جامـــــعة عمار ثليجي الاغواط

كـلية الحــقوق والعـــلوم السـياسية

**قسم الحـقوق**

**مذكـرة تخرج ضمن مقتضيات نيل شهادة الماستر**

**تخصص: قانون جنائي وعلوم جنائية**

# اليوروبول و دوره في مكافحة الجريمة الإلكترونية

مذكرة في إطار مقتضيات نيل شهادة الماستر في القانون الجنائي والعلوم الجنائية

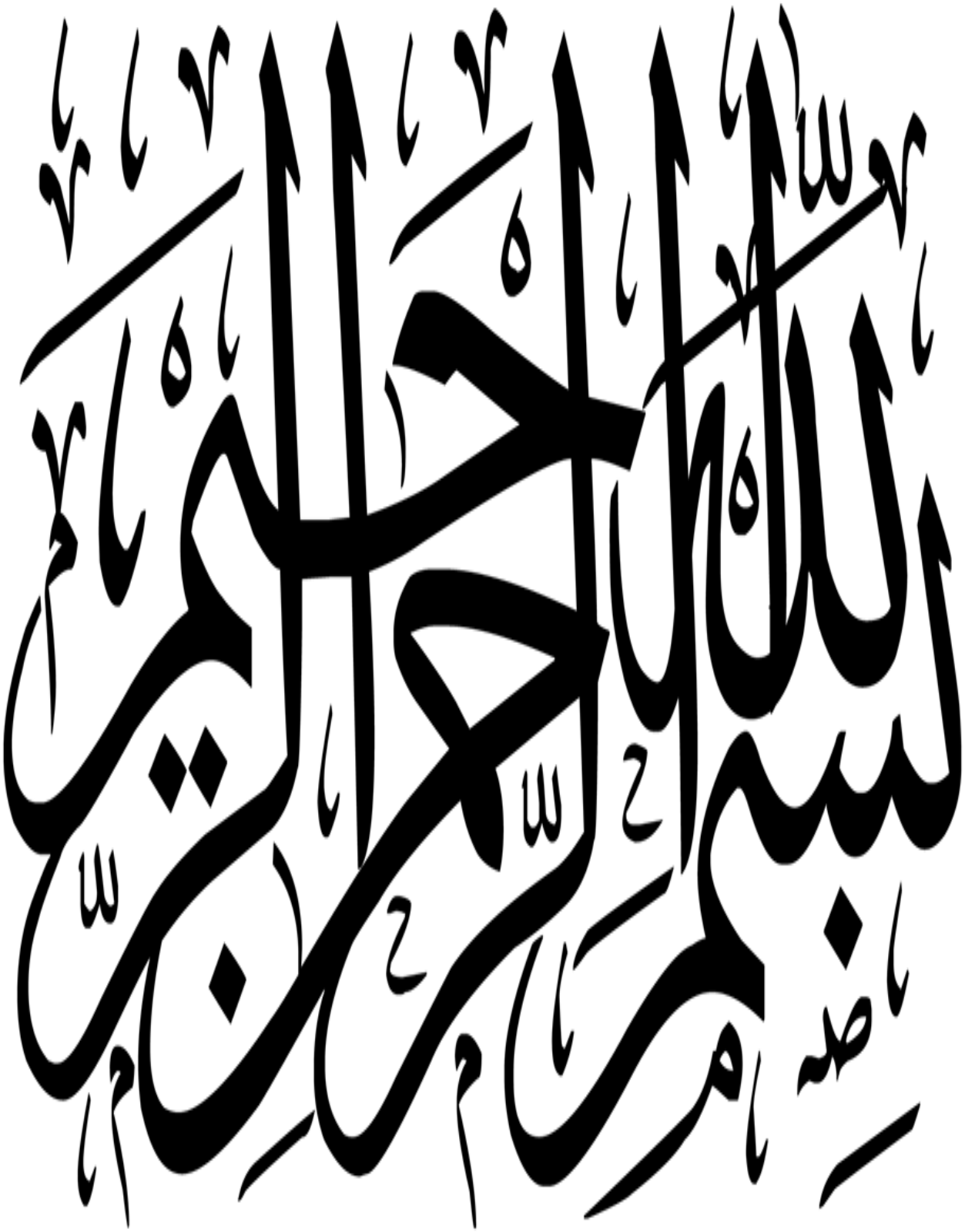
**إعداد الطالبة:** قفاف أمينة

**إشراف الأستاذ:** بن عرفة محمد نذير

أعضاء لجنة المناقشة:

| | |
|---|---|
| أ.د. محمد الحاج عيسى بن صالح | رئيسا |
| د. بن عرفه محمد نذير | مشرفا ومقررا |
| د. مسعود خطوي | ممتحنا |

السنة الجامعية: 2024/2023


بسم الله الرحمن الرحيم

# كلمة شكر

بسم الله الرحمن الرحيم

**قال الله تعالى "وإن شكرتم لأزيدنكم "**

الحمد لله رب العالمين، والصلاة والسلام على أشرف الأنبياء والمرسلين، سيدنا محمد وعلى آله وصحبه أجمعين.

أتقدم بخالص الشكر والعرفان إلى الله سبحانه وتعالى الذي وفقني ومنحني القدرة على إتمام هذه المذكرة.

كما أتوجه بأسمى عبارات الشكر والتقدير إلى والديَّ العزيزين اللذين كانا لي دائمًا سندًا ودعمًا في كل مراحل حياتي الدراسية. فبدعائهما وتشجيعهما المستمر استطعت الوصول إلى هذا الإنجاز.

ولا يفوتنى أن أتوجه بجزيل الشكر والتقدير إلى أستاذي ومشرفي الدكتور بن عرفة محمد

# إهداء

أقدم حصيلة هذا الجهد العلي المتواضع إلى:

من أضاءت لي الطريق بكل عزم وإصرار صاحبة القلب الكبير أطال الله في عمرها

والدتي الحبيبة.

رجل المواقف الشامخة والكرم الذي أنار لي دروب النجاح وكان سندا و معلمي أطال الله

في عمره.

والدي الحبيب.

واهدي محبتي وإخلاصي ودعائي إلى إخوتي

و إلى كل من قدم لي العون والمساعدة في انجاز هذه المذكرة

**قفاف أمينة**

# مقدمـــة

تعتبر الجريمة ظاهرة قديمة ارتبطت بوجود الإنسان البدائي على الأرض، فلا يمكن تصور وقوع جريمة بغير إنسان، كما أنها تطورت وازداد انتشارها بتطور هذا الإنسان على مر العصور. وقد شهد عصرنا الحالي تطوراً غير مسبوق في الاعتماد على التقنيات الحديثة، وأصبح الحاسوب والبرمجيات ركيزة أساسية لأهداف التطور في كافة مجالات الحياة، في مختلف الأنشطة سواء كانت اقتصادية، علمية، تجارية، عسكرية أم اجتماعية، على المستوى الفردي والمؤسسي والمجتمعي والدولي.

وعلى الرغم مما تحمله هذه التقنيات الحديثة من تسهيلات وإمكانات هائلة يسرت على الإنسان الوقت والجهد والمال، فإن البعض قد أساء استخدامها، وهذا ما أدى إلى ظهور نمط جديد من الجرائم، وهي ما يسمى بالجرائم الإلكترونية (المعلوماتية)، والتي تختلف في شكلها ومضمونها ووسائلها عن الجريمة بشكلها التقليدي، ويستمد هذا النوع المستحدث من الإجرام نشاطه من الإمكانات الهائلة للحاسوب والبرامج، وتطور شبكة الإنترنت، والتطور الثقافي والعلمي في التعامل مع التكنولوجيا الحديثة بمختلف أنواعها.

تتعاظم المخاطر الناتجة عن الجرائم الإلكترونية لقدرتها الفائقة على التطور والانتشار وتخطيها للحدود الجغرافية، مستغلة في ذلك ما أتاحته شبكة الإنترنت من انفتاح معلوماتي على العالم بأسره، تعد مكافحة الجريمة بمختلف أنواعها وأصنافها من أبرز الرهانات التي تواجه العدالة الجنائية ككل وأجهزة الشرطة بشكل خاص في العالم بأسره، خاصة في ظل تطور وسائل التكنولوجيا والاتصالات والمواصلات وظهور العولمة التي مست مختلف المجالات الحياتية للأفراد، مما جعل مشكلة الجريمة تأخذ منحنى خطير بسبب هذه التغيرات السياسية والاجتماعية البارزة التي حدثت في أوروبا والدول العربية ومؤخراً في الدول الإفريقية.

ما استدعى من الدولة ضرورة التحرك لحفظ الأمن والاستقرار الذي قد ينزع من المجتمع، وذلك بالتعاون مع جميع الجهات المتخصصة في حفظ الأمن، فالتعاون هو طبيعة بشرية إذ لا يمكن

للإنسان أن يعيش بمعزل عن الآخرين. وفي العصر الحديث، كانت العلاقات بين الدول في هذا المجال أكثر ترابطاً، حيث أصبحت معركة مكافحة الجرائم الإلكترونية أمراً حتمياً.

في هذا السياق، تأسست وكالة اليوروبول في عام 1991 في لاهاي الهولندية بهدف مكافحة الجريمة المنظمة، وتدريجياً توسع دورها في عام 1999 للعمل على مكافحة الإرهاب والتهديدات التي تواجهها أوروبا، لتصبح وكالة رسمية تابعة للاتحاد الأوروبي في عام 2010، تشمل اليوروبول وكالة إنفاذ القانون التابعة للاتحاد الأوروبي، ويطلق عليها "المكتب الأوروبي للشرطة". تعمل الوكالة على مواجهة التهديدات الإلكترونية بشكل مباشر، وبالنظر إلى المستقبل، تظل اليوروبول ملتزمة بالبقاء في مقدمة الجهود لمكافحة الجريمة الإلكترونية عن طريق اعتماد التكنولوجيا الناشئة مثل الذكاء الاصطناعي والتعلم الآلي. إذ تستعد اليوروبول لتعزيز قدراتها في الكشف عن التهديدات وتتبّعها والوقاية منها[1]. علاوة على ذلك، مع استمرار تطور المناظر الرقمية وانتشار أجهزة الإنترنت المحمولة، والحوسبة الكمية، تقوم اليوروبول بالتكيف والابتكار، حفاظاً على النظام الإلكتروني للأجيال القادمة.

فأهمية الموضوع تعود لكون الجريمة هادمة لمختلف المجالات الحياتية الاقتصادية والاجتماعية والسياسية. يستوجب على سلطة اتخاذه مختلف الآليات الصارمة لمكافحتها.

لذا فهذه الآليات التي تتخذها الدول هي في حد ذاتها تعد جديرة بالبحث لدراسة ومعرفة الإجراءات الخاصة في مكافحة الجريمة والقوانين التي تعمل على تسهيل إجراءات مكافحة الإجرام.

تتجسد أهداف هذه الدراسة إلى:

التعرف على الإجراءات الإقليمية والعربية والدولية والجهات المخولة لها مهمة حفظ الأمن ومحاربة مختلف الأعمال غير المشروعة.

التعرف على مدى فعالية هذه الآليات المعتمدة للحد من انتشار الجريمة والمجرمين.

[1] يحيى إبراهيم دحشان، المسؤولية الجنائية عن جرائم الذكاء الإصطناعي، مجلة القانون و الشريعة العدد 82، أفريل 2020,

و تعود أسباب اختيار الموضوع الذاتية إلى:

انتمائي إلى كلية العلوم القانونية واهتمامي بدراسة التعاون الشرطي الدولي ودوره الإيجابي في مكافحة الجريمة وملاحقة المجرمين.

أما الأسباب الموضوعية فتكمن في حداثة الموضوع وتعطش جميع المهتمين لكل المساهمات التي من شأنها إثراء البحوث المتعلقة بالتعاون بين أجهزة الشرطة في الدول الأعضاء في منظمة اليوروبول في مجال مكافحة الجريمة، والتعاون لضبط المجرمين لمساعدة أجهزة الشرطة في مختلف الدول.

ندرة الدراسات القانونية في هذا المجال وضعف الاهتمام الإعلامي الجزائري بمنظمة اليوروبول.

أدى هذا إلى تغييب المنظمة في الجامعة الجزائرية وبالتالي عدم تعرف طلبة القانون، خاصة المتخصصين في القانون الجنائي والقانون الدولي، على الدور الفعال الذي تلعبه المنظمة في قمع الجريمة والحفاظ على الأمن والسلم الدوليين.

وتعود صعوبات الموضع إلى نقص المصادر والمعلومات باللغة العربية تبقى الكتابات حول هذا الموضوع معدودة ولم تصل إلى عامة الناس. لذلك سنحاول من خلال هذه الدراسة ولو بالقليل في التعريف بمنظمة اليوروبول والآليات المستخدمة في مكافحة الجريمة وملاحقة المجرمين الدوليين.

فإشكالية الموضوع تبحث عن كيفية تحديد الآليات والسبل التي تتبعها الدول لمكافحة الإجرام لحماية المجتمع ومصالحه عامة بحكم النتائج السلبية والأضرار التي تخلقها الجرائم. ومن هذا المنطلق، نطرح الإشكالية التالية:

- **ما مدى فعالية اليوروبول كآلية لمكافحة الجريمة الإلكترونية في ظل التحديات المتزايدة والتطورات التكنولوجية السريعة؟**

حتى يتم الإجابة عن الإشكالية المطروحة، لابد من اتباع منهج يلائم طبيعة الموضوع، لأن المنهج هو طريقة تصور وترتيب البحث الذي يهدف إلى تحقيق وتخطيط العمل حول الموضوع الذي قمنا بدراسته. أي أن كل باحث يعتمد على منهج معين لفهم وتحليل المشكلة المطروحة والوصول إلى حقائق موضوعية. لذلك، فقد اعتمدنا "المنهج الوصفي" وذلك باستقراء ما جاء في الاتفاقيات والقوانين ووصف النصوص الخاصة بآليات التعاون الإقليمي والعربي والدولي.

وللإحاطة بكل جوانب الموضوع وللتوصل إلى الإجابة عن الإشكالية المطروحة، ارتأينا أن نقسم الموضوع إلى فصلين. الفصل الأول بعنوان: "جهاز اليوروبول والجريمة الإلكترونية"، الذي يتضمن مبحثين. المبحث الأول خصصناه للحديث عن جهاز اليوروبول، والمبحث الثاني عن مفهوم الجريمة الإلكترونية. أما الفصل الثاني، فكان بعنوان: "دور اليوروبول في مكافحة الجريمة الإلكترونية والتطورات المستقبلية"، والذي يتضمن مبحثين أيضاً. الأول منها كان بعنوان: "دور اليوروبول في مكافحة الجريمة الإلكترونية"، والمبحث الثاني: "التحديات التي تواجه آليات مكافحة الجريمة المنظمة". حيث ختمنا الموضوع بخاتمة عامة للدراسة.

# الفصل الأول

## جهاز اليوروبول و الجريمة الإلكترونية

في ظل التقدم التكنولوجي السريع والتوسع الهائل في استخدام الإنترنت، أصبحت الجرائم الإلكترونية تشكل تهديداً كبيراً على الأمن العالمي. الجرائم الإلكترونية تشمل مجموعة واسعة من الأنشطة غير القانونية التي تستغل التكنولوجيا الرقمية، من اختراقات البيانات وسرقة الهوية إلى الهجمات السيبرانية المدمرة على البنية التحتية الحيوية. مع زيادة تعقيد هذه الجرائم وتطور تقنياتها، أصبح من الضروري وجود جهات متخصصة تستطيع مواجهة هذا التحدي بفعالية.

يأتي في هذا السياق دور جهاز اليوروبول، وهو وكالة تطبيق القانون الأوروبية التي تأسست لمكافحة الجرائم الدولية والإرهاب في الاتحاد الأوروبي. جهاز اليوروبول يلعب دوراً محورياً في التنسيق بين الدول الأعضاء وتبادل المعلومات الاستخباراتية وتحليل البيانات لمكافحة الجريمة المنظمة بأشكالها المختلفة، بما في ذلك الجرائم الإلكترونية.

يتمتع جهاز اليوروبول بقدرات متقدمة في مجالات التحقيق الرقمي وتحليل الجرائم السيبرانية، حيث يعمل على تتبع المجرمين السيبراني و تحليل البرمجيات الخبيثة وتقديم الدعم الفني للدول الأعضاء. من خلال التعاون الوثيق مع وكالات إنفاذ القانون الوطنية والدولية، يسعى اليوروبول لتعزيز الاستجابة المشتركة ضد التهديدات السيبرانية المتزايدة.

## المبحث الأول: جهاز اليوروبول.

المكتب الأوروبي للشرطة EUROPOL هو منظمة تابعة للاتحاد الأوروبي تتعامل مع المخابرات الجنائية، وهدفها تحسين فعالية وتعاون السلطات المختصة في الدول الأعضاء المسؤولة عن منع ومكافحة الجريمة المنظمة الدولية الخطيرة والإرهاب. مهمة يوروبول تتمثل في تقديم مساهمة كبيرة في العمل القانوني للاتحاد الأوروبي ضد الجريمة المنظمة، مع التركيز على استهداف المنظمات الإجرامية، والأهم من ذلك، المساهمة في أمن المواطنين ودول الاتحاد. سيؤدي تحقيق هذا السعي إلى تبديل رأي الذين يشككون في الاتحاد الأوروبي، الذين رحبوا بفكرة وكالة تنفيذية أوروبية فوق الدولية [1]

### المطلب الأول: الظروف المحيطة بتأسيس اليوروبول

سنحاول من خلال هذا المطلب عرض لمحة بسيطة عن نشأة اليوروبول كآلية أوروبية لمكافحة الجريمة عموما و ربطها بموضوع دراستنا و الظروف المحيطة بذلك .

#### الفرع الأول: نشأة اليوروبول.[2]

تأسيس يوروبول كان خطوة هامة فعلا في تعزيز التعاون القانوني بين الدول الأوروبية. ولدت من الإدراك بأن مع زيادة التكامل والحرية في التنقل داخل الاتحاد الأوروبي، يأتي أيضا الحاجة إلى جهود متنسقة لمكافحة الجريمة العابرة للحدود.

---

[1] يوروبول وشرطة مكافحة الإرهاب الدولية: مكافحة الإرهاب في منظور عالمي – ماثيو دفليم – ص (336 – 359) – 18 فبراير 2007.

