الجامعة اللبنانية

كليّة الحقوق والعلوم السياسية والإدارية

العمادة

المجرم والضحيّة المعلوماتيّين على ضوء علم الإجرام

رسالة أعدت لنيل شهادة الماستر2 بحثي في القانون الجزائي

إعداد

رامي وسام أبو ملحم

لجنة المناقشة

د. جنان الخوري	الأستاذ المشرف	رئيسًا
د. وسام غياض	أستاذ	عضوًا
د. رامي عبد الحي	أستاذ	عضوًا

2020

" الجامعة اللّبنانية غير مسؤولة عن الآراء الواردة في هذه الرسالة وهي تعبّر عن رأي صاحبها فقط "

الإهداء

إلى....

الله، الله الموجود في كلّ مكان

أبي وأمي اللّذين لا نجاح لي دونهما

أستاذتي المشرفة الّتي كان لي الفخر بإختيارها

العقل وما أنجز، القلب ومن فيه، الروح وبما آمنت

إلى روح الشهيدتين لين وليا وسيم الحسيني

إلى الأخوة، الأقارب، والأصدقاء الّذين كانوا سندًا في زمن كثر فيه الخائنون ...

إلى الأشخاص غير الواثقين بأنفسهم، بقدراتهم، الّذين يحدّون من كينونتهم البشريّة الّتي لا حدود لها إلاّ الله.

أدعوهم جميعًا إلى الخروج من سجن المستحيل إلى سماء الأحلام، كائنًا من كانوا، فكلّ منّا ناجح بشيء معيّن كما أنّ كلّ واحد منّا جميل بطريقة ما.

إلى الّذين ظنّوا أنّ منعطفات الطّريق ومطبّاتها ستوقفني، من راهنوا على سقوطي في وقت كان فيه السقوط محتمًا، والمطلوب مني أن أفشل، ولكن وبفضل الله ولا أحد غيره، إخترت السّير على الحافة الخطرة تلك الّتي يطلق عليها إسم " الحلم "، تلك الواقعة بين الفراغ والحقيقة. سرت مدعومًا بالأمل، ومؤمنًا بما أملك من قدرات، وموقنًا أنّي سأصل إلى ما أطمح إليه ولو وصلت ممزقًا، مهترئًا، وعاجزًا. سأصل لأنّني صاحب حلم، وخياري المقاومة، والحرب في سبيل ما أهدف إليّه مشروعة. لذلك قرّرت أن أنجح، فأنا اليّوم في بداية الطّريق، وبالرّغم من كلّ شيء، أدعوهم جميعًا ليرافقوني في رحلتي نحو كتابة تاريخ ما، على وجه هذه الكرة الأرضية.

القسم الأوّل: ماهيّة المجرم والضحية المعلوماتيين.

الباب الأوّل: المجرم المعلوماتي.

الفصل الأوّل: تطوّر شخصية المجرم في الإجرام المعلوماتي.

المطلب الأوّل: مفهوم مجرم المعلوماتية

المطلب الثّاني: السلوك الجرمي للمجرمين المعلوماتيين.

الفصل الثّاني: تصنيف علم الإجرام للمجرمين المعلوماتيين.

المطلب الأوّل: الدّوافع المحفّزة لإرتكاب الإجرام المعلوماتي.

المطلب الثّاني: درجة إلمام المجرمين المعلوماتيين بالتقنيّة المعلوماتية.

الباب الثّاني: ضحيّة الإجرام المعلوماتي.

الفصل الأوّل: تطوّر شخصية الضّحيّة في الإجرام المعلوماتي.

المطلب الأوّل: مفهوم ضحيّة الإجرام المعلوماتي.

المطلب الثّاني: إختيار ضحيّة الإجرام المعلوماتي.

الفصل الثّاني: تصنيف علم الإجرام لضحايا الإجرام المعلوماتي.

المطلب الأوّل: الشخص الطبيعي.

المطلب الثّاني: الشخص المعنوي.

القسم الثّاني: المسؤوليّة الجزائية للإجرام المعلوماتي بين ردع المجرمين وضمانات الضّحايا.

الباب الأوّل: أوجه المسؤوليّة الجزائية المعاصرة الّتي يطرحها الإجرام المعلوماتي.

الفصل الأوّل: المسؤولون جزائيًا عن الإجرام المعلوماتي.

المطلب الأوّل: المسؤوليّة الجزائية للمجرم المعلوماتي.

المطلب الثّاني: لجهة مسؤوليّة الضّحيّة.

الفصل الثّاني: الإشكاليّات المؤثّرة في المسؤوليّة الجزائية.

المطلب الأوّل: على مستوى القواعد الإجرائية.

المطلب الثّاني: المسؤوليّة الجزائية عن الحدث المعلوماتي المنحرف.

الباب الثّاني: بين العقوبات والتدابير المناسبة وأهمّية الوقاية.

الفصل الأوّل: آثار المسؤوليّة الجزائية على مجرم وضحيّة الإجرام المعلوماتي.

المطلب الأوّل: الجزاء العقابي.

المطلب الثّاني: الحقوق الملازمة لضحايا الإجرام المعلوماتي.

الفصل الثّاني: أساليب مكافحة السّلوك الإجرامي المعلوماتي.

المطلب الأوّل: الوقاية من الإجرام المعلوماتي.

المطلب الثّاني: التّصدي للإجرام المعلوماتي.

إنّ أهم ما يُميّز العصر الحالي عن غيره من العصور، هو ما نشهده اليوم من تطوّر مثير في المجالات التّكنولوجية، الأمر الّذي إنعكس على معظم مجالات الحياة. حيث نستطيع القول بثقة أنّه لم يُعد هنالك شق يتّصل بالحياة الإنسانية، إلاّ وقد تأثر بهذا التّطوّر التّكنولوجي المثير الّذي أحدث ثورة أدخلت البشرية في عصر جديد.

فكانت النّقلة النّوعية في هذا التّطوّر التّكنولوجي بإكتشاف تقنيّة الإنترنت الّتي جعلت من العالم قرية كونية صغيرة. وعلى الرّغم من الإيجابيات العديدة الّتي أحدثتها هذه التقنيّة في تسهيل نقل وتبادل المعلومات، إلاّ أنّ هناك خشية متزايدة من تنامي الخروق والسّلبيات والأعراض الجانبية لهذه الشّبكة، وإستغلالها من قبل بعض الشّركات، الهيئات، العصابات والأفراد لإرتكاب وتعميم أعمال وأفعال، تتعارض مع القوانين والأعراف والأخلاق والآداب.

لقد صاحب التّطوّر التّكنولوجي الهائل الّذي أحدثته تقنيّة المعلومات، ظهور بعض الفئات الّتي سعت إلى تحويل هذه التّقنيّة إلى وسيلة لإرتكاب الجرائم وأصبح يُطلق عليها مصطلح الجرائم الإلكترونية أو المعلوماتية. فيعتبر الإجرام المعلوماتي نوعًا شائعًا من الإجرام الذي يتميّز مجرموه بأساليبهم الذّكيّة والعلميّة في إرتكابه، والدّقة في إختيار الضّحايا لتحقيق أهداف معيّنة ومحدّدة، وإختلاف الغاية بإختلاف نوع المجرم المعلوماتي وتنوّع الضّحايا حسب الغاية الجرمية[1].

وبفعل عامل السّرعة وصعوبة إكتشاف الدّليل الرّقمي أو الإلكتروني الّذي يتميّز به الإجرام المعلوماتي، وكونه من الإجرام العابر للحدود الّذي لا يسلم منه أي حيّز جغرافي عالمي، أو أي كائن بشري، إلاّ إذا كان ليس بهدف للمجرمين المعلوماتيين[2]، أصبح هذا الإجرام محط أنظار المجتمع الدّولي

[1] د. جنان الخوري، **الجرائم الإقتصادية الدولية والجرائم المنظمة العابرة للحدود**، المنشورات الحقوقية، صادر، 2009، ص: 300.

[2] د. فتوح الشاذلي، عفيف كامل عفيفي، **جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون**، دراسة مقارنة، منشورات الحلبي الحقوقية، 2007، ص: 10.

والإقليمي والمحلّي، محاولين التّصدي له ووضع التّشريعات القانونية المناسبة لمكافحته وإلقاء القبض على مجرميه. وذلك بتشريع قوانين تجرّم هذه الأعمال، وهذا ما ذهب إليه المشرّع اللّبناني حديثًا بتشريعه قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي رقم 81 تاريخ 2018/10/18 لإصباغ الشّرعية للتّصدي للإجرام المعلوماتي من قبل القضاء اللّبناني.

ولمّا كان الإجرام التقليدي ينال إهتمام باحثين علم الإجرام في التّعرف على الجرائم المختلفة فيه ودرس السّلوكيات الإجرامية لمرتكبيه، محاولين تبيان الدّوافع والأسباب التي تحدو بهم لإقتراف الجرائم العادية أو التّقليدية، وإعمال التّصنيف الشّخصي للمجرمين كلّ حسب جرمه المرتكب، وصولًا إلى الأساليب المسبقة واللّاحقة لمكافحة هذه الجرائم من جهة. ومن جهة أخرى التّعرف على ضحايا هذا الإجرام وتبيان عنصريّ الجذب والمنفعة الّتي يوفّرانها للمجرمين العاديين[1]. أصبحنا اليوم أمام إشكاليّة حقيقية بصدد ظهور الإجرام المعلوماتي، تتمثّل في غموض كل من شخصيّة المجرم والضّحيّة المعلوماتيين ، بإختلاف الغاية والدّافع وطبيعة المجرم المعلوماتي، وإختلاف نوعيّة الضّحايا الّتي ترتكب الجرائم عليهم[2] .

هذا الغموض في شخصية كلّ من مجرم وضحية الإجرام المعلوماتي أوجد مجموعة من التساؤلات على المستوى القانوني، حول مدى صلاحية وإنطباق دراسات علم الإجرام السابقة لأطراف الجريمة التقليدية على أطراف الإجرام الحديث وخصوصًا الإجرام المعلوماتي. فهل هناك طبيعة خاصّة للمجرمين المعلوماتيين تميّزهم عن غيرهم من المجرمين التقليدين في مؤهلاتهم، دوافعهم، والأشخاص القائمين بالعمل الجرمي ؟ وهل عمليّة إختيار ضحايا هذا الإجرام أصبحت محكومة بمجموعة من المعايير بعيدًا عن العشوائية؟ وماذا عن أحكام كلّ من المسؤولية الجزائية والمساهمة الجرمية في ظلّ إقتراف الفعل الجرمي

[1] د. سمير عالية، **مبادئ علم الإجرام والعقاب والسياسة الجزائية، أسباب الإجرام ومكافحته جزائيًا**، منشورات الحلبي الحقوقية، 2019، ص: 11.

[2] د. جنان الخوري، **الجرائم الإقتصادية الدولية والجرائم المنظمة العابرة للحدود، المنشورات الحقوقية**، صادر، 2009، ص: 312.

في بيئة جرمية إفتراضية، ومشاركة جرمية من نوع خاص في كثير من الأحيان يمكن أن يكون للضحية دورًا مساعدًا فيها؟ أينفع عندها العقاب الجزائي التقليدي، أم أنّ هناك نوع خاص من العقوبات والتدابير الخاصة بهذه الظاهرة الإجرامية؟ وأخيرًا كيف سيؤسّس علم الإجرام آليّة لمكافحة هذا الإجرام على المستوى الداخلي والدولي في ظلّ التطوّر المثير في الأساليب الجرمية للمجرمين المعلوماتيين؟

فإنّ كان علم الإجرام هو العلم الّذي يدرس طبيعة المجرم والضّحيّة في الجرائم العادية، لمعرفة كل من الدّوافع والحاجات والأسباب الكامنة وراء إرتكاب أيّ جريمة وإنعكاسها على الضّحيّة وصولًا إلى وضع أطر لمكافحتها والحدّ منها، فلا بُدّ من الإستفادة من هذا العلم لدراسة الإجرام المعلوماتي من ناحيتين، المجرم المعلوماتي من جهة أولى، ومن جهة ثانية الضّحيّة المعلوماتية. من هنا تأتي أهمّية دراسة علم الإجرام للمجرم والضّحيّة المعلوماتيين والّتي تكمن في التّصدّي للإجرام المعلوماتي الّذي لا يمكن أن يتمّ كشفه، ملاحقته وتقرير العقوبات المناسبة لمجرميه والضّمانات الخاصّة لضحاياه، دون المعرفة اليقينة لأطراف هذا الإجرام.

ولكن كيف سيحقق علم الإجرام دوره في التصدّي للإجرام المعلوماتي أمام ما يطرحه هذا الأخير من تحدّيات على مستوى غموض شخصيّة كلّ من المجرم والضحيّة فيه؟ خصوصًا أنّنا بأمس الحاجة لهذه المعرفة لإيجاد السّبل المناسبة لنزع الفكر الإجرامي المعلوماتي من عقول المجرمين المعلوماتيين، وتوعية العامّة حول مخاطره كخطوة إستباقية على العمل الجرمي المعلوماتي الّذي بات الأسبق في سبله الإجرامية المتطوّرة والّذي يصوّر في ذهنية المجتمع أنّ مرتكب الإجرام المعلوماتي، هو البطل والذّكي الّذي يستحق الإعجاب، لا صورة المجرم الّذي يستوجب التجريم والعقاب [1].

لذلك تهدف هذه الدّراسة إلى فهم ماهية كل من المجرم والضحية المعلوماتيين على ضوء علم الإجرام،

[1] بن منصور صالح، كوش أنيسة، **السلوك الإجرامي للمجرم المعلوماتي**، مذكرة لنيل شهادة الماستر في الحقوق، جامعة عبد الرحمان ميرة، سنة 2015/2014، ص: 31.

وتحديد الأُطُر القانونية لردع المجرمين وضمان حقوق الضّحايا. بالإضافة إلى التّعرّف على أنماط المجرميين والضّحايا المعلوماتيين، والسّمات الّتي يتمتّع بها كلٌّ منهم. علاوة على معرفة نوعيّة الجرائم المرتكبة في البيئة المعلوماتية، وتبيان الأسباب والدّوافع والغايات الكامنة وراء إقتراف مثل هذا النّوع من الجرائم. كما تهدف إلى التّعرّف على نوعيّة الضّحايا الّذين يصيبهم هذا الإجرام ودورهم السّابق واللّاحق لمواجهته، ومدى مسؤولية الأخيرة عن الجرائم الواقعة عليها. وصولًا إلى التّعرّف على أساليب مكافحة هذا الإجرام، والضّرورة الملحّة للتعاون الدّولي في مجال مكافحته. زد على ذلك، تهدف إلى الإضاءة على بعض الإشكاليّات الّتي يطرحها هذا الإجرام من حيث طبيعته، وما يثيره من صعوبات في تحديد المسؤوليّة الجزائية الّتي يمكن أن تتخطّى مفهوم المساهمة الجرمية إلى الجماعة الإجرامية، فضلًا عن صعوبة إكتشاف المجرم فيه وإثبات الأدلّة ضدّه ممّا يشكّل إفتقارًا في الضّمانات الإجرائية والقانونية للضحيّة والمجتمع. وأخيرًا تبيان دور الذّكاء المعلوماتي في ترتيب المسؤوليّة الجزائية الكاملة على الحدث المعلوماتي، ومدى ملاءَمة قانون الأحداث على الإجرام المعلوماتي المرتكب من هذا الأخير. بالإضافة إلى التّطرّق إلى قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي لمعرفة مدى إنطباقه مع التّطوّر الّذي وصل إليّه الإجرام المعلوماتي، خصوصًا على مستوى الأطراف المرتكبين لهذا الإجرام والأطراف الذين يقع عليهم العمل الجرمي.

كما أنّ هذه الدراسة تتميّز عن غيرها من الدراسات في كونها فريدة من نوعها في معالجة ماهية كلّ من مجرم وضّحيّة الإجرام المعلوماتي بأشكاله المتعدّدة، وما طرأ من إشكاليّات قانونية وعمليّة بفعل هذا التّطوّر على مستوى أطراف الإجرام المعلوماتي. حيث ستشكّل أساس يبنى عليه في مواجهة الإجرام المعلوماتي الّذي لا يمكن أن يأتي بنتائج سليمة دون فهم وضعيّة كلّ طرف من أطراف هذه الجريمة.

وبناءً على ما تقدّم، تمّ تقسيم هذه الدّراسة الّتي تتناول المجرم والضّحيّة المعلوماتيين في ضوء علم الإجرام إلى قسمين رئيسين، في القسم الأوّل، سنتطرّق إلى ماهيّة مجرم وضّحيّة الإجرام المعلوماتي،

محاولين وضع تعريف لكلّ منهما، وتبيان السّمات الّتي يتمتّعان بها لوقوعهما مجرمين أو ضحايا الأعمال الجرمية في البيئة المعلوماتية الّتي سنستعرضها تباعًا، مع المقارنة بقانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي اللّبناني، وصولًا إلى إقامة التّصنيف المفصّل لكلّ من المجرم والضّحيّة في الجريمة المعلوماتية للوقوف على الأسباب والدّوافع وطبيعة الأشخاص الّذين يقعون في دائرة هذه الجريمة.

أمّا في القسم الثّاني، سنتناول المسؤوليّة الجزائية في الإجرام المعلوماتي بين ردع المجرمين وضمانات الضّحايا، من حيث الإضاءة على بعض الإشكاليّات الّتي لم تبحث في إطار المسؤولية الجزائية النّاتجة عن الإجرام المعلوماتي من جهة المجرم والضّحيّة المعلوماتيين. وأيضًا بعض الإشكاليّات على المستوى الإجرائي الّتي لا يزال البحث فيها قائمًا حتّى اليوم، في سبيل تطويرها كي تتلاءم مع الطّبيعة التّطوريّة المتسارعة للإجرام المعلوماتي، والأهميّة البالغة للعقوبات الماليّة وبعض التّدابير الإحترازية المساعدة على مواجهة هذا الإجرام، وصولًا إلى وضع آليّة لمكافحتها بشكل مسبق ومواجهتها بشكل لاحق لإرتكابها.

القسم الأوّل

ماهيّة المجرم والضّحيّة المعلوماتيين

لاشكّ أنّ الإجرام المعلوماتي بإعتباره نوعًا من الإجرام الحديث، يقع في بيئة جرمية مختلفة عن البيئة الجرمية التّقليديّة، وتعتبر البيئة المعلوماتية هي المحل الأساسي الّتي يقع فيه. فهي بيئة غير مادّية أيّ غير ملموسة، تتضمّن البيانات والبرمجيات وغيرها من الأمور التّقنيّة والمعلوماتية حتى لو إستهدفت أجهزة مادّية، وذلك لأنّ الوسيلة المستعملة في إرتكاب الإجرام المعلوماتي غير مادّية أصلًا. فيستهدف الإجرام المعلوماتي كلّ من المعلومات والأجهزة، أو أشخاص محددين أو جهات أمنية وعسكرية وحكومية مختلفة.

وإذا كان لكلّ جريمة مجني ومجنى عليه، أيّ مجرم يرتكب الفعل الجرمي وضحيّة يقع عليها هذا الفعل، فإنّ ما يثيره الإجرام الحديث بشكلٍ عام والإجرام المعلوماتي بشكلٍ خاص من إشكاليّات على مستوى تحديد أطراف الجريمة، هو إختلاف نوعيّة المجرمين فيه عن المجرمين التّقليدين. كذلك الأمر بالنّسبة إلى الضّحايا، حيث أنّ نوعيّة الجرائم إختلفت تبعًا للتغيير الحاصل على مستوى محل وقوع الجريمة والقائم بها، والغايات الجرمية الّتي يطمح إلى تحقيقها المجرمين المعلوماتيين.

فيحاول علم الإجرام بكونه ذلك الفرع من العلوم الجزائية، البحث في أسباب الجريمة ومكوّناتها وسياقها ونتائجها. فيدرس الإجرام المعلوماتي كحقيقة واقعية بأسبابه وبواعثه العضوية والبيئية من أجل علاجه والوقاية منه، فهو العلم الذي يبحث في الجريمة بإعتبارها ظاهرة إجرامية في حياة الفرد وحياة المجتمع للتعرف على أسبابها، تمهيدًا للوصول إلى أفضل الوسائل للقضاء على هذه الأسباب أو للحد من تأثيرها قدر الإمكان.

لا يمكن فهم الظاهرة الإجرامية المعلوماتية دون فهم كلّ من المجرم والضّحيّة المعلوماتيين، فالمجرم

المعلوماتي بحسب علم الإجرام هو مجرم حديث له صفاته الخاصّة الّتي جعلت منه مجرمًا متمكّنًا واثقًا بنفسه وبقدراته، معتقدًا أنّه متفوّق على الجميع حتى على أجهزة الدّولة، خصوصًا الإستقصائية والقضائية منها. أمّا الضّحيّة، الّتي بدأ الإهتمام الكبير بها في الجرائم التّقليدية، أصبح هناك ضرورة للتعرّف عليها في الإجرام المعلوماتي، ذلك لما يعكسه هذا الإجرام من سلبيّات على ضحاياه، خصوصًا أنّه يشكّل حاجز خوف يدفعهم إلى إخفائه عن الجميع حتّى عن أجهزة الدّولة حفاظًا على سمعتهم أو خصوصيتهم.

هذا ما أعطى لدراسة مجرم وضّحيّة الإجرام المعلوماتي أهمّية وذلك من خلال علم الإجرام الّذي يسلّط الضوء على مفهوم كلّ من المجرم والضّحيّة، طبيعة كلّ منهما والدّوافع الّتي تؤدي إلى إرتكاب الإجرام المعلوماتي وصولًا إلى وضع معالجة وحلول للحدّ من هذه الظاهرة الإجرامية. بالإضافة إلى إمكانية تأثيره على كلّ من قانون العقوبات وقانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي، فكلّما كانت الدّراسات الإجرامية تكشف عن جديد كان المشرّع يعمد إلى إدخال تعديلات جوهرية على سياسة التجريم والجزاء. فكثيرًا ما ترتبط القاعدة القانونية بالمجتمع والضّرر الإجتماعي الّذي تسببه الجريمة والّذي من خلال تحديد هذا الضّرر يمكن أن نؤسس للعقاب والجزاء.

لذلك سنقوم في هذا القسم من الدّراسة بالتّعرّف على مجرمي الإجرام المعلوماتي وأبرز السّلوكيات الجرمية التي يقومون بها، بالإضافة إلى تصنيف علم الإجرام لمجرمي المعلوماتية من حيث الدّوافع المحفّزة لإرتكاب الجريمة المعلوماتية أم من حيث درجة الإلمام بالتّقنيّة المعلوماتية وذلك في باب أوّل. ثمّ سنستعرض في الباب الثّاني ضحايا الإجرام المعلوماتي من حيث التعرّف على مفهومهم وسماتهم الخاصّة، والآليّة التي يتمّ إختيارهم فيها كضحايا من قبل مجرمي المعلوماتية، وصولًا إلى تبيان تنوّعهم من حيث وجود ضحايا طبيعيين وآخرين معنويين يختلف إختيارهم حسب الغاية الجرمية للمجرم المعلوماتي.

الباب الأوّل

المجرم المعلوماتي

إذا كان هدف علم الإجرام تحديد أسباب الجريمة وصولًا إلى وضع حلول لها، فذلك لا يتمّ دون التطرّق إلى فاعل هذه الجريمة ألا وهو المجرم. ولعلّ أبرز ما قدّمه علم الإجرام في إطار مكافحته للظاهرة الإجرامية هو في ضرورة الدراسة والتحقق المسبق من ظروف المدّعى عليه، وذلك من حيث دراسة الأسباب والدوافع التي دفعته إلى إرتكاب إجرامه، ومعرفة ما إذا كانت هذه الدوافع داخلية ناتجة عن شعور داخلي شخصي يعني المجرم، أم كان الدافع خارجيًا يتعلّق بيئته الإجتماعية أو وضعه الإجتماعي العام.

أمّا بالنسبة إلى الإجرام المعلوماتي فإنّ ما زاد من تعقيدات هذا الإجرام هو إختلاف شخصيّة المجرم القائم به عن المجرم التّقليدي، وذلك لإختلاف البيئة الّتي يقع فيها الإجرام، الحيّز المكاني، وإختلاف المؤهلات أو السّمات الّتي يتطلّبها لتحقيق أهدافه. أيّ بمعنى أكثر دقة، لا يمكن إجراء القياس في علم الإجرام بين الأسباب والدّوافع الّتي أدّت بالمجرم التّقليدي لإرتكاب أعماله الجرمية، وبين تلك الدّوافع والأسباب الّتي دفعت المجرم المعلوماتي لإرتكاب فعله الجرمي، وذلك لعدّة إعتبارات جوهرية أبرزها إختلاف البيئة الجرمية والأسلوب ومتطلبات الجريمة. هذا ما يبرر ضرورة دراسة علم الإجرام للمجرم المعلوماتي وذلك من خلال ما يوفّره هذا العلم من تقنيات وأساليب تمكّننا من التعرّف على شخصيّة مجرم المعلوماتية وصفاته والدّوافع الّتي تدفعه لإرتكاب جرائمه المتنوّعة في البيئة المعلوماتية.

لذلك سنقوم في هذا الباب بالبحث في تطوّر شخصية المجرم في الإجرام المعلوماتي في فصل أوّل لبناء مفهوم علمي وقانوني له، والتعرّف على أهم الصّفات الّتي تميّزه عن غيره من المجرمين التقليديين والسلوكيّات الجرمية الّتي يرتكبها في البيئة المعلوماتية. أمّا في الفصل الثّاني فسنتطرّق إلى تصنيفات علم الإجرام للمجرم المعلوماتي أولًا من حيث الدّوافع المحفّزة لإرتكاب هذا الإجرام، وثمّ من حيث درجة الإلمام بالتّقنيّة المعلوماتية للتعرّف على مختلف الأشخاص المرتكبين لهذا الإجرام.

الفصل الأوّل

تطوّر شخصيّة المجرم في الإجرام المعلوماتي

كان المجرم التّقليدي في نظر علم الإجرام محدّد الغاية الّتي من أجلها يرتكب جريمته، والّتي تكون في معظمها دوافع ماليّة أو إبتزازية، وكان دائمًا على علم بأنّه يرتكب جريمة معنويّة وأخلاقيّة ومجتمعيّة بحق طرف آخر، في حين أنّ الضّحية تقع فريسة هؤلاء لأنّها الأقرب إليهم والأسهل في إنهاء مشروعهم الجرمي. أمّا اليوم وبصدد الإجرام المعلوماتي، فهناك نوع من التّلطيف لمفهوم الإجرام المعلوماتي وإعتباره نوعًا من الأعمال الّتي تُمكّن المجرم المعلوماتي من الظهور أمام المجتمع بمظهر القويّ، الذّكيّ، المسيطر على التّقنيّة وكلّ ما يرتبط بها [1]. فالمجرم المعلوماتي لا تحدّه أيّة ضوابط أخلاقيّة حتّى ولو إصطدم بالقانون، وأصبحت الضّحيّة المعلوماتية عرضة لإجرام حديث يعتبر أعماله مشروعة ومرغوبة على عكس حقيقتها.

لذلك كان لا بُدّ من دراسة السلوك الجرمي للمجرم المعلوماتي من خلال علم الإجرام الّذي يبحث الظاهرة الإجرامية من خلال أربعة أطراف، الجريمة، المجرم، الضّحيّة والمجتمع. لذلك سنقوم في هذا الفصل بعرض مفهوم للمجرم المعلوماتي وذلك في مطلب أوّل، أمّا في المطلب الثّاني سنتناول السّلوكيات الجرمية التي يرتكبها المجرم المعلوماتي في البيئة المعلوماتية.

المطلب الأوّل: مفهوم مجرم المعلوماتية

إنّ شخصيّة المجرم المعلوماتي وآليّة إرتكاب الجريمة تجعل منه شخصًا يتّسم بسمات خاصّة، تضاف إلى الصّفات الأخرى الّتي يجب أن تتوافر في المجرم العادي. ولا يمكن لأيّ قانون وأيّ عقوبة أن تحقّق هدفها، سواء في مجال الرّدع العام أو الرّدع الخاص، ما لم نفهم وبدقة شخصيّة المجرم. وذلك عبر محاولة لإيجاد مفهوم قانوني يتناسب مع وضعه الّذي يأخذ مفهومًا غير متناسق بين نظرة المجتمع

[1] David Johnson, **Electromnic Privacy**, stodder, Canada, 1997, p: 66.

للمجرم المعلوماتي وتلك الّتي يأخذها القانون، ذلك بغيّة التّمكن من إعادة تأهيله إجتماعيًا ودمجه في المجتمع بشكل سليم. ومن خلال هذا المطلب سنحاول الوصول إلى تعريف للمجرم المعلوماتي في نبذة أولى، أمّا في النّبذة الثّانية فسنتعرّف على أبرز الصّفات الّتي يتمتع بها.

النّبذة الأولى: تعريف مجرم المعلوماتية

إنّ أبرز إشكاليّة تعترض الإجرام المعلوماتي بعد مسألة تحديد مفهوم محدّد للجريمة المعلوماتية، هي في إيجاد تعريف للمجرم المعلوماتي الّذي يرتكب هذه الجرائم عبر تقنيّة المعلومات. حيث تهتم أبحاث علم الإجرام بدراسة المجرم بإعتباره موضوعًا لها وذلك حتّى تتعرّف على مختلف جوانب شخصيّته وتكوينه البدني والنّفسي.

فإنّ تحديد مفهوم المجرم في نطاق الدّراسات الإجرامية ليس بالأمر اليسير، فلم يحدّد القانون متى تبدأ الحالة الّتي يوصف فيها الشّخص بأنّه مجرم وبالتّالي لا يحدّد نهايتها. وفي نفس الوقت فإنّ إعتبار الشّخص مجرمًا من عدمه، تحكُمه إعتبارات ومعتقدات إجتماعية راسخة وأفكار مسبقة، كل ذلك يعطي مدلولًا نسبيًا لمفهوم المجرم. فتحديد مفهوم المجرم يكتنفه بعض الصّعوبات، فيُعرّف الفقه التّقليدي المجرم بأنّه ذلك الشّخص الّذي يرتكب جريمة ممّا نصّ عليه في قانون العقوبات، هذا يعني أنّ الشّخص يجب أن يُثبت إرتكابه للجريمة من خلال محاكمته قانونًا [1].

مع ذلك فقد وَجّه علماء الإجرام لهذا التّعريف عدّة إنتقادات، فمن ناحية يعرّف التّشريع الحديث عددًا هائلًا من النّصوص الجزائيّة الّتي لا يَعرف بوجودها الكثيرون، من بينها ما يهدف إلى تنظيم إداري لبعض أوجه الحياة في المجتمع، ومخالفة هذه القواعد لا يساعد في إضفاء صفة المجرم على من يخالفها. ومن ناحية أخرى، هناك أنواع من السّلوك تعتبر ذات طبيعة إجرامية في حقيقتها، بصرف النّظر عمّا إذا كان

[1] بن منصور صالح، كوش أنيسة، **السلوك الإجرامي للمجرم المعلوماتي**، مذكرة لنيل شهادة الماستر في الحقوق، جامعة عبد الرحمان ميرة، سنة 2015/2014، ص: 23.

المشرّع قد خلع عليها هذا الوصف الإجرامي أم لا. وقد أدّت هذه الإنتقادات إلى نشأة إتّجاه حديث يبحث عن تعريف جديد للمجرم [1]، وأهمّ ما يميّز المجرم وفقًا لهذا المفهوم الحديث أنّه يتمتّع بعقلية لا إجتماعية، أيّ عقلية غير قادرة على التكيّف إجتماعيًا.

بالرّغم من شموليّة هذا التّعريف لكافّة السّلوكيات الإجرامية للمجرم إلاّ أنّه يصطدم بشكل مباشر بمبدأ الشّرعيّة، أيّ عدم إمكانية التّجريم والعقاب على فعل أو سلوك غير منصوص عليه في القانون من جهة، ومن جهة أخرى عدم مراعاته وإحترامه للحريّة الفرديّة الّتي يتمتّع بها كل فرد بمقتضى الدّستور والنّصوص القانونية الأخرى.

وإذ كان علم الإجرام ينتقد التّعريف القانوني المقرّر للمجرم التّقليدي من حيث تضييقه لمحتوى دراساتهم وأبحاثهم، وإبتعاده عن متناول أيدي الكثير من الأشخاص الّذين لا يعترف القانون بإجرامهم أو أغفل أو لم يواكبها، إلاّ أنّه بصدد دراسة المجرم المعلوماتي لا نستطيع الإكتفاء بالتّعريفات القانونية لهذا المجرم، وذلك لعدم وضوح الإجرام المعلوماتي بشكله الكامل بعد، وعدم إمكانيّة الإحاطة بكافّة وسائله كونه إجرامًا تطوّريًّا، متغيرًا بشكل مستمر وسريع.

لذلك كان لا بدّ من تحديد مفهوم معاصر للمجرم المعلوماتي وأن نستعين بكافة العلوم والمجالات العلميّة للوقوف على تعريف مناسب له. وفي صدد تعريفنا للمجرم المعلوماتي لا بدّ من الإنطلاق من تعريف الجريمة المعلوماتية والّتي تُعرّفها منظمة الأمم المتّحدة عام 2000، على أنّها الجريمة الّتي يمكن إرتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب، أو في بيئة إلكترونية [2]. وإستنادًا إلى هذا التّعريف، حاول البعض بشكل مبدئي تعريف المجرم المعلوماتي على أنّه الشّخص أو الجماعة

[1] د. سمير عالية، **مبادئ علوم الإجرام والعقاب والسياسة الجزائية**، المرجع السابق نفسه، ص: 150.

[2] د. جنان خوري، **الجرائم الإقتصادية الدّوليّة والجرائم المنظمة العابرة للحدود**، المرجع السابق نفسه، ص: 301.

الّتي ترتكب الجريمة المعلوماتية، بحيث يُستخدم الحاسوب كأداة للجريمة أو هدف لها أو كليهما [1].

لكن هذا التّعريف للمجرم المعلوماتي ضعيف نسبيًا أمام ما يثيره هذا المجرم من سمات وخصائص تميّزه عن غيره من المجرمين التّقليديين، وأهم عنصرين يجب أن يشملهما أي تعريف للمجرم المعلوماتي هما: عنصر الذّكاء والمستوى العلمي الّذي يتمتّع به هذا المجرم في البيئة المعلوماتية الّتي تُرتكب فيها الجريمة.

ويُعرّف البعض المجرم المعلوماتي على أنّه المجرم الّذي لديه قدرة على تحويل نواياه الجرمية إلى لغة رقميّة بإستخدام التّقنيّة الرّقميّة المعلوماتية، وذلك بأداء فعل أو الإمتناع عنه، ممّا يُحدث إضطرابات في المجتمع المحلّي أو الدّولي نتيجة مخالفته قواعد الضّبط الإجتماعي محليًا ودوليًا [2].

إزاء كلّ هذه التّعريفات للمجرم المعلوماتي، نرى أنّه لا زال هناك قصور في تحديد مفهوم مناسب له. بناءً على ذلك يمكن تعريف المجرم المعلوماتي على أنّه الشّخص أو الجماعة الّتي ترتكب الجريمة المعلوماتية إمّا بأداء فعل أو الإمتناع عنه، بإستخدام الحاسوب كأداة للفعل الجرمي أو هدف له أو كليهما، معتمدين على المستوى العلمي والذّكاء البشري في المجال الإلكتروني الّذي يتمتّع به الشّخص والّذي يمكن توظيفه في أفعال جرمية شخصيّة أو غير شخصيّة.

ولكن نظرة المجتمع إلى المجرم المعلوماتي تختلف عن نظرة القانون أو الدّولة وحتّى الضّحيّة، وذلك لأنّ المجرم المعلوماتي برأي المجتمع لا يُعتبر مجرمًا إنّما هو شخص يمتلك قيمة إجتماعية مهمّة وهي الذّكاء البشري، الّتي تجعل منه شخصًا مهمًا يتقبله الجميع ويحترمه أكثر من غيره من عامة الناس. وهذه تعتبر من أبرز الإشكاليّات الّتي نعاني منها في ظلّ ظهور الجرائم الحديثة وبشكل خاص الإجرام المعلوماتي، حيث أنّ مفهوم الجريمة لهكذا نوع من الجرائم لازال غائبًا عن ذهن المجتمع الّذي نعايشه وخصوصًا في بلدان العالم الثّالث. فيتحوّل المجرم من شخص مسؤول عن جريمته ويجب أن يفرض عليه

[1] محمد علي سالم، حسون عبيد هجيج، **الجريمة المعلوماتية**، المرجع السابق نفسه، المجلد 14، العدد 2، سنة 2007، ص:88.

[2] حيى بن محمد أبو مغايضا، **لأبعاد الإستراتيجية في مواجهة الجريمة الإلكترونية**، أكاديمية نايف للعلوم الأمنية، مؤتمر الجرائم المعلوماتية، 2009، ص:4.

العقاب الجزائي، إلى شخص يتمتّع بمستوى إجتماعي مرموق وسط مجتمعه لما يمتلك من ذكاء في السيطرة والتحكم على التقنيّة المعلوماتية لا يملكها غيره من أفراد مجتمعه، ولو تمّ توظيف هذا الذّكاء في أفعال غير مشروعة، وهذا على عكس نظرة القانون والضّحيّة والدّولة له ممّا يسبغ عليه الصّفة الجرمية إن إقترف أعمالًا جرميّة منصوصًا عليها قانونًا حتّى لو كان المجتمع يناقض ذلك.

هذا التعارض له أثره بشكل مباشر أو غير مباشر، حيث أنّ عدم إدانة المجتمع للمجرم المعلوماتي تشجّع على مزيد من التجاوزات القانونية في التّقنيّة المعلوماتية وتصبح عمليّة التأهيل والإصلاح للمجرمين المعلوماتيين دون أيّ مفعول. ونتيجة لهذا التّعقيد الكبير الّذي يواجه وجود تعريف موحّد للمجرم المعلوماتي والتناقض الحاصل في إعتباره مجرمًا من عدمه بين المجتمع والقانون، كان لا بُدّ من تبيان صفات هذا المجرم للتعرّف على شخصيّته الجرمية بشكل أفضل، والخصائص الّتي تميّزه عن غيره من المجرمين.

النّبذة الثّانية: صفات مجرم المعلوماتية

إنّ تحديد السّمات الّتي يتمتّع بها المجرم لا يخلو من الأهمّية لتقرير الجزاء والعقاب، وإذا تنوّعت الجرائم المرتكبة في السّاحة الجرمية، في هذا الصّدد يقول الخبير الأميريكي "دون باركر" Don Parker " أنّ المجرم المعلوماتي وإن كان يتميّز ببعض السّمات الخاصّة إلاّ أنّه لا يخرج في النّهاية عن كونه مرتكبًا لفعل إجرامي يتطلّب توقيع العقاب عليه، فكلّ ما في الأمر أنّه ينتمي إلى طائفة خاصّة من المجرمين تقترب في سماتها من جرائم ذوي الياقات البيضاء (الإجرام المكتسب). وليس معنى ذلك أنهم أقلّ خطورة من النّاحية الإجرامية من المجرمين ذوي الياقات الزرقاء (المجرم بطبيعته) "[1] . وبإختلاف السّمات الجرمية للمجرم بين جريمة وأخرى، هناك في الإجرام المعلوماتي إختلاف وتمايز في السّمات الّتي يتميّز بها المجرم المعلوماتي العادي عن الجماعة الإجرامية، وذلك حين يشترك أكثر من شخص في نشاط جرمي واحد

[1] علي عبود جعفر، **جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة** (دراسة مقارنة)، منشورات زين الحقوقية، سنة 2013، ص: 107.

