مجلة دراسات في سيكولوجية الانحراف
مجلة علمية دولية نصف سنوية ISSN :2602- 554X EISSN :2773-2568
المجلد : 07 العدد 03 السنة : 2022 ص- ص : 177- 193

الجرائم المعلوماتية والجهود المبذولة لمكافحتها

Cybercrimes and efforts to combat it

سعاد مقدم *
جامعة الشاذلي بن جديد -الطارف-الجزائر
mokeddem.souad@yahoo.com

تاريخ الاستلام: 2022/02/09 تاريخ القبول : 2022/12/07

ملخص:

أصبحت الجرائم االمعلوماتية من الظواهر الإجرامية المستحدثة، حيث ساهمت عوامل التحضر وانتقال المجتمعات من المجتمع الواقعي إلى المجتمع الافتراضي، في انتشارها وزيادة الفرص المتاحة لارتكابها وسرعة الكسب غير المشروع.

فهي جرائم عابرة للحدود، لذلك لابد من تكاثف جهود الدول من أجل مكافحة هذا النوع المستحدث من الجرائم، وتعزيز التعاون بينها واتخاذ تدابير فعالة للحد منها والقضاء عليها ومعاقبة مرتكبيها.

الكلمات المفتاحية: *الجرائم المستحدثة؛ الجرائم المعلوماتية؛ المجرم المعلوماتي.*

Abstract:

Cybercrimes have become a newly developed criminal phenomenon, the factors of urbanization and the transition of societies from the real society to the virtual one have contributed to the spread of these crimes, the increase in the opportunities available to commit them, and the speed of graft. Cybercrimes are transnational crimes, so it is necessary to intensify the efforts of states to combat this new type of crime, enhance cooperation between them, and take effective measures to combat them, eliminate them and punish their perpetrators.

Keywords:

emerging crimes; Cybercrime; cybercriminal.

* المؤلف المرسل .

مقدمة:

إن انتشار شبكة الانترنت ونظم المعلومات في المجتمعات المعاصرة، أفرزت وسائل جديدة وحديثة ساهمت في التواصل الثقافي بين الشعوب حيث أصبح العالم عبارة عن قرية صغيرة من زجاج، مما كسر حواجز العزلة الاتصالية بينها، هذا من جهة ومن جهة أخرى ساعد كل هذا على شيوع الجرائم بمختلف أنواعها وأشكالها وظهرت ما يسمى الجرائم المعلوماتية التي تعتمد على شبكة الانترنت على وجه الخصوص، وظهر معها نوع جديد من المجرمين انتقلوا من الجريمة في صورتها التقليدية إلى أخرى إلكترونية قد يصعب التحكم فيها، حيث أصبحت تهدد كيان المجتمع الإنساني وأمنه الاجتماعي والاقتصادي.

وما يميز هذه الجرائم سهولة ارتكابها بعيدا عن الرقابة الأمنية وصعوبة التنبؤ بالمشتبه بهم وسهولة إتلاف الأدلة من قبل الجناة، بالإضافة إلى كونها جرائم عابرة للحدود تتميز بالتباعد الجغرافي لذلك يصعب التحكم في تحديد حجم الضرر الناتج عنها قياسا بالجرائم التقليدية.

وعلى الرغم من تنامي جهود التصدي لظاهرة الجريمة المعلوماتية إلا انه يصعب التعامل معها، لأنها من الظواهر الحديثة، وذلك لارتباطها بتكنولوجيا حديثة هي تكنولوجيا المعلومات والاتصالات.

ومنه يكتسي هذا الموضوع أهمية بالغة في الوقت الراهن، فأيا كان بإمكانه أن يخترق الحياة الخاصة للآخرين عن طريق شبكة الانترنت، بعد أن أضحت هذه التقنية فضاء يمارس فيه المجرمون الإلكترونيون أعمالهم الإجرامية.

لكل ذلك رأينا من الأجدر إعطاء صورة بسيطة عن الجوانب الاجتماعية لهذا الموضوع.

1- تعريف الجرائم المستحدثة:

الجريمة هي السلوكات والأفعال الخارجة عن القانون والتي تضر بمصالح المجتمع.

وبما أن "الجريمة ظاهرة اجتماعية فإن أنماطها و أساليب ارتكابها سوف تظل في تغير مستمر مع حركة المجتمعات وأساليب أفرادها في التعامل و ممارسة الأنشطة اليومية".(البشرى،2004، ص ص 15-16)

ومع التطور العلمي و التكنولوجي الهائل للعالم ظهرت أشكال وأنواع كثيرة من الجرائم عرفت بالجرائم المستحدثة.

ويرى رفيق شلبي إن الجرائم المستحدثة و المعبر عنها بالجرائم المستجدة، هي ظواهر إجرامية أفرزتها تيارات إنحرافية برزت على الساحة الإجرامية في وقتنا الراهن وهي وليدة التحولات التي شهدتها

الحياة المعاصرة المعقدة في كل ما له صلة بالمسائل الاجتماعية والاقتصادية والثقافية والسياسية وغيرها. (الشلبي، 1999، ص 72)

ويقصد بالجرائم المستحدثة "أنماط من الجرائم تستخدم فيها التكنولوجيا الحديثة من أجل تسهيل عملية الإجرام مثل: جرائم الإرهاب والجريمة المنظمة وجرائم العنف وجرائم غسيل الأموال والجرائم الاقتصادية وأنماط الفساد الإداري والجرائم المتعلقة بالكمبيوتر وجرائم تزوير بطاقات الائتمان والجرائم الناتجة عن التعامل غير المشروع بجسد الإنسان، وجرائم العنف العائلي وغيرها من أنماط الجرائم المعاصرة"(مجموعة من المؤلفين،2014، ص 198)

من خلال ما سبق يمكن القول أن الجرائم المستحدثة هي تلك الجرائم الحديثة والمعاصرة والتي لازمت التقدم العلمي والتكنولوجي وعصر المعلومات وبالتالي عرفت انتشارا واسعا، إذ استعمل مرتكبوها تقنيات وطرق حديثة لتسهيل عملياتهم، وامتازت بالتخطيط والتنظيم والسرعة في تنفيذها مما جعلها تشكل خطرا على المجتمع، فهي تهدد أمنه واستقراره، لذلك لابد من مكافحتها.