[2] ألفريدو نانزي– المكتب الأوروبي للشرطة – يوروبول – مجلة القانون الجنائي الدولية المجلد ١١ | جانفي 2006– ألفريدو نانزي – من الصفحة 285الى 292

في أوائل التسعينات، وضعت وحدة مكافحة المخدرات في يوروبول الأسس لما سيصبح يوروبول، مركزة بشكل أساسي على مكافحة تهريب المخدرات داخل أوروبا، ومع ذلك، واعترافا بالطبيعة المتطورة للجريمة والحاجة إلى تفويض أوسع، توسعت مسؤوليات يوروبول مع مرور الوقت لتشمل مجموعة واسعة من الأنشطة الإجرامية بعيدا عن تهريب المخدرات.

و هو يمثل الاستجابة الرئيسية من الدول الأعضاء في الاتحاد الأوروبي لتطور الجريمة الدولية، وذلك جزئياً بسبب مبدأ حرية تنقّل الأفراد، من معاهدة ماستريخت، التي دخلت حيّز التنفيذ في نوفمبر 1993، على إنشاء هذه الهيكلية الأوروبية للتعاون الشرطي، المكلّفة في البداية بتسهيل نقل المعلومات الجنائية المتعلقة بتجارة المخدرات. في يوليو 1995، وقّعت الدول الخمسة عشرة في الاتحاد اتفاقية يوروبول؛ وبالتالي، وتوسّعت اختصاصات المكتب الأوروبي للشرطة لتشمل نقل وتحليل المعلومات الجنائية المرتبطة بتجارة المخدرات، وتجارة المواد النووية والإشعاعية، وتجارة البشر، وتجارة المركبات المسروقة، والهجرة غير الشرعية، وخلال فترة لا تتجاوز عامين، مكافحة الإرهاب. دخلت اتفاقية يوروبول حيز التنفيذ في أكتوبر 1998، ومع ذلك، لا يمكن لمكتب الشرطة الأوروبي أن يبدأ مهامه إلا بعد دخول نصوص تنفيذ الاتفاقية حيّز التنفيذ. في هذه الأثناء، انتقلت وحدة متخصصة في مكافحة المخدرات إلى لاهاي، وشكّلت سابقاً ليوروبول، وقد نصت معاهدة أمستردام لعام 1997 على منح الهيكل اختصاصات تشغيلية، مما يقرّبها بذلك من النموذج المُنشأ للشرطة الفيدرالية الألمانية، بعد تحليل الآليات القانونية المختارة لإنشاء يوروبول، يتعين تقييم فوائد ونقائص هذه الهيكلية الجديدة للتعاون الشرطي، وتحديد جدوى تحويلها إلى شرطة أوروبية فيدرالية.[1]

نص معاهدة ماستريخت نصٌ قانونيٌ لتأسيس يوروبول، بينما المعاهدة التالية ليوروبول، التي أقرتها جميع الدول الأعضاء في الاتحاد الأوروبي، شكلت هيكله التشغيلي. وهذا ما سمح

[1] التعاون الشرطي، سوق المعلومات، وتوسع الجهات الدولية: حالة يوروبول ناديا غيرسباشر المركز الدولي للجريمة المقارنة جامعة مونتريال و فريدريك ليميو أستاذ مساعد، كلية الجريمة المركز الدولي للجريمة المقارنة جامعة مونتريال,

ليوروبول ببدء أنشطته التشغيلية الكاملة في عام 1999، بتفويض لمكافحة أشكال الجريمة الدولية الخطيرة.

يمكن تتبع أصول يوروبول إلى مجموعة تريفي، حيث أدرك مسؤولو إنفاذ القانون من الدول الأوروبية الحاجة إلى تعزيز التعاون لمواجهة التحديات التي تواجهها التكامل المتزايد والجريمة عبر الحدود. وأسس المبادئ التي وضعتها المفوضية الأوروبية لحرية حركة السلع والخدمات ورأس المال والأشخاص على ضرورة اتخاذ تدابير مكافحة الجريمة والسيطرة عليها المتوافقة، مما دفع بتطوير يوروبول كمنظمة شرطة إقليمية.[1]

و قد لعب يوروبول دورا حاسما في تسهيل التعاون بين وكالات إنفاذ القانون في الدول الأعضاء في الاتحاد الأوروبي، وتقديم الدعم التحليلي والتشغيلي، وتنسيق الإجراءات المشتركة لمكافحة مختلف أشكال الجريمة العابرة للحدود في أوروبا.

**المطلب الثاني: هياكل اليوروبول المعنية بمكافحة الجريمة الإلكترونية**

نتيجة لاتفاق مشترك في ديسمبر 2020، أعلنت يوروبول عن إطلاق "منصة فك تشفير مبتكرة" ضمن اختصاصها، والتي ستديرها مركز الجرائم الإلكترونية الأوروبي (3EC) وتطويرها بالتعاون الوثيق مع مركز البحوث المشتركة للاتحاد الأوروبي (JRC) (يوروبول 2020)، وفقًا للمفوضة الأوروبية للشؤون الداخلية يلفا يوهانسون والمديرة التنفيذية ليوروبول كاثرين دي بول، تهدف منصة فك التشفير إلى دعم الجهات الإنفاذ الوطنية من خلال فك تشفير أدلتها الرقمية (يوروبول 2020)، علاوة على ذلك، توفر يوروبول هذه الخدمة مجانًا (فان جيمرت 2019)، وبالتالي تهدف منصة فك التشفير التي أُنشئت بدوافع إنسانية إلى مشاركة خبرة 3EC وJRC

[1] اليوروبول.. حارس أوروبا، الجزيرة، 2016/2/1 تاريخ الإطلاع 12 -04-2024

https://www.aljazeera.net/encyclopedia/2016/2/1 يوم 2024/04/24 على الساعة 00.30 .

ومواردهما التكنولوجية مع الجهات الإنفاذ الأوروبية. تهدف المنصة إلى توفير حلا مستدامًا للجهات الإنفاذ للوصول إلى الموارد التقنية والحسابية دون امتلاكها.[1]

مع التوجهات الرقمية الجديدة في الجرائم الخطيرة وطبيعتها العابرة للحدود، انتقلت المناقشات الأكاديمية في الأدبيات المتعلقة بمجال الحرية والأمان والعدالة في الاتحاد الأوروبي إلى آفاق جديدة. أصبحت التحديات القانونية التي تواجهها يوروبول مع شركائها الخارجيين في العثور على توازن بين الأمن والحرية، مثل توافق بيانات الجريمة وحماية الحقوق الأساسية، هي التركيز الجديد للأدبيات الحالية المتعلقة بالحرية والأمان والعدالة. وتُعتبر يوروبول وسيطًا بين الجهات العامة والخاصة في هذه المناقشات (بوسونغ وفاغنر 2018). في هذا الصدد، تم ترويج نموذج جديد للشراكة العامة–الخاصة (3P)، والمعروف أيضًا باسم "اقتصاد المشاركة" أو "أوبريزيشن" كنموذج جديد للتعاون ليوروبول.[2]

بناءً على التاريخ القصير لمنصة فك تشفير يوروبول، لا تزال الأدبيات المتعلقة بهذا المجال في بدايتها. ووفقًا للمسؤولين في يوروبول، فإن وكالة الشرطة الأوروبية في طريقها لتصبح مركزًا للابتكار لحلول الشرطة مع هذه المنصات. وقد تحول دورها السابق في جمع البيانات إلى دور إدارة بيانات متكاملة أكثر بين الجهات العامة والخاصة، ومع ذلك فإن غياب إطار قانوني وعملي دولي شامل يعد من النقاط المشتركة المبرزة في النقاش حول التشفير.[3]

تتفاوت القدرة المالية والتقنية لدول الاتحاد الأوروبي في التحقيق في التواصل المشفر بين الدول الأعضاء[4].

---

[1] يوروبول والجريمة الإلكترونية: منصة فك التشفير المشتركة ليوروبول" للمؤلفين إيثم إلبيزا وكريستيان كاونرت

[2] إيثم إلبيزا وكريستيان كاونرت، مرجع السابق

[3] نايلة الصليبي، النشرة الرقمية ، كيفية الحماية من الوقوع ضحية برامج الفدية؟ شرت في: 2022/09/29 – 15:03، كيفية الحماية من الوقوع ضحية برامج الفدية؟ – النشرة الرقمية ((mc-doualiya.com

[4] أولدريش بوري، دور اليوروبول في مكافحة الإرهاب: معضلة البيضة والدجاجة ، الصفحات 65–95

فبعض الدول تفتقر إلى الموارد البشرية والمالية للتعامل مع التشفير في التحقيقات الجنائية، بينما تقوم دول أخرى بالحصول على خدمات فك التشفير من شركات خاصة مؤهلة أو من المؤسسات الجنائية الوطنية التي تتعاون مع الجهات الإنفاذية. لذا، تعتبر الحلول على مستوى الاتحاد الأوروبي مفضلة لجميع الدول الأعضاء. في هذا السياق، تجرى مناقشة شرسة في الاتحاد الأوروبي حول كيفية توفير الوصول للجهات الإنفاذية للتواصل المشفر لجمع الأدلة. تقف حلاً تقنياً عند المقدمة لهذه المناقشة، حيث يتم التفكير في بناء أبواب خلفية في البرمجيات المشفرة أو كسر التشفير بالقوة الحاسوبية. بعد عدة سنوات من المناقشة، تم تأجيل حلاً الأبواب الخلفية بسبب المخاوف المتعلقة بحقوق الخصوصية وضعف أمان التشفير. بدلاً من ذلك، اتفقت الدول الأعضاء في الاتحاد الأوروبي على تعزيز قدرات فك تشفير يوروبول لدعم السلطات الوطنية. كنتيجة لاتفاق مشترك في ديسمبر 2020، أعلنت يوروبول إطلاق "منصة فك تشفير مبتكرة"، التي تهدف إلى دعم الجهات الوطنية للإنفاذ بفك تشفير دلائلها الرقمية. هذه الخدمة متاحة مجاناً، وتعتبر منصة الفك تشفير التي تم إنشاؤها بدوافع إنسانية حلاً مستداماً للجهات الإنفاذ للوصول إلى الموارد التقنية والحسابية.[1]

[1] – 21 منصة فك التشفير الجديدة التي أطلقتها يوروبول والمفوضية الأوروبية أدوات برمجية وأجهزة لتقديم المساعدة في الوصول إلى المواد المشفرة للتحقيقات القانونية.ديسمبر 2020. Europol and European Commission Launch New Decryption Platform (cisomag.com)

## المبحث الثاني: مفهوم الجريمة الإلكترونية

لا شك أن الحواسيب في عصرنا الحالي والإنترنت أصبحتا جزءاً لا يتجزأ من حياتنا، حيث أصبحت لا غنى عنهما في مختلف المجالات، توفر هذه التقنيات إمكانيات هائلة للاتصال وتبادل المعلومات، مما يعزز التفاعل الاجتماعي والتطور الاقتصادي، ومع ذلك لا يمكن تجاهل الجانب السلبي، حيث أدت هذه التقنيات أيضًا إلى زيادة حالات جرائم الإنترنت، مثل الاحتيال المالي وسرقة البيانات، مما يهدد أمن المعلومات والخصوصية الشخصية، يتطلب التصدي لهذه التحديات تعاونا دولياً قوياً وتعزيزاً للتشريعات وتطوير استراتيجيات فعالة للحماية السيبرانية.[1]

شمل الجريمة الإلكترونية، كما هو موضح، مجموعة واسعة من الأنشطة غير المشروعة التي ترتكب باستخدام الحواسيب والإنترنت، بدءاً من سرقة البيانات والاحتيال المالي إلى الإرهاب الإلكتروني والاستغلال، وبسبب الطبيعة غير المحدودة للإنترنت، يصعب مكافحة جرائم الإنترنت، حيث يمكن للجناة العمل من أي مكان مع خطر الكشف الأدنى.[2]

واقتباس الدكتور محمد صالح العدلي لجريمة الإنترنت ك "نسل غير شرعي" لثورة التكنولوجيا المعلوماتية والعولمة، يصورها كتحدي هائل يتجاوز الحدود الجغرافية والدينية والوطنية، ويشير النص أيضاً إلى الآثار المالية والأمنية الكبيرة لجرائم الإنترنت، مستشهداً بالإحصائيات لتسليط الضوء على انتشارها وتأثيرها.[3]

مع غزو الإنترنت، أصبح من الصعب بمكان ضبط وكشف جرائم الإنترنت، حيث تتجاوز هذه الجرائم الحدود ولا تلتزم بدين أو وطن، يتم تنفيذها بسرعة فائقة دون رقيب أو حسيب، وبدون

---

[1] عبد الكريم الشامي–جرائم الكمبيوتر والإنترنت في التشريع الفلسطيني – ورقة عمل مقدمة للأمانة العامة لمجلس وزراء الداخلية العرب (سبتمبر 2004)

[2] هبه جمال الدين، الأمن السيبراني والتحول في النظام الدولي، مجلة كلية الاقتصاد والعلوم السياسية، المقالة 7، المجلد 24، العدد 1 – 94، يناير 2023، الصفحات 189–230

[3] الجريمة الإلكترونية – د. كامل مطر. 17 أبريل 2016.

رقابة من أي دولة. تشمل هذه الجرائم القرصنة والسطو على الأموال، والتجسس باستخدام البيانات المسروقة، والإرهاب الإلكتروني الذي يهدد أمن الدول. كما تشمل أيضًا جرائم الإباحية الإلكترونية، خاصة تلك المستهدفة للأطفال، والتي تتضمن استغلال دعارة الأطفال والنساء، جميع الدراسات تؤكد على أن الهدف الرئيسي للمجرمين الإلكترونيين هو تحقيق مكاسب مادية بحتة، سواء من خلال سرقة الأموال أو البيانات السرية، أو تدمير برامج المعلوماتية لدول بأكملها لتهديدها في أمنها القومي وسلامة أراضيها.[1]

## المطلب الأول: الجرائم الإلكترونية أنواعها و تطورها

تعد الجرائم الإلكترونية من أخطر التحديات التي تواجه المجتمع في العصر الحالي حيث إن تطور تكنولوجيا المعلومات و الاتصالات صاحبه ظهور أنواع جديدة للجريمة الإلكترونية و أنماط و أساليب جديدة من النشاط الإجرامي و تعددت عبر الأنظمة الرقمية و الفضاء السيبراني.

### الفرع الأول: تعريف الجريمة الإلكترونية:

الجريمة الإلكترونية هي نوع من الجرائم التي ترتكب باستخدام التقنيات الحديثة، مثل أجهزة الكمبيوتر والإنترنت، والتي تهدف إلى الإضرار بالأفراد أو المؤسسات أو البيانات الإلكترونية[2]. يمكن تعريف الجريمة الإلكترونية بأنها أي نشاط غير قانوني يتم بواسطة أو ضد أجهزة الكمبيوتر أو الشبكات الإلكترونية، ويشمل ذلك مجموعة متنوعة من الأعمال الإجرامية مثل الاختراقات السيبرانية، والاحتيال الإلكتروني، وانتهاكات حقوق الملكية الفكرية عبر الإنترنت، وغيرها.

تعريف الجريمة الإلكترونية يمكن أن يكون متنوعًا بناءً على المنظور والسياق القانوني والتشريعي لكل دولة. ولذلك، هناك تعريفات متعددة للجريمة الإلكترونية تتنوع بين الواسعة والضيقة.

---

[1] عبد الصبور عبد القوي علي– الجريمة الإلكترونية والجهود الدولية للحد منها – ماجستير في القانون – كلية الحقوق – جامعة بني سويف .

[2] د. ليلى عبد المجيد، التنظيم التشريعي والقانوني للإعلام التقليدي والإلكتروني، 2 يونيو 2021

**أولا: التعريف الواسع للجريمة الإلكترونية:**

يتضمن هذا التعريف جميع أنواع الجرائم التي ترتكب باستخدام التكنولوجيا الحديثة، مثل الحواسيب والشبكات الإلكترونية.

يشمل استخدام الحاسوب كأداة رئيسية لارتكاب الجريمة، بالإضافة إلى الوصول غير المصرح به لبيانات الآخرين، والاعتداء على الأجهزة الإلكترونية، والاستخدام غير القانوني للمعلومات الشخصية، والتزوير الإلكتروني، والتلاعب في البيانات المالية، والاحتيال الإلكتروني.[1]

**ثانيا: التعريف الضيق للجريمة الإلكترونية:**

يركز هذا التعريف على الأنشطة الجنائية التي تتطلب معرفة تقنية متقدمة، مثل اختراق النظم الأمنية، وتقنيات التشفير.

يستثني الأنشطة التي قد تكون جرائم بشكل تقليدي ولا تتطلب معرفة تقنية متقدمة، مثل سرقة الأموال عبر الإنترنت دون استخدام تقنيات معقدة.[2]

التحديد القانوني للجريمة الإلكترونية يعتمد على تشريعات كل دولة، حيث يتم تحديد الأفعال والعقوبات المناسبة لمنع ومكافحة هذا النوع من الجرائم، وقد تتضمن تلك التشريعات تعديلات على قوانين العقوبات لتشمل جرائم الإنترنت وتقنيات الحاسوب.[3]

---

[1] عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية و أزمة الشرعية الجزائية، كلية القانون، جامعة الكوفة، العدد 7 ،2008 ص112 – 113.

[2] عبد الحكيم موالي ابراهيم، الجرائم االلكترونية، مجلة الحقوق و العلوم االنسانية، جامعة زيان عاشور، الجلفة، الجزائر، المجلد الثاني، العدد 23 ،2015 ص 213.

[3] عادل محمد فريد نائلة، جرائم الحاسب آاللي االقتصادية، ط ،1 منشورات الحلبي الحقوقية، بيروت، لبنان، ،2005 ص27 .

**الفرع الثاني: اختراق الأمان والاحتيال الإلكتروني**

اختراق الأمان والاحتيال الإلكتروني يشكلان تحديًا كبيرًا في عصرنا الحالي مع تطور التكنولوجيا. يمكن أن يحدث اختراق الأمان عن طريق استغلال الثغرات في نظام الحماية الخاص بالبيانات أو الأنظمة الإلكترونية. وقد يتم ذلك من قبل متسللين يرغبون في الوصول غير المشروع إلى معلومات حساسة أو لأغراض أخرى غير شرعية. من جهة أخرى، يشمل الاحتيال الإلكتروني محاولات النصب والاحتيال التي تتم عبر الإنترنت، والتي قد تشمل الرسائل الاحتيالية والبريد الإلكتروني المزيف والمواقع الويب المزيفة.

