المتعلقة بالتشهير والسب عبر المكالمات الهاتفية[1].

تمنح المادة 116 النيابة العامة بعض الصلاحيات الخاصة بإصدار أمر باعتراض ومراقبة الاتصالات عبر الإنترنت. ومن شأن هذا أن يمنح وكلاء النيابة العامة سلطات واسعة لا

[1] "**Cybercrime Law in Egypt: Scope and Implications**", 2019, منشور على موقع https://www.accessnow.org/.

ينبغي منحها إلا للقضاة تماشيا مع مبدأ الفصل بين وظائف النيابة ووظائف القضاء. وتجدر الإشارة إلى أن هذه هي المرة الأولى في تاريخ قانون الإجراءات الجنائية الشامل التي تُمنح فيها هذه الصلاحيات للنيابة العامة من دون رقابة قضائية.

نتفق مع الإجراءات الخاصة للأمم المتحدة، التي أكدت في رسالتها إلى الحكومة المصرية في نوفمبر الماضي أن هذه الأحكام قد تتعارض مع التزامات مصر الدولية، وسيكون لها آثار ضارة على الصحفيين والمدافعين عن حقوق الإنسان والمعارضين، وسوف تمنعهم من ممارسة حقهم في حرية التعبير والتجمع السلمي وتكوين الجمعيات، سواء عبر الإنترنت أو غير ذلك[1].

ورغم هذا التقدم، تواجه الاستراتيجية المصرية تحديات مثل ضعف الثقافة القانونية الرقمية لدى فئات واسعة من المجتمع، وعدم كفاية الكوادر المتخصصة، والحاجة إلى تحديث مستمر للأدوات التقنية والتشريعية لمواكبة تطور الجريمة الإلكترونية.

**الفرع الثاني: الاستراتيجية الإماراتية في مكافحة الجرائم المعلوماتية**

تعد دولة الإمارات العربية المتحدة من الدول العربية الرائدة في مجال مكافحة الجرائم المعلوماتية، حيث عملت على تطوير استراتيجية شاملة تستند إلى التشريعات الصارمة والتعاون الدولي، وتطوير البنية التحتية التكنولوجية، إلى جانب رفع الوعي المجتمعي بمخاطر الجرائم الإلكترونية.

**1. الاطار القانوني:**

وضعت الإمارات إطارًا قانونيًا متقدمًا لمواجهة الجرائم المعلوماتية، ويعد القانون الاتحادي رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، المعدّل بالقانون رقم 12لسنة 2016، حجر الزاوية في هذه الاستراتيجية[2].

يجرّم هذا القانون أفعالاً مثل اختراق أنظمة الحواسيب، نشر محتوى يسيء للدولة أو يخلّ

[1] "**Cybercrime Law in Egypt: Scope and Implications**", 2019, منشور على موقع https://www.accessnow.org/.

[2] عبد العزيز الفاضلي، مرجع سابق، ص 112.

بالأمن العام الابتزاز الإلكتروني، تزوير المستندات الإلكترونية، وانتحال الشخصيات عبر الوسائط الرقمية.

وقد عُدّلت بعض مواد هذا القانون لاحقًا لتشمل الجرائم المتعلقة بالذكاء الاصطناعي والحسابات المزيفة، وتضليل الرأي العام عبر المنصات الرقمية، مما يعكس المرونة التشريعية لمواكبة التطورات التقنية المتسارعة.

**2. البنية المؤسساتية:**

أنشأت الدولة عددًا من الهيئات والكيانات المتخصصة في الأمن السيبراني، من أبرزها:

- الهيئة الوطنية للأمن الإلكتروني.
- المجلس الأعلى للأمن الوطني.
- مركز الإمارات للأمن الإلكتروني.
- برنامج حماية الطفل من الجرائم الإلكترونية الذي أطلقته وزارة الداخلية[1].

