الرقم الأسود في الجرائم المتعلقة بأنظمة معالجة المعطيات

The dark figure of crimes related to data processing systems

زراري نسرين *
- جامعة عباس لغرور خنشلة
مخبر البحوث القانونية السياسية والشرعية
zerari.nesrine@univ-khenchela.dz

بوقرة إسماعيل
- جامعة عباس لغرور خنشلة
مخبر البحوث القانونية السياسية والشرعية
smailbouguerra3@gmail.com

تاريخ الإيداع:2021/05/08 تاريخ المراجعة:2022/01/22 تاريخ القبول:2022/01/23

ملخص:

نهدف من خلال هذه الدراسة إلى تسليط الضوء على الرقم الأسود في الجرائم المتعلقة بأنظمة معالجة المعطيات. فغايتنا هي محاولة إبراز أهم الأسباب التي تؤدي إلى إرتفاع الرقم الأسود في الجرائم المتعلقة بأنظمة معالجة المعطيات، لأن إرتفاع الرقم الأسود في هذا النوع من الإجرام وعدم إكتشاف الجرائم المتعلقة به، وعدم القبض على جناتها يؤثر تأثير سلبي على السياسة الجنائية التي وضعتها الدولة بغرض مكافحته.

ولعل أهم النتائج التي تتجلى لنا من خلال هذه الدراسة تتمثل في خصوصية الجرائم المتعلقة بأنظمة معالجة المعطيات والتي تؤدي إلى إرتفاع الرقم الأسود من خلال صعوبة كشفها، وكذلك ضعف الوعي لدى ضحايا هذه الجرائم وهذا ما ترجمته الإحصائيات الجنائية من خلال عدم تبليغهم عنها والتكتم عليها، ناهيك عن دور الجاني في إرتفاع الرقم الأسود من خلال إخفاءه وتدميره للدليل الرقمي بعد إرتكابه للجرائم المتعلقة بأنظمة معالجة المعطيات مباشرة.

الكلمات المفتاحية: الرقم الأسود؛ نظم معالجة المعطيات؛ الجريمة المعلوماتية؛ الجاني المعلوماتي؛ المجني عليه.

Abstract:

The present study aims at shedding light on the issue of dark figure of crimes related to data processing systems. Accordingly, the study opts for revealing the major factors and causes that prompt a rise of the dark figure which imperatively affect the criminal policy deployed by the state to combat crime as more criminals are either loose or unknown and more crimes are undetected.

Consequently, the study revealed that dark figure crimes are extremely peculiar vis-à-vis data processing systems that makes crimes hard to detect and victims unwilling to report such crimes due to their lack of conscience combined with a deliberate destruction of crime's

* المُؤلف المُراسِل.

evidences and leads committed by the felon himself which are proven by official criminal statistics.

Keywords: dark figure; data processing systems ; cyber crime ; cyber criminal; victim.

مقدمة:

إن التطور التكنولوجي والاستخدام المتزايد للوسائل والآليات المعلوماتية المختلفة، أدى إلى ظهور نوع جديد من الإجرام يتمثل في الإجرام المعلوماتي الذي جاء نتيجة الإستخدام السلبي ولأغراض غير شرعية للتكنولوجيات الحديثة، فظهور هذا الإجرام ما هو إلا إنعكاس للتطور الذي شهده العالم والعصر الذي نعيشه والذي سُمي بعصر الرقمنة، وبطبيعة الحال فالجريمة التي هي ظاهرة إجتماعية تواكب التطورات والتكنولوجيات المستحدثة والانترنت فهي تطورت بتطور هذه التكنولوجيات الحديثة، حيث أصبحت المعطيات والبيانات والمعلومات هي محل الجريمة فلم يعد المال المادي هو محلها مثلما كان في السابق وإنما أصبح المال المعنوي هو المستهدف والمرجو من قبل المجرمين المعلوماتيين.

والجريمة المعلوماتية شتان بينها وبين الجريمة التقليدية لأنها تتميز بطابع خاص يميزها عن غيرها من الجرائم فهي ترتكب في بيئة معنوية تختلف عن البيئة التي تكون فيها الجريمة التقليدية، وكذلك "المجرم الرقمي" أو "المجرم المعلوماتي" يختلف كثيرا عن المجرم التقليدي من حيث خصائصه ومميزاته فهو يُشترط فيه الذكاء والمهارة والقدرة على التحكم في التكنولوجيات الحديثة وإستخدامها.

ونظرا لتفاقم هذه الجريمة في المجتمعات أصبحت كل الدول تنتهج سياسات معينة لأجل التصدي لهذا النوع من الإجرام بغرض التقليل منه ولما لا إستأصله من المجتمع، ولغرض مكافحة هذه الجرائم لابد من تقديم تفسير علمي لهذه الظاهرة الإجرامية بغية الإحاطة بها من جميع جوانبها والكشف عنها، وذلك من خلال إعتماد الأساليب المتبعة في العلوم الجنائية، ومن أهم الأساليب التي تُستخدم في هذا المجال الأسلوب الإحصائي الذي من خلاله يتم تحويل وترجمة الظاهرة الإجرامية إلى لغة الأرقام.

والعالم المختص في علم الإجرام من خلال استخدامه للأسلوب الإحصائي يتجلى له ثلاثة أنواع من الإجرام تتمثل في الإجرام القانوني والإجرام الظاهر والإجرام الحقيقي، ففي الغالب الجرائم المتعلقة بأنظمة المعطيات يتم ارتكابها من طرف الجناة لكنها تبقى مخفية ولا تصل لعلم السلطات وهذا يعتبر عائق للباحث المختص في علم الإجرام الذي يدرس الظاهرة الإجرامية من جميع جوانبها ليجد الحلول المناسبة لمكافحة هذه الظاهرة الإجرامية والمتمثلة في دراستنا في الإجرام المتعلق بأنظمة المعالجة الآلية للمعطيات، وذلك حتى يجد سبل تطويقها. ولهذا ارتأينا من خلال هذه الدراسة البحث عن الرقم الأسود في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات.

وعليه نطرح الإشكالية التالية: فيما تتمثل أسباب ارتفاع الرقم الأسود في الجرائم المتعلقة بأنظمة معالجة المعطيات؟

تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف التي نوجزها في ما يلي:

التعرف على الرقم الأسود في الجرائم المتعلقة بأنظمة معالجة المعطيات، والتطرق إلى الخصوصيات المميزة للجرائم المتعلقة بأنظمة معالجة المعطيات التي تساهم بشكل مباشر في تضخم الرقم الأسود، ضف إلى ذلك التطرق لدور الجاني المعلوماتي في إرتفاع الرقم الأسود وإلى خطورته الإجرامية، والتطرق كذلك للمجني عليه ودوره في التكتم عن الجريمة والنتائج المترتبة عن هذا التكتم.

إتبعنا المنهج الوصفي التحليلي لأن هذه الدراسة ذات طبيعة إستكشافية، لذا تم الإعتماد على المنهج الوصفي التحليلي لجمع المعلومات والبيانات وتحليلها، وكذلك تحليل نتائج بعض الإحصائيات بهدف تقديم صورة وصفية للموضوع المدروس.

