

خصائص الفضاء السيبراني المهيئة للسلوك الإجرامي

Cyberspace characteristics predisposing to criminal behavior

دليلة جلول*

جامعة باتنة الجزائر dalila.djelloul@univ-batna.dz

تاريخ الاستلام: 2025/06/05 تاريخ القبول: 2025/06/15 تاريخ النشر: 2025/06/30

ملخص:

انتقلت كثير من السلوكات الإجرامية من الواقع المادي إلى الواقع الافتراضي، بصورة مرنة حيث وفر الفضاء السيبراني مجمعة من الظروف المهيئة لإرتكابها دون التقيد بعوامل الخطورة الموجودة في العالم الواقعي، ويرجع هذا إلى خصائص تقنية وإجتماعية سهلت الانتقال إلى الفعل الإجرامي، فكيف تساهم هذه الخصائص في حدوث الجريمة الإلكترونية؟ ولماذا يفضلها المجرم المعلوماتي دون العالم الافتراضي؟ من خلال اتباع المنهج الوصفي، تم جمع أهم خصائص العالم الافتراضي وبخاصة منها شبكات التواصل الإجتماعي، ثم من خلال المنهج التحليلي تم تحليل السلوك الإجرامي في ضوءها. وتم التوصل إلى أن شبكات التواصل الإجتماعي بالدرجة الأولى تعد الفضاء الخصب لارتكاب الجريمة الإلكترونية نظرا لسهولة استخدامها من طرف شريحة واسعة من الأشخاص، إلى جانب سهولة إخفاء الأثر الإجرامي نظرا لاعتماد الهوية المزيفة.

كلمات مفتاحية: المجرم المعلوماتي، الجريمة الإلكترونية، شبكات التواصل الإجتماعي، الفضاء السيبراني.

Abstract:

The traditional crimes had transmitted by the cyber criminals to be committed in the cyber space, where there are a lot of characteristics that facilitated the criminal

How and why these specific technological and social aspects pushed the .action cybercriminal to exerce the electronic crimes?

After using the descriptive and analytic method to analyse such aspects, the results showed that the social networks are the major field for cyber crimes because of the easy use from a large population, and the anonymity of criminals.
key words: the cyber crime, the social networks, the cyber space, the cyber criminal.

مقدمة:

ساعد مجال الدراسة في علم الإجرام والضحايا عن الكشف عن عوامل الخطورة المرتبطة بالأفعال الإجرامية، ومنها أيضا جاءت الدراسات الوقائية للحد من وقوع الجريمة، من خلال البحث في العوامل المهيئة للفعل الإجرامي، والدوافع الجنائية المحتملة لدى شريحة واسعة من المجرمين. ومع ظهور أنماط مستحدثة للسلوك الإجرامي ضمن الفضاء السيبراني، برزت مجموعة من الدراسات التخصصية في هذا المجال وتحديد الدراسات المتعلقة بسلوك المجرمين في الفضاء السيبراني منها على سبيل المثال التنمر الإلكتروني (Cyberbullying)، وقد عرف بأنه من المظاهر الاجتماعية للجريمة المعلوماتية (Igoneleon (Vicent,2015,19 وما يميز التنمر الإلكتروني عن التنمر التقليدي شكل دافعا لدراسة الظاهرة. حيث أشارت نتائج دراسة (Arslan,Savaser,Hallett and Balci,2012) أن 80% من ضحايا التنمر لا يعرفون هوية المتنمر (الشناوي، 2014، ص 4) وهذا بفضل خصائص الجريمة الإلكترونية التي يكون عامل التخفي فيها دافعا قويا للمتنمر (المعتدي عموما)، ومن جانب آخر للإعتداء فإن ضعف التعاطف الوجداني الذي ينبثق من أن المتنمر لا يرى آثار أفعاله على الضحية (الشناوي، 2014، ص 4) ولعل أهم ما يميز الظاهرة أن هناك مشاعر مؤلمة لشخص الضحية ومريحة للآخر (التنمر) عكس توازن القوة وتساويها في العدوان، غير أنها غير متوازنة في حالة التنمر، ومن هنا تبرز الحاجة الماسة لتدخل الكبار (الصباحين والقضاة، 2013، ص 13).