**3. حماية الأفراد والمؤسسات من الجرائم الالكترونية:**

- إنشاء قاعدة معلومات متطورة تهتم بحصر عناصر مجرمي المعلوماتية التي تستخدم الشبكة الإلكترونية في الداخل والخارج، ومعرفة الجماعات والجهات والخلايا التي تدعمهم وأهدافهم ومخططاتهم.
- تسهيل إجراءات تبادل المعلومات – بصفة عاجلة – وفق طرق وأساليب سرية محكمة بين الأجهزة الأمنية المعنية داخل الدولة لمكافحة الجرائم الإلكترونية.
- إقامة تعاون فعَّال بين الأجهزة المعنية وبين المواطنين، وإيجاد ضمانات وحوافز مناسبة لتشجيعهم على الإبلاغ عن أي "جرائم معلوماتية" تستخدم الشبكة الإلكترونية، وتقديم المعلومات التي تساعد في الكشف عنها، والتعاون في القبض على مرتكبيها.
- إجراءات المراقبة الداخلية لمعرفة الأشخاص الذين لهم التوجهات والميول الإلكترونية في الخارج واتخاذ جميع التدابير الأمنية اللازمة؛ لمنعهم من ممارسة نشاطهم.

[1] عبد العزيز الفاضلي، مرجع سابق، ص 112.

- تكثيف اللقاءات والاجتماعات الدورية بين الأجهزة الأمنية، وتبادل وجهات النظر والمعلومات المستجدة ، وإعادة تقييم المواقف من أن إلى آخر؛ لمنع أي جرائم معلوماتية عن طريق الشبكة الإلكترونية.
- عدم توفير الملاذ الآمن لمن يُمَوِلُون الأعمال الإرهابية الإلكترونية، أو يديرونها، أو يدعمونها، أو يرتكبونها، ولمن يوفرون الملاذ الآمن للإرهابيين.
- رصد أسماء الأشخاص المتورطين في أعمال إرهابية عن طريق الشبكة الإلكترونية في القائمة السوداء، وتعميمها على المطارات والموانئ والمنافذ.[1]

كما تتعاون الإمارات مع عدد من المنظمات الدولية مثل الإنتربول، واليوروبول، والاتحاد الدولي للاتصالات، وقد شاركت في إعداد الاتفاقيات الدولية والإقليمية لمكافحة الجرائم الإلكترونية، وتسعى باستمرار لتبادل الخبرات والمعلومات حول الشبكات الإجرامية العابرة للحدود.

يتضح من خلال ما سبق أن دولة الإمارات العربية المتحدة قد تبنت نهجاً متقدماً وشاملاً في مكافحة الجرائم المعلوماتية، من خلال إصدار تشريعات صارمة، وبناء بنية تحتية تقنية وأمنية متطورة، إضافة إلى تعزيز التعاون الدولي والإقليمي في هذا المجال. وقد أظهر القانون الاتحادي رقم 5لسنة 2012وغيره من النصوص القانونية، مدى الجدية والإرادة السياسية لدى الدولة في التصدي لهذا النوع من الإجرام المعقد والمتطور. كما يعكس التحديث المستمر لهذه القوانين استجابة سريعة للتغيرات التقنية المتلاحقة، وهو ما يجعل من التجربة الإماراتية نموذجًا عربيًا رائدًا يُحتذى به في هذا المجال الحيوي.

[1] جمال محمد خلفان، سلطان محمد سالم، "**التعاون الوطني والدولي في الجرائم الالكترونية المشاكل والحول**"، مجلة المعهد العالي للدراسات النوعية، المجلد 3، العدد 16، 2023، الامارات العربية المتحدة، ص 5465.

## المطلب الثالث : مقارنة بين الاستراتيجيات الدولية والعربية في مكافحة الجرائم المعلوماتية

باتت الجرائم المعلوماتية من أبرز التحديات الأمنية التي تواجه المجتمع الدولي بالنظر إلى طبيعتها المتطورة، العابرة للحدود، والمعقدة من حيث وسائل ارتكابها. وفي ضوء تنامي هذا الخطر، تبنت الدول استراتيجيات وطنية وإقليمية متنوعة، سعت من خلالها إلى بناء منظومات تشريعية، مؤسساتية، وتقنية لمواجهة هذا النوع المستحدث من الجريمة.

### الفرع الأول: أوجه التشابه والاختلاف بين التجارب الدولية والعربية

**1. أوجه التشابه:**

- إقرار الإطار التشريعي لمكافحة الجريمة المعلوماتية

معظم الدول – سواء الغربية أو العربية – سارعت إلى إصدار قوانين وطنية متخصصة لمكافحة الجرائم الإلكترونية، كخطوة أولى في بناء بيئة قانونية رادعة. على سبيل المثال:

- أصدرت فرنسا القانون المتعلق بثقة الاقتصاد الرقمي.LCEN
- تبنت مصر القانون رقم 175لسنة 2018بشأن مكافحة جرائم تقنية المعلومات.
- أصدرت الإمارات القانون الاتحادي رقم 5لسنة 2012بشأن مكافحة جرائم تقنية المعلومات[1].