وسنجيب على الإشكالية الآنفة الذكر من خلال الخطة التالية:

المحور الأول: العلاقة بين الرقم الأسود والجرائم المتعلقة بأنظمة معالجة المعطيات

المحور الثاني: دور الجاني والمجني عليه في بروز الرقم الأسود في الجرائم المتعلقة بأنظمة معالجة المعطيات

المحورالأول: العلاقة بين الرقم الأسود و الجرائم المتعلقة بأنظمة معالجة المعطيات

تعتبر الجرائم المتعلقة بأنظمة معالجة المعطيات من الجرائم المستحدثة التي تختلف كثيرا عن الجرائم التقليدية من جميع جوانبها، وذلك يعود لعدة أسباب منها ما هو مرتبط بخصوصية الجريمة في حد ذاتها، كونها جريمة سيبرانية محلها أنظمة معالجة المعطيات. ولمعرفة أسباب وجود الرقم الأسود في هذه الجرائم نتطرق في المقام الأول إلى مفهوم الرقم الأسود في الجرائم المتعلقة بأنظمة معالجة المعطيات (أولا)، ثم في المقام الثاني نتطرق إلى مبررات وجود الرقم الأسود في جرائم المساس بأنظمة المعالجة الآلية للمعطيات التي ترجع للجريمة في حد ذاتها (ثانيا).

أولا: مفهوم الرقم الأسود في الجرائم المتعلقة بأنظمة معالجة المعطيات

1_ تعريف الرقم الأسود:

الرقم الأسود أو ما يُعرف كذلك بالرقم المظلم في علم الإجرام، هذه التسمية تُطلق على الإجرام الذي يظل مخفي ويُعبر بها على عدد الجرائم التي يكون فيها الإجرام الحقيقي متزايد على الإجرام الرسمي، فالرقم المظلم هو الجزء الذي لا يمكن قياسه من الإجرام ويبقى بعيدا عن وسائل القياس الرسمية كالإحصاء مثلا، فيكون من الصعب قياسه وذلك لوجود عدة مبررات تساعد في هذا الإخفاء[1].

وبالتالي فالرقم الأسود يعتبر من أهم العقبات التي تواجه الإحصاء الجنائي حيث أن كثيرا من الجرائم يتم ارتكابها وتبقى في طي الكتمان أو الخفاء وهذا ما يُعبر عنه علماء الإجرام بالرقم الأسود أو الرقم المخفي والذي يُمثل الفرق بين عدد الجرائم الحقيقية التي ارتُكِبت فعلا، وبين عدد الجرائم التي تظهر في الإحصائيات الرسمية [2]

ومما سبق بيانه يتبين لنا أن الرقم الأسود يمثل مجموع الجرائم التي ارتُكِبت حقيقة لكنها لم يتم إحصائها ضمن الإحصاءات الرسمية بسبب عدم وصولها إلى علم السلطات المختصة بذلك سواء الشرطة أو الجهات القضائية المختصة.أي الرقم الأسود يمثل الفرق بين الإجرام الحقيقي والإجرام القانوني (الإجرام الرسمي) الذي وصل لعلم السلطات وصدر فيه حكم، أو الفرق بين الإجرام الحقيقي والإجرام الظاهر أي الإجرام الذي يظهر لنا سواء صدر فيه حكم جزائي أي إجرام رسمي أم لم يصدر فيه حكم بسبب عدم كفاية الأدلة أو غياب المشتبه فيه لكنه وصل لعلم السلطات المختصة . وبهذا المعنى تتضح لنا صورة الرقم الأسود.

2_ وجود الرقم الأسود في الجرائم المتعلقة بأنظمة معالجة المعطيات

1- غنام محمد غنام، علم الإجرام وعلم العقاب، الطبعة الأولى، دار الفكر والقانون للنشر والتوزيع، المنصورة، 2015 ، ص51.

2- نبيه صالح، دراسة في علمي الإجرام والعقاب، الطبعة الأولى، الدار العلمية الدولية للنشر والتوزيع ودار الثقافة للنشر والتوزيع، عمان، 2003، ص38.

شهدت جرائم الانترنت في الجزائر إرتفاع كبير خاصة في السنوات الأخيرة مقارنة بالسنوات الماضية، حيث أنه في سنة 2020 تم تسجيل 1362 قضية على مستوى مصالح الدرك الوطني والشرطة، فيما لم تتجاوز 843 قضية خلال سنة 2018[1].

وبالمقابل وفي سنة 2020 تم تسجيل 5163 جريمة موزعة بين المساس بالأشخاص وبالأنظمة المعلوماتية، وكذا النصب والاحتيال والإرهاب الإلكتروني[2]

فنرى من خلال هذه الإحصائيات أن سبب إرتفاع عدد الجرائم المعلوماتية في الجزائر هو زيادة عدد مستخدمي الأنترنت مقارنة بالسنوات السابقة، التي كان فيها عدد مستخدمي الانترنت قليل.

وما يلاحظ أن الرقم الأسود ترتفع نسبته خاصة في الجريمة الإلكترونية بصفة عامة و الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات بصفة خاصة ومرد ذلك خصوصية هذه الجريمة المستحدثة ونعومتها التي تميزها عن الجريمة التقليدية التي يُستعمل فيها العنف وتكون ظاهرة للعيان أثناء ارتكابها في الغالب.

فالجرائم التي كُشفت لدى السلطات المختصة بذلك كانت أقل بكثير من التي لم تُكتشف، فالفارق بين ما هو مرتكب حقيقة وما تم اكتشافه يشكل رقم خطير جدا وهذا ما خلق فجوة كبيرة بينهما [3]

وكذلك الأمر بالنسبة للتي اكتُشفت أو تم التبليغ عنها فإنه يتم معالجة نسبة منها فقط على مستوى السلطات المختصة، فمثلا على مستوى المديرية العامة للأمن الوطني تم تسجيل 657 قضية تتعلق بجرائم الانترنت من قبل الفرق المختصة في مكافحة الجرائم المعلوماتية، وذلك خلال 8 أشهر الأولى من سنة 2016، وكان عدد المتورطين فيها 543 شخص، تم معالجة 385 جريمة معلوماتية فقط ، وتم تسجيل 57 قضية متعلقة بجرائم الإعتداء على سلامة الأنظمة المعلوماتية، من العدد الإجمالي للقضايا المسجلة، وهذه 57 قضية تمت معالجة 31 قضية منها، أي تم معالجة نسبة 55% [4] فقط من العدد الإجمالي لهذا النوع من القضايا.

وحسب قرأتنا لهذه الإحصائيات يتضح لنا أن هذا مرده عدة أسباب تتمثل أهمها في نقص المهارة الفنية لدى جهاز الشرطة ونقص المعرفة بجهاز الكومبيوتر وتقنيات إستخدام البرامج المستخدمة من قبل الجناة في الجريمة وكذلك صعوبة اللغة العلمية المستخدمة من طرف المجرمين المعلوماتيين.

وما يمكن ملاحظته مما سبق بيانه أنه يتفق وما أشارت له مختلف الدراسات في علم الإجرام والعلوم الجنائية المتعلقة بهذا النوع من الإجرام حيث تدل على أن الجرائم الحقيقية التي وقعت يفوق عددها بكثير الجرائم التي صدرت فيها أحكام قضائية أو وصلت لعلم السلطات. والأمر كذلك أيضا بالنسبة للجرائم التي تصل إلى علم السلطات لكن لا يتم معالجتها كاملة وإنما جزء منها فقط.