كما أن العالم الافتراضي وما يحتويه من وسائط متعددة صار فضاء رحبا لهذه الممارسات بعيدا عن الرقابة الاجتماعية أو الأمنية، نظرا لما يوفره من حرية متناهية وفرص متاحة باستمرار، مستثمرين مهاراتهم وفتياتهم الخاصة في مجال الأنظمة الرقمية. ففي حين يكون الأفراد منغمسين في تفاعلاتهم الافتراضية وفي علاقاتهم التبادلية لمختلف المتوجات، سواء كانت سلعا أو خدمات أو معرفة أو خبرات، منهمكين في تسوية مختلف الإجراءات اللازمة لإتمام العمليات التجارية، إذ تهاجمهم على حين غرة، ومن حيث لا يحتسبون، فلن ينتهوا

إلا بعد أن يجدوا سلعهم قد افتقدت وتم السطو عليها، دون أن يدركوا الطريقة أو الجهة الفاعلة والمسؤولة عن العملية الإجرامية، مما يجعل هؤلاء الضحايا يقعون في حيرة كبيرة واضطراب شديد يسيطر على نفسيتهم، تستمر أحقابا زمنية، ويصعب علاجها أو القضاء عليها في فترة قصيرة (قريعة و الجوزي، 2021، ص661-662).

إن الخصائص المرتبطة بالفضاء السيبراني بقدر ما توفر من تيسير في تفاعلات الحياة اليومية، توفر في الجانب الموازي فرصا كبيرة للمجرمين المعلوماتيين ومقتنصي الفرص لتحقيق أغراضهم الجنائية. ومع حتمية التطور التكنولوجي يقع على عاتق المستخدمين تطوير رصيدهم ومكتسباتهم المعرفية في طبيعة هذا الفضاء وخصائصه.

الإشكالية:

يشير مصطلح الفضاء السيبراني أو الافتراضي إلى عالم بديل بتشكيل في ذاكرة الحواسيب يخلق حالة من التواجد المكتمل، ويعطي أفقا آخر لتطور البشرية، وهو مصطلح ابتكره العالم "جورن لاينر" ويعمل الواقع الافتراضي على نقل الوعي الإنساني إلى بيئة افتراضية يتم تشكيلها إلكترونيا من خلال تحرر العقل للغوص في تنفيذ الخيال بعيدا عن مكان الجسد، وهو عالم ليس وهميا وليس حقيقيا بل دليل حدوثه ومعايشة بيئته، فيه يتم تنفيذ الأحداث في الواقع المفترض لكن ليس في الحقيقة (قريعة والجوزي، 2021، ص664).

ارتبط الفعل الإجرامي في الفضاء السيبراني بخصائص كثيرة، حيث أن ظرف الزمان والمكان على وجه التحديد جعل المجرم المعلوماتي يطور الكثير من المهارات والأساليب لنشاطه. كما أن التطور التكنولوجي مكن من برمجة الجرائم دون الحاجة لوجود شخص يقوم بذلك، وهناك العديد من جرائم القتل التي نفذت على الأشخاص دون الحاجة للتفاعل وجها لوجه، بل أنه تم تحديدها وتوقيتها مسبقا. تترجم أهداف الجريمة المعلوماتية الكثير من الدوافع التي يبحث المجرم المعلوماتي لتحقيقها، فقد تكون دوافع شخصية مرتبطة بالفضول وتحدي المهارات الذاتية، أو رغبة في الانتقام من شخص معين عن طريق الإبتزاز الإلكتروني أو السب والشتيم، أو التهديد كما قد تكون دوافع أمنية، سياسية أو اقتصادية.

إن ارتباط الإجرام الإلكتروني بالفضاء السيبراني إنطلق من مساحة كبيرة من الحرية وضعف المراقبة على هذا النشاط، ما أثار التساؤلات التالية:

ما هي أهم خصائص الفضاء السيبراني المهينة للسلوك الإجرامي المعلوماتي؟

كيف تشجع هذه العوامل على ارتكاب الجريمة المعلوماتية خارج هذه الخصائص؟

ضمن الورقة البحثية تم الاعتماد على المنهج الوصفي، لمعالجة المعلومات وتحليلها للإجابة عن تساؤلات الدراسة، من خلال انتهاج العناصر البحثية التالية:

1. الخصائص المرتبطة بظرفي الزمان والمكان:

المجتمع المعلوماتي لا يعترف بالحدود الجغرافية فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود. فبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالمقدرة التي تتمتع بها الحواسيب وشبكتها في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الأميال قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد. فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان ارتكاب جريمة عن طريق الحاسوب موجود في دولة معينة يتحقق الفعل الإجرامي في دولة أخرى.

