## ظهور الجرائم الإلكترونية

احتلّ التقدّم في مجال المعلومات والاتّصالات جانباً كبيراً ومُهمّاً في حياة النّاس وتعاملاتهم؛ فصار الحاسوب أساس التّعامل بين الأشخاص والشّركات والمؤسسات، وقد ازداد التوجّه لاستخدام شبكات المعلومات الإلكترونيّة في الفترة الأخيرة بصِفَتها أداة اتّصال دولية في مُختلف مناحي الحياة، مُوفِّرةً بذلك الكثير من السّرعة والمسافات والجهد على الإنسان .إنّ الاستخدام الكبير لِلأنظمة التكنولوجية قاد إلى الكثير من المشاكل والمَخاطر، وقدّم أصنافاً من الجرائم لم تكن مُتداولةً سابقاً، سُميّت بالجرائم الإلكترونية، فما هي الجرائم الإلكترونية؟ وما هي أنواعها؟

## تُعرّف الجرائم الإلكترونية (الرقمية) Digital crime Or Electronic crime

بأنّها المُمارسات التي تُقَع ضدّ فرد أو مجموعةٍ مع توفّر باعثٍ إجراميّ بهدفِ التَّسبُّبِ بالأذى لسمعة الضحيّة عمداً، أو إلحاق الضَّرر النفسيّ والبدنيّ به سواءً أكان ذلك بأسلوبٍ مباشر أو غير مباشر بالاستعانة بشبكات الاتّصال الحديثة كالإنترنت وما تتبعها من أدوات كالبريد الإلكتروني وغرف المُحادثة، والهواتف المحمولة وما تتبعها من أدوات كرسائل الوسائط المُتعدّدة.

They are practices carried out against an individual or a group, with the presence of a criminal motive, aimed at deliberately causing harm to the victim's reputation, or inflicting psychological and physical damage, whether directly or indirectly, through the use of modern communication networks such as the Internet and its related tools like email and chat rooms, as well as mobile phones and their associated tools such as multimedia messages.

### Digital Evidence الدليل الرقمي

**الدليل المستخلص من أجهزة الحاسب الآلي وملحقاته، أو من شبكة الإنترنت، أو أي جهاز آخر له خاصية معالجة أو تخزين المعلومات، وهو عبارة عن مجالات أو نبضات مغناطيسية أو كهربائية، يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة، لتشكل لنا معلومات أو بيانات مختلفة، يمكن الاعتماد عليها في مرحلة التحقيق**

**Digital evidence extracted from computers and their peripherals, the Internet, or any other device capable of processing or storing information. It consists of magnetic or electrical fields or pulses that can be collected and analyzed using specialized programs and applications, forming various types of information or data that can be relied upon during the investigation stage.**

## تحملُ الجرائم الإلكترونيّة مُسمّياتٍ عدّة، منها:

- جرائم الكمبيوتروالإنترنت
- الجرائم السيبرانية Cyper crime
- جرائم التقنية العالية High Tech Crime

## أنواع الجرائم الإلكترونية

للجرائم الإلكترونية أنواعٌ كثيرةٌ، منها:

**جرائمٌ إلكترونية ضدّ الأفراد**: هي الجَرائم التي يتمّ الوصول فيها إلى الهويّة الإلكترونية للأفراد بطرقٍ غير مشروعة؛ كحسابات البريد الإلكتروني وكلمات السِّر التي تخصُّهم، وقد تصل إلى انتحالِ شخصيّاتهم وأخذ الملفّات والصّور المُهمّة من أجهزتهم، بهدفِ تهديدهم بها ليمتَثلوا لأوامرهم، وتُسمّى أيضاً **بجرائم الإنترنت الشّخصية** .

**جرائم إلكترونية ضدّ الحكومات**: هي جرائمٌ تُهاجم المواقع الرّسمية للحكومات وأنظمة شبكاتها وتُركّز على تدمير البنى التحتيّة لهذه المواقع أو الأنظمة الشّبكية بشكلٍ كاملٍ، ويُسمّى الأشخاص المرتكبون لهذه الجريمة بالقراصنة، وغالباً ما تكون أهدافُهم سياسيّة

**جرائم إلكترونية ضدّ الملكية**: هي جرائمٌ تستهدف المؤسسات الشخصيّة والحكومية والخاصّة، وتهدف لإتلاف الوثائق المُهمّة أو البرامج الخاصة، وتتمُّ هذه الجرائم عن طريق نقل برامج ضارّة لأجهزة هذه المؤسسات باستخدام الكثير من الطُّرق كالرسائل.

