**International Journal of Legal and Comparative Jurisprudence Studies (LCJS)**

Volume.5, Issue.2 pp: 132-144 Article 5
*Aug (2024)*

# دور المجتمع الدولي في مكافحة الجرائم المعلوماتية

# The Role of the International Community in Combating Information Crimes

**خيرالدين العايب**

**Kheireddine Laib**

أستاذ العلاقات الدولية المشارك- الجزائر

كلية الشرطة- أبو ظبي

Associate Professor of International Relations, Algeria

Police College, Abu Dhabi

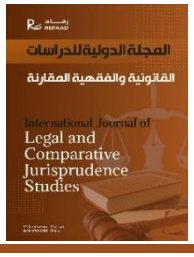
khiredine12@hotmail.com

| Accepted<br>قبول البحث | Revised<br>مراجعة البحث | Received<br>استلام البحث |
|---|---|---|
| 2024/8/10 | 2024 /7/18 | 2024 /6/23 |

**DOI:** https://doi.org/10.31559/LCJS2024.5.2.5

رفـــاد REFAAD
www.refaad.com

*International Journal of Legal and Comparative Jurisprudence Studies (LCJS)*
المجلة الدولية للدراسات القانونية والفقهية المقارنة
Journal Homepage: https://www.refaad.com/Journal/Index/9
E-ISSN 2708-6607 | P-ISSN 2708-6593




# دور المجتمع الدولي في مكافحة الجرائم المعلوماتية

# The Role of the International Community in Combating Information Crimes

**الملخص:**

**الأهداف:** تهدف الدراسة إلى الوقوف على طبيعة الجرائم المعلوماتية وخصائصها ومخاطرها الأمنية ودور المجتمع الدولي في مكافحتها.

**المنهجية:** اعتمدت الدراسة على المنهج الوصفي والتحليلي لكونهما من بين أكثر المناهج الملائمة لمثل هذه الدراسات.

**النتائج:** توصلت الدراسة إلى أن الجرائم المعلوماتية تشكل تحديًا أمنيًا جديدًا أمام الأجهزة الشرطية والأمنية، كما إنه من الصعوبة التعرف على مرتكبي الجرائم المعلوماتية الذين يمتلكون خبرات كبيرة في ارتكاب أنواع شتى من الجرائم فضلًا إلى وجود جهود دولية لمكافحة الجرائم المعلوماتية من خلال الاتفاقيات الدولية والمنظمة الدولية للشرطة الجنائية.

**الخلاصة:** توصي الدراسة باتخاذ إجراءات تشريعية صارمة تتماشى مع هذا النوع من الجرائم المعلوماتية تأخذ بعين الاعتبار الطبيعة الخاصة لهذه الجرائم بالإضافة إلى مضاعفة التنسيق والتعاون بين الدول على المستويات الإقليمية والدولية في التصدي لهذا النوع من الجرائم المستحدثة.

***الكلمات المفتاحية:*** *الجريمة المعلوماتية؛ الثورة التكنولوجية؛ الانتربول.*

**Abstract:**

**Objectives:** The study aims to identify the nature of information crimes, their characteristics, security risks, and the role of the international community in combating them.

**Methods:** The study relied on the descriptive and analytical approaches because they are among the most appropriate approaches for such studies.

**Results:** It concluded that cybercrimes constitute a new security challenge for the police and security services, it is also difficult to identify the perpetrators of cybercrimes who have extensive experience in committing various types of crimes, in addition to the existence of international efforts to combat cybercrimes through international agreements and the International Criminal Police Organization.

**Conclusions:** The study recommends taking strict legislative measures consistent with this type of information crimes, taking into account the special nature of these crimes, in addition to doubling coordination and cooperation between countries at the regional and international levels in confronting this type of emerging crimes.

***Keywords****: information crime; technological revolution; Interpol.*

## المقدمة:

واكب تطور المجتمعات البشرية عبر التاريخ تطور في نوع الجرائم التي تعانيها هذه المجتمعات،الأمر الذي كان يدعو إلى تبني التشريعات والقوانين التي تحد من الآثار السلبية لهذه الجرائم على الفرد والمجتمع، وإن كانت العقود الأخيرة من عمر البشرية تعتبر عصرًا فرضت فيه التكنولوجيا نفسها وبكل أشكالها على الجميع، فقد فتحت هذه التكنولوجيا بابًا جديدًا لأنواع لم تكون معهودة من الجرائم، جرائم قد يغيب عن العيان مشهد مرتكبها، بل ويغيب حتى الجاني عن مكان الضحية، جرائم عابرة للقارات، سلاح المجرم فيها خبرة تكنولوجية عالية يوظفها في خدمة أهداف غير مشروعة، بعيدًا عن أي نوع من الرقابة، مستهدفًا مصالح الأفراد والمؤسسات والدول، مستغلًا قدرته على إتلاف الأدلة ليحاول الهرب من العقاب، لينتقل عبر العالم الافتراضي إلى مكان آخر في العالم يمارس فيه جرائمه الإلكترونية ومستغلًا بعدم وسمه بسمات المجرم التقليدي ليبقى مختفيًا حتى عن أقرب الناس إليه.

الأمر الذي يعقد من مهمة متعقبي الجرائم من رجال الشرطة، ويتطلب أن يكون مطبقو العدالة في مجال محاربة هذا النوع من الجرائم على معرفة علمية عالية، ملمين إلمامًا كاملًا بكل ما هو جديد في عالم التقنية والتشريعات والعلوم الأمنية ليستطيعوا حماية المجتمع من هذا الخطر الدائم.

### مشكلة الدراسة:

تكمن مشكلة الدراسة في كون الجرائم المعلوماتية صارت تمثل اليوم تحديًا أمنيًا خطيرًا يصعب على الاجهزة الشرطية والأمنية مواجهتها من دون توافر الإمكانات التكنولوجية المتطورة والتنسيق الدولي على اعتبار أن هذه الجرائم المستحدثة عابرة للحدود ويستحيل فيها التعرف على الجاني أو الوصول إلى الدليل الجنائي ولذلك يطرح التساؤل عن قدرة المجتمع الدولي في مواجهة جرائم معقدة وسرعة الانتشار توظف فيها التقنية المتطورة ويصعب فيها التعرف على الجاني ويستحيل فيها الوصول إلى الدليل الجنائي في بعض الأحيان.

### أهمية الدراسة:

تنقسم الدراسة إلى قسمين:

**الأهمية العلمية:**

تظهر أهمية الدراسة في محاولتها استكشاف وتحديد معالم الجرائم المعلوماتية وخصائصها ودور التعاون الدولي في مكافحتها بوصفها جرائم مستحدثة صارت تشكل تحديًا جديدًا أمام الأجهزة الشرطية والأمنية.

**الاهمية العملية:**

كما تكمن أهمية هذا الموضوع في إبراز اهم الجرائم المعلوماتية التي صارت منتشرة في دول العالم وفي مدى خطورة هذه الجرائم وتزايدها المطرد والآثار السلبية الخطيرة التي تنتج عنها وآثارها البالغ على المجتمعات العالمية. ومما يزيد أهمية هذه الدراسة الانتشار المتزايد لشبكة الإنترنت مما يفسر زيادة أعداد الجرائم التي باتت تهدد البشر عبر فضاء الإنترنت.

### أهداف الدراسة:

ترمي الدراسة إلى تحقيق الأهداف التالية:

- تحديد مخاطر الثورة التكنولوجية.
- تحديد مفهوم الجريمة المعلوماتية وطبيعتها.
- أهمية التعاون الدولي في مكافحة الجرائم المعلوماتية.
- دور المنظمة الدولية للشرطة الجريمة في مكافحة الجرائم المعلوماتية.

### منهجية الدراسة:

سيتم الاعتماد على المنهج الوصفي والمنهج التحليلي وربط الأسباب بالنتائج مما يسمح بمعرفة مختلف جوانب الظاهرة محل الدراسة عبر عرض مختلف الرؤى المتعلقة بمواجهة الجرائم المعلوماتية.

### خطة الدراسة:

قسمت الدراسة إلى مبحثين، خصصنا المبحث الأول لدراسة طبيعة الجريمة المعلوماتية وخصائصها من خلال مطلبين اثنين، تناول المطلب الأول دراسة مخاطر الثورة التكنولوجية وتناول المطلب الثاني تعريف الجريمة المعلوماتية.

أما المبحث الثاني فخصص لدراسة آليات مكافحة الجريمة المعلوماتية حيث تناول المطلب الأول دراسة التشريعات الوطنية التي أصدرتها بعض الدول عن الجريمة المعلوماتية وتناول المطلب الثاني دراسة دور المنظمة الدولية للشرطة الجنائية في مكافحة الجريمة المعلوماتية.

## المبحث الأول: طبيعة الجريمة المعلوماتية وخصائصها

**تمهيد:**

تعد الثورة التكنولوجية- كأهم التطورات التي يعيشها العالم اليوم- هي المحرك الأساسي للتطورات الحادثة في الوقت الحالي، ولكن هذا التقدم التقني جاء مصحوبًا بصور مستحدثة لارتكاب الجرائم التي تستعير من هذه التقنية أساليبها المتطورة، فأصبحنا أمام ظاهرة إجرامية جديدة هي ظاهرة الجريمة المعلوماتية.