ومشترك في البيئة المعلوماتية. لذلك سنتناول أوّلًا السّمات المشتركة بين المجرمين المعلوماتيّين، ثمّ السّمات الّتي تتميّز بها الجماعة الإجرامية .

السّمات المشتركة بين المجرمين المعلوماتيين

يتّفق الفقهاء والباحثون في علم الإجرام أنّه لا يوجد نموذج واحد للمجرم المعلوماتي، وإنّما هناك سمات شخصيّة مشتركة تجمع هؤلاء، أبرزها الذّكاء والمستوى التعليمي.

1. التّخصّص

لا يمكن لأيّ كان أن يعمل عاى تقنيّة المعلومات ويحيط بها ويستغلّها في إرتكاب الجرائم الواقعة عليها أو عن طريقها. فالشّخص القائم بهذا النّوع من الإجرام يجب أن يكون لديه حدّ أدنى من التّخصّص في المجال الإلكتروني أو المعلوماتي، الّذي بدوره يمكّنه من إكتساب المهارة الّتي هي جوهر سمات المجرم المعلوماتي [1].

يجب الإشارة في هذا المجال إلى أنّ عمليّة التّخصّص يقصد بها التّخصّص الفعلي في إختصاص المعلومات والهندسة المعلوماتية والإلكترونية. أمّا تعلّم الخروقات السّلبية والقرصنة وإرتكاب الجرائم في البيئة المعلوماتية، يعود بالقدر الكبير إلى جهود المجرم الّذي يحاول أن يوظّف ما تعلّمه في المجال الإلكتروني على نحو مخالف للقوانين والأنظمة والآداب.

2. الذّكاء

إذا عزّيت بعض الجرائم القديمة أو التّقليدية إلى جنون العقل والذّهن، فتعزّى بعض الجرائم الحديثة إلى جنون العظمة أو البارانويا "Paranoia"، حيث أنّ الأغبياء أو ضعفاء العقل لا يشكّلون إلاّ نسبة ضئيلة من هذه الجرائم. عمليًا تحتاج الجرائم الحديثة إلى التّفكير، التّخطيط، التّحضير، الحكمة، التّدبّر، الرؤية، التّعقل وغير ذلك ممّا لا يتوافر لدى أصحاب العقل المشوّش [2].

---

[1] علي عبود جعفر، **جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة**، المرجع السابق نفسه، ص:107.

[2] د. جنان الخوري، **الجرائم الإقتصادية الدّوليّة والجرائم المنظمة العابرة للحدود**، المرجع السابق نفسه، ص: 146.

وكون جرائم المعلوماتية من الجرائم الحديثة، يعتبر الذّكاء البشري من أهم صفات مرتكبي هذه الجرائم. إذ يقال عادة أنّ الإجرام الحديث هو إجرام الأذكياء بالمقارنة مع الإجرام التقليدي الّذي يميل إلى العنف [1]، فإجراء عمليّات القرصنة المعلوماتية لا يمكن أن تكون أو تنجح دون وجود ذكاء بشري متمكّن منها وقادرعلى بنائها وإستغلالها بشكل يخدم دوافع المجرم [2].

3. الخبرة

إنّ عنصريّ التّخصّص والذّكاء يُعتبران من السّمات الأساسيّة للمجرم المعلوماتي، لكن ما يعزّز من وضعية هذا المجرم في عالم الإجرام هو عنصر الخبرة الّذي يحوّل المجرم المعلوماتي المبتدىء، إلى مجرم محترف بفعل الممارسة المستمرّة لها. إستنادًا إلى الباحث في علم الإجرام "دون باركر" Don Parker ، فإنّ المهارة هي أبرز خصائص مجرم تكنولوجيا المعلومات، حيث تتطلّب تنفيذ الجريمة التقنيّة أن يتمتّع الفاعل بقدر كبير من المهارة الّتي قد يكتسبها عن طريق الدّراسة المتخصّصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات [3].

4. السّنّ والمكانة

إنّ الجرائم التّقليدية كانت تُعرف بجرائم الفقراء، حيث كانت تبلغ ذروة إرتكاب الجرائم التّقليدية والعادية لدى الذكور بين 21 و25 سنة، أمّا في جرائم المعلوماتية فنرى أنّ الأفعال الجرمية تُرتكب من أشخاص ناضجين جسديًا وفكريًا وإجتماعيًا، ومنتظمين في مؤسّسات إقتصادية وطنيّة ودولية وإجتماعية، بحيث يوظفون كلّ هذه المعطيات لبلوغ أهدافهم[4]. من جهة أخرى لم يعد يقتصر إجرام الأحداث على الحدث المنحرف، المتسوّل، المشرّد، فقير الحال، مهمل الوالدين ووليد الشّارع بل غدونا أمام صغار المجرمين أو جرائم الصّغار، وليد العائلة الثّرية، الّذي يرتكب جرائمه داخل غرفته المجهّزة

[1] نصر شومان، **التكنلوجية الجرمية وأهميتها في الإثبات، دراسة في الحقوق**، سنة 2011، ص: 25.

[2] طوم توماس، **الخطوة الأولى نحو أمان الشبكات، الدار العربية للعلوم**، سنة 2004، ص: 27.

[3] علي عبود جعفر، **جرائم تكنلوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة**، المرجع السابق نفسه، ص:26.

[4] د. جنان خوري، **الجرائم الإقتصادية الدّوليّة والجرائم المنظمة العابرة للحدود**، المرجع السابق نفسه، ص: 147 –148.

بأحدث التّقنيّات.

5. العودة إلى الإجرام أو الإعتياد الجرمي

يتميّز المجرم المعلوماتي بأنّه يعود للجريمة دائمًا، فهو يوظّف مهاراته في كيفيّة عمل الحواسيب، تخزين البيانات والمعلومات، والتّحكم في أنظمة الشّبكات في الدّخول غير المصرّح به مرّات ومرّات [1]. فهو قد لا يحقّق جريمة الإختراق بهدف الإيذاء وإنّما نتيجة شعوره بقدرته ومهارته في الإختراق.

6. الميل إلى التّقليد

يبلغ الميل إلى التّقليد عندما يتواجد الفرد وسط الجماعة، إذ يكون عندئذٍ أسهل وأسرع إنسياقًا لتأثير الغير عليه. ويظهر ذلك في الجريمة المرتكبة عبر الإنترنت، لأنّ أغلب الجرائم تتمّ من خلال محاولة الفرد تقليد غيره بالمهارات الفنّيّة ممّا يؤدي به الأمر إلى إرتكاب الجرائم [2]. لا شكّ أنّ ذلك نتيجة عدم الإستواء في شخصيّة الفاعل الفرد الذي يتأثّر بخاصّيّة الميل إلى التّقليد بسبب عدم وجود ضوابط يؤصّلها في ذاته، ممّا يحجم لديه غريزة التّفاعل مع الوسط المحيط، وينتهي إلى إرتكاب الجريمة.

سمات الجماعة المعلوماتية الإجرامية

إن عمل الجماعة المعلوماتية الإجرامية يُبنى على أسس مترابطة، متينة وتتّخذ من التّنظيم والتّخطيط وتقسيم العمل عاملًا أساسيًّا في نجاح مشروعها الجرمي. لذلك سنستعرض السّمات الّتي تتميز بها هذه الجماعات.

1. الصّفة المهنيّة

تتصف الجرائم المرتكبة من قبل الجماعة المعلوماتية ب " الصّفة المهنيّة " وتحديدًا بمهنيّة متقدّمة وتقنيّة، من خلال اللّجوء إلى الوسائل الأكثر حداثة [3]. بالتّحديد إلى الآليّات الإلكترونية المتطوّرة والأكثر أمانًا، للهروب وإخفاء معالم الجريمة والأكثر صعوبة للمراقبة والتّحقيق.

---

[1] نصر شومان، **التكنلوجية الجرمية وأهميتها في الإثبات**، المرجع السابق نفسه، ص: 25.

[2] بن منصور صالح، طباش عز الدين، **السلوك الإجرامي للمجرم المعلوماتي**، المرجع السابق نفسه، ص: 27.

[3] د. جنان الخوري، **الجرائم الإقتصادية الدّوليّة والجرائم المنظمة العابرة للحدود**، المرجع السابق نفسه، ص: 101.

2. التّنظيم والتّخطيط

إنّ أغلب الجرائم المعلوماتية في البيئة المعلوماتية والّتي تكون على قدر كبير من الأهمّية، تُرتكب من قبل مجموعة مكوّنة من عدّة أشخاص، يحدّد لكلّ شخص دور معيّن، ويتمّ العمل بينهم وفقًا لتخطيط وتنظيم سابق على إرتكاب الجريمة[1]. أمّا من ناحية البنية والعدد، تُعتبر هذه الجماعات جماعات إجرامية مهيكلة ومنظّمة من العصابات أو المافيا، وتتألف من ثلاثة أشخاص كحد أدنى [2]. فمثلًا جريمة زرع الفيروسات، هذه العمليّة الجرمية تحتاج إلى مجموعة من الأشخاص أحدهم المبرمج الّذي يقوم بكتابة البرنامج، وآخر يكون المستخدم الّذي يقوم بعمليّة زرع الفيروسات داخل الأجهزة الأخرى.

3. عدم العشوائية

تُشكَّل هيكليّة الجماعة المعلوماتية الإجرامية على شكل غير عشوائي[3]، كون طبيعة إجرامها والسّلوك الجرمي فيها يرتكز بشكل أساسي على الذّكاء، التّخصّص، الخبرة والسّرية. فإختيار المنضمين إلى هذه الجماعات يكون على مستوى كبير من الأهمّية من ناحية المؤهلات الشّخصيّة، ومن ناحية تلائم هذه المؤهلات مع الدّور المقرّر له داخل هذه الجماعة.

4. التطوّر في السّلوك الإجرامي

إنّ إنخراط الفرد ضمن جماعة إجرامية يزيد لديه الملكة الإجرامية والتفوّق العلمي، نتيجة عمليّة التّعلّم والتّعليم الّتي تحصل داخل هذه الجماعة. فالجريمة المعلوماتية تحتاج إلى دقّة في تنفيذ العمليّات غير المشروعة ومشاركة ومساعدة أشخاص آخرين. ممّا ينعكس فيها على الفرد إيجابًا، حيث يقوم بمساعدته أو بمساعدة الآخرين بأمور مادّية أو معنوية [4].

---

[1] بن منصور صالح، طباش عز الدين، **السلوك الإجرامي للمجرم المعلوماتي**، المرجع السابق نفسه، ص: 27.

[2] نصر شومان، **التكنلوجية الجرمية وأهميتها في الإثبات**، دراسة في الحقوق، سنة 2011، ص: 26.

[3] د. جنان الخوري، **الجرائم الإقتصادية الدّوليّة والجرائم المنظمة العابرة للحدود**، المرجع السابق نفسه، ص: 105.

[4] بن منصور صالح، طباش عز الدين، **السلوك الإجرامي للمجرم المعلوماتي**، المرجع السابق نفسه، ص: 29.

5. السّرية والإنخراط الإجتماعي

إنّ عمل الجماعة الإجرامية المعلوماتية يضمّ قادة ومنفّذين ميدانيين، يتوزعون ضمن هيكليّة منظّمة بطريقة مدروسة وتصميم مخفي بعيد عن الشّبهات، ويلتزم أعضاؤه فيها السّرية التّامّة، حيث تجمعهم الوحدة، المصير، الإستمرارية، تقسيم العمل، وتحديد الأدوار [1]. لكن بالمقابل، وبالرّغم من السّرية الحادّة الّتي تتميّز بها هذه الجماعة، نرى أنّ أعضاء هذه الجماعة أشخاص متكيّفين إجتماعياً لاسيما فيما بينهم، إمتدادًا لسمة التّخطيط والتّنظيم والتّكيّف مع غيره من أفراد المجتمع، في حين أنّه لا يضع المجرم المعلوماتي نفسه في عداء مع أفراد المجتمع الّذي يحيط به [2].

6. البعد الدّولي

إنّ الجماعة المعلوماتية يمكن أن تكون عابرة للحدود من وجهتين: الوجهة الأولى، من ناحية إشتراك بضعة فاعلين في دول عدّة وبُعد متخط للحدود الدّوليّة في مشروع إجرامي واحد في البيئة المعلوماتية [3]. بينما الوجهة الثّانية، يمكن أن تكون الصّفة العابرة للحدود أو الدّوليّة على مستوى المكان أو الحيّز المستهدف من هذه العمليّة، كأن يقصد مجموعة من المعلوماتيين بشنّ هجمات على مصرف أجنبي، وتحويل أموال منه إلى بلد آخر وفي هذه الوجهة الأخيرة تشترك الجماعة مع المجرم المعلوماتي الفرد فيها. لكن ما يجب الإشارة إليه في صدد حديثنا عن الجماعة الإجرامية المعلوماتية، هو ما يثيره تقسيم العمل داخل هذه الجماعات تجاه نظريّة قانون العقوبات التّقليدي الّذي يركّز على الجرائم المقترفة من خلال فاعلين منفردين، والّذي لم يعدّ العدّة الكافية لمواجهة الجرائم المقترفة من قبل جماعات ذات هيكليّة غامضة وخفيّة.

إذًا تختلف صفات المجرم المعلوماتي عن غيره من المجرمين التّقليديين، وأبرز إختلاف هو تمتّعه بالذّكاء البشري الّذي يمكّنه من السّيطرة والتّحكم بالتّقنيّة المعلوماتية. وتشتد خطورة الإجرام المعلوماتي حين

---

[1] د. جنان الخوري، **الجرائم الإقتصادية الدّوليّة والجرائم المنظمة العابرة للحدود**، المرجع السابق نفسه، ص: 105.

[2] بن منصور صالح، طباش عز الدين، **السلوك الإجرامي للمجرم المعلوماتي**، المرجع السابق نفسه، ص: 28.

[3] د. جنان الخوري، **الجرائم الإقتصادية الدولية والجرائم المنظمة العابرة للحدود**، المرجع السابق نفسه، ص: 101.

يكون العمل الجرمي يمارس عبر تنظيم إجرامي معلوماتي، بحيث يؤسس هذا الأمر إلى نتيجة أكثر خطورة من العمل الفردي كون هناك مجموعة من الخبرات الفردية تتعاون في مشروع جرمي جماعي واحد.

ولا شكّ أنّ الإجرام المعلوماتي ليس واحد إنّما متعدّد ومتنوّع، فالسّلوك الجرمي للمجرم المعلوماتي يتحدّد بحسب الغاية الجرمية التي يهدف إليها هذا الأخير. مثلما هناك تعدّد في الجرائم التقليدية هناك أيضًا تعددية في الجرائم المرتكبة من قبل المجرم المعلوماتي في البيئة المعلوماتية، خصوصًا مع ما توفّره هذه البيئة من مساحة للأعمال الجرمية المختلفة والّتي سنستعرضها في المطلب الثّاني.

المطلب الثّاني: السّلوك الجرمي للمجرمين المعلوماتيين

لا تعدّ الدّراسات الّتي تناولت سلوك المجرمين في الجرائم التّقليديّة كافيّة لتفسير السّلوك الجرمي للمجرم المعلوماتي في الإجرام المعلوماتي، فإختلاف البيئة الّتي يقع فيها الإجرام من جهة، وبروز جرائم جديدة تطال المعلومات الرّقميّة وغير الرّقميّة في الحاسب الآليّ، دفع العلماء إلى محاولة تفسير السّلوك الجرمي للمجرم المعلوماتي، وذلك بعد معرفة الجرائم الّتي ترتكب في هذه البيئة أو بواسطتها. إذ يختلف سلوك المجرم المعلوماتي في إرتكاب إجرامه في الأنظمة المعلوماتية بإختلاف الجريمة، فمحل هذه الجريمة إمّا يكون الذّمة الماليّة للغير أو المساس بالحياة الخاصّة للأشخاص عبر الإنترنت، وفي هذه الحالة تكون تقنيّة المعلومات وسيلة لإرتكاب هذه الجرائم وليست محلًا لها. وإمّا تكون المعلومة في حدّ ذاتها هي محل الجريمة المعلوماتية، ويظهر ذلك بوضوح في جرائم التّعدي على أمن الدّولة المعلوماتي أو سرقة المال المعلوماتي، وجرائم الإتلاف والتّزوير المعلوماتي ممّا يؤدي إلى توقّف أو عرقلة عمل النّظام المعلوماتي.

لذلك سنتطرّق في نبذة أولى من هذا المطلب إلى دراسة السلوك الجرمي المرتكب بواسطة تقنيّة المعلومات، وفي نبذة ثانية سنعرض السلوك الجرمي الواقع على تكنولوجيا المعلومات. ذلك بهدف الإضاءة على السلوك الجرمي للمجرم المعلوماتي في البيئة المعلوماتية، والّتي تقع على الضّحيّة، مع ربط كل جريمة من الجرائم المعلوماتية المذكورة بقانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي اللّبناني رقم

81 تاريخ 2018/10/18.

النّبذة الأولى: السّلوك الجرمي المرتكب بواسطة تقنيّة المعلومات

يلعب الحاسوب وشبكة الإنترنت والإتّصال دورًا ثنائيًا في حقل الجريمة المعلوماتية ، فهما إمّا وسيلة متطوّرة لإرتكاب الجرائم التّقليديّة بفعاليّة وسرعة أكبر ، والّتي يُطلق عليها "الأعمال الجرمية الّتي ترتكب بمساعدة الحاسوب " [1]. وإمّا لإرتكاب جرائم على تكنولوجيا المعلومات بحدّ ذاتها.

في هذه النّبذة سنبحث في السّلوك الجرمي للمجرم المعلوماتي المرتكب بواسطة تقنيّة المعلومات، أيّ كوسيلة لإرتكاب الجريمة التّقليدية بطريقة أسرع وفاعليّة أكبر. لذلك سنتطرّق في هذه النّبذة الأولى أولا إلى دراسة السلوك الجرمي المعلوماتي الواقع على الأموال، ثانيًا إلى السلوك الجرمي الواقع على حرمة الحياة الخاصّة.

أولًا: السّلوك الجرمي المعلوماتي الواقع على الأموال

لقد رافق تطوّر الشّبكة المعلوماتية تطوّر في نظام المعاملات التّجارية والماليّة الّتي أصبحت تعتمد على الشّبكة المعلوماتية لنقل الأموال والقيام بعمليّات البيع والشّراء، ممّا أدّى إلى تطوّر في وسائل الدّفع والوفاء الّتي أصبحت جزءًا لا يتجزّأ من هذه المعاملات. ونتيجة هذا التّطوّر الّذي شهده القطاع المالي والإقتصادي والتّغيّر الّذي أحاط بالبيئة الّتي كانت تجري فيها هذه المعاملات، ظهرت بدورها وسائل جرميّة جديدة تحقّق جرائمها الواقعة على الأموال بإستعمال تقنيّة المعلومات كوسيلة لتحقيق مشروعها الجرمي.

ويتعدّد السّلوك الجرمي المرتكب بواسطة تقنيّة المعلومات، حيث أن عددًا قليلًا من الجرائم التّقليدية لا يمكن أن ينفّذ بواسطة هذه التّقنيّة أو على أقلّ تقدير يمكن أن يسهّل في إقترافها. ومن هذه الجرائم الإحتيال المعلوماتي، والجرائم الواقعة على بطاقات الدّفع الإلكتروني وغيرها.

[1] زينات طلعت شحادة، **الأعمال الجرمية الّتي تستهدف الانظمة المعلوماتية**، المنشورات الحقوقية صادر، سنة 2009، ص: 16.

1. الإحتيال المعلوماتي

يُعرّف الإحتيال المعلوماتي بأنّه التّلاعب العمدي بمعلومات وبيانات تمثّل قيمًا مادّية يختزنها نظام الحاسب الآليّ، أو الإدخال غير المصرّح به لمعلومات وبيانات صحيحة، أو أيّ وسيلة أخرى من شأنها التأثير على الحاسب الآليّ، حتّى يقوم بعمليّة بناء على هذه البيانات، أو الأوامر أو التّعليمات من أجل الحصول على ربح غير مشروع وإلحاق الضّرر بالغير [1].

تتعدّد وسائل الإحتيال المعلوماتي تبعًا للتّطوّر التّكنولوجي الّذي تشهده المعلوماتية. فمن جهة، يُعتبر التّلاعب في البيانات المدخلة إلى جهاز الحاسب الوسيلة الأولى للإحتيال المعلوماتي. أمّا الوسيلة الثّانية فتتمثّل في التّلاعب في البرامج المعلوماتية المطبّقة بالفعل داخل المؤسّسة المعتدى عليها إمّا بتعديل برامج تعمل عليها المؤسّسة أو بإصطناع برامج وهميّة.

موقف المشرّع اللّبناني

إن المشرّع اللّبناني كفل حماية قانونيّة للمجنيّ عليه في جرائم الإحتيال المعلوماتي، وذلك وفقًا للمادّة 112 من قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي حيث جاء في نصّ المادّة " يعاقب بالحبس من ستّة أشهر إلى ثلاث سنوات وبالغرامة من ثلاثة ملايين إلى مئتي مليون ليرة لبنانية أو بإحدى هاتين العقوبتين كلّ من أدخل بيانات رقميّة، بنيّة الغش، في نظام معلوماتي وكلّ من ألغى أو عدّل، بنيّة الغش، البيانات الرّقمية الّتي يتضمّنها نظام معلوماتي ".

2. الجرائم الواقعة على بطاقات الدّفع الإلكترونية

نظرًا للتطوّر الّذي أصاب القطاع المالي من النّاحية التّكنولوجية وظهور ما يعرف بالبطاقات الإئتمانية، أصبحنا أمام جرائم حديثة تقع على هذا النّوع من البطاقات الّتي يمكن أن تحوي العديد من العمليّات المالية فيها. والبطاقات الإئتمانية هي بطاقات تصدر عن المصارف إلى زبائنهم، تمنحهم بموجبها العديد من

[1] محمد طارق عبد الرؤوف الحق، **جريمة الإحتيال عبر الإنترنت، الأحكام الموضوعية والأحكام الإجرائية**، منشورات الحلبي الحقوقية، سنة 2011، ص: 39.

الحقوق والمزايا الماليّة الّتي تسهّل في عمليّة التّبادل والبيع والشّراء وغيرها.

وتتجلّى العمليّات الجرمية الّتي يمكن أن ترتكب على البطاقات الماليّة بعدّة وسائل، أوّلها تتمثّل في إساءة إستخدام بيانات بطاقة الإئتمان من قبل حاملها الشّرعي، إمّا إستعمالها دون وجود رصيد في المصرف معدّ للدفع مع علم العميل بذلك، وإمّا إستعمالها منه بعد إنتهاء مدّة صلاحيتها أو إلغائها [1]. بينما الوسيلة الثّانية فتتمثّل في العمليّات الجرمية الواقعة على البطاقة الإئتمانية من قبل الغير، إمّا عبر سرقة البطاقة أو في حالة فقدانها، وإمّا السّحب بإستخدام بطاقات مزوّرة من قبل الغير.

موقف المشرّع اللّبناني

إنّ المشرّع اللّبناني كفل حماية قانونية للمجنيّ عليه الّذي يتعرّض لجريمة واقعة على البطاقات المصرفية الإلكترونية، وذلك في المادّة 116 من قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي، حيث جاء في نصّ المادّة أنّه " يعاقب بالحبس من ستّة أشهر إلى ثلاث سنوات وبالغرامة من عشرة ملايين إلى مئتيّ مليون ليرة لبنانية أو بإحدى هاتين العقوبتين كل من:

- قلّد بطاقة مصرفية أو زوّرها
- إستعمل أو تداول، مع علمه بالأمر، بطاقة مصرفية مزوّرة أو مقلّدة
- قبل قبض مبالغ من النّقود مع علمه بأنّ الإيفاء تمّ بواسطة بطاقة مصرفية مزوّرة أو مقلّدة
- قلّد نقودًا إلكترونية أو رقمية
- إستعمل مع علمه بالأمر، نقودًا إلكترونية أو رقمية مقلّدة
- قلّد شيكًا إلكترونياً أو رقميًا
- إستعمل مع علمه بالأمر، شيكًا إلكترونيًا أو رقميًا".

ثانيًا: السّلوك الجرمي المعلوماتي الواقع على حرمة الحياة الخاصّة

لم تسلم الحياة الشّخصيّة للأفراد من كونها محلًا للإعتداء في الإجرام المعلوماتي، فقد يستخدم النّظام المعلوماتي في الإعتداء على حرمة الحياة الخاصّة. كما لو قام شخص يعمل بالنّظام المعلوماتي، بإعداد ملف يحتوي على معلومات تخصّ شخصًا آخر بدون علمه وبدون إذن منه. وتتعدّد السلوكيات الجرمية

[1] بن منصور صالح، طباش عز الدين، **السلوك الإجرامي للمجرم المعلوماتي**، المرجع السابق نفسه، ص: 48.

الماسّة بحرمة الحياة الخاصّة منها جرائم القدح والذّم، إنتحال شخصيّة الغير وإستدراجها.

1. القدح والذّم

تعتبر جرائم القدح والذّم من أكثر الجرائم إنتشارًا على شبكة الإنترنت، حيث يكون الذّم والقدح في الشّبكة المعلوماتية إمّا مباشرة عبر إتصال مباشر، وإما كتابيًا أو غيابيًا أو يكون بواسطة المطبوعات الإلكترونية. وكلّ ما تقدّم يتمّ بواسطة ما توفّره الشّبكة المعلوماتية من برامج وقنوات للتّواصل، إمّا عبر خدمة البريد الإلكتروني أو شبكة الويب العالمية وغرفة الدّردشة، وبعض التّطبيقات كتويتر وفايسبوك وغيرها، الّتي تمكّن الأشخاص من التّخاطب عن بعد عن طريق الكتابة [1]. ويتحقّق شرط العلنيّة الواجب لتحقّق هذه الجريمة في إمكانية إطّلاع العامّة على الكتابات أو الصّور أو الفيديوهات، الّتي تتضمن الذّم والقدح.

موقف المشرّع اللّبناني

عدّل قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي في المادّة 118 منه، نصّ المادّة 209 من قانون العقوبات على النّحو التالي: " الكتابة والرسوم والصور والأفلام والشّارات والتّصاوير على إختلافها إذا عرضت في محل عام أو مكان مباح للجمهور أو معرّض للأنظار أو بيعت أو عرضت للبيع أو وزّعت على شخص أو أكثر أيًا كانت الوسيلة المعتمدة لذلك بما فيها الوسائل الإلكترونية ». إذ يتبيّن من هذا التّعديل أنّ المشرّع قام بإضافة الوسيلة الإلكترونية من وسائل النّشر الّتي تحقق العلانية في جريمة الذّم والقدح، وبهذا تعتبر كلّ الكتابات والصّور والشّعارات والأفلام على إختلافها، معدّة لتحقيق العلانية إن تمت في وسيلة إلكترونية.

2. إنتحال الشّخصيّة والتّعدي على البيانات ذات طابع شخصيّ

تعتبر عمليّة إنتحال الشّخصيّة من الجرائم المعاقب عليها قانونيًا، فهي من الجرائم التّقليديّة الّتي يمكن أن تتمّ في الجرائم المعلوماتية. وتتّخذ جريمة إنتحال الشّخصيّة عبر الإنترنت شكليّن، الأوّل يتمثّل في

[1] بن منصور صالح، طباش عز الدين، **السلوك الإجرامي للمجرم المعلوماتي**، المرجع السابق نفسه، ص: 53.

إنتحال شخصيّة الفرد. أمّا الشّكل الثّاني فيقوم على إنتحال شخصيّة الموقع[1] .

موقف المشرّع اللّبناني

نصّت المادّة 106 من قانون المعاملات الإلكترونية على المعاقبة بالغرامة من مليون ليرة لبنانية إلى ثلاثين مليون ليرة لبنانية، وبالحبس من ثلاثة أشهر حتّى ثلاث سنوات أو بإحدى هاتين العقوبتين كلّ من أقدم:

1. على معالجة بيانات ذات طابع شخصي دون تقديم تصريح، أو دون الإستحصال على ترخيص مسبق قبل المباشرة بعمله.
2. على جمع أو معالجة بيانات ذات طابع شخصي دون التّقيّد بالقواعد المقرّرة.
3. ولو بالإهمال، على إفشاء معلومات ذاتع طابع شخصي موضوع معالجة لأشخاص غير مخوّلين الإطّلاع عليها.

3. إستغلال القاصرين في المواد الإباحية الإلكترونية

وتعتبر جريمة إستغلال القاصرين في المواد الإباحية من أكثر الجرائم المرتكبة في البيئة المعلوماتية. بحيث يُقصد منها تصوير أو إظهار أو تمثيل مادّي لأيّ قاصر، بأيّ وسيلة كانت، كالرّسوم أو الصّور أو الكتابات أو الأفلام أو الإشارات، يمارس ممارسة حقيقيّة أو مصطنعة بالمحاكاة أنشطة جنسيّة صريحة، أو تصوير للأعضاء الجنسيّة للقاصر.

موقف المشرّع اللّبناني

نصّ المشرّع اللّبناني في المادّة 120 من قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي على إلغاء النّبذة الثّالثة من الباب السّابع المُعَنوَن " في الجرائم المخلّة بالأخلاق والآداب العامة " من المرسوم الإشتراعي رقم 340 تاريخ 1943/3/1 قانون عقوبات، وإستبدالها بأحكام تُجرّم إستغلال القاصرين في المواد الإباحية. حيث إعتبر في المادّة 536 أنّ " إعداد أو إنتاج مواد إباحية يشارك فيها قاصرون بصورة فعليّة، وتتعلّق بإستغلال القاصرين في المواد الإباحية، يعتبر من قبيل الإتجار بالأشخاص، ويعاقب مرتكبها وفقًا لنصّ المادّة 586 وما يليها من قانون العقوبات والمتعلّقة بالإتجار بالأشخاص. وإذا لم يشارك

[1] بن منصور صالح، طباش عز الدين، **السلوك الإجرامي للمجرم المعلوماتي**، المرجع السابق نفسه، ص: 54.

القاصر بصورة فعليّة في المواد الإباحية المتعلّقة بإستغلال القاصرين، فيعاقب الفاعل بالحبس من سنة إلى ثلاث سنوات وبالغرامة من خمسة مئة ألف إلى مليوني ليرة لبنانية، ويعاقب بالحبس من سنة إلى ثلاث سنوات وبالغرامة من خمس مئة ألف إلى مليونيّ ليرة لبنانية من قدّم أو نقل أو نسخ أو عرض أو وضع بالتّصرف أو وزع أو صدّر أو إستورد أو نشر أو بثّ أو روّج بأيّ وسيلة كانت المواد الإباحية المتعلّقة بإستغلال القاصرين، وذلك إلى جمهور غير محدّد ".

النّبذة الثّانية: السّلوك الجرمي الواقع على تكنولوجيا المعلومات

بالإضافة إلى السّلوك الإجرامي للمجرم المعلوماتي الواقع بواسطة تقنيّة المعلومات، هناك نوع آخر لسلوك المجرم، وهو السلوك الجرمي الواقع على النّظام المعلوماتي بحدّ ذاته. تلك المتمثّلة في الأعمال الجرمية الّتي تستهدف إمّا المكوّنات غير المادّية للنظام المعلوماتي، أو المكوّنات المنطقيّة الموجودة داخل هذا النّظام أو الأعمال الواقعة على المعلومات داخل الأنظمة المعلوماتية [1].

لذلك سنبحث في النّبذة الثّانية من هذا المطلب أولًا في السّلوك الجرمي الواقع على المنتجات المعلوماتية غير المادّية، وثانيًا في السلوك الجرمي المستهدف للمعلومات داخل الأنظمة المعلوماتية.

أولًا: السّلوك الجرمي الواقع على المنتجات المعلوماتية غير المادّية

النّظام المعلوماتي وفق معناه الواسع بأنّه " كلّ وسيلة مخصّصة لصناعة المعلومات أو لمعالجتها أو لتخزينها أو لعرضها أو لتلفها يتطلّب تشغيلها الإستعانة بشكل أو بآخر بالوسائل الإلكترونية "[2].

1. جرائم التّعدي على نظم المعالجة الآليّة للبيانات

تعتبر جريمتي الدّخول والبقاء غير المصرّح بهما في النّظام المعلوماتي من أخطر الجرائم الّتي يمكن أن تستهدف النّظام المعلوماتي، والّتي يمكن أن تشكّل إعتداء على نُظم المعالجة الآليّة للبيانات.

---

[1] بن منصور صالح وطباش عز الدين، **السلوك الإجرامي للمجرم المعلوماتي**، المرجع السابق نفسه، ص: 61.

[2] طوني ميشال عيسى، **التنظيم القانوني لشبكة الإنترنت، دراسة مقارنة في ضوء القوانين الوضعية والإتفاقيات الدّوليّة**، صادر، الطبعة الأولى سنة 2001، ص: 178.

1.1 الدّخول غير المشروع لنظام المعلومات

يُقصد بالدّخول إلى نظام المعالجة الآليّة للمعطيات، الدّخول المعنويّ لمجرم المعلوماتية إلى العمليّات الذّهنيّة الّتي يقوم بها نظام المعالجة الآليّة للمعطيات، عبر توجيه هجمات إلى معلومات الحاسوب بقصد المساس بالسّرية، أو فعل الإختراق وهي عبارة عن عمليّة دخول غير مصرّح بها إلى أجهزة الغير وشبكاتهم الإلكترونية. ويتمّ ذلك من خلال إستخدام المجرم لبرامج متطوّرة يستخدمها كلّ من يملك خبرة في ذلك [1].

2.1 البقاء غير المصرّح به في النّظام المعلوماتي

إنّ هذه الجريمة ليست كسابقتها، حيث أنّ الجاني في جريمة الدّخول غير المشروع للنظام المعلوماتي يسعى بنفسه إلى تحقيق الإتصال ممّا يتطلّب منه فعلًا إيجابيًا. أمّا جريمة البقاء غير المصرّح به في النّظام المعلوماتي فإنها تتطلّب الخروج من البرنامج وعدم البقاء فيه وتتحقّق في الحالات الّتي يكون فيها الإتصال عن طريق الخطأ، لذلك على الجاني الإتيان بفعل إيجابي وهو قطع الإتصال والخروج من النّظام. ويتمثّل السّلوك الإجرامي في هذه الجريمة بفعل البقاء، ويقصد به التّواجد داخل نظام المعالجة الآليّة للمعطيات دون إرادة صاحب الموقع أو النّظام [2].

2. جرم الإعتداء العمدي على نظام المعالجة الآليّة

تتعلّق هذه الجريمة بتجريم كلّ فعل من شأنه أن يؤدّي إلى عرقلة عمل نظام المعالجة الآليّة أو عدم أدائه لوظائفه الطّبيعية[3]، إذ إنّ المصلحة القانونية المحميّة هي مصلحة مشغلي ومستخدمي نظم الحاسب في إستمرار عمل تلك الأنظمة بشكل سليم.

3. جرائم التّعدي على برامج الحاسب الآلي

إكتسبت البرمجيات في عصرنا الحالي والثّورة التّقنيّة في مختلف مجالات الفكر البشري أهمية كبرى،

---

[1] د. حسين محمد الغول، **جرائم شبكة الإنترنت والمسؤوليّة الجزائية الناشئة عنها، دراسة مقارنة**، مكتبة بدران الحقوقية، سنة2008، ص: 55.

[2] نائلة عادل محمد فريد قورة، **جرائم الحاسب الآلي الاقتصادية**، المرجع السابق نفسه، ص: 37.

[3] زينات طلعت شحادة، **الأعمال الجرمية الّتي تستهدف الانظمة المعلوماتية**، المرجع السابق نفسه، ص: 61.

قابلها تعديّات جمّة. حيث أصبحت هذه البرامج عرضة لأن يقع عليها جرائم مختلفة، فتُعرّف برامج هذه الحاسب الآليّ على أنّها المكوّنات غير المادّية للأنظمة المعلوماتية بحيث تعتبر جريمة التقليد أبرز الجرائم[1].

موقف المشرّع اللّبناني من هذه الجرائم

عاقب المشرّع اللّبناني في المادّة 110 من قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي على الولوج غير المشروع إلى نظام معلوماتي. حيث عاقب بالحبس من ثلاثة أشهر إلى سنتين، وبالغرامة من مليون إلى عشرين مليون ليرة لبنانية أو بإحدى هاتين العقوبتين، كلّ من أقدم بنيّة الغش على الوصول أو الولوج إلى نظام معلوماتي بكامله أو في جزء منه أو على المكوث فيه.

كما شدّد المشرّع اللّبناني في المادّة نفسها العقوبة من ستّة أشهر إلى ثلاث سنوات، والغرامة من مليونين إلى أربعين مليون ليرة إذا نتج عن العمل إلغاء البيانات الرّقميّة أو البرامج المعلوماتية أو نسخها أو تعديلها أو المساس بعمل النّظام المعلوماتي. بالإضافة إلى ذلك، نصّ المشرّع في المادّة 113 من القانون نفسه على أنّه " كلّ من أعاق أو شوّش أو عطّل قصدًا وبأيّ وسيلة عن طريق الشّبكة المعلوماتية أو أحد أجهزة الحاسب الآليّ وما في حكمها، الوصول إلى الخدمة أو الدّخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات يعاقب بالحبس من ثلاثة أشهر إلى سنتين وبالغرامة من مليونين إلى ثلاثين مليون ليرة لبنانية أو بإحدى هاتين العقوبتين "[2].

ثانيًا: السّلوك الجرمي المستهدف للمعلومات داخل الأنظمة المعلوماتية

تتعدّد الأعمال الجرمية الّتي تستهدف المعلومات داخل الأنظمة المعلوماتية، حيث أطلق الفقه وبحق على المعلومات إسم البترول الرّمادي، وقد شيّدت على أساسها صناعة حقيقيّة ومتطوّرة حتّى باتت إحدى أهمّ المصالح المستهدفة. هذه الأهمّية للمعلومات جعلتها فريسة سهلة للقراصنة وعرّضتها للعديد من المخاطر والإعتداءات منها سرقة المال المعلوماتي، الإتلاف المعلوماتي، وأخيرًا التّزوير المعلوماتي.

[1] زينات طلعت شحادة، **الأعمال الجرمية الّتي تستهدف الانظمة المعلوماتية**، المرجع السابق نفسه، ص: 77- 88.

1. سرقة المال المعلوماتي

ينقسم المال المعلوماتي إلى قسمين، الأوّل هو مال طبيعي أيّ مكوّنات العناصر المادّية للنظام المعلوماتي، والّتي تحتوي على المعلومات الّتي لها كيان مادّي ملموس المتمثّلة في وحدات العرض والتّسجيل والشّاشة والملحقات الّتي تُمكّن من إدخال وإخراج المعلومة. أمّا الثّانية فتتمثّل في جانب آخر لا مادّي، وهو ما يطلق عليه المال المعلوماتي المنطقي أو المعنوي الّذي سنتكلم عنه تباعًا. فالمعلومة لها قيمة ماليّة معيّنة يمكن أن تخضع للسرقة بإعتبار أنّ المعلومة هي عبارة عن نتاج ذهني وإبتكار، ممّا يترتب على ذلك وجود علاقة تبني بين المعلومة ومؤلّفها، وتشبه العلاقة الّتي تنشأ بين المالك والشّيء الّذي يملكه. فالمعلوماتية هي من قبيّل الأموال الّتي لها قيمة إقتصادية نظرًا إلى قيمتها ونفعتها [1].