### الإرهاب الإلكتروني Cyber terrorism

أن الباحثين والمراقبين اجتمعوا على تعريفه بأنه:

" هو استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين أو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو بيئية"

وعليه يمكننا أن نقترح تعريفا للإرهاب الإلكتروني بأنه اختراقاتٌ للأنظمةِ الأمنيّة الحيوية على مواقع الإنترنت، تكونُ جُزءاً من مجهودٍ مُنظّم لمجوعةٍ من الإرهابيين الإلكترونيين أو وكالات مخابراتٍ دوليّة، أو أيّ جماعات تَسعى للاستفادة من ثغرات هذه المواقع والأنظمة الوصول للمواقع المُشفّرة والمحجوبة

**الجرائم السّياسية الإلكترونية**: هي جرائم تستهدفُ المواقع العسكرية للدول بهدف سرقة معلومات تتعلّق بالدّولة وأمنها .سرقة المعلومات: تَشمل المَعلومات المحفوظة إلكترونياً وتوزيعها بأساليب غير مشروعة.

### جرائم الاحتيال والاعتداء على الأموال

تشملُ هذه الجرائم الكثير من الممارسات منها:

- إدخال بيانات غير صحيحة أو تعليمات من غير المشروع التصّريح بها، أو استعمالُ بياناتٍ وعمليّاتٍ غير مسموح الوصول إليها بغيةَ السّرقة من قِبل موظّفين فاسدين في الشّركات والمؤسسات المالية
- حذف أو تعديل المعلومات المحفوظة، أو إساءة استعمال أدوات الأنظمة المُتوافرة وحزم البرامج .

### جرائم الابتزاز الإلكترون(Cyber extortion crime)

هي أن يتعرّض نظامٌ حاسوبيّ او موقعٌ إلكترونيّ ما لهجماتِ حرمانٍ من خدمات مُعيّنة؛ حيثُ يشنّ هذه الهجمات ويُكرّرها قراصنة محترفون، بهدفِ تحصيلِ مُقابلٍ ماديّ لوقف هذه الهجمات.

## المطاردة الإلكترونية:

هي الجرائم المُتعلّقة بتعقّب أو مطاردة الأفراد عن طريق الوسائل الإلكترونيّة لغاية تعريضهم للمضايقات الشّخصية أو الإحراج العام أو السّرقة المالية، وتهديدهم بذلك؛ حيث يجمع مرتكبو هذه الجرائم معلوماتِ الضّحية الشخصية عبر مواقع الشّبكات الاجتماعي وغرف المحادثة وغيرها.

## مخاطر الجرائم الالكترونية

يُؤدّي انتشار الجرائم الإلكترونية في المُجتمعات إلى الكثير من المخاطر والتهديدات، ومنها: المساس بالاقتصاد والأمن الوطني وتهديده المساس بالعلاقات الأسرية وتشكيل الخلافات بين أفراد الأسرة ممّا يؤدّي إلى التفكك الأسري، وذلك بسبب الكثير من النتائج التي تُسبّبها بعض أنواع الجرائم الإلكترونية كالتّشهير ببعض الأفراد ونشر الأخبار الكاذبة والإشاعات.

## خصائص الجرائم الإلكترونية

تتميّز الجرائم الإلكترونية بعدّة خصائص، منها:

- صعوبة معرفة مرتكب الجريمة، إلّا باستخدام وسائل أمنيّة ذات تقنية عالية
- صعوبة قياس الضّرر المُترتِّب عليها، كونه ضرراً يمسّ الكيانات المعنوية ذات القيم المعنوية أو القيم الماديّة أو كلاهما سويّةً.
- سهولة الوقوع فيها؛ بسبب غياب الرّقابة الأمنية
- سهولة إخفاء وطمس مَعالم الجريمة وآثارها والدّلائل التي تُدلّ على مرتكبها .هي أقلّ جهداً وعُنفاً جسديّاً من الجرائم التّقليدية .سلوكٌ غير أخلاقيّ في المجتمع .جريمةٌ لا تتقيّد بمكانٍ أو زمانٍ مُحدّدين.