لحماية الأنظمة والبيانات من الاختراق والاحتيال، يجب اتباع مجموعة من الممارسات الأمنية مثل تحديث البرامج بانتظام، واستخدام كلمات مرور قوية، وتشفير البيانات الحساسة، وتنفيذ تدابير الوقاية من البرمجيات الخبيثة. بالإضافة إلى ذلك، يجب على المستخدمين توخي الحذر وعدم الوثوق بالرسائل أو الروابط الغريبة التي تصلهم عبر الإنترنت.[1]

يعتمد الحد من اختراق الأمان والاحتيال الإلكتروني على التوعية المستمرة وتبني الثقافة الأمنية القوية داخل المؤسسات والمجتمعات، بالإضافة إلى استخدام التكنولوجيا الحديثة للكشف عن ومكافحة التهديدات الإلكترونية بشكل فعال.

[1] أمن الحوسبة السحابية: الأهداف والمجالات والمكونات وطرق تطبيقها ، كتابة : بكه، 24 أبريل 2024 أمن الحوسبة السحابية: الأهداف والمجالات والمكونات وطرق تطبيقها – بكه للتعليم ((bakkah.com

**الفرع الثالث: أنواع جرائم الاحتيال الإلكترونية**

يشكل الإحتيار الإلكتروني أحد أوجه الجرائم المستحدثة التي انتشرت في الآونة الأخيرة في الدولة، و أصبحت تهدد الكثير من أفبراد المجتمع، خاصة بعد تزايد استخدام التكنولوجيا الحديثة في مجالات الاتصالات و الإدارة و الأعمال المصرفية و المالية، وهي المعطيات التي تشكل بيئة خصبة لعمل عصابات الإجرام الإلكتروني.

ومن أنواع جرائم الاحتيال الإلكتروني نذكر منها :

**أولا. الجرائم الموجهة ضد نظم المعلوماتية:**

**1. الجرائم الواقعة على المكونات المادية للنظام المعلوماتي:**[1]

يشمل هذا النوع من الجرائم التلاعب بالأجهزة الحاسوبية والمعدات ذات الصلة. يمكن أن يتضمن ذلك سرقة الأجهزة أو تدميرها بوسائل مختلفة مثل الفيروسات والبرمجيات الخبيثة.

في السياق الأعم، تشمل هذه الجرائم الهجمات الجسيمة على البنى التحتية للإنترنت، مثل هجمات حجب الخدمة (DDoS) التي تعطل خدمات الإنترنت للمستخدمين.

**2. الجرائم الواقعة على المكونات المنطقية للنظام المعلوماتي:**[2]

يشمل هذا النوع من الجرائم اختراق الأنظمة والبرمجيات بغية الوصول غير المشروع للبيانات والمعلومات الحساسة.

يمكن أن تتضمن أيضًا اختراق البنية التحتية للشبكات لأغراض التجسس أو القرصنة الإلكترونية.

[1] خالد ممدوح ابراهيم، الجرائم المعلوماتية، ط،2 دار الفكر الجامعي االسكندرية، مصر، ،2019 ص 116 .

[2] هدى حامد قشقوش، جرائم الحاسب آللي في التشريع المقارن، دار النهضة العربية، القاهرة، ،1992 ص15 .

### 3. الجرائم الواقعة على المعلومات المسجلة بالنظام المعلوماتي:

هذه الجرائم تشمل سرقة البيانات الشخصية والمالية، سواءً من خوادم الشركات أو من قواعد بيانات المستخدمين.

يمكن أن تشمل أيضًا هجمات التشويه وتعديل البيانات بهدف إلحاق الضرر بالمؤسسات أو الأفراد.

ثانيا. الجرائم الواقعة بواسطة النظام المعلوماتي:

### 1. جرائم اقتصادية ومالية:

تشمل هذه الجرائم الاحتيال المالي عبر الإنترنت، حيث يتم استغلال البيانات الشخصية والمالية لغايات الاحتيال والاستيلاء على الأموال.

يمكن أن تتضمن أيضًا جرائم الاختراق المالي، مثل تزوير الشهادات البنكية الإلكترونية والتلاعب بالأسواق المالية.[1]

### 2. جرائم الاعتداء على الأشخاص:

تشمل هذه الجرائم الابتزاز والتهديد عبر وسائل التواصل الاجتماعي والإنترنت، حيث يتم استخدام البيانات الحساسة لإرهاب الأفراد أو المؤسسات.

يمكن أن تتضمن أيضًا جرائم صناعة ونشر المحتوى الغير لائق أو الإباحي بهدف تشويه سمعة الأفراد أو الشركات.[2]

---

[1] خالد ممدوح ابراهيم، المرجع السابق، ص .76

[2] يوسف صغير، الجريمة المرتكبة عبر ألنترنت، رسالة لنيل شهادة الماجستير، تخصص القانون الدولي لألعمال، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، الجزائر، 2013 ، ص 50.

### 3. جرائم أمن الدولة:

تتضمن هذه الجرائم الإرهاب الإلكتروني والتجسس الإلكتروني، حيث يتم استخدام التكنولوجيا للتأثير على الأمن القومي والاقتصادي للدول.

يمكن أن تتضمن أيضًا جرائم القرصنة الإلكترونية التي تستهدف البنية التحتية للدولة مثل الشبكات الحكومية والعسكرية.[1]

### الفرع الرابع: تهديدات الخصوصية و التجسس الالكتروني

يتمثل الحق في الخصوصية في الحماية اللازمة للشخصية الفردية، وقد اتجهت التشريعات الوطنية والدولية نحو تعزيز هذا الحق وحمايته من أي انتهاك، سواء كانت من جهات حكومية أو أفراد. يُعتبر الحق في الخصوصية حقًا أساسيًا من حقوق الإنسان، حيث يحمي الأفراد من أي تدخل تعسفي في حياتهم الشخصية، وشؤون أسرهم، وممتلكاتهم، ومراسلاتهم، ويحميهم أيضًا من حملات التشهير التي تؤثر على سمعتهم وشرفهم.[2]

ومع التطور السريع في التكنولوجيا، خاصة في الفضاء الرقمي، زادت التحديات المتعلقة بحق الخصوصية وتزايدت حالات انتهاكه. فقد أصبح من السهل على المتسللين الرقميين الوصول إلى معلومات الأفراد والمؤسسات عن طريق الاختراق الإلكتروني والتجسس الرقمي. يشكل التجسس الرقمي تهديدًا كبيرًا للأمن الرقمي، ويشكل تحديًا للسيطرة على المعلومات وحفظ الأمان القومي.[3]

---

[1] خالد ممدوح ابراهيم، المرجع السابق، ص115 .

[2] جمال عبد الله، الآثار الاجتماعية والنفسية والمخاطر المجتمعية للتكنولوجيا الحديثة، جامعة زايد – أبو ظبي– الإمارات العربية المتحدة، المجلد 24، العدد 10، 2023، الصفحات 186–199

[3] هبه جمال الدين، مرجع سابق

بالتالي، تعتمد الدول اليوم على استخدام التقنيات السيبرانية لحماية أمنها الوطني ومعلوماتها الحساسة، وتوجه جهودها نحو تطوير سياسات وإطار قانوني يحمي حقوق الأفراد في الفضاء الرقمي، ويحد من حالات التجسس الرقمي والاختراق الإلكتروني.

**أولا: تعريف التجسس الإلكتروني**

التجسس الإلكتروني هو استخدام التكنولوجيا الحديثة، مثل الأنظمة الحاسوبية والشبكات الإلكترونية، للحصول على معلومات سرية أو حساسة دون موافقة صاحبها، سواء كانت تلك المعلومات عبارة عن بيانات شخصية أو سر تجاري أو معلومات استخباراتية. يشمل ذلك استغلال الثغرات في الأمن الإلكتروني، أو استخدام البرمجيات الخبيثة مثل الفيروسات وبرامج التجسس، أو حتى استخدام تقنيات الهندسة الاجتماعية لاختراق أنظمة المعلومات.[1]

التجسس الإلكتروني يعتبر نوعًا من الجوسسة الحديثة التي تعتمد على التكنولوجيا، وقد أصبح تهديدًا كبيرًا للأفراد والمؤسسات وحتى للدول، نظرًا لقدرته على الوصول إلى معلومات حساسة واستخدامها في أغراض غير شرعية مثل الابتزاز أو التجسس الصناعي أو الهجمات السيبرانية.[2]

**ثانيا: تأثير التجسس الالكتروني على الحق في الخصوصية المعلوماتية**

التجسس في معناه الاصطلاحي يشير إلى البحث والتنقيب عن معلومات سرية أو حساسة، خاصة تلك المتعلقة بالعدو، باستخدام وسائل سرية وفنية، يتم ذلك عادةً من خلال العملاء والجواسيس الذين يقومون بنقل هذه المعلومات للاستفادة منها في إعداد الخطط أو في غايات

[1] عبد الرحمن شامخ الرشيدي، دور معلمي الدراسات الاجتماعية فى تعزيز قيم المواطنة الرقمية من وجهة نظرهم، المقالة 1، المجلد 2021، العدد 61، يناير 2021، الصفحات 53-73.

[2] أمن المعلومات د. دلال صادق + د. حميد ناصر الفتال, دار اليازوري العلمية للنشر والتوزيع

أخرى، في القانون الدولي، يتم تعريف الجاسوس بأنه الشخص الذي يعمل بسرية أو يختبئ للحصول على معلومات في منطقة العمليات بهدف تبليغها للفريق الخصم.[1]

التجسس الكلاسيكي، كما جاء في القوانين الدولية، يشمل جمع المعلومات التابعة لطرف في النزاع باستخدام الأساليب الخادعة أو التخفي، بهدف تبليغها للعدو. وعلى الصعيدين الدولي والوطني، قد يكون تعريف التجسس مختلفًا، حيث تحدد التشريعات الوطنية صور السلوك المجرم للجريمة بدلاً من تقديم تعريف دقيق للتجسس.[2]

في السياق الحديث، يشير التجسس الإلكتروني أو الرقمي إلى استخدام التقنيات الحديثة مثل الحواسيب والشبكات الإلكترونية للحصول على المعلومات بطرق غير شرعية، مثل الاختراق أو التنصت على المحادثات الشخصية عبر الإنترنت أو تقاطع البيانات الشخصية.[3]

التجسس الإلكتروني يشمل مجموعة من الطرق التي يستخدمها الفاعل لاختراق المواقع الإلكترونية بهدف سرقة المعلومات الحساسة التي قد تكون خطيرة إذا وصلت إلى الطرف الآخر. يمكن أن تكون هذه المعلومات تتعلق بالأمن الوطني، أو العلاقات الخارجية، أو السلامة العامة، أو الاقتصاد الوطني.[4]

---

[1] ليت الدين صلاح حبيب، التجسس وأحكامه إبان النزاعات المسلحة الدولية، مجلة جامعة الانبار للعلوم القانونية والسياسية، المجلدة، العدد1 ص310.

[2] إسراء يوسف هادي، أسامة احمد النعجي، جريمة التجسس الالكتروني في إطار مشروع قانون جرائم المعلوماتية العراقي لسنة 2011، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد10، العدد36، 2021، ص 35-36.

[3] الذهبى خدوجة، حق الخصوصية في مواجهة الاعتداءات الالكترونية،(دراسة مقارن)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد الأول، العدد الثامن،جامعة المسيلة، 2017، ص 147.

[4] إسراء يوفس هادي، أسامة احمد النعجي، مرجع سابق، ص 37.

في القانون الأردني، تم تعريف التجسس الإلكتروني كدخول الجاني إلى الشبكة المعلوماتية أو نظام المعلومات بأي وسيلة كانت، بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني.[1]

تحمل جريمة التجسس الإلكتروني صلة بالإرهاب الإلكتروني، حيث يُمكن اعتبارها شكلاً من أشكال العدوان أو التخويف أو التهديد المادي أو المعنوي، الذي يتسبب في آثار مدمرة على محطات التحكم وشبكات الاتصال. يربط بعض الأشخاص بين التجسس الإلكتروني والإرهاب الإلكتروني، حيث يُعتبران نوعًا من العدوان أو التهديد على الأفراد والمؤسسات.[2]

تختلف جريمة التجسس الإلكتروني عن جريمة القرصنة الإلكترونية في الأغراض والنوايا، حيث يركز التجسس الإلكتروني على التنصت أو انتهاك سرية البيانات، في حين تنطوي القرصنة الإلكترونية على الوصول غير المشروع إلى الملكية الفكرية أو المعلومات المحمية بحقوق النشر.[3]

**ثالثا: خصائص التجسس الرقمي**

لتجسس الإلكتروني يتميز بعدة خصائص تجعله تحديًا كبيرًا للأجهزة الأمنية والقوانين الجنائية:

**الحداثة والسرعة والسهولة:** يعتمد التجسس الإلكتروني على تقنيات حديثة وسريعة في التنفيذ، كما يسهل إخفاؤه ومحو أثاره بسرعة. هذا يجعل من الصعب على الأجهزة الأمنية تحديد هوية المجرمين والتحقيق في جرائم التجسس الإلكتروني.[1]

---

[1] أبو ذر شأكر عبد، التجسس الالكتروني في ظل التشريع الأردفي، مجلة العلوم السياسية والقانون، مجاد+،العدد26، المركز الدمقراطي العربي– برلين، المانياء 2020، ص 43.

[2] عبد الهادي محمود الزيدي، التجسس الإسرائيلي الالكتروني على الدول العربية، مجلة دراسات دولية، العدد58، 2014، ص 140.

[3] ضرغام جابر علوش آ مواش، جريمة التجسس المعلوماتي، المركز العربي، 2017، ص 96.

1. **عبور الحدود الجغرافية:** بسبب طبيعة الشبكات الإلكترونية التي لا تعترف بالحدود الجغرافية، يمكن لجريمة التجسس الإلكتروني أن تؤثر على أشخاص في دول مختلفة، حتى وإن كانت العمليات الإجرامية تتم في دولة معينة.[2]

2. **تأثير واسع النطاق:** يمكن للتجسس الإلكتروني أن يؤثر على عدد كبير من الأفراد والمؤسسات في وقت قصير، نظرًا لقدرته على نقل كميات كبيرة من المعلومات وتبادلها بين الأنظمة المختلفة بسرعة.[3]

تواجه الأجهزة الأمنية صعوبات في مكافحة جرائم التجسس الإلكتروني، لذلك يجب أن تكون ملمة بأنظمة المعلوماتية وتقنياتها المتطورة، وتكون لديها القدرة على استخدام التقنيات المتقدمة للتحقيق والتحري في هذه الجرائم.

**3. أنواع التجسس الالكتروني أو الرقمي:** للتجسس الالكتروني أنواع تختلف بالنظر للوسيلة الالكترونية التي يتم بها، فقد يتم التجسس على الأشخاص عبر شبكة الانترنت أو من خلال الشبكات السلكية واللاسلكية أو عن طريق الهواتف النقالة أو الجوال، كما يمكن أن يحدث عبر الموجات والترددات، وكذلك التجسس الالكتروني من خلال الأقمار الصناعية.

### 1 تجسس الأشخاص عبر الإنترنت:

هذا النوع من التجسس يتم من خلال استخدام برامج خارجية تبدو كبرامج طبيعية تقدم خدمات معينة، ولكن في الواقع، تقوم بتجسس على نشاطات المستخدمين على الإنترنت. يستخدم

---

[1] عبد الحميد احمد، جرائم الشبكة العنكبوتية وغسل الأموال في إطار الملاحقة الأمنية والقضائية الدولي، مكتبة الوفاء القانونية، الطبعة الأولى، الإسكندرية، 2018، ص 72.

[2] د. ليلى عبد المجيد ، التنظيم التشريعي والقانوني للإعلام التقليدي والإلكتروني، 2 يونيو 2021

[3] أمن المعلومات د. دلال صادق + د. حميد ناصر الفتال د. دلال صادق + د. حميد ناصر الفتال, دار اليازوري العلمية للنشر والتوزيع

المخترقون أو الهاكرز برامج مثل البرامج الخادم والعميل للاتصال بجهاز الضحية والقيام بعمليات التجسس.[1]

**2 التجسس الإلكتروني عبر الشبكات السلكية واللاسلكية:**

في هذا النوع من التجسس، يتم اعتراض وتسجيل البيانات المرسلة عبر الشبكات السلكية أو اللاسلكية. يستخدم القراصنة برامج مثل برامج الـ "sniffer" لاصطياد الحزم المرسلة واستخراج المعلومات منها. واحدة من الهجمات الشهيرة التي حدثت باستخدام هذا النوع من التجسس كانت في كوريا الجنوبية عام 2011.[2]

**3 التجسس الإلكتروني عبر الهواتف المحمولة:**تمثل التكنولوجيا المتقدمة للهواتف المحمولة والخدمات التي تقدمها تحدياً كبيراً لخصوصية الأفراد. يتيح استخدام الهواتف المحمولة تجسسًا سهلاً على الأفراد، ويمكن من خلالها التجسس على الرسائل النصية والملفات وتحركات الأفراد.[3]

**4 التجسس الإلكتروني عبر الموجات والترددات:**

يمكن استخدام جميع أنواع الموجات والترددات في التجسس، وتشمل هذه الموجات المستخدمة في الراديو والتلفزيون والهواتف وأجهزة الحاسوب. ومع ذلك، هناك ترددات سرية يمكن استخدامها للتجسس، وتتطلب هذه العملية جهاز استقبال لاسلكي متقدم ومعرفة في مجال البرمجيات والتشفير.[4]

---

[1] حسن بن احمد الشهري، الأنظمة الالكترونية الرقمة المطورة لحفظ وحماية سرية المعلومات من التجسس، المجلة العربية للدراسات الأمنية والتدريب، امجلد28، العدد56، 2012، ص 12

[2] اوشن حنان، وادي عاد الدين، التجسس الالكتروني واليات مكالحته في التشريع الجائي الجزائري، مجلة الحقوق والعلوم السياسية،العدد2 جامعة عباس لغرور خنشلة، 2014، ص 132.

[3] صبرينة بن سعد، حراية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا الإعلام والاتصال، أطروحة دكتوراه، كلية الحقوق، جامعة باتنة ،2015 ص112.