ولقد تعددت صور الجرائم المستحدثة بقدر ما تعددت الوسائل المستعملة في ارتكابها. وتعتبر الجرائم المعلوماتية من الجرائم المستحدثة التي غيرت من مفهوم الجريمة العادية لتصبح أشد تأثيرا وأسرع انتشارا و تنوعا.

2- تعريف الجرائم المعلوماتية:

تعددت تعريفات الجرائم المعلوماتية باعتبارها صنف جديد من الجرائم التي انتقلت من الجريمة التقليدية إلى أخرى إلكترونية قد يصعب التعامل معها، وذلك لارتباطها بالتكنولوجيا الحديثة للاتصالات، مما أدى إلى صعوبة التوصل إلى الحلول المناسبة لمكافحتها.

ويشير مصطلح الجرائم المعلوماتية إلى أي جريمة تتضمن الحاسب الآلي، فقد يستخدم الحاسوب في ارتكاب الجريمة وقد يكون هو نفسه الهدف، وقد عرفت الجرائم المعلوماتية بأنها: " الجرائم التي تتم باستخدام جهاز الكمبيوتر من خلال الاتصال بالانترنت ويكون هدفها اختراق الشبكات أو تخزينها أو التحريف أو التزوير أو السرقة والاختلاس أو قرصنة وسرقة حقوق الملكية الفكرية ". (شفيق،2015،ص 16)

ويذهب رأي آخر في تعريف الجريمة المتصلة بالحاسب بأنها: " أي عمل غير قانوني يستخدم فيه الحاسب كأداة أو موضوع للجريمة ". (مجموعة من المؤلفين،2014، ص 102)

كما يحاول البعض تعريفها بأنها " تلك الجرائم التي لا تعرف الحدود الجغرافية والتي يتم ارتكابها بأداة هي الحاسب الآلي، عن طريق شبكة الانترنت وبواسطة شخص على دراية فائقة بها " (منير محمد الجنبيهي وممدوح محمد الجنبيهي، 2004، ص 13)

أما تعريف منظمة التعاون الاقتصادي والتنمية الخاص باستبيان الغش المعلوماتي عام 1982 والذي أوردته بلجيكا في تقريرها بأن الجرائم المعلوماتية هي: " كل فعل أول امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية "(الملط، 2006، ص 87)

أما التعريف الذي أقره المؤتمر العاشر للأمم المتحدة لمنع الجريمة حول الحاسب الآلي وشبكاته إذ عرف الجريمة المعلوماتية " بأنها جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب وتشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية " (زيدان، 2011، ص 43).

وقد اصطلح المشرع الجزائري على تسمية الجرائم المعلوماتية بمصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وعرفها بموجب أحكام المادة 02 من قانون (09-04) هي أنها " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية "(قانون 09-04 مؤرخ في 16 شعبان 1430 الموافق لـ 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. الجريدة الرسمية، العدد 47 لسنة 2009).

إن المشرع الجزائري في هذا التعريف اصطلح على الجرائم المعلوماتية تسمية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وترك المجال واسع لأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية وبالتالي فالجريمة المعلوماتية هي كل استغلال للنظام المعلوماتي في السلوك الإجرامي.

بعد استعراض التعريفات التي قيلت بشأن جرائم نظم المعلومات نلاحظ في البداية أنها متقاربة من بعضها البعض وأنها حاولت استيعاب هذا النوع المستحدث من الإجرام بالرغم من حداثته وارتباطه بالتقنية الرقمية.

وبالتالي نعرّف الجرائم المعلوماتية هي كل جريمة تستخدم فيها الحاسوب كأداة أو كهدف بطريقة غير قانونية، كسرقة معلومات لتحقيق أرباح شخصية أو سرقة مكونات الحاسب الفيزيقية أو البرمجيات وإحداث ضرر بها، وهي بذلك ظاهرة إجرامية مستحدثة تتميز من حيث موضوع الجريمة ووسيلة ارتكابها وسمات مرتكبيها وأنماط السلوك الإجرامي.

وقد يكون جهاز الكمبيوتر في مجال ارتكاب الجرائم هدفا للجريمة أو أداة لارتكابها أو مسرحا لها. وقد يكون لجهاز الكمبيوتر دورا رئيسيا في حقل اكتشاف الجريمة.

3 – سمات المجرم المعلوماتي:

تتوافر لدى معظم الجناة مرتكبي الجرائم المعلوماتية مجموعة من الصفات تميزهم عن سواهم من الجناة المتورطين في أنماط الانحراف الأخرى لعل من أبرز هذه السمات:

- **المجرم المعلوماتي صغير السن:** حيث تتراوح أعمار مقترفي الجريمة المعلوماتية بين (18-46) سنة والمتوسط العمري لهم 32 سنة وهذا مؤشر على أن المجرم المعلوماتي يكون من صغار السن لأن كبار السن لم يألفوا التعامل مع الحاسب الآلي، كما أن حداثة الطفرة المعلوماتية الهائلة التي شهدها العالم المعاصر كانت عاملا في بلورة هذه السمة.

- **المجرم المعلوماتي ذكي:** يوصف الإجرام المعلوماتي بأنه إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف، فالمجرم المعلوماتي إنسان على مستوى من الذكاء إضافة إلى أنه مجرم متكيف اجتماعيا لا يناصب العداء للمجتمع.

- **المجرم المعلوماتي متخصص:** لابد أن تتوافر لدى الجناة مرتكبي الجرائم المعلوماتية قدر من المعرفة المعلوماتية أي أنهم متخصصون في هذا الشكل من الانحراف والإجرام.

- **المجرم المعلوماتي مجرم محترف:** لابد أن تتوفر لدى الجناة مرتكبي الجرائم المعلوماتية قدر من المعرفة المعلوماتية، ولكن هذه السمة ليست عامة ومطلقة وإنما تقتصر على الجرائم التي يستلزم ارتكابها التعامل مع الحاسب الآلي ومعالجة المعلومات للتغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الحاسوب كما في البنوك أو المؤسسات العسكرية...