تكمن أهم المشاكل المتعلقة بالتعاون الدولي حول الجريمة المعلوماتية في أنه لا يوجد هنا مفهوم عام مشترك بين الدول حول صور النشاط المكون لهذه الجريمة. بالإضافة إلى نقص الخبرة لدى الشرطة في وجهات الإدعاء والقضاء في هذا المجال لتمحيص عناصر الجريمة إن وجدت وجمع الأدلة عنها للإدانة فيها يشكل عائقا كذلك أمام التعاون في مجال مكافحة ذا النوع من الجرائم (مومني، 2010، ص 52-53).

فالفكرة تلخص في أن مرتكبي الجرائم يستغلون الثغرات القانونية المتمثلة في:

- 1- صعوبة التوصل إلى اتفاق عالمي حول نوعية الأفعال والأنشطة التي تدخل في نطاق الجرائم المعلوماتية.
- 2- عدم وجود اتفاق عالمي موحد حول التعريف القانوني للسلوك الإجرامي.
- 3- غياب التعاون بين الدول فيما يتعلق بتبادل المتهمين في تلك الجرائم وتسليمهم للقضاء (جلي و أحمد، 2011، ص 220).

وبالتالي من أجل التصدي للإجرام المعلوماتي لا بد أن تعمل الدول في اتجاهين:

الأول: داخلي حيث تقوم الدول المختلفة بسن القوانين الملزمة لمكافحة هذه الجرائم.

الثاني: دولي عن طريق عقد الاتفاقيات الدولية، حتى لا يستفيد مجرمو المعلوماتية من عجز التشريعات الداخلية من ناحية، وغياب الاتفاقيات الدولية التي تتصدى لحماية المجتمع الدولية من نتائج وآثار هذه الجرائم (مومني، 2010، ص 53).

مفهوم الزمان والمكان في مجال الجريمة المعلوماتية يعتبر من المؤشرات القوية في تحليل طبيعة السلوك الإجرامي، ذلك أن وقوع الجريمة يكون بصورة كبيرة في الفترة الليلية حيث تضعف وتراجع مستويات الرقابة الشعورية للسلوك تحت تأثير تغيرات بيولوجية عصبية، وكذلك مستوى الأكسجين في الدماغ لأن طبيعة الدورة الدموية المغذية للخلايا العصبية تكون غنية بالمواد السامة، ومن هنا تكون عملية التحليل المنطقي ومستويات الإدراك والإنتقاء المعرفي أقل كفاءة منها في الفترة الصباحية. لذلك فإن أغلب الممارسين في مجال مكافحة الجريمة المعلوماتية، ينصحون بتجنب التواصل الافتراضي واتخاذ القرارات في مجال التجارة الإلكترونية مثلا أو التوقيع الإلكتروني في الفترة المسائية.

2. الخصائص المرتبطة بآثار الجريمة المعلوماتية:

من أبرز خصائص الجريمة المعلوماتية الغفلية anonymity، وتعني غياب الهوية والاسم المحدد absence of identity، حيث يمكن استخدام أسماء مستعارة وغير حقيقية، فالإنسان يستطيع أن يتفاعل مع آخرين في الفضاء الإلكتروني دون أن يحدد أو يذكر شخصيته الحقيقية، مستخدما أسماء مستعارة، وأماكن غير محددة، وحقائق غير صادقة، وقد يسر الأنترنت تلك الغفلية في هذا المجال.

وساعدت الغفلية الأفراد على ارتكاب أفعال وأنشطة إجرامية مع إخفاء شخصياتهم الحقيقية، لذا يتعذر اكتشاف شخصية القائم بهذا النشاط غير القانوني، فلا تستطيع السلطات المختصة تحديد هوية مرتكب هذا النشاط ومعاقبته. وفي بعض الأحيان، يعتمد المجرم أيضا على عمليات التخفي proxy 70 أثناء التجوال عبر الأنترنت، التي تسمح لمستخدمها بالانطلاق على أي موقع على الشبكة دون أن يتم اكتشاف الشخص الذي زار تلك المواقع. وعلى الرغم من أهمية البروكسيات والهدف الذي صممت من أجله لتأمين الشبكات والمواقع ضد عمليات الاختراق، إلا أنها استغلت استغلالا سيئا، حيث يصعب الوصول إلى الفرد الذي يستخدم تلك التكنولوجيا. كما أن الأمر لم يقف عند هذا الحد، بل يقوم صانعو الفيروسات من خلال استخدام تلك التكنولوجيا بإطلاق فيروساتهم، مما يشكل صعوبة في التوصل لمرتكب هذا الفعل الإجرامي. (جلبي و أحمد، 2011، ص 218).