## Characteristics of Cybercrimes

Cybercrimes are characterized by several features, including:

• The difficulty of identifying the perpetrator, except through the use of advanced, high-technology security methods.

• The difficulty of measuring the resulting damage, as it often affects intangible entities involving moral values, material values, or both.

• The ease with which such crimes can occur due to the absence or weakness of security oversight.

• The ease of concealing and erasing the traces, evidence, and indicators that may lead to identifying the offender.

• They require less effort and involve less physical violence compared to traditional crimes.

• They represent unethical behavior within society.

•They are crimes that are not restricted by a specific place or time.

## مكافحة الجرائم الإلكترونية

تسعى الدّول والحكومات بشكلٍ جديّ للحدّ من الجَرائم الإلكترونيّة وآثارها عبر طُرقٍ كثيرة منها

- فرضُ سياساتٍ دوليّة وعقوباتٍ كبيرة على مُرتكبي هذه الجَرائم .
- تفعيل أحدث التقنيات والوسائل للكشفِ عن هويّة مُرتكبي الجرائم
- نشر التّوعية في المُجتمعات حول الجرائم الإلكترونية ومَخاطرها، وتَعريف الأفراد بكيفيّة الحِفاظ على معلوماتهم وخصوصيّاتهم؛ كحساباتهم البنكية وبطاقاتهم الائتمانية
- إنشاء خطوط هاتفيّة ومؤسسات مُعيّنة تابعة للدّولة للإبلاغ عن الحالات التي تتعرّض لمثل هذا النّوع من الجرائم.
- توجيه التّشريعات والقوانين وتحديثها بما يَتماشى مع التّطورات التكنولوجية، لفرض قَوانين جديدة فيما يستجدّ من هذه الجرائم.

## الصعوبات المسجلة في مواجهة الجرائم الإلكترونية

1. **الطبيعة غير المرئية للدليل الجنائي الرقمي**
2. **سهولة تدمير ومحو الدليل الجنائي الرقمي**
3. **إعاقة الوصول إلى الدليل الجنائي الرقمي**
4. **ضخامة البيانات المتعين فحصها**
5. **صعوبة التوصل إلى الأدلة الرقمية والتحفظ عليها**

**Recorded Challenges in Combating Cybercrimes**

1. **The invisible nature of digital forensic evidence.**
2. **The ease with which digital forensic evidence can be destroyed or erased.**
3. **Obstacles to accessing digital forensic evidence.**
4. **The massive volume of data that must be examined.**
5. **The difficulty of locating, preserving, and securing digital evidence.**

## الوسائل المادية الحديثة المستخدمة في جمع الأدلة الجنائية الرقمية

وسائل فنية الهدف منها جمع مختلف الأدلة الجنائية الرقمية التي يمكن من خلالها الكشف عن ملابسات الجريمة المعلوماتية، ومنه عندما يستعمل المستخدم شبكة الانترنت، فإنه يترك آثارا وراءه عن كل موقع يزوره.

### أولا :استخدام بروتوكولIP\TCP

IP/TCP من أكثر البروتوكولات المستخدمة في شبكة الانترنت لأنه يعتبر جزء أساسي منه، والمسؤول عن تراسل حزم البيانات عبره وتوجيهها إلى أهدافها .

### ثانيا :استخدام معلومات الكوكيزCookies

عند زيارة مستخدم الإنترنت أي موقع من مواقع الويب، تفتح هذه الأخيرة ملفا صغيرا على القرص الصلب يسمى كوكيCookie بهدف جمع بعض المعلومات عنه وتحسين عملية تصفح الموقع و منه فهو يسجل العديد من المعلومات التي يمكن أن تساعد في التحقيق من بينها تاريخ زيارة الموقع الإلكتروني، أو تاريخ إجراء التعديلات عليه أو الانتهاء منها، وزيادة على ذلك الاحتفاظ بكلمات السر الخاصة بالمستخدم عند زيارته للموقع.