- الاعتماد على التكنولوجيا الحديثة في الكشف والتحقيق:

سواء من خلال إنشاء وحدات متخصصة في الأمن السيبراني، أو عبر توظيف برامج التحليل الجنائي الرقميDigital Forensics ، سعت الدول إلى اعتماد مقاربات تقنية لتتبع مرتكبي الجرائم الإلكترونية.

- الاتجاه نحو التعاون الدولي والإقليمي:

تشترك معظم الاستراتيجيات الوطنية في إدراكها لأهمية التعاون عبر الحدود، سواء عبر الانضمام إلى الاتفاقيات الدولية مثل اتفاقية بودابست أو من خلال الشراكات الأمنية مع المنظمات الدولية كالإنتربول ويوروبول.Europol

[1] علي القهوجي، مرجع سابق، ص 453.

### 2. أوجه الإختلاف

- مستوى النضج المؤسسي والتقني

- تتميز الدول الغربية كألمانيا، الولايات المتحدة، بريطانيا بوجود بنى تحتية سيبرانية متطورة، وأجهزة شرطية قضائية رقمية متخصصة ومدربة.
- أما في الدول العربية، فرغم الخطوات المتقدمة لبعضها مثل الإمارات، السعودية، لا تزال مؤسسات المكافحة تعاني من قلة الكفاءات التقنية، وضعف الاستثمار في التكنولوجيا خاصة في دول تعاني من أزمات سياسية أو اقتصادية.

- **التنسيق مع القطاع الخاص**

- في الدول الغربية، يُعد القطاع الخاص شريكًا رئيسيًا في بناء الاستراتيجية الرقمية، سواء من خلال شركات الأمن السيبراني، أو منصات التواصل الاجتماعي.
- في المقابل، لا يزال التعاون بين الحكومات العربية والشركات الخاصة محدودًا وموسميًا في كثير من الأحيان، ما يضعف من فعالية الكشف المبكر عن الجرائم.

- **حماية البيانات والخصوصية**

- الاتحاد الأوروبي، من خلال اللائحة العامة لحماية البياناتGDPR، يقدم نموذجًا متقدمًا لحماية البيانات الشخصية.
- بينما لا تزال معظم الدول العربية تفتقر إلى تشريعات شاملة ومحدثة في هذا المجال مما يفتح الباب أمام اختراقات قانونية وأمنية.

- **التحديث المستمر للقوانين**

- القوانين الغربية تخضع لتحديثات دورية تعكس التطورات التقنية.
- أما بعض القوانين العربية فتعاني من الجمود أو التأخر في التعديل، ما يجعلها أقل ملاءمة للتغير السريع في تقنيات الجريمة[1].

[1] علي القهوجي، مرجع سابق، ص 455.

**الفرع الثاني: فعالية الاستراتيجيات وتحديات التنفيذ**

رغم تعدد الاستراتيجيات وتنوع مقاربات المواجهة، فإن فعالية تنفيذ هذه السياسات على أرض الواقع تصطدم بجملة من التحديات، بعضها مشترك بين الدول، وبعضها خاص بطبيعة السياقات السياسية والاجتماعية لكل دولة.

**1. تقييم الفعالية:**

- الدول الغربية أحرزت تقدمًا ملموسًا، تمثل في انخفاض نسبة بعض أنواع الجرائم، وارتفاع مستوى التنسيق بين الهيئات الأمنية.
- الدول العربية أحرزت تقدمًا متفاوتًا، ففي حين أحرزت الإمارات والسعودية خطوات رائدة في المجال لا تزال دول أخرى تفتقر حتى إلى بنيات مؤسسية متخصصة[1].

**2. التحديات المشتركة:**

- النقص الحاد في الكفاءات المؤهلة:

رغم تطور الوسائل، فإن عدد الخبراء في مجال التحقيقات الرقمية لا يزال محدودًا عالميًا، وهو ما يشكل فجوة كبيرة في الاستجابة السريعة للتهديدات.