موقف المشرّع اللّبناني

ما يُعاب به على المشرّع اللّبناني أنّه لم يتضمّن نصًا صريحًا في قانون المعاملات الإلكترونية، يجرّم فعل سرقة المال المعلوماتي المعنوي، وعليه يجب العودة إلى قواعد قانون العقوبات الّتي تحكّم فعل السّرقة. فوفقًا لنصّ المادّة 635 من قانون العقوبات اللّبناني السّرقة هي " أخذ مال الغير المنقول خفية أو عنّوة بقصد التّملك "، وكما ذكرنا أنّ البرامج والنّظم المعلوماتية تعتبر بمثابة مال معنوي له قيمة مادّية معيّنة لذلك يمكن تطبيق الأحكام العامّة لجريمة السّرقة على سرقة المال المعلوماتي.

2. جريمة الإتلاف المعلوماتي

تتعدّد أساليب إرتكاب هذه الجريمة حيث تبدأ بالفيروس، مرورًا بالدّودة، وإنتهاءً بالقنابل المعلوماتية. فالفيروس هو عبارة عن برنامج معلوماتي أعطي تسميّة الجرثومة بسبب وجود أوجه شبه كثيرة مع الجراثيم الّتي تهاجم الجسم البشري، ذلك أنّه ينتقل من جهاز إلى آخر [2].

---

[1] بن منصور صالح وطباش عز الدين، **السلوك الإجرامي للمجرم المعلوماتي**، المرجع السابق نفسه، ص: 62.

[2] د. نائلة عادل محمد فريد قورة، **جرائم الحاسب الآليّ الإقتصادية (دراسة نظرية وتطبيقية)**، منشورات الحلبي الحقوقية، سنة 2005، ص: 117.

فالجرثومة عبارة عن برنامج ضارّ يضاف إلى برامج الحاسوب ويقوم بمسح المعلومات الموجودة في الذّاكرة، أو يدمّر فهرس الملفات بحيث لا يستطيع الحاسوب الإستدلال عليها مرة أخرى. كما بإمكانه أن يدخل إلى البيانات الموجودة في الملفات المخزّنة في الحاسوب، أو يجتزّئ بعضها ليضيفها في ملفات أخرى. وبهذا فهو يقوم بعمليّة خلط كاملة تفقد البيانات والمعلومات قيمتها ويؤدي إلى تدميرها [1]. بينما الدّودة المعلوماتية هي عبارة عن برامج تستغل أيّة فجوات في نظم التّشغيل كي تنتقل من حاسوب إلى آخر، وتتميّز بقدرتها الهائلة على الإنتشار والتّكاثر عن طريق توليد نفسها، وبالتّالي فهي برامج تعطي نسخًا عن فحواها [2]. أمّا القنابل المعلوماتية فتنقسم إلى قسمين، القنابل المنطقيّة الّتي تؤدي إلى تدمير المعلومات عند حدوث ظرف معيّن أو لدى تغيّير أمر ما، والقنابل الزمنيّة الّتي تعمل في ساعة محدّدة من يوم معيّن وفي لحظة زمنيّة محددة بالسّاعة واليوم والسّنة.

موقف المشرّع اللّبناني

نصّ المشرّع اللّبناني في المادّة 111 من قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي، على الحبس من ستّة أشهر إلى ثلاث سنوات وبالغرامة من ثلاثة ملايين إلى مئتي مليون ليرة لبنانية أو بإحدى هاتين العقوبتين، كلّ من أقدم بنيّة الغش وبأي وسيلة على إعاقة عمل نظام معلوماتي أو على إفساده. حيث ينطبق هذا النصّ على الأفعال الجرمية السّابق ذكرها والّتي تؤدي إلى إتلاف المعلومات داخل النّظام.

3. التّزوير المعلوماتي

يتجاوز التّزوير الإلكتروني التّزوير الورقي، وإن كان هو نفسه في المفهوم الوظيفي لناحية تحريف الحقائق أو البيانات، حيث سيتطلّب التّعامل مع تقنيات المعلوماتية ممّا يصعب من إمكانيّة كشفه. فهو يضمّ الإدخال، المحو، والتّغيير لبيانات معلوماتية أو مخزّنة في الحاسوب، ممّا يولد بيانات غير صحيحة ويكون

[1] إنتصار نوري الغريب، **فيروسات الحاسوب**، دار الراتب الجامعية، بيروت 1994، ص: 27.

[2] زينات طلعت شحادة، **الأعمال الجرمية الّتي تستهدف الانظمة المعلوماتية**، المرجع السابق نفسه، ص: 127.

الهدف من ذلك إستعمال هذه البيانات لأغراض قانونية كما لو كانت صحيحة.

موقف المشرّع اللّبناني

نصّ المشرّع اللّبناني على عقوبة جريمة التّزوير الإلكتروني في المادّة 119 من قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي، حيث عدّل نصّ المادّة 453 من قانون العقوبات على النّحو الآتي" التّزوير هو تحريف متعمّد للحقيقة، في الوقائع أو البيانات الّتي يثبتها صك أو مخطوط أو دعامة ورقية أو إلكترونية أو أيّة دعامة أخرى للتعبير تشكّل مستندًا، بدافع إحداث ضرر ماديّ أو معنوي أو إجتماعي".

لا شكّ أنّ تحديد السّلوكيات الجرمية للمجرم المعلوماتي يساعد في فهم هذا المجرم، لكن بالإضافة إلى ذلك فإنّ هذا التّحديد للأعمال الجرمية المرتكبة بواسطته في البيئة المعلوماتية له دور أساسي للإستعانة به في دراسات علم الإجرام لتصنييف للمجرمين المعلوماتيين وذلك على ما سنعرضه في الفصل الثّاني من هذا الباب. هذا الأمر الّذي يمكن أن يؤدي لفهم أفضل للأسباب والدّوافع الّتي تؤدي بالمجرم لإرتكاب أفعاله الجرمية، ويمكن أن يشير السّلوك الجرمي إلى طبيعة الأشخاص المرتكبين له ونوعهم ودرجة إلمامهم بالتّقنيّة المعلوماتية الّتي تعتبر السّاحة الجرمية لإرتكاب الإجرام المعلوماتي.

الفصل الثّاني

تصنيف علم الإجرام للمجرميين المعلوماتيين

يتّفق علماء الإجرام على أنّ المهمة الرئيسية لعلم الإجرام هي تفسير الظاهرة الإجرامية بإستخلاص الدّوافع أو الأسباب الّتي تؤدّي إليها، وذلك بهدف الوصول إلى حلول أو معالجة لها. فالسلوك الإجرامي للمجرمين المعلوماتيين لا بُدّ من أن يكون هناك محرّك له، أيّ دافع يكون السّبب لإقتراف العمل الجرمي. ومع ذلك فإنّ علماء الإجرام يختلفون بعض الشيء في تحديد مدلول الدّافع في هذا العلم، فالبعض يأخذ بفكرة الدّافع الأوحد فيفسر الجريمة على أنّها ثمرة دافع واحد ينبغي توافره في حالات الإجرام كافة، مثال ذلك ما ذهب إليه " فرويد" من أنّ جميع الجرائم يمكن تفسيرها على نحو ما بأنّها نتيجة لنوع معيّن من التكوين الجسدي أو النفسي للمجرم. غير أنّ الفكرة السائدة لدى علماء الإجرام هي فكرة تعدّد الدّوافع الإجرامية، ومؤدي هذه النظرية أنّه لا يمكن الإعتماد على دافع معيّن بأهمّيته في حالات الإجرام كافة [1].

هذا الدّافع الجرمي يتأثر بشكل أو بآخر بنوّعية الشّخص المرتكب للعمل الجرمي، خصوصًا درجة إلمامه بالتّقنيّة المعلوماتية في كونه محترف من عدمه، موقعه الإجتماعي والعمل الذي يمارسه. فمثلًا فإنّ الشّخص الّذي يعمل في مجال الإقتصاد سيكون الدّافع لإرتكابه الإجرام المعلوماتي ماليًا، على عكس الشّخص الّذي يعاني مثلًا من الكبت الجنسيّ حيث سيكون الدّافع لإرتكاب الإجرام عاطفيًا.

وبناءً على ما تقدّم سنقوم في الفصل الثّاني من الباب الأوّل بالتعرّف على الدّوافع المختلفة لإرتكاب الإجرام المعلوماتي الّذي ينقسم إلى دوافع داخلية وأخرى خارجية، أيّ وبعنى آخر الدّوافع المحفّزة لإرتكاب الإجرام المعلوماتي وذلك في مطلب أوّل. أمّا في المطلب الثّاني فسنبحث في درجة إلمام المجرمين المعلوماتيين بالتّقنيّة المعلوماتية حيث سنتطرّق إلى طبيعتهم ونوعية كلّ منهم وعلاقتهم بالتّقنيّة المعلوماتية.

---

[1] د. سمير عالية، **مبادئ علم الإجرام والعقاب والسياسة الجزائية، أسباب الإجرام ومكافحته جزائيًا**، منشورات الحلبي الحقوقية، 2019، ص: 65-66.

المطلب الأوّل: الدّوافع المحفّزة لإرتكاب الإجرام المعلوماتي

الدافع هو قوّة نفسيّة تدفع الإرادة إلى الإتجاه نحو إرتكاب الجريمة إبتغاء تحقيق غاية معيّنة، وهو يختلف من جريمة إلى أخرى تبعًا لإختلاف النّاس من حيث السنّ والجنس ودرجة التعلّم[1].

بالنّسبة إلى الإجرام المعلوماتي فإنّ الدّوافع المحفّزة لإرتكابه يُمكن تقسيمها إلى فئتين رئيسيتين، تضمّ أولهما: الدّوافع الدّاخلية، أيّ تلك الّتي تتّصل بشخصيّة المجرم المعلوماتي، وتتمثّل في صفات أو خصائص عضوية أو نفسية معيّنة. وتضمّ ثانيهما: العوامل الخارجية، وهي تلك الّتي تعودإلى البيئة المحيطة بالمجرم المعلوماتي والّتي تؤثر بصفة مستمرة على شخصيّته وتتيح له فرصًا عديدة للإجرام [2]. وبناءً على ما تقدم سوف يُقسّم هذا المطلب إلى نبذتين، تخصصّ أولهما لبحث الدّوافع الدّاخلية للسلوك الإجرامي، أما ثانيهما فتخصصّ لدراسة الدّوافع الخارجية منها. بالإضافة إلى البحث في كلا النبذتين عن الدّوافع الّتي تنفرد بها المنشأة عن الشّخص الطبيعي في الإجرام المعلوماتي.

النّبذة الأولى: الدّوافع الدّاخلية للسلوك الإجرامي

أصبح العالم اليوم بوجود الجرائم الحديثة ومنها الإجرام المعلوماتي، أمام نمط جديد من المجرمين الّذين لا يلوّثون أيديهم بالدّماء إلاّ كخيار نادر، إنّما يواجهون المجتمع بياقاتهم البيضاء وأيديهم النّاعمة، وحديثهم اللّبق كأنّهم رمز للرجال الشّرفاء، ولكن في الواقع جرائم هؤلاء أخطر وأخبث وأنمق من المجرمين العاديين[3].

بالرّغم من إختلاف العصر الحديث وأهمّها جرائم المعلوماتية عن الجرائم التقليدية، إلّا أنّ الدّوافع

---

[1] بن منصور صالح، طباش عز الدين، **السلوك الإجرامي للمجرم المعلوماتي**، المرجع السابق نفسه، ص: 29.

[2] د. سمير عاليه، **مبادئ علوم الإجرام والعقاب والسياسة الجزائيّة (أسباب الإجرام ومكافحته جزائيًا)**، المرجع السابق نفسه، ص: 66.

[3] د. جنان الخوري، **الجرائم الإقتصادية الدولية والجرائم المنظمة العابرة للحدود**، المرجع السابق نفسه، ص: 140.

الدّاخلية المحرّكة للسلوك الجرمي تتشابه فيما بين الجريمتين، مع وجود إختلاف بسيط تنفرد به الجرائم الحديثة وخصوصًا فيما يتعلق بالإجرام المعلوماتي. فتنقسم العوامل الدّاخلية الفردية إلى عوامل أصليّة، وأخرى عارضة أو مكتسبة[1]. فالعوامل الأصليّة هي عبارة عن الصّفات أو الخصائص الّتي تتوافر في الشّخص منذ ولادته ويدخل فيها التّكوين الشّخصي للمجرم، الوراثة، السّلالة، النّوع، الضعف والخلل العقلي، والأمراض العصبية والنّفسية. أمّا العوامل المكتسبة أو العارضة فهي الخصائص الّتي يكتسبها الإنسان بعد ولادته، سواء بإرادته أم رغمًا عنه. مثال على ذلك التّغيير الّذي يطرأ على شخصيته كلّما تقدّم به العمر، والحالة المدنية للمجرم من حيث كونه متزوجًا أو مطلقًا أو عازبًا وغيرها من الأمور.

لكن في الإجرام المعلوماتي تنحصر هذه العوامل الأصليّة والمكتسبة في دافعين، فتعتبر الدّوافع الدّاخلية المحفّزة لإرتكاب الإجرام المعلوماتي إمّا دوافع نفسية كقهر النّظام والشّعور بالسّيطرة عليه أو إثبات الذّات، أو بقصد التعلّم وذلك بإكتشاف كلّ ما هو جديد في التقنية المعلوماتية وكيفية التّغلب والسّيطرة عليها.

1. الدّوافع النّفسيّة

للدّوافع النّفسيّة أثر بالغ في الإجرام المعلوماتي، ويلعب عنصرا التّكوين الذّهنيّ وإثبات الذّكاء، الدّور البارز من هذه النّاحية. فالصّورة الذّهنية لمرتكبي جرائم الحاسوب والإنترنت، غالبًا هي صورة البطل والذّكي الّذي يستحق الإعجاب، لا صورة المجرم الّذي يستوجب محاكمته. فغالبًا ما يكون الدّافع لدى مرتكبي جرائم المعلومات هو الرّغبة في إثبات الذّات وتحقيق إنتصار على تقنيّة المعلومات دون أن يكون لهم دوافع

[1] د. سمير عالية، **مبادئ علم الإجرام والعقاب والسياسة الجزائية، أسباب الإجرام ومكافحته جزائيًا**، منشورات الحلبي الحقوقية، 2019، ص: 68.

آثمة[1]. فيعتمد المجرم المعلوماتي على تكوينه الذّهني الّذي يوظّفه لتنفيذ مآربه، وهو يتمتّع بعقل سليم وكامل ونوعًا ما بتفوّق في الذّكاء، ويحاول من خلال جريمة المعلوماتية أن يُثبت العظمة على التّقنيّة وعلى المجتمع الّذي يستهلك هذه التّقنيّة. فأصبحت هذه الجريمة تعزى إلى جنون العظمة، الّتي تحتاج إلى التّخطيط، التّحضير، الحكمة، التّدبّر، الرّؤية والتّعقّل لتنفيذها.

2. دافع التعلّم

عادةً يرتبط هذا الدّافع بدافع إثبات الذّات وذكاء الشّخص والتّغلّب غلى التّقنيّة، إذ يكون إرتكاب الإجرام المعلوماتي بغيّة الحصول على الجديد من المعلومات وكشف خفايا هذه التّقنيّة المتسارعة في النّمو والتّطوّر.

ويمكن أن يقوم هؤلاء الأشخاص بالبحث وإكتشاف الأنظمة والعمل من خلال الجماعة وتعليم بعضهم البعض، حتّى أنّه يكرّس البعض منهم كامل وقته في تعلّم كيفيّة إختراق المواقع الممنوعة [2]. ويدخل في هذا المجال المجرم المعلوماتي عن طريق الصّدفة والفضول، حيث أنّ الدّوافع إلى الجريمة هي عوامل داخلية دفعته لإكتشاف كل ما هو جديد.

النّبذة الثّانية: الدّوافع الخارجية للسلوك الإجرامي

إذا كانت الدّوافع الدّاخلية تحرّك السّلوك الجرمي المعلوماتي بحسب كل شخص وتحدّد الغاية من الجريمة، فإنّ الدّوافع الخارجية تتسم بالطّابع الأكثر خطورة كونها تسيطر على مقومات المجرم وذكائه في هذا المجال وتجعله هشًا، يسهل إستغلاله أو وقوعه فيها.

ويقصد بالعوامل الخارجية مجموع الظروف أو الوقائع الّتي لا تتعلق بشخص المجرم، إنما ترجع إلى

[1] بن منصور صالح، طباش عز الدين، **السلوك الإجرامي للمجرم المعلوماتي**، المرجع السابق نفسه، ص: 31.

[2] بن منصور صالح، طباش عز الدين، **السلوك الإجرامي للمجرم المعلوماتي**، المرجع السابق نفسه، ص: 32.

البيئة التي يعيش فيها، ويكون من شأنها التأثير على سلوكه وتوجيهه لإرتكاب الجريمة، فالدوافع الخارجية لا يكون منشأها شخصي أو داخلي بل يكون منشأها خارجي ولكنها تؤثر على سلوك المجرم وتدفعه الى إرتكاب إجرامه. وتعتبر من أبرز الدّوافع الخارجية لإرتكاب المجرم المعلوماتي لإجرامه، هي دافع الإنتقام، دافع التهديد، دوافع عاطفية، دوافع سياسية، ودوافع إقتصادية.

1. دافع الإنتقام

يشكّل دافع الإنتقام أخطر الدّوافع لإرتكاب الإجرام المعلوماتي، حيث يكون التّكوين النّفسي والجسدي والعقلي متّجه إلى الإضرار بالغير وتحقيق عمليّة إنتقاميّة تجاه أشخاص أو مؤسّسات أو حتّى حكومات. خاصة وأنّ الإنتقام عادة ما يأتي من شخص إمّا يملك معلومات عن الضّحيّة تمكّنه من القيام بجريمته، وإمّا من شخص كان في الأصل جزءًا من الشّركة أو المؤسّسة أو الحكومة الّتي سوف تتّجه نحوها الجريمة[1]. وغالبًا ما يتم إرتكاب الإجرام المعلوماتي بدافع الإنتقام من قبل الموظّفين أو المستخدمين تجاه ربّ العمل لأسباب إنتقامية تتعلّق بالوظيفة أو في معرضها.

2. دافع التّهديد

إنّ دافع التّهديد يتمثّل في أن يُمارَس إكراه معيّن تجاه المجرم، حيث يقوم تحت الضّغط بإرتكاب جريمة في البيئة المعلوماتية [2]. وعادةً ما يتم إختيار المجرم من الموظّفين أو المستخدمين أو الأشخاص الّذين يتمتّعون بسمعة جيّدة في مجال العمل، وذلك لتسهيل هذه العمليّة وضرب ركائز المؤسّسة أو الشّركة الّتي يعمل فيها هذا الشّخص.

[1] د. سمير عالية، **مبادئ علم الإجرام والعقاب والسياسة الجزائية**، المرجع السابق نفسه، ص: 163.

[2] بن منصور صالح، طباش عز الدين، **السلوك الإجرامي للمجرم المعلوماتي**، المرجع السابق نفسه، ص: 33.

3. دوافع عاطفية

لقد ميّز علماء الإجرام بين أنواع المجرمين، وتحدثوا عن المجرم العاطفي الّذي تتكوّن الدّوافع لديه من المشاعر العاطفية، والّتي تنسحب تداعياتها السّلبية عادة إلى تكوين جريمة معيّنة. ويظهر هذا الدّافع كثيرًا في الإجرام المعلوماتي حيث يُعتبر عامل الإبتزاز الإلكتروني والدّخول إلى بيانات الآخرين بطريقة غير مشروعة، وسرقة بعض البيانات الشخصيّة والتّشهير فيها جرم أساس تكوينه المجرم العاطفي. فضلًا عن تميّز المجرم العاطفي بإزدياد درجة حساسيّته وحدّة تأثره بالإنفعالات والعواطف، ممّا يجعله يستجيب لها بشكل مبالغ فيه. بالتالي يعود سلوكه الاجرامي إلى أسباب عاطفية كالحماس، الغيرة والدّفاع عن الشّرف، وأغلب جرائمه تكون إعتداءً على الأشخاص أو جرائم سياسيّة.

4. دوافع سياسية

إنّ الجريمة الّتي ترتكب لدوافع سياسيّة تتمّ غالبًا في المواقع السّياسية المعادية للحكومة، أو حتّى ترتكب من قبل أحزاب أو أشخاص يتعارضون فيما بينهم. ويتمثّل في تلفيق الأخبار والمعلومات ولو زورًا، أو حتّى الإستناد إلى جزء بسيط جدًا من الحقيقة، ومن ثم نسخ الأخبار الملفّقة حولها. فتعدّ الدّوافع السّياسية من أبرز المحاولات الدّوليّة لإختراق شبكات حكومية في مختلف دول العالم.

5. دوافع إقتصادية

من أهمّ الدّوافع الإقتصادية الّتي تدفع لإرتكاب الإجرام المعلوماتي هي التّقلبات الاقتصادية، الفقر والبطالة[1]. تعتبر التّقلبات الإقتصادية عدم ثبات الوضع الإقتصادي وسرعة تبدّله كإرتفاع وإنخفاض الأسعار، وتقلّب قيمة النّقد والمداخيل الفردية حيث تؤثّر هذه التّقلبات بطريقة غير مباشرة على سلوك

[1] د. سمير عالية، **مبادئ علم الإجرام والعقاب والسياسة الجزائية**، المرجع السابق نفسه، ص: 165.

الإنسان وأسلوب معيشته.

بالإضافة إلى ذلك يعتبر الفقر بمعناه الشّامل دافع لإرتكاب الجريمة المعلوماتية، فالفقر هو تلك الحالة المادّية الّتي لا تمكّن الشّخص من تلبية الحدّ الأدنى لمتطلبات الحياة، إمّا لعدم كفاية دخله بصورة كافية وإمّا لعدم وجود دخل له على الإطلاق. ولا يشكّل الفقر في حدّ ذاته عاملًا مباشرًا لإرتكاب الجرائم لكّنه يساعد على ذلك، فالشّخص الّذي لا يستطيع أن يحقق الحدّ الأدنى من مطالب الحياة قد لا يجد أمامه وسيلة لإشباع حاجته إلّا الجريمة فيسلك طريقها.

أمّا أكثر العوامل الإقتصادية تأثيرًا على الجريمة وخصوصًا الإجرام المعلوماتي هي مشكلة البطالة، الّتي يقصد بها توقف الإنسان عن العمل سواء كان ذلك نتيجة مرض بدني أو عقلي أو نفسي، أم كانت نتيجة لتعسر الأعمال وإزدياد المنافسة بين العمال، أم لإنهيار مشروع تجاري أو صناعي كان يعمل فيه الشّخص. وفي الإجرام المعلوماتي تعتبر بطالة الأشخاص الّذين كانوا يتولّون وظيفة تقنيّة في المجال المعلوماتي أكثرهم عرضة لإرتكاب هذا النوع من الجرائم، وعادة ما تكون الجريمة مزدوجة الهدف الأوّل للإنتقام والثّاني لتحقيق مردود مادّي. فالبطالة تهيّئ للإنسان فرصة للإنحراف، سواء لناحية الفراغ الّذي ينشأ عنها وإستغلاله في طريقة سيئة، أم لناحية حرمان الإنسان من وسيلة مشروعة لتحقق رغباته. فالمهنة تعتبر مصدر أمان وإستقرار للإنسان وتتيح له القيام بدوره في المجتمع.

خلاصة القول أنّ كُلًا من الفقر والبطالة يمارس أثرًا واضحًا في تحقيق ظاهرة الإجرام المعلوماتي. إذًا تتعدد الدّوافع والعوامل الّتي تؤدّي بالمجرم المعلوماتي إلى إرتكاب جريمته، فيمكن أن يكون هناك دافع واحد ساهم في ذلك، ويمكن أن يكون هناك تظافر لعديد من العوامل والدّوافع الّتي ساهمت في إرتكاب الجريمة. ويبقى الدّافع مختلف بين مجرم وآخر وبين غاية جرمية وأخرى، لذلك لا بُدّ من تحديد الدّافع الجرمي لكلّ مجرم يرتكب الإجرام المعلوماتي بشكل خاص لمعرفة الآليّة الّتي يجب من خلالها معالجة الجريمة والحدّ من الخطورة الجرمية الكامنة فيه.

إذًا كما بيّنا أنّ السّلوك الإجرامي للمجرم المعلوماتي مبنيّ وبشكل أساسي على الدّافع المحرّك لهذا السّلوك، سواء كان داخليًّا أم خارجيًّا. هذا ما يمكّننا من تحديد أسباب الجرائم لوضع الحلول لها، ويقتضي في هذا المجال الإشارة إلى الدّوافع الخاصّة بالمنشأة والّتي تتجلّى في عنصر الثّقة والأمانة الّتي تمنحهم لأحد الموظفين [1]. ليقوم هذا الأخير بإستغلال هذه الثّقة والصّلاحيات المعطاة له لإرتكاب جرائمه، ويكون الدّافع في هذه الجريمة سهولة حصولها وضمان نجاحها.

وبعد عرضنا للدوافع الّتي تساهم بشكل خاص في إرتكاب الإجرام المعلوماتي، لا بُدّ من التعرّف على طبيعة الأشخاص القائمين بهذا السّلوك الإجرامي ومدى إلمامهم بالتّقنيّة المعلوماتية وذلك في المطلب الثّاني من هذا الفصل.

المطلب الثّاني: درجة إلمام المجرمين المعلوماتيين بالتّقنيّة المعلوماتية

تشير أبحاث علم الإجرام إلى أنّه من النّاحية العملية، كلّ تقنيّة مستحدثة ينشأ عنها بالضّرورة وفي أيّ مرحلة من مراحل تطوّرها ظاهرة إجرامية خاصّة بها، وينطبق ذلك وبشكل خاص على تقنيّة المعلومات نظرًا للإمكانيات الّتي يقدمها الحاسب الآليّ والإنترنت، وهذا ما أدى إلى وجود محاولات كثيرة لوضع تصنيف لمرتكبي جرائم المعلومات. وتُعد من أهمّها دراسة الأستاذ " ويليام فونستارش" الّذي ذهب إلى تصنيف مجرمي التّقنيّة الحديثة إلى ثلاثة أصناف مختلفة المخترقون، المحترفون، والحاقدون[2].

وفي إطار هذه الدّراسة سوف نقسّم تصنيف المجرمين المعلوماتيين حسب درجة إلمامهم بالتّقنيّة

[1] د. منى الأشقر، د. محمود عارف جبور، القانون والإنترنت (تحدي التكيف والضبط)، المنشورات الحقوقية صادر، 2008، ص: 70.

[2] حمزة بن عفون، **السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية**، جامعة الحاج لخضر، سنة 2012، ص: 34.

المعلوماتية إلى فئتين، الفئة الأولى هم المجرمون غير المحترفون كالمجرم الهاوي أو المبتدئ، صغار المجرمين والهاكرز وذلك في نبذة أولى. أمّا الفئة الثّانية فهم المجرمون المحترفون منهم المخربون، المتمرسون والمتجسسون وذلك سنبيّنه في النّبذة الثّانية.

النّبذة الأولى: المجرمون غير المحترفون

إنّ المجرم الهاوي أو المبتدئ، هو المجرم الأقلّ خطورة من بين المجرمين الآخرين. أمّا بالنّسبة إلى صغار المجرمين أو المجرم الحدث، فتختلف درجة خطورته بدرجة الخطورة الإجرامية الّتي يستطيع أنّ يصل إليها، أو بدرجة ذكائه وفهمه للجريمة ومدى خبرته في هذا المجال وتمكّنه من الوسيلة.

1. صغار المجرمين

لم يعد يقتصر إجرام الأحداث على الحدث المنحرف، المتسوّل، المشرّد، فقير الحال، مهمل الوالدين ووليد الشّوارع والأزقة، بل غدونا أمام " صغار المجرمين " أو "جرائم الصّغار "، وليد العائلة الثّرية يرتكب جرائمه من داخل غرفته المجهزة بأحدث التّقنيّات [1]. فهم فئة من صغار السنّ مولعون بالثّورة المعلوماتية عن طريق إستخدام الحاسبات الآليّة الخاصّة بهم أو بمدارسهم، حيث يمارسون مواهبهم في إستخدام الحاسب الآليّ بغرض اللّهو أو هواية اللّعب أو إثبات الذّات من أجل الوصول إلى نظم معلوماتية خاصّة. وعادة ما يتم إستغلال هؤلاء من قبل كبار المجرمين وذلك من خلال توجيههم لإرتكاب جرائم معلوماتية لمصلحة الغير، مقابل نفع ماديّ أو معنويّ أو عن طريق التّهديد.

ولا شيء يمنع من تحوّل المجرم الصّغير من مجرد هاوٍ صغيرٍ للأفعال غير المشروعة إلى محترف

[1] د. جنان الخوري، **الجرائم الإقتصادية الدولية والجرائم المنظمة العابرة للحدود**، المرجع السابق نفسه، ص: 148.

بها. مثال على ذلك، الفتى الكندي (15 عامًا) الّذي تمكّن من إختراق عدد من الحواسيب وسيطر عليها وإستخدمها في شنّ هجمات متفرّقة في شباط فبراير 2000 ضد شركتي "أمازون" Amazon و "ياهو" Yahoo ومواقع أخرى بارزة في مجال التّجارة[1].

2. الهاكرز (Hackers)

هم متطفّلون يتحدّون إجراءات أمن النّظم والشّبكات، ولا تتوفر لديهم في الغالب الأعمّ دوافع حاقدة أو تخريبية، وإنّما ينطلقون من دوافع التّحدي وإثبات الذّات ومحاولة كشف عيوب الأنظمة لإبراز سيطرتهم وسلطتهم على تقنيّة المعلومات. كما تضمّ أيضًا الأشخاص الّذين يستهدفون الدّخول إلى أنظمة الحاسبات الآليّة غير المصرّح لهم بالدّخول إليها، وكسر الحواجز الأمنية الموضوعة لهذا الغرض وذلك بهدف إكتساب الخبرة وبدافع الفضول، أو لمجرد إثبات القدرة على إختراق هذه الأنظمة[2].

3. المجرم الهاوي

وهم الأشخاص الّذين يرتكبون الإجرام المعلوماتي بغرض التّسلية والمزاح ولشعورهم بالفراغ مع الآخرين، دون أن يكون في نيّتهم إحداث أي ضرر بالمجني عليه. ولكن هذا لا يعني أن أفعالهم الجرمية لا تشكّل ضرر على الغير، إنّما فقط يفتقدون لنيّة إحداث الضّرر.

النّبذة الثّانية: المجرمون المحترفون

تنقسم هذه الفئة من المجرمين المعلوماتيين إلى ثلاث فئات لكل منهم خطورته في البيئة المعلوماتية

[1] بن منصور صالح، كوش أنيسة، **السلوك الإجرامي للمجرم المعلوماتي**، المرجع السابق نفسه، ص: 24.

[2] أندرو كونري موراي، فينسنت ويفر، **دليل سمانتك إلى أمن الإنترنت في المنزل**، الدار العربية للعلوم، 2006، ص:16.

نظرًا لما يتمتّعون به من أسآليّب فنّيّة معلوماتية ورقمية لإرتكاب الإجرام المعلوماتي. الفئة الأولى هي فئة المخربون، بينما الفئة الثّانية فهي "الكراكرز" (crackers) أو المجرم المتمرّس، أمّا الفئة الثّالثة فهي فئة المتجسسين.

1. المخرّبون

إنّ هذه الفئة من المجرمين لا يرتكبون أعمالهم طمعًا في الإشادة العقليّة أو إثبات الذّات، بل عادة يكونون مستخدمين في منشأة أو مؤسّسة تساعدهم صفتهم فيها على إرتكاب جرائمهم ضدّ تلك المنشأة. وهم نوعين، الأوّل هم "المستخدمون " وهم أشخاص مستخدمون فقط، تتوافر لديهم المعرفة الكافية بآليّة عمل الحاسب الآليّ ومكوّناته ووظائفه الأساسيّة. بالإضافة إلى معرفة بعض البرامج الّتي يجري العمل بها في المنشأة، كبرامج المحاسبة والتّطبيق، ولديهم أيضًا معرفة كافية بآليّة عمل الشبكات المعلوماتية [1]. تتمّ طريقة إرتكاب هذه الفئة لجرائم التّقنيّة إمّا بالدّخول إلى مراكز الحاسب الآليّ المركزي مباشرة بأي وسيلة، أو بإستخدام إحدى وحدات الحاسب الأعلى الفرعيّة المرتبطة بالحاسب الآليّ المركزي، سواء بإستخدام كلمة السّر أو بإستخدام البطاقة الممغنطة أو أي وسيلة أخرى تسمح بذلك. وعادة ما تلجأ المؤسّسات والمنشآت إلى عدم إخبار السّلطات بهذا النّوع من الجرائم حفاظًا على سمعة المؤسّسة أو المنشأة، وتكتفي بإجراء تأديبيّ خاص فيها فتخفي الأمر عن سلطات الملاحقة والتّحقيق ممّا يؤدي إلى عرقلة سير العدالة الجزائيّة.

أمّا النّوع الثّاني وهم " الغرباء " (bola) وهم أشخاص أجانب عن تلك المؤسّسة ويندرج تحت هذه الطائفة المستخدمون الّذين ليس لديهم تصريح بالعمل على النّظام المعلوماتي الخاص بتلك المؤسّسة أو الشّركة. وفي الغالب يكون التّخريب هو هدف هؤلاء الدّخلاء، أي أنهم يقومون بالدّخول إلى الحاسوب

[1] بن منصور صالح، طباش عز الدين، **السلوك الإجرامي للمجرم المعلوماتي**، المرجع السابق نفسه، ص: 38.

بغرض إرتكاب جرائم التّخريب أو قد يكون المكسب الماديّ هو الهدف من عمليّة الدّخول [1].

2. المجرمون المتمرّسون

ويطلق على المجرمين المتمرّسين الذين يرتكبون الإجرام المعلوماتي مسمّى "الكراكرز". الكراكر هو شخص متخصّص وخبير في مجال الحاسب الآليّ، وتتمثّل أعماله بأنشطة غير قانونية تسعى إلى تدمير الأنظمة المعلوماتية لإحداث أضرار بالغير وتحقيق المكسب المادّي لهم أو لجهة كلفتهم بإرتكاب جرائم التّقنيّة الحديثة. كما تهدف إعتداءات بعضهم إلى تحقيق أغراض سياسيّة والتّعبير عن مواقف فكريّة أو نظريّة أو فلسفيّة، وتبعًا لتخصصهم في نوع معيّن من الجرائم أو تبعًا للوسيلة المتّبعة من قبلهم في إرتكاب الجريمة[2]. في الوقت نفسه يعكس إعتداؤهم ميولَهم الإجرامي والرّغبة في الإتلاف، التّخزين، التّعديل والتّخريب بإستخدام الفيروسات أو القنابل المنطقيّة أو فكّ الشّيفرات إذ لهم الهيمنة الكاملة على تقنيّات الحاسوب والشّبكة المعلوماتية. وتتعدّد تصنيفات مجرمي المعلوماتية إمّا من حيث وسيلة إرتكاب الجريمة، أو شخصيّة المجرم أو كليهما، وهذا ما ينعكس على الضّحيّة الّتي دائمًا يكون الهجوم واقعًا عليها لامحالة.

3. المتجسسون

يعتبر هؤلاء من أخطر المجرمين المعلوماتيين كون عملهم قائم على التّجسس الّذي هو بطبيعته سرّي وغير قابل للكشف إلاّ عن طريق الصّدفة أو الخطأ. بالإضافة إلى ذلك، يقوم هؤلاء بالعبث أو الإتلاف في محتويات الشّبكة بعد وصولهم إلى أسرار المنشآت والأفراد، فيعمدون إلى تغييرها وتشويهها. وينقسم أعمال التجسس الإلكتروني إلى العديد من الأنواع، فهناك التّجسس المعلوماتي العسكري والأمني والّذي يتم عادة

[1] حمزة بن عفون، **السلوك الإجرامي للمجرم المعلوماتي**، المرجع السابق نفسه، ص: 37.

[2] بن منصور صالح، طباش عز الدين، **السلوك الإجرامي للمجرم المعلوماتي**، المرجع السابق نفسه، ص: 39.

بين الدّول المتنازعة وغير المتنازعة وخصوصًا الأعمال المخابراتية. وهناك أيضًا التّجسس الإقتصادي والصّناعي والّذي يتم بين الشّركات والمؤسّسات المالية المتنافسة. وعلى سبيل المثال قد يتمّ تحميل الأسرار الصّناعية من حاسوب في إحدى الشّركات وإرسالها بالبريد الإلكتروني مباشرة إلى منافستها. ومن أهم أهداف هذه الفئة في إستخدام الأنظمة المعلوماتية، هو الحصول على معلومات الأعداء والأصدقاء على حد سواء.

بالنّتيجة مهما كانت طبيعة المجرم المعلوماتي ومهما كانت درجة إلمامه بالتّقنيّة المعلوماتية سواء كان محترفًا أم غير محترف، لا ينفي الصّفة الإجرامية عن فعله. ولكن يمكن أن يساعد في تحديد درجة العقوبة الّتي ستفرض عليه، خصوصًا بعد ربطها بالدّوافع المحفّزة لإرتكاب الإجرام المعلوماتي الأمر الّذي يساعد بشكل فعلي في وضع آليّة للمعالجة وللحدّ من الإجرام المعلوماتي بأشكاله المتعدّدة.

وبعد التّعرف على مفهوم المجرم المعلوماتي والصّفات الّتي تميّزه عن غيره من المجرمين، بالإضافة إلى السّلوك الجرمي الّذي يمارسه في البيئة المعلوماتية وأبرز الدّوافع الّتي تحفّزه على إرتكاب الإجرام المعلوماتي وصولًا إلى التعرّف على مختلف أشكال المجرميين المعلوماتيين، كان لا بُدّ في الباب الثّاني من القسم الأوّل من التعرّف على ضحيّة هذا الإجرام، الّتي أيضًا يجب التعرّف على ماهيّتها ومفهومها وأبرز الصّفات الّتي تجعل منها ضحيّة إضافة إلى تنوّعها مع تنوّع السّلوك الجرمي الّذي يسلكه المجرم والواقع عليها.

الباب الثّاني

ضحيّة الإجرام المعلوماتي

لم يهتم علم الإجرام في السّابق بدراسة الضّحيّة كطرف من أطراف الجريمة الّتي يقتضي حمايتها، وإنّما كان يتم تهميشها ممّا يؤدّي إلى ضعف الضّمانات الخاصّة بها. لكن مع التطوّر الملحوظ في السّياسات الجزائية المختلفة أصبح الإهتمام بالضّحيّة أمرًا ضروريًّا وواجبًا، ليس فقط لتأمين الحماية وصون الضّمانات القانونية الأساسية الّتي ينبغي أن يتم إقرارها لها، وإنّما من أجل فهم الجريمة بطريقة أفضل من حيث دراسة العوامل المؤثّرة لوقوعها ضحيّة أيّ إجرام، ودورها المباشر أو غير المباشر في إرتكاب الجرائم عليها وصولًا إلى إيجاد أفضل الأساليب الّتي يمكن أن تساعد في عدم وقوعها تحت تهديد أيّ إجرام.

إذ كان مفهوم الضّحيّة في الإجرام المعلوماتي يثير بعض الإشكاليّات خصوصًا أنّ الضّحيّة عادة ما توجد نفسها بشكل إرادي في البيئة المعلوماتية الّتي تعتبر السّاحة الجرمية للإجرام المعلوماتي، وتقبل بتحمل المخاطرة الّتي تفرضها إستعمال هذه التّقنيّة دون أخذها في الإعتبار حماية نفسها ومحتوياتها المعلوماتية من أيّ تعرّض، إضافة إلى تهوّرها في إستعمال التّقنيّة المعلوماتية دون سابق خبرة.