فالمصالح التقليدية التي تحميها كل التشريعات والنظم القانونية منذ زمن بعيد بدأت تتعرض إلى أشكال مستحدثة من الاعتداء بواسطة التقنيات الحديثة، فبعد أن كان الاعتداء على الأموال يتم بواسطة السرقة التقليدية أو النصب وكانت الثقة في المحررات الورقية يعتدى عليها بواسطة التزوير، أصبحت هذه الأموال يعتدي عليها عن طريق اختراق الشبكات المعلوماتية وإجراء التحويلات الإلكترونية من أقصى مشارق الأرض إلى مغاربها في لحظات معدودة، كما أصبحت تلك الحقوق الثابتة في الأوعية الورقية يتم الاعتداء عليها في أوعيتها الإلكترونية المستحدثة عن طريق اختراق الشبكات والأنظمة المعلوماتية دون الحاجة إلى المساس بأي وثائق أو محررات ورقية.

### المطلب الأول: مخاطر الثورة التكنولوجية

إن الفضاء السيبيري- كأحد معطيات الثورة التكنولوجية- وضع دول العالم في حالة اتصال دائم، وأصبحت شبكة الإنترنت اليوم تشهد تعايشًا مستمرًا في جميع المجالات العلمية والبحثية والاقتصادية بل والسياسية والاجتماعية على السواء.

لقد فرضت الثورة التكنولوجية، ووليدتها شبكة الإنترنت، تحديات أمنية وقانونية جديدة، تمثلت في ظهور طائفة مستحدثة من الجرائم أطلق عليها الجرائم المعلوماتية، وعليه فإن إعطاء صورة عامة عن الجريمة المعلوماتية، وما تثيره خصائصها وسمات مرتكبيها، من إشكاليات أمنية، وقانونية يقتضي ضرورة التعرف عليها، وكشف صورها المختلفة والإلمام بكافة جوانب هذا النوع المستحدث من الجرائم.

لقد بدأت الثورة التكنولوجية نتيجة اقتران تقنيتي الاتصالات من جهة، والمعلومات وما وصلت إليه من جهة أخرى، حتى بات يطلق على هذا العصر عصر المعلومات علمًا أن المعلومة تعد أهم ممتلكات الإنسان فقد اهتم بها على مر العصور فجمعها ودونها وسجلها على وسائط متدرجة التطور، بدأت بجدران المعابد والمقابر ثم انتقلت إلى ورق البردي وانتهت باختراع الورق الذي تعددت أشكاله، حتى وصل بها المطاف إلى الأقراص الإلكترونية الممغنطة (جميل،2001).

الإنترنت، شبكة الشبكات، ومحرك الحضارات الجديدة، التي تقوم على فكرة الاتصال لا الانتقال، وهي نتاج ثورة تكنولوجيا المعلومات والاتصالات.

والإنترنت كلمة انجليزية Internet مشتقه من جملة International Network بمعنى الشبكة الدولية، ويعرّفها البعض بأنها شبكة طرق المواصلات السريعة حيث تتكون الإنترنت من عدد كبير من شبكات الحاسب المترابطة والمتناثرة في أنحاء كثيرة من العالم، ويحكم ترابط تلك الأجهزة وتحادثها بروتوكول موحد يسمى "بروتوكول تراسل الإنترنتTCP/IP (حشمت،2005).

هذه الشبكة لم تكن في خاطر من بدؤوها عندما كانت هناك نقطة للبداية، فالإنترنت هي منتج غير مستهدف في صراع طال بين الشرق والغرب لسنوات طويلة، ففي عام1969 قامت وزارة الدفاع الأمريكية عن طريق بول بارن Paul Baran باحث الاتصالات الشهير بإنشاء شبكة اتصالات عسكرية تعمل على أسس لامركزية، للربط بين قواعدها العسكرية المنتشرة حول العالم بشكل يضمن استمرار السيطرة على ترسانة الصواريخ والقاذفات إذا ما تعرضت الولايات المتحدة الأمريكية كلها أو جزء منها لهجوم نووي وبما يضمن إمكانية الرد على هذا الهجوم.

وقد كانت الشبكة الأولى والتي سُميت شبكة وكالة المشروعات المتقدمة (ARPA NET)، مكونة من4 حاسبات رئيسية موزعة بين أربع جامعات أمريكية.

وفي عام 1973، طور فين سيرف -(Vint Cerf) والذى يطلق عليه أبو الإنترنت- طور بروتوكول سمي (TCP/IP)، حيث سمح هذا البروتوكول بتوصيل أجهزة الكمبيوتر التي تعمل بأنظمة عمل مختلفة وشبكات الكمبيوتر (التي تعمل ببروتوكولات مختلفة) ببعضها البعض. وقد قررت وزارة الدفاع الأميركية تبنى هذا البروتوكول على شبكتها ولكنها استخدمت لأول مرة الاتصالات اللاسلكية وشبكة الاتصالات عبر الأقمار الصناعية (حشمت، 2005).

في عام 1983 تطّور المشروع وتحوّل إلى الاستعمال السلمي حيث انقسم إلى شبكتين، احتفظت الشبكة الأولى باسمها الأساسي (ARPANE) وبغرضها الأساسي وهو خدمة الاستخدامات العسكرية في حين سُمّيتْ الشبكة الثانية باسم (MILNET) وخصصت للاستخدامات المدنية، أي تبادل المعلومات.

وشهد عام 1992 مولد الشبكة العنكبوتية العالمية (WWW: World Wide Web)، وما استتبعه من ظهور مصطلح العالم الافتراضي.Cyber World (الشنيفي،2007).

لا أحد في الوقت الراهن يملك الإنترنت، وإن كان يمكن القول في البداية بأنّ الحكومة الأمريكية ممثلة في وزارة الدفاع ثم المؤسسة القومية للعلوم هي المالك الوحيد للشبكة ولكن بعد تطّور الشبكة ونمّوها لم يعد يملكها أحد واختفى مفهوم التملك ليحل محله ما أصبح يسمي بمجتمع الإنترنت.

كما أنّ تمويل الشبكة تحول من القطاع الحكومي إلى القطاع الخاص ومن هنا ولدت العديد من الشبكات الإقليمية ذات الصبغة التجارية والتي يمكن الاستفادة من خدماتها مقابل اشتراك.

لقد أفرزت الثورة التكنولوجية نظامًا دوليًا جديدًا للمعلومات، مما جعلها تتسم بعدد من الخصائص الهامة منها (الشنيفي، 2007):

- **التسارع:** إن سنة الحياة هي التغير المستمر وإذا كان التغير في فجر التاريخ بطيئًا فإنه حاليًا يتسم بتزايد سرعته باستمرار، ويخلق بذلك فجوة تتزايد بين الدول المتقدمة والنامية.
- **التطور:** للتكنولوجيا طبيعة اقتحاميه، بمعنى أنها تقتحم المجتمعات سواء كانت تحتاج إليها أو غير راغبة فيها، لكون التكنولوجيا الجديدة تتسم بالتطور الدائم، فهي أكثر كفاءة في الأداء وأقل ثمنًا أو أصغر وأخف وزنًا وأكثر تقدمًا من سابقتها.
- **اللامكان:** أنتج النظام الدولي للمعلومات ما يسمى بالفضاء اللامتناهي (Cyber Space)، الذي انهارت فيه الفواصل الجغرافية، وخلق عالم تخيليًا (Virtual World) يتعامل فيه الناس دون أن يلتقوا وجهًا لوجه.
- **اللازمان:** في النظام الدولي للمعلومات، كل مواقع العمل والإنتاج والخدمات تعمل بلا توقف لتلبية احتياجات العملاء بجميع أنحاء العالم بالرغم من الفواصل الزمنية، فيما يعرف باستمرار العمل والإنتاج وتقديم الخدمة 24/7.
- **اللامادية:** تضاءلت قيمة المكونات المادية في المنتجات الجديدة بصورة كبيرة، فبعد أن كانت هذه المكونات تصل إلى 30% من قيمة المنتج، فإنها قد وصلت إلى حوالي 2% ليتزايد قيمة المكون المعرفي والتكنولوجي.

هذا وللأنظمة المعلوماتية على مختلف مظاهرها- كالحاسب الآلي وشبكات الاتصالات الدولية، وشبكة المعلومات العالمية(web) ، والبريد الإلكتروني أو الرقمي(E-mail)، والمجاميع الإخبارية (New Groups) ، ومواقع نقل الملفات (File Transferee Protocol) وغرف المحادثة (Chatting Rooms) ، ومواقع التواصل الاجتماعي، ووسائل التواصل الاجتماعي على أجهزة المحمول .... الخ- مزايا في مجال الإعلام والاتصالات والتراسل وإجراء المكالمات الهاتفية الدولية والاتصالات البريدية بأسعار زهيدة، وحالات التعارف الاجتماعي بصورة رسمت شكلًا جديدًا للعلاقات الإنسانية تعتمد على التفاهم والتفكير المشترك، كما أن لهذه الأنظمة مزايا أخرى في مجال التعليم والبحث العلمي، وكذلك تتبع أخبار العالم كما تراها وكالات الأنباء ومحطات الأخبار العالمية والصحف، وإنجاز المال والأعمال، ولكن للثورة التكنولوجية مظاهر سلبية عديدة أيضًا، لعل من أهمها (طارق،2009):

- **مخاطر اجتماعية:**

تتمثل في إضعاف المشاركة الاجتماعية والوجدانية بين أفراد المجتمع وتفضيل العزلة المؤدية للاغتراب، فضلًا عن التهديد المروع للقيم الدينية والهوية الثقافية والتعرض للغزو الثقافي والفكري المتطرف والإباحي، والذي يمكن أن يصل بمستخدم الشبكة في تلك المجالات إلى حد درجة الإدمان، بمختلف أنواعه (الجنسي والإباحي، المقامرة الاليكترونية، التصنت على الغير...الخ).