- تسارع تطور أدوات الجريمة:

التطور السريع في أدوات الجريمة، كبرمجيات الفدية والذكاء الاصطناعي التخريبي يجعل من الصعب وضع استراتيجيات استباقية فعالة، ويجبر الدول على اتباع سياسة رد الفعل بدلًا من الوقاية الاستباقية

- صعوبة الإثبات الرقمي وتعقيد الإجراءات القضائية:

الأدلة الرقمية تتطلب إجراءات تحقيق وحفظ وتحليل دقيقة، وقد لا تُقبل أحيانًا في المحاكم بسبب قصور في التشريعات أو نقص الخبرة الفنية لدى القضاة.

- ضعف التعاون الدولي والفعلي:

رغم كثرة الاتفاقيات، فإن التطبيق العملي لتبادل المعلومات لا يزال يصطدم بعوائق تتعلق بالسيادة أو اختلاف الأنظمة القانونية.

[1] عبد الله أبو هنية، " **أمن المعلومات في الوطن العربي**"، مركز دراسات الشرق الأوسط، 2021، ص 165.

- ضعف الوعي المجتمعي والوقائي:

تظل فئة واسعة من مستخدمي الإنترنت، في كثير من الدول، تفتقر إلى الحد الأدنى من الوعي بالمخاطر، مما يجعلهم فريسة سهلة للابتزاز أو الاحتيال أو التجسس.

تكشف المقارنة بين الاستراتيجيات الدولية والعربية أن هناك تقاربًا في إدراك خطورة الجريمة المعلوماتية ولكن تفاوتًا واضحًا في الإمكانيات، الجاهزية، والفعالية .وتحقيق مواجهة ناجعة يتطلب مزيدًا من الاستثمار في الكفاءات، وتحديث التشريعات، وتعزيز التعاون الدولي، بما يحقق استجابة أمنية وعدلية متكاملة لهذا التحدي الرقمي العالمي[1].

[1] عبد الله أبو هنية، مرجع سابق، ص 165.

## خلاصة الفصل

تطرق هذا الفصل إلى دراسة شاملة ومقارنة لمختلف الاستراتيجيات الوطنية والدولية المعتمدة في مجال مكافحة الجرائم المعلوماتية، بهدف الوقوف على مقومات فعالية هذه المقاربات، وتحديد أوجه القوة والقصور فيها، خاصة في ظل التطور السريع والمستمر لهذه الظاهرة الجرمية المعقدة والعابرة للحدود.

ففي البداية، تم التركيز على الاستراتيجية الجزائرية، حيث تبين أن الجزائر تبنّت إطارًا تشريعيًا متقدمًا إلى حد ما من خلال تعديل قانون العقوبات واستحداث مواد خاصة بالجريمة المعلوماتية، كما أدرجت أجهزة أمنية متخصصة .ومع ذلك، فإن هذه الاستراتيجية لا تزال بحاجة إلى تدعيم أكبر من حيث البنية التقنية والتنسيق المؤسساتي، وكذا تطوير القدرات البشرية العاملة في المجال الرقمي.

ثم انتقل التحليل إلى إجراءات إثبات الجريمة المعلوماتية، باعتبارها حجر الزاوية في تحقيق العدالة الرقمية .وقد تم إبراز أن النظام القانوني الجزائري يعاني من بعض الصعوبات المرتبطة بإثبات الأفعال الإجرامية المعلوماتية، خاصة فيما يخص الأدلة الرقمية وتعامل القضاء معها، بالنظر لطبيعتها التقنية الدقيقة.

كما تم التطرق إلى تجريم الأفعال المعلوماتية في التشريع الجزائري، حيث تبين وجود تطورات ملموسة شملت تجريم الاختراق، الاحتيال الإلكتروني، نشر الفيروسات، انتهاك الحياة الخاصة الرقمية وغيرها  الا أن بعض الأفعال المستجدة لا تزال تحتاج إلى تقنين واضح ومفصل.

وفي الشق المقارن، تم عرض وتحليل الاستراتيجيات الدولية، من خلال استعراض التجربتين الفرنسية والأمريكية كنموذجين للغرب، وتجربتي مصر والإمارات كنموذجين عربيتين .وقد تم إبراز تقدم واضح في الأنظمة الغربية من حيث تطور البنية التشريعية، التنسيق المؤسسي التكامل مع القطاع الخاص ومستوى الحماية التقنية والتدريب .أما في السياق العربي، فبرزت جهود ملحوظة، خاصة في الإمارات ومصر غير أنها تظل متأثرة بالبيئة السياسية، وضعف الموارد البشرية، وضعف حماية الخصوصية الرقمية.