لذلك كان لا بُدّ من دراسة ضحيّة الإجرام المعلوماتي على ضوء علم الإجرام، وذلك في محاولة لبناء مفهوم لها والتعرّف على أبرز السّمات الّتي تتميّز بها والّتي تسهّل في جعلها ضحيّة الإجرام المعلوماتي إضافة إلى الآليّة الّتي يتم إختيارها بها كضحيّة وذلك في فصل أوّل. ثمّ في الفصل الثّاني سنتعرّف على تصنيف علم الإجرام لضحايا الإجرام المعلوماتي بشكل يوضح طبيعة الأشخاص ونوعيّة الجهات الّتي يقع عليهم هذا الإجرام.

الفصل الأوّل

تطوّر شخصيّة الضّحيّة في الإجرام المعلوماتي

لا جريمة من دون ضحيّة، ولكن مفهوم الضّحية يختلف من جريمة إلى أخرى. فيُقصد بمصطلح الضّحية، الشخص الّذين أُصيب بضرر فردي أو جماعي، بما في ذلك الضرر البدني، العقلي، المعاناة النّفسيّة، الخسارة الإقتصادية أو الحرمان بدرجة كبيرة من التّمتّع بحقوقه الأساسيّة عن طريق أفعال أو حالات إهمال تُشكّل إنتهاكًا للقوانين الجنائية النّافذة في الدّول، بما فيها القوانين الّتي تُحرّم الإساءة لإستعمال السّلطة [1].

لكن إذا كان الإجرام بوجهه التّقليدي يوجّه إعتدائه على حق الحياة والممتلكات الفرديّة، فإنّ الإجرام بوجهه الحديث وخصوصًا الإجرام المعلوماتي منه، جعل من الضّحيّة في مثل هذا النّوع من الإجرام شخصيّة مبهمة يَسهُل الوصول إليها بكثير من الذّكاء والحنكة المعلوماتية. مقابل جهل، عدم وعي، تهوّر، ضعف نُظُم أمان أو ثغرات موجودة في نظام معلوماتي معيّن تُمَكّن من الوصول إلى الضّحيّة دون عنف. فضحيّة الإجرام التّقليدي عادة ما كانت ضحيّة مجرمين يقومون بسلوكيّات عنفية لتحقيق أهدافهم الجرمية، وكانوا يختارون الضّحيّة الأقرب إليهم والّذين يملكون معلومات عنها تفيدهم في تحقيق نشاطهم الجرمي. على عكس الإجرام المعلوماتي الّذي كثيرًا ما تكون الضّحيّة فيه غير معروفة من قبل المجرميين المعلوماتيين، فضلًا عن أنّ الأساليب الّتي ترتكب بواسطتها الجريمة بعيدة عن العنف، بحيث يستعمل الذّكاء البشري في التّقنيّة المعلوماتية ويوظّف في أعمال غير مشروعة.

أمام هذا الإختلاف في ضحيّة الإجرام المعلوماتي عن ضحيّة الإجرام التقليدي، كان لا بُدّ من تحديد المقصود بضحيّة الإجرام المعلوماتي وذلك في مطلب أوّل نحاول فيه بناء تعريف لها وتحديد أبرز السّمات

[1] الأمم المتحدة، الإعلان العالمي الخاص بالمبادئ الأساسية لتوفير العدالة لضحايا الجريمة وإستعمال السلطة، قرار رقم 401434، تاريخ 1985/11/29.

الّتي تتمتّع بها، وفي مطلبٍ ثانٍ نحاول تبيان طريقة أو آليّة إختيارها لضحيّة الإجرام المعلوماتي من قبل مجرمي المعلوماتية.

المطلب الأوّل: مفهوم ضحيّة الإجرام المعلوماتي

تواجه المجتمعات إرتفاعًا ملحوظًا في عدد الإجرام المعلوماتي الّتي لم يعد مقتصر على عمليّات القرصنة الإلكترونية وإختراق أجهزة الكمبيوتر أو الإحتيال عبر المواقع المزيّفة، بل تعدّدت بالتّوازي مع تطوّر وسائل التّكنولوجيا والإنتشار الواسع لتقنيّات المعلومات في كلّ نواحي الحياة. ويمكن أن يقع الملايين ضحايا للإجرام المعلوماتي الّتي قد يعتبرها البعض أحداثًا عابرة فلا يقومون برفع شكاوى ضد مرتكبيها، ممّا أثبت أنّ معظمها يمكن أن يؤثّر على الصّحة النّفسيّة والحياة العمليّة وحتّى على العلاقات الاجتماعية. فضلًا عن أنّ الشباب خصوصًا النّساء والأطفال الّذين يتعرّضون على سبيل المثال للتنمّر عبر الإنترنت أو الإبتزاز، قد يكونون أكثر عرضة للإصابة بالإكتئاب وتزيد إحتمالات إقدامهم على إيذاء أنفسهم والإنتحار بمقدار الضعف مقارنة بغيرهم.

فكان من الأهمّية بمكان ما أن يتم توجيه الأنظار إلى ضحيّة الإجرام المعلوماتي، الّتي أصبحت تشكّل في السّياسة الجزائية المعاصرة عنصرًا من العناصر الّتي يهتم علم الإجرام بدراستها إلى جانب كلّ من الجريمة والمجرم والمجتمع. حيث أصبحت ضحيّة الإجرام المعلوماتي أكثر غموضًا، تارة تكون عشوائية وتارة محدّدة من دون وجود أيّ حماية يمكن أن تستنجد بها في ظلّ إستباق الإجرام المعلوماتي على القانون. لذلك كان لا بُدّ من محاولة تعريفها وتبيان موقعها من الجريمة وعمليّة التأثّر والتأثير بينها وبين العناصر الثّلاثة المار ذكرها. ففهم الضّحيّة يساعد في التعرّف على عوامل جذب المجرمين لها الّذين بدورهم يساعدون في تحديد طرق الوقاية والتصدّي للإجرام المعلوماتي بأشكاله المختلفة، إضافة إلى

تبصير الضّحايا بكيفيّة وقاية أنفسهم من الجريمة وإتخاذهم التّدابير الإحترازية من الوقوع في مصايد المجرمين.

وبناءً على ما تقدّم، سنقوم في هذا المطلب بتعريف ضحيّة الإجرام المعلوماتي وذلك في نبذة أولى، ثمّ في النّبذة الثّانية سنستعرض أبرز سماتها الّتي تجعل منها ضحيّة هذا الإجرام.

النّبذة الأولى: تعريف ضحية الإجرام المعلوماتي

لا شكّ أنّ تقنيّة المعلومات أدخلت العالم في عصر جديد من الإجرام، فبالرّغم من التّطوّر الإيجابي لهذه التّقنيّة، إلاّ أنّ هناك تخوّف من إشتداد خطورة الإجرام بشكله الحديث عن شكله التّقليدي، وإعتدائه على الحقوق الإنسانيّة والإقتصادية والسّياديّة للدول. فالضّحيّة في الجريمة بصفة عامّة، هي كل شخص طبيعي أو معنوي، أصيب بخسارة أو ضرر أو بعدوان نتيجة إرتكاب جريمة سواء بفعل أو بالإمتناع عن فعل. أمّا المقصود بالضّحيّة في الجريمة المعلوماتية هي كلّ شخص أصابه ضرر ماديّ أو معنويّ نتيجة الإستخدام غير المشروع لتقنيّة المعلومات، فقد يكون شخصًا عامًا ممثلًا في مؤسّسات الدّولة وهيئاتها، وقد يكون خاصًا ممثلًا في أشخاص طبيعيين ومعنويين. وبحسب ذلك، فإنّ ضّحايا الإجرام المعلوماتي يختلفون عن ضّحايا الإجرام التقليدي من مجرّد كونهم أشخاصًا عاديين، إلى مؤسّسات ماليّة أو عسكريّة أو قطاعات حكوميّة، يصعب على المجرم التّقليدي إرتكاب أي جرائم فيها أو في مواجهتها [1].

بالتّالي إن الإجرام المعلوماتي هو إجرام يقع على المؤسّسات العامّة أو الخاصّة أو الشّركات أو

[1] سعيداني نعيم، **آليّات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية (علوم جنائية)، إشراف د. زرارة صالحي الواسعة، جامعة الحاج لخضر، باتنة، 2013، ص: 64.

الأفراد مستخدمي أجهزة الحاسب الآليّ أو أجهزة الهواتف الذّكيّة [1]، يهدف بشكل مباشر إلى الإضرار بهؤلاء الضّحايا، إمّا بهدف النّيل من سمعتهم والتّشهير بهم، أو الإنتقام منهم، أو إبتزازهم وتهديدهم وذلك من أجل الحصول على مكسب مادّي أو معنوي، أو من أجل إنتهاك فِكر الضّحيّة وخطفه ذهنيًا لأجل غايات إجرامية معيّنة، أو بهدف الحصول على المعلومات.

وبتعدد آليّات إرتكاب الإجرام المعلوماتي وأنواعه، يتعدّد بالدّور نفسه نوع الضّحايا الّذين يقعون فريسة هذا الإجرام. ففي حين كان دور الدّولة في الإجرام التقليدي الحدّ منه وملاحقة مرتكبيه ومحاكمتهم، أصبحت الدّولة هي بذاتها ضحيّة مباشرة ومحدّدة، وهدف لعدد من المجرمين والجماعات الإجرامية المعلوماتية. كما أصبحت بدورها الضّحيّة مسؤولة بشكل مباشر أو غير مباشر ولو عن طريق الخطأ، بوقوع الإجرام المعلوماتي عليها.

فعلى الرغم من إمكانيّة تعرّض الجميع للإجرام المعلوماتي سواء كانوا أشخاصًا معنويين أم طبيعيين، إلاّ أنّ معظم الجرائم المعلوماتية تُرتكب من أجل أمرين وهما: المال والمعلومات. لكن إذا كان الغالب الأعمّ ممّن يرتكب الإجرام المعلوماتي شخصًا طبيعيًا، فإن المجني عليه هنا هو بالغالب شخص معنوي كالبنوك والشّركات الكبرى والمؤسّسات الحكومية والوزارات والمنظمات والهيئات الماليّة، وغيرها من الشّخصيات الإعتباريّة الّتي تُعتمد في إنجاز أعمالها على الحواسيب [2].

بناءً على ما تقدّم سنقوم بالتّعرف أكثر على شخصيّة الضّحيّة المعلوماتية عبر عرض أبرز السّمات الّتي يمكن أن تتمتّع بها.

---

[1] جلال الجنيدي، الجرائم الإلكترونية وطرق الوقاية منها، مدونات جزيرة (موقع إلكتروني)
الجرائم-الإلكترونية-وطرق-الوقاية-منها/https://blogs.aljazeera.net/blogs/2018/7/24

[2] عبد الله دغش العجمي، **المشكلات العملية والقانونية للجرائم الإلكترونية (دراسة مقارنة)**، مذكرة مقدمة لنيل شهادة الماجستير في القانون العام، إشراف د. أحمد اللويزي، جامعة الشرق الأوسط، 2014، ص: 34.

النّبذة الثّانية: صفات ضحايا الإجرام المعلوماتي

أصبحت الضّحيّة تتمتّع بمكانة هامّة في نظام العدالة الجزائيّة بعد أن كان كلّ الإهتمام يصب حول معرفة شخصيّة المجرم وأعماله. إذ لم تقع جريمة إلاّ وكان سببها فاعل، فليست الجريمة واقعة إلا ونتيجتها ضحيّة، الّتي لم تعد فقط ركنًا قانونيًا بل أصبحت شخصيّة إنسانيّة لها مكوّناتها ومقوّماتها الطبيعيّة والنّفسانيّة والإجتماعيّة الّتي يقتضي حمايتها.

لذلك سنحاول في هذه النّبذة تبيان أهمّ السّمات الّتي تتمتّع بها ضّحيّة الإجرام المعلوماتي، كونها من الجرائم الحديثة الّتي لا يزال الغموض يلّف حولها.

1. خوض تجارب حديثة

لدى الكثير من الأشخاص الفضول للدخول في تجربة جديدة في البيئة المعلوماتية، فيحاول المجرم المعلوماتي إثارة فضول الضّحيّة وإغرائها للغوص أكثر في المساحة المعلوماتية الّتي يكون قدّ حدّدها مسبقًا، وجهّز بنيتها وآليّاتها للتّمكن من الضّحيّة فيها [1]. فالإنفتاح على التّجربة يجعل الشّخص عرضة بشكل أكبر للوقوع ضحيّة الإجرام المعلوماتي، فبدل أن يكون في حيّز آمن في البيئة المعلوماتية، يضعه فضوله على جانب خطر ويدفعه نحو المجرم المعلوماتي دون عناء هذا الأخير.

2. عدم ضبط النّفس

إنّ إنخفاض ضبط النّفس يشكّل خطرًا على وجه التّحديد، ويعاني من هذه المشكلة عدد كبير من

[1] Eric Rutger Leukfeldt, **Big Five Personality Traits of Cybercrime Victims**, ResearchGate,2017,https://www.researchgate.net/publication/317987452_Big_Five_Personality_Traits_of_Cybercrime_Victims. Date of entry to site: 13/10/2019.

الضّحايا خصوصًا الّذين يطمعون بموارد مادّية، أو الّذين لا يملكون القدرة على ضبط عواطفهم. وتلعب الضّحيّة الّتي تملك هذه السّمة دورا ضرورا وأساسيا في العمليّة الجرمية وتصبح في خطر متزايد لأن تصبح ضحيّة هذا الإجرام [1]. فعمليّة الإحتيال الإلكتروني مثلًا تكون أسهل في وجه ضحيّة لا تستطيع ضبط نفسها، حيث يسهل إغوائها بمطامع ماليّة للتمكّن من الإحتيال عليها.

3. عدم الإستقرار العاطفي

إنّ عدم الإستقرار العاطفي للضحيّة يكون عنصر جذب للمجرم المعلوماتي، كونه يهيّئ بيئة نفسيّة ملائمة للوصول إليها معتمدًا على النّقص العاطفي. حيث يحاول المجرم التّمكن من الضّحيّة بأساليب تناسب وضعها العاطفي للوصول إليها أو خرق بياناتها أو الحصول على معلومات بشأنها. فالأشخاص الّذين لديهم إستقرار على المستوى العاطفي هم أقلّ عرضة للتعرّض للإجرام المعلوماتي [2]. ونشير إلى أنّ المؤسّسات العامّة والخاصّة والشّركات لا تكون عرضة للإجرام المعلوماتي بسبب هذه السّمة، فهي تخصّ أكثر الشّخص الطبيعي وخصوصًا النّساء والأطفال.

4. الخوف

كثيرًا ما يشعر ضحايا الإجرام المعلوماتي بالخوف من الإعلان عن الجريمة الّتي طالتهم، وذلك خوفًا من الإعلان السّيء وما ينتج عنها من إعتداء على سمعتهم، حيث يفضّلون عدم التّقدّم بالشّكوى ومحاولة تسوية الأمر بطرق المفاوضات أو المساومات أو التّكتّم عنها خوفًا من الفضيحة [3]. كما نرى أنّ

[1] Eric Rutger Leukfeldt, **Big Five Personalty Traits of Cybercrime**, the same recourse.

[2] Eric Rutger Leukfeldt, **Big Five Personality Traits of Cybercrime**, the same resource.

[3] د. جنان الخوري، **الجرائم الإقتصادية الدولية والجرائم المنظمة العابرة للحدود**، المرجع السابق نفسه، ص: 170.

المؤسّسات الماليّة كثيرًا ما تلجأ إلى هذا الأسلوب، وذلك حفاظًا على السُمعة التّجارية العائدة إليها، فتحاول تسوية الأمر من داخل المؤسّسة دون التوجّه إلى إتّباع الإجراءات القضائية.

5. الجهل بجرائم المعلوماتية

يكون الجهل بالجرائم المعلوماتية من قبل الضّحيّة المعلوماتية إمّا بشكل كليّ، حيث أنّ عددًا كبيرًا من هذه الجرائم تبقى غير مرئية ومخفيّة. وإمّا بشكل جزئي، حيث أن هناك قسم لا يستهان به من هذا الإجرام يُعرف في دعاوى عدّة، إنّما لا يرسل إلى مراقبة الأجهزة المختصّة بالملاحقة الجزائيّة. هذا فضلًا عن أنّ القليل من ضحايا الإجرام المعلوماتي يتقدّمون للمدافعة عن حقوقهم وذلك لجهلهم بأنّهم خُدعوا أو إستغلّوا من قبل المجرمين المعلوماتيين، أو الجهل بنقص القوانين الدّاخلة حيّز التّنفيذ في هذا المجال [1].

6. عدم المبالاة

إنّ الإجرام المعلوماتي هو من الجرائم الحديثة بحيث أنّ الضّحيّة فيه لا تعي بعد كيفيّة المطالبة بحقها، وتحديد مقدار الضّرر الّذي لحق بها أو التكاليف المادّية الّتي سوف تستنزفها لتقديم شكوى بهذه الجرائم، هذا فضلًا عن التّحفظ على العديد من الخصومات من قبل سلطة الملاحقة. وهذه الأمور تجعل من شخصيّة الضّحيّة المعلوماتية شخصيّة غير مبالية بهذه الجريمة.

إذًا فإنّ ضحيّة الإجرام المعلوماتي تختلف نوعًا ما عن ضحيّة الإجرام التّقليدي، خصوصًا في نوعيّة الجريمة المرتكبة عليها والسّاحة الجرمية الّتي ترتكب فيها الجريمة، وصولًا إلى السّمات الّتي تتميّز بها والّتي تجعل منها مصدر جذب للمجرمين المعلوماتيين فقط.

وبعد أن كان علماء علم الإجرام يتساءلون عن مفهوم ضحايا الإجرام المعلوماتي والسّمات الّتي تميّزهم

[1] د. جنان الخوري، **الجرائم الإقتصادية الدولية والجرائم المنظمة العابرة للحدود**، المرجع السابق نفسه، ص: 169.

عن ضحايا الإجرام التّقليدي، إهتم علماء الإجرام بعدها بالأسس الّتي يحدّد بموجبها المجرم المعلوماتي ضحيته أيّ ما هي المعايير الّتي يتمّ بموجبها إختيار ضحيّة الإجرام المعلوماتي من قبل مجرمي المعلوماتية؟ الأمر الّذي سنبحثه في المطلب الثّاني من هذا الفصل، حيث سنتكلّم عن كيفيّة إختيار ضحيّة الإجرام المعلوماتي من قبل مجرمي المعلوماتية.

المطلب الثّاني: إختيار ضّحيّة الإجرام المعلوماتي

من الخطأ أنّ يظنّ أيّ منّا أنّه في مأمن من الإجرام المعلوماتي، حتّى ولو كان الحاسوب يتمتّع بنظم أمان متطوّرة أو يحتوي على بعض المستندات والصّور الشخصيّة غير المهمّة. فممكن أن يكون الحاسوب الخاص بنا إمّا هدف للمجرم المعلوماتي، أو يكون وسيلة من خلالها يتمّ إرتكاب الإجرام المعلوماتي ضدّ الغير من خلاله[1]. لكن تطرح إشكاليّة حول مدى إيجاد هدف ملائم للمجرم المعلوماتي يتمكّن من خلاله من تحقيق غايته الجرمية، إذ أنّ المجرم عادة يبحث عن الضّحيّة الّتي تستعمل نظم معلوماتية أقلّ حماية وأمان من غيرها هذا من جهة. ومن جهة ثانية يعتمد على خطأ الضّحيّة وتقصيرها وعدم إنتباهها، للتّمكّن منها في حال كان نظام الأمان المعوّل عليه أقلّ حداثة من الفيروسات المستعملة. هذا مع العلم إلى وجوب التّنبه إلى أن هناك دائمًا شخص، أي مجرم معلوماتي، أذكى أو أكثر إطّلاعًا أو مجهّز بشكل أفضل منا، يمكن أن يعتدي على نظم الأمان الخاصّة بالأفراد والمؤسّسات والشركات والدولة.

لكن السؤال الأساسي الّذي يُطرح في صدد الإجرام المعلوماتي، هو كيفيّة إختيار الضّحيّة من قبل المجرم المعلوماتي، فهل تكون الضّحيّة هدف فرصة تسمح للمجرم المعلوماتي من تنفيذ جريمته عليها عن

[1] أندرو كونري موراي، فينسنت ويفر، **دليل سيمانتك إلى أمن الإنترنت في المنزل**، الدار العربية للعلوم، سنة 2006، ص: 19.

طريق الصّدفة؟ ذلك سنبحثه في نبذة أولى، أم هدف خيار محدّد من قبل المجرم المعلوماتي بشكل مباشر لتنفيذ غاية في ذهنه؟ وهو ما سنبحثه في النّبذة الثّانية.

النّبذة الأولى: هدف فرصة

في حالات عديدة يطوف القراصنة خلسة على الإنترنت بإستعمال مجموعة متنوّعة من الأدوات، ويكون في ذهنهم عادة جدول أعمال عندما يكتشفون هدفًا محتملًا. وغالبًا ما يكون صغار المجرمين المعلوماتيين الأكثر ميلًا إلى هكذا نوع من الضّحايا، حيث يتمّ إستعمال أساليب وبرامج أو نصوص برمجية معروفة جيّدًا ويسهل العثور عليها، بغية البحث وإستغلال نقاط الضّعف في الحواسيب الأخرى على الإنترنت وبشكل عشوائي في أغلب الأحيان [1]. لتحديد ما إذا كانت الضّحيّة هدفًا لفرصة هي مسألة تعتمد على البنية التحتية لأمانه. فهناك قاعدة جيّدة مبنيّة على التجربة، توضّح أنّ عدم إمتلاك جدار نار أو عدم تحديثه منذ فترة، سيجعل الشّخص على الأرجح هدفًا لفرصة [2]. نظرًا لأنّ مجرمي المعلوماتية يستخدمون أدوات جرمية تبحث عن نقاط الضعف في نظم الأمان، لذلك تعتبر أسهل الطّرق للفرد أو للمنشاة، لكي يضمنوا أنّهم لن يكونوا هدفًا لفرصة، هي بتحديث بنيتهم التحتية بأحدث نظم الأمان.

وعادة ما يبحث القراصنة عن أهداف الفرصة، حيث يأملون أن يكونوا في أعداد كبيرة لشن هجوم موحّد عليهم. والهدف الفرصة هو هدف يتوفر في لحظة معيّنة ومحدّدة يستغلّ من خلالها مجرم المعلوماتية نقاط الضّعف في البنية الحاسوبية والمعلوماتية للضحيّة، فينفذّ جرمه عليه. وعلى الأغلب فإنّ هذا الهدف، أيّ الضّحيّة، تكون محدّدة بطريقة عشوائية أو عن طريق الصّدفة دون تحديد مسبق لنوع الضّحيّة أو شخصيتها، بل كل ما يتطلّع إليه المجرم المعلوماتي هو إنطباق هذا الهدف على جدول أعماله

[1] طوم توماس، **الخطوة الأولى في عالم أمان الشبكات**، الدار العربية للعلوم، 2004، ص: 24.

[2] المرجع السابق نفسه، ص: 25.

الجرمي أيّ الغاية الجرمية الّتي يتطلّع لتحقيقها. وعمومًا من يقع في فخ ضحايا الفرصة هم الضّحايا العاديين، غير المتمكّنين من التّقنيّة المعلوماتية والّذين لا يفقهون عمل أنظمة الحماية والأمان، فيغلب عليهم طابع اللامبالاة تجاه التّقنيّة ليقعوا فريسة المجرمين المعلوماتيين بكل سهولة ودون عناء.

النّبذة الثّانية: هدف خيار

قد لا تكون الضّحيّة هدفًا لفرصة، لكنها يمكن أن تكون هدفًا من أهداف خيار القراصنة، فغالبًا ما يكون لدى مجرمي المعلوماتية غاية في ذهنهم عند إنتقائهم هدفًا، فيختارون أهدافهم بدقّة ومهنيّة عالية. وذلك بعد درس أهدافهم والإطلاع على الخيارات الموجودة، وما إذا كان الهدف المختار يحقّق الغاية الجرمية الّتي يطمح لها المجرم المعلوماتي أم لا [1]. فمثلًا إذا كان لديك شركة معيّنة، وهذه الشركة ستنتج منتج جديد يُحدث ثورة في مجال الأعمال، ويُحدث تطورًا ضخمًا على الصّعيد المحلّي أو العالمي، يمكن أن يعمد المنافسون إلى الإضرار بشركتك عبر الجريمة المعلوماتية، فيحدّدون الضّحيّة بشكل مباشر ويختارونها بدقّة لمنع التّطوّر الإقتصادي الّذي كانت ستجنيه الشّركة.

غير أنّ المجرم المعلوماتي ليس دائمًا مجرمًا ساخطًا، غاضبًا من العالم، يعاني من إحترام متدنّي لذاته أو لا يحترم السّلطة، غير متأقلم إجتماعيًا، عشوائيًا في إختيار ضحيّته ولا يركزّ في أهداف جرمية محدّدة. بل على العكس، نجد أنّ مجرم المعلوماتية هو شخص ذكيّ، دقيق في إختيار الضّحيّة وله هدف وغاية معيّنة من هذه الجريمة الّتي يحاول تحقيقها. فعمليّة إختيار الضّحيّة تحتاج الى عمل منظّم، أيّ يجب أن يكون هناك تخطيط مسبق ومراقبة معلوماتية للضحيّة المختارة، وذلك بهدف التّمكّن منها وتحقيق المشروع الجرمي. إذ أنّ الهجوم الإلكتروني الّذي تشنّه دولة على أخرى أو عصابة إجرامية على دولة

[1] طوم توماس، **الخطوة الأولى في عالم أمان الشبكات**، المرجع السابق نفسه، ص: 25،26.

معيّنة، لا يخلو من هذه الصّفات. وكثيرًا ما يكون هناك عمل جماعي بين مجموعة من المجرمين المعلوماتين، فيقوم كل واحد منهم بدور محدّد في الجريمة. غير أنّ مسألة إختيار الضّحيّة وتحديدها وتوجيه العمل الجرمي عليها، يصبغ على الفعل الجرمي طابع الخطورة أكثر منه على الضّحايا المحدّدين عن طريق الصّدفة والفرصة. فمثلًا فعل السّرقة بواسطة التّقنيّة المعلوماتية يحتاج إلى تحديد هدف معيّن ملييء ماديًا، وعادة ما تكون الضّحية في هذا النّوع من الجرائم هي المصارف والمؤسّسات الماليّة، فيصبح إختيار الضّحيّة أمر ضروري لتحقيق أعلى مستوى من المشروع الجرمي المعلوماتي.

بناءً على ما تقدّم، يمكن أن تكون الضّحيّة إمّا ضحيّة فرصة تتواجد أمام المجرم المعلوماتي فيستغلّ الثّغرات الّتي تعتليها ويحقق مشروعه الجرمي. وإمّا تكون ضحيّة خيار، فيقوم المجرم المعلوماتي بإختيارها بدقّة عالية، فبدون هذا التّحديد للضحيّة لا يمكن تحقيق المشروع الجرمي والجريمة.

وبعد عرضنا لكلّ من تعريف ضحيّة الإجرام المعلوماتي والسّمات الخاصّة الّتي تتميّز بها، كان لا بُدّ في ظلّ ربطنا للضحيّة بعلم الإجرام من القيام بإعمال التّصنيف العلمي والقانوني لضحايا الإجرام المعلوماتي، والّذي سيتم بحثه في الفصل الثّاني.

الفصل الثّاني

تصنيف علم الإجرام لضحايا الإجرام المعلوماتي

إنّ الإهتمام بالضّحيّة ظهر حديثًا ضمن نظام العدالة الجزائيّة، ويهدف في الإجرام المعلوماتي إلى المحافظة على حقوقهم وذلك من خلال وسائل قانونية، حقوقية وإتفاقيّات ونصوص قانونية. وكما هي العادة، يقع الإجرام في الجريمة التّقليدية على حقّ الحياة والممتلكات الفرديّة. بينما في الجرائم الحديثة وخصوصًا الإجرام المعلوماتي، يمتد الأمر إلى أمن المجتمعات والأمم ويتحدى تشريعاتها ومؤسّساتها وأُسسها الإقتصادية الضّريبية والماليّة والمعلوماتية.

وبسبب تنامي ظاهرة الإجرام المعلوماتي في ظلّ تحوّل معظم دول العالم إلى النّظام الرّقمي أو المعلوماتي، تنوّعت ضحايا هذا الإجرام الّذي شكّل مفاجأة لعلماء الإجرام أمام الدّراسات السّابقة الّتي أعدّت لدراسة الضّحيّة في الجرائم التّقليدية. وكانت نقطة التحوّل تكمن في التّهديد الكبير الّذي أصبح الإجرام المعلوماتي يمارسه بوجه السّياسات الجزائية التّقليدية وأمن المجتمعات والدّولة ومفهوم السّيادة. حيث شهدنا تحوّل في طريقة إرتكاب الجريمة أسفر عنها إتّساع رقعة الضّحايا، بحيث يمكن التعرّض لهم في هجوم معلوماتي واحد من قبل مجرم معلوماتي واحد. لذلك كان لا بُدّ من إجراء التّصنيف العلمي لضحايا الإجرام المعلوماتي لمعرفة الطّبيعة القانونية لكلّ طرف منهم، والتعرّف على الأشكال الجديدة من الضّحايا الّتي لم تكن يومًا ضحيّة للإجرام التّقليدي، وأهمّية موقعهم داخل منظومة المجتمع وما ينتج عن وقوعهم ضحايا الإجرام المعلوماتي. وما إذا كان هناك فئة من الضّحايا أكثر عرضة للجريمة المعلوماتية من غيرها، وما إذا كان الإعتداء يقتصر فقط على الشّخص الطّبيعي أو يصيب أيضًا الشّخص المعنويّ العام والخاص.

لذلك سنقسم هذا الفصل إلى مطلبين، سنتناول في المطلب الأوّل تصنيف علم الإجرام للأشخاص الطّبيعيين، الّذين يقع عليهم الإجرام المعلوماتي، أمّا في المطلب الثّاني سنتناول الأشخاص المعنويين.

المطلب الأوّل: الشخص الطبيعي

لا يختلف الإجرام المعلوماتي عن الإجرام التقليدي من حيث وقوعه على ضحيّة تتمثّل في شخص طبيعي، كالأفراد والمؤسّسات أو المنظّمات الّتي لا تملك الشّخصيّة المعنوية. لكن ما يميّز هذا الإجرام عن غيره من الجرائم هو وقوعه على نوعيّة من الضّحايا أكثر من غيرها، كسهولة وقوعه على الأحداث، وإرتفاع نسبة النّساء كضحيّة لهذا الإجرام أكثر من الذّكور.

يندرج تحت هذه الفئة كلّ منظمة أو جمعيّة أو مؤسّسة لا تتمتّع بالشخصيّة المعنويّة، والّتي من الممكن أن تتعرّض للإجرام المعلوماتي وذلك عند إستعمالها في أعمالها لتقنيّة الحاسب والإنترنت وللبرامج المعلوماتية. يتمثّل الإعتداء على هذه الفئة من الضّحايا في نقل برمجيات ضارّة إليها، مضمّنة في بعض البرامج التّطبيقية الخدماتية أو غيرها، أو تشويه المعلومات الّتي تملكها أو سرقتها، أو تشويه سمعتها عبر بث أخبار كاذبة مسيئة عنها سواء على مواقع معلوماتية متعدّدة أو على موقع المنظمة أو المؤسّسة نفسها بعد إختراقه والسّيطرة عليه.

ويندرج أيضا تحت هذا التصنيف " الفرد " كونه جزء من المجتمع والشخص الّذي تقع الجريمة عليه، لكن تختلف الضّحيّة الفرد بين حدث وراشد فلكلّ منهم وضعه إزاء الإجرام المعلوماتي، ويلعب في الوقت نفسه عنصر النّوع البشري عامل مساعد لإرتكاب هذه الجريمة، حيث يشكّل الإعتداء على النّساء النّسبة الأكبر. كما تسمّى بجرائم الإنترنت الشخصيّة أي الواقعة على شخص معيّن، وتتمثّل في سرقة الهويّة ومنها البريد الإلكتروني، أو سرقة الإشتراك في موقع شبكة الإنترنت وإنتحال شخصيّة أخرى بطريقة غير شرعية عبر الإنترنت بهدف الإستفادة من تلك الشخصيّة، أو لإخفاء هويّة المجرم لتسهيل عمليّة الإجرام، أو في جرائم الإبتزاز والجرائم الواقعة على الملكيّة الخاصّة والشخصيّة في البيئة المعلوماتية.

ولا يختلف وضع الشّخص الطّبيعي الراشد في الإجرام المعلوماتي عن الإجرام التقليدي، إذ يكفي أن

تكون الضّحيّة قد أتمّت الثامنة عشر من عمرها، ولم يكن محجورًا عليها لخلل يعيب إرادتها. لكن ما يلزم البحث فيه، في صدد هذه الجريمة هو في الضّحيّة القاصر وأهمّية العنصر البشري في إختيار الضّحيّة من قبل المجرمين. لذلك سنقسم هذا المطلب إلى نبذتين، سنتناول في النّبذة الأولى القاصر كضحيّة للإجرام المعلوماتي، أمّا في النّبذة الثّانية سنتناول العنصر الأنثوي كضحيّة أيضًا للإجرام نفسه.

النّبذة الأولى: القاصر ضحيّة الإجرام المعلوماتي

كما كان لهذه الجريمة وضعها الخاصّ تجاه القدرة العالية للحدث في إرتكاب الإجرام المعلوماتي وإعتباره فئة من المجرمين الخطرين الّذين يملكون القدرة على السّيطرة على تقنيّة الحاسوب والإنترنت، نرى في المقابل أن القاصر يمثّل ضحيّة تجذب المجرمين المعلوماتيين نحوها وذلك يتمّ عبر وسيلتين[1]:

- الأولى أن يكون القاصر مُكرَه على تنفيذ الجريمة المعلوماتية من قبل مجرمين يستغلّون ذكاءه ومعرفته التّقنيّة والفنّيّة في البيئة الرقميّة والمعلوماتية، فيعمدون إلى تشغيله لإرتكاب جرائم معلوماتية ربما لا يعلم حقيقتها أو يعلم ولكنّه مجبر على تنفيذها. فيُعتبر القاصر في هذه الحالة ضحيّة غيره من المجرمين، كونه يُقدم على أفعال جرمية دون علمه أو إرادته وبالإكراه، عن طريق إستغلاله كوسيلة لتنفيذ هذه الجرائم المعلوماتية تحت طائلة تعرّضه للعنف أو التّهديد أو غيرها من أساليب الإكراه.
- الثّانية هي عندما يكون القاصر بحدّ ذاته هو هدف المجرمين المعلوماتيين سواء كانوا راشدين أم قُصّر، ويعتبر القاصر مصدر جذب لهؤلاء كونه محدود الإدراك والمعرفة ولا قدرة له على التّمييز بين النّافع والضّار بشكل كليّ. هذا بالإضافة إلى فضوله لإكتشاف كل ما هو جديد في البيئة المعلوماتية.

وكون ضّحيّة الإجرام المعلوماتي قاصر لم يبلغ سِنّ الرّشد، فهذه مسألة لا يوجد سابقة لها في الإجرام

[1] د. ماري آيكن، التأثير السيبراني، **كيف يغير الإنترنت سلوك البشر**، الدار العربية للعلوم ناشرون، سنة 2017، ص: 136.

التقليدي، كون القاصر في الجريمة التّقليديّة يسهل حمايته وإتّخاذ إجراءات سابقة لمنع وقوع أي جريمة عليه أو منه. بينما في الإجرام المعلوماتي، فإنّ الأداة والوسيلة ألاّ وهي الحاسوب والإنترنت، أصبحت موجودة داخل كل منزل تقريبًا وبيدّ كلّ شخص قاصر كان أم راشد. ومهما كان مستوى الرّقابة من قبل الأهل على التّقنيّة فعالًا، يبقى هذا القاصر عرضة لأن يكون ضحيّة كون الإجرام المعلوماتي متجدّد ومستمرّ ومتتابع، يمكن إيقافه لفترة زمنيّة محدّدة بإنشاء نظم أمان، ولكن في النهاية ستُخترق وسيجد المجرمون وسيلة يتمكّنون من خلالها الوصول الى القاصر.

النّبذة الثّانية: العنصر الأنثوي ضحيّة الإجرام المعلوماتي

لم تسلم المرأة من الإجرام المعلوماتي بل أصبحت الضّحيّة الأكثر تعرّضًا لها، حيث يمارس ضدها كل أنواع الإجرام من تحرّشات جنسيّة، سرقة للمعلومات الخاصّة والمهنية، وسرقة الصّور بغرض إبتزازها. كما في بيع النّساء وإقحامهم في المنظمات المشبوهة والعصابات الخاصّة بالدّعارة والتّجارة بالمخدرات الّتي تتم بالوسائل الإلكترونية. بالإضافة إلى أنها تُستخدم كطعم لجلب ضحايا آخرين من الجنسين، وسرقة بطاقات الإئتمان عن طريق التّحايل أو وعود العمل أو الزواج.

فالإجرام المعلوماتي ضدّ المرأة لا تتعرّض له الفتاة القاصر فقط، بالرّغم من أنّها الفئة الأكثر عرضة لهذا الإجرام، بل تعاني منّها كل النّساء القاصرات والرّاشدات، العاملات والماكثات في المنازل، المتعلمات وغير المتعلمات. فأصبح الإجرام المعلوماتي عابر للفئات العمرية والنّوع البشريّ على السّواء[1].

في حين أنّ الإنترنت يجب أن يكون وسيلة لمعالجة المشكلات الّتي تعاني منها المرأة خاصّة العنف والجريمة، إلاّ أنّها أصبحت مصدرًا من مصادر ممارسة العنف والجريمة عليها بعمليّات تحرّش وإستغلال

[1] د. بن غذفة شريفة، د. القص صليحة، **دراسة قانونية حول الجريمة الإلكترونية الممارسة ضد المرأة على صفحات الإنترنت وطرق محاربتها**، جامعة سطيف 2 الجزائر، 2017، ص: 33.

جنسيّ، تجسّس وتسجيل مكالمات، تهديد وتشويه السّمعة، القدح والذّم، نشر صور خاصّة دون إرادتها، التّلاعب بمشاعرها عبر مواقع الإنترنت، سرقة بطاقات الإئتمان وغيرها من الأمور. وتعتبر المرأة الأكثر عرضة لهذه الجرائم كونها أكثر إنجرارًا نحو المشاعر العاطفية، إذ يسهل وقوع الكثيرين منهن ضحايا لأشخاص وهميين يحاولون إستدراجهنّ نحو الجريمة.

فالإجرام المعلوماتي لم يوفّر أحدًا من الأشخاص الطّبيعيين، بل كان الإجرام النّاتج عنه أكثر خطورة نظرًا لإهتمامه بنوعيّة ضحايا أكثر من غيرهم وهم القاصرين والنساء، الّذين دون شك بحاجة للحماية القانونية والقضائية. لكن الإجرام المعلوماتي لم ينتهِ عند هذا الحدّ إنّما أيضًا كان للشخص المعنوي النّصيب الأكبر من هذا الإجرام نظرًا لما يتمتّع به الأشخاص المعنويّون من مركز مالي وأمني، الأمر الّذي سنبحثه في المطلب الثّاني.

المطلب الثّاني: الشّخص المعنوي

ممّا لا شكّ فيه أنّ الشّخص الطّبيعي هو ضحيّة الإجرام المعلوماتي، ولكن يختلف الأمر حينما ترتبط شبكة المعلومات بين حواسيب متعددة وتكون جميعها تابعة لنفس الشّخص أو الجهة، كالمؤسّسات والبنوك وغيرها التي تحمل صفة الشّخص المعنوي، حيث يتمّ الإعتداء الجرمي المعلوماتي عليها لأسباب متعدّدة ويمكن أن يكون الإعتداء واقع على الدّولة أو إحدى المؤسّسات التّابعة لها لأهداف سياسيّة، إقتصاديّة، إنتقاميّة أو إجتماعيّة يهدف لها المجرم المعلوماتي. ومن هنا يتمثّل لدينا أنّ الشّخص المعنوّي الّذي يقع ضحيّة الإجرام المعلوماتي يمكن أن يكون خاص كالشّركات والبنوك وغيرها أو شخص معنويّ عام كالدولة والمؤسسات العامة والبلديّات.