- **مخاطر نفسية:**

تتعلق بحدوث اضطرابات نفسية وصراعات ذهنية ونفسية داخلية، بسبب مقارنته للخيال والوهم الذي يراه ويستشعره- من تعامله التخيلي مع العالم الافتراضي- بالواقع الذي يحيا بأبعاده وتحدياته المختلفة.

- **مخاطر بدنية وصحية:**

من جرّاء الإشعاعات الصادرة عن شاشات الكمبيوتر والتي تؤثر سلبًا على أعضاء الجسم البشري، وكذا الأضرار التي تصيب العمود الفقري والرقبة والأرجل نتيجة طول الفترة الزمنية أمام جهاز الكومبيوتر

- **مخاطر اقتصادية:**

أدى إقبال البعض على شراء أحدث أجهزة المحمول والأجهزة اللوحية الرقمية، إلى تبديد أموال طائلة كان يمكن إنفاقها في شراء الأشياء النافعة أو تنمية القدرات الذاتية، أو مساعدة المجتمع والفقراء.

- **مخاطر جنائية:**

تنبع من كون الشبكة بمثابة مصيدة تكنولوجية عالمية يمكن أن تقود مستخدميها إلى عالم الجريمة، كفاعلين أصليين أو مشاركين أو ضحايا، دون أي إدراك أو علم من جانبهم، وأوضح مثال لذلك أقبال بعض الشباب على تعاطي المخدرات الرقمية على شبكة الإنترنت.

- **مخاطر الهجرة الاليكترونية للعالم الافتراضي:**

تحققت الهجرة الإلكترونية لما يطلق عليه بالعالم الافتراضي (Virtual Organization) أو العالم الثاني(second life)، من خلال بعض المواقع الإلكترونية التي تسمح لمستخدميها بتحميل تطبيق خاص، يتيح لكل مستخدم فرص التواصل مع مستخدمي البرنامج الآخرين من مختلف دول العالم، وكل منهم يسمى ساكنًا أو مقيمًا (avatar) في العالم الثاني second life ويقوم باختيار وتقمص شخصية ثلاثية الأبعاد) على نحو تمثيل الأشخاص في الفيلم الأمريكي أفاتار(avatar) ، ويستطيع ممارسة أنشطة فردية أو جماعية ويتبادل سلعًا وخدمات كلها خيالية (بيومي،2009) .

وقد وصل عدد سكان هذا العالم الافتراضي على شبكة الإنترنت لأكثر من عشرة ملايين، ينتمون إلى أكثر من مائة وعشرين دولة في عالم الواقع، وسكان العالم الثاني هم الذين يملكون ويشيدون البنية التكنولوجية بما في ذلك المنازل والمركبات والنوادي الليلية والمتاجر، وكذلك المعالم الرئيسية والملابس والألعاب والمدارس والشركات، وفي استطاعة أي شخص أن يطلب العضوية المجانية بتسجيل اسمه في العالم الثاني وابتكار شخصية له في هذا العالم الافتراضي يتعامل من خلالها بهذا العالم، ويتم التعامل خلاله باستخدام العملة الخاصة به (دولار ليندن)، ويمكن مبادلتها في سوق الصرف الافتراضي، واتفق سكان العالم الثاني على أن سعر الصرف هو 265 دولار ليندن مقابل كل دولار أمريكي.

ولم يقتصر الأمر على مشاركة الأفراد في هذا العالم الافتراضي، بل تجاوز الأمر إلى مشاركة الدول والمؤسسات العالمية، حيث بدأت تشارك في هذا العالم الافتراضي.

وقد تلاحظ مؤخرًا تنامي تواجد الحكومة الأمريكية في هذا العالم الافتراضي، وتبرر الجهات والوكالات الحكومية الأمريكية ذلك بأنها تستخدم مجال الحقيقة الافتراضية في التوعية والتواصل، والإدارة الأمريكية لشؤون المحيطات والغلاف الجوي هي التي تملك أكثر المنشآت تطورًا وتقدمًا في العالم الافتراضي حتى الآن، وفي جزيرتها الخاصة المسماة (ميتيورا) يستطيع الزوار تجربة الحياة أثناء هبوب إعصار قوي وهم على جناح طائرة أبحاث، أو الصعود عبر الغلاف الجوي وهم يتشبثون ببالون اختبار، أو الوقوف على أحد الشواطئ أثناء اكتساح موجات المد العاتي للتسونامي ، أو الغوص في أعماق البحار على متن غواصة افتراضية (عبدالقادر،2012).

وتكمن خطورة الانخراط في التعامل مع هذا العالم الافتراضي في زيادة الفجوة الاجتماعية والشعورية بين أفراد الأسرة الواحدة والمجتمع الواحد، وما يمكن أن يسببه ذلك من نتائج سلبية في العلاقات الاجتماعية والحياة الاقتصادية للمجتمع، نظرًا لأن الانخراط في هذا العالم الافتراضي يعد بمثابة هروب من الحياة الواقعية التي نحياها وهروبًا مما تزخر به من مشاكل وأزمات، كما أنه سيؤدي إلى سلوكيات غير مشروعة لم يخبرها مجتمعنا الواقعي من قبل.

**المطلب الثاني: تعريف الجريمة المعلوماتية**

**أولًا: تعريف الجريمة المعلوماتية**

يبدو أنه لا اتفاق بين الفقهاء حول مصطلح موحد للدلالة على هذه الظاهرة المستحدثة، فالبعض يطلق عليها الجريمة الإلكترونية، والبعض يطلق عليها جريمة العالم الافتراضي، أو جريمة الحاسب والإنترنت، أو جريمة التقنيات العالية، أو الإجرام السيبيري...الخ، وهذا الاختلاف في تسميتها عبر عنه بالاختلاف في تعريفها وتصنيفها بالشكل الذي سنورده كما يلي:

أُشْتُقَتْ كلمة الجريمة- بصفة عامة- في اللغة من الجُرم، وهو التعدي أو الذنب، وجمع الكلمة إجرام وجروم وهو الجريمة. وقد جَرَمَ يَجْرِمُ واجْتَرَمَ وأَجْرَم فهو مجرم وجريم.

وعَرَّفت الشريعة الإسلامية الجريمة بأنها: "محظورات شرعية زجر الله عنها بحد أو تعزير(معن،2012).

أما الجريمة المعلوماتية، وبصفة خاصة، فقد تعددت تعريفاتها، فعرفتها الدكتورة هدي قشقوش بأنها " كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات (هدى،1992).

وعرفها Rosenblatt بأنها "كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب." (بيومي،2005)

كما عرفها الفقيه Artar Solarz بأنها "أي نمط من أنماط الجرائم المعروف في قانون العقوبات طالما كان مرتبط بتقنية المعلومات (هشام،1992).

ويرى Eslie D.Ball أنها "فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية ( Barry,2013).

كما عرفتها وزارة العدل الأمريكية بأنها "أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها (الرشيدي،2011)

ويعرفها Sheldon بأنها "واقعة تتضمن تقنية الحاسب، ومجني عليه يتكبد أو يمكن أن يتكبد خسارة، وفاعل يحصل عن عمد أو يمكنه الحصول على مكسب (عوض،1993).

كما يعرفها خبراء منظمة التعاون الاقتصادي والتنمية OECD بأنها "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها(سلامة،1971).

ويعرفها الفقيه الفرنسي Vivant بأنها " مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب (عفيف،بدون تاريخ).

ويعرفها كل من Robert, J.Lindquist Jack Bologna بأنها "جريمة يستخدم فيها الحاسوب، كوسيلة أو أداة لارتكابها، أو يمثل إغراء بذلك، أو جريمة يكون الكمبيوتر نفسه ضحيتها (خالد،2013).

من التعريفات المذكورة نستطيع القول أن بالجريمة الإلكترونية هي تلك الجريمة المستحدثة التي توظف فيها التقنية المتطورة ويستطيع من خلالها الجاني ان يظل بعيدًا عن الرقابة الأمنية كما يستحيل على الأجهزة الشرطية والأمنية الوصول إليه أو الحصولب على الديل الجنائي الذي يثبت تورط الجاني في ارتكاب الجريمة.

**ثانيًا: خطورة الجرائم المعلوماتية**

يقع مليون ضحية يوميًا للجرائم المعلوماتية في مختلف بقاع العالم، أو 17 ضحية في كل ثانية، وفقًا لتقرير شركة "سمانتيك"، والذي ذكر إن كلفة الجرائم المعلوماتية عام 2022 بلغت (388) مليار دولار، أي أكثر من ثلاث جرائم في السوق السوداء (الماريجوانا والكوكايين والهروين) مجتمعةً والتي تبلغ (288) مليار دولار، ويشير التقرير نفسه والذي أجرى في 42 دولة- ومن ضمنهم دولة الإمارات، أن شخصين على الأقل كل عشرة من القاطنين في دولة الإمارات يقعان ضحية أنشطة الجريمة المعلوماتية في الدقيقة الواحدة، بفعل فيروسات وغيرها، وأن الإمارات خسرت مليار درهم في الأعوام الخمسة الماضية، وأن ثلاثة أرباع سكان دولة الإمارات تعرضوا لجريمة معلوماتية ويقول التقرير إن أغلبية الضحايا لم يتقدموا ببلاغات، ويفيد التقرير نفسه أن ثلثي البالغين حول العالم أي 69% كانوا ضحايا للجرائم المعلوماتية في حياتهم، وأظهرت النتائج أيضًا، أن 10% من البالغين تعرضوا لجرائم معلوماتية على هواتفهم النقالة. (السويدي،2013).