- **المجرم المعلوماتي مجرم عائد:** غالبا ما يعود مرتكبي الإجرام المعلوماتي إلى ارتكاب جرائم أخرى في مجال المعلوماتية رغبة منه في سد الثغرات التي أدت إلى التعرف عليهم في المرة الأولى، فينتهي بهم الأمر في المرة الثانية إلى كشفهم وتقديمهم للمحاكمة. (الشكري،2008،ص ص117-118)

إن المجرم المعلوماتي يختلف تماما عن المجرم العادي فيتمتع بمستوى عال من التدريب والخبرة والذكاء في مجال تكنولوجيا المعلومات، وفي المستقبل ومع ازدياد هذا النوع من الجرائم سوف يتغير شكل المجرم من مجرد مجرم لص جاهل إلى شخص متعلم على أعلى مستوى وقادر على التعامل مع أحدث الوسائل العلمية. (سالم، 2003، ص 113)

إن التقدم التكنولوجي أفرز أنماطا جديدة من الجريمة، وكذا من المجرمين، وكان له أثره على نوعية الجرائم، وأستغل المجرم هذا التطور في تطويع المخترعات العلمية الحديثة لخدمة أهدافه الإجرامية.

ولا شك أن مرتكبي الجريمة الإلكترونية يختلفون عن مرتكبي الجريمة التقليدية، من حيث السن والجنس والمستوى التعليمي وغير ذلك من المؤثرات الخارجية، وتعد المهارة التقنية من أبرز صفات المجرم المعلوماتي، فتنفيذ هذه الجرائم يتطلب قدرا من المهارات التقنية سواء تم اكتسابها عن طريق الدراسة المتخصصة أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات والاتصالات.

4- التطور التاريخي للجرائم المعلوماتية:

مرت جرائم الإنترنت بتطور تاريخي تبعًا لتطور التقنية واستخداماتها، ولهذا مرت بثلاث مراحل:

4-1-المرحلة الأولى:

من شيوع استخدام الحواسيب في الستينات إلى السبعينات اقتضت المعالجة على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر، وترافقت هذه النقاشات مع التساؤل حول ما إذا كانت هذه الجرائم مجرد شيء عابر أم ظاهرة إجرامية مستحدثة، وأن الجدل حول ما إذا كانت جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في بيئة أو مهنة الحوسبة، ومع تزايد استخدام الحواسيب الشخصية في السبعينات ظهرت عدد من الدراسات المسحية والقانونية التي اهتمت بجرائم الكمبيوتر وعالجت عددا من قضايا الجرائم الفعلية، وبدأ الحديث عنها بوصفها ظاهرة إجرامية لا مجرد سلوكيات مرفوضة.

4-2-المرحلة الثانية:

في الثمانينات، حيث طفا على السطح مفهوم جديد لجرائم الكمبيوتر والانترنت ارتبطت بعمليات اقتحام نظام الكمبيوتر عن بعد وأنشطة نشر وزرع الفيروسات الالكترونية التي تقوم بعملية تدميرية للملفات أو البرامج شاع اصطلاح "الهاكرز" المعبر عن مقتحمي النظم، لكن الحديث عن الدوافع لارتكاب هذه الأفعال ظل محصورا في رغبة المحترفين تجاوز امن المعلومات وإظهار تفوقهم التقني، لكن هؤلاء المغامرون أصبحوا أداة إجرام .وظهر المجرم المعلوماتي المتفوق المدفوع بأغراض إجرامية خطيرة القادر على ارتكاب أفعال تستهدف الاستيلاء على المال أو التجسس أو الاستيلاء على البيانات السرية والاقتصادية الاجتماعية والسياسية والعسكرية.

4-3-المرحلة الثالثة:

شهدت التسعينات تناميا هائلا في حقل الجرائم الالكترونية، وتغييرا في نطاقها ومفهومها وكان ذلك بفعل ما أحدثته شبكة الإنترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكة المعلومات ظهرت أنماط جديدة إنكار الخدمة التي تقوم عل فكرة تعطيل نظام تقني ومنعه من القيام بعمله

المعتاد وأكثر ما مورست ضد مواقع الانترنت التسويقية الهامة التي يتسبب انقطاعها عن الخدمة لساعات في خسائر مالية بالملايين.

ونشطت جرائم نشر الفيروسات عبر المواقع الالكترونية لما تسهله من انتقالها إلى ملايين المستخدمين في ذات الوقت، وظهرت الرسائل المنشورة على الانترنت أو المراسلة بالبريد الالكتروني المنطوية على إثارة الأحقاد أو المساس بكرامة واعتبار الأشخاص أو المروجة لمواد غير القانونية أو غير المشروعة.(رضوان، 2018، http://www.soutalomma.com).

وعلى مدى السنوات القليلة الماضية توسعت الانترنت أضعافا مضاعفة، ولقد وفرت السهولة النسبية في الحصول على أجهزة الكمبيوتر واستخدام الانترنت وظهور ما يسمى الفضاء الالكتروني أو العالم الافتراضي، كل ذلك مكن الأفراد من التواصل وتكوين الصداقات، والترفيه والتعلم والتجارة. وازدادت التفاعلات بين الأفراد والجماعات سواء كانت شخصية أو مؤسسية، وانتقلت بذلك تعاملاتهم من العالم الواقعي إلى العالم الافتراضي وكذلك انتقلت معها الجريمة من الجريمة التقليدية إلى الجريمة المستحدثة، وخلق معها المجرمين المعلوماتيين الذين يرتكبون جريمتهم عن طريق الاحتيال والسرقة والتعدي والتخريب ...إلخ باستخدام المعالجة الآلية للمعلومات. وازدادت الجرائم المعلوماتية على الرغم من توفير وسائل الحماية المتعددة إلا أنها تثبت عدم فعاليتها أمام قرصنة شبكة المعلومات، وأصبحت بذلك الجرائم المعلوماتية، محط حديث وسائل الإعلام و الباحثين والعلماء، بوصفها ظاهرة اجتماعية قد أسفرت عن عوامل مستحدثة.

5- خصائص الجرائم المعلوماتية:

تتميز الجرائم المرتكبة بواسطة الحاسب الآلي كأداة أو كهدف للجريمة بمجموعة من الخصائص التي تؤدي إلى ارتكاب الجرائم المعلوماتية منها:

- **سرعة التنفيذ:** لا يتطلب تنفيذ الجرائم المعلوماتية الوقت الكثير، وبضغطة واحدة على لوحة المفاتيح، يمكن تنتقل ملايين الدولارات من مكان إلى آخر.

- **التنفيذ عن بعد:** لا تتطلب الجرائم المعلوماتية في أغلبها وجود الفاعل في مكان الجريمة، بل يمكن للفاعل تنفيذ جريمته وهو في دولة بعيدة كل البعد عن التفاعل.