وفي الأخير، خُصص المطلب الثالث لتحليل أوجه التشابه والاختلاف بين الاستراتيجيات وتقييم مدى فعاليتها، حيث تبيّن أن هناك تقاربًا في الأهداف العامة والتوجه نحو الردع القانوني والتقني، في مقابل اختلافات جوهرية تتعلق بمستوى الجاهزية، مرونة التشريعات التكامل مع القطاع التكنولوجي، وفعالية التنفيذ .كما تم تسليط الضوء على التحديات الكبرى التي تعيق هذه الاستراتيجيات، وعلى رأسها نقص الكفاءات المتخصصة، ضعف التنسيق الدولي، وتطور الجريمة بشكل أسرع من القوانين.

وعليه، فقد أبان هذا الفصل أن أي استراتيجية ناجحة لمكافحة الجرائم المعلوماتية يجب أن تقوم على ركيزتين أساسيتين: تحديث مستمر للترسانة التشريعية والمؤسساتية، وتكوين متخصص ومتجدد للعنصر البشري، مع ضرورة بناء تعاون دولي حقيقي وتكاملي، يواكب الطابع العالمي لهذا النوع من الجرائم.

# خاتمة

لقد استعرضنا في هذا البحث بعمق الجريمة المعلوماتية من جوانبها النظرية والقانونية، كما درسنا الاستراتيجيات الوطنية والدولية المتبعة لمكافحتها. انطلقنا في الفصل الأول من تحديد مفهوم الجريمة المعلوماتية وخصائصها وأركانها، وفصلنا الفرق بينها وبين الجرائم التقليدية، ثم انتقلنا إلى تحليل الإطار القانوني الجزائري من حيث التشريعات الوطنية والهيئات المكلفة بالتنفيذ، وأبرزنا تحديات تطبيق هذه القوانين، قبل أن نبحث التعاون الدولي وإشكالياته القانونية والأخلاقية.

أما في الفصل الثاني، فتناوبنا على عرض الاستراتيجية الوطنية الجزائرية، بدءًا من الجانب التشريعي وصولًا إلى آليات إثبات الجريمة المعلوماتية وتجريم الأفعال المعلوماتية في قانون العقوبات والإجراءات الجزائية. ثم انتقلنا إلى الاستراتيجية الدولية من خلال دراسة نموذجَي فرنسا والولايات المتحدة، ولاحقًا نماذج مصر والإمارات، مع إبراز أوجه التشابه والاختلاف. وختامًا قدّمنا تحليلًا مقارنًا لفعالية هذه الاستراتيجيات، وآليات التعاون الدولي في مجالات التدريب وتبادل المعلومات، وسلّطنا الضوء على أبرز التحديات التقنية والقانونية التي تعترض التنفيذ.

بناءً على ما خلُصت إليه الدراسة من نتائج واستنتاجات، تبرز الحاجة إلى تبني مجموعة من التوصيات التي من شأنها أن تعزز الجهود الوطنية والدولية في مواجهة الجرائم المعلوماتية، وتضمن فعالية أكبر في مجابهة التحديات المتسارعة في هذا المجال الحيوي.

أولًا، يُوصى بضرورة مواصلة تحديث التشريعات الوطنية المتعلقة بالأمن السيبراني، بما يتماشى مع التطورات التقنية الحديثة، لا سيما تلك المرتبطة بالذكاء الاصطناعي، والعملات الرقمية، وأساليب الاختراق المستحدثة، حتى لا تُصبح النصوص القانونية عاجزة عن التجريم أو الإثبات.

ثانيًا، ينبغي إنشاء مراكز تدريب متخصصة في الأمن السيبراني داخل الأجهزة القضائية والأمنية بالتنسيق مع الجامعات المحلية والمؤسسات البحثية الدولية. هذه المراكز يجب أن تركز على تطوير قدرات الكوادر في مجالات التحليل الرقمي، وتتبع الأدلة، والاستجابة السريعة للهجمات الإلكترونية.

ثالثًا، تُوصى الدراسة بتطوير آليات فعالة لتبادل المعلومات والأدلة الرقمية بين الدول، من خلال إبرام اتفاقيات ثنائية وإقليمية قابلة للتنفيذ الفوري، تتضمن إجراءات واضحة بشأن تبادل البيانات، والتحقيق المشترك، والمساعدة القانونية المتبادلة في الجرائم السيبرانية.