وبالرغم من حداثة الجرائم المعلوماتية نسبيًا، إلا أن دراسة للمباحث الفيدرالية أظهرت أنّ متوسط تكلفة جريمة الحاسب الآلي الواحدة حوالي ستمائة ألف دولار سنويًا، مقارنة بمبلغ ثلاثة آلاف دولار متوسط الجريمة الواحدة من جرائم السرقة بالإكراه سنويًا. وأنه من الصعوبة بمكان، تحديد أيّ الجرائم المعلوماتية المرتكبة هي الأكبر من حيث الخسائر، حيث لا يعلن الكثير عن مثل هذه الجرائم. ومن أكبر الجرائم المعلنة هي جريمة لوس انجلوس، حيث تعرضت أكبر شركات التأمين على الاستثمارات المالية (EFI) للإفلاس، وبلغت خسائرها (2.000.000.000) ملياري دولار أمريكي. (Caey,2014)

وتعتبر هذه الخسائر بسيطة نسبيًا مع الخسائر التي تسببها جرائم نشر الفيروسات والتي تضر بالأفراد والشركات وخاصة الشركات الكبيرة حيث ينتج عنها توقف أعمال بعض تلك الشركات نتيجة إتلاف قواعد بياناتها، وقد يصل الضرر في بعض المنشئات التجارية والصناعية إلى تكبد خسائر مادية قد تصل إلى مبالغ كبيرة وعلى سبيل المثال وصلت خسائر فيروس (Code Red) إلى ملياري دولار أمريكي في حين وصلت الأضرار المادية لفيروس الحب الشهير (8.7) مليار دولار واستمر انتشار الفيروس لخمسة أشهر وظهر منه (55) نوعًا (المطردي،2012).

**ثالثًا: خصائص الجريمة المعلوماتية**

تتميز الجريمة المعلوماتية بعدد من الخصائص الفريدة التي تفصح عن ذاتيتها منها:

- سهولة ارتكاب الجريمة بعيدًا عن الرقابة الأمنية .
- صعوبة التحكم في تحديد حجم الضرر الناجم عنها قياسًا بالجرائم التقليدية.
- مرتكبها من بين فئات متعددة تجعل من التنبؤ بالمشتبه بهم أمرًا صعبًا.
- تنطوي على سلوكيات غير مألوفة عن المجتمع.
- سهولة إتلاف الأدلة من قبل الجناة.
- لا تعترف بعنصر المكان والزمان فهي تتميز بالتباعد الجغرافي واختلاف التوقيتات بين الجاني والمجني عليه.
- جريمة ذات بعد دولي، فهي عابرة للحدود، وهو ما يثير تحديات قانونية، بل وسياسية بشأن مواجهتها لاسيما فيما يتعلق بإجراءات الملاحقة الجنائية.
- هي جريمة اللاعنف المادي، وجريمة الاكراه المعنوي.
- جريمة مستمرة في اغلب الأحوال، فما يحمله الجاني على الشبكة يصعب حذفه إلا بمعرفته.
- صعوبة إثباتها بالتوصل إلى الأدلة الرقمية والتحفظ عليها.
- جريمة متطورة، تستخدم أساليب تكنولوجية متنوعة تصعب عملية تتبعها فنيًا.
- عدم وجود مفهوم قانوني دولي مشترك لتعريف الجريمة الإلكترونية.
- قصور التعاون الدولي بين الدول في مجالات المكافحة.

**رابعًا: المجرم المعلوماتي**

يمكن تصنيف أنواع المجرم المعلوماتي الجناة في تلك الجرائم إلى أربعة فئات:

- الفئة الأولى: المستخدمون العاديون لأجهزة الحاسب الآلي.
- الفئة الثانية: الموظفون الساخطون على منظماتهم.
- الفئة الثالثة: أعضاء الجريمة المنظمة.
- الفئة الرابعة: فئة المتسللين او القراصنة.(Hackers) and (Crackers)

ففي نهاية الثمانينيات شاع اصطلاح (الهاكرز) المعبر عن مقتحمي النظم، لكن الحديث عن الدوافع لارتكاب هذه الأفعال ظل في أغلب الأحيان محصورًا بالحديث عن رغبة المخترقين في تجاوز إجراءات أمن المعلومات وفي إظهار تفوقهم التقني، وعن صغار السن المتفوقين الراغبين بالتحدي والمغامرة، وأنهم يؤدون خدمة في التوعية لأهمية معايير أمن النظم والمعلومات، لكن الحقيقة أن مغامري الأمس أصبحوا عتاة إجرام فيما بعد، إلى حد

إعادة النظر في تحديد سمات مرتكبي الجرائم وطوائفهم، وظهر المجرم المعلوماتي المتفوق المدفوع بأغراض جرمية خطيرة، القادر على ارتكاب أفعال تستهدف الاستيلاء على المال أو تستهدف التجسس او الاستيلاء على البيانات السرية الاقتصادية والاجتماعية والسياسية والعسكري (سالم،2000).

ويتسم المجرم المعلوماتي بعدد من السمات جعلت بعض النظريات التقليدية (كنظرية لمبروزو) تسقط أمامه...ومن هذه السمات:

- يتمتع بذكاء متقد، وملكات ذهنية حادة، منفتح، متطور.
- ذو مهارات فنية وتكنولوجية عالية ومحترف في التعامل مع شبكات الحاسبات.
- متخصص في الإجرام المعلوماتي، وصغير السن.
- توافر حالة العود.
- شخص غير عنيف لان تلك الجريمة لا تلجأ للعنف في ارتكابها.
- شخص اجتماعي له القدرة على التكيف مع الآخرين.
- حالته التعليمية، والثقافية، والاجتماعية تبعد عنه الشبهات (المجرمين ذوي الياقات البيضاء).

## المبحث الثاني: آليات مكافحة الجريمة المعلوماتية

**تمهيد:**

يستلزم تطور الإجرام التقني تطور في طرق إثبات الجريمة والتعامل معها، فالجرائم العادية يسهل -على سبيل المثال- تحديد مكان ارتكابها، بل أن ذلك يعتبر خطوة أولى وأساسية لكشف ملابسات الجريمة، في حين أنه من الصعوبة بمكان تحديد مكان وقوع الحادثة عند التعامل مع الجرائم المعلوماتية، لكون الرسائل والملفات الحاسوبية تنتقل من نظام إلى آخر في ثواني قليلة، كما أنه لا يقف أمام تنقل الملفات والرسائل الإلكترونية أي حدود دولية أو جغرافية، ونتيجة لذلك فإن تحديد أين حدثت وقائع الجريمة وما هي القوانين التي تخضع لها أمر في غاية الحساسية والتعقيد خاصة وأن كل دولة تختلف قوانينها عن الدولة الأخرى، فما يعتبر جريمة في الصين مثلًا قد لا يعتبر جريمة في فرنسا والعكس صحيح، بل أن الأمر يصل إلى حد اختلاف قوانين الولايات المختلفة داخل الدولة الواحدة كما الحال في الولايات المتحدة الأمريكية.

وهذا ما أستلزم أن تتضافر الجهود الدولية بين الدول بعضها البعض لتدعم وتتناغم مع الآليات الوطنية الحثيثة لمحاربة هذه الظواهر الإجرامية المستحدثة.

**المطلب الأول: التشريعات الدولية لمكافحة الجريمة المعلوماتية**

إن التعاون الدولي هام جدًا عند التعامل مع الجرائم المعلوماتية بأن هذه الجرائم هي جرائم عابرة للقارات ولا حدود لها، وفي المقابل فإن عدم التعاون الدولي سيؤدي إلى زيادة القيود على تبادل المعلومات عبر حدود الدول مما سيعطي الفرصة للمجرمين من الإفلات من العقوبة ومضاعفة أنشطتهم الإجرامية.

كما أن هذا التعاون سيطّور أساليب دولية متشابهة لتحقيق قانون جزائي وإجرائي وطني لحماية وسائل تقنية المعلومات المختلفة ويساهم في تحديد وتحديث آليات العمل الوطني لمكافحة هذه الطائفة من الجرائم المستحدثة. وسوف نستعرض ذلك من خلال:

أدى التطور التقني إلى ظهور جرائم جديدة لم يتناولها القانون الجنائي التقليدي مما أجمع معه مشرعي القانون الوضعي في الدول المتقدمة على جسامة الجريمة المعلوماتية والتهديدات التي يمكن أن تنشأ عن استخدام وسائل تقنية المعلومات المختلفة، ودفع هذا الفقه إلى دراسة هذه الظاهرة الإجرامية الجديدة وما أثارته من إشكاليات قانونية حول تطبيق القانون الجنائي.

ولقد أدركت الدول أهمية التعاون الدولي، وأحست بأنه أمر محتِّمٌ لتجاوز تحديات الجرائم المعلوماتية، فعمد الكثير منها إلى عقد اتفاقيات إقليمية ودولية لتسهيل مهمة تفعيل التعاون الدولي في مجال مكافحة الجريمة الإلكترونية والتحقيق فيها.

**أولًا: تطورتجريم الجريمة المعلوماتية في بعض التشريعات المقارنة**

تعتبر السويد أول دولة تسن تشريعات خاصة بالجرائم المعلوماتية حيث صدر قانون البيانات السويدي عام 1973 الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي، إضافة إلى شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشرع عليها.(Mowshowitz,2013).