- **إخفاء الجريمة:** إن الجرائم المعلوماتية جرائم مخفية إلا أنه يمكن أن نلاحظ آثارها والتخمين بوقوعها.

- **الجاذبية:** نظرا لما تمثله سوق المعلومات والحاسب والانترنت من ثروة كبيرة للمجرمين فقد غذت أكثر جذبا لاستثمار الأموال وغسيلها والدخول إلى الشبكات وسرعة المعلومات وبيعها أو سرقة البنوك.

- **عابرة للدول:** إن ربط العالم بشبكة من الاتصالات من خلال الأقمار الصناعية والفضائيات والانترنت جعل الانتشار الثقافي وعولمة الثقافة والجريمة أمرا ممكنا وشائعا لا يعترف بالحدود الإقليمية للدول، ولا بالمكان ولا بالزمان وأصبحت ساحتها العالم أجمع.

- **جرائم ناعمة:** الجرائم المعلوماتية تمتاز بأنها جرائم ناعمة لا تتطلب عنفا فنقل بيانات من حاسب إلى آخر أو السطو الإلكتروني على أرصدة بنك ما لا يتطلب أي عنف.

- **صعوبة إثباتها:** تتميز الجرائم المعلوماتية عن الجرائم التقليدية بأنها صعبة الإثبات وهذا راجع إلى افتقاد وجود الآثار التقليدية للجريمة، وغياب الدليل الفيزيقي(بصمات، تخريب، شواهد مادية) وسهولة محو الدليل، يضاف إلى ذلك عدم كفاية القوانين القائمة. (البداينة، 2014، ص ص19-20) .

إن الهدف من الجرائم المعلوماتية هو الحصول على المعلومات أو الاستيلاء على الأموال أو استهداف الأفراد أو الجماعات أو الدول وأحيانا أخرى نجدها تستهدف أجهزة الكمبيوتر كهدف لها، فهي لا حدود جغرافية لها، أي تتخطى حدود الدولة التي ارتكبت فيها ، وبما أن الحاسب هو أداة ارتكاب الجرائم المعلوماتية فإن مرتكب الجريمة هو شخص ذو خبرة فائقة في نظم المعلومات، وشبكة الاتصال والتي تمكنه الحصول على المعلومات التي تكون إما محفوظة على أجهزة الكمبيوتر وإما منقولة عبر شبكة الانترنت والتي تمكنه من تنفيذ جريمته والعمل على عدم اكتشافها.

6- صور الجرائم المعلوماتية:

الجرائم المعلوماتية جرائم يستخدم فيها الحاسوب كوسيلة أو أداة لارتكابها أو جرائم يكون الكمبيوتر نفسه ضحيتها:

-**جرائم الأضرار بالبيانات:** يعتبر هذا النوع من الجرائم المعلوماتية من أشدها خطورة وتأثيرا وأكثرها حدوثا وتحقيقا للخسائر للأفراد والمؤسسات. ويشمل هذا النوع كل أنشطة تعديل أو محو أو سرقة أو إتلاف أو تعطيل العمل للمعلومات وقواعد البيانات الموجودة بصورة إلكترونية على الحواسيب الآلية المتصلة أو غير المتصلة بشبكات المعلومات أو مجرد الدخول بطريقة غير مشروعة عليها.

- **جرائم الاعتداء على الأشخاص:** المقصود بالاعتداء هذا هو السب والقذف والتشهير وبث أفكار وأخبار من شأنها الإضرار الأدبي أو المعنوي بالشخص أو الجهة المقصودة وتتنوع طرق الاعتداء بداية من الدخول على الموقع الشخصي للشخص المشهر به وتغيير محتوياته، والذي يندرج تحت الجرائم التي تتم ضد الحواسيب والشبكات أو عمل موقع آخر يتم بنشر أخبار ومعلومات غير صحيحة والذي يندرج تحت الجرائم باستخدام الحواسب الآلية والشبكات.

-استخدام الحواسيب الآلية وشبكة الانترنت في **انتهاك حقوق الملكية الفكرية** لبرامج الحاسب والمصنفات الفنية المسموعة والمرئية ونشرها وتداولها عبر شبكة فيما يعرف بالقرصنة الأمر الذي يلحق الضرر المادي والمعنوي بالشخص أو الجهة المالكة تلك الموارد.

- **التخابر أو الاتصال** بين أفراد منظمة أو نشاط يهدد أمن واستقرار الدولة أو نشاط محرم قانونا مثل شبكات الدعارة والشذوذ التي باتت وسيلة الاتصال الرئيسية لها هي حجرات الدردشة المنتشرة عبر شبكة الانترنت.

- **جرائم الاعتداء على الأموال:** مع زيادة اعتمادية المؤسسات المصرفية والمالية على تكنولوجيا المعلومات والاتصالات والتحول التدريجي في كافة أنحاء العالم نحو ما يطلق عليه البنوك والمصارف والمؤسسات المالية الإلكترونية، فقد شهد هذا التطور ظهور عدد كبير من الجرائم الإلكترونية.

- كما تعد **ظاهرة غسل الأموال** المتحصلة من أنشطة غير مشروعة من أبرز الأنماط الإجرامية المستحدثة التي تقوم بها شبكات منظمة تمتهن الإجرام وتأخذ درجات عالية من التنسيق والتخطيط والانتشار في كافة أنحاء العالم. (يوسف، 2011، ص ص105-118)

إن الصور الأكثر شيوعا للجرائم المعلوماتية هي جرائم الأموال وجرائم الأشخاص، وفقا لهذا المفهوم تظهر الجرائم المعلوماتية صورتين جرائم واقعة باستخدام الكمبيوتر لأغراض الدخول غير المشروع للبيانات والمعلومات المخزنة على الكمبيوتر وذلك عبر شبكات الاتصال أو جرائم واقعة على الكمبيوتر، المتعلقة بالجانب المادي، كالسرقة والإتلاف.

كما أننا نلاحظ أنه ليست كافة جرائم الحاسب الآلي جرائم أموال بل يمكن أن تكون جرائم أشخاص ترتكب باستخدام الكمبيوتر، يكون محلها الشخص كالسب والقذف والتهديد، التي أصبح الكمبيوتر يوفر لها أسلوبا وموضوعا جديدا.