نظرا للطابع الخاص الذي تتميز به الجريمة المعلوماتية، فإن إثباتها يحيط به كثيرا من الصعوبات، والتي تتمثل في صعوبة إكتشاف هذه الجرائم، لأنها لا تترك أثرا خارجي. فالجرائم المعلوماتية لا عنف فيها، ولا سفك دما، ولا آثار اقترام لسرقة الأموال مثلا. وإنما هي أرقام وبيانات تتغير أو تمحى من السجلات المخزنة في ذاكرة الحواسيب وليس لها أي أثر خارج مرئي.

وهي جريمة هادئة لا تتطلب العنف، ورغم كل ذلك فإن البعض يشبه هذه الجرائم بجرائم "العنف الرقمي" مثل ما ذهب إليه مكتب التحقيقات الفيدرالي بالولايات المتحدة الأمريكية FBI نظرا لتماثل دوافع المعتدين على نظام الحاسوب مع مرتكبي العنف.

فإذا تم اكتشاف الجريمة المعلوماتية، فلا يكون إلا بمحض الصدفة، نظرا لعدم وجود أثر كتابي لما يجري خلال تنفيذها من عمليات حيث تم بالنبضات الإلكترونية نقل المعلومات، ولذلك يستطيع المجرم تدمير دليلا لإدانة في أقل من ثانية، إلى جانب إمكانية ارتكابها عبر الوطنية والقارات دون عناء التنقل (الريان، 2004، ص 53-54).

غالبا لا يمكن تحديد حجم الأثر المعنوي الذي تحدثه الجريمة المعلوماتية، ولا حتى الاقتصادي لسبب بسيط وهو غياب التبليغ خوفا من وصمة العار. أما تفسير استغلال هذه الخاصية كدافع لاقتراف الجريمة المعلوماتية، فيرجع لمرحلة مهمة من التفكير الإجرامي وهي لحظة التحضير المسبق للجريمة المعلوماتية قبل المرور إلى الفعل *le passage à l'acte criminel*، حيث أن المجرم يستغل عوامل ضعف الضحية ويدرسها جيدا ليستغلها كنقاط قوة بالنسبة إليه فيلجأ إلى استخدام حسابات مزورة أو وهمة للإيقاع بضحاياه، كما يسعى إلى التغيرير بهم واستدراجهم قدر المستطاع باستخدام اللغة أو الدعاية الإلكترونية المستندة إلى الخطاب الوجداني، والذي يجعل الرشادة العقلانية القائمة وراء اتخاذ القرارات والتفضيلات السلوكية كما هو الحال في التسويق الإلكتروني في مستوى متدني.

3. الخصائص المرتبطة بطبيعة الفضاء السيبراني:

يوفر الفضاء السيبراني مجموعة من الظروف التي تميزه عن الفضاء الواقعي، وتتمثل في كل من (عبد الجليل، 2017، ص 76):

- غياب التفاعل الجسدي، حيث لا يوجد تفاعل جسدي بين الأطراف المتواصلة (الجاني، المجني عليه)، ولا تتطلب طاقة وشجاعة كبيرة في مواجهة الضحايا مثل العنف التقليدي، كما يعتمد على المهارة والكفاءة الذهنية والعقلية وليست الجسدية.

- سهولة الوصول للضحية وصعوبة دفاعها عن نفسها حيث يمكن الوصول للضحية في أي وقت ليلا ونهارا وفي أي وقت وفي أي مكان، كما يصعب على الضحية تجنب العنف الواقع عليها، أو الدفاع عن نفسها أو القضاء على هجوم المجرم.

- يتطور الإجرام في الفضاء السيبراني بصفة مستمرة مع تطور الأساليب التكنولوجية الحديثة التي تساعد، على بقاء أثر هذا العنف لوقت طويل، كما أنها سلوكيات مستمرة في معظم أحوالها كما في حالات السب والقذف والتشهير ما لم يتم ضبط الفاعل والتدخل الفني لإنهائها.

- سهولة حدوثه وسرعة انتشاره، وذلك بسبب سرعة انتشار المعلومات الخبيثة والمكذوبة والشائعات وسهولة الوصول إليها، وغالبا ما تكون غير قابلة للاسترجاع، فبمجرد نشرها على الانترنت لا يستطيع المجرم إيقافها. - غياب التفاعل الجسدي، حيث لا يوجد تفاعل جسدي بين الأطراف المتواصلة (المجرم والضحية)، ولا تتطلب طاقة وشجاعة كبيرة في مواجهة الضحايا مثل العنف التقليدي، كما يعتمد على المهارة والكفاءة العقلية وليست الجسدية.