رابعًا، لا يمكن إغفال أهمية الوعي المجتمعي، لذا توصي الدراسة بإطلاق برامج تعليمية وتوعوية ثابتة تُدمج ضمن المناهج التربوية ووسائل الإعلام، وتركز على توعية المواطنين، خاصة فئة الشباب بمخاطر الجريمة المعلوماتية، وسبل الحماية منها.

أخيرًا، ينبغي تفعيل دور القطاع الخاص كشريك أساسي في جهود المكافحة، وذلك عبر سنّ حوافز تشريعية وتشجيع التعاون من خلال منصات تشاركية تجمع بين الشركات التقنية، والجهات الأمنية والهيئات الرقابية، لرصد التهديدات المستجدة، ومشاركة الخبرات وأفضل الممارسات.

تشكل هذه التوصيات في مجموعها خارطة طريق عملية لتقوية المنظومة الوطنية والدولية في مواجهة الجريمة المعلوماتية، كما تعكس الحاجة إلى تبني رؤية شاملة تُعلي من قيمة التعاون، التخصص والاستباقية في ظل عالم رقمي يتغير باستمرار.

ختامًا، إن مكافحة الجرائم المعلوماتية تتطلب مقاربة شاملة تدمج بين القانون، والتقنية، والإنسان. فلن يتحقق الأمن الرقمي المنشود إلا بجهود متواصلة ومتضافرة، قادرة على مجابهة تحديات اليوم واستشراف تهديدات الغد.

## قائمة المصادر والمراجع


**أولا: النصوص القانونية**

جمهورية مصر العربية، القانون رقم 175لسنة 2018**بشأن مكافحة جرائم تقنية المعلومات**، الجريدة الرسمية – العدد (33 مكرر ب)، 2018/08/14.

القانون رقم 23/06 المؤرخ في 20 سبتمبر معدل والمتمم لقانون العقوبات، ج.ر، عدد 84.

قانون رقم 06-22 مؤرخ في 2006/12/20، يعدل ويتمم رقم 66-155، يتضمن قانون الاجراءات الجزائية، جريدة رسمية عدد 84، صادرة بتاريخ 2006/12/24.

قانون رقم 09-04 المؤرخ بـ 14 شعبان 2009، والمتضمن للقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها ج ر ع 47، صادر بتاريخ 2009/08/16.

**ثانيا: المصادر العربية**

**الكتب:**

علي عبد القادر القهوجي، "**الجرائم الالكترونية –دراسة مقارنة–**"، دار الجامعة الجديدة، الاسكندرية.

طارق ابراهيم الدسوقي، "**الأمن المعلوماتي النظام القانوني لحماية المعلوماتي**"، دار الجامعة الجديدة للنشر، الاسكندرية، 2009.

شحاتة علا الدين، "**التعاون الدولي لمكافحة الجريمة**"، ايتراك للنشر والتوزيع، القاهدرة، مصر.

عبد الرحمان فتحي سمحان، "**الجوانب الاجرائية المتعلقة بالانترنت**"، دار النهضة العربية، مصر 2012.

جمال الدهشان، "**الجرئم الالكترونية: دراسة قانونية مقارنة**"، **دار النهضة العربية**، القاهرة، مصر 2019.

عبد العزيز الفاضلي، **الجرائم الإلكترونية في التشريع المقارن**، دار النشر للجامعات، مصر، الطبعة 1 2019.

**الرسائل الجامعية:**

سمير شعبان، "**الجريمة الالكترونية، مقارنة تحليلية لتحديد مفهوم الجريمة والمجرم**"، جامعة باتنة الجزائر.

حكيم سياب، "**السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية**"، جامعة 20 أوت 1955 سكيكدة.

الطاهر ياكر، "**مكافحة الجرائم المعلوماتية بين التشريعات الوطنية والاتفاقيات الدولية**"، كلية الحقوق والعلوم السياسية

بخميس مليانة، الجزائر، 2022.

عقباش بريزة، عقباش حنان، "**اليات مواجهة الجريمة الالكترونية في التشريع الجزائري**"، مذكرة لنيل شهادة الماستر، جامعة محمد البشير الابراهيمي، الجزائر، 2022.