تبعت الولايات المتحدة الأمريكية السويد حيث شرعت قانونًا خاصًا بحماية أنظمة الحاسب الآلي 1976، وفي عام 1986 صدر قانونًا تشريعًا يحمل الرقم (1213)، عرّف فيه جميع المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية، كما وضعت المتطلبات الدستورية اللازمة لتطبيقه، وعلى إثر ذلك قامت الولايات الداخلية بإصدار تشريعاتها الخاصة بها للتعامل مع هذه الجرائم، وقد خولت وزارة العدل الأمريكية في عام (2000م) خمسة جهات منها مكتب التحقيقات الفيدرالي (FBI) للتعامل مع الجرائم المعلوماتية.(Yvonne,2007)

وأتت بريطانيا كثالث دولة تسن قوانين خاصة بالجرائم المعلوماتية حيث أقرت قانون مكافحة التزوير والتزييف عام 1981، الذي شمل في تعاريفه الخاصة تعريف أداة التزوير وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى.

وتطبق كندا قوانين متخصصة ومفصلة للتعامل مع الجرائم المعلوماتية حيث عدلت في عام 1985 قانونها الجنائي، بحيث شمل قوانين خاصة بجرائم الحاسب الآلي والإنترنت، كما شمل القانون الجديد تحدد عقوبات المخالفات الحاسوبية، وجرائم التدمير، أو الدخول غير المشروع لأنظمة الحاسب الآلي، كما وضّح فيه صلاحيات جهات التحقيق كما جاء في قانون المنافسة (The Competition Act) مثلًا ما يخول لمأمور الضبط القضائي متى ما حصل على أمر قضائي حق تفتيش أنظمة الحاسب الآلي والتعامل معها وضبطها (حمودة،2003).

وسنّت الدنمارك في عام 1985 أول قوانينها الخاصة بالجرائم المعلوماتية، والتي شملت في فقراتها العقوبات المحددة لجرائم الحاسب الآلي كالدخول غير المشروع إلى الحاسب الآلي، أو التزوير، أو أي كسب غير مشروع، أو التلاعب غير المشروع ببيانات الحاسب الآلي، كإتلافها أو تغييرها أو الاستفادة منها (الطوالبة،2018).

وكانت فرنسا من الدول التي اهتمت بتطوير قوانينها الجنائية للتوافق مع المستجدات الإجرامية حيث أصدرت في عام 1988 القانون رقم (19-88) الذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لها، كما تم عام 1994 تعديل قانون العقوبات لديها ليشمل مجموعة جديدة من القواعد القانونية الخاصة بالجرائم المعلوماتية وأوكل إلى النيابة العامة سلطة التحقيق فيها بما في ذلك طلب التحريات وسماع الأقوال (بن يونس،2004).

أما في هولندا فلقاضي التحقيق الحق بإصدار أمره بالتصنت على شبكات الحاسب الآلي متى ما كانت هناك جريمة خطيرة (المري،2018).

كما يجيز القانون الفنلندي لمأمور الضبط القضائي حق التنصت على المكالمات الخاصة بشبكات الحاسب الآلي (المراغي،2017).

وتعطي القوانين الألمانية الحق للقاضي بإصدار أمره بمراقبة اتصالات الحاسب الآلي وتسجيلها والتعامل معها وذلك خلال مدة أقصاها ثلاثة أيام (المراغي،2017).

وفي اليابان قوانين خاصة بجرائم الحاسب الآلي والإنترنت، ونصت تلك القوانين على انه لا يلزم مالك الحاسب الآلي المستخدم في جريمة ما التعاون مع جهات التحقيق أو إفشاء كلمات السر التي يستخدمها إذا ما كان ذلك سيؤدي إلى إدانته، كما أقرت عام 1991 شرعية التنصت على شبكات الحاسب الآلي للبحث عن دليل (سامة،2000).

كما يوجد في المجر وبولندا قوانين خاصة بجرائم الحاسب الآلي والإنترنت توضح كيفية التعامل مع تلك الجرائم ومع المتهمين فيها، وتعطي تلك القوانين المتهم الحق في عدم طبع سجلات الحاسب الآلي أو إفشاء كلمات السر أو الأكواد الخاصة بالبرامج، كما تعطي الشاهد أيضًا الحق في الامتناع عن طبع المعلومات المسترجعة من الحاسب الآلي متى ما كان ذلك إلى إدانته أو إدانة أحد أقاربه. بل تذهب القوانين الجنائية المعمول بها في بولندا إلى أبعد من هذا حيث أنها تنص على ألا يقابل ذلك أي إجراء قسري أو تفسيره بما يضر المتهم (المطردي،2012).

ويعد قانون تقنية المعلومات الهندي لسنة 2000 من أكثر القوانين تفصيلًا ووضوحًا، وجاء في 13 فصلًا تضم 94 مادة تحدد نطاق سريان القانون وتعرف أكثر من 35 مصطلح وعبارة.

كذلك سارعت دولة الامارات العربية المتحدة إلى سن القانون رقم (2) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات لضمان أمن وحماية المجتمع،ثم جاء مرسومًا بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، وتضمن تعديلات لما ورد في القانون الاتحادي رقم (2) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات، الذي ألغي بموجب المرسوم القانون المذكور ثم صدر المرسوم بالقانون الاتحادي رقم 34 لسنة 2021 في شان مكافحة الشائعات والجرائم الإلكترونية

وفي المملكة السعودية أقر مجلس الوزراء بالقرار رقم 79 لعام 1428 هـ نظام مكافحة الجرائم الإلكترونية، الذي يهدف إلى الحد من نشوء جرائم المعلوماتية، وذلك بتحديد تلك الجرائم والعقوبات المقررة لها.

أما في مصر ففي عام 2011 تم إعداد مشروع قانون جزائي خاص لمكافحة الجريمة المعلوماتية، كما يطبق قانون التجارة الإلكترونية وقانون التوقيع الإلكتروني وقانون الاتصالات (المري،2018).

إلا أنه من المعلوم أن تطوير القوانين الجنائية وتحديثها أمر يستغرق بعض الوقت، فهناك تعديلات كثيرة مطلوب ادخالها على التشريعات التي تتعامل مع الجريمة، لكي تأخذ في الاعتبار المعطيات الجديدة التي نشأت عن استخدام وسائل تقنية المعلومات المتسارعة.

هذا وأن أجهزة إنفاذ القانون لا تستطيع تجاوز حدودها الإقليمية لممارسة ولايتها على المجرمين الفارين، لذا كان لابد من إيجاد مبادئ دولية للتعاون بين الدول أعضاء المجتمع الدولي، ومن أهم هذه المبادئ:

- التعاون الدولي القضائي.
- التعاون الدولي في تسليم المجرمين.

- التعاون الدولي في مجال التدريب وتبادل الخبرات.

ففي مجال الجرائم المعلوماتية فإن بطء الإجراءات الرسمية يجازف بفقدان الأدلة، وقد تكون بلدان متعددة متورطة في الأمر، لذا تشكل متابعة وحفظ سلسلة الأدلة تحديًا كبيرًا، بل حتى الجرائم "المحلية" قد يكون لها بعد دولي، وربما تكون هناك حاجة إلى طلب المساعدة من جميع البلدان التي مرت الهجمة من خلالها.

وإذا كانت هناك جريمة واضحة تستحق التحقيق بالفعل، فقد تكون هناك حاجة إلى مساعدة من السلطات في البلد الذي كان منشأ الجريمة، أو من السلطات في البلد أو البلدان التي عبر من خلالها النشاط المجرَّم وهو في طريقه إلى الهدف، أو حيث قد توجد أدلة الجريمة، وهناك عنصران أساسيان للتعاون:

**المساعدة غير الرسمية من محقق لآخر، والمساعدة الرسمية المتبادلة.**

وقد تكون "المساعدة غير الرسمية" أسرع إنجازًا، وهي الوسيلة المفضلة للنهج حين لا تكون هناك حاجة إلى صلاحيات إلزامية (أي أوامر تفتيش أو طلب تسليم المجرم). وهي تقوم على وجود علاقات عمل جيدة بين أجهزة شرطة البلدان المعنية، وتولد نتيجة الاتصالات التي جرت مع الوقت في مسار المؤتمرات، وزيارات المجاملة، والتدريب المشترك، والتحقيقات المشتركة السابقة.

ومن ناحية أخرى فإن "المساعدة الرسمية المتبادلة"- ورغم أنها عملية أكثر إرهاقًا –إلا أنه يتم اللجوء إليها عادة في التحقيقات التي تتطلب تبادل الوثائق الرسمية، وهي تشترط في الغالب الأعم أن تكون الجريمة المعنية على درجة معينة من القسوة، وأن تشكل جريمة في كل من البلدان الطالبة والموجه إليها الطلب، ويشار إلى هذا الأمر الأخير باعتباره "تجريمًا مزدوجًا،" أو أن تكون كلا الدولتين موقعتين على اتفاقيات دولية بهذا الشأن.

**لذلك يمكن القول ان التشريعات الدولية في مجال مكافحة الجرائم المعلوماتية تساهم في تضييق الخناق على التنظيمات الاجرامية التي تستخدم التقنية في ارتكاب مختلف الجرائم لكون التشريعات الدولية تضع الآليات المناسبة للتعاون الثنائي والجماعي بين الدول في مكافحة الجرائم.**

**ثانيًا: المؤتمرات الدولية**

مؤتمر دول أسيا والباسفيك، المنعقد 1989، الذي لفت النظر إلى نتائج التطور والتقدم التكنولوجي فيما يتعلق بالجريمة المعلوماتية واقترح تشجيع اتخاذ إجراء دولي حيال هذه الجريمة.