لكن الملاحظ بعد هذا العرض لبعض صور الجرائم المعلوماتية أن أي وصف منها لم يكن شاملا لكافة جرائم الكمبيوتر.

7– دوافع ارتكاب الجرائم المعلوماتية:

هناك عدة دوافع إلى ارتكاب الجرائم المعلوماتية قد يقف وراءها مصدر واحد هو الرغبة الإجرامية ويمكن إيجاز هذه الدوافع كالآتي:

- **الدوافع الشخصية:** يمكن رد الدوافع الشخصية لدى مرتكب الجريمة المعلوماتية إلى السعي لتحقيق الربح فهذا الدافع المادي يعد من أهم البواعث إلى ارتكاب الجريمة المعلوماتية بما يحققه من

ثراء شخصي فاحش، وقد يكون الرغبة في إثبات الذات وتحقيق انتصار شخصي على نفس الأنظمة المعلوماتية من بين أهم الدوافع الذهنية لارتكاب الجريمة.

- **الدوافع الخارجية:** الإنسان بطبيعته مخلوق هش من الناحية السيكولوجية يمكن في بعض المواقف أن يستسلم للمؤثرات الخارجية ولعل أبرزها الحاجة إلى اختصار عنصر الزمن وتوفير سنوات عدة من البحث وتحاشي استثمار الملايين من الأموال في مجال البحث العلمي، إذ تدفع الحاجة بعض المنشآت بل وحتى بعض الدول إلى الاتصال بالأفراد الذين يشغلون أماكن حساسة في إحدى المنشآت كي يعملوا لصالح منشآت أخرى منافسة لهدف الاطلاع على بعض المعلومات والتقنيات المتوفرة لديها للاستفادة منها، وتستخدم في ذلك عدة أساليب منها الرشوة أو الإقناع والإغراء المقترن بالتهديد، والذي قد يصل في بعض الأحيان إلى زرع جواسيس في تلك المنشآت.

-وقد يكون **دافع جنون العظمة** أو الطبيعة التنافسية هي التي تدفع بعض العاملين في المؤسسة لإظهار قدراتهم الفنية الخارقة لإدارة المؤسسة، فيقضي به ذلك إلى ارتكاب مثل هذه الجرائم حتى ينافس زملائه للوصول إلى أعلى المراكز المرموقة.

-وقد يكون **دافع الانتقام** من رب العمل أو أحد الزملاء أو الأصدقاء من بين البواعث الدافعة إلى ارتكاب الجريمة. (الشكري،2008،ص ص114-115)

- **الاستيلاء على المعلومات**: الإقدام على ارتكاب هذا الجرم بواسطة تقنية المعلومات بهدف الحصول على المعلومة ذاتها والاستياء عليها والتصرف فيها يتمثل ذلك في الحصول على المعلومة المحفوظة في الحاسب الآلي أو المنقولة أو تغييرها أو حذفها أو إلغائها نهائياً من النظام. ويختلف الدافع لهذا التصرف فقد يكون دافع تنافسي أو سببه الابتزاز أو الحصول على مزايا ومكاسب اقتصاديه، كثيراً ما يكون هدف هذه الجرائم ذو طابع سياسي أو اقتصادي

- **إلحاق الأذى بأشخاص أو جهات:** بعض المجرمن الذين يقدمون على ارتكاب الجريمة عبر شبكة المعلومات العالمية وتقنية المعلومات بصورة عامة يتركز الدافع من ورائها على إلحاق الأذى بأشخاص محددين أو جهات معينة، وغالبا ما تكون تلك الجرائم مباشرة تتمثل في صورة ابتزاز أو تهديد أو تشهير. وكما يمكن أن تكون هذه الجرائم غير مباشرة وتتمثل في الحصول على البيانات والمعلومات الخاصة بتلك الجهات أو الأشخاص لاستخدامها فيما بعد في ارتكاب جرائم مباشرة.

- **تهديد الأمني القومي والعسكري:** بعض الجرائم الالكترونية الهدف منها أسباب ودوافع سياسية كتهديد الأمن القومي والعسكري ومن ذلك ظهر ما يعرف بالتجسس الإلكتروني والإرهاب الإلكتروني

والحرب المعلوماتية كما هو الحاصل بن الدول المتقدمة إلكترونياً. (البادي وآخرون، 2016، ص ص 28-30)

ويمكن القول أن هناك دوافع كثيرة تدفع بهؤلاء الأشخاص نحو الإقدام على ارتكاب الجرائم المعلوماتية كالمحبة والانتقام وكسب المال، ابتغاء تحقيق غاية معينة، لذلك فإن مرتكبي الجريمة المعلوماتية يختلف عن مرتكبي الجريمة التقليدية، ويأتي في مقدمة دوافع الجريمة المعلوماتية الدوافع الشخصية للجاني لإبراز الذات وإثبات القدرة والسعي لتحقيق الربح والكسب الذي قد يدفع إلى التعدي على الحواسب ونظم المعلومات. وثمة دوافع تتمثل في الرغبة في الاستيلاء على المعلومات التي قد تكون محفوظة في أجهزة الحاسب الآلي أو منقولة عبر الشبكة المعلوماتية، كما قد تكون الدوافع الرغبة في الإضرار بالغير، سواء كانوا أشخاص أو جهات أو أمن قومي للمجتمع، والتي قد تكون سببا في ارتكاب الجرائم المعلوماتية.

8- صعوبة الكشف عن الجرائم المعلوماتية وإثباتها:

إن أهم ما يميز جرائم نظم المعلومات صعوبة اكتشافها وإثباتها وهي صعوبة يعترف بها جميع الباحثين في هذا المجال:

-انعدام الدليل المرئي: يلاحظ أن ما ينتج عن نظم المعلومات من أدلة عن الجرائم التي تقدم عليها أو بواسطتها ما هي إلا بيانات غير مرئية لا تفصح عن شخصية معينة وهذه البيانات مسجلة إلكترونيا بكثافة بالغة وبصورة مرمزة مما يقطع أي صلة بين المجرم وجريمته ويعوق أن يحول دون الكشف عن شخصيته.

- سهولة محو الدليل أو تدميره: من الصعوبات التي يمكن أن تعترض عملية الإثبات في مجال جرائم نظم المعلومات سهولة محو الجاني أي تدميره لأدلة الإدانة في فترة زمنية وجيزة فضلا عن سهولة تنصله من هذا العمل بإرجاعه إلى خطأ في نظام الحاسب أو الشبكة أو في الأجهزة.