لذلك سنبحث في هذا المطلب في الإجرام المعلوماتي الواقع على الشخص المعنوي الخاص وذلك في نبذة أولى، أمّا في النّبذة الثّانية فسنتطرّق إلى الشخص المعنوي العام.

النّبذة الأولى: الشّخص المعنوي الخاص

عادة ما يرتكب الإجرام المعلوماتي على الشّخص المعنوي الخاص لأهداف إقتصاديّة دون إستبعاد الأسباب الأخرى. وتتعدّد ضحايا هذا الإجرام بين شركات محليّة أو أجنبيّة أو متعدّدة الجنسيّات، وتصيب بإجرامها المساهمين، الشّركاء، الدّائنين، المأجورين، الزّبائن، المستهلكين، المنافسين وحتّى البيئة الإجتماعيّة والإقتصاديّة للشركة. ويتجلّى الإعتداء على الشّخص المعنوي الخاص في الإجرام المعلوماتي في عدّة أساليب، منها الإعتداء على الملكيّة، سرقة البيانات والأسهم، تحويل رأس المال، تخريب البيانات وغيرها من الجرائم. لكن ما يجعل الإعتداء على الشّخص المعنوي الخاص أكثر خطورة من غيره، كون الإجرام المعلوماتي المرتكب على هؤلاء يبقى سريّا حتّى لو إستطاعت المؤسّسة أو الشّركة معرفة الفاعل، وذلك للحفاظ على سمعة الشّركة أمام الزّبائن وعدم لفت إنتباه الرّأي العام لها [1] . وغالبًا ما تكون المصارف، المؤسّسات الماليّة، الشّركات والمؤسّسات الأكثر عرضة لهذا النّوع من الإجرام، وذلك نظرًا للمكاسب الماديّة المرتفعة المتتالية من هذه العمليّة، وهذا ما يضع القطاع الإقتصادي والمصرفي رهينة بيدّ المجرمين المعلوماتيين.

النّبذة الثّانية: الشّخص المعنوي العام

لم تكن الدّولة في الإجرام التقليدي عنصر جذب للمجرمين، إذ كانت تستطيع حماية مكتسباتها

[1] د. جنان الخوري، **الجرائم الإقتصادية الدولية والجرائم المنظمة العابرة للحدود**، المرجع السابق نفسه، ص: 170.

وموجوداتها ورأس مالها بإتّباع أساليب أمنيّة وقائيّة. لكن في ظلّ ظهور الإجرام المعلوماتي، أصبح التّساؤل يدور حول ما إذا كانت الدّولة ضحيّة لهذه الجريمة أم لا، وما إذا كانت الدّولة بتخلفها وعدم تكاملها وتطورها التّكنولوجي تجعل من ذاتها ضحيّة لهذا الإجرام [1].

في الحقيقة إنّ الإجرام المعلوماتي ليس فقط عابر للقارات والفئات العمرية والنّوع البشري، إنّما أيضًا أوجد في علم الإجرام نوعًا أساسيًا ومهمًا من الضحايا الّتي يمكن أن يعتدى عليهم، ألا وهي الدّولة بمؤسّساتها ومرافقها ومنشآتها. وذلك لعدّة أسباب منها إقتصاديّة ومنها إجتماعيّة وأهمّها سياسيّة، لفرض قواعد جديدة في الحرب القائمة بين الدّول في البيئة المعلوماتية. فيما يتمثّل الإجرام المعلوماتي الواقع على الدّولة في مهاجمة المواقع الرّسميّة وأنظمة الشّبكات الحكومية والّتي تستخدم تلك التطبيقات على المستوى المحلّي والدّولي، كالهجمات الإرهابية على شبكة الإنترنت، حيث تركّز على تدمير البنى التّحتية ومهاجمة شبكات الحاسوب وغالبًا ما يكون هدفها سياسي. أمّا بالنّسبة إلى دور الدّولة في جعل ذاتها ضحيّة لهذه الجريمة هي واقعة مثبتة، حيث أنّ عدم مواكبة التّطوّر التّكنولوجي على المستوى التّقني، الفنّيّ، القانوني، اللّوجستي والحمائي، جعل من ضعف الدّولة في البيئة المعلوماتية عامل جذب للمجرمين المعلوماتيين لإرتكاب جرائمهم نظرًا لسهولة إختراقها وصعوبة إكتشاف الجريمة.

بالنتيجة فإنّ الإجرام المعلوماتي لا يوفّر أحد، فإختلاف الدّوافع الجرمية يقتضي بالمقابل تنوّع وتعدّد في نوعيّة ضحايا هذا الإجرام. فالشخص المعنوي أصبح كالشخص الطّبيعي عرضة لإرتكاب جرائم العصر الحديث عليه، وخصوصًا الإجرام المعلوماتي الّذي يتّسم بالإجرام اللاعنفي والنّاعم والقادر بسهولة الوصول إلى أيّ شركة أو مؤسّسة ماليّة ببعض البرمجيات المعلوماتية، هذا إضافة إلى دخول الدّولة كنوع جديد من ضحايا الإجرام المعلوماتي ممّا يؤثّر على الأمن القومي وعنصر السّيادة.

إذًا المجرم المعلوماتي في الإجرام المعلوماتي هو ليس ذاك المجرم في الإجرام التّقليدي، بل هو مجرم

[1] د. جنان الخوري، المرجع السابق نفسه، ص: 160.

يتمتّع بصفات جديدة وسمات تميّزه عن غيره من المجرمين، يوظّف ذكاءه المعلوماتي في أعمال غير مشروعة ومجرمة، كما يستغل كونه شخصًا مرغوبًا فيه إجتماعيًا بحيث لا أحد يعترف بإجرامه إنّما يقدّرون ذكاءه المعلوماتي وإن وظّف لغايات جرمية ومهما كانت الدّوافع الّتي دفعته لإرتكاب عمله الجرمي. وتقع خطورة هذا الأمر على المجرمين المعلوماتيين القاصرين الّذين يجدون أنّ المجتمع يحفّزهم على إرتكاب إجرامهم المعلوماتي بدل لومهم، ممّا يؤدي إلى إصطدامهم بالقانون الّذي يعاقب على الفعل ولكنّه لا يستطيع وحده الحدّ من الخطورة الجرمية المستقبلية النّاتجة عن هؤلاء، من دون عمليّة تعاونية بين أطراف الجريمة: المجرم، الضّحيّة والمجتمع. أمّا على مستوى ضحايا الإجرام المعلوماتي فقد شهدنا على نوعيّة جديدة منهم وطرق مختلفة لوقوعهم في يد المجرمين المعلوماتيين، وأبرز هؤلاء كانوا يتمتّعون بسمات تشجّع المجرمين على إختيارهم كوسيلة لتحقيق هدفهم الجرمي.

لذلك وعلى ضوء علم الإجرام الّذي يهدف إلى تحديد أسباب الجريمة وصولًا إلى وضع حلول لها، سنقوم في القسم الثّاني من هذه الدّراسة بالتطرّق إلى المسؤوليّة الجزائية للإجرام المعلوماتي بين ردع المجرمين وضمانات الضّحايا. وذلك لتحقيق غاية علم الإجرام المتمثّلة بردع مجرمي المعلوماتية عن إرتكاب إجرامهم المعلوماتي، ووضع نظام قانوني وعملي للضحايا لحمايتهم وتجنيبهم الوقوع كضحايا لهذا الإجرام الحديث.

القسم الثّاني

المسؤوليّة الجزائية للإجرام المعلوماتي بين ردع المجرمين وضمانات الضّحايا

إنّ إعتبار الإجرام المعلوماتي من الجرائم المعاقب عليها في القانون يستتبع ترتيب المسؤوليّة الجزائية على الأشخاص الذين يرتكبون هذه الأفعال الجرمية ألا وهم المجرمون فيها. لكن المسؤولية الجزائية بشكلها التّقليدي لم تكن كافية لمواجهة الإجرام المعلوماتي وتداعياته الّذي يعتبر من الجرائم الحديثة، لذلك إعترضته العديد من الإشكاليّات والثّغرات الّتي لم يبحثها القانون ولا يمكن معالجتها من خلال قانون العقوبات اللّبناني الّذي ينظم الجرائم التّقليدية دون الحديثة. هذا الغياب في التّشريعات إنعكس سلبًا على ضحايا الإجرام المعلوماتي، فأدّى بدوره إلى نقص في الضّمانات الخاصّة بهم، بالإضافة إلى عدم ملاءمة العقوبات التّقليدية للإجرام المعلوماتي الحديث محليًا ودوليًا.

لذلك كان لا بُدّ من التّطرّق إلى المسؤوليّة الجزائية للإجرام المعلوماتي إنطلاقًا من أوجهها المعاصرة الّتي ظهرت مع ظهور هذا الإجرام من ناحية المجرم والضّحية وذلك في قسم أوّل. أمّا في القسم الثّاني فسنتطرّق إلى آثار الإجرام المعلوماتي على المجرم من جهة، وضمانات الضّحيّة من جهة أخرى، وصولًا إلى الأساليب التّقنيّة والقانونية الّتي تساعد على الحدّ منه ومواجهته والتّصدّي له.

الباب الأوّل

أوجه المسؤوليّة الجزائية المعاصرة الّتي يطرحها الإجرام المعلوماتي

بالرّغم من إمكانيّة تطبيق القواعد العامّة للمسؤوليّة الجزائية على المجرمين المعلوماتيين، إلاّ أنّه وبصدد التّحدّيات الّتي أحدثتها ظاهرة الإجرام المعلوماتي أصبحنا بحاجة إلى إعادة النّظر في كيفيّة ترتيب المسؤوليّة الجزائية على مجرميها. فقد أدّت هذه الظاهرة إلى إحداث تغيّرات على مستوى المساهمة الجرمية فيها، بحيث شهدنا على جرائم يأخذ فيها شكل التّعاون والمساهمة فيها الطّابع الجماعي وليس الفردي الّذي بدوره كان أساس المساهمة الجرمية في قانون العقوبات اللّبناني. بالإضافة إلى طرح العلاقة بين المجرم المعلوماتي المنفّذ والمجرم والأصلي المتخفّي، هذا الّذي جعل للمسؤوليّة الجزائية أوجه جديدة لم تكن موجودة فيما سبق. هذا الواقع الّذي فرضته الظاهرة الإجرامية المعلوماتية أدّى إلى بروز العديد من الإشكاليّات المؤثّرة في المسؤوليّة الجزائية، إمّا على صعيد القواعد الإجرائية أو على مستوى القواعد الموضوعية الّتي تعالج جرائم الأحداث في الجريمة المعلوماتية.

لذلك سنقوم في إطار بحثنا عن الأوجه الحديثة للمسؤولية الجزائية بالتطرق في فصل أوّل إلى المسؤولين جزائيًا عن الإجرام المعلوماتي، بينما في الفصل الثّاني سنتطرّق إلى الإشكاليّات المؤثّرة في ترتيب المسؤولية الجزائية في الإجرام نفسه.

الفصل الأوّل

المسؤولون جزائيًا عن الإجرام المعلوماتي

يثير الإجرام المعلوماتي التّساؤل عن نوع المسؤوليّة الّتي تترتّب على إرتكابه، بحيث قد يترتّب تنوّع في المسؤوليّة المثارة أو المترتّبة على الفعل. فبالرّغم من إمكانيّة إحاطة أحكام المسؤوليّة الجزائية في قانون العقوبات على الإجرام المعلوماتي، إلاّ أنّ بعض الثّغرات تبقى هناك، تلك الّتي وجدت مع بروز هذه الظاهرة الإجرامية، والّتي تؤدي في حال لم يتمّ معالجتها إلى منفّذ يتمكّن من خلاله المجرمين من التّهرّب من المسؤولية والعقاب. لكن بفعل الطّبيعة الخاصّة للإجرام المعلوماتي، كان لسلوك الضّحيّة فيه عامل مؤثّر في المسؤوليّة الجزائية في العديد من الحالات الّتي يمكن أن تجعل منها محل جذب للمجرمين، بناءً على أفعال ترتكبها بصورة القصد أو الخطأ.

وبناءً على ما تقدّم سندرس في هذا الفصل، المسؤوليّة الجزائية للمجرم المعلوماتي في مطلب أوّل، أمّا في المطلب الثّاني فسنتطرّق لمسؤوليّة الضّحيّة عن الإجرام المعلوماتي الواقع عليها، وذلك في محاولة لمعالجة بعض الثّغرات الّتي وجدت مع بروز الإجرام المعلوماتي.

المطلب الأوّل: المسؤوليّة الجزائية للمجرم المعلوماتي

قد يكون المسؤول عن الجريمة واحدًا عندما تقع الجريمة منه بمفرده، فيسأل عنها جزائيًا وحده. هذه الحالة لا تثير صعوبة إلاّ عندما يكون الشّخص هيئة إعتبارية أو معنوية، فتثور حينئذ مشكلة مسؤوليّة الهيئات المعنوية. لكن قد يكون المسؤولون عن الجريمة عدّة أشخاص أسهموا في إرتكاب جريمة واحدة بتوزيع الأدوار فيما بينهم، فتقوم بذلك مسؤوليتهم جميعًا وإن بصورة مختلفة، ويعبّر عنها بنظرية الإسهام في

الجريمة الّذييضمّ أربع صور لتحميل المسؤوليّة الجزائية، ألا وهم الفاعل والشّريك، المحرّض، المتدخّل، والمخبّئ[1].

لكنَّ صور المساهمة الجرمية بصورتها التّقليديّة أصبحت موضع نقاش بعد أن ظهر نوع جديد من الإسهام الجرمي، وهو الإسهام الجماعي الّذي أدّى إلى ضرورة البحث في المسؤوليّة الجماعية عن الجريمة الّتي ترتكبها الجماعة الإجرامية المعلوماتية. بالإضافة إلى ذلك، كان التّساؤل حول مسؤوليّة المجرم المنفّذ للإجرام المعلوماتي والّذي يعتبر عمله فنّي، ومسؤوليّة صاحب الأمر بإرتكاب العمل الجرمي والّذي يعتبر من رجال الأعمال أو ذوي الياقات البيضاء والتي تعتبر صورة جديدة من صور الإسهام الجرمي في الإجرام المعلوماتي.

لذلك سنناقش في هذا المطلب المسؤوليّة الجماعية عن الإجرام المعلوماتي وذلك في نبذة أولى. أمّا مسؤوليّة المجرم المنفّذ التّقني، والمجرم الخفي، مُصدِر الأمر بإرتكاب الإجرام المعلوماتي سنعالجهما في نبذة ثانية.

النّبذة الأولى: المسؤوليّة الجماعية عن الإجرام المعلوماتي

إنّ الحديث عن المسؤوليّة الجماعية لا يمكن أن يكون إلاّ في إطار عمل جرمي جماعي، يقوم به مجموعة من الأشخاص الّذين تربطهم غاية جرمية معيّنة. ويعتبر الإجرام المنظّم المحلّي والدّولي، أي العابر للحدود، الشّكل الأوّل للمسؤوليّة الجماعية.

ينطلق التّعريف القانوني للإجرام المنظّم من المنظّمات الإجرامية أكثر من إنطلاقه من الجريمة المنظّمة، وذلك لأنّ المنظّمة الإجرامية هي الأساس الّذي تنتشر إنطلاقًا منه الأنشطة الإجرامية المتعدّدة

[1] تم معالجة صور الإسهام الجرمي في الجريمة المعلوماتية بصورها الأربعة في مؤلف د. حسين محمد الغول، **جرائم شبكة الإنترنت والمسؤولية الجزائية الناشئة عنها**، دراسة مقارنة، مكتبة بدران الحقوقية، سنة 2017.

وعلى مدى واسع. حيث أنّ الجريمة المنظّمة عبارة عن عنف منظّم، بقصد الحصول على مكاسب ماليّة بطرق وأساليب غير شرعية. فتختلف عن الجريمة الإعتيادية بأنّها تأتي بعد تدبير وتنظيم وتنفيذ أفراد العصابة، وبأساليبها المتمثّلة في السّطو، الاحتلال، القتل والتّزوير [1]. لكن مع بروز جرائم العصر الحديث أبرزه الإجرام المعلوماتي، أصبح الإجرام المنظّم الّذي يعتمد على تضافر جهود الجماعة في تحقيق النّشاط الجرمي يشكّل تحدّي جديد لقانون العقوبات العام الّذي يعالج المساهمة الجرمية في شكلها التّقليدي. بالتّالي يشكّل عنصر التّنظيم في الجرائم المنظّمة سواء في الجرائم التّقليدية أم الحديثة، الأمر المستجد فيها والّذي ينتج عنه مخاطر هائلة، إتّساع في نطاق المساهمة الجزائية، وإنصهار الإرادات الجرمية في إرادة واحدة هي إرادة المنظّمة الإجرامية المعنيّة.

فالإجرام المعلوماتي كما بيّنا هو من الإجرام الحديث الّذي يمكن أن يتحقّق في شكلين، إمّا في شكل إجرامي فردي، أو المساهمة الجرمية العاديّة الّتي تعبر عن مجموعة من الإرادات الجرمية المختلفة [2]. وإمّا بشكل جماعي ويطلق عليه الإجرام المعلوماتي المنظّم، يكون فيه التّنظيم والتّخطيط والتّنفيذ بين مجموعة من الأفراد ضمن هيكليّة معيّنة، الأساس في النّشاط الإجرامي وينتج عنه إرادة واحدة هي إرادة المنظّمة الإجرامية.

لذلك كان للإجرام المعلوماتي المنظّم بعض الخصوصية في تحديد المسؤوليّة الجزائية، من أهمها أنّ هذا النّوع من الإجرام المعلوماتي يشكّل إجرامًا تقترفه مجموعة من الأشخاص، يثير تقسيم المهام داخل الجماعات الإجرامية إشكاليات تجاه نظرية قانون العقوبات التّقليدي الّذي يركّز على الجرائم المقترفة من خلال فاعلين منفردين، والّذي لم يَعُدّ العدّة الكافية لمواجهة الجرائم المقترفة من قبل جماعة معلوماتية ذات هيكليّة غامضة وخفيّة وذات ترؤس خفي.

---

[1] د. جنان الخوري، **الجرائم الإقتصادية الدولية والجرائم المنظمة العابرة للحدود**، المرجع السابق نفسه، ص: 211.

[2] د. حسين محمد الغول، **جرائم شبكة الإنترنت والمسؤولية الجزائية الناشئة عنها**، دراسة مقارنة، مكتبة بدران الحقوقية، سنة 2017، ص: 353.

فبدلًا من أن يتمّ ترتيب المسؤوليّة الجزائية بشكل فردي على الفاعلين، المشتركين، المتدخلين، المخبئين والمحرضين في الإجرام المعلوماتي حسب درجة إسهامهم في الجريمة، يجب علينا الحديث عن المسؤوليّة الجزائية للجماعة الإجرامية المعلوماتية وإعتبار هذا التّنظيم الجماعي كالكائن الواحد، الّذي يجب أن تفرض المسؤوليّة الجزائية عليه بشكل تسلسلي ومنظّم حسب هيكليّة الجماعة الإجرامية. إذ يعتبر كلّ فرد في هذه الجماعة مسؤول عن الجريمة المعلوماتية المقترفة إستنادًا إلى معيارين، الأوّل هو جسامة الجريمة المقترفة والّذي على أساسه يتمّ تحديد المسؤوليّة الأوليّة للجماعة ككلّ، أمّا المعيار الثّاني فهو مركز كلّ فرد في الجماعة الإجرامية الّذي منه يتمّ تحديد مستوى أو درجة المسؤوليّة الجزائية والعقاب الجزائي الأنسب لكلّ فرد من أفراد هذه الجماعة. فمثلًا جريمة إتلاف البيانات الإلكترونية إذا تمّت ضمن تنظيم إجرامي معلوماتي، فإنّ الجماعة الإجرامية ككائن واحد تُسأل عن الجريمة المقترفة، وذلك لإنصهار الإرادات الجرمية لأعضائها في إرادة واحدة ألا وهي إرادة المنظّمة الإجرامية. لكن يستعان في تحديد المسؤولية الجزائية والعقاب الجزائي لكلّ فرد من أفراد هذه الجماعة حسب موقعه التّنظيمي والتّنفيذي في الجماعة المذكورة، فرئيس المنظّمة عادة ما يجب أن ينال عقاب أشدّ من المنفّذ كونه هو من أصدر القرار. أمّا المنفّذ فكان قد قام بالأعمال التنفيذية فقط تحقيقًا لمصلحة الجماعة الإجرامية دون معرفته لأسباب هذا الفعل ودراسة نتائجه.

وبفعل كل ما تقدّم، أصبحنا اليوم وبفعل الإجرام المنظّم وخصوصًا على مستوى الإجرام المعلوماتي، نواجه تحديًا للمسؤوليّة الجزائية ليس فقط في السّياسة الجزائية وإنّما أيضًا لنظرية قانون العقوبات. حيث طرح الإجرام المنظّم إشكاليّة المسؤوليّة الجماعية والّتي ينتج عنها إمّا عقاب جماعي موحّد، أو عقاب جماعي يأخذ بالتّسلسليّة الهرمية في دور كلّ فرد من هذه الجماعة في الجريمة المقترفة. لكن ما نشهده اليوم من تطوّر على المستوى الجرمي ببروز الجماعات الإجرامية المنظّمة المحلّية من جهة والعابرة للحدود من جهة أخرى، وضعنا أمام ضرورة إعادة النّظر في قانون العقوبات اللّبناني بجعله بالإضافة إلى توجهه

ضدّ الأفراد، يجب أن يكون موجهًا ضدّ الجماعات الإجرامية المنظّمة الخفيّة أو المختبئة وراء أشخاص معنويين، يبرزون للعامّة على أنّهم يمارسون أعمالًا مشروعة ولكن الحقيقة تكون على عكس ذلك. ممّا قد يؤدّي نتيجة لهذا التّعديل والتّطوّر لقانون العقوبات لإنعكاسه على المسؤوليّة الجزائية، فإذا كنّا أمام جرم جماعي فيستتبع الأمر ترتيب المسؤوليّة الجماعية.

النّبذة الثّانية: مسؤوليّة المجرم الأصلي الخفي والمجرم المعلوماتي التّقني المنفّذ

إنّ الإجرام المعلوماتي بإعتباره من الإجرام الحديث يمكن إرتكابه بأوجه متعدّدة، إمّا من قبل مجرم معلوماتي يرتكب الفعل الجرمي بشكل فردي ولحسابه الخاص محققًا غاية جرمية معيّنة، وإمّا من خلال الجماعة الإجرامية المنخرط فيها والّتي يعمل لحسابها، فيتحمل المسؤولية الجزائية عن أعماله تبعًا للمسؤوليّة الجماعية للجماعة الجرمية كما بيّناها فيما سبق.

لكن طريقة إرتكاب الإجرام المعلوماتي تطوّر أيضًا بفعل إزدياد الإهتمام بهذا الإجرام من قبل رجال الأعمال أو ذوي الياقات البيضاء، بحيث أصبح يشكل بيئة جرمية يَصعُب إخضاعها لرقابة القانون، فيصعب إكتشاف الجريمة وملاحقة المجرمين فيها. كما يعتبر إجرام مستحدث يمكن من خلاله إرتكاب الفعل الجرمي بطريقة سريعة وفعّالة دون عنف، وبكسب أرباح وإيرادات عن طريق الأعمال غير المشروعة بشكل كبير وسهل. فجرائم ذوي الياقات البيضاء مصطلح يطلق على الجرائم غير العنيفة والمرتكبة لدوافع ماليّة من قبل رجال الأعمال وأصحاب النّفوذ [1].

وبالرّغم من كل هذه المغريات الّذي يقدمه الإجرام المعلوماتي الى أصحاب الياقات البيضاء، إلاّ أنّ إرتكابهم أيّ فعل جرمي سيّما عبر أفعال جرمية مرتكبة بواسطة تقنيّة المعلومات أو واقعة على تقنيّة

[1] FBI White-Collar Crime، FBI، مؤرشف من الأصل في 10 يونيو 2016.

المعلومات في حدّ ذاتها، يحتاج وبالدّرجة الأولى إلى شخص متخصّص في التّقنيّة المعلوماتية وخبير في فكّ الشّيفرات والرّموز الإلكترونية وإختراق البرامج الحمائية ونظم الأمان، وهذا غالبًا لا يتوفّر لدى أصحاب الياقات البيضاء الّذين يملكون المال والرّاغبين في تحقيق المزيد منه بطريقة غير مشروعة عبر الجريمة المعلوماتية. لذلك كان الحلّ لهؤلاء الإستعانة بأشخاص متخصّصين في إرتكاب الإجرام المعلوماتي، مقابل بدل مادّي عالي بالإضافة إلى تأمين التّغطية والحماية لهم عبر القنوات السّياسية وغير السّياسية. وعادة ما تكون الأهداف الجرمية محدّدة بشكل كبير للمجرمين المعلوماتيين المنفّذين للجريمة من قبل أصحاب الياقات البيضاء الّذين يتخفّون خلف هؤلاء. فوجود مجرمان، أوّلهما هو رجل أعمال يملك المال والنّفوذ والهدف الجرمي الثمين، وثانيهما شخص متخصّص بالتّقنيّة المعلوماتية يملك الخبرة والذّكاء المعلوماتي، وضعا المساهمة الجرمية أمام تحدّ جديد مؤثّر بشكل أو بآخر على المسؤوليّة الجزائية. فيطرح التّساؤل حول الأشخاص المسؤولين جزائيًا عن الإجرام المعلوماتي، وإذا ما كان هناك إختلاف في درجة ترتيب المسؤوليّة الجزائية ومسألة العقاب الجزائي بين المجرم التّقني المنفّذ والمجرم المتخفي صاحب المال والنّفوذ[1].

بالعودة إلى قانون العقوبات اللّبناني فإنّه لم يأتِ على ذكر هذه الحالة، إذ وفقا للمبادئ العامة للإسهام الجرمي يعتبر في المبدأ كل من المجرم المنفّذ أو المادّي، والمجرم المتخفي صاحب السّلطة والمال والنّفوذ، مجرمَين بنظر القانون بإرتكابهم للجريمة المعلوماتية ولو أنّه كان أحدًا منهم يعمل لحساب الآخر. لأنّ الإرادة الجرمية لم تكن متعيّبة أو منتقصة لحظة إرتكاب المجرم المادّي الفنّي للجرم، بل على العكس كان يعلم أنّه يرتكب جريمة معلوماتية لصالح شخص آخر وسواء نجح في تحقيق الجريمة أم لم ينجح سيتقاضى أتعاب فعله. أمّا بالنّسبة إلى طريقة ترتيب المسؤوليّة الجزائية على المجرم المادّي المنفّذ والمجرم المتخفي مصدر الأمر، يكون الإثنان مسؤولين عن الجريمة المعلوماتية، حيث يكون برأينا أنّ المجرم

[1] د. جنان الخوري، **الجرائم الإقتصادية الدولية والجرائم المنظمة العابرة للحدود**، المرجع السابق نفسه، ص: 108.

المتخفي صاحب المال والسّلطة هو الفاعل الأصلي للجريمة كونه يؤمّن المعدّات الجرمية، ويمدّ الفاعل المادّي بالمال ويؤمن حمايته، وكون الفعل الجرمي هو لحسابه الخاص. أمّا الفاعل المادّي أيّ الفنّي فهو شريك للفاعل الأصلي، وذلك كونه قد ساهم في إرتكاب الجريمة المعلوماتية لصالح الأخير عبر شراكة وتضافر جهود كل من المجرم المتخفي والمجرم المادّي، وهذا ما نصّ عليه قانون العقوبات في المادة 212 منه أنّ الشّريك هو كل شخص ساهم مباشرة في إرتكاب الجريمة.

من هنا حاولنا معالجة بعض الإشكاليّات الّذي يطرحه الإجرام المعلوماتي على مستوى المساهمة الجرمية الّتي تؤثّر على المسؤوليّة الجزائية والّتي من خلالها يلقى المجرم عقابه وتضمن بالمقابل الضّحيّة حقوقها، الّتي ما لبث لهذه الأخيرة أن لعبت دورًا في تحديد المسؤوليّة الجزائية للمجرم المعلوماتي إمّا من خلال مساهمتها بشكل مباشر فيها أو عن طريق خطأها وهذا ما سنعالجه في المطلب الثّاني.

المطلب الثّاني: لجهة مسؤوليّة ضحيّة الإجرام المعلوماتي

إنّ الإجرام الحديث وخصوصًا الإجرام المعلوماتي، يمثّل التّهديد الأكبر لإستقرار أمن المجتمعات والأمم، ويشكّل التّحدي الأبرز لتشريعاتها ومؤسّساتها وأفرادها. حيث بات الإجرام المعلوماتي يصيب ضحايا من نوع آخر مختلفة عن ضحايا الإجرام التّقليدي، وقد إنعكس هذا التطور لمفهوم المجرم والضّحيّة على المسؤوليّة الجزائية، فأصبحت الضّحيّة في بعض الحالات تشكّل بيئة جذب للمجرمين المعلوماتيين بسبب التّهور أو الإندفاع العشوائي لأفعالها الّتي تمارسها في البيئة المعلوماتية هذا من جهة، ومن جهة أخرى يشكّل الخطأ الّذي تقع فيه خلال غوصها في التّقنيّة المعلوماتية عوامل يمكن أن تؤثّر على المسؤوليّة الجزائية للإجرام المعلوماتي.

وبذلك أصبحت الضّحيّة مساهمة بشكل أو بآخر في بعض أنواع الإجرام المعلوماتي ممّا إنعكس على المسؤولية الجزائية فيها. وذلك وفقًا لدورين يمكن أن تلعبهما الضّحيّة في الإجرام المعلوماتي، أوّلهما دورهم المباشر في الإجرام المعلوماتي (نبذة أولى)، وثانيهما مسؤوليّة الضّحايا أنفسهم عن الأخطاء الّتي يرتكبونها (نبذة ثانية).

النّبذة الأولى: مساهمة الضّحيّة في الإجرام المعلوماتي

بدأ الإهتمام العلمي والتّركيز على الضّحايا (أو المجني عليهم) بعدما نادى الفقيه الإيطالي "جريسبيني" Jerispina، بضرورة دراسة دور الضّحيّة في إنتاج الجريمة [1]. وبظهور مدرسة الدّفاع الإجتماعي إهتمّت نظم السّياسة الجنائية في معظم الدّول الغربية على وجه الخصوص بالضّحيّة، وأشار "مارك آنسل" Marc Ansel إلى ذلك بقوله: " من الواضح، عندما ندقق في مستوى السّياسة الجنائية، والّتي ينبثق أصلها من الدّفاع الإجتماعي، أنّ مشكّل الضّحيّة يمثّل أهمّية معتبرة؛ ويجب أن يؤدي إلى إعادة التّفكير في تنظيم رد الفعل الإجتماعي ضد الإجرام". ويُعد ذلك إعترافًا منه بفضل علم الضّحيّة على ما أتى به من جديد في العلوم الإجرامية [2]، وخصوصاً في الجريمة المعلوماتية لما تتمتّع به الضّحيّة المعلوماتية من صفات تساعد على إرتكاب الجريمة.

لذلك يمكننا القول أنّ تحديد دور الضّحيّة كسبب في وقوع الإجرام المعلوماتي عليهم يعتمد على وصف الضّحايا وخصائصهم، وعلى تصنيفاتهم المختلفة، والعوامل البيئية المساعدة في جعلهم ضحايا هذا

[1] Nathalie Pignoux, **La ré paration des victimes d'infraction pénales**, edition l'harmattan, 2008, collection sciences criminelles.

[2] د. حميد بن ناصر الحجري، ضحايا الجريمة قبل وبعد وقوعها، شرطة عمان https://www.rop.gov.om/media/arabic/articledetails.aspx?articleid=35 ، تاريخ الدخول إلى الموقع 2020/2/7.

الإجرام. بالإضافة إلى أنّ العوامل الدّاخلية والخارجية تختلف من مجتمع إلى آخر وفقًا لنوع الأنظمة السائدة في ذلك المجتمع. ففي الحين الّذي نتمكن فيه من عزو سبب الإجرام إلى عوامل تتعلّق بالجاني في بلد يتّسم بالإستقرار السّياسي والإقتصادي والأمني، فإنّنا قد نلوم الضّحيّة الّذي يمنح الفرصة في مكان تَغلُب عليه الفوضى وعدم الإستقرار، إذ إنّ دور الضّحيّة نسبيّ ويختلف بإختلاف المواقف وأنماط الجرائم وملابسات وقوعها.

ونرى أنّ عدم إحتراز المجني عليه وتشكيله لحالة جذب للمجرمين المعلوماتيين من أهم الأسباب الّتي تلعب فيها الضّحيّة دورًا في إرتكاب الإجرام عليها. بناءً على ذلك، قدّم أستاذ علم الإجتماع الجنائي الأمريكي ورئيس معهد علم الإجرام في جامعة بنسلفانيا، "وولف قانق" Wolfgang، عام 1958م في كتابه "أنماط جرائم القتل الجنائية" الّذي فجّر كثيرًا من الجدل خاصة من قبل منظمات المجتمع النّسائية، الّتي إعترضت على تقديمه لمفهوم الإستفزاز والّذي ترى فيه هذه المنظمات بأنه يحمِل معاني مبطّنة ضدّ النّساء ويَنِمّ عن عنصرية ذكورية، كونهن أكثر من يقعن ضحايا للجريمة. حتّى أنّه وصفهن بأنّهن مستفزّات للجاني الّذي تأتي مبادرته للقيام بالفعل الإجرامي كرد فعل على إستفزاز الضّحيّة. فهو أوّل من أشار إلى دور الضّحيّة من خلال تهوّره وإستفزازه، حيث وجد أنّ 25%من جرائم القتل سببها تهوّر المجني عليهم وإستفزازهم للجاني من خلال المواجهة معه سواء بالألفاظ أو الكلمات أو الحركات[1].

ففي الإجرام المعلوماتي، عدم إحتراز المجني عليه ومساهمته في إرتكاب الإجرام المعلوماتي أقرب من دور الضّحيّة في الجرائم التّقليديّة، لأنّ الأفعال الجرمية تتمّ في بيئة إفتراضية يسهل إخفاء مرتكبيها وبالمقابل يسهل التعرّف على الضّحايا فيها. ونرى أنّ الضّحايا عادة ما يجذبون المجرمين لإرتكاب الإجرام

[1] Cédric Ribeyne, **La victim de l'infraction pénale, Nouveaité**, (Thémes et commerciales), edition, 2016, Dalloz.

المعلوماتي بحقهم، وذلك إمّا بسبب تهورهم في إستعمال النظم المعلوماتية والفضول غير المبرّر لديهم وإمّا بكونهم يستفزّون المجرمين عبر عرض أمور تجعل منهم صيدًا ثمينًا.

ويُطرح الحديث عن دور الضّحيّة في إرتكاب الإجرام المعلوماتي أيضًا في حالة عدم إحتراز الضّحيّة بالدّخول إلى مواقع محرّم الدّخول إليها، إستفزاز أو جذب المجرم المعلوماتي بشكل غير عادي عبر الحشرية المفرطة في التّعرّف على كلّ ما هو جديد في البيئة المعلوماتية دون أخذ إحتياطات حمائية. لذلك أصبح دور الضّحيّة في المساهمة في الإجرام المعلوماتي يشكّل نقلة نوعيّة في المسؤوليّة الجزائيّة، بحيث تتوزّع المسؤوليّة بين المجرم من جهة والضّحيّة من جهة أخرى، وذلك حسب كل جريمة والوقائع الّتي تثيرها، وما إذا كانت الضّحيّة بفعل فعلها قد ساعدت على إرتكاب الإجرام بحقها. أمّا إذا كان دور الضّحيّة لا يغيّر من الجريمة بشيء، فيبقى المجرم هو المسؤول الوحيد عن إرتكابه للإجرام المعلوماتي ويبقى المجني عليه هو الضّحيّة الّتي إرتكب الإجرام عليها، بالرّغم من تهوّره وإستفزازه وجذبه للمجرم المعلوماتي، وذلك لأنّ نشاطه لم يسفر عن أيّ مساعدة أو تدخل إيجابي او سلبي يمكن أن يسهل إقتراف الجريمة.

لذلك إنقسم الفقه في تحديد دور الضّحيّة في إرتكاب الجريمة، فمنهم من إعتبر أنّ مسؤوليّة المتّهم كانت تقاس على خطورة الفعل الّذي قام به، فإذا كان الفعل يشكّل خطورة عالية فتكون العقوبة مشدّدة، أمّا إذا كان لا يشكّل خطورة كبيرة تكون العقوبة مخفّضة. ثم بعد ذلك، وفي طور الإهتمام بشخصيّة المجرم في تقرير الجريمة والعقاب، نادى البعض من الفقهاء أنّ المجرم لديه عوامل وأسباب تدفعه لإرتكاب الفعل الجرمي، وبالتّالي في هذه الحالة مسؤوليته لا تقوم على أساس خطورة الفعل إنّما على درجة الخطورة الإجرامية الكامنة فيه. وفي ظلّ الحديث عن دور الضّحيّة في إرتكاب الجريمة، فإنّ بعض الفقهاء يقولون

أنّ مسؤوليّة الجاني لا تقوم على أساس خطورة الفعل ولا على أساس الخطورة الإجرامية الكامنة فيه، إنّما تقاس مسؤوليته على أساس مدى مساهمة الضّحيّة في وقوع الفعل عليه [1].

بالمقابل، فإنّ الفقهاء الّذين يأخذون بدور الضّحيّة في إرتكاب الجريمة يقولون أن الجريمة عندما تقع، لا تُخلق عند الجاني من العدم، إنّما هي مجموعة من الإيحاءات والعوامل والصّفات والخصائص الّتي تجذب الجاني لإرتكاب الفعل على المجني عليه وهي تختلف من حالة إلى أخرى، فلولا وجود هذه الصفات والخصائص لما كانت الجريمة ستُرتكب. وعلى هذا الأساس فإنّ هذه العوامل الّتي تجذب الجاني لإرتكاب الجريمة يمكن أن يكون للضحيّة دورًا ثانويا او أساسيا فيها [2] .

وبناءً على ما تقدّم، إنّ أغلب جرائم الإجرام المعلوماتي من وجهة نظرنا لا تُخلق من العدم، إنّما من أسباب ومعطيات وتصرّفات وعوامل داخلية وخارجية، كما تشكّل الضّحيّة المعلوماتية في بعض الأحيان جزءًا لا يتجزّأ من هذه الدّوافع والعوامل الّتي تؤدي لإرتكاب الإجرام المعلوماتي عليها. ولكن بالرغم من الأخذ بدور الضّحيّة في الإجرام المعلوماتي، إلاّ أنّه لا يمكن أن تقاس مسؤوليّة الجاني عن إرتكاب الإجرام المعلوماتي على أساس مساهمة الضّحيّة في وقوع الفعل الجرمي عليه، وفي الوقت عينه لا يمكن تجاهل هذا الدور الّذي تلعبه الضّحيّة في إرتكاب الجريمة. ذلك لأن هذا الدور نسبيّ وغير موجود في كافّة الجرائم المرتكبة في البيئة المعلوماتية، وعليه يجب العودة إلى قياس المسؤوليّة على أساس الخطورة الإجرامية للفاعل مع الأخذ بمساهمة الضّحيّة في إرتكاب الإجرام المعلوماتي عليها كأسباب تخفيفية للعقاب أو معفيّة منه حسب كل حالة على حدة، مع إعطاء القضاء السّلطة التّقديرية في تحديد هذه الأسباب.