[4] اوشن حنان، وادي عماد الدين، مرجع سابق، ص 135.

### 5 التجسس الإلكتروني عبر الأقمار الصناعية:

توفر الأقمار الصناعية فرصاً للتجسس على الأفراد من خلال مراقبة حركتهم وأنشطتهم في أي مكان في العالم. تستخدم الأقمار الصناعية المخصصة للتجسس لمراقبة الحركة والأنشطة لأشخاص معينين. ومن ابرز الاقمار الصناعية التي استخدمت في التجسس نذكرّ :[1]

– أقمار التجسس الأمريكية، التي انطلقت في استخدامها مع نهاية الخمسينيات، مثل القمر الصناعي كورونا (corona)، وساموس(Samos)، وارغوه (Argon) ولانيار(Lanyard) وغامبيت (gambit) وكريستال(crystal) وغيرها ...

– أقمار التجسس التابعة للاتحاد السوفياتي سابقا، مثل كوسموس (cosmos)، رورسات(rorstal)،

– الماز (almaz)،إضافة إلى أقمار أطلقتها دول أخرى كبريطانيا والهند وألمانيا والصين وكوريا الجنوبية ...

### رابعا: انتهاك التجسس الإلكتروني لحق الخصوصية المعلوماتية

تعدّ حماية الخصوصية المعلوماتية أمرًا بالغ الأهمية في العصر الرقمي الحديث، حيث تزداد حجمًا وتنوعًا بيانات الأفراد والمؤسسات المخزّنة والمعالجة عبر الإنترنت. ومع ذلك، يتعرض هذا الحق الأساسي إلى تهديدات خطيرة بفعل التجسس الإلكتروني، الذي يستهدف استغلال البيانات الشخصية بطرق غير قانونية وغير مشروعة.[2]

5 مظاهر اعتداء التجسس الرقمي على حق الخصوصية المعلوماتية

---

[1] عبير علي عبد العزيز شري، مشروعية التجسس عبر الأقار الصناعية في القانون الدولي العام، مجلة جامعة الانبار للعلوم القانونية والسياسية، المجاد9، العدد2019،2، ص 788.

[2] د. ليلى عبد المجيد، مرجع سابق

يعتمد التجسس الرقمي على مجموعة متنوعة من الأساليب لاختراق البيانات الشخصية واستغلالها. ومن بين هذه المظاهر:

### 1. دس الفيروسات الإلكترونية

دس الفيروسات الإلكترونية يعد أحد أساليب التجسس الرقمي الشهيرة والخطيرة التي تهدد الأمان السيبراني وتنتهك حقوق الخصوصية المعلوماتية. يتمثل هدف هذه الفيروسات في زرع برامج ضارة في أنظمة الحاسوب بهدف الاستيلاء على البيانات الحساسة أو تعطيل الأنظمة، مما يؤدي في النهاية إلى تخريب الأجهزة وفقدان البيانات.[1]

يعتبر برنامج "حصان طروادة" من بين الفيروسات الإلكترونية الأكثر شهرة وخطورة. يتم استخدامه بشكل خفي ومتقن في البرامج التطبيقية، مما يسمح بالوصول إلى قواعد البيانات الحساسة واستخدامها بطرق غير قانونية. ومن ثم، يمكن للقراصنة إرسال هذا الفيروس عبر البريد الإلكتروني، المحادثات، أو حتى من خلال تنزيل ملفات من مواقع أنترنيت مشبوهة.[2]

يتميز برنامج "حصان طروادة" بقدرته على تغيير البرامج والبيانات داخل الحاسوب، مما يجعله صعب الكشف عنه. يمكن لهذا النوع من الفيروسات أيضًا تدمير نفسه بعد إكمال مهمته، مما يجعل من الصعب تتبعه والقضاء عليه.[3]

وتشير الدراسات إلى أن أعدادًا متزايدة من البرامج الضارة تهدف لاختراق أجهزة الاتصالات الإلكترونية يوميًا، مما يعزز الحاجة الملحة لتعزيز أنظمة الحماية الإلكترونية وتعزيز الوعي الأمني لدى المستخدمين.[1]

---

[1] شريقي الشريف، مدى احترام الحق في الخصوصية في الحسابات الالكترونية على الانترنت، مجلة القانون والمجتمع، المجاد4، العدد1،2019، ص 121

[2] هروال هبة نبيلة، جرائم الانترنت (دراسة مقارنة)، أطروحة دكتوراه،جامعة تلمسان، 2013/2014، ص 374.

[3] صبرينة بن سعد، مرجع سابق، ص150

التطور المستمر في أساليب التجسس الإلكتروني، خاصة فيما يتعلق بتطوير الفيروسات الإلكترونية، يشكل تحديًا كبيرًا لأنظمة الحماية الإلكترونية. في الدراسة التي أجرتها شركة "كاسبرسكي لاب" (Kaspersky Lab) سنة 2014 في مجال مكافحة الفيروسات وحماية الأجهزة الإلكترونية من الهجمات، أظهرت النتائج وجود حوالي 300 ألف تطبيق ضار يحاول اختراق أجهزة الاتصالات الإلكترونية يوميًا.[2]

## 2. استخدام أساليب تقنية أخرى للتجسس الرقمي

استخدام أساليب تقنية أخرى للتجسس الرقمي يمثل تحديًا إضافيًا لأمن المعلومات وخصوصية الأفراد. من بين هذه الأساليب:

أ -إخفاء المعلومات داخل المعلومات: يعتمد المجرمون في هذه الطريقة على إخفاء المعلومات الحساسة داخل معلومات أخرى عادية في الحاسوب. يتم ذلك من خلال كتابة برامج تنفيذية بسرية على حواسيب الضحايا، والتي تقوم بفحص جميع البيانات المخزنة على الحاسوب ونقلها بشكل مخفي.

ب – استخدام تقنية الأبواب المصيدة أو الحفية: يقوم المهاجمون في هذه الطريقة بإنشاء باب خفي في البرنامج المستخدم بواسطة الشركات أو المؤسسات، مما يتيح لهم سرقة البرامج والبيانات.

---

[1] سوزان عدنان الأستاذ، اتهاك حرمة الحياة الخاصة عبر الانترنت، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية (دراسة مقارنة)، المجاد 29 لعدد 3، 2013، ص 435.

[2] سليم حميدائي، اختراق الخصوصي في العالم الرقمي: حدود الظاهرة ومطالب الحماية القانونية، مجلة البحوث في الحقوق والعلوم السياسية، ص43

ت – ربط الهوائيات مع حاسوب خاص: يمكن للمهاجمين استخدام الهوائيات لالتقاط الموجات الكهرومغناطيسية التي تنبعث من الحواسيب على بعد مسافة تصل إلى 300 قدم خلال تشغيلها، ومن ثم تسجيلها ومعالجتها لاستخراج المعلومات.

هذه التقنيات تظهر التطور المستمر في مجال التجسس الرقمي والحاجة الملحة إلى تطوير استراتيجيات أمنية فعالة للتصدي لهذه التهديدات وحماية خصوصية الأفراد والمؤسسات.

### 3. وسائل حماية الخصوصية المعلوماتية من جريمة التجسس الالكتروني

تطورت وسائل حماية الخصوصية المعلوماتية لمكافحة جريمة التجسس الإلكتروني بشكل ملحوظ، وتضمنت عدة تقنيات وأدوات للوقاية والدفاع ضد التهديدات الإلكترونية. إليك بعض الوسائل الرئيسية لحماية الخصوصية المعلوماتية:

أ برامج مكافحة الفيروسات وبرمجيات الأمان: تستخدم هذه البرامج للكشف عن الفيروسات والبرمجيات الخبيثة وإزالتها من الأجهزة. تشمل هذه البرامج برامج مضادة للبرمجيات الخبيثة، وجدار الحماية، وبرامج كشف التجسس.[1]

ب – التحديثات الدورية للأنظمة والبرامج: يجب تحديث أنظمة التشغيل والبرامج بانتظام لسد الثغرات الأمنية وتحسين الحماية ضد التجسس الإلكتروني.

ت – استخدام تقنيات التشفير: يتم استخدام التشفير لحماية البيانات وجعلها غير قابلة للقراءة من قبل أي شخص غير مخول. يمكن تشفير البيانات أثناء النقل وأثناء التخزين لضمان سرية وأمان المعلومات.[2]

[1] صيرينة بن سعد، مرجع سابق، ص 205.

[2] حسن بن احمد الشهري، مرجع سابق، ص 23-24.

2- **التحقق الثنائي**Two-Factor Authentication)) : يضيف هذا النوع من الحماية طبقة إضافية من الأمان عند تسجيل الدخول إلى الحسابات عبر طلب إدخال رمز تأكيد إضافي بجانب كلمة المرور.

1.**التدريب على الوعي الأمني:** يتضمن تعزيز وعي المستخدمين بشأن مخاطر التجسس الإلكتروني وكيفية التعامل مع الرسائل الاحتيالية والملفات المشبوهة والتصرف بحذر عند تبادل المعلومات عبر الإنترنت.

2.استخدام أدوات تقييم الأمان السيبراني: تقوم هذه الأدوات بفحص الأنظمة والشبكات لتحديد الثغرات الأمنية وتقديم توصيات لتعزيز الأمان.

تطبيق هذه الوسائل والتقنيات يساهم في تقوية الأمان السيبراني وحماية البيانات الحساسة من جريمة التجسس الإلكتروني وغيرها من التهديدات الأمنية على الإنترنت.

4.الوسائل القانونية لمكافحة التجسس الرقمي

التشريعات تختلف في درجة تعاملها مع جريمة التجسس الإلكتروني، حيث تتباين بين التشريعات التي اكتفت بالنصوص التقليدية المجرمة للتجسس وتلك التي أصدرت تشريعات خاصة تحمي الخصوصية المعلوماتية بشكل جنائي. وهناك تشريعات تعديلت على قوانين العقوبات لتشمل تجريم مثل هذه الانتهاكات.[1]

من الجدير بالذكر أن التشريعات المقارنة استخدمت مصطلحات مختلفة عن "التجسس"، مثل "التصنت"، و"الالتقاط"، و"الاعتراض"، و"الدخول دون تصريح" وغيرها، وهذا دون تجريم خاص لفعل التجسس الرقمي، على الرغم من أنها تجرم التجسس التقليدي.[2]

[1] محمود احمد له، المواجهة التشريعية لجرائم الكمبيوتر والانترنت (دراسة مقارنة)، دار الفكر والقانون، المنصورة، 2012، ص 61.

[2] أبو ذر شأكر عبد، مرجع سابق، ص49- 51.

في السياق الجزائري، يجد التشريع أيضًا تجريم فعل التجسس التقليدي في مادة 61 من قانون العقوبات، دون الإشارة إلى التجسس الرقمي. ومع ذلك، تعمل التشريعات الجزائرية على حماية خصوصية الأفراد بطرق قانونية أخرى، من خلال فصل مكرر من الباب الثاني للكتاب الثالث من الأمر 66/156 المتضمن قانون العقوبات، الذي يتناول المساس بأنظمة المعالجة الآلية للمعطيات.

هذه التشريعات تمثل خطوات هامة في مكافحة جريمة التجسس الإلكتروني وحماية خصوصية المعلومات، على الرغم من أنه قد يكون هناك حاجة لتحديثها لتواكب التطورات التكنولوجية وتحديات الأمان الرقمي المعاصرة.[1]

**المطلب الثاني: آثار الجريمة الإلكترونية**

في ظل التقدم الهائل للتكنولوجيا والتحول الرقمي الذي شهدته العديد من الدول، أصبحت الجرائم الإلكترونية واحدة من أخطر التحديات التي تواجه الاقتصاد العالمي. تعتبر هذه الجرائم تهديدًا كبيرًا للأفراد والشركات والحكومات على حد سواء، حيث تؤدي إلى خسائر مالية هائلة وتعطيل الأنشطة الاقتصادية.[2]

مع توسع استخدام الإنترنت وتبادل البيانات الرقمية بشكل متزايد، أصبحت القطاعات الاقتصادية عرضة لمخاطر عديدة تتمثل في الجرائم الإلكترونية المتنوعة[3]. تشمل هذه الجرائم

[1] اوشن حنان، وادى عماد الدين، مرجع سابق، ص 139.

[2] أماني محمد شريف عبد السلام ، تصور مقترح لتنمية الوعي الأمني لدى طلاب جامعة أسيوط في ضوء خبرات بعض الدول،لية التربية – جامعة أسيوط،– المجلد الثامن والثلاثون– العدد الثانيِ عشر – ديسمبر 2022م

[3] بن جدو بن علية . درار عياش، الآثار الاقتصادية للجريمة الالكترونية، المجلد 5، العدد 1، الصفحات 558-577، 31 مارس 2022

الاحتيال الإلكتروني، والاختراقات السيبرانية، وتهديدات البرمجيات الخبيثة، والتجارة الإلكترونية غير الشرعية، وغيرها من الأنشطة غير المشروعة التي تؤثر بشكل كبير على الاقتصاد.

تتطلب مكافحة هذه الجرائم جهودًا مشتركة من قبل الحكومات والشركات والمجتمع الدولي، من خلال تبني استراتيجيات شاملة لحماية الأنظمة الإلكترونية، وتعزيز الوعي بأهمية الأمن الإلكتروني، وتشديد القوانين وتطبيق العقوبات على المتورطين في هذه الجرائم.

إن التحديات التي تطرحها الجرائم الإلكترونية تستدعي استراتيجيات فعّالة لمكافحتها وضمان استمرارية النمو الاقتصادي والتنمية المستدامة في جميع القطاعات الاقتصادية.

**الفرع الأول: تأثير الإحتيال المصرفي على الإقتصاد**

يمكننا أن نرى أن التحول من الاقتصاد التقليدي إلى الاقتصاد الرقمي قد زاد من تعقيدات الأمور وزاد من حجم التحديات التي تواجه القطاع المصرفي والاقتصاد بشكل عام. مع التزايد الكبير في استخدام الإنترنت للتعاملات المصرفية والمالية، أصبحت الجرائم الإلكترونية والاحتيال المصرفي تهديداً أكبر على الاقتصاد العالمي.

تظهر الأرقام أن الخسائر الناتجة عن الجرائم الإلكترونية تبلغ تريليون دولار سنوياً، ومع زيادة هذه الجرائم، يتجاوز الخطر المالي الحقيقي مجرد حجم الخسائر. فهذه الجرائم تمثل عائقاً كبيراً أمام ممارسة الأعمال التجارية في جميع أنحاء العالم.

من المتوقع أن تتجاوز التكاليف الإجمالية للجرائم الإلكترونية في جميع أنحاء العالم 6 تريليونات دولار في عام 2021، وهو معدل يسجل ارتفاعاً ملحوظاً مقارنة بالسنوات السابقة. وتشير التقديرات إلى أن قطاع الخدمات المالية يعتبر الأكثر عرضة للهجمات بنسبة 46٪، تليه قطاع الرعاية الصحية بنسبة 24٪، وثم قطاع الطاقة بنسبة 22٪.[1]

[1] خالد ممدوح العزي،جرائم املالية إلالكترونية /الجرائم املصرفية نموذجا، أعمال مؤتمر الجرائم إلالكترونية المنعقد في طرابلس/ لبنان، يومي 21-24|92|،2911 ص 12

منطقة الشرق الأوسط تعتبر من بين الأكثر تضرراً في العالم من الهجمات الإلكترونية، حيث خسرت حوالي 199 ألف دولار من الشركات المنطقة الواحدة التي تعرضت للهجوم الإلكتروني.[1]

توضح هذه الأرقام الخطورة التي تمثلها الجرائم الإلكترونية على الاقتصاد العالمي، حيث تتجاوز خسائرها حجم الخسائر الناتجة عن العديد من المصادر الأخرى للتهديدات، مثل التجارة غير المشروعة وتجارة المخدرات. وفي هذا السياق، تعتبر الجرائم الإلكترونية تحدياً كبيراً يتطلب استراتيجيات متكاملة لمكافحتها وحماية الأنظمة المالية والبنوك والشركات من هذه التهديدات المتزايدة.

**الفرع الثاني: تداعيات اختراق البيانات الخصوصية الفردية**

مفهوم الخصوصية في سياق التكنولوجيا يعني حماية البيانات الشخصية والمعلومات الحساسة والخاصة بالأفراد والشركات. الخصوصية تعتبر الحق الأساسي للأفراد في الحفاظ على خصوصيتهم وسرية معلوماتهم، وتحظى بأهمية كبيرة في منع الفساد والاعتداء على الحقوق الشخصية و المالية.[2]

في عام 1890، أشار لويس براندیس (Louis Brandeis)، قاضي أمريكي، إلى أن الخصوصية هي "الحق في الانسجام والوحدة"، مما يعني حق الفرد في أن يكون له مساحة خاصة يمكنه أن يكون فيها نفسه دون تدخل خارجي. في نفس السياق، وضع ألان ويستن (Westin Alan)، باحث في الخصوصية، تعريفاً للخصوصية بأنها "حالة من عدم التدخل في الأمور الخاصة التي

[1] ..16ليان عوده، لجرائم إلالكترونية أبرز مخاطر الثورة الصناعية الرابعة 18 يناير على الموقع http://www.alarabiya.net/ar/aswaq/world-economic-forum/2017/01/18 2911 consulté le 2017/05/25

[2] عائشة لخشين، جامعة الأمير عبد القادر، الجزائر، حماية الحق في الخصوصية في العصر الرقمي في المواثيق الدولية، مقال منشور في مجلة جيل حقوق الانسان العدد 39 في الصفحة 109

يتمتع بها الأفراد بحق، وحالة من الحرية من الاعتداء والتدخل الغير مرغوب فيه في الأمور الشخصية".

مفهوم معلومات الخصوصية (Privacy Information) يشمل جميع المعلومات التي تتعلق بالأفراد أو الشركات، سواء كانت معلومات مالية أو طبية أو شخصية، بما في ذلك بيانات الاتصال والتفاصيل الشخصية الأخرى، ويتم تنظيمها وإدارتها بموجب مجموعة من القوانين واللوائح.

الخصوصية ومعلومات الخصوصية تصبح ذات أهمية خاصة في العصر الرقمي الحديث، حيث يتم استخدام البيانات الشخصية بشكل واسع في التسويق والتجارة الإلكترونية، ويتزايد خطر انتهاك الخصوصية وسرقة البيانات مما يهدد الأفراد والشركات بخسارة الثقة والسمعة، ويتطلب منهم اتخاذ التدابير اللازمة لحماية خصوصيتهم ومعلوماتهم.