ليندة شرابشة،"**السياسة الدولية والاقليمية في مجال مكافحة الجريمة الالكترونية، الاتجاهات الدولية في مجال مكافحة الجريمة الالكترونية**"، المركز الجامعي بسوق أهراس، الجزائر.

سامح أحمد موسى، "**الجوانب الاجرائية للحماية الجنائية لشبكة الانترنت**"، رسالة دكتوراه، كلية الحقوق الاسكندرية، مصر، 2010.

قاضي خولة، جباس منال، "**التعاون الدولي في مكافحة الجريمة المعلوماتية**"، مذكرة لنيل شهادة ماستر كلية الحقوق والعلوم االسياسية بورقلة، الجزائر.

حاحة عبد العالي، قلات سمية، "**المكافحة الاجرائية للجرائم الالكترونية –دراسة حالة الجزائر–**"، كلية الحقوق و العلوم السياسية محمد خيضر ببسكرة، الجزائر، مجلة المفكر، المجلد 13، العدد 02، 2018.

سالم محمد سليمان الأوجلي، "**أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات**"، رسالة دكتوراه، كلية الحقوق عين شمس، مصر.

سليمان أبو نمر، يوسف بوكشريدة، "**مكافحة الجريمة المعلوماتية في اطار القانون الدولي**"، مذكرة ماستر، كلية الحقوق والعلوم السياسية محمد خضير بسكيكدة، الجزائر، 2021.

**رابعا: المقالات:**

مليكة بن عودة، "**الجرائم الالكترونية، في القانون الجزائري**"، مجلة الدراسات القانونية والسياسية، جامعة باتنة، العدد14، 2019، ص 92.

عبد المؤمن بن صغير، "**الطبيعة الخاصة بالجريمة المرتكبة عبر الانترنت في التشريع الجزائري**" الملتقى الوطني حول المعلوماتية بين الوقاية والمكافحة، المنعقد بجامعة بسكرة، 2015.

سمحية بلقاسم، حميد بوشوشة، "**الجريمة الالكترونية بعد جديد للاجرام في الجزائر**"، جامعة قسنطينة الجزائر، مجلة العلوم الانسانية، المجلد 10، العدد 1، 2023.

وريدة جندلي، "**التعاون الدولي لمكافحة الجريمة العلوماتية: الفاعلية والتحديات**"، مجلة القانون والعلوم السياسية، جامعة سكيكدة، المجلد 10، العدد 2، 2024.

بيدي أمال، "**جهود الأمم المتحدة في مكافحة الجرائم السبيرانية**"، مجلة البحوث في كلية العلوم القانونية والسياسية"، جامعة الجلفة، المجلد 8، العدد 1.

سمير قط، "**أثر الجرائم المعلوماتية على أمن واستقرار الدول: قرصنة الموقع الالكتروني لوكالة الأنباء القطرية نموذجا**"، جمعة محمد خيضر ببسكرة، الجزائر، مجلة الناقد للدراسات السياسية، العدد 3، 2018.

سعاد مقدم، "**الجرائم المعلوماتية والجهود المبذولة لمكافحتها**"، جامعة الطارف، مجلة الدراسات في سيكولوجية الانحراف، المجلد 7، العدد 3، 2022.

بوضياف اسمهان، "**الجريمة الالكترونية والاجراءات التشريعية لمواجهتها في الجزائر**"، جامعة بوضياف بالمسيلة، الجزائر، مقال، العدد 11.

فاروق خلف، "**الاليات القانونية لمكافحة الجريمة المعلوماتية**"، كلية الحقوق والعلوم السياسية بالوادي الجزائر، مجلة الحقوق والحريات، العدد 2، 2015.

مهدي رضا، الجرائم السبيرانية واليات مكافحتها في التشريع الجزائري، مجلة ايليزا للبحوث والدراسات جامعة محمد بوضياف بالمسيلة، الجزائر، المجلد 06، العدد 02، 2021.

بوقرين عبد الحليم، قطاف سليمان، "**الاليات القانونية الموضوعية لمكافحة الجرائم السبرانية في ظل اتفاقية بودابست والتشريع الجزائري**"، كلية الحقوق والعلوم السياسية بالأغواط، الجزائر، المجلة الأكاديمية للبحوث القانونية والسياسية، مجلد 6، العدد 1.