أما المؤتمر الدولي السادس للجمعية المصرية للقانون الجنائي عام (1993م) فقد تناول موضوع جرائم الحاسب الآلي والجرائم الأخرى في مجال تكنلوجيا المعلومات وتوصل الي توصيات احاطت بجوانب مشكلة جرائم الحاسب الآلي، ويكتسب أهميته أيضًا لاعتباره تحضيرًا للمؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات الذي عقد في البرازيل عام 1994 الذي تناول ذات الموضوع (البشري،2000).

والمؤتمر الثامن للأمم المتحدة لمنع الجريمة ومعاملة المجرمين المنعقد في كوبا 1990 الذي ناشد في قراره المتعلق بالجرائم ذات الصلة بالحاسب الآلي الدول الأطراف إلى ضرورة تكثيف جهودها لمكافحة الجرائم المعلوماتية من عدة أوجه

بالإضافة لمؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين الذي انعقد في فيينا أيام 10 – 17 ابريل 2000، وكذلك خلال مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية عام 2019 (أحمد،2007).

**ثالثًا: الاتفاقيات الدولية**

عالجت العديد من الاتفاقيات موضوع الجرائم المعلوماتية والتي بدأت باتفاقية فينا لسنة 1988، والتي حثت الدول على عقد الاتفاقيات لتسهيل مهمة مكافحة في هذه الجرائم، ومن ذلك الحين والدول تعمل على عقد الاتفاقيات الدولية والإقليمية والثنائية ونظرًا لتعددها فأننا سنكتفي بالإشارة لأهم اتفاقية دولية وإقليمية في هذا المجال وهي: اتفاقية بودابست لسنة 2001 بشأن الإجرام الكونيCybercrime ، والتي تشكل نصوصها منظومة تعاون دولي تتسم بالمرونة والفعالية وتعمل على إحداث تقارب بين التشريعات الجنائية الخاصة بهذه الجرائم وتكفل استخدام الوسائل الفعالة في البحث والتحقيق وملاحقة مرتكبيها وما يتعلق بالنصوص الخاصة بالتعاون الدولي، وقد أعلن المجلس الأوربي مشروع هذه الاتفاقية في 27 ابريل 2000 ، وأكد المجلس المذكور أن الاعتداءات الحديثة على مواقع الإنترنت، هي التي لفتت نظر المجتمع الدولي إلى المخاطر والتحديات التي تواجهها الشبكة الدولية للمعلومات وشبكات الحاسب الآلي، وأن الجرائم المعلوماتية أصبحت تهدد بشكل واضح التجارة والمصالح الحكومية، خاصة مع الأخذ في الاعتبار الطابع الدولي الذي يميز هذه النوعية من الجرائم، وبعد سنة ونصف تقريبًا من المناقشات والتعديلات على هذا المشروع تمّ التوقيع على اتفاقية بودابست بتاريخ 23 نوفمبر 2001 بشأن الإجرام الكوني، أو المعلوماتي إيمانًا من الدول الأعضاء في المجلس الأوربي والدول الأخرى الموقعة على هذه الاتفاقية بضرورة مواجهة هذا النمط الجديد من الإجرام (Parker,2007 ).

ونشير إلى أن هذه الاتفاقية تتكون من ثمان وأربعين مادة موزعة على أربعة أبواب، يعالج الباب الأول منها استخدام المصطلحات، أما الباب الثاني فهو مخصص للإجراءات الواجب اتخاذها على المستوي الوطني، سواء من الناحية الموضوعية أو الإجرائية، أما الباب الثالث فقد تم تخصيصه للتعاون الدولي في حين يتعرض الباب الرابع للشروط الختامية.

ومن أهم الاتفاقيات الإقليمية في هذا المجال هي: "الاتفاقية العربية لمكافحة جرائم تقنية المعلومات" لسنة 2012، والذي قامت بأعدادها اللجنة المشتركة لمجلسي وزراء الداخلية والعدل العرب، والتي تهدف إلى تعزيز التعاون بين الدول العربية في مجال مكافحة الجرائم المعلوماتية حفاظًا على أمن وسلامة المجتمعات العربية، وجاءت في عدد 43 مادة، ومن أهم ما جاء بها أن على الدول الأعضاء وفقاً لنظامها ان تكفل وجود جهاز متخصص قادر على مكافحة هذه الجرائم، متفرغ على مدار الساعة لتقديم المساعدة الفورية المطلوبة من أي دولة عضو أخرى (عياد،20013).

ويظهر أن مجلس وزراء الداخلية العرب قد حرص على الاهتمام العربي بمكافحة الجرائم المعلوماتية خاصة أن البيئة الدولية صارت متسارعة ومتداخلة وتحتاج إلى التنسيق المستمر لمكافحة جرائم صارت تشكل تهديدًا مباشرًا للأمن العربي.

**رابعًا: المنظمات الدولية**

تعمل العديد من المنظمات الدولية والإقليمية في مجال الحد من أخطار الجرائم المعلوماتية ومن أهمها:

- منظمة الأمم المتحدة.
- منظمة اليونسكو.
- المنظمة العالمية للملكية الفكرية.
- منظمة التجارة العالمية.
- الانتربول.
- الايوروبول (وكالة تطبيق القانون الأوروبية).
- المكتب العربي للشرطة الجنائية.

ولكن، وعلى الرغم من ضرورة التعاون الدولي وتضافر الجهود من أجل تفعيله، إلا أن هناك العديد من العقبات التي تعترض سبيله من أبرزها:

- عدم وجود اتفاق عام بين الدول على مفهوم الجرائم المعلوماتية.
- عدم وجود توافق بين قوانين الإجراءات الجنائية للدول بشأن التحقيق في تلك الجرائم.
- النقص الظاهر في مجال الخبرة لدى الشرطة وجهات الإدعاء والقضاء.

**المطلب الثاني: جهود المنظمة الدولية للشرطة الجنائية في مكافحة الجريمة المعلوماتية**

تمثل الجريمة إحدى القضايا الرئيسية في الكثير من دول العالم وهي تشغل بال الحكومات والمختصين والأفراد على حد سواء، ولقد أثبت الواقع العملي أن الدولة -أي دولة- لا تستطيع بجهودها المنفردة مكافحة الجريمة مع هذا التطور الكبير في كافة ميادين الحياة. فنتيجة للتطور الملموس في الاتصالات وتكنولوجيا المعلومات وظهور الإنترنت والانتشار الواسع والسريع لها أدى إلى ظهور أشكال وأنماط جديدة من الجرائم منها الجرائم المتعلقة بشبكة الإنترنت وهي نوعٌ من الجرائم المعلوماتية التي باتت تشكل خطرًا لا على سرية النظم الحاسوبية أو سلامتها أو توافرها فحسب بل تعدت إلى أمن البنى الأساسية الحرجة.

ومع تميزها بالعالمية وبكونها عابرة للحدود فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي الجنائي، بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة، وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالإنترنت وتعميمها.

فمثلًا في جرائم البث والنشر الفيروسي قد يكون مرتكب الهجوم يحمل جنسية دولة ما ويشن الهجوم الفيروسي من حواسيب موجودة في دولة أخرى وتقع الآثار المدمرة لهذا الهجوم في دولة ثالثة. فمن البديهي أن تقف مشاكل الحدود والولايات القضائية عقبة أمام اكتشاف هذه الجرائم ومعاقبة مرتكبيها، لذا فإن التحقيقات في الجرائم المتصلة بالحاسب الآلي وملاحقتها قضائيًا تؤكد على أهمية المساعدة القانونية المتبادلة بين الدول ، حيث يستحيل على الدولة بمفردها القضاء على هذه الجرائم الدولية العابرة للحدود، لأن جهاز الشرطة في هذه الدولة أو تلك لا يمكنه تعقب المجرمين وملاحقتهم إلا في حدود الدولة التابع لها بمعنى آخر أنه متى ما فرّ المجرم خارج حدود الدولة يقف الجهاز الشرطي عاجزًا.

لذلك أصبحت الحاجة ماسة إلى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة وتتعاون من خلاله أجهزة الشرطة في الدول المختلفة، خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنة بالإضافة إلى تعقب المجرمين الفارين من وجه العادلة.

منذ عام 2015 اعتمدت المنظمة الدولية للشرطة الجنائية (الإنتربول) برنامجًا لمكافحة الجرائم المعلوماتية نجح إلى اليوم في اعتقال آلاف المجرمين حول العالم، إلا أن التطور السريع للتكنولوجيا يطرح تحديات واسعة وتساؤلات عما إذا كان الإنتربول سينجح في مواجهة هذه التحديات الأمنية.

لقد قام الانتبول بالاشراف على سيناريو افتراضي حيث أشرف 43 محققًا في الجرائم المعلوماتية من 23 دولة عضوة في الانتربول بالتحقيق في محاكاة هجوم إلكتروني على بنك تم إطلاقه من خلال جهاز ضمن إنترنت الأشياء، وفي هذا السيناريو هاجم مجرمو الإنترنت أحد البنوك في محاولة لسرقة مبالغ كبيرة من المال، وقام المحققون بتحليل أجهزة الكمبيوتر الخاصة بالبنك لتحديد التاريخ والوقت والملفات التي تم فيها تثبيت البرامج الخبيثة المجرمين (أبو الحاج،2018).