التهديدات الإلكترونية التي تشكل تهديداً على الخصوصية تتنوع بشكل كبير، وتشمل ما يلي:

**أولا: سرقة الهوية:**

يتمثل هذا التهديد في سرقة معلومات شخصية حساسة مثل الأسماء وتواريخ الميلاد وأرقام الضمان الاجتماعي ومعلومات البطاقة الائتمانية.

يتم استخدام هذه المعلومات للقيام بأنشطة احتيالية مثل فتح حسابات بنكية مزيفة، أو التسوق عبر الإنترنت بطريقة غير شرعية، أو التقدم بطلبات قروض بأسماء مزيفة.[1]

[1] دانيال ج. سولوف، الضعف الجديد: أمان البيانات والمعلومات الشخصية كلية القانون في جامعة جورج واشنطن : 9 أغسطس 2011

**ثانيا: الاحتيال عبر الإنترنت**

يشمل هذا التهديد الاستخدام غير الشرعي للإنترنت لخداع الأفراد والحصول على معلوماتهم الشخصية أو المالية.

يتضمن أمثلة على الاحتيال عبر الإنترنت الرسائل الاحتيالية (الفيشنج)، ومواقع الويب المزيفة التي تحاكي المواقع الرسمية للبنوك أو الشركات لسرقة معلومات تسجيل الدخول، والعروض المضللة للشراء عبر الإنترنت.[1]

**ثالثا: الاختراق**

يتمثل هذا التهديد في دخول غير مشروع لأنظمة الكمبيوتر أو الشبكات بهدف الوصول إلى المعلومات أو التلاعب بها.

يمكن أن يتسبب الاختراق في سرقة بيانات شخصية أو مالية، أو تعطيل خدمات الإنترنت، أو التسبب في أضرار أخرى للأفراد أو المؤسسات.[2]

تلك التهديدات تتطلب توعية شاملة للمستخدمين حول أفضل الممارسات لحماية خصوصيتهم وأمانهم عبر الإنترنت، بما في ذلك استخدام كلمات مرور قوية، وتحديث البرامج والتطبيقات بانتظام، والحذر من الرسائل الاحتيالية والمواقع الويب المشبوهة. كما تتطلب تلك التهديدات جهودا مشتركة من الحكومات والشركات والأفراد لمكافحتها والحد من تأثيرها السلبي.

1. **الاختراق والاختراق السيبراني:** يشمل هذا التهديد دخول أو اختراق الأنظمة الإلكترونية أو الشبكات بهدف الوصول إلى المعلومات الحساسة أو التلاعب بها. يمكن أن يؤدي الاختراق إلى سرقة بيانات شخصية أو مالية أو تعطيل خدمات الإنترنت.[1]

[1] داريل لونغ.هندسة أنظمة المعلومات عبر الويب .المجلد 36، العدد 3، مايو 2011، الصفحات 675-705

[2] من المعلومات د. دلال صادق + د. حميد ناصر الفتال, دار اليازوري العلمية للنشر والتوزي

2.**البرمجيات الضارة والفيروسات:** تتضمن هذه التهديدات البرمجيات الخبيثة مثل الفيروسات وأحصنة طروادة وبرامج التجسس التي يمكن أن تقوم بسرقة معلومات المستخدمين أو تتلف الأنظمة.

تتطلب مكافحة هذه التهديدات جهودًا مشتركة من الحكومات والشركات والأفراد لتحسين أمان البيانات وحماية الخصوصية عبر الإنترنت. يجب على المستخدمين أيضًا اتخاذ إجراءات وقائية مثل استخدام برامج مضادة للفيروسات والحفاظ على كلمات المرور القوية والحذر من الرسائل والروابط الغير معروفة.

[1] الدولية برج اسمهان; مسيود سميرة ; مزعاش أكرم، الهجمات السيبرانية وأثرها على العلاقات السياسية. 2022

**خلاصة الفصل:**

ندرك بوضوح أن التطور التكنولوجي والانتشار الواسع للإنترنت قد أحدثا تحولًا جذريًا في طبيعة الجريمة وطرق مكافحتها، ومع تعقيدات هذا التحدي المتزايد، يبرز دور الهياكل الأوروبية مثل اليوروبول كمركز للتنسيق والتعاون الدولي في مجال مكافحة الجريمة الإلكترونية، هذا النوع من الجريمة يشكل تحدياً كبيراً للأمن العام نظراً لتطور التكنولوجيا واستخدامها في أنواع مختلفة من الجرائم، تسعى هياكل يوروبول كآلية أوروبية لمكافحة الجريمة الإلكترونية إلى توحيد الجهود بين الدول الأعضاء، وتبادل المعلومات والخبرات لتعزيز قدرات الدول على مكافحة هذا النوع المتطور من الجريمة.

# الفصل الثانـي

## دور اليورويول في مكافحة الجريمة الإلكترونية

في عصر الثورة الرقمية، أصبحت الجرائم الإلكترونية تهديداً متنامياً للأمن العالمي، تتنوع من اختراقات البيانات وسرقة الهوية إلى الهجمات السيبرانية على البنية التحتية الحيوية. جهاز اليوروبول، وهو وكالة تطبيق القانون الأوروبية، يلعب دوراً محورياً في مكافحة هذه الجرائم من خلال التنسيق بين الدول الأعضاء، وتبادل المعلومات الاستخباراتية، وتحليل البيانات. يمتلك اليوروبول قدرات متقدمة في التحقيق الرقمي وتحليل الجرائم السيبرانية، ويساهم في تتبع المجرمين السيبرانيين وتحليل البرمجيات الخبيثة وتقديم الدعم الفني للدول الأعضاء.

طور اليوروبول مبادرات وبرامج عديدة لتعزيز قدراته في مواجهة الجرائم الإلكترونية، منها تشكيل فرق متخصصة، وتوفير التدريب والموارد اللازمة للدول الأعضاء. كما يتبنى استراتيجيات مبتكرة لمواكبة التطورات التكنولوجية السريعة، مثل الاستثمار في التكنولوجيا المتقدمة كالذكاء الاصطناعي وتحليل البيانات الكبيرة. بالإضافة إلى ذلك، يعزز اليوروبول التعاون الدولي لمواجهة التهديدات السيبرانية العابرة للحدود .

## المبحث الأول: دور اليوروبول في مكافحة الجريمة الإلكترونية

اليوروبول (المكتب الأوروبي للشرطة) يلعب دوراً حيوياً في مكافحة الجريمة الإلكترونية في أوروبا ومناطق أخرى. يعمل اليوروبول كمركز للتعاون الدولي بين الدول الأعضاء في الاتحاد الأوروبي وكذلك مع الدول غير الأعضاء، بهدف مكافحة الجريمة المنظمة والإرهاب، وبما في ذلك الجرائم الإلكترونية.[1]

من بين الأدوار الرئيسية التي يقوم بها يوروبول في مكافحة الجريمة الإلكترونية:

التحليل والمعلومات: يوروبول يقدم تحليلات استخباراتية ومعلومات عن الأنشطة الإجرامية على الإنترنت والتهديدات الأمنية ذات الصلة.

التدريب والدعم الفني: يوفر يوروبول التدريب والدعم الفني للشرطات الوطنية في دول الاتحاد الأوروبي لتمكينها من مكافحة الجريمة الإلكترونية بفعالية.

تنسيق التحقيقات: يعمل يوروبول على تسهيل التعاون بين الوحدات الوطنية للتحقيق في الجرائم الإلكترونية، ويسهل تبادل المعلومات والخبرات.

تطوير القدرات: يعمل يوروبول على تعزيز قدرات الشرطات الوطنية في مجال مكافحة الجريمة الإلكترونية من خلال تبادل المعرفة والتدريب.

تم إنشاء مركز الجريمة الإلكترونية الأوروبي (3EC) بواسطة اليوروبول في عام 2013 لتعزيز استجابة إنفاذ القانون لجرائم الإنترنت داخل الاتحاد الأوروبي، بهدف حماية المواطنين الأوروبيين والشركات والحكومات من الأنشطة الإجرامية على الإنترنت. منذ بدايته، ساهم 3EC بشكل كبير

[1] يوروبول والجرائم الإلكترونية: منصة مشاركة الفك التشفير ليوروبول إثم إلبيز وكريستيان كاونرت الصفحات 270-283 | نشر عبر الإنترنت: 10 نوفمبر 2021

في مكافحة جرائم الإنترنت من خلال العمليات البارزة، والنشرات الميدانية الفورية، والعديد من الاعتقالات، وتحليل الملفات الضارة.[1]

في المستقبل، من المتوقع أن يلعب يوروبول دوراً أكبر في مواجهة التحديات المستقبلية للجريمة الإلكترونية، مثل زيادة التعقيد والتطور في الهجمات الإلكترونية، والتحديات المتعلقة بالتشفير والأمن السيبراني. قد يتطلب ذلك تعزيز التعاون الدولي وتطوير تقنيات جديدة لمواجهة هذه التحديات المتزايدة.

**المطلب الأول: تبادل المعلومات و التحليلات الجنائية**

تبادل المعلومات بين الجهات الأمنية والتحليلات الجنائية المشتركة يسهم في تعزيز الفهم والتصدي للجرائم الإلكترونية بشكل أكبر. فعندما تشترك الجهات الأمنية في تبادل المعلومات حول الأنماط الجديدة للجريمة الإلكترونية أو النشاطات الجنائية على الإنترنت، يمكنها تحديد التهديدات بشكل أسرع واتخاذ إجراءات محددة لمكافحتها.

من ناحية أخرى، يلعب التحليل الجنائي دورًا حيويًا في فهم أعمق للبيانات الرقمية والأدلة المتاحة. باستخدام تقنيات التحليل المتقدمة، يمكن للمحللين الجنائيين تحليل البيانات لتحديد الأنماط والاتجاهات والعلاقات بين الجرائم المختلفة. هذا يمكنهم من رسم صورة شاملة للجريمة الإلكترونية وتحديد المشتبه بهم وتطوير استراتيجيات فعالة لمكافحتها.

بالتالي، يعمل تبادل المعلومات والتحليلات الجنائية المشتركة على تعزيز التعاون والتنسيق بين الجهات المعنية في مكافحة الجرائم الإلكترونية، ويساهم في تحسين الاستجابة الشاملة والفعالة لهذه التهديدات المتزايدة.[1]

[1] افتتاح مركز الجريمة الإلكترونية الأوروبي (3EC) في 11 يناير" (بيان صحفي). المفوضية الأوروبية. 9 يناير 2013. مؤرشف من الأصل في 23 يونيو 2017. الوصول في 21 سبتمبر 2017.

**الفرع الأول: أهمية تحليل البيانات في مكافحة الجريمة الإلكترونية**

تحليل البيانات يلعب دوراً حيوياً في مكافحة الجريمة الإلكترونية، حيث يساهم في تحديد الأنماط الجديدة للجرائم وتحليل السلوكيات الإلكترونية للمشتبه بهم من خلال تحليل البيانات، يمكن تحديد الاتجاهات الجديدة في الجريمة الإلكترونية وتطوير استراتيجيات فعالة لمكافحته. بالإضافة إلى ذلك، يمكن استخدام تحليل البيانات لتحديد الضحايا والمشتبه بهم، وتقديم دعم للتحقيقات وتعزيز القدرة على اتخاذ إجراءات قانونية فعالة

تحليل البيانات يساهم أيضا في تحديد الأماكن التي تحدث فيها الجرائم الإلكترونية بشكل متكرر، وبالتالي يمكن توجيه الجهود التحقيقية والوقائية بشكل أفضل بالاعتماد على تحليل البيانات، يمكن للجهات الأمنية تحديد الثغرات الأمنية وتعزيز الجهود الوقائية لمنع واكتشاف الجرائم الإلكترونية بفعالية.[2]

في النهاية، يعتبر تحليل البيانات أداة حيوية في مجال مكافحة الجريمة الإلكترونية، حيث يساهم في تعزيز القدرة على التصدي للتهديدات السيبرانية وتحقيق العدالة الرقمية.

**الفرع الثاني: أساليب تحليل البيانات المستخدمة من قبل اليوروبول**

ستخدم اليوروبول بالفعل أساليب تحليل البيانات المتقدمة لمكافحة جرائم الإنترنت بفعالية. تشمل هذه الأساليب مجموعة من التقنيات المتقدمة، بما في ذلك:

[1] – د. بوضياف إسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر / جامعة محمد بوضياف – المسيلة – 2018\05\09.

[2] ضحايا الجريمة الإلكترونية عبر مواقع التواصل – الفايسبوك أنموذجا – مجلة دراسات في سيكولوجية الانحراف, سلامي لخضر المجلد 6، العدد 1، الصفحات 186-213. 2021-06-30.

**أولا: رصد البيانات الرقمية:**

تستخدم اليوروبول أدوات متطورة لرصد تيارات البيانات الرقمية، بما في ذلك حركة الإنترنت وقنوات الاتصال والمعاملات عبر الإنترنت. يتيح ذلك لهم جمع معلومات استخباراتية حول التهديدات الإلكترونية المحتملة والأنشطة الإجرامية.

**ثانيا: تقنيات الذكاء الاصطناعي:**

تستفيد اليوروبول من قوة الذكاء الاصطناعي لتحليل كميات ضخمة من البيانات بسرعة ودقة. يمكن لخوارزميات الذكاء الاصطناعي اكتشاف الأنماط والشواذ والاتجاهات في البيانات، مما يساعد المحققين على اكتشاف تكتيكات جديدة لجرائم الإنترنت وتحديد التهديدات المحتملة.[1]

**ثالثا: التعرف على الأنماط:**

من خلال تطبيق خوارزميات التعلم الآلي، يمكن لليوروبول تحديد الأنماط في سلوك المجرمين الإلكترونيين، مثل نماذج الهجوم الشائعة وتوقيعات البرامج الضارة أو أنماط الاحتيال. يتيح لهم ذلك التوقع والوقاية من هجمات الإنترنت المستقبلية بشكل أكثر فعالية.[2]

**رابعا: تحديد الضحايا والمشتبه بهم:**

يتم استخدام تقنيات تحليل البيانات لتحديد الضحايا لجرائم الإنترنت والمشتبه بهم المحتملين. من خلال تحليل الأدلة الرقمية، يمكن لليوروبول تتبع مصادر الهجمات الإلكترونية، وتحديد الجناة، وتقديم الدعم للضحايا.

---

[1] استخدام تقنيات الرصد والتحليل والتنبؤ – توظيف الذكاء الاصطناعي للحدِّ من التطرف والإرهاب – د.عمران عوان خبير محاربة الإرهاب وأستاذ علم الجريمة في جامعة برمنجهام، المملكة المتحدة 2024/03/28

[2] أحمد عنتر، تقنيات الأمن السيبراني والتحديات المستقبلية، 2023/12/4 – تقنيات الأمن السيبراني والتحديات المستقبلية | تكنولوجيا | الجزيرة نت ((aljazeera.net

**خامسا: دعم التحقيقات:**

تقدم اليوروبول الدعم التحليلي لوكالات إنفاذ القانون خلال التحقيقات في جرائم الإنترنت. يساعد تحليل البيانات المحققين على جمع الأدلة، وتأسيس الصلات بين الحالات المختلفة، وبناء قضايا قانونية أقوى ضد المجرمين الإلكترونيين.

**سادسا: تعزيز الإجراءات القانونية:**

يسهل تحليل البيانات جمع المعلومات الاستخباراتية القابلة للتنفيذ، مما يعزز قدرة وكالات إنفاذ القانون على اتخاذ إجراءات قانونية ضد المجرمين الإلكترونيين. تتعاون اليوروبول مع السلطات الوطنية والدولية لمكافحة جرائم الإنترنت بفعالية.

بشكل عام، تعزز استخدام اليوروبول لأساليب تحليل البيانات المتقدمة، بما في ذلك تقنيات الذكاء الاصطناعي، قدراتها في مكافحة التهديدات الإلكترونية وحماية النظم الرقمية. تلعب هذه الأساليب دورًا حاسمًا في تحديد ومنع ومحاسبة أنشطة جرائم الإنترنت عبر الحدود.

**المطلب الثاني: مدى فعالية آليات اليوروبول في الحد من الجرائم الإلكترونية**

آليات اليوروبول قد أظهرت فعالية كبيرة في الحد من الجرائم الإلكترونية. يعمل المركز الأوروبي لمكافحة الجريمة الإلكترونية (3EC)، الذي أنشأته اليوروبول، على تقديم الدعم التشغيلي والاستراتيجي والتحليلي والجنائي لتحقيقات الدول الأعضاء في مجال مكافحة الجرائم الإلكترونية. كما يركز المركز على أنواع معينة من الجرائم الإلكترونية مثل الجرائم التي تعتمد على التكنولوجيا، استغلال الأطفال جنسياً، والاحتيال في الدفع. بالإضافة إلى ذلك، يقدم المركز دعمًا لمكافحة الجريمة على الويب العميق والمنصات البديلة

**الفرع الأول: الآليات الدولية لتبادل المعلومات و التعاون القضائي**

بناءً على المصادر المقدمة، الآليات الدولية لتبادل المعلومات والتعاون القضائي لمكافحة الجريمة الإلكترونية تعتبر جزءًا أساسيًا من الجهود العالمية لمكافحة الجريمة المنظمة. تشمل هذه الآليات تبادل المعلومات بين الدول،[1] تنسيق التدابير الإدارية وغير الإدارية للكشف المبكر عن الجرائم، وتسهيل تسليم المجرمين عبر الحدود. كما تركز على تطوير نظم تبادل المعلومات لمحاربة الجريمة الإلكترونية على مستوى عالمي، وتعزيز التعاون القضائي لتعقب ومحاكمة المشتبه بهم وتنفيذ العقوبات.