### ثالثا :استخدام معلومات البروكسيProxy

ومن بين أهم ما تتميز به مزودات البروكسيProxy هو إمكانيتها في تسريع الوصول إلى شبكة الإنترنت، بالإضافة إلى احتوائها على تدابير أمنية للتحكم بعملية الاتصال بالإنترنت، و مثال ذلك التعرف على الأشخاص المسموح لهم بالاتصال بالشبكة، وتحديد الخدمات التي يمكن استخدامها، أو حتى تحديد الأيام والأوقات المسموح بها بزيارة شبكة الإنترنت وعليه فكل هذه العمليات والمعلومات التي يحتويها البروكسي يتم حفظها في قاعدة بياناته، مما يجعل دورها قوي في الإثبات عن طريق فحص تلك العمليات المحفوظة بها والتي تخص المتهم والموجودة عند مزود الخدمة.

### رابعا :استخدام برامج التتبع وكشف الاختراق

إن طبيعة عمل هذه البرامج تكمن في التعرف على محاولات الاختراق، وكشف كافة المعلومات المتعلقة بمن قام بها، وأيضا إشعار الجهة المتضررة من هذه العملية، ومن بين هذه البرامج، برنامج Hack Tracerفعندما يرصد أي محاولة للقرصنة أو اختراق جهاز الحاسب الآلي، يسارع بإغلاق منافذ الدخول أمام المخترق، ثم يبدأ في عملية اقتفاء أثره حتى يصل إلى الجهاز الذي حدث العملية من خلاله، ويستعرض هذا البرنامج مجموعة شاملة من بيانات المخترق من حيث عنوانIP الخاص به، وتاريخ حدوث الاختراق باليوم والساعة، وفي الأخير المعلومات الخاصة بمزود الخدمة.

## الاجراءات المتخذة عند التعامل مع مسرح الجريمة الالكترونية

### 1- تحريز جهاز تسجيل كاميرات المراقبة (DVR)

**يتم ذكر نوعه والرقم التسلسلي للجهاز والتأكد من وجود تسجيلات فيدوية و مدتها و عدد الكاميرات و مكان تثبيتها و مدى الرؤية الهندسية التي تغطي كافة أجزاء الموقع وبيان فيما اذا كانت تعمل ام متوقفة او كانت تستخدم للمراقبة او للمراقبة والتسجيل و تحديد الوقت والتاريخ المضبوط علية الجهاز.**

## 2 - تحريز أجهزة الكمبيوتر المكتبية او لابتوب

**يذكر الرقم التسلسلي للجهاز و نوعه وتسجيل كافة المعلومات يتم تسجيل المعلومات المفعلة في الجهاز من برامج او مواقع او مراسلات وغيرها في سجل خاص بالإضافة الى تصويرها وبعدها يتم إطفاء الجهاز و تحريز كافة الملحقات المرتبطة به ونقله الأجهزة الى المختبر بعد حفضها في صندوق خاص بأجهزة الكمبيوتر .**


## 3 - الوحدات الخزينة المتحركة

**تحريز كافة وسائل الخزن الموجودة في محل الحادث ( هارد . فلاش رام . رام .الخ) وبيان نوعها و الحجم و موقعها في مسرح الجريمة و تسجيل المعلومات المتعلقة بها و حفظ المبارز في صندوق خاص لغرض نقله الى المختبر .**

## 4 ـ كاميرات المراقبة السرية

البحث عن كاميرات المراقبة السرية و تحديد نوعها و شكلها و حالتها ان كانت في وضع التشغيل او متوقفة حيث يتم تحريزها واطفاءها للمحافظة على التسجيلات الموجودة و ملاحظه حاله الكاميرا ان كانت مربوطة عن طريق شبكة الانترنيت حيث يتم قطع كافة و حفظها في صندوق خاص لغرض نقلها الى المختبر.

## 5 ـ أجهزة الموبايل (لوحية – الاعتيادية)

**تحريز كافة أجهزة الهواتف النقالة مع ذكر النوع واللون والموديل والرقم التسلسلي و حاله الجهاز اثناء تحريزه حيث في حاله كون الجهاز يعمل ومفتوح يتم قطع الاتصال عن الشبكة و عن الانترنيت و تسجيل و تصوير كافة المعلومات و بيان حاله الجهاز اذا كان يحتوي على رمز سري للقفل من عدمه و بعدها يتم نقل الجهاز للمختبر بعد حفظه داخل كيس خاص بأجهزة الموبايل .**