1- https://www.echoroukonline.com/6525- تم الإطلاع عليه بتاريخ 05/ 07/ 2021 على الساعة 09:02.

2- https://www.echoroukonline.com/6525- تم الإطلاع عليه بتاريخ 05/ 07/ 2021 على الساعة 09:02.

3- خالد ممدوح إبراهيم، حوكمة الأنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2019، ص369.

4- https://www.algeriepolice.dz تم الإطلاع عليه بتاريخ 01/ 07/ 2021 على الساعة 20:40.

ويمكن إرجاع ذلك لعدة أسباب أهمها ما يتعلق بخصوصية الجريمة في حد ذاتها (طبيعتها، محلها، صعوبة اكتشافها، وسهولة محو أثارها).

ثانيا: مبررات وجود الرقم الأسود في جر ائم المساس بأنظمة المعالجة الآلية للمعطيات التي ترجع للجريمة في حد ذاتها

1_ البيئة التي ترتكب فيها الجرائم المتعلقة بأنظمة معالجة المعطيات:

فهذه الجرائم ترتكب في بيئة افتراضية وبواسطة جهاز الحاسب الآلي أو أي جهاز ذكي أو لوحة إلكترونية أو حتى هاتف ذكي، يقوم بواسطتها الجاني المعلوماتي بالاعتداء على أنظمة المعالجة الآلية للمعطيات من خلال الدخول غير المشروع لهذه المعطيات والإطلاع عليها فمجرد الإطلاع يعتبر عمل غير مشروع قانونا، ناهيك عن إتلاف هذه المعطيات أو تعديلها، أو تزويرها، أو محوها...، فجميع الأفعال السابقة الذكر تم تجريمها بموجب قانون العقوبات الجزائري في القسم السابع مكرر.

فتتم كل هذه الأفعال داخل بيئة تكنولوجية افتراضية ويتم ترجمتها في شكل إشارات إلكترونية، وتعتبر هذه البيئة أكثر تعقيدًا من البيئة الواقعية التي تُرتكب فيها الجرائم التقليدية، حيث تصعب إمكانية اكتشافها، ومرد ذلك الطابع الخاص لهذه الجريمة الإلكترونية، فهذه الطبيعة الخاصة هي التي تفرض وجود خبرة خاصة لدى رجال الضبطية القضائية المنوط لهم القيام بإجراءات البحث، التحري والتحقيق فيها، فصعوبة كشف الستار عنها من طرف السلطات المختصة بالبحث والتحري سببها عدم توافر الخبرة الخاصة والتدريب الكافي[(1)]، وذلك نظرا لكون هذه الجرائم ترتكب في الخفاء، حيث يتم نقل البيانات والمعلومات في شكل نبضات إلكترونية[(2)]. وبالتالي فارتكاب هذه الجريمة يكون في بيئة معلوماتية افتراضية قوامها النظم المعلوماتية[(3)]

فبناءً على ما تقدم سابقا نستنتج أن ما جعل هذه الجريمة في غالب الأحيان غير معلومة هو أن كونها من الجرائم الغير ظاهرة للعيان والتي لا تقبل المشاهدة عند ارتكابها بسبب البيئة التي تُرتكب فيها، فهذه البيئة هي التي تلعب الدور الأساسي في تخفيها وعدم كشفها من قبل الجهات المعنية بذلك، وبطبيعة الحال فخصوصيتها جعلتها تتطلب وجود خبرة وتدريب خاص ومهارات تقنية وفنية في هذه الجهات.

2_ صعوبة اكتشاف الجريمة أو إكتشافها المتأخر:

إن الجرائم الماسة بأنظمة معالجة المعطيات من الجرائم التي يصعُب اكتشافها، لأن في الغالب إكتشافها يتم عن طريقين إما إبلاغ المجني عليه بحدوث هذه الجريمة وتقديمه لشكواه أمام المصالح المختصة بتلقي الشكاوى والبلاغات.

أو يتم عن طريق الفحص أو التدقيق، والأمر بالنسبة لهذه الفئة من الجرائم معقد نوعا ما فالجهات المكلفة بالتحقيق في هذه الجرائم خبرتها تعتبر قليلة بالنسبة للخبرة التي تملكها للتحقيق في الجرائم التقليدية لأنه يتطلب في هذه

[1]- أحمد عبد اللاه المراغي، الجريمة الإلكترونية ودور القانون الجنائي في الحد منها- دراسة تحليلية تأصلية مقارنة-، الطبعة الأولى، المركز القومي للإصدارات القومية، القاهرة، 2017، ص118-119.

[2]- غنية باطلي، الجريمة الإلكترونية-دراسة مقارنة-، منشورات الدار الجزائرية، الجزائر، 2016، ص34.

[3]- لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، الطبعة الأولى، دار الحامد للنشر والتوزيع، الأردن، 2015، ص25.

الجهات المعرفة الواسعة والإحاطة الكاملة بالتكنولوجيا الحديثة والتطورات التي تواكبها يوميا من خلال تحديثها لمختلف المعارف و التقنيات، ومن جهة أخرى الضحية كذلك له دور رئيسي في هذه الصعوبة وذلك لعدم تبليغه في الغالب عن هذه الجرائم[1]، وهذا ما سنفصل فيه في المحور الثاني.

وبالتالي وحسب رأينا فإنه يجب أن يكون هناك تناسب بين معرفة وخبرة المحقق مع مهارة وخبرة المجرم المعلوماتي ومع نوع الجريمة الإلكترونية، أو أن تكون معرفة المحقق بالتكنولوجيات الحديثة تفوقها حتى يتمكن من اكتشاف الدليل الرقمي والذي يعتبر دليل مخفي وغير ظاهر للعيان هو كذلك لأنه يتمثل في مجرد نبضات الكترونية متواجدة داخل الدعامة المعنوية لنظم المعطيات.

فما يتم إكتشافه من هذه الجرائم غالبيته يرجع للصدفة، وما يدُل على ذلك أنه لم يُكتشف إلا نسبة1% فقط منها، وأن 15 % منها تم الإبلاغ عنها، وخمس النسبة الأخيرة هي التي يصدر فيها حكم بإدانة مرتكبيها [2].

وبناءً على تحليل هذه الإحصائيات نستنتج أن النسبة المتبقية من عدد الجرائم تبقى متخفية ومتسترة، فهذه الأرقام والإحصائيات لا تترجم حقيقة حجم هذه الظاهرة الإجرامية. بل تعبر عن الإجرام الذي تم كشفه فقط.

3_ سهولة إخفاء وطمس أثار الجرائم المتعلقة بأنظمة معالجة المعطيات:

وذلك لاستخدام الجاني أو الجناة وسائل المحادثة التي يصعُب إعتراضها كغرف المحادثة أو مختلف غرف الدردشة التي تكون سرية، ويتم استخدام وسائل التشفير التي تجعل هذه المعطيات حتى وإن تم اعتراضها أو ضُبطت يصعب أو يستحيل قراءتها، ويستخدم الجناة هذه الوسائل في البريد الإلكتروني والهاتف الخلوي ومختلف الوسائل التكنولوجية التي لديها وقاية من التشفير والاختراق وبرامج الأمان، ويستخدمون كذلك البطاقات الهاتفية المسددة الثمن مسبقا حتى لا تتعرف الجهات التي وفرت الخدمة بالهوية الشخصية والعناوين الجغرافية لأجل إرسال فواتير التحصيل، لغرض طمس الأدلة الرقمية[3].