يشكل الفضاء السيبراني مجالا للتحدي المستمر، حيث يشهد مستخدميهم مهاراتهم التكنولوجية باستمرار، لمواكبة التغيرات السريعة مما يلبي احتياجاتهم المعرفية. حيث أن تقدير الذات لديهم يرتبط بمدى القدرة على الإنجاز، والتمكن من استخدام المهارات الجديدة والتمكن من استخدام التطبيقات المستحدثة.

4. الخصائص المرتبطة بمواقع التواصل الاجتماعي:

تتميز شبكات التواصل الاجتماعي بعدة خصائص تجعلها وسيط مناسب بحدوث وانتشار مظاهر العنف الإلكتروني، ومن هذه الخصائص:

1.4. **الجدّة والدوام:** وذلك لأن تأثيرها والتفاعلات تكون فورية ومتجددة دائما، مع إمكانية التغيير الفوري وتفسير منشوراتها عبر التعليقات وتطويعها لأغراض أخرى.

2.4. **التوازن:** وذلك بين الحرية والخصوصية في التفاعل بين المشتركين، فبقدر ما يستطيع الفرد أن يعبر عن ذاته بحرية تامة دون قيود، وينشر آراءه وأفكاره وتعليقاته يجد قدرا كبيرا من الخصوصية في تفاعلاته مع الآخرين.

3.4. **التفاعلية:** وتعد من أهم خصائص شبكات التواصل الاجتماعي حيث وجود مرسل ومستقبل، وتكون الأدوار قابلة للتبديل بينهما، ووجود تأثير متبادل لكل منهما على الآخر.

4.4. **التكرارية:** بمعنى أنه من السهل نسخ صورة أو تعليق أو مقال أو فيديو ما على الانترنت لموقع آخر بدون تغيير أي من ملامحه.

5.4. **البحث:** وهي قابلية البحث عن أصدقاء ذوي اهتمامات واتجاهات متشابهة وهو ما لا يمكن عمله في الحياة العادية.

كل مستهلك هم ومنتج: حيث إن أي عضو على شبكات التواصل الاجتماعي يمكنه النشر بمجرد أن يصبح عضواً، ما أن أي مستخدم يمكنه كتابة وتعديل وإزالة أي منشور، وأن يقرر ما إن كان سيسمح بالتعليقات أم لا (عبد الجليل، 2017، ص 77-78).

التواصل والتفاعل الافتراضي عبر مواقع التواصل الاجتماعي، يعتمد على العديد من مهارات التفاعل الاجتماعي الواقعي، غير أن هناك بعضاً من الخصوصية والحماية التي توفرها فضاءات التواصل الاجتماعي تجعل الرقابة التي يمارسها الأنا الأعلى على السلوكات الإجتماعية ضعيفة، ومرد ذلك عدم ووضوح معالم الجريمة المعلوماتية في وسط المستخدمين، وعدم مواكبة النصوص القانونية للتطورات التكنولوجية بما يسهل نفاذ المجرمين من العقوبات لان القوانين لا تنطبق على سلوكياتهم الإجرامية المستحدثة.

5. الخصائص المرتبطة بالجرم والضحية في الجريمة المعلوماتية :

1.5. المجرم المعلوماتي: المجرم الذي يقترف الجريمة المعلوماتية الذي يطلق عبه المجرم المعلوماتي يتسم بخصائص معينة تميزه عن المجرم الذي يقترف الجرائم التقليدية.

فإذا كانت الجرائم التقليدية لا أثر فيها للمستوى العلمي والمعرفي للمجرم في عملية ارتكابها —باعتبارها قاعدة عامة— فغن الأمر يختلف بالنسبة للجرائم المعلوماتية فهي جرائم فنية تقنية في الغالب الأعم، ومن يرتكبها عادة يكون من ذوي الاختصاص في مجال تقنية المعلومات، أو على الأقل شخص لديه حد أدنى من المعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الأنترنت.

فعلى سبيل المثال فإن الجرائم المعلوماتية ذات الطابع الاقتصادي مثل التحويل الإلكتروني غير المشروع للأموال يتطلب مهارة وقدرة فنية عالية جداً من قبل مرتكبها.

كذلك فإن الدوافع على ارتكاب المجرم المعلوماتي هذا النوع من الإجرام المعلوماتي قد تكون مختلفة عن دوافع ارتكاب الجرائم من قبل المجرم التقليدي (مومني، 2010، ص 58-59).

تتميز الجريمة المعلوماتية بأنها تتم عادة بتعاون أكثر من شخص على ارتكابها إضراراً بالجهة المجني عليها، وغالباً ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والانترنت يقوم بالجانب الفني من المشروع الإجرامي، وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه.