---

[1] برنامج دفاعكم: دور الضّحيّة في إرتكاب الجريمة، مجرد نظرية أم واقع يستوجب المراجعة، قناة النهار، https://www.youtube.com/watch?v=ZpiMOPZn5sI، تاريخ الدخول إلى الموقع 2019/11/3.

[2] Fawn T. Ngo, Raymond Paternoster, **Cybercrime Victimization –An examination of In–dividual and Situational level factors**, International Journal of Cyber Criminology, Vol 5, Issu 1 January, July 2011, page: 774.

النّبذة الثّانية: خطأ الضّحيّة عن الإجرام المعلوماتي

تختلف مساهمة الضّحيّة في الإجرام المعلوماتي عن خطئها فيه، إذ تتعلّق مساهمة الضّحيّة في الإجرام المعلوماتي بفعل إيجابي تقوم به الضّحيّة يتمثّل في الإستفزاز أو التّهوّر أو فعل جذب من الضّحيّة إلى المجرم، فيؤثر بشكل مباشر أو غير مباشر على مسؤوليّة المجرم المعلوماتي. بينما يُعتبر خطأ الضّحيّة عن الإجرام المعلوماتي متمثلًا في قلّة الإحتراز أو الإهمال أو مخالفة القوانين والأنظمة. فيتحقّق خطأ الضّحيّة في عدم إتّباع أنظمة حماية متوفرة له، وإتّباع إجراءات حمائية من شأنها أن تحد من الهجمات الإلكترونية وتمنع إختراق النّظام المعلوماتي. وذلك عبر إتّباع أدوات وأنظمة الأمان الّتي سيأتي الكلام عنها لاحقًا. لكن ما تطرحه إشكاليّة خطأ الضّحيّة عن الإجرام المعلوماتي الواقع عليها هي تأثيرها على مسؤوليّة المجرم في حال تحقّقت[1]، وما إذا كانت مساهمة الضّحيّة في إرتكاب الإجرام المعلوماتي تماثل الخطأ فيها من جهة المسؤوليّة أيضًا.

بالعودة إلى ما بيّناه في النّبذة السّابقة عن مساهمة الضحية في إرتكاب الإجرام المعلوماتي ودورها المباشر فيه، تحدّثنا عن أنّه لا مجال لتجاهل دور الضّحيّة فيها في قياس المسؤوليّة الجزائيّة للمجرم. فنرى أنّ دور الضّحيّة يؤثّر على المسؤوليّة الجزائيّة للمجرم المعلوماتي سواء بشكل مباشر أو غير مباشر، لكن في الحديث عن خطأ الضّحيّة عن الإجرام المعلوماتي الأمر يختلف بشكل كبير عن ما هو معمول به في مساهمة الضحية في الإجرام المعلوماتي لناحية تحديد مسؤوليّة المجرم. فخطأ الضّحيّة، بالرّغم من أنّه يشكّل نوعًا ما خطأ من الضّحيّة بعدم إتّباع إجراءات الأمان الحمائية الّتي يمكن أن تعترض الإجرام المعلوماتي وتحد من خطورته، إلاّ أنّ هذا الخطأ لا يبيح للمجرم أن يقوم بإستغلاله لإرتكاب جريمته[2]. ذلك لأنّ الحق في

[1] د. جنان الخوري، **الجرائم الإقتصادية الدّوليّة والجرائم المنظمة العابرة للحدود**، المرجع السابق نفسه، ص: 160.

[2] Kaitlyn N. Ryan1, Tracey Curwen, **Cyber–Victimized Students– Incidence, Impact, and Intervention**, October–December 2013, page: 1 –7.

الخصوصيّة وحماية البيانات وعدم إستغلال التّقنيّة المعلوماتية في أمور غير مشروعة تشكّل قواعد إلزاميّة يقتضي عدم مخالفتها، وبمجرّد مخالفة هذه القواعد يتحقّق الجرم المعلوماتي بغض النّظر عن الخطأ الّذي إرتكبته الضّحيّة من ناحية عدم إتّباعها نظم الأمان والحماية الخاصّة.

ولا يمكن قياس هذا التّحليل المتعلّق بنفي أي تأثير بين خطأ الضّحيّة عن الإجرام المعلوماتي ودرجة مسؤوليّة المجرم عن الجريمة نفسها على مساهمة الضحية في الإجرام المعلوماتي، وذلك لأنّ فعل الضحية الأخير يتمثّل في فعل تدخل من الضّحيّة في السّاحة الجرمية أو يهيئ بطريقة ما للساحة الجرمية في البيئة المعلوماتية أو يضع نفسه ضحيّة في السّاحة الجرمية المعلوماتية الّتي تؤدي إلى وقوع الجرم المعلوماتي عليه، فيشكّل فعله عامل مساعد يجذب المجرم المعلوماتي إليه.

لذلك بناءً على ما تقدّم، يعتبر مساهمة الضحية في الإجرام المعلوماتي مؤثّر على مستوى المسؤوليّة الجزائيّة للمجرم المعلوماتي ولكن بشكل نسبيّ، حيث يختلف من جريمة إلى أخرى. بينما يُعتبر خطأ الضّحيّة عن الإجرام المعلوماتي غير مؤثّر على المسؤوليّة الجزائيّة للمجرم المعلوماتي إذ يبقى وحده يتحمّل مسؤوليّة الفعل الّذي أتاه.

هذا ولم تنتهِ المسؤوليّة الجزائية من التعرّض لأساسها القانوني فقط، وإنّما رافق ظهور الإجرام المعلوماتي العديد من الإشكاليّات المؤثرة بشكل مباشر أو غير مباشر على النّظام القانوني للمسؤوليّة الجزائية، والّذي يتعلّق بأمور عمليّة إجرائية وقانونية ملحة وهذا ما سنعالجه في الفصل الثّاني من هذا الباب.

الفصل الثّاني

الإشكاليّات المؤثّرة في المسؤوليّة الجزائية

عادةً ما يستفيد المجرمون من عدم أو نقص التّجريم في النّصوص القانونية، ويستغلّون الثّغرات القانونية إمّا على مستوى القواعد الإجرائية أو الموضوعية، للتهرّب من الملاحقة والعقاب. ولم يكن الإجرام المعلوماتي بمنأى عن هذا الأمر، إذ كانت الثّغرات القانونية تعتري عملية تجريم الإجرام المعلوماتي قبل النّص على قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي اللّبناني والّذي وضّح وجرّم الأفعال الجرمية المرتكبة بواسطة تقنيّة المعلومات أو الواقعة على تكنولوجيا المعلومات نفسها وأنزل العقاب بمجرميها. كما وضع آليّات الملاحقة والتّحقيق والمحاكمة، وحدّد طرق الإثبات فيها، ولكنّها لم تخلُ من بعض الثّغرات والصّعوبات الّتي يستفيد منها المجرمون المعلوماتيون، فتؤثر بدورها على حقوق الضّحايا والّتي سنتناولها في المطلب الأوّل.

هذه الإشكاليّات على مستوى مراحل الملاحقة والتّحقيق كان قد تنبّه لها الفقهاء ورجال القانون والمجتمع الدّولي المعنيّ بهكذا مواضيع. ولكن بسبب التّوسع الحاصل على مستوى الأشخاص الّذين يرتكبون الإجرام المعلوماتي، والّتي كان فيها للمجرم المعلوماتي الحدث النّصيب الأكبر لما يمكن أن يتمتّع به من ذكاء ذهنيّ حيويّ، أصبحت دراسة مسألة الأهليّة من ناحية الإدراك والوعي والتّمييز مقابل الذّكاء الذّهني أمرًا ضروريًا لمعرفة ما هو وضع القاصر تجاه المسؤوليّة الجزائيّة، إضافة الى مدى ملاءمة قانون الأحداث اللبناني على الحدث المعلوماتي والّتي سنعالجها في المطلب الثّاني.

المطلب الأوّل: على مستوى القواعد الإجرائية

صحيح أن النّقص كان متواجدًا في التّشريع لناحية مراحل الملاحقة، التّحقيق، المحاكمة، وعمليّة الإثبات الإلكتروني. لكن لا شكّ أنّه لا زال هناك العديد من الصّعوبات الّتي تعترض الإجرام المعلوماتي، وتُأمّن للمجرم مساحة واسعة لإرتكاب إجرامه المعلوماتي مستفيدًا من الثّغرات الموجودة في النّظام القانوني والّذي يؤثر بشكل أو بآخر على ضمانات ضحايا هذا الإجرام ويحد من التطبيق الفعلي للمسؤوليّة الجزائية. لذلك كان لا بُدّ من الحديث عن هذه الثّغرات والصّعوبات الّتي تعترض مراحل الملاحقة والتّحقيق في الإجرام المعلوماتي في نبذة أولى، وعمليّة الإثبات الإلكتروني والإختصاص في نبذة ثانية، مع التّطرّق في كلا النّبذتين إلى موقف التّشريع اللّبناني منهما.

النّبذة الأولى: الملاحقة والتّحقيق

تُواجه عملية التجريم للإجرام المعلوماتي اليوم صعوبة في إجراءات الملاحقة والتّحقيق، المتمثّلة في إخفاء الجريمة وسهولة وسرعة محو أو تدمير الأدلّة فيها، والضّخامة البالغة لكميّة البيانات المراد فحصها على الشّبكة. كذلك تبرز صعوبات في مسائل جمع الأدلّة من المعاينة والتّفتيش والضّبط وغيرها من الإجراءات، فضلًا عن الطّابع العالمي الّذي تمتاز به هذه الجرائم لكونها من الجرائم الّتي تتجاوز عنصري الزمان والمكان، فينتج عن ذلك تهرب المجرمين من الجزاء والعقاب وهدر لحقوق الضّحايا بسبب هذا العجز في كل مرحلة من مراحل الملاحقة والتّحقيق، ويؤدي إلى تناقص مفهوم العدالة الجزائية الإجرائية مقابل الإفلات من العقاب.

1. الملاحقة

يقصد بالملاحقة عمليّات التّحرّي والإستقصاء، حيث يتمّ بواسطتها جمع المعلومات عن الجريمة وكشفها من خلال عدّة عمليّات تقوم بها الجهات المختصّة. تعتبر إجراءات التّحري والملاحقة وجمع الأدلّة المرحلة الأولى من إجراءات إثبات الجريمة [1].

وقد أعطى المشرّع اللّبناني في قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي في المادّة 131 من الفصل السّابع منه، إجراءات التّحرّي وضبط الأدلّة وحفظها في جرائم المعلوماتية إلى الضّابطة العدليّة، ويؤازره مكتب مكافحة جرائم المعلوماتية الّذي أنشئ سنة 2005 والّذي يعود إلى مديريّة قوى الأمن الدّاخلي. وهو يتحرّك في الدّعوى وفقًا لإشارة النّيابة العامّة المختصّة إمّا بناءً على معلوماته الخاصّة، أو بناءً على شكاوى المواطنين. كما أشار المشرّع اللّبناني في القانون نفسه من المادّة 123 و124 منه على كيفيّة ضبط الأدلّة المعلوماتية، حفظها، تحليلها، فحصها، نقلها، إستنساخها وكيفيّة الحفاظ عليها من أيّ تشويه أو تغيير يمكن أن يطالها. فضلًا عن أنّ القانون نفسه في المادّة 126 قد أعطى حقوق للنّيابة العامّة، بحيث يمكنها تقرير وقف خدمات إلكترونية أو حجب مواقع إلكترونية أو تجميد حسابات بصورة مؤقتة لمدّة أقصاها ثلاثين يومًا قابلة للتجديد مرة واحدة بقرار معلّل. كذلك يحق لقاضي التّحقيق والمحكمة تقرير ذلك بصورة مؤقتة لحين صدور الحكم النّهائي في الدّعوى.

لكن ما لم يحدّده قانون المعاملات الإلكترونية هو كيفيّة الكشف عن الجرائم الإلكترونية، وذلك يتمّ بوضع برمجيات حاسوبية معيّنة خصوصًا فيما يخصّ جرائم القرصنة أو نشر المواد الإباحيّة. إذ يُعتبر إستحداث الأدوات البرمجية الحاسوبية الّتي من خلالها يُمكن التّعرف على الأنماط الإجرامية مسألة لا غنى عنها في كشف الجريمة، نظرًا لضخامة حجم المعلومات المتوافرة في شبكة الإنترنت. فهناك وسيلتان

[1] د. حسنّ عثيذ هجيج، صفاء كاظى غازي، **آثار جريمة قرصنة البريد الإلكتروني**، جامعة القادسية، مجلة القادسية للقانون والعلوم السياسية، العدد الثاني، المجلد السابع، كانون الأول 2016، ص: 175.

لأعضاء الضّبط القضائي لغرض الحصول على البيانات المتعلّقة بإرتكاب الجريمة من نظام حاسوب، وهما تستندان إلى معايير تقنيّة وقانونية [1]، تتمثّل بما يأتي:

1. يتمّ الحصول على المعلومات من الموقع نفسه الّذي تمّ من خلاله إرتكاب الجريمة، بعد أن يتمّ إكتشافه بإستخدام البرمجيات الحديثة.
2. يتمّ الحصول على المعلومات عن طريق إعتراض، أو رصد البيانات المنقولة من الموقع، أو إليه، أو في إطاره.

أمّا إذا كانت الجريمة مشهودة كما لو تمّ ضبط الفاعل وهو يستخدم موقع الإنترنت لإرتكاب إحدى الجرائم، فعلى عضو الضّبط القضائي إخبار قاضي التّحقيق والإدّعاء العام بوقوع الجريمة. ثم ينتقل فورًا إلى محل الحادثة، ويسأل المتّهم عن التّهمة المُسندة إليه، ويضبط كل ما يظهر أنّه أستُعمل في إرتكاب الجريمة من مخرجات ورقيّة وشرائط وأقراص ممغنطة وغيرها من الأشياء، الّتي يُعتقد أن لها صلة بالجريمة. كما يَسمع أقوال من يُمكن الحصول منه على معلومات وإيضاحات في شأن الحادثة ومرتكبها ويُنظّم محضرًا بذلك.

وبشكلٍ عام، على المكلّفين بمعاينة مسرح الجريمة إتّباع جملة من الإرشادات الّتي قد تُسهم بإزالة الغموض المحيط بملابسات إرتكاب الجريمة [2]، وذلك على الشكل التّالي:

1. التّحفظ على الأجهزة وملحقاتها والمستندات الموجودة من مخرجات ورقيّة وشرائط وأقراص ممغنطة وغيرها من الأشياء الّتي يعتقد أن لها صلة بالجريمة.
2. إثبات الطّريقة الّتي تمّ بواسطتها إعداد النّظام والعمليّات الإلكترونية، وخاصّة ما تحتويه السّجلات الإلكترونية التي تزوّد بها شبكات المعلومات لمعرفة موقع الإتصال، ونوع الجهاز الذي تمّ عن طريقه الدّخول إلى النظام.
3. عدم نقل أيّ مادّة متحفّظ عليها من مسرح الجريمة قبل التّأكد من خلو المحيط الخارجي بموقع

[1] عبد الله دغش العجمي، **المشكلات العملية والقانونية للجرائم الإلكترونية**، دراسة مقارنة، جامعة الشرق الأوسط، سنة 2014، ص:88.

[2] د. حسنّ عثيذ هجيج، صفاء كاظى غازي، **آثار جريمة قرصنة البريد الإلكتروني**، المرجع السابق نفسه، ص: 176.

الحاسب الآليّ من أيّ مجالات لقوّة مغناطيسية يُمكن أن تسبب في محو البيانات المسجّلة عليها.

4. إثبات حالة الكبلات المتّصلة بمكوّنات النّظام كلّه، وذلك لإجراء مقارنة لدى عرض الأمر على القضاء.

وبناءً على ما تقدّم، إنّ أكثر ما نحتاجه اليوم للتّصدي للجريمة المعلوماتية وإلقاء القبض على المجرمين وإنصاف ضحايا الإجرام المعلوماتي، هو في وضع آليّة سريعة لإجراء عمليّة الملاحقة وذلك يتمّ عبر تعديل قانوني يحدّد الوسائل الّتي يمكن إتّباعها في عمليّة الملاحقة، والتّقصي عن الجريمة تتلاءم مع التّطوّر الّذي شهدته التّقنيّة المعلوماتية، بالإضافة إلى التّدريب المستمر والفعال للأشخاص الذين يقومون بعمليّة الملاحقة، مع الإشارة إلى أنّه هناك العديد من الجرائم الواقعة على الإناث لا يتم التبليغ عنها خوفًا على سمعتهن وهذا ما يؤثر بشكل مباشر على عمليّة الملاحقة وتقصي الجريمة.

2. التّحقيق

أمّا التّحقيق هو بذل الجهد للكشف عن الحقيقة، وهو مجموعة من الإجراءات تقوم بها السّلطة المختصّة بالتّحقيق وفقًا للشروط والأوضاع الّتي يحدّدها القانون، بهدف الكشف عن الحقيقة في شأن الجريمة لتقرير مدى لزوم محاكمة المدّعى عليه أو عدم لزومها [1]. ونظرًا لكون التّحقيق يهدف للكشف عن الحقيقة لتحضير الدّعوى، لذلك يجب الإسراع في إجراءاتها لأنّ أيّ تأخير يؤدّي إلى ضياع أدلّة الجريمة.

إنّ الإشكاليّة الّتي يمكن أن تطرأ على إجراءات التّحقيق تتمثّل في معرفة الوسائل الّتي من خلالها يمكن أن تتمّ عبرها هذه العمليّة. وكون عمليّة التّحقيق عمليّة فنّيّة، فإنّ إجرءاتها في الجرائم التّقليديّة عادة تتمّ بواسطة مجموعة إجراءات تقليديّة وهي المعاينة، الشّهادة، الخبرة، التّفتيش والإستجواب. ونظرًا لكون مرتكب الجريمة المعلوماتية يترك آثارًا إلكترونية ذات طابع غير مادي، لذلك يجب إتّباع إجراءات التّحقيق بالوسائل الإلكترونية، وتتمثّل بالمعاينة الإلكترونية، الشّهادة، الخبرة والتّفتيش الإلكتروني.

[1] د. حسيّ عثيذ هجيج، صفاء كاظى غازي، **آثار جريمة قرصنة البريد الإلكتروني**، المرجع السابق نفسه، ص: 179.

بيد أنّ عمليّة المعاينة تعتبر إجراء، بمقتضاه ينتقل المحقّق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلّقة بالجريمة وكيفيّة وقوعها، وكذلك كشف الأشياء الّتي تفيد في كشف الحقيقة. فمرتكب الجريمة الإلكترونية كالقرصنة مثلًا، يترك آثارًا رقميّة في مسرح الجريمة، قد تتعلّق بشبكات الإتصال أو المواقع المرتبطة بها، والّتي تخترق من قبل القراصنة. في حين أنّ الشّهادة يُعتمد فيها على الشّاهد المعلوماتي، ولا تختلف الشّهادة في جريمة إلكترونية عن الشّهادة في الجرائم العادية. كما يجب على القائمين في التّحقيق سماع، أي الشّهادة، من أيّ شخص تكون لديه معلومات عن كيفيّة الإختراق، الدّخول لنظام المعالجة الآليّة، الخبرة الإلكترونية والتّفتيش الإلكتروني. أمّا بالنّسبة إلى الخبرة المعلوماتية فإنّ الخبير المعلوماتي هو الشّخص الّذي تعمّق بدراسة العمل الإلكتروني وأصبحت خبرته كبيرة حيث تُمكّنه هذه الخبرة من إبداء الرأي الإلكتروني الرقمي.

عقب ذلك، فقد أقرّ المشرّع اللّبناني في قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي الّذي يحمل الرقم 81 في المادّة 12 منه في الفقرة الثّانية، على أنّ للقاضي أن يطلب من الفرقاء تقديم جميع الآثار الإلكترونية الّتي بحوزتهم، أو تكليف خبير البحث عنها، كما يمكنه الإستعانة بالخبرة الفنّيّة. إذن فإنّ الخبرة المطلوبة هي خبرة إلكترونية وليست خبرة عادية. بينما التّفتيش يقصد به تقصي الأدلّة لأجل ضبطها من أجل الإستعانة بها للوصول إلى الحقيقة، حيث يجب ضبط كل ما ينتج عن التّفتيش من أدلّة بطريقة علميّة وفنّيّة. علاوة على ذلك، فإنّ عمليّة التّفتيش تحتاج إلى إتباع بعض الإجراءات، لتكون صحيحة وغير باطلة، والّتي تتمثّل بتلك الّتي نصّ عليها قانون المعاملات الإلكترونية في الفصل السّابع منه.

النّبذة الثّانية: الإثبات الإلكتروني والإختصاص المكاني

1. الإثبات

يقصد بالإثبات الإلكتروني، إقامة الدّليل على وقوع هذه الجريمة أو عدم وقوعها لكي يتمّ إدانة المتّهم أو براءته. بعبارة أخرى، الإثبات هو كل ما يؤدّي إلى إثبات وقوع الجريمة، حتّى يمكن توجيه التّهمة إلى المتّهم وإصدار الحكم العادل. من أدلّة الإثبات في الجرائم الإلكترونية، الآثار المعلوماتية المستخرجة من أجهزة إلكترونية والّتي تكون عبارة عن أدلّة رقميّة أو معلوماتية نصيّة، صورية أو صوتية. كما تعتبر الأدلّة الإلكترونية سندات إلكترونية، أو بيانات ثبوتية يكون إستخراجها بشكل رقمي، يمكن طباعتها على شكل ورق والإستفادة منها في إثبات الجريمة [1] .

كذلك عرّف قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي في المادّة 121 منه الآثار المعلوماتية، الّتي إعتبرها من قبيل الأدلّة الرقميّة أو المعلوماتية، بأنها البيانات الّتي يرتكبها الأشخاص بصورة إرادية أو لا إرادية على الأنظمة، قواعد البيانات، الخدمات المعلوماتية والشّبكات المعلوماتية. وتابع المشرّع في المادّة نفسها، بأنّ الأدلّة المعلوماتية تتضمّن التّجهيزات المعلوماتية، البرامج، البيانات، التّطبيقات، الآثار المعلوماتية وما يماثلها. كما جاء في الفصل الثاني من الباب الأول في المادّة السابعة من القانون نفسه، أنه يُقبل السّند الإلكتروني في الإثبات، وتكون له ذات المرتبة والقوّة الثّبوتية الّتي يتمتّع بها السّند الخطي المدوّن على الورق، شرط أن يكون ممكنًا تحديد الشّخص الصّادر عنه وأن ينظّم ويحفظ بطريقة تضمن سلامته.

تباعًا لذلك، ورد في المواد 8، 9، 10 و12 شرح طرق إثبات الأسناد الإلكترونية، ولكنّ المشرّع لم يتطرّق إلى وسائل الإثبات في جرائم المعلوماتية ولا في غيرها، سوى أنّه أشار في المادّة 12 على أن

[1] ثنيان ناصر آل ثنيان، **إثبات الجريمة الإلكترونية**، رسالة مقدمة للحصول على شهادة الماجستير، جامعة نايف العربية للعلوم الأمنية، سنة 2012، ص: 70.

للقاضي أن يطلب من الفرقاء تقديم جميع الآثار الإلكترونية الّتي بحوزتهم. إلاّ أنّه أضاف في المادّة 122 من القانون نفسه، أنّه يعود للمحكمة تقدير الدّليل الرّقمي أو المعلوماتي وحجيته في الإثبات، ويشترط أن لا يكون قد تعرّض لأيّ تغيير خلال عمليّة ضبطه أو حفظه أو تحليله .

وكما هي العادة، فإنّ إثبات الجرائم الإلكترونية تتمّ عادة ببذل مجهود وبحث شاق ودقيق، فتأتي فائدة الإثبات من خلال تمكّن القاضي أن يبرّر الإدانة أو البراءة للمتّهم، من خلال توفير الدّليل القاطع في إثبات وقوع هذه الجريمة الّتي تعتبر عمليّة الإثبات فيها من المسائل الّتي تحتاج إلى الخبرة المعلوماتية لدى القضاة، لتقدير الدّليل الرّقمي أو المعلوماتي على النّحو الصّحيح. وإلاّ الإستعانة بالخبرة المعلوماتية، الّتي لا تغني عن ضرورة وجود معرفة معلوماتية لدى القاضي لتقدير الخبرة المعطاة.

2. الإختصاص المكاني

من المؤكّد أنّ موضوع الإختصاص في الجريمة المعلوماتية، وفي غياب إطار تشريعي يحكمه وينظّمه، يتمّ التّعامل معه وفق قواعد الإختصاص المكاني. وهذا ما يطرح جملة من الصّعوبات، خصوصًا أنّ مكان إرتكاب الجريمة الإلكترونية، الّذي يكون دائمًا في البيئة الإفتراضية غير الملموسة، يختلف عن مكان إرتكاب باقي الجرائم التّقليديّة الأخرى في العالم الماديّ الملموس.

لذلك أوجدت معايير جديدة لإنعقاد الإختصاص، تتجاوز المعايير التّقليديّة الّتي يتمّ اللّجوء إليها من أجل تقرير ضوابط الإختصاص في مختلف الجرائم العادية الأخرى، وذلك انطلاقًا من مجموعة إجتهادات قضائية فرنسية في هذا المجال، سيما أنّ هذه المعايير مرتبطة بالخصوص ببعض الجرائم كما أشرنا إلى ذلك سابقًا. وكما هو الحال في جرائم الصّحافة المرتكبة في البيئة الرقميّة، فإن من بين المعايير الّتي ظهرت إلى الوجود والمرتبطة أساسًا بهذا النّوع من الجرائم، المعيار الّذي يعطي الإختصاص للمكان المادي حيث يتواجد الموقع الّذي نشرت الأقوال أو المعلومات بواسطته. كما ظهرت معايير جديدة ترتبط بالجرائم

الماسّة بحقوق الملكية الفكرية، كما هو الحال في جرائم التّقليد عبر الإنترنت، حيث يرجع الإختصاص إمّا لمحكمة المكان الذي أرتكب فيه التّقليد أو مكان نشره، وإمّا لمعيار إمكانية الوصول للموقع كأساس لإختصاص المحكمة في حالة الإعتداء على حق من حقوق المؤلّف من خلال الإنترنت [1].

بالإضافة إلى هذه المعايير تمّ إيجاد معايير أخرى مرتبطة أيضًا بالجرائم المرتكبة ضدّ الأحداث، حيث أنّ الإختصاص في هذا النّوع من الجرائم ينعقد لمكان إرتكاب الجريمة. ومكان إرتكاب الجريمة هذا يأخذ المعايير التاليّة[2]، والّتي يتمّ تقديمها بالأسبقية وهي:

- المكان الّذي شوهد فيه وجود الموقع غير المشروع، أو الّذي تمّ فيه مشاهدة الصّور والنّصوص ذات الطّبيعة غير المشروعة.
- المكان الّذي يوجد فيه خادم الإيواء إذا ظهر بعد المعاينات الأولى أنّ الموقع يمكن تحديده من خلال التّراب الإقليمي.

إلاّ أنّ قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي لم ينص على تحديد الإختصاص في النّظر في الدعاوى النّاشئة عن جرائم المعلوماتية. بالمقابل حسمت محكمة التّمييز الجزائيّة النّاظرة إستئنافًا في دعاوى المطبوعات، النّقاش القائم حول الجهة القضائية المخوّلة قانونًا النّظر في الجرائم المقترفة على مواقع التّواصل الإجتماعي، وتحديدًا فايسبوك وتويتر، الأكثر إستخدامًا من قبل النّاس بمختلف شرائحهم الإجتماعية. فقد أعلنت بقرار هو الأوّل من نوعه في هذا الموضوع، بأنّ محكمة المطبوعات ليست مختصّة للبتّ إلاّ في الجرائم المرتكبة عبر وسائل الإعلام المكتوبة والمسموعة والمرئية والإلكترونية، من قدح وذم وتشهير وتحقير ونشر أخبار كاذبة والواقعة ضمن قانون المطبوعات لأنّه قانون خاص. بينما الجرائم الواردة على الفايسبوك ينظر فيها القاضي المنفرد الجزائي، وبالتّآليّ تقع تحت طائلة قانون العقوبات [1].

[1] د. حسيّ عثيذ هجيج، صفاء كاظى غازي، **آثار جريمة قرصنة البريد الإلكتروني**، المرجع السابق نفسه، ص: 85.
[2] يان ناصر آل ثنيان، **إثبات الجريمة الإلكترونية**، المرجع السابق نفسه، ص: 88.

ختامًا، تعتبر هذه الإشكآليّات الّتي تعترض الجريمة المعلوماتية على قدر من الأهميّة بالنّسبة لوضع المجرم من جهة، والضّحيّة من جهة أخرى. لأنّ أيّ ثغرة موجودة في مراحل الملاحقة والتّحقيق وعلى مستوى الإختصاص والإثبات يعطي للمجرم حريّة ودافع لإرتكاب جرائمه دون خوف، ممّا يؤثّر على وضع الضّحيّة الّتي ستتأثّر بإفلات المجرم المعلوماتي من العقاب والمسؤوليّة فيختل التّوازن بينهما فتضعف بنتيجتها العدالة الجزائيّة.

المطلب الثّاني: المسؤوليّة الجزائيّة عن الحدث المعلوماتي المنحرف

لا يكفي لتوقيع الجزاء على الجاني أن يقع منه الرّكن الماديّ المكوّن للجريمة كما هو موصوف في النّص الجزائي، وأنّ يتوافر لديه الرّكن المعنوي اللّازم لتمامها، إنّما يلزم أيضًا أن تتوافر في حقه شروط المسؤوليّة الجزائيّة الموجبة للجزاء [2]. تعني المسؤوليّة الجزائيّة أهليّة الإنسان العاقل المميّز، لأن يتحمّل الجزاء العقابي نتيجة إقترافه جريمة ممّا نصّ عليها قانون العقوبات. وبذلك لكي يسأل الشّخص جزائيًا عن جريمة يجب أن يكون متمتعًا بالأهليّة الجزائيّة، وأن يتوافر في جانبه شروط المسؤوليّة الجزائيّة القائمة على الوعي والإرادة. والأهليّة الجزائيّة تعني أنّ الإنسان لا يكون أهلًا لتحمّل المسؤوليّة الجزائيّة، إلا إذا كان حيًا وعاقلًا وبالغًا سنًّا معيّنًا، والّتي حدّدها المشرّع اللّبناني على أنّها بإتمام الجاني السابعة من عمره. ولكنّ المشرّع لم يحمّل القاصر الّذي أتمّ السّابعة من عمره، ولم يبلغ سنّ الرّشد المتمثّلة بثمانية عشر عامًا في القانون اللّبناني المسؤوليّة الكاملة كالرّاشد، وإنّما نصّ له على تدابير وعقوبات مخفّضة، ومحدّدة حصرًا في

[1] قرار صدر علنًا في بيروت، بتاريخ 2016/1/19، منشور في مجلة محكمة، العدد5، آذار 2016.

[2] د. سمير عاليه، **الوسيط في شرح قانون العقوبات**، المرجع السابق نفسه، ص: 327.

قانون الأحداث المنحرفين وجعل لكل فئة عمرية خصوصيّتها تجاه المسؤوليّة الجزائية والعقاب.

بالإضافة إلى شرط الأهليّة الجزائيّة يجب أن يتوفّر لدى الجاني الوعي والإرادة. فالوعي يراد به الإدراك أو التّمييز، وهو قدرة الشّخص على فهم ماهيّة سلوكه وتقدير ما يترتّب عليه من نتائج. أمّا الإرادة فيعني بها المشرّع حريّة الإرادة، أي حريّة الإختيار، ويقصد بها قدرة الإنسان على توجيه نفسه إلى عمل معيّن أو الإمتناع عنه [1].

فالمسؤوليّة الجزائيّة في جرائم المعلوماتية تتطلّب لتقريرها توفّر شروط المسؤوليّة من أهليّة ووعي وإرادة، وهي لا تختلف عن تلك الّتي نصّ عليها قانون العقوبات. لكن ما تثيره هذه الجريمة يتمحور في مدى تحقّق المسؤوليّة الجزائيّة الكاملة للمجرم المعلوماتي الحدث، وذلك من خلال تبيان ما إذا كان للذّكاء المعلوماتي للقاصر المميّز من تأثير على مستوى الوعي والإرادة إيجابًا، بحيث تصبح المسؤوليّة الجزائيّة المقرّرة عليه كالرّاشد نفسه، أم أنّ لا إرتباط بين الذّكاء والوعي أو الإرادة (نبذة أولى). بالإضافة إلى مدى ملاءمة قانون الأحداث اللّبناني الصّادر في 6 حزيران 2002 تحت رقم 422، على مسؤوليّة إنحراف الحدث المعلوماتي في ظلّ التحديات المتعلّقة بالجريمة المعلوماتية (نبذة ثانية).

النّبذة الأولى: تأثير الذّكاء المعلوماتي للحدث على المسؤولية الجزائية

ينصّ المشرّع اللّبناني في المادّة الأولى من قانون الأحداث المخالفين للقانون أو المعرّضين للخطر، أنّ الحدث الّذي يطبّق عليه هذا القانون هو الشّخص الّذي لم يتمم الثامنة عشرة من عمره، إذا إرتكب جرماً معاقباً عليه في القانون أو كان معرضاً للخطر في الأحوال المحدّدة لاحقاً في هذا القانون. وينصّ في المادّة الثّالثة منه على أنّه لا يلاحق جزائياً من لم يتم السّابعة من عمره حين إقترافه الجرم.

[1] د. سمير عالية، **الوسيط في شرح قانون العقوبات**، القسم العام، المرجع السابق نفسه، ص:339.

وكما يتبيّن من نصّ هاتين المادتين، أنّ المشرّع إعتبر أن القاصر المسؤول جزائيًا هو الذي إقترف جرم ينصّ عليه القانون، وكان قد أتم السّابعة من عمره ولم يتجاوز الثّامنة عشر منه، على أن يكون غير فاقد للأهليّة لأسباب تتعلّق بشخصه كالجنون. فالحدث المعلوماتي هو ذلك القاصر المميّز، شرط أن يكون قد تمتّع بالإضافة إلى شرط الأهليّة الجزائيّة، بشروط قيام المسؤوليّة الجزائيّة ألا وهما الوعي والإرادة.

أيضًا، فقد أشار المشرّع اللبناني إلى هذين الشرطَين في المادّة 210 من قانون العقوبات على أنّه " لا يحكم على أحد بعقوبة ما لم يكن قد أقدم على الفعل عن وعي وإرادة ". بغية تحقّق الوعي لدى المجرم المعلوماتي، يجب أن يكون قد أتى بفعله عن إدراك أو تمييز، ويراد بالإدراك أو التّمييز هو قدرة الشّخص على فهم ماهيّة سلوكه وتقدير ما يترتّب عليه من نتائج. هذا الفهم يجب أن يحيط بالفعل في ذاته، كإدراكه أنّه يرتكب جريمة معلوماتية، وبنتائج هذا الفعل كسرقة المال المعلوماتي أو التّعدي على البيانات الرقميّة. بالإضافة إلى فهم القيمة الإجتماعية له بكون فعله ممنوعًا وليس مباحًا، لذلك إعتبر المشرّع اللبناني من بلوغ الإنسان سنّ السّابعة قرينة على حصول الوعي أو الإدراك وتحقق التّمييز.

أمّا الإرادة فيجب كما ذكرنا أن تكون حرّة وواعية، ولتحقّقها لا بُدّ من وجود أمرين، أولهما إمكانيّة تحقّق السّلوك الجرمي من الفاعل، كأن يكون لدى المجرم المعلوماتي القدرة على الدّخول إلى نظام معلوماتي معيّن غير مصرّح له بالدّخول إليه. أمّا الثّاني، وجود بدائل للسلوك كأن لا يكون الفاعل أمام خيار واحد مجبر عليه كالإكراه، أو حالة الضّرورة. عندها لا مكان للقول بحريّة الإختيار، كأن يُكره أحدٌ قاصر، مميّز، على الولوج إلى نظام معلوماتي تحت التّهديد.

بالرّغم من ترتيب المسؤوليّة الجزائيّة على الحدث، إلاّ أن المشرّع وضع له قانون خاص ينظّم هذه المسؤوليّة، والعقوبات والتّدابير الّتي يمكن أن تطاله، والّتي تعتبر إصلاحية وتخفيفية عمّا هي معمول بها في قانون العقوبات. ذلك لإعتبار أن الحدث لم يبلغ بعد سنّ الرّشد، والمقرّرة بثمانية عشر عامًا، فيُعتبر ناقصًا للأهليّة ويكون وعيه وإرادته، إن وجدت، غير مكتملَين. لكن السّؤال الّذي يطرح نفسه هو في دور

الذّكاء المعلوماتي للحدث المنحرف في تحقّق شروط المسؤوليّة الجزائيّة الكاملة، ممّا يستتبع تقرير المسؤوليّة عليه كالرّاشد نفسه.

فالإجرام المعلوماتي هو إجرام الذّكاء، ودونما الحاجة إلى إستخدام القوّة والعنف. فإنّ هذا الذّكاء هو مفتاح المجرم المعلوماتي لإكتشاف الثّغرات وإختراق البرامج المحصّنة [1]، وقد تكلّمنا فيما سبق عن أنّ النّسبة الأكبر من مجرمي المعلوماتية هم من الأحداث الّذين يتمتّعون بذكاء نشط. حيث يعتبر مفهوم الذّكاء من المفاهيم الأكثر تداولًا بين المختّصين في علم النّفس، حيث تحمل كلمة ذكاء أكثر من معنى ومدلول، لذلك هناك صعوبة في إعطاء معنى موحّد للذّكاء. وفقًا ل "ألفريد بينيه" Alferd Binet " الذّكاء هو في المقام الأوّل، مجموعة من المعرفة تترجم نحو العالم الخارجي ويشمل الفهم والإختراع "، في حين يعتبره "لويس تيرمان" Lewis Terman أنّه " القدرة على التّفكير المجرّد "، على غرار "وكسلر" Wechsler فالذّكاء هو " القدرة الكليّة للفرد على العمل الهادف والتّفكير المنطقي والتّفاعل النّاجح في البيئة " [2].

يعبّر مصطلح الذّكاء البشري عن جودة العقل الّتي يمنح الإنسان القدرة على التّعلّم من التّجربة والتّكيّف مع المواقف المختلفة والجديدة في الحياة. بالإضافة إلى زيادة القدرة على فهم المفاهيم المجرّدة والقيام بمعالجتها، والتّمكّن من إستخدام المعرفة للقيام بإحداث تغيير في بيئة الأفراد. كما أنّ الذّكاء ليس عمليّة معرفيّة أو ذهنيّة بشكل مطلق، بل هو مزيج إنتقائي من العمليّات الّتي تتضمّن التكيّف الفعّال، من حيث إجراء تغيير في الذّات من أجل التّعامل بشكل أكثر فعاليّة مع البيئة، أو تغيير البيئة وإيجاد بيئة

[1] رياض هاني بهار، قانون الجرائم المعلوماتية والمجرم المعلوماتي والعقوبات البديلة، موقع كتابات الإلكتروني، 2019/4/25، /قانون-الجرائم-المعلوماتية-والمجرم-ال/https://kitibat.com/2019/04/25

[2] حبال ياسين، **تقنين إختبار كاتل للذكاء، المقياس الثالث، على تلاميذ السنة أولى ثانوي**، أطروحة للحصول على شهادة دكتوراه في علم النفس، جامعة وهران 2، سنة 2016/2017، ص: 18.