بولحية شهرزاد، خلوفي رشيد، تحديات الجريمة الالكترونية في الجزائر، جامعة الجزائر 1، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد 02، 2019.

جمال محمد خلفان، سلطان محمد سالم، **التعاون الوطني والدولي في الجرائم الالكترونية المشاكل والحول** مجلة المعهد العالي للدراسات النوعية، المجلد 3، العدد 16، 2023، الامارات العربية المتحدة.

**ثالثا: المصادر الأجنبية:**

Clifford, R.D, (2015), "**Cybercrime : the investigation, Prosecution and defense of a computer-related crime**".

Weill Pierre-Alain. "**État de la législation et tendances de la jurisprudence relatives à la protection des données personnelles en droit pénal français**" Revue internationale de droit comparé. Vol. 39 N°3. Juillet-septembre.

JEAN francois auran, (10 May 2025), "**Examining the french military programming 2024-2030**", ESD, euro-sd.com/2024/01/articles/36190/examining-the-french-military-programming-act-2024-2030/.

Jacques Massey."**Enquête : le casse-tête des écoutes judiciaires**". La Lettre de l'Expansion. 4 September 2017.

Marc Watin-Augouard,"**La cybercriminalité : défi mondial**", CNRS éditions Paris, 2016, P 178.

**خامسا: المواقع الالكترونية:**

"**La loi pour une République numérique est promulguée**". economie.gouv.fr ( France). Le portail de l'Économie et des Financies. Retrievé 2016-12-01.

Watin-Augouard, M. (2011). "**Cybercriminalité : Défi mondial**"Paris: L'Harmattan, 2012,

"**Groupement interministériel de contrôle**". www.sgdsn.gouv.fr. 17 November 2022. Retrievé 2024-12-28.

AICTO نسخة محفوظة 14 مارس 2012، https://web.archive.org./

"**Cybercrime Law in Egypt: Scope and Implications**", 2019, منشور على موقع https://www.accessnow.org/.

# فهرس الموضوعات

**ملخص:**

يتناول هذا البحث موضوع الاستراتيجية الوطنية والدولية في مكافحة الجرائم المعلوماتية، باعتبارها من أبرز التحديات التي فرضتها الثورة الرقمية على المنظومات القانونية والأمنية حول العالم. وقد تم تقسيم الدراسة إلى فصلين رئيسيين: خصصنا الأول للإطار النظري والقانوني للجريمة المعلوماتية، من حيث تعريفها وخصائصها وأشكالها، مع التركيز على الوضع في الجزائر من حيث التجريم والتكييف القانوني وآليات الإثبات. أما الفصل الثاني، فقد ركّز على الاستراتيجيات العملية المتبعة سواء على المستوى الوطني في الجزائر، أو الدولي من خلال دراسة نماذج مختارة فرنسا، الولايات المتحدة، مصر الإمارات. وتم التطرق إلى آليات التعاون الدولي، وأهمية التدريب وتبادل المعلومات، مع مقارنة فعالية هذه الاستراتيجيات وتحليل أوجه قوتها وضعفها. وقد خلصت الدراسة إلى أن الجريمة المعلوماتية تتطلب استجابة تشريعية وتقنية متطورة، وتعاونًا دوليًا فعالًا، بالإضافة إلى بناء كفاءات بشرية مؤهلة وتعزيز الوعي المجتمعي. كما بيّنت أن الاستراتيجيات الحالية رغم تطورها، لا تزال تواجه تحديات تتعلق بسرعة تطور الجريمة وضعف التنسيق وغياب التشريعات الموحدة.

**الكلمات المفتاحية** :الجريمة المعلوماتية، الاستراتيجية، الأمن السيبراني، القانون الجزائري، التعاون الدولي، التشريع المقارن.

**Abstract:**

This study explores the strategies for combating cybercrime, focusing on the legal frameworks and international cooperation required to address this growing issue. It examines Algeria's national strategy against cybercrime, as well as the global efforts led by organizations such as INTERPOL and EUROPOL. The research also compares the approaches of Western countries (like France and the United States) and Arab nations (such as Egypt and the UAE), evaluating their effectiveness in combating cybercrime. Key challenges identified include a lack of skilled personnel, evolving cyber threats, and the need for improved international coordination.

**Keywords:** Cybercrime, National Strategy, International Cooperation, Algeria, EUROPOL, INTERPOL, France, United States, Egypt, UAE, Legal Frameworks, Cybersecurity.