تعتمد التعاون الدولي على وجود قوانين وطنية منسقة لمكافحة الجريمة الإلكترونية، تُجرم الأنشطة الإلكترونية غير القانونية، بالإضافة إلى وجود إجراءات قضائية وطنية تحدد قواعد الإثبات والإجراءات الجنائية. يُعتبر التنسيق بين الأطر القانونية وحقوق الإنسان جزءًا أساسيًا من تسهيل التعاون الدولي. بالإضافة إلى ذلك، يمكن أيضًا الاعتماد على الصكوك الثنائية والإقليمية والمتعددة الأطراف لمكافحة الجريمة الإلكترونية، حيث قد تدعو بعض الظروف إلى الانضمام إليها. تعمل الأمم المتحدة على وضع سياسات فعّالة في مجال منع الجريمة وتحقيق العدالة الجنائية، من خلال إقرار التوصيات وإنشاء اللجان المتخصصة. كما تنظم الأمم المتحدة مؤتمرات دورية لتعزيز التبادل المعرفي والخبرات بين الخبراء من مختلف الدول لتعزيز التعاون الدولي في مجال مكافحة الجريمة.[2]

[1] جامعة منيسوتا – مكتبة حقوق الإنسان – اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية*اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 25 الدورة الخامسة والخمسون المؤرخ في 15 تشرين الثاني/نوفمبر 2000

[2] الطاهر ياكر مكافحة الجرائم االلكترونية بين التشريعات الوطنية واالتفاقيات الدولية. الطاهر ياكر كلية الحقوق والعلوم السياسية جامعة الجيالللي بونعامة، خميس مليانة )الجزائر. 30/12/2022

الآليات الدولية لتبادل المعلومات والتعاون القضائي لمكافحة الجريمة الإلكترونية تعتبر جزءًا أساسيًا من الجهود العالمية لمكافحة الجريمة المنظمة. تشمل هذه الآليات:

**أولا: تبادل المعلومات بين الدول:**

يتم تبادل المعلومات ذات الصلة بالجرائم الإلكترونية بين الدول، سواء كانت معلومات استخباراتية أو أدلة جنائية، لتمكين السلطات القضائية من التحقيق والملاحقة الفعالة للمشتبه بهم.[1]

**ثانيا: تنسيق التدابير الإدارية وغير الإدارية:**

تتضمن هذه التدابير تنسيق الجهود بين الدول للكشف المبكر عن الجرائم الإلكترونية واتخاذ التدابير الوقائية لمنعها، بما في ذلك التحقيق في التهديدات الإلكترونية المحتملة وتبادل الخبرات والممارسات الجيدة.[2]

**ثالثا: تسهيل تسليم المجرمين عبر الحدود:**

تسهيل تسليم المجرمين عبر الحدود يعتبر جزءًا أساسيًا من الجهود الدولية لمكافحة الجريمة الإلكترونية. يشجع التعاون الدولي على تبادل المعلومات والتعاون القضائي لتيسير تسليم المجرمين بين الدول. هذا يشمل التدريب والمساعدة التقنية لتيسير عمليات التسليم والمساعدة القانونية المتبادلة بين الدول الأطراف.[3]

---

[1] قزران مصطفى . زرقين عبد القادر ،الاليات الدولية لمكافحة الجريمة الالكترونية. مجلة صوت القانون– المجلد: 8– العدد: 4، الصفحة: 1222–1244 – السنة: 2022–06–16

[2] الطاهر ياكر. نفس المرجع السابق

[3] ليندة شرا بشة السياسة الدولية و الإقليمية في مجال مكافحة الجريمة الالكترونية.الاتجاهات الدولية في مكافحة الجريمة الالكترونية. المركز الجامعي سوق أهراس

تعتبر هذه الآليات وسيلة فعالة لتعزيز التعاون الدولي في مكافحة الجريمة الإلكترونية وضمان تقديم المجرمين للعدالة بالإضافة إلى ذلك، تركز هذه الآليات على:

تطوير نظم تبادل المعلومات لمحاربة الجريمة الإلكترونية على مستوى عالمي: من خلال تحسين وتطوير الأنظمة والمنصات الدولية لتبادل المعلومات، يتم تعزيز القدرة على التصدي للتهديدات الإلكترونية عبر الحدود.

**رابعا: تعزيز التعاون القضائي:**

يتم تعزيز التعاون القضائي بين الدول لتبادل المعلومات القانونية وتقديم المساعدة القانونية المتبادلة في التحقيقات والمحاكمات المتعلقة بالجرائم الإلكترونية. هذا التعاون يهدف إلى تعزيز الجهود الدولية في مكافحة الجريمة الإلكترونية من خلال تسهيل تبادل المعلومات القانونية الضرورية للتحقيقات والمحاكمات، وتوفير الدعم القانوني المتبادل بين الدول لضمان تقديم المجرمين للعدالة وتحقيق العدالة في قضايا الجرائم الإلكترونية.[1]

تلك هي بعض التفاصيل حول الآليات الدولية لتبادل المعلومات والتعاون القضائي لمكافحة الجريمة الإلكترونية، والتي تلعب دورًا أساسيًا في جهود مكافحة الجريمة على مستوى عالمي.

**الفرع الثاني: التعاون المحلي بين الجهات التنفيذية بين اليوروبول و الجهات المتخصصة**

إن التعاون المحلي بين الهيئات التنفيذية ليوروبول والوكالات المتخصصة هو جانب أساسي في مكافحة الجريمة الدولية. يشمل هذا التعاون تعزيز مشاركة المعلومات وتقديم المساعدة القانونية وتنسيق العمليات بين يوروبول والكيانات المتخصصة لمواجهة الأنشطة الإجرامية عبر الحدود. تهدف الشراكة إلى تعزيز جهود إنفاذ القانون، وتسهيل التحقيقات المشتركة، وضمان استجابة منسقة لمختلف التهديدات الأمنية. يلعب التعاون بين يوروبول والوكالات المتخصصة

[1] هند نجيب، التعاون القضائي الدولي في مجال الجرائم الالكترونية، دون سنة النشر.

دورًا هامًا في مكافحة الجريمة الدولية من خلال استغلال الخبرات والموارد ومشاركة المعلومات لتعزيز التدابير الأمنية ومكافحة الشبكات الإجرامية بفعالية.[1]

**أولا: تعزيز مشاركة المعلومات:**

يتضمن هذا التعاون تبادل المعلومات الاستخباراتية والمعلومات الجنائية الحساسة بين يوروبول والوكالات المتخصصة، مما يسهم في فهم أفضل لأنماط الجريمة والشبكات الإجرامية العابرة للحدود.[2]

**ثانيا: تقديم المساعدة القانونية:**

يتعاون يوروبول مع الوكالات المختصة في تقديم المساعدة القانونية المتبادلة، مثل تسليم المشتبه بهم وتنفيذ الأوامر القضائية عبر الحدود، مما يعزز القدرة على محاكمة المتهمين بفعالية.[3]

**ثالثا: تنسيق العمليات:**

يسعى يوروبول والوكالات المتخصصة إلى تنسيق العمليات المشتركة لمكافحة الجريمة الدولية، مما يسهم في تحقيق نتائج أفضل وتوجيه الجهود بشكل أكثر فعالية.[4]

---

[1] أمن دولي . التعاون ما بين الاتحاد الأوروبي والناتو.. القدرات والتحديات فبراير 26, 2023

[2] نفس المرجع السابق

[3] هند نجيب، نفس المرجع السابق.

[4] مجلة الشرق الأوسط، أمين عام مجلس التعاون يجري مباحثات مع «اليوروبول» لمكافحة الجريمة الدولية، 26 أغسطس 2015 م أمين عام مجلس التعاون يجري مباحثات مع «اليوروبول» لمكافحة الجريمة الدولية ((aawsat.com

**رابعا: تطوير السياسات والإستراتيجيات:**

يعمل الجهاز التنفيذي ليوروبول والوكالات المتخصصة على تطوير السياسات والإستراتيجيات المشتركة لمواجهة التحديات الجديدة في مجال مكافحة الجريمة الدولية.[1]

**خامسا: تبادل التدريب والخبرات:**

يتيح التعاون المحلي فرص التبادل في التدريب والخبرات بين يوروبول والوكالات المتخصصة، مما يعزز القدرات والمهارات في مجال مكافحة الجريمة.[2]

يتضح أن التعاون المحلي بين يوروبول والوكالات المتخصصة يعد عنصراً أساسياً في جهود مكافحة الجريمة الدولية. من خلال تبادل المعلومات، وتقديم المساعدة القانونية، وتنسيق العمليات، يتم تعزيز قدرة الأجهزة الأمنية على التصدي لأنشطة الجريمة عبر الحدود بشكل فعال. وبفضل تطوير السياسات والإستراتيجيات المشتركة، وتبادل التدريب والخبرات، يتم تعزيز القدرات والمهارات اللازمة لتحقيق نتائج أفضل في هذا المجال. بالتالي، يعزز هذا التعاون المشترك بين يوروبول والوكالات المختصة الأمن والاستقرار على الصعيدين الوطني والدولي.

[1] نفس المرجع السابق

[2] أمن دولي . التعاون ما بين الاتحاد الأوروبي والناتو.. القدرات والتحديات فبراير 26, 2023 ملف: أمن دولي . التعاون ما بين الاتحاد الأوروبي والناتو.. القدرات والتحديات – ((europarabct.com

## المبحث الثاني: التحديات التي تواجه آليات مكافحة الجرائم الإلكترونية

تواجه مكافحة الجريمة السيبرانية تحديات فنية وقانونية متعددة. من بين التحديات الفنية، نجد نقص البنية التحتية لتكنولوجيا المعلومات في أجهزة وبرامج القضاء والشرطة، مما يؤثر سلباً على جودة التحقيقات. بالإضافة إلى ذلك، يعتبر التمويه على الإنترنت واحدًا من التحديات الرئيسية، حيث يجعل الهوية المجهولة صعبة تتبع وتحديد هوية المجرمين. كما يشكل الويب المظلم والتجارة غير القانونية تحديًا آخر، حيث يتم نقل الجرائم البشعة من العالم الفعلي إلى العالم السيبراني. فيما يتعلق بالتحديات القانونية، يشمل ذلك مسألة تحديد الاختصاص في الجرائم السيبرانية وعدم وجود تشريعات كافية لتغطية أشكال الجريمة الجديدة. بالإضافة إلى ذلك، هناك صعوبة في مشاركة المعلومات والتعاون الدولي في جمع الأدلة، حيث لا توجد ترتيبات قانونية محددة لتوطين البيانات التي يتم إنشاؤها، مما يجعل من الصعب على وكالات إنفاذ القانون الحصول على المعلومات من البلدان الأجنبية.[1]

### المطلب الأول: مدى استجابة آليات اليوروبول للتحديات الأمنية المستقبلية

تستجيب "يوروبول" بنشاط للتحديات المستقبلية في مكافحة الجريمة الإلكترونية من خلال مبادرات مختلفة. تؤكد الوكالة أهمية تطوير حلول تنظيمية مبتكرة لتعزيز التحقيق في جرائم الإنترنت واستغلال الأدلة الرقمية بشكل فعال. تشمل جهود "يوروبول" ما يلي:

#### أولا. تعزيز التعاون الدولي:

تعمل "يوروبول" بشكل وثيق مع مسؤولي إنفاذ القانون من عدة دول ومؤسسات أساسية في الاتحاد الأوروبي لتبادل المعلومات ومواجهة التهديدات الإلكترونية على الصعيدين الوطني والدولي.[2]

---

[1] بالسينج خاندوسينغ راجبوت، تحديد التحديات التي تواجه نظام العدالة الجنائية أثناء التعامل مع الجريمة الاقتصادية السيبرانية. معهد تاتا للعلوم الاجتماعية، مارس 2018

[2] مؤتمر الجرائم الإلكترونية المشترك بين "يوروبول" و"الانتربول" لعام 2021، الذي عُقد في 11 نوفمبر 2021

**ثانيا. الاستثمار في القدرات التكنولوجية:**

تركز "يوروبول" على تطوير أدوات تكنولوجية متقدمة لمواكبة الجناة الإلكترونيين وتحسين التقنيات التحقيقية، مثل فك تشفير الأدلة واستخدام حلول مبتكرة في إنفاذ القانون.[1]

**ثالثا. بناء القدرات العمالية:**

تعتبر الوكالة التدريب وبناء القدرات للموظفين في إنفاذ القانون من أولوياتها لتزويدهم بالمهارات اللازمة لمكافحة جرائم الإنترنت بفعالية على الصعيدين الوطني والدولي.[2]

**رابعا. تعزيز الوعي والوقاية:**

يشارك "يوروبول" في زيادة الوعي حول التهديدات الإلكترونية وتعزيز أفضل الممارسات الأمنية للحد من المخاطر. كما تؤكد على أهمية التعاون والشراكة في الاستجابة للتهديدات الإلكترونية على الصعيد العالمي.[3]

من خلال التركيز على هذه المجالات الرئيسية، تهدف "يوروبول" إلى تعزيز قدرات الاتحاد الأوروبي في مكافحة الجريمة الإلكترونية وحماية المواطنين والمصالح الأوروبية من التهديدات الإلكترونية المتطورة.

**الفرع الأول: التطورات المتوقعة في مجال الجريمة الإلكترونية**

من المتوقع أن تستمر التطورات في مجال الجريمة الإلكترونية بسرعة متزايدة، حيث يتبنى المجرمون تقنيات جديدة ومتطورة لتنفيذ جرائمهم عبر الإنترنت. هنا بعض التطورات المتوقعة:

[1] تقدم تقرير يوروبول نظرة عن اتجاهات الجريمة الإلكترونية. تاريخ النشر: أكتوبر 2023.

[2] معلومات عامة عن يوروبول، إطار الكفاءة لتدريب مكافحة الجرائم الإلكتروني، 2024/01/09

[3] تقدم تقرير يوروبول نظرة عن اتجاهات الجريمة الإلكترونية. تاريخ النشر: أكتوبر 2023

- تطور أنماط الجرائم: تظهر أنماط جديدة من الجرائم الإلكترونية مع تقدم تقنية الميتافيرس، مما يفتح المجال لظهور تهديدات جديدة وتحديات متنامية في مجال مكافحة الجريمة الإلكترونية.[1]

- أهمية الأدلة الرقمية: تعتبر الأدلة الرقمية أحد أبرز تطورات العصر الحديث في النظم القانونية، حيث تصبح ضرورية لإثبات الجرائم المعلوماتية التي قد تكون صعبة الإثبات دونها.[2]

- زيادة الجرائم الإلكترونية: من المتوقع زيادة حجم الجرائم الإلكترونية عالميًا، خاصة مع تطور التقنيات الجديدة مثل إنترنت الأشياء، مما يفرض ضرورة التأهب والتكيف مع أنواع جديدة من الجرائم.

- تحديث التشريعات: تشير التقارير إلى أهمية تحديث التشريعات المتعلقة بالجرائم الإلكترونية لمواكبة التطورات التكنولوجية وتغير أنماط الجرائم، مما يساهم في تعزيز القدرة على مكافحة الجرائم الإلكترونية بفعالية.[3]

بالاستناد إلى هذه المعلومات، يمكن القول إن التطورات المتوقعة في مجال الجريمة الإلكترونية تشمل تطور أنماط الجرائم، أهمية الأدلة الرقمية، زيادة الجرائم الإلكترونية، وضرورة تحديث التشريعات لمواكبة التحديات الناشئة في هذا المجال.

---

[1] عبير نيازي وجيد فتح الله، العوامل المؤدية للجرائم الالكترونية وأدوار الاخصائي الاجتماعي للتعامل معها من منظور الممارسة العامة في الخدمة الاجتماعية، المقالة 1، المجلد 61، العدد 3، يناير 2023، الصفحة 605-646، قسم مجالات الخدمة الاجتماعية – كلية الخدمة الاجتماعية – جامعة حلوان ( القاهرة)

[2] علاء رضوان، أخطر الجرائم المستحدثة.. قيمة الأدلة الرقمية فى الإثبات الجنائى.. المشرع وضع المادة 11 من قانون الجرائم الالكترونية لسد ثغرة الدليل.. وللقاضي حرية الأخذ بمبدأ الإثبات الجنائى من عدمه.. والنقض تتصدى للأزمة الأربعاء، 19 أغسطس 2020

[3] خالد محمود محمد مهران، الإجراءات التى تتخذها الدول فى مواجهة مخاطر الاستخدام غير المشروع للفضاء الإلكتروني، المجلد 14، العدد 6 ،نوفمبر 2022 ، الصفحة 1811-1848

## الفرع الثاني: استراتيجيات مستقبلية لتحسين فعالية مكافحة الجريمة الإلكترونية

بناءً على التطورات المتوقعة في مجال الجريمة الإلكترونية والتحديات الناشئة، هناك عدة استراتيجيات مستقبلية يمكن اتباعها لتحسين فعالية مكافحة هذه الجرائم:

### أولا: تطوير القدرات التقنية والبشرية

الاستثمار في تطوير أدوات التحليل والتحقيق الرقمي المتطورة لمواكبة التطورات التكنولوجية و تعزيز قدرات موظفي إنفاذ القانون من خلال التدريب المتخصص والدعم الفني لبناء مهارات التعامل مع الأدلة الرقمية.[1]

### ثانيا: تعزيز التعاون الدولي والشراكات

تعزيز التعاون بين الدول والمنظمات الدولية لتبادل المعلومات والخبرات في مكافحة الجريمة الإلكترونية عبر الحدود و إنشاء شراكات مع القطاع الخاص والمجتمع المدني لتعزيز الوعي وتبادل المعلومات الاستخبارية.[2]

### ثالثا: تحديث التشريعات والأطر القانونية المتعلقة بمكافحة الجريمة الإلكترونية

1. مراجعة وتحديث التشريعات المتعلقة بالجرائم الإلكترونية لمواكبة التطورات التكنولوجية وأنماط الجرائم الجديدة[3]

2. تعزيز الأطر القانونية لتنظيم الأدلة الرقمية وقبولها كأدلة إثبات في المحاكم

---

[1] أميرة محمد محمد سيد أحمد، استراتيجيات مكافحة الجرائم الإلكترونية في العصر المعلوماتي تعزيزًا لرؤية مصر 2030: دراسة استشرافية، أستاذ الصحافة المساعد– كلية الآداب– جامعة دمياط. المجلد 58، العدد 4 – الرقم المسلسل للعدد 4، يوليو 2021, الصفحة 1765–1808

[2] ناشف فريد، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 8، العدد 1، الصفحات 430–450 3 – يونيو 2022

[3] جيتندر كيه مالك*، الدكتور سانجايا تشودهوري، مراجعة موجزة حول جريمة الإنترنت – النمو والتطور، باحث مشارك، قسم القانون، جامعة باغوانت، أجمير (راجستان)، الهند، بدون تاريخ نشر.