جديدة مختلفة تمامًا [1]. فالذّكاء الإنساني لم يعد يقتصر على التّفكير المجرّد، الإستبصار بإدراك العلاقات الدّالة بين عناصر المنظومة، فهم المعاني، طلاقة اللسان، سرعة إجراء عمليّات، وضوح تصوّر العلاقات الزّمانية والمكانية وقوّة التّمييز والقدرة على الاستقراء. إنّما أصبح يشير بالأساس إلى مرونة التّعامل مع المواقف المغايرة والقضايا الطارئة، والقدرة على التّكيّف مع الصعوبات والتّغلب على المشاكل.

بطبيعة الحال، إذا كان الذّكاء هو قدرة عقلية فطرية تُمكّن الإنسان من التّغلّب على المشاكل الّتي تعترضه في الحياة والتأقلم مع الواقع الاجتماعي[2] ، فإن الوعي هو القدرة على معرفة طبيعة الفعل الّذي يقدم عليه الشّخص والنّتيجة المترتّبة عليه. أمّا الإرادة هي القيام بهذا الفعل أو الإمتناع عنه بتركه عن وعي وقصدية، وتتسلّح بالقدرة على التّحكم في الذّات والتّوقي من نتائج ذلك الفعل وتأثيراته في المحيط الطبيعي والنّسيج الثّقافي والإطار الإجتماعي.

ففي جريمة المعلوماتية يقتضي التّمييز بين الوعي والإرادة من جهة وذّكاء الحدث المعلوماتي المنحرف من جهة اخرى. حيث أنّ الوعي هو إدراك الفعل الجرمي وفهم ماهيّة السّلوك الّذي يقدم عليه الفاعل والنّتائج الّتي سوف تترتّب على إرتكابه الجريمة. أمّا الإرادة فتعني حريّة الإختيار لإرتكاب الجريمة المعلوماتية من عدمها. بينما الذّكاء المعلوماتي، فهو القدرة العقلية على إنتاج الوسائل الّتي يمكن من خلالها إرتكاب الفعل الجرمي. إذ أنّ الذّكاء المعلوماتي لدى مجرم المعلوماتية لا يعبّر عن وعي عقلي وذهني ودرجة عالية من الإرادة الحرّة، إنّما عن مجموعة القدرات العقلية المنتجة في النّظام المعلوماتي. حيث يمكن من خلال هذا الذّكاء القيام بالنّشاط الإجرامي بإحترافية إجرامية أكبر، وذلك بعد أن يكون قد تكوّن لدى المجرم المعلوماتي الحدث الوعي والإرادة اللازمين لترتيب المسؤوليّة الجزائيّة. فالوعي البشري

[1] غادة الحلايقة، مفهوم الذكاء، موقع موضوع، 17/ يوليو/ 2018، مفهوم_الذكاء/https://mawdoo3.com

[2] د. علي مشيك، الوعي البشري ظاهرة تاريخية (فكر)، موقع تحولات، 2017/1/17، http://www.tahawolat.net/MagazineArticleDetails.aspx?Id=1131 ، تاريخ الدخول إلى الموقع 2020/1/16.

يُحدّد على أساس معارف ومعتقدات وعادات ونظم تربية مختلفة، ليأتي الذّكاء ويعالج المشكلات الّتي تعترض هذا الوعي بناءً على ما تركّز في الوعي أساسًا. غير أنّ الحدث الّذي يتمتّع بمستوى عالٍ من الذّكاء، وتربى في بيئة إجرامية نقلت آليّه معارفها ومعتقداتها وثقافتها الإجرامية وتأصّلت فيه، سوف يوظّف في المستقبل ذكاءه في خدمة هذه المعتقدات والمعارف والثّقافات الإجرامية ممّا يزيده خطورة عن غيره من المجرمين.

إذا لا علاقة مباشرة بين مستوى الذّكاء ودرجة الوعي والإرادة للمجرم المعلوماتي الحدث، خصوصًا أنّ جرائم المعلوماتية تتطلّب لإقترافها أن يكون المجرم من الأشخاص الّذين يتمتّعون بمستوى معيّن من الذّكاء البشري، ليمكّنهم من إختراق الأنظمة المعلوماتية وتحقيق أهدافهم من الجريمة. لذلك يعتبر الذّكاء عامل مساعد ومسهل لإرتكاب جريمة المعلوماتية، وينذر عن مجرم أكثر خطورة من غيره بعد أن يكون الفاعل قد أدرك الفعل الذي يقدم عليه وإتّجهت إرادته إلى تحقيقه. هذا ما يفتح المجال للحديث عن مدى تناسب وملاءمة القوانين الموضوعية على الحدث المعلوماتي، خصوصًا أنّه يختلف بسماته ونوعيّة جريمته عن الحدث التّقليدي.

النّبذة الثّانية: مدى ملاءمة قانون الأحداث على إنحراف الحدث المعلوماتي

لقد بدا واضحًا في الآونة الأخيرة إنحراف الأحداث في مجال المعلوماتية منذ ظهور وإنتشار إستعمال الحاسوب، حيث ظهر ما يطلق عليه بنوابغ صغار المجرمين، من منتهكي نظم المعلوماتية. لاحقًا نتيجة الإنتشار الهائل للإنترنت، لم يعد مطلوبًا من المجرم المعلوماتي أن يكون على مستوى عالٍ من الذّكاء لإرتكاب مثل هذه الجرائم، بدءًا من جريمة الذّم والقدح، إلى الحضّ على الفجور والدّعارة، وإلى العديد من الجرائم الأخرى. ولعلّ الإستخدام الكبير للإنترنت من قِبَل الأحداث، ولاسيما على هواتفهم النّقالة

إضافةً إلى الحاسوب، أدّى إلى إنحرافهم وذلك بإرتكابهم للكثير من الجرائم [1].

ومن الجليّ إنعقاد الإختصاص لقضاء الأحداث في أيّ جريمة ترتكب من قبل الحدث، سواء كانت جريمة تقليديّة أم جريمة مستحدثة كجرائم المعلوماتية، حيث يطبّق حصرًا قانون الأحداث المنحرفين أو المعرّضين للخطر. من هنا يثور التّساؤل حول مدى ملاءمة هذا القانون على جنوح الأحداث المعلوماتي، وذلك في ظلّ غياب التّخصص من قبل الهيئات القضائية المختصّة بقضايا الأحداث، مع التّحديات الّتي تثيرها الجريمة المعلوماتية.

إلاّ أنّ جميع التّشريعات أكدّت، ومن ضمنها المشرّع اللّبناني، على عدم معاملة الحدث الجانح كالمجرم البالغ، وذلك لعدم إكتمال نموّه العقلي والجسدي، ممّا يستلزم معاملة خاصّة وإجراءات وتدابير، الهدف منها تأهيله وإصلاحه. ولا شكّ أنّ تحميل صغار السنّ مسؤوليّة إنحرافهم أمر غير مقبول، وبتأثر المشرّع بمدرسة الدفاع الإجتماعي وخاصّة نبذ فكرة العقاب، توَجّه إلى أفكار جديدة، منها مواجهة الخطورة الإجرامية الكامنة في الطفل ومحاولة إصلاحه وتقويمه. لذلك نصّ قانون الأحداث المنحرفين والمعرّضين للخطر في المادّة الخامسة منه على العقوبات الّتي تفرض على الحدث، حيث قسّمها إلى عقوبات غير مانعة للحريّة كاللّوم، الوضع قيد الإختبار، الحماية، الحريّة المراقبة وأخيرًا العمل للمنفعة العامّة أو العمل تعويضًا للضحيّة. فضلًا عن العقوبات المانعة للحريّة والّتي تتمثّل في الإصلاح والتأديب والعقوبات المخفّضة، بالإضافة إلى التّدابير الإحترازية الّتي يمكن للقاضي أن يفرضها على الحدث حيث يرى أن هناك ضرورة لذلك [2]. وقد راعى المشرّع إتّخاذ التّدابير المنصوص عليها في المادّة الخامسة من القانون نفسه سِنّ الحدث، والّذي يتدرّج من سنّ السّابعة إلى الثّامنة عشر.

عقب بروز التّحديات والمشاكل الكثيرة نتيجة أنشطة مكافحة جرائم الحاسوب والإنترنت، حاول قانون

[1] د. صفاء أوتاني، سوزان الأستاذ، **عدم ملائمة قانون الأحداث السوري لإنحراف الأحداث المعلوماتي**، مجلة جامعة البعث، المجلد 40، العدد 5، عام 2018، ص: 121.

[2] د. سمير عاليه، **الوسيط في شرح قانون العقوبات**، المرجع السابق نفسه، ص: 511.

المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي معالجتها من ناحية تحديد آثارها في مسرح الجريمة، وإجراءات التّفتيش، والضّبط، وأدلّة الإثبات الّتي ينبغي توفّرها. ولكن ما يؤخذ على هذا القانون أنّه لم يخصّص من يكون مسؤولًا عن التعامل مع الأحداث الذين يقومون بإرتكاب جرائم المعلوماتية. ولو أنّ قانون الأحداث قد أوجد أشخاص يتعاملون مع الأحداث المنحرفين، إلاّ أنّهم غير مختصين على مستوى تقنيّة المعلومات [1].

فعدم وجود قضاة أحداث مختصين بالإجرام المعلوماتي من أجل التّعامل مع قضايا إنحراف الأحداث المعلوماتي، بدءًا من قضاة النّيابة والتّحقيق وإنتهاءً بقضاة الحكم، يشكّل ضمانة أقل لهؤلاء الأحداث خصوصًا أنّ الطبيعة القانونية لجريمتهم تختلف عن الجرائم الأخرى. هذا بالإضافة إلى عدم وجود تخصّص وخبرة لدى بعض الأشخاص المعنيين بإنحراف الأحداث في الإجرام المعلوماتي مثل مراقبي السّلوك، أو المرشدين الإجتماعيين الذين ينبغي عليهم أن يكونوا ملمين بهذه التّقنيّة.

كما أنّ الأسباب غير الملائمة في قانون الأحداث لإنحراف الأحداث المعلوماتي، هو ضعف مراكز الملاحظة التي يوضع بها الأحداث المعلوماتيون تحت المراقبة، وكذلك معاهد الرّعاية والإصلاح فضلًا عن مكاتب الخدمة الإجتماعية المؤازرة للمحاكم وعدم وجود كوادر مؤهلّة للتّعامل مع إنحراف الحدث المعلوماتي. لذلك لا بدّ من ضرورة إصدار قانون جديد للأحداث في لبنان يتلاءم مع إنحراف الأحداث المعلوماتي، بحيث يؤخذ بالإعتبار وضع قواعد موضوعية تحكم وتقنّن جرائم إنحراف الأحداث في مجال المعلوماتية. بالمقابل يجب وضع تدابير إصلاحية تتلاءم مع طبيعة هذا الإنحراف وخصوصيته، كذلك وضع قواعد إجرائية واضحة والعمل على إنشاء مؤسّسات مؤهلّة بشكل جيّد وكافي من جميع النّواحي تلائم طبيعة هذا الإجرام. علاوة على ذلك، إنشاء وحدات أمنية وقضائية متخصّصة في الجرائم الرّقميّة وتأهيلها

[1] د. صفاء أوتاني، سوزان الأستاذ، **عدم ملائمة قانون الأحداث السوري لإنحراف الأحداث المعلوماتي**، المرجع السابق نفسه، ص: 144.

للتعامل مع الأحداث الجانحين أو المعرّضين لخطر الإنحراف في الأنظمة المعلوماتية.

وفي ختام هذا الفصل نكون قد تطرّقنا إلى معظم الإشكاليّات التي تعترض المسؤوليّة الجزائية، وتؤثر على وضعية كلّ من المجرم والضّحيّة مع إعطاء الحلول القانونية والعمليّة لها، بدءًا من مرحلة الملاحقة والتّحقيق ثمّ الإثبات وتحديد الإختصاص، وصولًا إلى وضعيّة الحدث المعلوماتي المنحرف الذي أكدّنا على ضرورة وجود قانون خاص به يحاكي ظهور الجريمة المعلوماتية.

الباب الثّاني

بين العقوبات والتدابير المناسبة وأهمّية الوقاية

إنّ ما واجهته المسؤوليّة الجزائية من إشكاليّات على مستوى تطبيقها في الإجرام المعلوماتي، إستتبعه ضرورة وجود جزاء عقابي يتناسب مع طابع هذا الإجرام الحديث، وضمانات لضحاياه يتمّ من خلاله تحقيق الرّدع العام وإرضاء شعور العدالة الجزائية بمختلف أطرافها. لذلك كان لا بد من إعطاء أهمّية لبعض العقوبات والتّدابير الّتي تلائم أكثر الإجرام المعلوماتي عن غيرها، وإيجاد بعض الحلول العمليّة والقانونية لتحويل الخطورة الإجرامية إلى فرصة يمكن أن يستفيد منها المجتمع والمحكوم عليه، بالإضافة إلى بعض الحقوق الملازمة لضحايا الإجرام المعلوماتي.

ولمّا كانت عمليّة التّصدّي للإجرام المعلوماتي تتمّ من خلال الجزاء العقابي الّذي يفرض على المجرمين المعلوماتيين، كان لا بُدّ بالمقابل من إيجاد أساليب معيّنة لمكافحته. وذلك إمّا من خلال خطة إستباقية وقائية تتمثّل بإستعمال تقنيات الحماية والأمان من جهة، وإتباع إستراتيجيات توعوية حول مخاطر التّقنيّة المعلوماتية من جهة أخرى، وإمّا عبر قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي اللّبناني ومن خلال التّعاون الدّولي الّذين يؤمنان الشّرعية اللّازمة للتّصدّي لهذا الإجرام.

لذلك سنقوم في هذا الباب بالتّطرّق في فصل أوّل إلى آثار المسؤوليّة الجزائية على كل من مجرم وضحية الإجرام المعلوماتي من جهة الجزاء العقابي الّذي يجب أن يفرض على المجرم المعلوماتي، وحقوق ضحايا الإجرام المعلوماتي الّذين تقع عليهم هذه الجريمة. أمّا في الفصل الثّاني فسنتطرّق إلى أساليب مكافحة الإجرام المعلوماتي على المستوى العملي والقانوني، وكذلك الأمر على المستوى المحلّي والدّولي لتأمين الحماية اللازمة في وجه هذا الإجرام.

الفصل الأوّل

آثار المسؤوليّة الجزائية على مجرم وضحيّة الإجرام المعلوماتي

لا ينتهي الإجرام إلاّ بإتّخاذ إجراءات بحق المجرمين تحدّهم عن معاودة إرتكاب جرائمهم، فعقابهم يُرضي شعور العدالة الجزائيّة من جهة، ومن جهة أخرى يصون سيادة الدّولة ويبرهن قوّتها على تطبيق القوانين والإقتصاص من المجرمين. والعدالة الجزائيّة من ناحية أخرى تحتّم لإكتمالها النّظر إلى الضّحيّة كعنصر أساسي يجب دراسته لتحقيقها، والإهتمام به ومعرفة مصيره بعد إرتكاب الجريمة. هذه النظرة للمجرمين والضّحايا، لها أهمّيتها في الإجرام المعلوماتي الّذي يوجب نوع عقاب معيّن ينبغي إنزاله بالمجرم المعلوماتي، ونظرة خاصة إلى ضحايا هذا الإجرام الذي عادة ما يكون تأثيره علنيًّا فيؤثر بشكل مباشر على الحياة الشخصيّة لهم.

لذلك سنتطرّق في هذا الفصل في مطلب أوّل إلى دراسة العقوبات والتّدابير التي يجب أن تنزل بالمجرم المعلوماتي من ناحية عامّة وتلك الّتي تنصّ عليها القوانين اللّبنانيّة من ناحية ثانية. أمّا في المطلب الثاني سنتطرّق إلى دراسة مصير ضحايا الإجرام المعلوماتي لتعزيز حقوقهم ومساعدتهم على إعادة التكيّف مقابل ما تعرضوا له من إجرام معلوماتي.

المطلب الأوّل: الجزاء العقابي

الجزاء العقابي هو الأثر الذي يقرّره النّص الجزائي على مخالفة الأمر أو النّهي الوارد فيه، وله صورتان: العقوبات والتّدابير الإحترازية[1]. هاتان الصّورتان تمثلان الوسيلتين اللّتين إستقرّت عليهما

[1] د. سمير عالية، **الوسيط في شرح قانون العقوبات (القسم العام)**، االمرجع السابق نفسه، ص:507.

التّشريعات لإسباغ الحماية الجزائيّة على المصالح والأموال الّتي يهم المشرّع العقابي حمايتها. فالإجرام المعلوماتي إجرام عصري يتطلب دراسة خاصة من ناحية تقرير العقاب الجزائي، وذلك لأنّه يمتاز بطابع الحديث ولا يتطلب في معظم الأوقات إتّساخ يد المجرم وتلطيخها في الدّماء. فهو يمارس عن بعد وبوسائل أكثرها تقنيّة ويصنف من ضمن الجرائم البيضاء، ويهدف في معظم إجرامه إمّا إلى تحقيق الرّبح المادّي، أو الإعتداء على الحياة الشخصيّة للأفراد.

لذلك سنعالج في نبذة أولى هذه الجزاءات التي يجب أن تفرض على المجرم المعلوماتي، وكيف عالجها المشرّع اللّبناني في قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي من جهة العقوبة والتدابير الإحترازية. وفي نبذة ثانية سنتطرّق إلى كيفيّة التّمكن من الإستفادة من المجرمين المعلوماتيين لصالح الدّولة كإجراء بديل عن العقوبة.

النّبذة الأولى: العقوبات وتدابير الإحتراز الواقعة على المجرم المعلوماتي

تتمثّل العقوبات بأنّها قدر من الألم يقرره المجتمع ممثلًا في مشرّعه، ليوقعه على مرتكبي الجرائم بمقتضى حكم مبرم يصدر عن القضاء، فيهدف إلى إيلام المجرم إيلامًا يتساوى مع جسامة جريمته. هذا الإيلام قد يكون بدنيًا مثل عقوبة الإعدام، وقد يكون معنويًا كالعقوبات المانعة للحريّة أو المقيّدة لها أو الماسّة بالإعتبار، وقد تكون ماديّة كالعقوبات الماليّة مثل الغرامة. أمّا التّدابير فهي إجراءات وقائية يَستهدف بها المجتمع حماية نفسه من الأضرار والأخطار الّتي تهدده من المجرمين ذوي الخطورة الإجرامية، الّذين إرتكبوا أو لم يرتكبوا جرائم بعد، ولكن لهم من الخطورة ما يستتبع إمكانيّة إرتكابهم جرائم في المستقبل. فهي شخصيّة وترمي إلى علاج الجاني ونزع الخطورة الجرمية منه [1].

[1] د. سمير عالية، **مبادئ علم الإجرام والعقاب والسياسة الجزائية، أسباب الإجرام ومكافحته جزائيًا**، منشورات الحلبي الحقوقية، 2019، ص:185

ونظرًا إلى خصوصية الإجرام المعلوماتي الذي لا ينتج عنه جرائم ضد الأشخاص على الأغلب، إلا أنّه لا يمنع من أن يكون وسيلة أساسيّة أو مساعدة لمثل هذه الجرائم، لكونه إجرامًا يصيب أنظمة معلوماتية وبرامجية كبرى، وتهدّد أمن وإستقرار مؤسّسات ماليّة وحكومية. ممّا كان ينبغي التّركيز في هذا النّوع من الإجرام على عقوبات وتدابير مختلفة لم يكن لها أهمّيتها في النّظام الجزائي للجرائم التّقليديّة. لذلك تُعتبر العقوبة الماليّة من أبرز العقوبات التي يجب أن تتصدر النّظام العقابي للإجرام المعلوماتي، لما تضفيه من طابع رادع على أفراد المجتمع والمجرم المعلوماتي، بالإضافة إلى تناسبها وملاءمتها لهكذا نوع من الإجرام. أمّا على مستوى التّدابير فتعتبر المراقبة والحجر على المحكوم بإستعمال التّقنيات المعلوماتية من أهمّها، والّتي من خلالها يمكن أن نضمن سلامة المجتمع من هؤلاء المجرمين والحدّ من خطورتهم.

1. العقوبات الماليّة

إذا تطرّقنا للحديث عن العقوبات الماليّة، لا يعني أنّ في الجريمة المعلوماتية لا وجود للعقوبات المانعة أو المقيّدة للحريّة. بل على العكس لا بدّ من وجود هذا النّوع من العقوبات، إنّما يجب دائمًا في الجرائم الحديثة، وخصوصًا في الجريمة المعلوماتية، إعطاء الأولويّة للعقوبات الماليّة على غيرها. فإنّ إحدى التّحولات الأساسيّة على الصّعيد المحلي أو الدولي، تَكمُن في تغيّر وجهة النّظام الجزائي من الملاحقات والعقوبات المانعة للحريّة والغرامات كآليّات عقابية أساسيّة. فالجرائم الّتي ترتكب بغيّة الحصول على الرّبح بأي وسيلة يجب أن يقابلها جزاء عقابي ماليّ صارم، ينهي المجرمين عن معاودة إرتكاب إجرامهم ويشكّل ردعًا عامًّا لغيرهم من أبناء المجتمع. من هنا برزت الحاجة إلى هذه العقوبات الّتي من أهمها عقوبتي المصادرة والغرامة الأصليّة، وليس الغرامة الإضافيّة. ذلك لمواجهة الإجرام المعلوماتي وتشكيل سدّ رادع أمام مجرميه.

1.1 المصادرة

تعدّ المصادرة بصفة عامّة عقوبة ماليّة تلجأ اليّها الدّولة عن طريق سلطاتها، من أجل مواجهة ظروف معيّنة لردعه أو للوقاية منه، بناءً على شروط معيّنة وفقًا لأحكام عامّة تحكمها. بالتّاليّ يمكن تعريفها على أنها نزع ملكيّة شيء ونقله جبرًا عن مالكه بغير مقابل، وإضافته إلى ملك الدولة [1].

فقد نصّ القانون اللبناني في قانون العقوبات، على المصادرة الشخصيّة كعقوبة إضافيّة تفرض على المجرم، وقد جاء في نص المادّة 69 منه على أنّه " يمكن مع الإحتفاظ بحقوق الغير ذي النيّة الحسنة مصادرة الأشياء الّتي نتجت عن جناية أو جنحة مقصودة أو الّتي إستعملت أو كانت معدّة لإقترافها. ويمكن مصادرة هذه الأشياء في الجنحة غير المقصودة أو في المخالفة إذا إنطوى القانون على نصّ صريح ...".

كما يتبيّن من نصّ هذه المادّة أن عقوبة المصادرة هي عقوبة إضافيّة في القانون اللّبناني يجب أن ينصّ عليها الحكم إلى جانب العقوبة الأصليّة. هذا ما يجب أن يحطاط منه المشرّع في جرائم المعلوماتية، لأنّ عقوبة المصادرة يجب أن تكون عقوبة فرعيّة تفرض على المجرم، وتصيب بشكل خاص الأجهزة والوسائل الماديّة الّتي إستعملها في عمليّته الجرمية، بالإضافة إلى الأرباح وعائدات العمل الجرمي الّذي يشكّل هدف هذه العقوبة.

بالعودة إلى قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي، لم ينصّ المشرّع اللبناني على عقوبة المصادرة على الوسائل والأجهزة والتقنيات الّتي تم إرتكاب الجرائم المعلوماتية بواسطتها، أو العائدات الناتجة عن الإجرام المعلوماتي، لذلك ينبغي العودة إلى النّصوص القانونية العامّة الموجودة في قانون العقوبات الّتي ترعى هذه العملية.

[1] ريمة موايعية، **النظام القانوني للمصادرة**، مذكرة مكملة لمتطلبات نيل شهادة الماستر، جامعة العربي التبسي، سنة 2016/2015، ص: 14.

2.1 الغرامة

تعني الغرامة إلزام المحكوم عليه بأن يدفع إلى خزانة الدّولة مبلغ الغرامة المقرّر في الحكم، وهي كعقوبة أصليّة تفرض في بعض عقوبات الجنح العاديّة والسياسيّة وعقوبات المخالفات، حيث تتراوح قيمة الغرامة في الجنح بين خمسين ألف ومليوني ليرة لبنانية، إلاّ إذا نصّ القانون على مبلغ أكبر. أمّا في المخالفات فتتراوح قيمة الغرامة فيها بين ستّة ألاف وخمسين ألف ليرة لبنانية، وتفرض كعقوبة خاصّة في بعض الجنايات والجنح إلى جانب عقوبة الحبس أو الإعتقال [1].

غير أنّ الغرامة الماليّة الّتي يفرضها المشرّع على العديد من الجرائم كعقوبة تطال مرتكبيها، لم يعد يُشهد لها حاليًا فعاليّة في النظام الجزائي اللّبناني. حيث أنّ هذه الغرامات لم تعد لها القوّة الرادعة الّتي كانت لها حين وضعت القوانين الجزائيّة، لإختلاف سعر صرف اللّيرة آنذاك عن تلك الحاليّة من جهة. ومن جهة أخرى، عدم ملاءمتها للجرائم الحديثة التي ترتكب لأجل النّفع المادّي غير المشروع النّاتج عن العمل الجرمي، والّذي لا يردعه سوى عقوبات ماليّة جازمة وصارمة ومرتفعة تجعل من النّفع المادّي الّذي كان يبغيه المجرم من الجريمة المعلوماتية عقوبة تطال ذمّته الماليّة. فبدل إكتساب المجرم نفع مادّي بطريقة غير مشروعة يفرض عليه غرامات ماليّة مرتفعة القيمة تتناسب مع العمل الجرمي الّذي قام به.

بالعودة إلى قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي، نرى أن المشرّع قد أعطى أهمّية بالغة للغرامة الجزائيّة كعقوبة تطال المجرمين المعلوماتيين الذين يرتكبون هذه الجرائم. فنصّ عليها إمّا كعقوبة أصليّة يمكن أن تفرض لوحدها على الجرم المرتكب، أو تفرض مع عقوبة الحبس. ولقد نصّ المشرّع في هذا القانون على عقوبات جزائيّة مختلفة للغرامة، فمثلاً في المادّة 106 من قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي، من الفصل الخامس منه، جعل عقوبة الغرامة تتراوح بين مليون ليرة وثلاثين مليون ليرة لبنانية على كل من معالجة بيانات ذات طابع شخصي أو جمعها أو إفشائها

[1] د. سمير عالية، **الوسيط في شرح قانون العقوبات**، المرجع السابق نفسه، ص: 210.

عن قصد أو إهمال. أمّا في المادّة 111 من القانون نفسه، فقد جعل المشرّع عقوبة الغرامة الجزائيّة تتراوح بين ثلاثة ملايين ومئتي مليون ليرة على كل من يتعدّى على سلامة النّظام المعلوماتي. إضافة إلى أنّه في المادّة 112، جعل عقوبة التّعدي على سلامة البيانات الرقميّة بالحبس من ستّة أشهر إلى ثلاث سنوات، وبالغرامة من ثلاثة ملايين إلى مئتي مليون أو بإحدى هاتين العقوبتين. أيّ أنّ هناك إمكانيّة لفرض عقوبة الغرامة فقط على مرتكب هذا النّوع من الإجرام المعلوماتي.

زد على العقوبات المنصوص عليها في قانون العقوبات ومن بينها العقوبات الماليّة الّتي تكلّمنا عنها، نصّ المشرّع في المادّة 125 من قانون المعاملات الإلكترونية على أنّه " يمكن للمحكمة النّاظرة في الدّعوى بموجب حكمها النّهائي وقف خدمات إلكترونية أو حجب مواقع إلكترونية أو إلغاء حسابات عليها إذا تعلّقت بالجرائم المتعلّقة بالإرهاب أو بالمواد الإباحية للقاصرين أو بألعاب مقامرة ممنوعة أو بعمليّات الإحتيال الإلكتروني المنظّمة أو تبيض الأموال أو الجرائم الواقعة على الأمن الداخلي والخارجي أو المتعلّقة بالتّعدي على سلامة الأنظمة المعلوماتية كنشر الفيروسات ". بالتّالي يتّضح من نصّ هذه المادّة أن هناك عقوبات مستحدثة نصّ عليها المشرّع في قانون المعاملات الإلكترونية تختص فقط بالجريمة المعلوماتية، وتتمثّل في إمّا وقف خدمات إلكترونية، أو حجب مواقع إلكترونية أو إلغاء حسابات.

ختامًا، لا شكّ بأنّ الإجرام الحديث وخصوصًا في الجريمة المعلوماتية يفرض على المشرّع الإهتمام بالعقوبات الماليّة كعقوبة تحقّق الرّدع العام، وترضي شعور العدالة الإجتماعية أكثر من فرض العقوبات المانعة أو المقيّدة للحريّة، الّتي يفضلها المجرم الحديث عن العقوبات الماليّة في حال كانت جريمته قد نجحت من ناحية تحقيق الكسب المادي غير المشروع. لكنها فشلت من ناحية إلقاء القبض عليه وإنزال الجزاء العقابي المانع والمقيّد للحريّة عليه، دون حصول الدّولة على عائدات النّشاط الجرمي الّذي يكون قد أخفاها أو وضعها بعهدة شخص آخر، ليتمتّع بها بعد إمضائه فترة محكوميته فيخرج شخصًا ذا قدرات ماليّة هائلة، لم يكن ليحصل عليها لو لم يرتكب جريمته، ولم يكن أحيانا ليحققها لو عمل في أي نشاط مشروع

آخر طيلة فترة السجن الّتي أمضاه فيه، فتكون العقوبة الماليّة إلى جانب العقوبات المقيّدة والمانعة للحرية مساعدة في مواجهة الإجرام المعلوماتي. فتمنع المكاسب المادّية غير المشروعة عن المجرمين، بالتالي تنتفي الغاية الّتي من أجلها تم إرتكاب الجريمة المعلوماتية الّتي عادة ما تكون غايتها إبتزاز المال أو الإحتيال، وبذلك تكون العقوبة الماليّة متلائمة مع نوع الجرم المرتكب إذا كان غايته الحصول على منفعة ماليّة معيّنة. وإلاّ إن سلمنا بالعقوبات المقيّدة والمانعة للحرية فقط، تكون العدالة الجزائية منقوصة لأنّ العقوبة لا تتلاءم مع طبيعة الجريمة المرتكبة ولا تحقق الردع العام.

2. التّدابير الإحترازية

إنّ التّدابير الإحترازية عادةً ما يحكم بها القاضي لإجتناب خطورة مجرم ما، فتُتخذ الحيطة منه بفرض تدبير معيّن عليه يحول بينه وبين إرتكاب الجريمة هذا من جهة. ومن جهة أخرى يمكن أن تفرض على المجرمين الّذين أنهوا فترة محكوميتهم، ولكن لا زال لديهم نزعة جرمية معيّنة تجعل هذا التّدبير الإحترازي واجبًا لحماية المجتمع. والتّدابير لها خصائصها في قانون العقوبات اللّبناني، فلا يحكم بها إلا من قِبَل القضاء، وعلى من كان خطرًا على السّلامة العامّة. فلا يقضى بها إلا بعد التّثبت من حالة الخطر التي تُعدّ متوافرة لدى كل شخص يقترف جريمة، ويُخشى أن يُقدم على أفعال أخرى[1]. حيث أن في الجريمة المعلوماتية تعدّ التّدابير الإحترازية من أهم الوسائل للتّصدي لهذا الإجرام، كونها تقيّد حريّة المجرم وتشلّ حركته، وتمنع عنه الوسائل التي بواسطتها يرتكب فعله الجرمي، التي من دونها لن يتمكّن من تحقيق هذا المشروع.

لذلك من أهم التّدابير الإحترازية التي تتلاءم مع جريمة المعلوماتية والتي تعتبر فعالة أكثر من غيرها، هي الحريّة المُراقبة والحجر على المحكوم بإستعمال الوسائل والآليّات التقنيّة والمعلوماتية التي ترتكب

[1] د. سمير عالية، **الوسيط في شرح قانون العقوبات**، المرجع السابق نفسه، ص: 526.

بواسطتها جريمة المعلوماتية.

1.2 الحريّة المُراقبة

الحريّة المُراقبة هي تدبير إحترازي، لغاية التّثبت من صلاح المحكوم عليه وإئتلافه مع المجتمع، حيث تتولى الدّولة أو هيئات خاصّة مهمة المراقبة [1]. فقد نصّ قانون العقوبات اللّبناني في المادّة 84 منه على أنّ " الغاية من الحريّة المراقبة التّثبت من صلاحية المحكوم عليه، وتسهيل إئتلافه مع المجتمع..."، وجعل مدّة الحريّة المراقبة في المادّة 85 من القانون نفسه، تتراوح بين سنة وخمس سنوات ما لم يرد في القانون نصّ خاص مخالف. بالتّاليّ يجب أن يُقدّم إلى القاضي تقريرعن سيرة المحكوم عليه مرة كل ثلاثة أشهر على الأقلّ.

أمّا في قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي لم يتكلم المشرّع عن التّدابير الإحترازية كجزاء لجريمة المعلوماتية، لذلك ينبغي تطبيق القواعد العامّة في قانون العقوبات على هذه الجريمة. حيث يجب أن تُفرض الحريّة المُراقبة على كل مجرم معلوماتي يرتكب جريمة معلوماتية وأُدين بها بحكم جزائي، بمراقبة إستعمال الوسائل الإلكترونية من قبل الهيئات التي تتولّى المراقبة، والمنع من إرتياد المحلات التي يكون موجود فيها مثل هذه الوسائل الإلكترونية غير الخاضعة لرقابتها.

ولا شكّ أنّ الحريّة المُراقبة تشكّل تحدي لجهات المراقبة في الجريمة المعلوماتية كون هذه الجريمة يمكن أن ترتكب من هاتف ذكيّ محمول يسهل إخفاؤه وتهريبه وإستعماله دون قيد. لذلك يجب عليها أن تتّخذ بعض الإجراءات كمراقبة العمليّات الّتي تتمّ عبر الشّبكة المعلوماتية في الموقع الموجود فيه المجرم المعلوماتي وخصوصًا مراقبة شبكات الإنترنت القريبة والمجاورة له.

[1] د. سمير عالية، **مبادئ علم الإجرام والعقاب والسياسة الجزائية**، المرجع السابق نفسه، ص:260.

2.2 الحجر بإستعمال تقنيات المعلوماتية

أمّا الحجر على إستعمال الوسائل والتّقنيات الإلكترونية فهو تدبير مقيّد للحريّة يمكن أن يفرض على المجرم المعلوماتي. فمن خلاله يمكن إصدار أمر بمنع بيع أو تأجير أو إعارة أي وسائل من هذا النّوع من المحلات الّتي تتعاطى تجارة الوسائل الإلكترونية. هذا الإجراء لم ينصّ عليه قانون العقوبات اللّبناني، ولا حتّى قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي. لكن لا صعوبة في فرض مثل هذا التّدبير الإحترازي، إذا كان المشرّع أصلًا قد نصّ على تدبير مقيّد للحريّة شبيه له، وهو منع إرتياد الخمّارات الخاصّة بالمجرمين الذين يرتكبون جرائم بتأثير المشروبات الكحولية. ولا شكّ أن التّدابير متنوّعة ومتفرّعة، ويمكن فرضها إلى جانب العقوبة أو بشكل مستقل على الجرمين. لكن يجب دائمًا أن يكون هناك تناسب وملاءمة بين الجريمة المرتكبة، والتّدبير الإحترازي الّذي يتضمّنه الحكم.

النّبذة الثّانية: إستغلال الذّكاء المعلوماتي لصالح الدّول

يعتبر الإجرام المعلوماتي من جرائم الأذكياء الّذي يتطلّب قدرات ومهارات، وطريقة تفكير ذهنيّة لا يملكها أيّ إنسان. وممّا لا شكّ فيه أنّهم قلّة من يرتكبون هذه الجرائم عن طريق القصد، بينما الأغلبيّة يرتكبونها إمّا عن طريق الصّدفة أو الخطأ. ومع إزدياد التّطوّر التّكنولوجي وتقدّم الشّعوب، تطوّرت بدورها أساليب الحرب والسّيطرة وإنتهاك السّيادات الوطنية. كما أصبح العالم قرية كونية مرتبط ببعضه البعض بفعل ظهور التّقنيّة المعلوماتية، ولا حدود بين دولة سوى القواعد الأخلاقية من جهة، والقوّة الدّفاعية الرّادعة من جهة أخرى.

إذ إنّ تطوّر تقنيّات وأساليب الحروب لم يكن الثّورة الحقيقية في هذا المجال، إنّما ما أدهش العالم في عصر المعرفة الّذي نعايشه اليوم هو إنتقال النّزاع بين الدّول، وبينهم وبين الأفراد، وبين الأفراد أنفسهم من

العالم الواقعي الّذي تستعمل فيه الأسلحة الحيّة والقاتلة والمضرّة، إلى حرب إفتراضية في البيئة المعلوماتية هدفها الحصول على المعلومات أو إتلافها أو تشويهها، وخرق سيادات الدّول والتّحكم بها إلكترونيًا مع صعوبة تحديد مصدر الهجوم أو الخطر الّذي يواجهها.

ممّا لا جدال فيه أنّ المعلوماتية دخلت كافّة مجالات الحياة، وأصبحت جميع الدّول المتقدّمة والشّركات الكبرى تعتمد على هذه التّقنيّة لتسيير أعمالها ومخاطبة جمهورها. كما أصبح سكان العالم بأغلبيتهم مستهلكين لهذه المادّة، الّتي لا يمكن بأي شكل من الأشكال التّخلي عنها. هذا الواقع دفع الدّول إلى تغيير إستراتيجياتها العسكرية ومفهومها للأدوات الّتي من خلالها تؤمّن الدّول حماية لنفسها ضد الغير، وكيفية تعزيز قدراتها العسكرية في أيّ حرب يمكن أن تخوضها. فضلًا عن عمل التّحري والإستقصاء وجمع المعلومات الّتي يمكن أن يكون أخطر من الحرب نفسها. فإندفعت الدّول الكبرى والمتطوّرة إلى الإهتمام بالجانب المعلوماتي في مشاريعها العسكرية، وأصبحت توليها أولويّة في مجال التّسلّح العسكري. لذلك أنشأت لهذه الغايات مجموعات متخصّصة لُقّبت بالجيوش الإلكترونية والّتي تخوض حرب حقيقيّة، ولكن في البيئة المعلوماتية لها عتادها وتدريباتها وأشخاصها المختارون بعناية. وبما أنّ الإجرام المعلوماتي مرتبط بالذّكاء، أصبحت الدّول الّتي تتمكّن من جمع العقول البشريّة الأكثر تخصصا في هذا المجال هي الأقوى في ساحة المعركة، فبدأ الإهتمام بالحصول على هؤلاء الأشخاص المتمكنين من التّقنيّة والأذكياء في طريقة إستغلالهم لها. بحسب ذلك، فمن يكون أفضل من المجرمين المعلوماتيين في الإنضمام إلى هذه المجموعات العسكرية التّابعة للدولة؟ الّذين بفضل قدراتهم يتمكنون من إختراق نظم حماية مختلفة ومتطوّرة في المجال المعلوماتي، حيث أنّ إختراقهم لبعض هذه النّظم يمكن أن يشهد لهم على قدراتهم ومؤهلاتهم وذكائهم في تقنيّة المعلومات بغض النّظر عن إلقاء القبض عليهم أم لا.