والاشتراك في إخراج الجريمة المعلوماتية على حيز الوجود قد يكون اشتراكا سلبيا وهو الذي يترجم بالصمت من جانب من يعلم بوقوع الجريمة في محاولة منه لتسهيل إتمامها، وقد يكون اشتراكا إيجابيا وهو غالبا كذلك يتمثل في مساعدة فنية أو مادية (مومني، 2010، ص58).

الجريمة المعلوماتية نشاط إجرامي منظم وخاضع للتحقيق، وهذا التخطيط لا يكون إلا من خلال أفراد مؤهلين في هذا النوع من النشاط، الذي يعتمد على المعرفة بتقنيات الحاسوب والأنترنت، فالجريمة المعلوماتية ليست نشاطا إجراميا عشوائيا، بل يخضع لتخطيط مسبق، ومن ناحية أخرى تعد الجريمة المعلوماتية جريمة منظمة لكونها تعتمد على أساليب تكنولوجية أكثر تعقيدا، وتلك الأساليب تكون أكثر صعوبة في الاكتشاف صعوبة في الاكتشاف من قبل أفراد الأمن (جلي و أحمد، 2011، ص220).

2.5. الضحية في الجريمة المعلوماتية: يلعب الضحية دورا رئيسيا في صعوبة اكتشاف وقوع الجريمة المعلوماتية حيث تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك أو تمنى بخسائر فادحة من جراء ذلك على عدم الكشف حتى بين موظفيها عما تعرضت له وتكتفي عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنباً للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها.

ويرى البعض أن للمجني عليه دورا مثيرا للريبة في بعض الأحيان، فهو قد يشارك بطريق غير مباشر في ارتكاب الفعل، وذلك بسبب وجوده في ظروف تجعل تعرضه لجريمة المعلوماتية أمرا مرتفعا بشكل كبير، ويرجع ذلك بشكل أساسي إلى القصور الأمني الذي يعترى الأنظمة المعلوماتية الذي قد يساعد على ارتكاب الفعل الإجرامي، ويترتب على ذلك نتيجة أخرى تميز الجريمة المعلوماتية هي أن هناك إمكانية للحيلولة دون وقوع هذه الجريمة مقارنة بغيرها من الجرائم، غذ يعتمد ذلك أساسا على تطوير نظم الأمن الخاصة بأنظمة الحاسبات وشبكاتها.

وفي الواقع فإن إحجام المجني عليه عن الإبلاغ عن وقوع الجرائم المعلوماتية يبدو أكثر ووضحا في المؤسسات المالية مثل البنوك والمؤسسات الإذخارية، حيث تخشى مجالس إدارتها من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية حيالها على تضائل الثقة فيها من جانب المتعاملين معها. حيث أن الجانب الأكبر من الجرائم المعلوماتية لا يتم الكشف أو التبليغ عنه فإن ذلك يؤثر سلبا في السياسة التي يمكن أن توضع لمكافحةها، وقد تم طرح عدة اقتراحات تكفل تعاون المجني عليه في كشف هذه الجرائم وبالتالي إنقاص حجم الإجرام المعلوماتي الخفي.

وإلى جانب ذلك فإن المجني عليه يتردد أحيانا في الإبلاغ عن هذه الجرائم خوفا من أن الكشف عن أسلوب ارتكاب هذه الجرائم قد يؤدي إلى تكرار وقوعها بناء على تقليدها من قبل الآخرين كما أن الإعلان عن هذه الجرائم يؤدي أحيانا إلى الكشف عن مواطن الضعف في برنامج المجني عليه ونظامه المعلوماتي مما يسهل عملية اختراقه (مومني، 2010، ص 54-55).

فقدان الثقة في تعامل السلطات المختصة مع مرتكبي تلك النوعية من الجرائم، وذلك لعدم كفاءة القوانين المعمول بها (جلبي و أحمد، 2011، ص 220).

من خلال تحليل سلوكيات المجرم والضحية والدوافع الجنائية، نجد بأن عامل الاستخدام هو الوعي الحقيقي ولا تنفع الحملات التحسيسية أو غيرها في رفع درجته، بمعنى يجب أن يطرح المستخدم السؤال الهدف والمغزى من استخدامه للإنترنت هل لأغراض طيبة أو إجرامية.

6. عوامل إنتشار الجريمة المعلوماتية:

فضلا عن الخصائص التي توفر بيئة خصبة لارتكاب الجريمة المعلوماتية، هناك عوامل كثيرة تساهم في إنتشارها نذكر منها مجموعة العوامل التالية (محمد فولان، 2010، ص 41):

- لا مركزية الأنظمة المعلوماتية، إذ كلما كثرت أجهزة الحاسوب المتصلة بالشبكة الأم كلما كثرت احتمالات الدخول إلى الشبكة.