**رابعا: التركيز على الوقاية والتوعية**

1. زيادة الوعي العام بمخاطر الجريمة الإلكترونية وتشجيع الممارسات الأمنية الجيدة

2. تطوير برامج توعوية موجهة للفئات المستهدفة كالشباب والأطفال لتعزيز السلوكيات الآمنة عبر الإنترنت[1]

من خلال تبني هذه الاستراتيجيات المتكاملة والتركيز على التطوير التقني والبشري، وتعزيز التعاون والشراكات، وتحديث الأطر القانونية، والتركيز على الوقاية والتوعية، يمكن تحسين فعالية مكافحة الجريمة الإلكترونية في المستقبل.

**المطلب الثاني: التوجهات المستقبلية لتعزيز دور اليوروبول في مكافحة الجريمة الإلكترونية**

تحديات جرائم الإنترنت تتطور بسرعة مع التقنيات الجديدة مثل الإنترنت من الأشياء، والطائرات بدون طيار، والروبوتات، والسيارات ذاتية القيادة. يجب على يوروبول أن تبقى على اطلاع دائم على هذه التطورات لتحديد ومعالجة اتجاهات جرائم الإنترنت الجديدة بفعالية. ومن ثم، تحديد كيفية تأثير التدابير القانونية والأمنية على تلك الجرائم يمكن أن يوجه استراتيجيات يوروبول لمواجهة التهديدات الإلكترونية المتطورة بشكل أفضل. التعاون الدولي أيضًا يلعب دورًا حيويًا في هذا المجال؛ إذ يمكن للتعاون مع الجهات الإنفاذية والأمنية الإقليمية والدولية مثل الإنتربول توفير رؤى وموارد قيمة لمواجهة الجريمة الإلكترونية على مستوى عالمي. بالإضافة إلى ذلك، يجب أن تستثمر الجهات الإنفاذية، بما في ذلك يوروبول، في تطوير حلول تطبيقية مبتكرة وتعزيز مهارات موظفيها لمواجهة الجريمة الرقمية بشكل فعال. ولتحقيق هذه الأهداف، من المهم أيضًا إنشاء آليات فعالة للتعاون والتوجيه الاستراتيجي، بما في ذلك من خلال برامج مثل مجلس برنامج مركز الجريمة الإلكترونية الأوروبي. التعاون مع القطاع الخاص والمجموعات الاستشارية يمكن أن يوفر رؤى قيمة ودعمًا في مواجهة الجريمة الإلكترونية. من خلال دمج هذه التوجهات

[1] أميرة محمد محمد سيد أحمد، مرجع سابق

في استراتيجياتها، يمكن ليوروبول تعزيز دورها في مكافحة الجريمة الإلكترونية ومواجهة التهديدات الإلكترونية المتطورة بفعالية.[1]

**الفرع الأول: تطوير الشراكات الدولية والمحلية**

لتعزيز دور اليوروبول في مكافحة الجريمة الإلكترونية، تركز الوكالة على تطوير شراكات دولية ومحلية قوية في عدة مجالات:

**أولا. التعاون الدولي**

1.يتعاون يوروبول مع شركاء دوليين مثل شبكة منع المجرمين الإلكترونيين الدولية (InterCOP) لتبادل المعلومات والخبرات في مكافحة الجريمة الإلكترونية على الصعيد العالمي.

2.تعزيز التعاون مع وكالات إنفاذ القانون في الدول الأعضاء في الاتحاد الأوروبي لتبادل المعلومات والخبرات.[2]

3.إنشاء شراكات مع منظمات دولية أخرى مثل الإنتربول لمكافحة الجريمة الإلكترونية عبر الحدود.

**ثانيا. الشراكات مع القطاع الخاص**

- إقامة شراكات مع شركات التكنولوجيا والاتصالات لتبادل المعلومات الاستخبارية وتطوير حلول أمنية مبتكرة.[3]

---

[1] مؤتمر الجريمة الإلكترونية المشترك بين يوروبول والإنتربول لعام 2021 هو "الابتكار للتغلب على تسارع جريمة الإنترنت" في 11 نوفمبر 2021

[2] علاء رضوان، عن أخطر الجرائم المستحدثة.. قيمة الأدلة الرقمية فى الإثبات الجنائى.. المشرع وضع المادة 11 من قانون الجرائم الالكترونية لسد ثغرة الدليل.. وللقاضي حرية الأخذ بمبدأ الإثبات الجنائى من عدمه.. والنقض تتصدى للأزمة، الأربعاء، 19 أغسطس 2020.

[3] علاء رضوان، مرجع سابق.

- التعاون مع مزودي خدمات الإنترنت والمنصات الرقمية لمكافحة المحتوى الإرهابي والإجرامي عبر الإنترنت.

**ثالثا . التعاون مع المجتمع المدني**[1]

1.إنشاء شراكات مع منظمات المجتمع المدني لزيادة الوعي العام بمخاطر الجريمة الإلكترونية وتشجيع الممارسات الأمنية الجيدة.

2.التعاون مع مراكز البحوث والجامعات لتطوير قدرات البحث والتحليل في مجال الجريمة الإلكترونية.

**رابعا. فرق العمل ضد الجريمة الإلكترونية**

تعمل فرق العمل المشتركة للعمل ضد الجريمة الإلكترونية (J-CAT) التابعة ليوروبول كمنصة للشراكات والتعاون لمكافحة الجريمة الإلكترونية بفعالية على الصعيدين الدولي والمحلي. من خلال تعزيز هذه الشراكات الدولية والمحلية[2]، تهدف يوروبول إلى تعزيز قدراتها في مكافحة الجريمة الإلكترونية، وتعزيز تبادل المعلومات، وتطوير حلول مبتكرة، ومواجهة التهديدات الإلكترونية بشكل جماعي على الصعيد العالمي.

من خلال تطوير هذه الشراكات على المستويين الدولي والمحلي، تسعى اليوروبول إلى تعزيز قدراتها في مكافحة الجريمة الإلكترونية بشكل فعال وشامل. يساهم التعاون مع الجهات المعنية المختلفة في تبادل المعلومات والخبرات وتطوير حلول مبتكرة لمواجهة التهديدات الإلكترونية المتطورة.

[1] يوروبول، وكالة إنفاذ القانون في الاتحاد الأوروبي، تقارير حول اتجاهات جرائم الإنترنت.04 أكتوبر 2023

[2] فرقة العمل المشتركة لمكافحة الجرائم الإلكترونية (J-CAT) مكافحة الجرائم الإلكترونية حول العالم، Joint Cybercrime Action Taskforce (J-CAT) | Europol (europa.eu)

**الفرع الثاني: التوعية و تعزيز الوعي في مكافحة الجريمة الالكترونية**

لا يمكن تأجيل الحاجة إلى تثقيف مستخدمي الإنترنت حول كيفية الاستفادة المثلى من التكنولوجيا. مكافحة الجريمة الإلكترونية ليست من مسؤولية سلطات إنفاذ القانون وحدها. يجب التفكير في برامج توعية مناسبة ومنظمة جيدًا لمستخدمي الإنترنت.

تذكر "الأجندة الرقمية لأوروبا" الصادرة عن الاتحاد الأوروبي في عام 2010:

تعاني أوروبا من نقص متزايد في مهارات تكنولوجيا المعلومات والاتصالات المهنية وعجز في محو الأمية الرقمية. هذه الفجوات تحرم العديد من المواطنين من المجتمع الرقمي والاقتصاد الرقمي وتعيق التأثير الكبير لتبني تكنولوجيا المعلومات والاتصالات على نمو الإنتاجية. يتطلب هذا رد فعل منسق، بمشاركة الدول الأعضاء وأصحاب المصلحة الآخرين في المركز.[1]

يجب على الحكومات الوطنية إطلاق حملات توعية لمساعدة الناس على حماية أنفسهم من الجرائم الإلكترونية. يمكن للاحتياطات الأمنية البسيطة، خاصة بين الشباب، أن تقلل بشكل كبير من الجرائم الإلكترونية. التوعية من خلال حملات إعلامية مستمرة، إعلانات تلفزيونية ومواقع إلكترونية مخصصة هي إحدى الخيارات لتحقيق هذا الهدف. في النهاية، يمكن أن تؤدي المعلومات العامة الأفضل حول سلامة الكمبيوتر إلى إنقاذ أعداد كبيرة من الناس من متاعب سرقة بياناتهم ومن أن يصبحوا ضحايا مباشرة للجريمة الإلكترونية (كما هو الحال في استغلال الأطفال جنسياً). وجد مقياس الأمن السيبراني الخاص لعام 2012 أن 74% من مواطني الاتحاد الأوروبي يعتقدون أن خطر أن يصبحوا ضحايا للجريمة الإلكترونية قد زاد في السنوات الأخيرة.

[1] بروكسل، 19 مايو 2010 COM(2010)245 اتصال من المفوضية إلى البرلمان الأوروبي،المجلس، اللجنة الاقتصادية والاجتماعية الأوروبية،ولجنة المناطق، أجندة رقمية لأوروبا، EN (europa.eu)

كما أن الغالبية العظمى من مستخدمي الإنترنت يتجنبون الكشف عن المعلومات الشخصية عبر الإنترنت(89%).[1]

بالانتقال الآن من التوعية العامة إلى الوعي المحدد بالجريمة الإلكترونية بين الممارسين القانونيين في الاتحاد الأوروبي، يبدو أن اكتساب المهارات المناسبة للتعامل مع الجرائم المتعلقة بالإنترنت في الإجراءات الجنائية أمر ضروري. في أعقاب برنامج لاهاي في نوفمبر 2004[2] وخطة العمل التابعة له[3]، أولى برنامج ستوكهولم 2010–2014 أهمية كبيرة للتدريب. ذكرت الفقرة 1.2.6 من البرنامج: من أجل تعزيز ثقافة قضائية وإنفاذ قانون حقيقية في الاتحاد الأوروبي، من الضروري تعزيز التدريب على القضايا المتعلقة بالاتحاد الأوروبي وجعلها متاحة بشكل منهجي لجميع المهن المشاركة في تنفيذ منطقة الحرية والأمن والعدالة. يشمل ذلك القضاة والمدعين العامين والموظفين القضائيين وضباط الشرطة والجمارك وحرس الحدود.[4]

يمكن تقديم التدريب على الجريمة الإلكترونية على ثلاثة مستويات مختلفة:

(أ) الدورات التمهيدية: (تقديم المعرفة والفهم الأساسيين للجريمة الإلكترونية، المخاطر المرتبطة بتكنولوجيا المعلومات والاتصالات، اتجاهات الجريمة الإلكترونية، أنواع الجرائم الإلكترونية والأدوات الرئيسية المستخدمة، التحديات القانونية على المستوى الوطني والأوروبي والدولي).

[1] مقياس يوروبارومتر الخاص 390 "الأمن السيبراني"، المفوضية الأوروبية، المديرية العامة للاتصالات (يوليو 2012)، متاح على: http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf.

[2] استنتاجات الرئاسة – بروكسل، 4 و5 نوفمبر 2004

[3] التواصل من المفوضية إلى البرلمان الأوروبي – برنامج لاهاي: عشر أولويات للسنوات الخمس القادمة. الشراكة من أجل تجديد أوروبا في مجال الحرية والأمن والعدالة (COM (2005) 184 النهائي).

[4] 26برنامج ستوكهولم – أوروبا مفتوحة وآمنة تخدم وتحمي المواطنين، استنتاجات الرئاسة – بروكسل، 10–11 ديسمبر 2009 (مجلس الاتحاد الأوروبي، بروكسل 3 مارس 2010، الوثيقة 10/5731، الصفحة 16)

(ب) دورات المحققين المتقدمة:[1] (تحديد وتتبع الجرائم المتعلقة بالكمبيوتر، أدوات واستراتيجيات التحقيق، البحث والمصادرة، التحقيق الجنائي للحواسيب والأجهزة ذات الصلة، التحقيق والسيطرة على الجرائم الإلكترونية، الإشراف وإدارة القضايا التي تنطوي على الجريمة الإلكترونية) .

(ج) دورات المتخصصين في الطب الشرعي المتقدمة: (اكتساب صور جنائية وفقًا للمبادئ والمنهجيات المعترف بها، التعرف على المشكلات التقنية وحلها، منتجات الإجراءات التحليلية، أداء دور الخبير في التحقيقات وفي المحكمة).

يجب تقديم الدورات الأساسية للقضاة لتعريفهم بالمفاهيم الأساسية للجريمة الإلكترونية مثل "بوت نت"، "هجمات الحرمان من الخدمة" أو "DOS"، "التصيد" وغيرها[2]. بدون هذا الفهم الأساسي والوعي، قد تكون فرص نجاح حتى القضايا الإلكترونية التي تم التحقيق فيها وملاحقتها بشكل جيد معرضة للخطر في المحاكم. نظرًا للطبيعة الشاملة للجريمة الإلكترونية، بغض النظر عن تخصص القضاة والمدعين العامين (سواء كانت إجراءات في قطاع المال والبنوك، أو في مجال الاتصالات، أو مكافحة الجريمة المنظمة والإرهاب، أو استغلال الأطفال جنسيًا، إلخ)، من الضروري أن يكونوا مجهزين بفهم أساسي لظاهرة الجريمة الإلكترونية. من المهم بنفس القدر تنظيم دورات متقدمة بانتظام للمحققين الجنائيين والمحللين الشرعيين، الذين، بعد استيعاب القواعد الأساسية والمفاهيم الرئيسية، يحتاجون إلى تحديثات مستمرة حول الاتجاهات الحالية والتهديدات والمنهجيات والتقنيات في هذا المجال سريع النمو والتطور.

[1] بغدادي, أدهم باسم نمر، وسائل البحث والتحري عن الجرائم الإلكترونية، جامعة النجاح الوطنية، 2018-04-05

[2] فريق مجلة أمناي، ما هي شبكة البوتات Botnet وما علاقتها بهجمات DDoS؟ 29 نوفمبر 2022، ما هي شبكة البوتات Botnet وما علاقتها بهجمات DDoS؟(amnaymag.com)

**خلاصة الفصل:**

يعتبر اليوروبول (مكتب الشرطة الجنائية الأوروبي) جهة حيوية في مكافحة الجريمة الإلكترونية على المستوى الدولي، حيث يعمل كوكالة للتنسيق والتعاون بين الدول الأعضاء في الاتحاد الأوروبي وشركائها لمواجهة التهديدات الأمنية الإلكترونية. من خلال تبادل المعلومات والتحليلات الجنائية، يمكن لليوروبول تقديم دعم مهم للدول الأعضاء في تحديد ومكافحة الجرائم الإلكترونية المعقدة مثل الاحتيال الإلكتروني، والقرصنة، وغسل الأموال الرقمي، والهجمات السيبرانية. ومع استمرار تطور التكنولوجيا، يجب على اليوروبول البقاء حذرًا ومتطورًا في استراتيجياته لمواجهة التحديات المتزايدة، بتطوير آليات جديدة وتعزيز التعاون الدولي والمحلي. كما يجب تعزيز الوعي بين الجمهور حول خطورة الجريمة الإلكترونية وكيفية الحماية على الإنترنت، ويمكن لهذا التعاون الدولي أن يسهم بشكل كبير في جعل الإنترنت بيئة أكثر أمانًا للمستخدمين في جميع أنحاء العالم.

# الخاتمـــة

اليوروبول، كونه المكتب الأوروبي للشرطة، فهو يلعب دوراً بارزاً في التصدي للجريمة الإلكترونية تشكل الجريمة الإلكترونية تحدياً متزايداً يتطلب استجابة فعالة ومنسقة من قبل الهيئات المسؤولة عن إنفاذ القانون، وعلى رأسها يوروبول. من خلال هذه الدراسة، استعرضنا دور يوروبول في مكافحة الجريمة الإلكترونية من خلال تحليل شامل لهيكليتها وآليات عملها، وتقييم فعالية هذه الآليات في الحد من الجرائم الإلكترونية، كما تطرقنا إلى الأنواع المختلفة للجرائم الإلكترونية وتأثيراتها السلبية على المجتمع والاقتصاد، مع التركيز على الاحتيال المصرفي وانتهاك الخصوصية.

أظهرت دراستنا أن تبادل المعلومات والتحليلات الجنائية يلعب دوراً محورياً في مكافحة الجريمة الإلكترونية، حيث يسهم في تحسين قدرة يوروبول على تتبع الأنشطة الإجرامية وتقديم الدعم اللازم للجهات التنفيذية على المستويات المحلية والدولية. كما ألقينا الضوء على التحديات التي تواجهها يوروبول في هذا السياق، بما في ذلك التهديدات المتطورة بسرعة والحاجة إلى استراتيجيات مبتكرة لمواجهتها.

كما حاولنا الإشارة أيضاً إلى أهمية التعاون الدولي والمحلي بين يوروبول والجهات المتخصصة، حيث يعتبر هذا التعاون أحد العناصر الأساسية لتعزيز فعالية مكافحة الجريمة الإلكترونية. وفي هذا الإطار، يلعب التدريب والتوعية دوراً حاسماً في زيادة الوعي بمخاطر الجرائم الإلكترونية وتعزيز قدرات الأفراد والمؤسسات على التصدي لها.

ختاماً، يتعين على يوروبول تبني استراتيجيات مستقبلية تتضمن تطوير الشراكات الدولية والمحلية، وتعزيز التوعية والتثقيف، لمواجهة التحديات المتزايدة في مجال الجريمة الإلكترونية. من خلال هذه الجهود المستمرة والمتكاملة، يمكن ليوروبول تعزيز دورها كآلية أوروبية فعالة في مكافحة الجريمة الإلكترونية وحماية المجتمع من تأثيراتها السلبي.

- و من النتائج المتوصل إليها ان جهاز اليوروبول قام اليوروبول بعمل كبير في مكافحة الجريمة المنظمة عموما والجريمة الإلكترونية على وجه الخصوص سيما بينه وبين الأجهزة الأوروبية.
- تعدد الجرائم وتطورها السريع أدى إلى حدوث ثغرات في حصر ومعالجة كل الجرائم وبالتالي نقص مواكبة هذه الإجراءات لهذه الجرائم.
- تعد الجرائم الإلكترونية من الجرائم العابرة للحدود لذلك فمكافحتها تحتاج إلى تعاون مختلف الهيئات الوطنية والدولية لمكافحتها.
- رصد الإتحاد الأوروبي عبر جهاز اليوروبول إمكانيات كبيرة من أجل التقليل والحد من الجرائم الإلكترونية من خلال عدة برامج على مدار عشر سنوات
- يعد التدريب والتكوين والتوعية من أهم وسائل عمل جهاز اليوروبول وأكثرها فعالية رغم تعدّد وتشعّب هذه الجرائم.
- رغم كل هذه الجهود فإنّ القضاء على الجريمة الإلكترونية نهائيا أمر غير ممكن نظرا للكم الكبير من النشاطات وتطور وسائل التخفي الإلكتروني وعدم التوازن بين إمكانيات الدول في ما يخص التعاون و التنسيق الأمني .