- بعد مكان ارتكاب الجريمة: يتم ارتكاب جريمة الحاسب الآلي عادة عن بعد حيث لا يتواجد الفاعل على مسرح الجريمة ومن تم تباعد المسافات بين الفعل والنتيجة، وهذه المسافات لا تقف عند حدود الدولة بل تمتد إلى النطاق الإقليمي لدول أخرى مما يضاعف صعوبة كشفها أو ملاحقتها. (الديربي و إسماعيل، 2012،ص ص327-334)

- إحجام المجني عليهم عن التبليغ: تبدو أكثر المشاكل جسامة لا في مجال صعوبة اكتشاف وإثبات جرائم الحاسب، بل وفي دراسة هذه الظاهرة في مجملها هي مشكلة امتناع المجني عليهم عن التبليغ عن

الجرائم المرتكبة ضد نظام الحاسب وهو ما يعرف بالرقم الأسود Chiffre noir. (Francillon ,1993,p293).

وبالتالي من المستحيل أن نحدد على نحو دقيق نطاق الجرائم المعلوماتية، ويعود ذلك إلى أن هؤلاء الضحايا يفضلون عدم الإبلاغ عنها ويفضلون الكتمان، وذلك لتجنب إفشاء سر انتهاك الأنظمة المعلوماتية لديهم.

تتصف الجرائم المعلوماتية بأنها صعبة الاكتشاف لأن المجرم المعلوماتي من الممكن أن يستخدم إسما مستعارا، إضافة إلى أنها صعبة الإثبات لأنها لا تترك أثرا.

من الملاحظ أن الجرائم المعلوماتية هي جرائم عابرة للحدود الوطنية أو الإقليمية أو القارية وأن مكافحتها تتطلب سن قواعد موضوعية وإجرائية على هذا النمط المستحدث من الجرائم والتنسيق بين قوانين الإجراءات الجنائية للدول المختلفة.

9- الجهود المبذولة لمكافحة الجرائم المعلوماتية:

الجرائم المعلوماتية هي واحدة من أخطر الظواهر الإجرامية المستحدثة في المجتمع الجزائري كما في المجتمعات الأخرى، حيث شهد المجتمع المعاصر ثورة تكنولوجية أفرزت ظواهر إجرامية خطيرة تستوجب مكافحتها. ويمكن تقسيم التدابير الواجب مباشرتها لمكافحة الجرائم المعلوماتية إلى نوعين أحدهما على المستوى الوطني والأخرى على المستوى الدولي:

9-1- الجهود المبذولة على المستوى الوطني:

بعد أن أصبح المجتمع المعلوماتي حقيقة واقعية بات واضحا لنا مدى قصور التشريعات الجزائية في التصدي لهذا النمط من الجرائم، لهذا كان لزاما على المشرع الجزائري (دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم (04-15) المؤرخ في العاشر من نوفمبر عام 2004 المتمم للأمر رقم (66-156) المتضمن قانون العقوبات والذي القسم السابع مكرر منه تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات والذي تضمن ثمانية مواد نص فيها على عدة جرائم) التدخل عبر العديد من النصوص القانونية لمواجهة الجريمة المعلوماتية والمجرم المعلوماتي.

لقد تطرق المشرع الجزائري على غرار باقي الدول إلى تجريم أفعال المساس بالنظم المعالجة الآلية حماية لها من كافة الاعتداءات التي تقع على مكوناتها غير المادية وتعوق دورة تقدمها في المجتمع.

وفيما يلي سنتطرق لموقف المشرع الجزائري من الجرائم المعلوماتية:

-تخصيص المشرع الجزائري هذه الجرائم بقسم خاص يدل على إقراره بأنها ظاهرة مستجدة متميزة من حيث المصالح التي طالتها، مبناها وطبيعتها، سلوكياتها ومحلها لا يمكن إدراجها تحت أي نوع من

الجرائم. وقد ذكر المشرع أشكال الاعتداء على نظم المعالجة الآلية.مبتعدا في ذلك عن الوصف القوي أو التفصيلي لها أو الصور التي تتخذها الجريمة الواحدة أو التي تندرج في نطاق الجريمة الواحدة. كما أن الإطار العام للنصوص الموضوعية لم يميز نوعية المعلومات، ولعل مرد ذلك سعى المشرع الجزائري لتعميم حماية المعلومات بكافة أنواعها.

- فعمد المشرع إلى حماية سرية نظم المعالجة الآلية ومعلوماتها فجرّم بذلك الدخول غير المصرح به إلى نظام المعالجة الآلية للمعلومات. وجرّم التعامل في المعلومات المتحصلة من إحدى الجرائم محل الدراسة.

- وحمى سلامة المعلومات ونظم معالجتها وتكاملها، فجرّم بذلك التلاعب بالمعلومات إدخالا وإزالة وتعديلا ما لم يكن مصرحا بذلك، وكذلك تخريب نظام المعالجة الآلية للمعلومات كظرف مشدد لهذه الجريمة.

- والنص على هذه الجرائم يحمي المعلومات ونظم معالجتها في إتاحتها ووفرتها. وهذه المصالح هي التي تصنع لجرائم الاعتداء على نظم المعالجة الآلية ذاتية تميزها عن باقي الجرائم تقليدية كانت أو تقنية. (بوكر، 2012، ص ص126-127)

لقد نص المشرع الجزائري على جملة من العقوبات الخاصة بالجرائم المعلوماتية منها عقوبات أصلية وأخرى تكميلية بالإضافة إلى عقوبة خاصة بالأشخاص المعنوية والأشخاص الطبيعية.

وبالرغم من النصوص القانونية التي تجرّم هذه الأفعال إلا أنها لا تعد كافية ولا تلم بجميع أنواع الجرائم المعلوماتية.