وبالتالي وما يُستدل على ما سبق أنه حتى لو تم اكتشاف هذه الجرائم من السلطات المختصة فإنه يمكن طمس أدلتها الرقمية بسهولة لأنها تتمثل في شكل نبضات كهربائية تظهر في نظام المعالجة الآلية للمعطيات، فالمجرم المعلوماتي الذي قام بالمساس بنظام المعطيات يمكنه محو وطمس الدليل من هذا النظام الذي قام بالاعتداء عليه ومن حاسوبه الذي بواسطته نفذ الجريمة.

المحور الثاني: دور الجاني والمجني عليه في بروز الرقم الأسود في الجرائم المتعلقة بأنظمة معالجة المعطيات

إن غالبية الجرائم المتعلقة بأنظمة معالجة المعطيات تبقى في طي الكتمان عن السلطات ولا تصل إلى علمهم وللمجني عليه دور كبير في ذلك بسبب السلوك السلبي الذي يتخذه بعدم تبليغه عن الجريمة، وللجاني كذلك دور في تفاقم الرقم الأسود في هذا النوع من الإجرام. وفيما يلي سنبين دور كل منهما حيث سنتطرق في المقام الأول إلى الجاني في

1- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، 2007، ص34.

2- بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، دار الخلدونية، الجزائر، 2017، ص21.

3- مناصرة يوسف، جرائم المساس بأنظمة المعالجة الآلية للمعطيات (ماهيتها، صورها، الجهود الدولية لمكافحتها)- دراسة مقارنة-، دار الخلدونية، الجزائر، 2018، ص42-43.

الجرائم المتعلقة بأنظمة معالجة المعطيات (أولا)، وفي المقام الثاني إلى المجني عليه في الجرائم المتعلقة بأنظمة معالجة المعطيات (ثانيا).

أولا: الجاني في الجرائم المتعلقة بأنظمة معالجة المعطيات

1_ التعريف بالمجرم المعلوماتي

من الناحية الجنائية تعني تسمية "المجرم المعلوماتي" ذلك الشخص الذي يمتلك مهارات تقنية أو دراية بالتكتيك المستخدم في نظام الحاسوب الإلكتروني والقادر على استخدام هذا التكتيك لاختراق "الكود" السري لتغيير المعلومات أو لتقليد البرامج أو التحويل من الحسابات عن طريق إستخدام الحاسوب نفسه(1) .

ويطلق عليه كذلك المجرم"المجرم الإلكتروني الرقمي" ويُعرف بأنه (من لديه القدرة على تحويل لغته إلى لغة رقمية وتخزينها واسترجاعها باستخدام الحاسب الإلكتروني أو الرقمي وملحقاته ووسائل الإتصال الرقمي وذلك بأداء فعل أو الإمتناع عنه مما يحدث إضطربات في المجتمع الدولي أو المحلي نتيجة مخالفته قواعد الضبط الإجتماعي محليا ودوليا) (2)

ويرى محمد محمد شتا أن " المتورطون في هذه الجرائم لديهم قدر كبير من الذكاء والتفوق يجعلهم يباشرون إجرامهم بدقة متناهية خشية إفتضاح أمرهم وضبطهم وهم في سن تساعدهم على المخاطرة والمغامرة. ولأن من يقترف هذه الجرائم يكون بين الإثني عشر (12) والسادسة والأربعون سنة (46)، وهم مثقفون ومتعلمون وأهل الثقة ممن يعتدون على حقوقهم في غالب الأحيان" (3).

فحسب الإحصائيات المسجلة في الجزائر 90 % من الجناة في الجرائم المعلوماتية لهم معرفة بالمعلوماتية (تقني أو طالب)، و84 % منهم له علاقة بالضحية، وغالبا تكون هذه العلاقة مهنية(4)

فمن خلال ما سبق بيانه يتضح لنا جليا أن المجرم المعلوماتي يُشترط توافر أمرين أساسين فيه، هما الذكاء والقدرة على التحكم في الحاسب الآلي ومختلف ملحقاته والأجهزة الذكية التي يستخدمها كذلك في جريمته. وذلك من خلال قيامه بسلوك ايجابي غرضه الاعتداء على النظم المعلوماتية، فيخالف بذلك القواعد القانونية المتواجدة في التشريعات.

2_ الخطورة الإجرامية لدى المجرم في الجرائم المتعلقة بأنظمة معالجة المعطيات.

إن الخطورة الإجرامية لدى المجرم المعلوماتي تزداد كلما زاد تكيفه الاجتماعي مع توافر الشخصية الإجرامية لديه، فمن مواصفات هذا المجرم أنه إنسان اجتماعي.

ويعتبر اللهو وإظهار السلطة على النظم المعلوماتية من أبرز الدوافع التي تؤدي إلى هذه الأعمال الإجرامية لديه، وحسب الدراسات فإن أغلب المجرمين هدفهم من هذه الجريمة هو المساعدة وليس إلحاق الضرر بالغير، لكن لا ننكر الخطر الاجتماعي الذي تسببه هذه الفئة من المجرمين، حتى ولو كانت نواياهم غير آثمة والباعث عندهم نبيل، لأن مجرد القيام بهذا السلوك غير الواعي قد يتسبب في أضرار جسيمة، حتى ولو لم يكشف أي اعتداء على المجتمع (5)

1- عمار عباس الحسيني، جرائم الحاسوب والأنترنت-الجرائم المعلوماتية-، الطبعة الثانية، منشورات زين الحقوقية، لبنان، 2019، ص58.

2- علي نعمة جواد الزرفي، الجريمة المعلوماتية الماسة بالحياة الخاصة –دراسة مقارنة-، المكتب الجامعي الحديث، الإسكندرية، 2019، ص26.

3- غنية باطلي، المرجع السابق ، ص35.

4 مختار الأخضري، الإطار القانوني لمواجهة جرائم المعلوماتية وجرائم الفضاء الإفتراضي، نشرة القضاة، المديرية العامة للشؤون القضائية والقانونية مديرية الدراسات القانونية والوثائق، العدد 66، 2011، ص 69.

5- غنية بالطي، المرجع السابق، ص36-37.

والمجرم المعلوماتي تختلف أساليبه الإجرامية في ارتكاب جرائم المساس بأنظمة المعالجة الآلية للمعطيات باختلاف التقنيات المستعملة في الجريمة بحد ذاتها، فأساليبه متطورة ذات طبيعة إلكترونية مثل الفيروسات، ديدان الحاسوب، الإختراق...، وبواسطة هذه الأساليب يرتكب جريمته داخل الأنظمة المعلوماتية (1)

فمثلا بخصوص أسلوب الإختراق تمت معالجة 152 قضية متعلقة بالجرائم المعلوماتية والنصب والاحتيال عبر الانترنت من طرف فرق مكافحة الجريمة المعلوماتية التابعة للمديرية العامة للأمن الوطني، حيث تم توقيف 216 شخص خلال الفترة الممتدة من جانفي 2020 إلى سبتمبر 2020، فالمخترقين يقومون بإرسال رسائل مزيفة ليتمكنوا من الحصول على البيانات الشخصية والكلمات السرية المتعلقة بحسابات ضحاياهم الشخصية أو سرقة هويتهم الرقمية(2)

ونحن نرى في هذا الصدد أن مرونة وحداثة الأساليب المستعملة في هذا النوع من الإجرام وتنوعها تشكل عائق أمام دراسات علم الإجرام الحديثة التي تصنف المجرم المعلوماتي من خلال أسلوبه في ارتكاب الجريمة حيث يتم دراسة سلوكه الإجرامي والخطورة الإجرامية التي يكتسبها ودراسة ما إذا كان له خطورة إجرامية كامنة حتى تمكنهم من التعرف على أسباب العود للإجرام عند هؤلاء المجرمين.