و منه فيمكن إدراج الإقتراحات التالية بناءا على ما سبق و التي يمكن حصرها في :

تعزيز تبادل المعلومات والبيانات بين أجهزة الأمن.

- تعطيل الوحدات الدعائية لتنظيم داعش على الإنترنت.
- التحقيق السريع في حال وقوع عمليات إرهابية.
- تنسيق قائمة الإجراءات اللازمة لتشكيل اتحاد في مجال الأمن في أوروبا.
- تقاسم المعلومات في إطار نظام شبكة المعلومات.
- ضمان أمن المواطنين ومنشآت البنية التحتية الحيوية والأساسية لدول الاتحاد.
- تعزيز التعاون الدولي والإقليمي عن طريق إنشاء آليات مشتركة.
- تعزيز التكوين في مجال مكافحة الجريمة الإلكترونية.

- فتح تخصصات جامعية وهيكلية في مكافحة الجريمة الإلكترونية.
- تشديد الرقابة على الوسائل التكنولوجية مع الأخذ بعين الاعتبار الحريات الشخصية

# قائمة المصادر و المراجع

## أولا: الكتب:


1. خالد ممدوح ابراهيم، الجرائم المعلوماتية، ط2، دار الفكر الجامعي الإسكندرية، مصر، 2019، .
2. د. ليمى عبد المجيد ، التنظيم التشريعي والقانوني لإلعالم التقميدي واإللكتروني، 2 يونيو .2021
3. ضرغام جابر عموش آ مواش، جريمة التجسس المعلوماتي، المركز العربي، .2017
4. عبد الحميد احمد، جرائم الشبكة العنكبوتية وغسل الأموال في إطار المالحقة الألمنية والقضائية
5. الدولي، مكتبة الوفاء القانونية، الطبعة الأولى، الإسكندرية، .2018
6. هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النيضة العربية، القاهرة، 1992،
7. هند نجيب، التعاون القضائي الدولي في مجال الجرائم االلكترونية، دون سنة النشر.
8. عادل محمد فريد نائلة، جرائم الحاسب الآلي الاقتصادية، ط ،1 منشورات الحلبي الحقوقية، بيروت، لبنان، 2005، .


## ثانيا: الدراسات الأكاديمية:


9. د. بوضياف أسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر / جامعة محمد بوضياف – المسيلة – 09\05\2018.
10. دانيال ج. سولوف، الضعف الجديد: أمان البيانات والمعلومات الشخصية كلية القانون في جامعة جورج واشنطن : 9 أغسطس 2011.
11. عبد الصبور عبد القوي علي– الجريمة الإلكترونية والجهود الدولية للحد منها – ماجستير في القانون – كلية الحقوق – جامعة بني سويف .
12. صبرينة بن سعد، حراية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا الإعلام والاتصال، أطروحة دكتوراه، كلية الحقوق، جامعة باتنة ،2015 .
13. ليندة شرابشة السياسة الدولية و الإقليمية في مجال مكافحة الجريمة الالكترونية، الاتجاهات الدولية في مكافحة الجريمة الالكترونية. المركز الجامعي سوق أهراس.
14. هروال هبة نبيلة، جرائم الانترنت (دراسة مقارنة)، أطروحة دكتوراه، جامعة تلمسان، 2013/2014.
15. يوسف صغير، الجريمة المرتكبة عبر الأنترنت، رسالة لنيل شهادة الماجستير، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، الجزائر، 2013 .

## ثالثا: المقالات و المجلات العلمية:

16. ليت الدين صلاح حبيب، التجسس وأحكامه إبان النزاعات المسلحة الدولية، مجلة جامعة الانبار للعلوم القانونية والسياسية، المجلدة، العدد1 .

17. أبو ذر شأكر عبد، التجسس الالكتروني في ظل التشريع الأردفي، مجلة العلوم السياسية والقانون، مجاد+،العدد26، المركز الدمقراطي العربي– برلين، المانياء 2020.

18. استخدام تقنيات الرصد والتحليل والتنبؤ – توظيف الذكاء الاصطناعي للحدِّ من التطرف والإرهاب – د.عمران عوان خبير محاربة الإرهاب وأستاذ علم الجريمة في جامعة برمنجهام، المملكة المتحدة 2024/03/28.

19. إسراء يوسف هادي، أسامة احمد النعجي، جريمة التجسس الالكتروني في إطار مشروع قانون جرائم المعلوماتية العراقي لسنة 2011، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد10، العدد36، 2021.

20. افتتاح مركز الجريمة الإلكترونية الأوروبي (3EC) في 11 يناير" (بيان صحفي). المفوضية الأوروبية. 9 يناير 2013. مؤرشف من الأصل في 23 يونيو 2017. الوصول في 21 سبتمبر 2017.

21. ألفريدو نازي– المكتب الأوروبي للشرطة – الانتربول – مجلة القانون الجنائي الدولية المجلد 11 جانفي 2006.

22. ألفريدو نانزي ، الانتربول، حارس أوروبا، الجزيرة 2016/2/1.

23. أماني محمد شريف عبد السلام ، تصور مقترح لتنمية الوعي الأمني لدى طلاب جامعة أسيوط في ضوء خبرات بعض الدولية التربية – جامعة أسيوط،– المجلد الثامن والثلاثون– العدد الثانيِ عشر – ديسمبر 2022م

24. أمن الحوسبة السحابية: الأهداف والمجالات والمكونات وطرق تطبيقها ، كتابة : بكه، 24 أبريل 2024 أمن الحوسبة السحابية: الأهداف والمجالات والمكونات وطرق تطبيقها – بكه للتعليم ((bakkah.com

25. أمن المعلومات د. دلال صادق + د. حميد ناصر الفتال د. دلال صادق + د. حميد ناصر الفتال, دار اليازوري العلمية للنشر والتوزيع.

26. أمن المعلومات د. دلال صادق + د. حميد ناصر الفتال, دار اليازوري العلمية للنشر والتوزيع.

27. أميرة محمد سيد أحمد، استراتيجيات مكافحة الجرائم الإلكترونية في العصر المعلوماتي تعزيزًا لرؤية مصر 2030: دراسة استشرافية، أستاذ الصحافة المساعد– كلية الآداب– جامعة دمياط. المجلد 58، العدد 4 – الرقم المسلسل للعدد 4، يوليو 2021.

28. الانتربول وشرطة مكافحة الإرهاب الدولية: مكافحة الإرهاب في منظور عالمي – ماثيو دفليم ، 18 فبراير 2007.

29. الانتربول، وكالة إنفاذ القانون في الاتحاد الأوروبي، تقارير حول اتجاهات جرائم الإنترنت.04 أكتوبر 2023.

30. اوشن حنان، وادي عاد الدين، التجسس الالكتروني واليات مكافحته في التشريع الجزائي الجزائري، مجلة الحقوق والعلوم السياسية،العدد2 جامعة عباس لغرور خنشلة، 2014.

31. أولدريش بوري، دور الانتربول في مكافحة الإرهاب: معضلة البيضة والدجاجة.

32. برنامج ستوكهولم – أوروبا مفتوحة وآمنة تخدم وتحمي المواطنين، استنتاجات الرئاسة – بروكسل، 10–11 ديسمبر 2009 (مجلس الاتحاد الأوروبي، بروكسل 3 مارس 2010، الوثيقة 10/5731.

33. بغدادي, أدهم باسم نمر، وسائل البحث والتحري عن الجرائم الإلكترونية، جامعة النجاح الوطنية، 05-04-2018

34. بن جدو بن علية . درار عياش، الآثار الاقتصادية للجريمة الالكترونية، المجلد 5، العدد 1، الصفحات 558-577، 31 مارس 2022

35. جامعة منيسوتا – مكتبة حقوق الإنسان – اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية*اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 25 الدورة الخامسة والخمسون المؤرخ في 15 تشرين الثاني/نوفمبر 2000

36. جمال عبد الله، الآثار الاجتماعية والنفسية والمخاطر المجتمعية للتكنولوجيا الحديثة، جامعة زايد – أبو ظبي– الإمارات العربية المتحدة، المجلد 24، العدد 10، 2023.

37. جيتندر كيه مالك*، الدكتور سانجايا تشودهوري، مراجعة موجزة حول جريمة الإنترنت – النمو والتطور، باحث مشارك، قسم القانون، جامعة باغوانت، أجمير (راجستان)، الهند، بدون تاريخ نشر

38. حسن بن احمد الشهري، الأنظمة الالكترونية الرقمة المطورة لحفظ وحماية سرية المعلومات من التجسس، المجلة العربية للدراسات الأمنية والتدريب، امجلد28، العدد56، 2012.

39. خالد محمود محمد مهران، الإجراءات التي تتخذها الدول فى مواجهة مخاطر الاستخدام غير المشروع للفضاء الإلكتروني، المجلد 14، العدد 6 ،نوفمبر 2022.

40. خالد ممدوح ابراهيم، الجرائم المعلوماتية، ط،2 دار الفكر الجامعي الإسكندرية، مصر، ،2019 .

41. خالد ممدوح العزي جرائم املالية الإلكترونية /الجرائم المصرفية نموذجا، أعمال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس/ لبنان، يومي 24-11-2023.

42. د. كامل مطر ، الجريمة الإلكترونية ، 17 أبريل 2016.

43. د. ليلى عبد المجيد ، التنظيم التشريعي والقانوني للإعلام التقليدي والإلكتروني، 2 يونيو 2021.

44. داريل لونغ. هندسة أنظمة المعلومات عبر الويب. المجلد 36، العدد 3، مايو 2011.

45. الذهبى خدوجة، حق الخصوصية في مواجهة الاعتداءات الالكترونية،(دراسة مقارن)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد الأول، العدد الثامن، جامعة المسيلة، 2017.

46. سليم حميدائي، اختراق الخصوصي في العالم الرقمي: حدود الظاهرة ومطالب الحماية القانونية، مجلة البحوث في الحقوق والعلوم السياسية.

47. سوزان عدنان الأستاذ، انتهاك حرمة الحياة الخاصة عبر الانترنت، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية (دراسة مقارنة)، المجلد 29 لعدد 3، 2013.

48. شريقي الشريف، مدى احترام الحق في الخصوصية في الحسابات الالكترونية على الانترنت، مجلة القانون والمجتمع، المجاد4، العدد1،2019.

49. ضحايا الجريمة الإلكترونية عبر مواقع التواصل – الفاسبوك أنموذجا – مجلة دراسات في سيكولوجية الانحراف, سلامي لخضر المجلد 6، العدد 1، الصفحات 186-213. 2021-06-30.

50. ضرغام جابر علوش آ مواش، جريمة التجسس المعلوماتي، المركز العربي، 2017.

51. عادل يوسف عبد النبي الشكور، الجريمة المعلوماتية و أزمة الشرعية الجزائرية، كلية القانون، جامعة الكوفة، العدد 7 ،2008.

52. عائشة لخشين، جامعة الأمير عبد القادر، الجزائر، حماية الحق في الخصوصية في العصر الرقمي في المواثيق الدولية، مقال منشور في مجلة جيل حقوق الانسان العدد 39.

53. عبد الحكيم موالي ابراهيم، الجرائم الإلكترونية، مجلة الحقوق و العلوم الإنسانية، جامعة زيان عاشور، الجلفة، الجزائر، المجلد الثاني، العدد 23 ،2015.

54. عبد الحميد احمد، جرائم الشبكة العنكبوتية وغسل الأموال في إطار الملاحقة الأمنية والقضائية الدولي، مكتبة الوفاء القانونية، الطبعة الأولى، الإسكندرية، 2018.

55. عبد الرحمن شامخ الرشيدي، دور معلمي الدراسات الاجتماعية فى تعزيز قيم المواطنة الرقمية من وجهة نظرهم، المقالة 1، المجلد 2021، العدد 61، يناير 2021.

56. عبد الكريم الشامي– جرائم الكمبيوتر والإنترنت في التشريع الفلسطيني – ورقة عمل مقدمة للأمانة العامة لمجلس وزراء الداخلية العرب (سبتمبر 2004).

57. عبد الهادي محمود الزيدي، التجسس الإسرائيلي الالكتروني على الدول العربية، مجلة دراسات دولية، العدد58، 2014.

58. عبير علي عبد العزيز شري، مشروعية التجسس عبر الأقمار الصناعية في القانون الدولي العام، مجلة جامعة الانبار للعلوم القانونية والسياسية، المجاد9، العدد2019،2.

59. عبير نيازي وجيد فتح الله، العوامل المؤدية للجرائم الالكترونية وأدوار الاخصائي الاجتماعي للتعامل معها من منظور الممارسة العامة في الخدمة الاجتماعية، المقالة 1، المجلد 61، العدد 3، يناير 2023.

60. علاء رضوان، أخطر الجرائم المستحدثة.. قيمة الأدلة الرقمية فى الإثبات الجنائى.. المشرع وضع المادة 11 من قانون الجرائم الالكترونية لسد ثغرة الدليل.. وللقاضي حرية الأخذ بمبدأ الإثبات الجنائى من عدمه.. والنقض تتصدى للأزمة الأربعاء، 19 أغسطس 2020

61. علاء رضوان، عن أخطر الجرائم المستحدثة.. قيمة الأدلة الرقمية في الإثبات الجنائي.. المشرع وضع المادة 11 من قانون الجرائم الالكترونية لسد ثغرة الدليل.. وللقاضي حرية الأخذ بمبدأ الإثبات الجنائي من عدمه.. والنقض تتصدى للأزمة، الأربعاء، 19 أغسطس 2020.

62. قسم مجالات الخدمة الاجتماعية – كلية الخدمة الاجتماعية – جامعة حلوان ( القاهرة

63. محمود احمد له، المواجهة التشريعية لجرائم الكمبيوتر والانترنت (دراسة مقارنة)، دار الفكر والقانون، المنصورة، 2012.

64. منصة فك التشفير الجديدة التي أطلقتها الانتربول والمفوضية الأوروبية أدوات برمجية وأجهزة لتقديم المساعدة في الوصول إلى المواد المشفرة للتحقيقات القانونية. ديسمبر 2020.

65. مؤتمر الجرائم الإلكترونية المشترك بين "يوروبول" و"الانتربول" لعام 2021، الذي عُقد في 11 نوفمبر 2021

66. مؤتمر الجريمة الإلكترونية المشترك بين يوروبول والإنتربول لعام 2021 هو "الابتكار للتغلب على تسارع جريمة الإنترنت" في 11 نوفمبر 2021

67. ناشف فريد، آليات التعاون الدولي في مكافحة الجرائم الإلكترونية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 8، العدد 1،يونيو 2022

68. نايلة الصليبي، النشرة الرقمية ، كيفية الحماية من الوقوع ضحية برامج الفدية؟ شرت في: 2022/09/29 .

69. هبه جمال الدين، الأمن السيبراني والتحول في النظام الدولي، مجلة كلية الاقتصاد والعلوم السياسية، المقالة 7، المجلد 24، العدد 1 – 94، يناير 2023.

# فهرس المحتويات

# فهرس المحتويات

# ملخص

**ملخص**

الدراسة تقدم مقدمة شاملة لمنظمة اليوروبول و تاريخها، مع التركيز على دورها في مكافحة الجريمة الإلكترونية، نتناول الظروف التي أحاطت بتأسيس اليوروبول و تحليل الجريمة الإلكترونية بتفصيل، بما في ذلك أنواعها و تطورها، مع التركيز على الإختراقات و الاحتيال الإلكتروني و تهديد الخصوصية و التجسس، كما نناقش الاثار الإجتماعية و الاقتصادية للجريمة الإلكترونية، مع التركيز على تأثير الاحتيال المصرفي و اختراق البيانات الشخصية.

تستعرض الدراسة أيضا دور اليوروبول في مكافحة الجريمة الإلكترونية، مع التركيز على تبادل المعلومات و التحليلات الجنائية و التحديات المستقبلية و الاستراتيجيات المقترحة لتعزيزدور المنظمة في هذا المجال، بما في ذلك تطوير الشراكات الدولية و المحلية و تعزيز الوعي العام بمخاطر الجريمة الإلكترونية.

**الكلمات المفتاحية** : يوروبول، جريمة إلكترونية، تحليل، تبادل معلومات، تحديات.

**Résumé**

L'étude fournit une introduction complète à l'organisation Europol et à son histoire, en mettant l'accent sur son rôle dans la lutte contre la cybercriminalité. Nous abordons les circonstances entourant la création d'Europol et analysons en détail la cybercriminalité, y compris ses types et son évolution, en mettant l'accent sur les piratages. , la fraude électronique, les menaces à la vie privée et l'espionnage. Nous discutons également des impacts sociaux et économiques de la cybercriminalité, en mettant l'accent sur l'impact de la fraude bancaire et des violations de données personnelles.

L'étude examine également le rôle d'Europol dans la lutte contre la cybercriminalité, en mettant l'accent sur l'échange d'informations, l'analyse médico-légale, les défis futurs et les stratégies proposées pour renforcer le rôle de l'organisation dans ce domaine, notamment en développant des partenariats internationaux et locaux et en sensibilisant le public aux dangers de la cybercriminalité. .

**Mots clés :** Europol, cybercriminalité, analyse, échange d'informations, enjeux.

**Abstract**

The study provides a comprehensive introduction to the Europol organization and its history, with a focus on its role in combating cybercrime. We address the circumstances surrounding the founding of Europol and analyze cybercrime in detail, including its types and development, with a focus on hacks, electronic fraud, privacy threats, and espionage. We also discuss the social and economic impacts of cybercrime, with a focus on the impact of bank fraud and personal data breaches.

The study also reviews Europol's role in combating cybercrime, with a focus on information exchange, forensic analysis, future challenges, and proposed strategies to strengthen the organization's role in this field, including developing international and local partnerships and enhancing public awareness of the dangers of cybercrime.

**Keywords:** Europol, cybercrime, analysis, information exchange, challenges.