يبدو أن هناك محاولات جادة لتطوير المنظومة القانونية وإصدار تشريعات تواكب التطور الحاصل في المجال التكنولوجي خاصة ما تعلق منها بتكنولوجيات الإعلام والاتصال وفي ذلك مؤشر في خوض غمار الالتحاق بمصاف الدول الآخذة بناحية هذه التقنية. (زيدان، 2011، ص 20)

وفي السياق ذاته أن القانون الجزائري يعاقب في الغالب مرتكبي هذه الجرائم بالسجن القصير المدى أو بالغرامة المالية بحكم أن هذه الجرائم الإلكترونية المرتكبة في الجزائر تصب أو تصنف قانونيا كسرقة. إن على الحكومة ضرورة استحداث استراتيجيات عقابية وتقنية لحماية ضحايا هذه الجرائم. (بونعارة، الجريمة الإلكترونية،www.univ.emir.dz)

إن استصدار الجزائر قوانين لمعاقبة مرتكبي الجرائم المعلوماتية غير كاف، مع عدم تهيئة الأسس التقنية الكفيلة بتصنيف درجات هذه الجرائم وحدَة أضرارها قبل إصدار العقوبة، هذا فضلا عن غياب التواصل الدائم بين القضاء والمختصين في الاتصالات ما أفرز شبه تذبذب وغموض في شأن العقوبات الدقيقة في مثل هذه الجرائم.

وعليه لابد من إتباع أساليب مكافحة الجريمة المعلوماتية من خلال الاستخدام الأمثل للوسائل التكنولوجية والإلكترونية المتمثلة في نظم الحاسبات الآلية والاتصالات بـ: (البادي وآخرون، 2016، ص41)

-إصدار التشريعات المواكبة لتطورات الجريمة الإلكترونية وانسجام التشريعات الوطنية مع الاتفاقيات والقواعد الدولية والقوانين المقارنة ذات الصلة لتمكين أجهزة العدالة الجنائية من أداء دورها على النطاق الوطني والإقليمي والدولي بالصورة التي تسهم بالمكافحة الفعالة للجريمة الإلكترونية.

- رفع كفاءة الأجهزة التقنية المختصة برصد التهديدات والمخاطر والتبليغ بالإنذار المبكر وتزويدها بأحدث المعدات.

- تدريب وتأهيل الفنيين والمهندسين العاملين في مجال الأدلة الرقمية وترشيد وتطوير أدائهم.

- تدريب وتأهيل المختصين بأجهزة العدالة الجنائية على كيفية التعامل مع الأدلة الرقمية.

- إتباع كافة وسائل التوعية الأمنية للحد من مخاطر الجريمة الإلكترونية.

وبالتالي نأمل أن يتدخل القضاء لملأ هذا الفراغ التشريعي، بإصدار تشريعات جديدة أو تعديل التشريعات القائمة حتى تتلاءم مع ثورة الاتصالات والمعلومات التي يعيشها الأفراد في وقتنا الحالي، وبالشكل الذي يجعلها كفيلة بحماية النظام المعلوماتي ومكافحة الجرائم الناتجة عنه، وتقرير الجرائم وتحديد العقوبات المناسبة لها.

9-2-الجهود المبذولة على المستوى الدولي:

ونظرا لحداثة الجرائم المعلوماتية وتطورها السريع وسهولة ارتكابها واتساع نطاقها، دفع الحكومات والمنظمات الدولية للتدخل لحماية المجتمع الدولي من هذه الظاهرة الإجرامية المستحدثة.

لقد أضحت الجريمة المعلوماتية ظاهرة إجرامية متنامية وبات من الضروري أن تكثف جهود جميع الدول لمكافحتها نظرا لطابعها المتجاوز لحدود الدولة الواحدة، فالتقدم التكنولوجي لابد أن يرافقه التقدم في التشريع. (زيدان، 2011، ص 11)

إن القوانين لا تصدر إلا تلبية لاحتياجات المجتمع، فالقانون في حد ذاته يلبي حاجات المجتمع الذي يتطور باستمرار، وعلى ذلك لابد أن يكون هناك مواكبة من القوانين في مواجهة تلك الجرائم المستحدثة التي لم يكن لها مثيل من قبل.(سالم، 2003،ص 114)

وذلك بوضع قواعد قانونية جديدة لمكافحة الجريمة المعلوماتية من خلال التدابير المتعلقة بالمعرفة المتبادلة بين الدول على النحو التالي:

- يجب على الدول أن تتعاون بعضها مع البعض من خلال تطبيق المواثيق الدولية ذات الصلة بشأن التعاون الدولي في المسائل الجنائية وعلى وجه الخصوص في مجال تسليم المجرم المعلوماتي. حيث يجب تسليم مرتكبيها وذلك وفقا لمعيار معين لتكييف الجريمة كجريمة يجوز تسليم مرتكبيها.

- يجب على الدول أن تقدم لبعضها البعض المعونة المتبادلة لأغراض التحقيق والإجراءات الخاصة بالجرائم الجنائية المتعلقة بنظم وبيانات الحاسب الآلي.

- يجب على الدول أن تقبل وتستجيب إلى طلبات المعونة المتبادلة من خلال وسائل الاتصال السريعة كالفاكس والبريد الإلكتروني بالقدر الذي يوفر للطرف الطالب المستوى من الأمن والمصادقة.

- تخضع المعونة المتبادلة للاشتراطات المنصوص عليها في قوانين الدولة المدعية أو المنصوص عليها بموجب اتفاقيات المعونة المتبادلة.

- تحدد كل دولة سلطة مركزية تنهض بالمسؤولين إرسال طلبات المعونة المتبادلة والرد عليها وتنفيذها أو نقلها للسلطات المعنية للتنفيذ.

- يجوز للدولة المدعي عليها أن ترفض طلب المعونة إذا ما توافرت لديها القناعة بأن الالتزام لما ورد بالطلب قد يخل بسيادتها أو أمنها أو نظامها العام أو بأي من مصالحها الأساسية الأخرى.

- يجب على الدول المدعي عليها أن تخطر الدولة المدعية بصورة فورية بنتائج تنفيذ طلب المعونة فإذا ما رفض الطلب أو تم تأجيله يجب تقديم الأسباب إلى الرفض أو التأجيل.