مع ارتباط العالم رقميًا أكثر من أي وقت مضى، يستفيد المجرمون من هذا التحول عبر الإنترنت لاستهداف نقاط الضعف في الأنظمة والشبكات والبنية التحتية عبر الشبكة الإلكترونية وأصبح التصيد الاحتيالي وبرامج الفدية وخروقات البيانات مجرد أمثلة قليلة على التهديدات الإلكترونية المتزايدة في عالم اليوم وبينما تظهر أنواع جديدة من الجرائم المعلوماتية في كل وقت يتسم مجرمو الإنترنت بالمرونة والتنظيم ويستغلون التقنيات الجديدة ويصممون هجماتهم ويتعاونون بطرق جديدة لتنفيذ أهدافهم الخبيثة العابرة للحدود مستهدفين ضحاياهم من الأفراد والشركات والبنية التحتية للدول التي تنتمي إلى ولايات قضائية متعددة ما طرح تحديات عدة أمام التحقيقات والملاحقات القضائية.

ولهذا يضع الإنتربول تحت تصرف خدمات ومنصات دوله الأعضاء البالغ عددها 195 جهوده لمكافحة الجريمة المعلوماتية حيث يوفر قدرات شرطية لكل البلدان الأعضاء وتنسيق عمليات إنفاذ القانون بينها ويقدم منصات آمنة لتبادل البيانات والتحليل والتدريب من أجل الحد من التهديدات السيبرانية ومنع الجرائم المعلوماتية واكتشافها والتحقيق فيها وتعطيلها.

ويتمثل النطاق الأساس لبرنامج الإنتربول لمكافحة الجرائم الإلكترونية في استهداف الجريمة المعلوماتية والجرائم المرتكبة ضد أجهزة الكمبيوتر وأنظمة المعلومات حيث يكون الهدف هو الوصول غير المصرح به إلى جهاز كمبيوتر وزرع برامج خبيثة وضارة حيث يلعب الإنتربول بمدى انتشاره العالمي دورًا حيويًا في بناء شراكات بين القطاعات وتمكين التعاون الدولي في مجال إنفاذ القانون، كما ينظم الإنتربول حملات توعية منتظمة لتسليط الضوء على الأشكال الرئيسة للجرائم الإلكترونية وتقديم نصائح حول كيفية البقاء في أمان.

ونجح الإنتربول في تنسيق الجهود بين أطراف متعددة حول العالم لإحباط الجرائم المعلوماتية واعتقال منفذيها ومحاكمتهم، ففي أفريقيا على سبيل المثال، جمعت عملية "الطفرة الإفريقية في يوليو (تموز) من العام الماضي، مسؤولي إنفاذ القانون من 27 دولة، وعملوا معًا لمدة أربعة أشهر في شأن المعلومات الاستخباراتية القابلة للتنفيذ التي قدمها شركاء الإنتربول من القطاع الخاص، وركزت هذه المعلومات على فرص منع الجرائم الإلكترونية واكتشافها والتحقيق فيها وتعطيلها من خلال أنشطة منسقة تستخدم منصات وأدوات وقنوات الإنتربول.

وركزت هذه العملية على مجرمي الإنترنت والبنية التحتية للشبكات المعرضة للخطر في إفريقيا مما سمح للدول الأعضاء بتحديد أكثر من 1000 عنوان خبيث وأسواق الويب المظلمة والجهات الفاعلة في مجال التهديد الفردي، وتعزيز التعاون بين الإنتربول وأفريبول والدول الأعضاء والمساهمة في التواصل وأسفرت الجهود عن إزالة السوق المظلمة في إريتريا، والتحقيق في عمليات الاحتيال المتعلقة بالعملات المشفرة في الكاميرون، واعتقال مشغلي البنية التحتية الإلكترونية الضارة المستخدمة في شبكات الروبوتات، وحملات التصيد والابتزاز عبر الإنترنت (ابوالحاج،2018).

## الخاتمة:

ثمة تخوف كبير على الصعيد العالمي من مستقبل الجرائم المعلوماتية ذلك أن هذه الجرائم يمكن أن يستغلها مرتكبوها في ضرب البنى التحتية لأنظمة المعلومات في العالم أجمع وذلك بالنظر إلى الزيادة المطردة في حالات تعرض المؤسسات الاقتصادية والمالية الضخمة لهجمات دون تعريض الجناة لخطر الضبط أو الملاحقة، وفي مواجهة ذلك فمن الواجب على كافة الدول أن تسخر مؤسساتها للتصدي لهذا الخطر الذي لا يحتاج من الأدوات سوى فأرة كمبيوتر ولا يحتاج من جهد بغية التسبب بالتدمير الشامل سوى إلى نقرة خفيفة على هذه الفأرة.

### أولًا: النتائج

- ساهمت الثورة التكنولوجية في انتشار الجرائم المعلوماتية عبر مختلف دول العالم.
- تشكل الجرائم المعلوماتية تحديًا أمنيًا جديدًا أمام الأجهزة الشرطية والأمنية.
- من الصعوبة التعرف على مرتكبي الجرائم المعلوماتية الذين يمتلكون خبرات كبيرة في ارتكاب أنواع شتى من الجرائم.
- هناك جهودًا دولية لمكافحة الجرائم المعلوماتية من خلال الاتفاقيات الدولية والمنظمة الدولية للشرطة الجنائية.

### ثانيًا: التوصيات

- اتخاذ إجراءات تشريعية صارمة تتماشى مع هذا النوع من الجرائم المعلوماتية تأخذ بعين الاعتبار الطبيعة الخاصة لهذه الجرائم.
- مضاعفة التنسيق والتعاون بين الدول على المستويات الإقليمية والدولية.
- ضرورة التعاون الدولي في مجال مكافحة الجرائم المعلوماتية من حيث مواكبة التطور الحاصل في مجال التكنولوجيا الحديثة.
- تفعيل الدور الوقائي من خلال المؤسسات التوعوية (الأسرة، المدرسة، الجامعة، مواقع التواصل الاجتماعي، وسائل الإعلام) وذلك بالتوعية بخطورة هذه الجرائم على الأسرة والمجتمع والدولة.

## المراجع:

### أولًا: المراجع العربية


أبو الحجاج، يوسف. (2018). *أشهر جرائم الحاسب والإنترنت*. دار الكتاب العربي للنشر والتوزيع، القاهرة.

احمد، هلالي عبد الله. (2007). *اتفاقية بودابست لمكافحة الجرائم المعلوماتية (معلقاً عليها)*. دار النهضة العربية، الطبعة الأولى، القاهرة.

المراغي، أحمد عبد الاله.(2017). *الجريمة الإلكترونية ودور القانون الجنائي في الحد منها- دراسة تحليلية تأصيلية مقارنة*. المركز القومي لإلصدارات القانونية، القاهرة.

البشري، محمد الأمين. (2000). *التحقيق في جرائم الحاسب الآلي*. بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، 1 – 3 مايو، كلية الشريعة والقانون، الإمارات.

بن يونس، عمر محمد أبوبكر. (2004). *الجرائم الناشئة عن استخدام الإنترنت*. دار النهضة العربية، القاهرة.

الجملي، طارق محمد. (2009). *الدليل الرقمي في الإثبات الجنائي*. بحث مقدم الي المؤتمر المغاربي الأول للمعلوماتية والقانون، اكاديمية الدراسات العليا، 28-29 أكتوبر، طرابلس.

حجازي، عبد الفتاح بيومي. (2005). *جرائم الكمبيوتر والإنترنت*. دار الكتب القانونية، القاهرة، 2005، ص1 وما بعدها.

حجازي، عبد الفتاح بيومي. (2009). *الدليل الرقمي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة معمقة في جرائم الحاسب الآلي والإنترنت*. بهجت للطباعة والتجليد، القاهرة.

حمودة، علي محمود علي. (2003). *الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي*. بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، 26-28 أبريل، أكاديمية شرطة دبي، الامارات.

المري، راشد محمد. (2018). *الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر: دراسة مقارنة*. دار النهضة العربية القاهرة.

رستم، هشام فريد. (1992). *قانون العقوبات ومخاطر تقنية المعلومات*. مكتبة الآلات الحديثة، أسيوط.

الرشيدي، محمود. (2011). *العنف في جرائم الإنترنت*. الدار المصرية اللبنانية، القاهرة.

سالم، عمر. (2000). *المراقبة الإلكترونية طريقة حديثة لتنفيذ العقوبة السالبة للحرية خارج السجن*. دار النهضة العربية، الطبعة الأولي، القاهرة.

سلامة، مأمون محمد. (1971). *الإجراءات الجنائية في التشريع الليبي- الجزء الأول*. منشورات الجامعة الليبية، الطبعة الأولى، بنغازي..

السويدي ،جمال سند. (2013). *وسائل التواصل الاجتماعي ودورها في التحولات المستقبلية-من القبيلة إلى الفيسبوك*. بدون ناشر، الطبعة الأولى.

الشنيفي، عبد الرحمن. (2007). *سياسة أمن المعلومات في الأمن العام*. بحث مقدم إلى مؤتمر الجرائم الإلكترونية- الملامح والابعاد، كلية الملك فهد للعلوم الأمنية، 23-24 أبريل، الرياض.

الصغير، جميل عبد الباقي. (2001). *الإنترنت والقانون الجنائي*. دار النهضة العربية، القاهرة.