3_ دور الجاني في إرتفاع الرقم الأسود في الجرائم المتعلقة بأنظمة معالجة المعطيات من خلال إخفاء أدلة الجريمة:

إن الجاني المعلوماتي لديه قدرة على تدمير ما قد يتم اعتباره دليل إلكتروني يمكن أن يُستخدم ضده ولغرض إدانته وذلك في أقل من الثانية الواحدة (3)، مما يؤدي إلى تضييع أدلة الجريمة، لأن الجاني في هذه الجريمة يكون متخفيا وراء الحاسوب وربما يكون في قارة أو بلد مختلف، فهو لا يقوم بالاعتداء على مكونات الحاسوب المادية كما في الجريمة التقليدية (4) وإنما على مكوناته المعنوية والمتمثلة في البيانات والمعطيات الرقمية في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات التي يكون شكلها متمثل في نبضات الكترونية معنوية وليس لها مصدر مادي محسوس.

وبطبيعة الحال فالجاني المعلوماتي يكتسب مختلف المهارات التقنية والفينة وملم بمختلف الأساليب المستحدثة التي ترتكب من خلالها الجريمة المعلوماتية بصفة عامة والجرائم المتعلقة بأنظمة معالجة المعطيات بصفة خاصة، فهذا ما يعطيه الفرصة السانحة لكي يعيق عمل الشرطة، أو السلطة المنوطة بالتحري للوصول إلى الدليل، ويكون ذلك بإتباع الجاني لمجموع التدابير الفنية والإجراءات الواقية التي تعقد عملية التفتيش وتعرقلها وتُصعبها كإضافة كلمة سر أو دس تعليمات خفية بينها لتصبح كالرمز أو تشفير البيانات، وبالتالي تصبح عملية التفتيش صعبة جدا وتستدعي بالضرورة الإستعانة بالخبراء الفنيين والتقنيين في هذا الجانب أصحاب الخبرة الفنية عالية المستوى (5). فبمجرد النقر وفي ثوان معدودة يمكن حذف، إتلاف، تغيير ومحو المعطيات الإلكترونية، هذا ما يؤدي إلى صعوبة تقفي أثر المشتبه فيه، فالأمر

[1]- لحرش أيوب التومي، النحوي سليمان، طبيعة الخطورة الإجرامية للمجرم المعلوماتي، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 05، العدد 01، السنة 2020، ص993.

[2]- https://www.algeriepolice.dz تم الإطلاع عليه بتاريخ 01/ 07/ 2021 على الساعة 20:40.

[3]- بن مكي نجاة، المرجع السابق، ص23.

[4]- عمار عباس الحسيني، المرجع السابق، ص54.

[5]- لينا محمد الأسدي، المرجع السابق، ص28.

ليس هين وبالتالي يصعُب معرفة مرتكب هذه الجريمة [1]، فمحو أثارها وإتلاف أدلتها عملية سهلة وكشف هوية مرتكبها ليس بالأمر السهل [2].

ويستنتج مما سبق أن هذا يشكل عملية تضاد بين عملية تخريب الأدلة وكشف الجاني فالأولى سهلة بالنسبة للجاني والثانية ليست بالهينة. لذلك هذا النوع من الجرائم في الغالب لا يتم إكتشافه أو إذا تم إكتشافه فإنه لا يتم نسب الفعل الإجرامي إلى الجناة، فتبقى الجريمة مسجلة لدى المصالح المختصة بدون جاني أي تبقى مسجلة ضد مجهول.

ثانيا: المجني عليه في الجرائم المتعلقة بأنظمة معالجة المعطيات

1_ تعريف المجني عليه في الجريمة المعلوماتية:

التعريف القانوني للضحية: يعرف عادل الكردوسي "الضحية هي كل إنسان أو جماعة وقع عليها اعتداء من أي نوع في ذاته أو في حقوقه ......" [3]

وفي الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات يمكن أن تكون الضحية أشخاص طبيعية أو معنوية طالما أنها استخدمت الحاسب الآلي لأي غرض من الأغراض سواء كانت اقتصادية أو اجتماعية أو حتى سياسية وعسكرية....الخ، فمن الصعب تحديد نطاق الضحايا على وجه الدقة في الجرائم المعلوماتية بوجه عام وفي جرائم المساس بأنظمة المعالجة الآلية للمعطيات بوجه خاص، ومرد ذلك أن هؤلاء لا يعلمون شيئا عنها إلا بعد أن تقع بالفعل[4]

وبناءً على ما تقدم يكون مرتكب الجرائم التقنية (الجريمة المعلوماتية أو جرائم المساس بأنظمة المعالجة الآلية للمعطيات) شخص طبيعي، إلا أن الضحية في هذه الجرائم يمكن أن يكون شخص طبيعي أو معنوي ويتمثل الشخص المعنوي في مؤسسات وقطاعات مالية وشركات ضخمة. وأخطر أنواع هذه الجرائم هي التي تقع على الجهات العسكرية من خلال عمليات التجسس ورصد البيانات وتهريبها [5]

وحسب معلومات تم تجميعها عن ضحايا الجرائم المتعلقة بأنظمة معالجة المعطيات في الجزائر أن هؤلاء الضحايا يتمثلون في إدارات عمومية ومؤسسات ذات طابع صناعي وتجاري بنسبة 60 % ، و شركات خاصة بنسبة 20 %، و وشركات خاصة أجنبية بنسبة 11 % ، وأشخاص طبيعيين 6 %، وهيئة عمومية أجنبية 03 % من العدد الإجمالي لعدد الضحايا[6]

فبناءً على هذه الإحصائيات يتضح أن الأشخاص المعنوية التي يتم التعدي على أنظمتها ومعطياتها الإلكترونية يفوق عددها بكثير عدد الأشخاص الطبيعية التي تكون ضحايا لهذه الجريمة، وتفسيرنا لسبب ذلك هو نسبة الأرباح التي

1- مناصرة يوسف، المرجع السابق، ص 42.

2- لينا محمد الأسدي، نفس المرجع السابق، ص 11.

3- لموشي جهيدة، محمد كريم فريحة، دور الضحية في حدوث جريمة النصب والإحتيال- مقاربة سوسيولوجية-، مجلة العلوم الإجتماعية والإنسانية، العدد الخامس عشر، 2018، ص252.

4- غنية باطلي، المرجع السابق، ص 41.

5- أسامة أحمد لمناعسة، جلال محمد الزغبي، جرائم تقنية نظم المعلومات الإلكترونية –دراسة مقارنة-، الطبعة الثالثة، دار الثقافة للنشر والتوزيع ، الأردن،2017، ص81.

6- مختار الأخضري، المرجع السابق، ص 69.

يتم تحقيقها من خلال هذه الجريمة والتي تكون مرتفعة إذا كان الضحية شخص معنوي خاصة إذا كان تجاري أو صناعي سواء تابع للدولة أو خاص.