- يجوز للدولة المدعية أن تطلب من الدولة المدعي عليها أن تحتفظ بسرية الوقائع والمحتويات التي يتضمنها الطلب وإذا لم يكن بمقدورها الوفاء بمتطلبات سرية الطلب، يجب إخبار الدولة المدعية من أجل تحديد ما إذا كان سينفذ الطلب من عدمه. (الديربي و إسماعيل، 2012، ص ص349-351)

لهذا نرى أن هذه التدابير تعد قواعد قانونية تعتمد على أحكام حول جرائم المعلوماتية والتي أصبحت تهدد الدول المختلفة والتي سايرها القلق إزاء حساسية وخطورة هذه الجرائم، والتي أصبحت مؤمنة بأن المعونة المتبادلة بين الدول تتطلب تعاونا دوليا متزايدا وسريعا وفعالا في الأمور الجنائية، لأن تصارع الأنظمة القضائية بين الدول أمر وارد إذا لم يكن هناك اتفاقيات ثنائية أو قانون دولي تلتزم به الأطراف المعنية، كذلك مشكلة سيادة الدولة في سن التشريعات للأفعال التي تحصل على أراضيها. وكذلك الحاجة لحماية المصالح المشروعة في استخدام وتطوير تكنولوجيا المعلومات.

خاتمة:

لم يكن هناك قلق من نظم المعالجة المعلوماتية من جرائم يمكن أن ترتكب عليها نظرا لمحدودية مستخدميها، علاوة على ذلك كونها كانت مقصورة على فئة معينة من المستخدمين كالباحثين والجامعيين. إلا أنه ومع توسع استخدامها حيث أصبحت تستقطب جميع فئات المجتمع، ظهر المجرمون المعلوماتيون، وأصبحوا يوظفون معارفهم للاعتداء على حقوق الآخرين وخصوصيتهم، وظهرت بذلك الجرائم المعلوماتية وأصبحت تتميز بحداثة الأسلوب وسرعة التنفيذ وسهولة الإخفاء والقدرة على محو آثارها وتعدد صورها وأشكالها. والأمر الذي بات مؤكدا أن جرائم الكمبيوتر أكثر خطورة من الجرائم التقليدية، فهي تخلف حجما كبيرا من الخسارة وتشيع القلق وتهدد مستقبل سوق المال وتمس حق الأفراد في المعلومات إلى جانب خطرها على السيادة الوطنية.

ورغم تزايد التحصينات التي تكفل الحماية لأي جهاز كمبيوتر وكذلك وضع قوانين مفعّلة، إلا أن خطر إنتهاك أمن وسلامة جهاز الكمبيوتر واختراقه مستمرة مع استمرارية محاولات التحصين.

لذلك بالموازاة مع محاولات ابتكار أنظمة تكفل حماية جهاز الكمبيوتر ووضع قوانين رادعة، لابد من وجود حملة توعية شاملة لأفراد المجتمع وخاصة فئة الشباب على إعتبار أن المجرم المعلوماتي في أغلب الأحيان صغير السن، وبذلك تكون التوعية على مستوى المدارس والجامعات وحتى وسائل الإعلام لأن التوعية وتقويم الأفكار يمكن أن تساهم في الحد من هذه الظاهرة المستحدثة.

وبما أن العالم مترابط إلكترونيا، فلا يجب الاهتمام بمشكلة الجرائم المعلوماتية وطنيا فحسب بل الاهتمام أيضا على المستوى العالمي وخاصة في مجال التشريعات والتعاون المتبادل، فهي عابرة للحدود أي أنها ذات طبيعة عالمية.

- قائمة المراجع:

الكتب:

- أحمد خليفة الملط (2006)، الجرائم المعلوماتية، ط 2، دار الفكر الجامعي، الإسكندرية مصر.

-أمير فرح يوسف (2011)، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والأنترنت، ط1مكتبة الوفاء القانونية، الإسكندرية مصر.

- حسنين شفيق (2015)، الإعلام الجديد والجرائم الإلكترونية – التسريبات، التجسس الإلكتروني، الإرهاب، دار فكر وفن للطباعة والنشر والتوزيع، مصر.

-رشيدة بوكر (2012)، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، ط 1، منشورات الحلبي الحقوقية، بيروت لبنان.

- رفيق الشلبي(1999)، مدى كفاءة الأجهزة الأمنية العربية في التصدي للظواهر الإجرامية، أكاديمية نايف العربية للعلوم الأمنية، الرياض السعودية.

- زليخة زيدان (2011)،الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة الجزائر.

- سعيد بن سالم البادي و آخرون(2016)، الجريمة الالكترونية في المجتمع الخليجي و كيفية مواجهتها، مجمع البحوث والدراسات، سلطنة عمان.

- صلاح سالم(2003) تكنولوجيا المعلومات و الاتصالات و اظلمن القومي للمجتمع، ط1، عين للدراسات والبحوث الإنسانية و الاجتماعية،مصر.

-عبد العالي الديربي ومحمد صادق إسماعيل (2012)، الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة، ط1 المركز القومي للإصدارات القانونية، القاهرة مصر.

- مجموعة من المؤلفين(2014 م- 1434 هـ) ، الظواهر الإجرامية المستحدثة وسبل مواجهتها، ط 1، الأكاديميون للنشر والتوزيع، دار الحامد للنشر والتوزيع، الأردن.

- محمد الأمين البشرى(2004م-1425هـ)، التحقيق في الجرائم المستحدثة، ط1، جامعة نايف العربية للعلوم الأمنية، الرياض السعودية.

- منير محمد الجنيهي وممدوح محمد الجنيهي(2006)، جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية مصر.

القوانين:

- قانون 09-04 مؤرخ في 16 شعبان 1430 الموافق لـ 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47 لسنة 2009.

الملتقيات:

-ذياب موسى البداينة، الجرائم الإلكترونية – المفهوم والأسباب-، ورقة مقدمة في الملتقى العلمي الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية، خلال الفترة من 7-1435/11/9 هـ الموافق لـ: 2-2014/09/4 م، كلية العلوم الاستراتيجية، المملكة الأردنية الهاشمية، عمان الأردن، 2014.

مواقع الانترنت:

- علا رضوان (2018)، الجريمة المعلوماتية من النشأة في الستينات إلى "القرصنة" في القرن الـ 21. الموقع http://www.soutalomma.com ، اطلع عليه يوم 2021/01/04.

-ياسمينة بونعارة، الجريمة الإلكترونية، بحث على موقع www.univ.emir.dz اطلع عليه يوم 2021/12/15 .

المجلات:

-عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة دراسات الكوفة، جامعة الكوفة مركز دراسات الكوفة، العراق، مجلد 5، عدد 7، 2008 .

-Jacques Francillon , Les crimes informatiques et d'autre crimes dans le domaine de la technologie informatique en France , Revue internationale de droit pénal , vol 64.France , 1993 .