الطوالبة، علي حسن. مشروعية الدليل الرقمي المستمد من التفتيش الجنائي- دراسة مقارنة، www.startimes.com/f.aspx%3Ft%3D30245909

عمر، معن خليل. (2012). *جرائم مستحدثة*. دار وائل للنشر، عمان.

عوض، محمد محي الدين. (1993). *مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)*. ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في القاهرة 25 -28 أكتوبر.

عياد، سامي. (2013). *الجريمة المعلوماتية وإجرام الإنترنت*. دار الفكر الجامعي، الإسكندرية.

الفنتوخ، عبد القادر. (2012). *الجريمة في الإنترنت وطرق الحماية منها*. مكتبة العبيكان، الرياض.

حشمت، قاسم. (2005). *الاتصال العلمي في البيئة الإلكترونية*. دار الغريب، القاهرة.

قشقوش، هدى حامد. (1992). *جرائم الحاسب الإلكتروني في التشريع المقارن*. دار النهضة العربية، القاهرة.

كامل، عفيفي. (د،ت). *جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية- ودور الشرطة والقانون*. منشأة المعارف، الإسكندرية.

محمد سلامة، مأمون. (1971). *الإجراءات الجنائية في التشريع الليبي*. الجزء الأول، منشورات الجامعة الليبية كلية الحقوق، الطبعة الأولى.

مصطفى، خالد حامد. (2013). المسئولية الجنائية لناشري الخدمات التقنية ومقدميها عن سوء استخدام شبكات التواصل الاجتماعي. *مجلة رؤى الاستراتيجية*: 1(2).

المطردي، مفتاح بوبكر. (2012). *الجريمة الإلكترونية والتغلب على تحدياتها*. بحث مقدم إلي المؤتمر الثالث رؤساء المحاكم العليا في الدول العربية.


### ثانيًا: المراجع الأجنبية


Caey, E. (2007). *Computer Crime Investigation*. Academic Press California, California.

Caey, E. (2007). *Digital Evidence and Computer Crime*. Academic Press, 3rd ed California.

Leiner, B. M., Vinton G. C. (2013). *Brief History of the Internet*, at http://www.isoc.org/internet-history/brief.html

Mowshowitz, A. (2010). On the Theory of Virtual Organization. *Systems Research and Behavioral Science*, 14(6),

Parker, D. (2007). *Fighting Computer Crime: A New Framework for Protecting* Information. Butterworth Publishers, United States.

Yvonne, J. (2007). *Killed by the Internet" Crime online (ed) Willan pub*. U.K.

**ثالثًا: رومنة المراجع العربية:**

Abw Alhjaj, Ywsf. (2018). Ashhr Jra'em Alhasb Walentrnt. Dar Alktab Al'erby Llnshr Waltwzy'e, Alqahrh.

Ahmd, Hlaly 'Ebd Allh. (2007). Atfaqyh Bwdabst Lmkafhh Aljra'em Alm'elwmatyh (M'elqaan 'Elyha). Dar Alnhdh Al'erbyh, Altb'eh Alawla, Alqahrh.

Albshry, Mhmd Alamyn. (2000). Althqyq Fy Jra'em Alhasb Alaly. Bhth Mqdm Ela M'etmr Alqanwn Walkmbywtr Walentrnt, 1 – 3 Mayw, Klyh Alshry'eh Walqanwn, Alemarat.

Alfntwkh, 'Ebd Alqadr. (2012). Aljrymh Fy Alentrnt Wtrq Alhmayh Mnha. Mktbh Al'ebykan, Alryad.

Aljmly, Tarq Mhmd. (2009). Aldlyl Alrqmy Fy Alethbat Aljna'ey. Bhth Mqdm Aly Alm'etmr Almgharby Alawl Llm'elwmatyh Walqanwn, Akadymyh Aldrasat Al'elya, 28-29 Aktwbr, Trabls.

Almraghy, Ahmd 'Ebd Alalh.(2017). Aljrymh Aellktrwnyh Wdwr Alqanwn Aljna'ey Fy Alhd Mnha- Drash Thlylyh Tasylyh Mqarnh. Almrkz Alqwmy Lelsdarat Alqanwnyh, Alqahrh.

Almry, Rashd Mhmd. (2018). Aljra'em Alelktrwnyh Fy Zl Alfkr Aljna'ey Alm'easr: Drash Mqarnh. Dar Alnhdh Al'erbyh Alqahrh.

Almtrdy, Mftah Bwbkr. (2012). Aljrymh Alelktrwnyh Waltghlb 'Ela Thdyatha. Bhth Mqdm Ely Alm'etmr Althalth R'esa' Almhakm Al'elya Fy Aldwl Al'erbyh.

Alrshydy, Mhmwd. (2011). Al'enf Fy Jra'em Alentrnt. Aldar Almsryh Allbnanyh, Alqahrh.

Alsghyr, Jmyl 'Ebd Albaqy. (2001). Alentrnt Walqanwn Aljna'ey. Dar Alnhdh Al'erbyh, Alqahrh.

Alshnyfy, 'Ebd Alrhmn. (2007). Syash Amn Alm'elwmat Fy Alamn Al'eam. Bhth Mqdm Ela M'etmr Aljra'em Alelktrwnyh-Almlamh Walab'ead, Klyh Almlk Fhd Ll'elwm Alamnyh, 23-24 Abryl, Alryad.

Alswydy ,Jmal Snd. (2013). Wsa'el Altwasl Alajtma'ey Wdwrha Fy Althwlat Almstqblyh-Mn Alqbylh Ela Alfysbwk. Bdwn Nashr, Altb'eh Alawla.

Altwalbh, 'Ely Hsn. Mshrw'eyh Aldlyl Alrqmy Almstmd Mn Altftysh Aljna'ey- Drash Mqarnh, Bhth Mnshwr 'Ela Almwq'e Www.Startimes.Com/F.Aspx%3ft%3d30245909

Bn Ywns, 'Emr Mhmd Abwbkr. (2004). Aljra'em Alnash'eh 'En Astkhdam Alentrnt. Dar Alnhdh Al'erbyh, Alqahrh.

'Emr, M'en Khlyl. (2012). Jra'em Msthdthh. Dar Wa'el Llnshr, 'Eman.

'Ewd, Mhmd Mhy Aldyn. (1993). Mshklat Alsyash Aljna'eyh Alm'easrh Fy Jra'em Nzm Alm'elwmat (Alkmbywtr). Wrqh 'Eml Mqdmh Ela Alm'etmr Alsads Lljm'eyh Almsryh Llqanwn Aljna'ey Almn'eqd Fy Alqahrh 25 -28 Aktwbr.

'Eyad, Samy. (2013). Aljrymh Alm'elwmatyh Wejram Alentrnt. Dar Alfkr Aljam'ey, Alesskndryh.

Hjazy, 'Ebd Alftah Bywmy. (2005). Jra'em Alkmbywtr Walentrnt. Dar Alktb Alqanwnyh, Alqahrh, 2005, S1 Wma B'edha.

Hjazy, 'Ebd Alftah Bywmy. (2009). Aldlyl Alrqmy Waltzwyr Fy Jra'em Alkmbywtr Walentrnt, Drash M'emqh Fy Jra'em Alhasb Alaly Walentrnt. Bhjt Lltba'eh Waltjlyd, Alqahrh.

Hmwdh, 'Ely Mhmwd 'Ely. (2003). Aladlh Almthslh Mn Alwsa'el Alelktrwnyh Fy Etar Nzryh Alethbat Aljna'ey. Bhth Mqdm Llm'etmr Al'elmy Alawl Hwl Aljwanb Alqanwnyh Walamnyh Ll'emlyat Alelktrwnyh, 26-28 Abryl, Akadymyh Shrth Dby, Alamarat.

Hshmt, Qasm. (2005). Alatsal Al'elmy Fy Alby'eh Alelktrwnyh. Dar Alghryb, Alqahrh.

Kaml, 'Efyfy. (D,T). Jra'em Alkmbywtr Whqwq Alm'elf Walmsnfat Alfnyh- Wdwr Alshrth Walqanwn. Mnshah Alm'earf, Alesskndryh.

Mhmd Slamh, Mamwn. (1971). Alejra'at Aljna'eyh Fy Altshry'e Allyby. Aljz' Alawl, Mnshwrat Aljam'eh Allybyh Klyh Alhqwq, Altb'eh Alawla.

Mstfa, Khald Hamd. (2013). Alms'ewlyh Aljna'eyh Lnashry Alkhdmat Altqnyh Wmqdmyha 'En Sw' Astkhdam Shbkat Altwasl Alajtma'ey. Mjlh R'ea Alastratyjyh: 1(2).

Qshqwsh, Hda Hamd. (1992). Jra'em Alhasb Alelktrwny Fy Altshry'e Almqarn. Dar Alnhdh Al'erbyh, Alqahrh.

Rstm, Hsham Fryd. (1992). Qanwn Al'eqwbat Wmkhatr Tqnyh Alm'elwmat. Mktbh Alalat Alhdythh, Asywt.

Salm, 'Emr. (2000). Almraqbh Alelktrwnyh Tryqh Hdythh Ltnfyd Al'eqwbh Alsalbh Llhryh Kharj Alsjn. Dar Alnhdh Al'erbyh, Altb'eh Alawly, Alqahrh.

Slamh, Mamwn Mhmd. (1971). Alejra'at Aljna'eyh Fy Altshry'e Allyby- Aljz' Alawl. Mnshwrat Aljam'eh Allybyh, Altb'eh Alawla, Bnghazy.