2_ دور المجني عليه في ظهور الرقم الأسود في الجرائم المتعلقة بأنظمة معالجة المعطيات

أحيانا تكون العلاقة بين الضحية (المجني عليه) والجاني لها دور في حدوث الجريمة، وذلك عندما يكون الجاني يعمل لحساب الضحية، فيكون على علم بكل خبايا النظام المعلوماتي والثغرات التي تتواجد به، وذلك عندما يكون مؤتمنا عليه ويلم بكل خفاياه، فمن خلال مسؤوليته عن المركز المعلوماتي يستغل تلك الثقة [1].

وبالتالي يستخدمها في أعمال غير مشروعة تمس أنظمة المعطيات الرقمية، فتلعب تلك العلاقة بين الجاني والمجني عليه دورها في حدوث الجريمة.

وللضحية الدور الرئيسي غالبا في إرتفاع الرقم الأسود في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، وذلك بسبب إحجامها عن الإبلاغ بوقوع الجريمة الإلكترونية بمجرد اكتشافها [2]. ويمكن رد الإحجام عن التبليغ ل:

الأمر الأول: ويتمثل في عدم اكتشاف الضحية لها لذا نجد أغلب جرائم الانترنت تم اكتشافها بالمصادفة، بعد وقت طويل من ارتكابها [3]، وذلك لسبب فني وتقني يتمثل في أن هذا النوع من الإجرام لا يترك وراءه أثرا ماديا ملموسا كما هو الحال في الجرائم التقليدية[4]، لذلك يصعب على المجني عليه معرفة إذا ما وقعت جريمة أم لا، فيكون هنا للصدفة فقط دور في الكشف عن هذه الجرائم وملاحقتها [5]، لأن الضحية في هذه الجريمة لا ترى الجاني ولا تتعرف عليه، بل ترى أثر عمله الجرمي فقط وقد يكون ذلك في الغالب كما قولنا سابقا بمحض الصدفة، وإذا تم مشاهدة أثر الجريمة فالمجني عليه غالبا ما يحجم عن التبليغ[6] لأسباب أخرى سنبينها لاحقا.

وكذلك أحيانا الضحية لا يرى حتى أثر الجريمة لأنه يرى أمامه مجرد معطيات أو بيانات وأرقام ورموز لا يمكنه من خلال رؤيتها معرفة ما إذا تم المساس بها أم لا إلا إذا كان مثل الجاني المعلوماتي له معرفة وخبرة في المعلوماتية فنيا وتقنيا.

الأمر الثاني: الخشية من التشهير والفضيحة خاصة في جرائم الانترنت الماسة بالعرض والشرف[7]، ففي الأغلب يكون دور الضحية سلبيا وذلك بإبقاء ما لحقهم سرا خوفا على سمعتهم أو على سمعة تجارتهم[8]

ومثال ذلك الجرائم المتعلقة بالمعطيات الشخصية أو الاسمية وخاصة تلك المعطيات الشخصية الحساسة التي تتعلق بالضحية، وبالحياة الخاصة للضحية كأصولها العنصرية، وحالتها الطبية وسوابقها القضائية [9].

[1]- حمد خليفة، المرجع السابق، ص35-36.

[2]- أحمد عبد اللاه المراغي، المرجع السابق، ص 119.

[3]- خالد ممدوح إبراهيم، حوكمة الأنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2019، ص 369.

[4]- عمار عباس الحسيني، المرجع السابق، ص52.

[5]- أسامة أحمد لمناعسة، جلال محمد الزغبي، المرجع السابق، ص82.

[6]- أحمد عبد اللاه المراغي، المرجع السابق، ص 117-118.

[7]- أحمد عبد اللاه المراغي، المرجع نفسه، ص 119.

[8]- أسامة أحمد لمناعسة، جلال محمد الزغبي، نفس المرجع السابق، ص82.

[9]- محمد خليفة، المرجع السابق، ص92-93.

وما يمكن ملاحظته أنه لا يهم شكل المعطيات في هذه الجريمة سواء كانت صور، بيانات، رموز، أصوات... حتى تقوم الجريمة وتتوافر عناصرها.

وكذلك الأمر بالنسبة للمؤسسات الاقتصادية والمالية التي تخاف من التبليغ عن الجرائم التي تقع عليها وتكتفي باتخاذ إجراءات إدارية داخلية دون إحاطة السلطات المختصة علما بالجريمة وذلك للحفاظ على مكانتها المالية وسمعة المؤسسة[1]، وحفاظا على اسمها وشهرتها، وحرصا على سمعتها وتجنبا للإضرار بمكانتها وزعزعة الثقة فيها، وأبرز هذه الجهات هي المؤسسات المالية والادخارية ومؤسسات السمسرة، حتى أن بعض التقديرات أشارة إلى أن نسبة (20- 25 %) من الجرائم المعلوماتية لا يتم الإبلاغ عنها خشية الإساءة للسمعة[2].

فبناءً على الإحصائيات السابقة يتضح لنا أنه حوالي ربع الجرائم المعلوماتية من عددها الإجمالي يتم التكتم عليه خوفا على السمعة، خاصة إذا كان المجني عليه شخص معنوي ممثل في مؤسسة أو شركة أو إدارة.

الأمر الثالث: خشية الضحايا من خسارة المستخدمين لديهم أو خسارة الثقة العامة من عملائهم، أو معرفة نقاط الضعف في أنظمتها المعلوماتية لغير الجاني[3]، ففي هذه الحالة المجني عليه يرى أنه من الحكمة عدم الإبلاغ عن هذه الجرائم، وهنا غالبا ما يكون المجني عليه مؤسسة مالية أو مصرفا أو شركة ضخمة، وبالتالي مجالس إدارة هذه المؤسسات تخشى من التبليغ عن هذه الجرائم لما قد ينتج من دعاية سلبية من خلال الكشف عنها أو اتخاذ الإجراءات القضائية حيالها والتي تمس بالثقة التي وضعها المتعاملين فيها وتؤدي إلى تضاؤله، وبالتالي يحبذ المجني عليهم المحافظة على هذه الثقة أكثر من الكشف عن الجريمة، ولا يحبذون معرفة أن نظامهم المعلوماتي قد تعرض للإنتهاك أو تم اختراقه أو هكره أو الاعتداء عليه[4].

وكنتيجة لذلك فالمساس بالثقة لدى المتعاملين مع هذه المؤسسات يؤدي بدوره إلى المساس بالقيم المالية لهذه المؤسسات من خلال خسارة المتعاملين بالرغم من أن محل الجريمة يتمثل في عناصر معنوية أي قيم معنوية إلا أنها تؤثر تأثيرا سلبيا وبشكل كبير على أرباحها المالية.