- ترابط الأنظمة المعلوماتية في كل المستويات سواء الداخلية منها أو الدولية والخاصة أو العامة فإن ربط الشبكة لتبادل المعلومات يعرضها لخطر الفيروسات والدخول غير الشرعي.

- العراقيل ومحدودية البحث، أين تشكل حدود الدول عرقلة جدية لضمان تحديدها بدقة ومعاقبة مرتكبيها بصرامة فلكل دولة تشريعها الخاص لمواجهة الظاهرة علما أن كثيرا من الدول ما تزال تفتقر إلى تشريع في هذا الميدان، ولذلك تعتبر الجزائر من الدول العربية السباقة في هذا الميدان.

- تحديد هوية ومكان المعتدي، ولا يمكن التغلب على هذه الصعوبة إلا بالدخول لبطاقات التخزين لموردي الإنترنت مع ضمان الحياة الخاصة للأفراد.

- ماهية وطبيعة التطورات المعاصرة في البيئة الإقتصادية العالمية، إن التطورات الهائلة التي حدثت خلال السنوات الأخيرة يمكن إرجاعها إلى عنصرين رئيسيين هما تطور التقنية، وهيئة البيئة العالمية المناسبة. يتمثل العنصر الأول في مدى التطورات الهائلة في تكنولوجيا المعلومات والاتصالات، في حين يتمثل العنصر الثاني

في توفير وإتاحة وتهيئة البيئة لانتقال كافة التغيرات ونفاذها من مكان لآخر بدون مواجهة أية حواجز جغرافية، وهو ما يعرف بعملة السوق أو الإقتصاد (أمير يوسف، 2008، ص 19).

- صورة المعلومات وتطورات المجتمع المعلوماتي: لقد أصبحت المعلومات في بيئة اليوم ترتبط بمختلف جوانب الحياة وتمثل ركيزة نشاط الإنسان الإقتصادي والإجتماعي والثقافي والسياسي، وتتيح المعرفة بالواقع ومشكلاته وأبعاد هذه المشكلات، بل إنها أصبحت تتيح ميكنة إتخاذ القرارات في كافة المجالات تقريبا، وعلى الرغم من تعدد المصطلحات التي تطلق على ثورة المعلومات، إلا أنه بات هناك نوع من الإتفاق حول مسمى المجتمع المعلوماتي للتعبير عن التقدم التكنولوجي. وتتمثل المكونات الرئيسية للمجتمع المعلوماتي في ثلاثة مكونات رئيسية، هي الحواسيب والإتصالات، والشبكات والوسائط المتعددة (يوسف، 2008، ص 20).

- تزايد وعي المجرمين بارتفاع عائد جرائم المعلوماتية، وتدني مخاطرها إذا ما قورنت بأية جريمة أو نشاط إجرامي آخر.

- إحباط وإستياء أفراد الطبقة المتوسطة من المجتمع من الأوضاع والضغط الإقتصادية المهينة - تحت وطأة ما قد يتعرضون له من مشاكل حادة - لاستغلال مراكزهم الوظيفية في إدارة وتشغيل الحاسوب لارتكاب الجرائم باستخدامه (محمد سلامة، 2006، ص 17).

خاتمة:

إن الاستخدام السوي للتقنيات التكنولوجية يخضع لإرادة الإنسان في توجيه هذا الاستخدام، كما أن وضوح الهدف والغاية هما الضمانين الوحيدين للوعي التكنولوجي، والاستجابة لليقظة التكنولوجية والتربية الإعلامية الموجهة للمستخدمين في هذه الخصوص. وفي ختام الدراسة الوصفية لموضوع الورقة البحثية توصلنا لمجموعة من النتائج، ومجموعة من التوصيات المقترحة.

النتائج:

1- التبليغ هو المفتاح الأول للوقاية من انتشار الجريمة المعلوماتية، وتوفير أقصى قدر من الحماية من المجرم المعلوماتي.

2- الأثر المعلوماتي يمكن الحصول عليه ولو كان المجرم محترفا و متمكنا في مجال المعلوماتية، إلا أن كل ما يحدث على فضاء الأنترنت يمكن العثور عليه وغير أن الأمر قد يتطلب مهارات متحدة ومدة زمنية أطول.

3- الإعلانات المتخللة لمواقع التواصل الاجتماعية المختلفة، تعتمد على مبادئ الإقناع السيكلوجية المركزة على الخطاب الوجداني، لتغيب المنطق التحليلي وفقا لما تنص عليه نظرية الترشيح العقلاني في علم التسويق.