وأحيانا يتكتم المجني عليه عن الجريمة بتردده عن الإبلاغ عن هذه الجرائم خوفا من أن يتم التعرف على أسلوب إرتكاب هذه الجرائم من قبل الجناة محترفي الإجرام المعلوماتي مما يؤدي إلى إرتكابها مرة أخرى من طرفهم، أو أنه قد يؤدي إلى الكشف عن مواطن الضعف في برامجه ونظامه المعلوماتي مما يسهل على المجرمين معرفة الثغرات ونقاط الضعف التي من خلالها يتم اختراقه بسهولة، بل وحتى بالنسبة لموظفي المؤسسة ممن لم يحترفوا الإجرام المعلوماتي[5]

وبالتالي من خلال تكتم المجني عليه وعدم تبليغه عن الجريمة يكون قد ساهم بنسبة كبيرة في ارتفاع الرقم الأسود في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، فالمجني عليه يرى هنا أن الضرر الذي لحقه من جراء هذا الاعتداء

1- نسرين محسن نعمة الحسيني، محمد حسن مرعي، الجرائم الإلكترونية الواقعة على الأموال – دراسة مقارنة-، المكتب الجامعي الحديث، الإسكندرية، 2019، ص38.

2- عمار عباس الحسيني، نفس المرجع السابق، ص52.

3- أحمد عبد اللاه المراغي، نفس المرجع السابق، ص 119.

4- غنية باطلي، المرجع السابق، ص41.

5- نسرين محسن نعمة الحسيني، محمد حسن مرعي، المرجع السابق، ص38- 39.

أقل بكثير من الضرر الذي يلحق مؤسسته عند التبليغ من خلال التشهير بها والمساس بسمعتها وخسارة الثقة من عملائهم، ومعرفة نقاط ضعفها مما يجعلها مستهدفة من المجرمين المعلوماتيين.

3_ النتائج المترتبة عن إحجام الضحية عن التبليغ في الجرائم المتعلقة بأنظمة معالجة المعطيات

يكون للمجني عليه دور كبير في إخفاء الجريمة خاصة في الجرائم المتعلقة بأنظمة معالجة المعطيات، وبالتالي ما تحدثنا عنه سابقا يقودنا إلى أنه لا توجد إحصائيات دقيقة لهذا النوع من الإجرام، والسبب يرجع إلى عدم تعاون ضحية الجريمة المعلوماتية مع الأجهزة الأمنية، حيث أنه لا يُبلغ عن الجريمة التي وقعت في حقه[1]، فالأرقام المتوفرة من الدراسات الموضوعية لا تعكس بأي صورة واقع الظاهرة بل تقدم صورة عن حقائقها العامة فقط، وبالتالي فحجم الظاهرة ونطاق الجريمة وحجم الخسائر يكون بالضرورة أكثر مما تقدمه هذه الدراسات من نتائج[2]

فالإحصائيات تشير إلى أن ما يتراوح بين (20- 30%) من الجرائم المعلوماتية لا يتم الإبلاغ عنها مطلقا [3]، كما أشارت إحصائية مكتب التحقيق الفيدرالي في الولايات لمتحدة أن حوالي 1% من الجرائم المعلوماتية قد تم اكتشافها وأن واحد فقط من كل "22000" مجرم معلوماتي قد تم إدانتهم[4]، فتم إقتراح عدة آليات من جانب الدول لغرض تعاون المجني عليهم مع السلطات المختصة من خلال الإبلاغ على هذه الجرائم والكشف عنها وكذلك لغرض قياس الإجرام المعلوماتي[5]، وبعض الإقتراحات التي طُرِحت في الولايات المتحدة الإمريكية تضمنت المطالبة بفرض الالتزام على موظفي الجهة المجني عليها بالإبلاغ عما يصل إلى علمهم من جرائم في هذا المجال مع تقرير جزاء لكل من يخالف هذا الالتزام بتكتمه عن الجريمة وعدم التبليغ عنها، وبعد أن تم عرض الاقتراح على لجنة الخبراء في المجلس الأوربي، تم رفضه وبرروا الرفض بالقول أنه من غير المقبول تحويل المجني عليه إلى جاني وإحلاله محله وهو ضحيته[6].

وبالتالي فالتكتم عن الجريمة وعدم التبليغ عن فاعلها يعتبر السبب الرئيسي في تفشي هذا النوع من الإجرام وانتشاره، وحافزا للجناة لتكرار نفس الجريمة والعود فيها ، رغم أن البعض يقول بعكس هذا فيُرجع تكرار الجريمة إلى الكشف عنها بالتبليغ وإظهار مواطن الضعف في النظام المعلوماتي للمجني عليه مما يسهل على اختراقه والوصول إليه، وهذا ما أدى إلى ظهور سوق سوداء للمعلومات وهي ترتبط بالجريمة المعلوماتية، وخاصة الجرائم المتعلقة بأنظمة المعطيات لأن مختلف الأنشطة الاجتماعية والاقتصادية تتعلق بالمعلومات التجارية أو الصناعية أو بالاستثمارات ناهيك عن المعلومات الشخصية المخزنة بكافة أشكالها وصورها في ذاكرة الحاسب التابع للجهات التي يتعامل معها الأشخاص سواء كانت هذه المعلومات إسمية أو مالية وقد تمس هذه الجرائم المعلومات الخاصة بالدفاع الوطني[7].

[1] - لينا محمد الأسدي، المرجع السابق، ص26.

[2] - الحذيفي أمين أحمد، جرائم الكمبيوتر والإنترنت، مجلة العدل، وزارة العدل المكتب الفني، العدد الأربعون، السنة الخامسة عشر، 2013، ص 146.

[3] - نسرين محسن نعمة الحسيني، نفس المرجع السابق، ص 39.

[4] - عمار عباس الحسيني، المرجع السابق، ص 53.

[5] - نسرين محسن نعمة الحسيني، نفس المرجع السابق، ص 39.

[6] - عمار عباس الحسيني، نفس المرجع السابق ، ص 52.

[7] - غنية باطلي، المرجع السابق، ص 42.

لأنه وكما هو معلوم حاليا أنه أصبحت قيمة المعلومات والمعطيات اقتصاديا تفوق بكثير قيمة الأموال المنقولة، لأن الاعتداء عليها يسبب خسارة جسيمة للمؤسسات المالية وللأشخاص، وهذا نتيجة حتمية للتطور الذي أفرزته التكنولوجيات الحديثة.

خاتمة:

إن إرتفاع الرقم الأسود في الجرائم المتعلقة بأنظمة معالجة المعطيات، له تأثير كبير على السياسة الجنائية التي يتم انتهاجها من طرف الدولة بغرض مكافحة هذا النوع من الإجرام،فلا تتم الإحاطة بالظاهرة من جميع جوانبها لأن أغلب الجرائم المرتكبة تبقى متخفية ولا يتم البحث فيها وفي أسباب وقوعها وبالتالي لا يتم إيجاد الحلول المناسبة لمجابهتها.

فمن خلال هذه الدراسة يمكننا أن نتبين بوضوح أسباب إرتفاع الرقم الأسود في الجرائم المتعلقة بأنظمة معالجة المعطيات، وعدم وصول هذا النوع من الإجرام للجهات المختصة من الضبطية القضائية والجهات القضائية المعنية، وذلك نظرا لطبيعة هذه الجريمة في حد ذاتها وخصوصيتها وكونها جريمة تقع على المال المعنوي ومسرح هذه الجريمة يكون معنوي كذلك ولا يمكن مشاهدته، ونظرا لمرتكب هذه الجريمة ومميزاته وخطورته الإجرامية التي يتميز بها. وكذلك هناك دور كبير للضحية في هذا الإرتفاع لأن الضحية في هذه الجرائم لا يبلغ في الغالب الأعم عنها وذلك خشية على شرفه وسمعته أحيانا خاصة إذا تعلق الأمر بالاعتداء على بياناته ومعطياته حتى لو كانت حساسة، وفي الغالب يكون مرد تكتمه وكبحه للجريمة الخوف على زعزعة الثقة في المتعاملين معهم خاصة إذا كان هذا الضحية مؤسسة مالية أو تجارية أو اقتصادية، وخوفا من التشهير.