4- سهولة التخفي وراء أسماء مستعارة أو استخدام حواسيب عمومية مختلفة لممارسة نشاطه الإجرامي، تدفعه لارتكاب الجرائم بسهولة.

5- وجود العديد من المستخدمين الذين لا يتقنون التحكم في التكنولوجيا ما يجعلهم عرضة للتعدي المعلوماتي، ويسهل التغرير والإيقاع بهم.

6- هناك علاقة طردية إيجابية بين التطور التكنولوجي وتطور الجريمة المعلوماتية.

التوصيات: نقترح التوصيات التالية:

1- تعزيز القيم والروابط الأسرية والاجتماعية داخل الأسرة ومنها إلى المجتمع، مع تفعيل أنشطة اجتماعية تشاركية خاصة لفئة الأطفال والمراهقين من طرف مختلف فعاليات المجتمع المدني.

2- تنصيب برامج الحماية الأمنية الموثوقة والأصلية ضمن أجهزة الحواسيب والابتعاد عن برامج التحميل المجاني.

3- تحيين المعلومات الشخصية سواء من المواطنين أنفسهم من خلال التكوين والدراسة، أو من خلال الدورات التكوينية للموظفين في القطاعين العام والخاص.

4- عدم الاستهتار أمام الاستخدام العشوائي للإنترنت والحسابات المختلفة لمواقع التواصل الاجتماعي من خلال نشر الصور الخاصة، أو الفيديوهات القصيرة.

5- الابتعاد عن استخدام مواقع التواصل الاجتماعي للتسلية، وتعويضها بأنشطة ومهارات حياتية واقعية كالرياضة أو ممارسة الهوايات المختلفة.

6- الرقابة الأسرية والتوعية للأطفال والمراهقين بصورة دورية أو مستمرة، تسمح بالوقاية من خطر التصيد المعلوماتي وتجنب الوقوع في فخ الابتزاز الإلكتروني.

قائمة المراجع:

إبراهيم، ريهام السيد عبد الجليل (أوت 2017)، دور الجامعة في مواجهة مخاطر العنف الإلكتروني عبر شبكات التواصل الاجتماعي "دراسة تحليلية"، مجلة تطوير الأداء الجامعي، المجلد 05، العدد 02، مصر، ص1-16.

العريان، محمد علي (2004)، الجرائم المعلوماتية، د ط، دار الجامعة الجديدة للنشر، مصر.

جابوري، اسماعيل (ديسمبر 2020)، دور الأمن السيبراني في مواجهة التهديدات الإلكترونية دراسة حالة الجزائر، مجلة تحولات، المجلد 03، العدد 02، الجزائر، ص 65-80.

جلي، علي عبد الرزاق و أحمد، هاني خميس (2011)، العولمة والحياة اليومية، ط1، مكتبة الأنجلو المصرية، مصر.

فولان، محمد (2010)، الحماية القانونية لتكنولوجيات الإعلام، مجلة المحكمة العليا، العدد الأول 01، قسم الوثائق، المؤسسة الوطنية للاتصال النشر والإشهار وحدة الطباعة، الجزائر.

سلامة، محمد عبد الله أبوبكر (2006)، جرائم الكمبيوتر والإنترنت، ط1، منشأة المعارف، مصر. مومني، نهلا عبد القادر (2010)، الجرائم المعلوماتية، ط1، دار الثقافة للنشر والتوزيع، الأردن.

يوسف، أمير فرج (2008)، الجرائم المعلوماتية على شبكة الإنترنت، بدون طبعة، دار المطبوعات الجامعية، مصر.

قريعة، عمر والجوزي، وهيب (2021)، العالم الافتراضي فضاء خصب لممارسة الجريمة الإلكترونية في ميدان التجارة الإلكترونية، مجلة علوم الإنسان والمجتمع، المجلد 10، العدد 02، الجزائر، ص 689-657.

الشناوي، أمنية إبراهيم (2014)، الكفاءة السيكومترية لمقياس التنمر الإلكتروني (الضحية-المعتدي). pdf

الصباحين، علي موسى والقضاة، محمد فرحات (2013)، سلوك التنمر عند الأطفال والمراهقين (مفهومه-أسبابه-علاجه)، ط1، جامعة نايف للعلوم العربية الأمنية، الرياض: السعودية.

Vicente, Igone Leon (2015) : cybervictimization by cyberbullying
« children at risk and children as risk ».

تم تصفح الدراسة من الموقع Addi. ehu.es بتاريخ: 2017/3/12، على الساعة: 14.17