النتائج المتوصل لها من خلال هذه الدراسة:

_ الرقم الأسود يمثل أهم العقبات التي تواجه الإحصاء الجنائي وتمس السياسة الجنائية في الجرائم المتعلقة بأنظمة معالجة المعطيات

_ الرقم الأسود في الجرائم المتعلقة بأنظمة معالجة المعطيات يتمثل في الفرق بين الإجرام الحقيقي والإجرام الرسمي، وبالتالي يكون اختلاف بين عدد الجرائم التي تقع فعلا والجرائم التي تم تسجيلها في الإحصائيات الجنائية فهذه الإحصائيات لا تعبر حقيقة على حجم الظاهرة الإجرامية المدروسة.

_ من أهم مسببات ارتفاع الرقم الأسود التي ترجع إلى الجريمة المتعلقة بأنظمة معالجة المعطيات تتمثل في إرتكابها في بيئة رقمية وهذا ما يؤدي إلى صعوبة اكتشافها أو الاكتشاف المتأخر لها وسهولة طمس أثار هذه الجريمة.

_ الجاني الرقمي يختلف عن الجاني التقليدي في كونه يتميز بالذكاء والقدرة على استخدام التكنولوجيات الحديثة، وتختلف طرق إرتكابه للجرائم المتعلقة بأنظمة المعطيات باختلاف أساليب إرتكاب الجريمة، ولهذا الجاني القدرة على إخفاء وتدمير الدليل الرقمي بعد إرتكابه لجريمته في ثوان هذا ما يؤدي إلى بقاء الجريمة متخفية وبالتالي إرتفاع الرقم الأسود

_ للمجني عليه في الجرائم المتعلقة بأنظمة معالجة المعطيات دور في كبح الجريمة من خلال إحجامه عن التبليغ عنها وهذا راجع لعدة أسباب تعود له.

_ بسبب الإجرام المعلوماتي ظهرت سوق سوداء تتعامل بالمعلومات التي يتم الحصول عليها من خلال الجرائم المتعلقة بأنظمة معالجة المعطيات. وهذا ما أدى إلى تزايد عدد هذه الجرائم وتفاقمها في المجتمع.

لذلك نقترح عدة إقتراحات أهمها:

_ لابد على مؤسسات المجتمع المدني من القيام بدورها في هذا الشأن من خلال التوعية بخطورة هذا النوع من الإجرام، لأن هذا الإجرام يمس بالمال المعلوماتي والمعطيات والبيانات الرقمية، التي يراها المجني عليه لا تمثل أي قيمة مادية وبالتالي تبدو له هذه الجريمة بسيطة لا يستوجب التبليغ عنها.

_ لابد من إدراج مواد قانونية في التشريعات تُلزم المجني عليه بالتبليغ عن الجرائم المتعلقة بأنظمة معالجة المعطيات، لكن دون المساس بمركزه كضحية لأنه لا يمكن إحلال الضحية محل الجاني.

_ ضرورة تطوير جهاز الشرطة والبحث المختص في عملية التفتيش عن الجرائم المتعلقة بأنظمة معالجة المعطيات، لغرض الحصول على الدليل الرقمي المتعلق بالجريمة المعلوماتية والذي في غالب الأحيان يصعب الحصول عليه نظرا لطبيعته الخاصة وسهولة طمسه.

_ عند قيام الباحث المختص في علم الإجرام بالإحصائيات الجنائية لابد أن تكون هذه الإحصائيات دقيقة وصحيحة، لأنها تعبر عن الظاهرة الإجرامية من خلال لغة الأرقام، وذلك بغرض تطويقها ومكافحتها.

قائمة المراجع:

1-الكتب:

_ أحمد عبد اللاه المراغي، الجريمة الإلكترونية ودور القانون الجنائي في الحد منها- دراسة تحليلية تأصلية مقارنة-، الطبعة الأولى، المركز القومي للإصدارات القومية، القاهرة، 2017.

_ أسامة أحمد لمناعسة، جلال محمد الزغبي، جرائم تقنية نظم المعلومات الإلكترونية –دراسة مقارنة-، الطبعة الثالثة، دار الثقافة للنشر والتوزيع، الأردن، 2017.

_ بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، دار الخلدونية، الجزائر، 2017.

_ خالد ممدوح إبراهيم، حوكمة الأنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية،2019.

_ علي نعمة جواد الزرفي، الجريمة المعلوماتية الماسة بالحياة الخاصة –دراسة مقارنة-، المكتب الجامعي الحديث، الإسكندرية،2019.

_ عمار عباس الحسني، جرائم الحاسوب والأنترنت-الجرائم المعلوماتية-، الطبعة الثانية، منشورات زين الحقوقية، لبنان، 2019.

_ غنام محمد غنام، علم الإجرام وعلم العقاب، الطبعة الأولى، دار الفكر والقانون للنشر والتوزيع، المنصورة، 2015.

_ غنية باطلي، الجريمة الإلكترونية-دراسة مقارنة-، منشورات الدار الجزائرية، الجزائر، 2016.

_ لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، الطبعة الأولى، دار الحامد للنشر والتوزيع، الأردن، 2015.

_ محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية،2007.

_ مناصرة يوسف، جرائم المساس بأنظمة المعالجة الآلية للمعطيات (ماهيتها، صورها، الجهود الدولية لمكافحتها)- دراسة مقارنة-، دار الخلدونية، الجزائر، 2018.

_ نبيه صالح، دراسة في علمي الإجرام والعقاب، الطبعة الأولى، الدار العلمية الدولية للنشر والتوزيع ودار الثقافة للنشر والتوزيع، عمان، 2003.

_ نسرين محسن نعمة الحسيني، محمد حسن مرعي، الجرائم الإلكترونية الواقعة على الأموال – دراسة مقارنة-، المكتب الجامعي الحديث، الإسكندرية،2019.

2-المجلات:

_ الحذيفي أمين أحمد، جرائم الكمبيوتر والإنترنت، مجلة العدل،وزارة العدل المكتب الفني، العدد الأربعون، السنة الخامسة عشر، 2013.

_ لحرش أيوب التومي، النحوي سليمان، طبيعة الخطورة الإجرامية للمجرم المعلوماتي، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 05، العدد 01، السنة 2020.

_ لموشي جهيدة، محمد كريم فريحة، دور الضحية في حدوث جريمة النصب والإحتيال- مقاربة سوسيولوجية-، مجلة العلوم الإجتماعية والإنسانية، العدد الخامس عشر، 2018.

_ مختار الأخضري، الإطار القانوني لمواجهة جرائم المعلوماتية وجرائم الفضاء الإفتراضي، نشرة القضاة، المديرية العامة للشؤون القضائية والقانونية مديرية الدراسات القانونية والوثائق، العدد 66، 2011.

3- المو اقع الإلكترونية:

https://www.algeriepolice.dz _ تم الإطلاع عليه بتاريخ 30/ 07/ 2021 على الساعة 20:40.

_ https://www.echoroukonline.com/6525- تم الإطلاع عليه بتاريخ 05/ 07/ 2021 على الساعة 09:02.