من هنا برزت أهميّة الإستفادة من إدارة المخاطر ومحاولة تحويل الخطر إلى فرصة، أيّ بدلًا من إلقاء الجزاء على المجرم وتقرير التّدابير الإحترازية عليه والتخوّف المستمر من معاودة إرتكابه للإجرام

المعلوماتي، يمكن للدول أن تستفيد من المجرم المعلوماتي الّذي يتمتّع بقدرات ذهنيّة ومهارات عاليّة في العمل لصالح الدولة. فيتحوّل بهذا الفعل التّهديد النّاتج منه إلى فرصة لتعزيز قدرات الدّولة العسكرية وغير العسكرية من جهة، ومن جهة أخرى تضمن أن هذا المجرم لن يعود إلى الإجرام المعلوماتي لأنّه أصبح يقوم بتفريغ قدراته ونزعته للتقنيّة المعلوماتية بعمل مشروع ضمن الحدود الّتي ترسمها له الدّولة. وبهذا يجب على الدّول أن تتنبّه إلى هذا الإجراء الّذي يمكن أن يكون حلًا مناسبًا لدرء الخطورة الناجمة عن المجرمين المعلوماتيين، وتعزيز قدراتها المعلوماتية بأشخاص قادرين على إحداث التّطوّر التّقني اللازم للدفاع عن سيادة الدّولة الإفتراضي.

المطلب الثّاني: الحقوق الملازمة لضحايا الإجرام المعلوماتي

إنّ الإجرام المعلوماتي عادة ما يكون الغاية منه تحقيق ربح ماديّ معيّن بطريقة غير مشروعة، فيلجأ المجرمون إلى الأشخاص والمؤسّسات والشّركات الّتي تتمتّع بمركز ماليّ جيّد، وأخصُّ بالذّكر المصارف التّجارية. أيضًا يمكن أن تستهدف العمليّة في البيئة المعلوماتية أشخاصًا محددين للنّيل من سمعتهم وإبتزازهم والتّشهير بهم، كما يمكن أن تكون الدّوافع إنتقامية أو عدائية بين دولة وأخرى، أو دولة ومنظمة إجرامية أو أفراد. لذلك تختلف ضحيّة الإجرام المعلوماتي فيما بينها، وهذا الإختلاف ينبع من الغاية التي يهدف لها المجرمون المعلوماتيون من الجريمة [1]. لكن لا جدال في أنّ لكلّ جريمة ضحيّة، وللإجرام المعلوماتي ضحاياه التي ينبغي على المشرّع حمايتهم وضمان حقوقهم تجاه الجريمة المرتكبة. وتتعدّد الضّمانات الّتي يجب أن يتمتّع بها هؤلاء كتلك المقرّرة للضحايا في الجرائم التّقليديّة أو الجرائم الحديثة المقوننة. مثال على ذلك قانون الإتجار بالبشر الذي نصّ على نصوص صريحة تمنح الضّحيّة

[1] ماري آيكن، **التأثير السيبراني**، المرجع السابق نفسه، ص: 269.

ضمانات مختلفة بعد إرتكاب الجريمة بحقها.

وتُعتبر من أهم الضّمانات الّتي يجب أن يضمنها المشرّع لضحايا الإجرام المعلوماتي تتمثّل في إثنين، الأولى هي الحق في سريّة المعلومات (نبذة أولى)، والثّانية تتمثّل في الحق في التّعويض (نبذة ثانية).

النّبذة الأولى: الحق في سريّة المعلومات

الحق في سريّة المعلومات له وجهان، الأوّل هو الحق في الخصوصيّة المعلوماتية أيّ الحق الشّخصي في عدم التّعرّض للبيانات الشخصيّة على الإنترنت. أمّا الثّاني يتمثّل في الحق في سريّة البيانات المعلوماتية في مراحل الدّعوى القضائية وما قبلها وما بعدها، لما يمكن أن يكون لها من أهميّة معيّنة يجب أن لا تظهر للعلن[1].

فالخصوصيّة المعلوماتية تتمثّل بالقواعد المنظّمة لجميع إدارات البيانات الخاصّة الموجودة على الأجهزة الإلكترونية أو على شبكة الإنترنت. "البيانات الخاصّة"، "الخصوصيّة المعلوماتية"، "والمعلومات الإسميّة"، جميعها مصطلحات تشير إلى حق الشّخص في أن يتحكّم بالمعلومات الّتي تخصُّه. بحيث يُطلق على هذه المعلومات "خاصّة" كونها تتعلّق بالشّخص الطّبيعي الّذي تتّصل به هذه المعلومات، كالمعلومات الّتي تتعلّق بأحواله الشخصيّة: كالإسم، الصّورة الشخصيّة، تاريخ ومكان الميلاد، الجنس، ومحل الإقامة؛ أو كالمعلومات الّتي تتعلّق بحالته الصحيّة، حيث تقوم المستشفيات بإعداد ملفات طبيّة للمرضى تتضمّن مجموعة من المعطيات الشخصيّة عن المريض مثل إسمه، جنسه، تاريخ ومكان ولادته، عوارض المرض، وتشخيصه إلخ.. وتكتسب هذه المعلومات طابعها الشّخصي إنطلاقًا من حرص الأشخاص المعنيين بها

[1] Fawn T. Ngo, Raymond Paternoster, **Cybercrime Victimization, An examination of Individual and Situational level factors**, International Journal of Cyber Criminology, Vol 5 Issue 1 January, July 2011, page: 780.

على عدم إفشائها، بالتّاليّ فإنّ أيّ خطأ بسيط في عنوان البريد الإلكتروني أو رقم الفاكس أو الهاتف في إرسال معطيات شخصيّة من قبل المستشفى مثلًا إلى أشخاص لا يتمتّعون بالصّفة لإستلام هذه المعلومات، يُعدّ إفشاءً لمعطيات سريّة ويؤدّي إلى ترتيب المسؤوليّة على عاتق من أفشى هذه المعلومات، ولا سيما إذا كانت الحالة المرضية حرجة كمرض الإيدز مثلًا؛ أو كالمعلومات التي تتعلّق بحالته الماليّة، كبيانات بطاقات الإعتماد، ورقم الحساب المصرفي أو الرّقم الماليّ الوظيفي، وغيرها من المعلومات الّتي تأخذ شكل بيانات وثيقة الإرتباط بكل شخص طبيعي مُعرّف أو قابل للتعريف.

كما تُعرّف الخصوصيّة المعلوماتية بأنها حق الأفراد أو المجموعات أو المؤسّسات في أن يحددوا لأنفسهم متى وكيف وأين يمكن للمعلومات الخاصّة بهم أن تصل للآخرين. وهي حق الفرد في أن يضبط عمليّة جمع المعلومات الشخصيّة عنه، وعمليّة معالجتها آليًّا، وحفظها، وتوزيعها وإستخدامها في صنع القرار الخاصّ به أو المؤثّر فيه [1]. وقد نصّ قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي في الباب الخامس منه، على آليّة حماية البيانات ذات الطّابع الشّخصي وتجميعها، والإجراءات المطلوبة لوضع المعالجات قيد التّنفيذ. بالإضافة إلى حق الوصول والتّصحيح، فقد جاء في المادّة 93 من القانون نفسه على أنّه " على المسؤول عن معالجة البيانات ذات الطّابع الشّخصي أن يتّخذ جميع التّدابير، في ضوء طبيعة البيانات والمخاطر النّاتجة عن المعالجة، لضمان سلامة البيانات وأمنها ولمنع تعرّضها لتشويه أو تضرّرها أو وصولها إلى الأشخاص غير المخولّين الإطّلاع عليها ". بالتّالي في حال تمّ مخالفة الأمر، يمكن أن تُصبح هذه المعلومات والبيانات بين أيدي أشخاص يستغلونها لتحقيق مطامع جرمية بحق أصحابها.

لذلك كان لا بُدّ من التّأكيد على هذه الضّمانة أو الحق للأشخاص في حماية البيانات الشخصيّة،

[1] د. هانيا محمد علي فقيه، **حماية الحق في الخصوصية المعلوماتية**، دراسة تحليلية لواقع الحماية وتحديات العصر، الجامعة اللّبنانية، مركز الدراسات والأبحاث في المعلوماتية القانونية، 2018/1/22.

كونها توفّر على المجرمين العناء لإصطياد الضّحايا، وتُسهّل عليهم إقتراف الجريمة بعد أن تكون كل المعلومات الّتي حصلوا عليها عن طريق الخطأ أو القصد مهمّة لتحقيق النّشاط الجرمي.

أمّا بالنّسبة إلى الحق في سريّة البيانات المعلوماتية في مراحل الدّعوى القضائية وما قبلها وما بعدها، والتي تكون موضوع الجريمة المعلوماتية، فتُعتبر من الحقوق الأساسيّة لضحايا الإجرام المعلوماتي كونها في الأصل معلومات مهمّة، ولو لم تكن كذلك لما كانت هدفًا للمجرمين. وذلك سواء كانت شخصيّة تخصّ فردًا واحدًا، أو تتعلّق ببيانات ومعلومات عن شركة أو مؤسّسة، أو عن الدّولة. فيجب دائمًا على سلطات الملاحقة والتّحقيق والمحاكمة التّقيّد بالسّريّة تجاه المعلومات والبيانات حفاظًا على حقوق الضّحيّة، وضمان عدم وصول هذه المعلومات إلى الغير.

النّبذة الثّانية: الحق في التّعويض

يتشابه التّعويض مع عقوبة الغرامة في أنّ كلّ منهما يمثّل إنتقاصًا للذّمة الماليّة للمحكوم عليه، إلا أنهما يختلفان في أنّ الغرامة الجزائيّة هي عقوبة تُفرض على المجرم بموجب نصّ جزائي، وتعود قيمتها إلى الدّولة ويكون الغرض منها إيلام الجاني وعقابه. بينما التّعويض هو عطل وضرر عن الأضرار الّتي أصابت الضّحيّة من الجريمة [1]. والحق في طلب التّعويض مكرّس في قانون أصول المحكمات الجزائيّة، حيث تنصّ المادّة الخامسة منه على " إنّ دعوى الحق العام، الرامية إلى ملاحقة مرتكبي الجرائم والمسهمين فيها وإلى تطبيق العقوبات والتّدابير في حقهم منوطة بقضاة النّيابة العامّة المعنيين في هذا القانون، أمّا دعوى الحق الشّخصي بالتّعويض عن الضّرر النّاتج عن الجرائم فهي حق لكلّ متضرر ..."، وكما يتبيّن من نصّ هذه المادّة أنّ التّعويض عن الضّرر هو حق مقرّر للجميع عن الجرائم المرتكبة

[1] د. سمير عالية، **الوسيط في شرح قانون العقوبات**، المرجع السابق نفسه، ص: 522.

بحقهم.

كذلك الأمر في الجريمة المعلوماتية، إذ لا تختلف عن باقي الجرائم بالنّسبة إلى التّعويض، الّذي يعود للقاضي أن يحدّده نظرًا لجسامة الجريمة، خطورة المجرم، وضع الضّحيّة، وقيمة البيانات والمعلومات التي تعرّض لها المجرمون. لكن ما تثيره مسألة التّعويض من إشكاليّة في جرائم المعلوماتية يتمثّل في أنّ هذه الجريمة يصعب إكتشاف المجرمين فيها بسبب طابعها الخاصّ القائم على سهولة وسرعة إخفاء الآثار الجرمية، وإرتكابها عن بعد من دون وجود آثار حيّة على أرض الواقع. كما يقابل هذه المشكلة نوعيّة الأضرار الّتي عادة ما تخلّفها هذه الجرائم، والمتمثّلة بالأضرار الماديّة أو الماليّة، الّتي يمكن في حال عدم التّعرف على المجرم ومحاكمته وتقرير التعويض عليه للضحيّة، أن يتأثّر المركز الماليّ لهذه الأخيرة ويزعزع إستقرارها الإقتصادي.

من هنا أصبحت مسألة التّعويض مهمّة جدًا في جرائم المعلوماتية، لأنّ الهدف من الجريمة لا يكون عادة التّعرض الجسدي للأشخاص إنّما التّعرض للبيانات والمعلومات، الّتي تمثّل قيمًا ماديّة وماليّة عاليّة، والّتي تعود بالأصل إلى الأشخاص أو الشّركات أو الدّولة.

من وجهة نظرنا، لا ينبغي إثبات وقوع الضّرر في جرائم المعلوماتية لإقرار التّعويض للضحيّة، لأنّ التّعرض للمعلومات، الدّخول وتشويه الحقائق، التّزوير والإحتيال الإلكتروني وغيرها من الجرائم تكفي بحد ذاتها لأن تُشكّل ضررًا للضحيّة يستحق بموجبها التّعويض.

ختامًا، إنّ حقوق ضحايا المعلوماتية بالسّريّة تجاه المعلومات والبيانات، والحق في التّعويض من المسائل المهمّة الّتي ينبغي على المشرّع تحديد آليّات معيّنة لضمانها. فالنّص على سريّة التّحقيق والمحاكمة في النّصوص الجزائيّة لجرائم المعلوماتية، يضمن إلى حدٍ ما قيمة هذه البيانات المعلوماتية، ويقلّل من الضّرر الّذي يمكن أن ينتج عن الجريمة. وبالمقابل النّص على آليّات تحدد التّعويض يخفّف

على القاضي العناء والجهد، خصوصًا أن هذه الجريمة يصعب تحديد قيمة الأضرار فيها ممّا لها من طابع غير ماديّ.

الفصل الثّاني

أساليب مكافحة السّلوك الإجرامي المعلوماتي

لسوء الحظّ أنّه تمّ توظيف الحاسوب والإنترنت ووسائل التّواصل والإتصال لتحقيق غايات جرمية، وأصبحت إمّا وسيلة أو هدفًا للمجرمين، يتمّ من خلالها إمّا إرتكاب جرائم بواسطة هذه التّقنيات أو جرائم واقعة على التّقنيات هذه بحد ذاتها. لكن على الرّغم من وجود هذه المخاطر الجرمية، إلاّ أنّ تجنّبها ليس مستحيلًا. ذلك بإستعمال أدوات وتقنيات ضرورية لمنع هذه الجرائم وتوظيفها بشكلها المناسب، ممّا يمكّننا من تكوين وقاية مسبقة تحدّ من إرتكاب جرائم المعلوماتية (مطلب أوّل).

أمّا في حال إرتكبت هذه الجرائم فيعتبر اللّجوء إلى القضاء أمرًا واجبًا للتّصدي لهذا الإجرام وكشفه ومعرفة مرتكبيه، وغاياته والحفاظ على قيمة المعلومات الّتي تم التعرّض لها. لذلك يعتبر اللجوء إلى القواعد القانونية الّتي تواجه الإجرام المعلوماتي عاملًا مساعدًا من هذه النّاحية كونه هو الّذي يشرّع هذه الجريمة وينظّم أعمال الملاحقة والتّحقيق والمحاكمة فيها، بالإضافة إلى دور التّعاون الدّولي في مجال التّصدّي للإجرام المعلوماتي الّذي تجاوز الحدود الإقليمية (مطلب ثان).

المطلب الأوّل: الوقاية من الإجرام المعلوماتي

إنّ ما يحمله الإجرام المعلوماتي من خطورة جعل الجميع في خطر، فلم يعد أحدٌ في مَسلَم من هذه الجريمة إلاّ إذا لم يكن هدفًا للمجرمين المعلوماتيين أو وقع ضحيّتهم نتيجة خطأ غير مقصود منهم لإختياره كضحيّة. لكن لا يمكن لنا أن نستغني عن الحاسوب والإنترنت نظرًا لما يحملاه من فؤائد [1]. مقابل هذه

[1] أندرو كونري موراي، فينيسيت ويفر، **دليل سمانتك إلى أمن الإنترنت في المنزل**، المرجع السايق نفسه، ص: 14.

الفوائد، يوجد بعض المخاطر الّتي يجب التّنبّه اليّها ومحاولة التّأكّد من وجود التّقنيات والوسائل الّتي يمكن أن تمنع وجود هذه المخاطر، وتحدّ من خطورتها في حال حصلت. لذلك تُعتبر الوقاية من الإجرام المعلوماتي أمرًا لا بُدّ منه لكلّ شخص يستعمل التّقنيات الإلكترونية والمعلوماتية، والّتي تتجلّى في أدوات وتقنيّات تشكّل خط دفاع أمام القراصنة. لذلك تعتبر الوقاية من الإجرام المعلوماتي خطوة تسبق الإجرام المعلوماتي، الّذي يعرف عنه أنّه دائمًا ما يكون هو السّبّاق في الإجرام عن نظم الحماية الّتي تحاول التّصدي للظاهرة الجرمية الواقعة على تقنيّة المعلومات.

غير أنّ أعمال الوقاية من جرائم المعلوماتية يمكن أن تتّخذ شكلين، أولهما إستعمال الأدوات والتّقنيات والوسائل الضرورية الّتي تمنع الأخطار النّاشئة عن إستعمال تقنيّة الحاسوب والإنترنت وتمنع الهجمات الإلكترونية وتحدّ منها (نبذة أولى). بينما ثانيهما يتمثّل برسم إستراتيجيات توعويّة كشكل من أشكال الوقاية، الّتي تعزّز الوعي لدى مستخدمي الحاسوب والإنترنت أمام المخاطر الّتي يمكن أن تعترضهم (نبذة ثانية).

النّبذة الأولى: الوقاية عبر أدوات الأمان وتقنيّاته

إنّ إستعمال تقنيّة الحاسوب والإنترنت لا بدّ أن يرافقها إتّخاذ العديد من الإجراءات الوقائية الّتي تساعد على إستعمالها بشكل سليم وآمن من أيّ خروقات يمكن أن تتعرّض لها. وتتنوّع هذه الإجراءات، فهناك العديد من التّقنيّات والوسائل البرمجية المساعدة في هذا المجال والّتي يعتبر أهمّها جدران النّار، بروتوكولات الأمان، والأمان اللّاسلكيّ. ويعتبر تطرّقنا في هذه الدّراسة إلى أدوات وتقنيّات الأمان الفنّية والتّقنيّة في في سبيل مساعدة الأشخاص الّذين يستعملون التّقنيّة المعلوماتية على عدم وقوعهم ضحايا هذا الإجرام وهذا هو اللّب من هذه الدّراسة.

1. جدران النّار

يعتبر جدار النّار قطعة برمجية أو قطعة من العتاد، تدير إتصالات الإنترنت من وإلى الحاسوب. حيث يراقب جدار النّار البرامج والتّطبيقات الّتي تحاول أن تقيم إتصال بين الحاسوب المزوّد بجدار نار والإنترنت، كما يقوم أيضًا بالتّحكم ببرامج الحاسوب المسموح لها إرسال المعلومات إلى الإنترنت [1].

لذلك تقوم جدران النّار بتنظيم الوصلات الواردة والصادرة من الحاسوب، ويؤدّي هذه المهمة بإختبار كل تطبيق، أو بروتوكول يحاول أن يفتح منفذًا على الحاسوب. وهذا يتمّ عادة عندما يستعمل الشّخص الإنترنت، فتحاول العديد من البرامج الإتصال به دون طلبه ذلك، ليقوم جدار النّار في هذه الحالة بتنبيهك في كلّ مرّة يحاول أيّ برنامج أن يقيم وصلة مع حاسوبك. بالإضافة إلى ذلك يكون جدار النّار قادرًا على إعتراض حوار الحاسب مع الإنترنت دون أخذ الإذن بذلك، وبذلك يمنع الحاسوب من أن يصبح مصدرًا لبدء عمليّات الهجوم على الحواسيب الأخرى. بحيث يصبح الحاسوب غير مرئي للمجرمين المعلوماتيين، فيغلق بالتّاليّ جميع المنافذ الّتي يمكن أن يتمّ الإختراق من خلالها [2].

2. بروتوكولات الأمان

يعرف بروتوكول الأمان بأنّه إجراء آمن لتنظيم إرسال البيانات بين الحواسيب، وهذه البيانات قد تكون بيانات شخصيّة، ماليّة، طبيّة زبائنيّة، عسكريّة أو غيرها [3]. تعتمد هذه البروتوكولات على نظام التّشفير، والّذي يشار إليه عادة بكلمة المرور، وهي المفتاح الّذي يسمح بالدّخول إلى مركز البيانات المنوي الوصول إليه.

---

[1] طوم توماس، **الخطوة الأولى نحو أمان الشبكات**، المرجع السابق نفسه، ص: 141.

[2] أندرو كونري موراي، فينسنت ويفر، **دليل سمانتك إلى أمن الإنترنت في المنزل**، المرجع السابق نفسه، ص: 45.

[3] طوم توماس، **الخطوة الأولى نحو أمان الشبكات**، المرجع السابق نفسه، ص: 118.

3. الأمان اللّاسلكيّ

بعد أن كانت الهواتف والحواسيب أجهزة مستقلّة عن بعضها البعض وتتفاوت درجة إتصالها بالإنترنت، أصبح من الصّعب اليّوم وضع حدّ يفصل بينها. فبفضل التّقنيّة اللّاسلكيّة، أصبحت هذه التّقنيات قادرة على التّجوال والتكيّف والإتصال فيما بينها، وبينها وبين شبكات الإنترنت الدّاخلية والخارجية[1]. إذ أنّ الوصلة اللّاسلكيّة تحتاج إلى مكوّنين: بطاقة لاسلكيّة أو رقاقة في الحاسوب، ونقطة وصول تدعى أحيانًا موجّه لاسلكيّ. بالإضافة إلى نظام WIFI (Wireless Fidelity) المنزلي أو المتوفّر في الأماكن العامّة والشّركات الخاصّة والمؤسّسات العامّة، أو خدمات الإنترنت المتوفّرة على الهواتف المحمولة[2]. ويأتي دور هذا الإجراء في توفير الأمن المعلوماتي، في أن تحدّد الشّركات أو الجهات الّتي تبيع خدمات WIFI وخدمات الإنترنت على الهواتف، مستوى الأمن والخصوصيّة في الإتصال اللّاسلكيّ بين الأجهزة وشبكات الإنترنت. فالتّكلفة المنخفضة لا تمنح ميزات حماية للمعلومات والخصوصيّة، ولكن يمكن لهذه الشّركات أن تؤمّن هذه الحماية لقاء تكلفة خاصّة.

ختامًا إنّ هذه الإجراءات هي تقنيّة، ويأتي الحديث عنها في هذا السياق كون القانون لا يمكن له وحده حماية الأشخاص من الإجرام المعلوماتي. إذ لا بدّ من أن يقوموا بالإحتياط وإتخاذ بعض الإجراءات الخاصّة الّتي يمكن أن تساعد السّلطة القضائية في إكتشاف الجريمة المعلوماتية وملاحقة مرتكبيها.

النّبذة الثّانية: الوقاية عبر إستراتيجيات التّوعية

في حين كان معظم مجرمي المعلوماتية وضحاياها يتواجدون في الدّول المتقدّمة، إلاّ أنّ عصر العولمة أتاح الفرصة للجناة لمدّ نشاطهم إلى الدّول المتخلّفة، مستفيدين من ضعفهم أمام الجرائم الحديثة

[1] كيم أتنغوف، **الملاحة في الشبكة العنكبوتية**، الدار العربية للعلوم ناشرون، سنة 2015، ص: 33.

[2] أندرو كونري موراي، فينسنت ويفر، **دليل سمانتك إلى أمن الإنترنت في المنزل**، المرجع السابق نفسه، ص: 188.

ومن سهولة النّفاذ إليها بالإبتكارات الإجرامية والتّكنولوجية الجديدة [1]. والأمر الّذي ساهم في تسهيل عمليّة التّسلل والخرق هذه، وإزدياد ضحايا الإجرام المعلوماتي، هو عدم وجود وعي بالتقنيّة التّكنولوجية الحديثة يمكن أن تحدّ من نتائجها السّلبية على الأشخاص والمؤسّسات وحتّى على الدّول. ولتعزيز هذا الوعي بالتّقنيّة المعلوماتية كان لا بُدّ من الدّول، خصوصًا النّامية منها، إتّباع إستراتيجيات معيّنة تُعرّف الأشخاص على مساوئ هذه التّقنيّة وبالتّاليّ تحدّ من نتائجها الإجرامية.

لهذا تفرض هذه الإستراتيجيات التوعويّة وجود خطط ممنهجة ومدروسة، تتبّعها الحكومات والمؤسّسات وحتّى الأهل على مستوى الأسرة، تستطيع من خلالها تأمين حماية لمستخدمي التّقنيّة المعلوماتية. فالعائق الأساس الّذي كان يقف في وجه هذا التّطوّر على مستوى الوعي بالتّقنيّة المعلوماتية، هو غياب التّنمية الإقتصادية عن البلدان النّامية. وذلك لأن فهم التّقنيّة المعلوماتية لا يمكن أن يتمّ دون وجود تنمية محليّة، والّتي تعتبر أساس وجود هذه التّقنيّة، والّتي كانت تهدف إلى تحسين وضع المجتمعات والأفراد، لكن للأسف تم إستغلالها لعمليّات جرمية متنوّعة. لذلك كان لا بُدّ من توظيف التّقنيّة المعلوماتية لصالح التّنمية الإقتصادية وليس خدمةً للأعمال الجرمية، ويتمّ بتكامل كافّة القطاعات والجهات وأفراد المجتمع حول أهميّة التّقنيّة المعلوماتية في العمليّة الإقتصادية، وبيان سلبياتها عليه في حال إستُغلّت بشكل غير سليم.

وللحدّ من جرائم المعلوماتية بتوظيفها في عمليّة التّنمية الإقتصادية، لا يمكن أن يتمّ دون وجود تنمية إجتماعية وفكرية. فوجود حضارات وثقافات تحكم على الإنسان بالجمود والتّقاليّد العمياء وعدم الإنفتاح على التّطوّر التّكنولوجي[2]، سوف يؤدّي إلى إستخدام سلبي للتقنيّة المعلوماتية، ووقوع الأشخاص ضحايا الإجرام المعلوماتي لإفتقادهم القيم الإجتماعية والأنماط الفكرية، الّتي يجب أن يمتلكوها حين يتعاملون مع هذه التّقنيّة.

[1] د. جنان الخوري، **الجرائم الإقتصادية الدّوليّة والجرائم المنظمة العابرة للحدود**، المرجع السابق نفسه، ص: 179.

[2] د. جنان الخوري، **الجرائم الإقتصادية الدّوليّة والجرائم المنظمة العابرة للحدود**، المرجع السابق نفسه، ص: 191.

بالإضافة إلى كلّ من التّنمية الإقتصادية والإجتماعية والفكرية، لا بُدّ للحكومات أن تضع برامج توعوية_حول مخاطر التّقنيّة المعلوماتية، وما ينتج عنها من جرائم، وأهمّيتها على المستوى الشّخصي والمحلي والدّولي. وذلك عبر ندوات وبرامج ودورات تدريبية يتمّ فرضها في جميع المدارس والشّركات والمؤسّسات العامّة والخاصّة. فضلًا عن دور الدّولة في مراقبة الفضاء الإلكتروني، والتّدخّل لحجب مواقع وغلق حسابات إلكترونية يمكن أن تكون خطرة على المجتمع، وإنشاء أجهزة فعّالة وتقنيّة مختصة في معالجة هكذا مواضيع.

إذًا إتّباع هذه الإستراتيجيات أمر بالغ الأهمّية يمكن أن يساعد في الحدّ من جرائم المعلوماتية، ولكن هذه الإستراتيجيات يجب أن تتكامل مع وجود قوانين لا يشوبها أي نقص أو ثغرات يمكن أن تؤدي إلى إفلات المجرمين من العقاب. هذا إضافة إلى ضرورة وجود تعاون دولي بين الدّول من جهة، وبينهم وبين المنظمات الدّوليّة المهتمة بالتّقنيّة المعلوماتية من جهة أخرى، ذلك نظرًا للطابع المعولم للجريمة المعلوماتية العابرة للحدود والمتعدّية على سيادة الدّول.

المطلب الثّاني: التصدّي للإجرام المعلوماتي

إنّ أساليب الوقاية من الإجرام المعلوماتي لا تكفي بحدّ ذاتها لمنع جرائم المعلوماتية، بلّ تحدّ منها. ونظرًا للطابع الخاصّ لهذه الجريمة المتطلّبة للذّكاء البشري بالتّقنيّة المعلوماتية الّتي تشكّل فضاءً واسع، يكثر فيه الثّغرات الّتي من خلالها يرتكب المجرم المعلوماتي عمليّاته الجرمية. فلمواجهة الجريمة المعلوماتية بكافّة مراحلها، لا بُدّ من وجود قانون ينظّم آليّات الملاحقة والتّحقيق والمحاكمة فيها، ويضع العقوبات المناسبة لها. هذا ما إتّجه إليه المشرّع اللّبناني بإصداره قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي (نبذة أولى). بالإضافة إلى ذلك، نظرًا للطابع العابر للحدود للجريمة المعلوماتية، لا بُدّ من

الحديث عن دور التعاون الدّولي في مكافحة هذه الجريمة وملاحقة مجرميها بشكل موجز (النّبذة الثّانية).

النّبذة الأولى: التصدّي من النّاحية القانونية

سنّ المشرّع اللّبناني قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي للتّصدّي للإجرام المعلوماتي، الّذي يعتبر شكلًا من أشكال الإجرام الحديث. وبالرّغم من معالجة القانون المذكور لمختلف أوجه الجريمة المعلوماتية من ناحية تنظيم آليّات الملاحقة والتّحقيق والمحاكمة فيها، بالإضافة إلى وضع آليّات الإثبات الإلكتروني، إلاّ أنّه لم يكن هذا القانون بالمستوى الّذي شرّع فيه ملائمًا للتطوّرات التّكنولوجية والفنّيّة في التقنيّة المعلوماتية.

ففي معالجتنا للمشكلات الّتي تعترض الإجرام المعلوماتي، بيّنا أنّ المجرمين المعلوماتيين يستغلّون الثّغرات الموجودة في قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي لإرتكاب جرائمهم. حيث أنّ آليّات الملاحقة الّتي تفتقد للمعرفة المتخصّصة، وأعمال التّحقيق الّتي تحتاج إلى ضمانات جديدة تراعي مصالح الضّحايا وتقر لهم حقوقًا ملازمة للجريمة المعلوماتية، بالإضافة إلى خلوّ القانون المذكور لنصوص تحدّد الإختصاص فيها، أدّى إلى فرض تطبيق الصّلاحيات الإقليمية والشخصيّة والذّاتية والشّاملة على الجريمة المعلوماتية، الّتي لا تتوافق مع الجرائم التّقليديّة الّتي تعتمد على هذه الآليّة لتحديد الإختصاص. هذا مع غياب المستوى الفنّيّ والتقنيّ الّذي يجب على القضاة التّمكّن منه لمواجهة الجريمة المعلوماتية بشكل يحقق العدالة الجزائيّة.

بناءً على كل ما تقدّم أصبح المجرمون المعلوماتيون يستغلّون الثّغرات القانونية الموجودة في قانون المعاملات الإلكترونية، ويوظّفونها بالطّريقة الّتي تحقّق مصالحهم الجرمية. وبالمقابل لم ينصف القانون نفسه الضّحايا لناحية إقرار ضمانات وحقوق لهم تتلاءم مع طبيعة هذه الجريمة وآثارها الجرمية المختلفة

عن الجرائم التّقليديّة.

هذا وقد بيّن التّطبيق العملي لقانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي إعطاء صلاحيات واسعة لمكتب مكافحة جرائم المعلوماتية والملكية الفكرية التّابع لقوى الأمن الدّاخلي، ممّا إنتقص من دور القضاء في هذا المجال. رغم أنّ هذا المكتب لم ينشأ وفقًا للأصول القانونية، إذ أُنشئ بموجب مذكّرة خدمة رقم 204/609ش2 تاريخ 2006/3/8 دون إصدار مرسوم لتعديل التّنظيم العضوي للأمن الدّاخلي[1]، ما يستدعي تساؤلات حول صلاحيته في ممارسة مهام الضّابطة العدلية والحصول على مساعدات ماليّة من جهات دوليّة ومحليّة في ظلّ عدم قانونيته. لكن رغم الإعتراف بأهمّية جمع الطّاقات والمعرفة التّقنيّة في مجال المعلوماتية لما تساهم بالحدّ من جرائم خطيرة كإباحيّة الأطفال وسرقة البطاقات المصرفية وغيرها، إلاّ أنّ ذلك لا يبرّر المخاوف المتعلّقة بالضّبابية في صلاحيات هذا المكتب.

فأبعد من عدم قانونيته، إنّ صلاحياته الواسعة في مكافحة الجرائم الّتي تستخدم فيها التّقنيات المعلوماتية العاليّة تتيح له عمليًا التعرّض لحريات أساسيّة تمارس على الشّبكة الإلكترونية كحريّة التّعبير والحق بالخصوصيّة. فبدلًا من أن تكتفي النّيابات العامّة بتكليف المكتب بتزويدها بما تحتاج اليّه من خبرات وإمكانات فنّيّة حول التّقنيات المعلوماتية الّتي إستُخدمت لإرتكاب جريمة ما، ذهبت النّيابات العامّة إلى إحالة مجمل الشكاوى المتعلّقة بجرائم إرتكبت على الشّبكة الإلكترونية اليّه مع تكليفه بإجراء تحقيقات جزائيّة كاملة. وقد فتح ذلك للمكتب مجالًا واسعًا لإستدعاء أيّ شخص للتّحقيق معه في مكتبه في قسم المباحث الجنائيّة الخاصّة، ومنه مثلًا من وردت بحقه شكوى بسبب كلام نشره في تغريدة على تويتر أو

[1] قانون تنظيم قوى الأمن الداخلي 17 /1990، المادّة 8، " يحدد بمرسوم يتخذ في مجلس الوزراء بناء على إقتراح وزير الداخلية بعد إستطلاع رأي مجلس القيادة: أ- إنشاء القطعات وتحديد تسمياتها إستنادا إلى التنظيم العضوي المنصوص عنه في المادّة السابقة..".

على صفحات الفايسبوك أو المدوّنات [1]. وقد أظهرت هذه الاستدعاءات خطورة التّمييز لجهة مرجعيّة التّحقيق بين الأعمال الّتي تحصل في العالم الماديّ والّتي تحصل في العالم الإفتراضي، على نحو يؤدّي إلى حرمان المشتبه فيه من الضّمانات القانونية المقرّرة له في مرحلة الملاحقة المقرّرة في قانون العقوبات.

بالإضافة إلى ذلك فإنّ هذا المكتب تمّ نصبه (بشكل غير قانوني) كرقيب على نشاط اللّبنانيين على الشّبكة الإلكترونية، مع تمكينه من التّحرك تلقائيًا في حال الجريمة المشهودة وفي حال ورود معلومات خاصّة به حول حصول نشاط غير شرعي على الإنترنت. لكن في ظلّ خلوّ قانون المعاملات الإلكترونية لتنظيم هذا المكتب الّذي يرعى نشاط اللّبنانيين في الفضاء الإلكتروني، أصبح العالم الإفتراضي عبارة عن أرض خاليّة وغير محمية، بالتّاليّ مشرّعة لكل أنواع التّدخل. فأن يتمّ نصب رقيب عليها دون أن يتمّ توضيح إطار عمله وتنظيم حدود رقابته، يبعث مخاوف عديدة حول إمكانية التّعرّض لخصوصيات المواطنين من مستخدمي الإنترنت عبر رصد أنشطتهم والمواقع الّتي يزورونها والعلاقات والإتصالات الّتي يقومون بها من خلاله. وعلى الرّغم من أن سرّية التّخابر الجاري بواسطة الوسائل الإلكترونية محمية قانونيًا بموجب القانون 1999/140، فإنّ هذا المكتب مجهّز بالإمكانيات التّقنيّة للإطّلاع على المراسلات الخاصّة الّتي يقوم بها اللّبنانيّون. ولا يرد على هذه المخاوف أن المكتب لا يتحرّك إلاّ بإشارة من النّيابات العامّة، لما لدى الضّابطة العدليّة من إمكانية واسعة للتأثير على مسار التّحقيقات، خاصّة في ظلّ قلّة خبرة الجسم القضائي لفهم التّقنيات المعلوماتية الجديدة.

ففي الوقت الّذي يناقش العالم كيفيّة حماية الحق بالخصوصيّة، نرى أنّ لبنان ينصّب رقيبًا على الشّبكة الإلكترونية دون وضع أي إطار حمائي بهدف ضمان عدم التّعرّض التّعسفي لحياة مستخدمي

[1] غيدة فرنجية: المفكرة القانونية، مكتب مكافحة الجرائم المعلوماتية، رقابة غير منظمة على المساحات الإلكترونية، 2013/12/3، https://www.legal-agenda.com/article.php?id=594، تاريخ الدخول إلى الموقع 2019/9/22.

الإنترنت الخاصّة، والّتي تشمل المراسلات والبيانات والصّور الخاصّة... وليس المطلوب تنظيم الأعمال الّتي تحصل على هذه الشّبكة، لكن المطلوب وضع ضوابط لإمكانية ممارسة رقابة هذا المكتب على نحو يحمي الحق بالخصوصيّة، ولا يفتح المجال للتعرّض لها سندًا للمادة 12 من الإعلان العالمي لحقوق الإنسان الّتي تكرّس الحق في حماية القانون من أيّ تَدخُّل تعسّفي في الحياة الخاصّة [1].

وبناءً على ما تقدّم يمكننا القول أنّ قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي المشرّع حديثًا يفتقد لكثير من النّصوص القانونية اللّازمة لمواجهة التّطوّر في تقنيّة المعلومات، والّتي من خلاله يتمّ إرتكاب هذه الجرائم. فالبداية كانت من إكتشاف الجرائم المعلوماتية، إلى ملاحقتها والتّحقيق فيها، ثم تحديد الإختصاص المكاني والنّوعي الصّالح للنظر في هذه الجرائم، وصولًا إلى تأمين محاكمة عادلة تضمّ قضاة مختصّين في التّقنيّة المعلوماتية ومواكبين للتطوّر الّذي تشهده.

النّبذة الثّانية: التصدّي عبر التّعاون الدّولي

إنّ أجهزة إنفاذ القانون لا تستطيع تجاوز حدودها الإقليمية لممارسة الأعمال القضائية على المجرمين الفارّين من وجه العدالة، وكذلك التّواصل وحماية الضّحايا الّتي تصيبهم جريمة المعلوماتية العابرة للحدود. لذلك كان لا بُدّ من إيجاد آليّة معيّنة للتعاون مع الدّولة الّتي ينبغي إتّخاذ الإجراءات القضائية فوق إقليمها، ولكي يتمّ ذلك ويكون هناك تعاون دولي ناجح في مجال تحقيق العدالة كان لزامًا تنظيم هذا النّوع من التّعاون الدّولي تشريعيًا وقضائيًا وتنفيذيًا. فالدّولة ما دامت عضوًا في المجتمع الدّولي لا بُدّ لها من الإيفاء بالإلتزامات المترتّبة على هذه العضوية ومن ضمنها الإرتباط بعلاقات دوليّة وثنائيّة تتعلّق بإستلام وتسليم

[1] غيدة فرنجية، المفكرة القانونية، مكتب مكافحة الجرائم المعلوماتية، رقابة غير منظمة على المساحات الإلكترونية، 2013/12/3، https://www.legal-agenda.com/article.php?id=594، تاريخ الدخول إلى الموقع 2019/9/22.

المجرمين. إنّ بطء الإجراءات الرّسميّة يجازف بفقدان الأدلّة، وقد تكون بلدان متعدّدة متورّطة في الأمر. لذا تشكّل متابعة وحفظ سلسلة الأدلّة تحدّيًا كبيرًا، بل حتّى الجرائم "المحلّية" قد يكون لها بعدًا دوليًّا، وربما تكون هناك حاجة إلى طلب المساعدة من جميع البلدان الّتي مرّت الهجمة من خلالها.

وإذا كانت هناك جريمة واضحة تستحق التّحقيق بالفعل، فقد تكون هناك حاجة إلى مساعدة من السّلطات في البلد الّذي كان منشأ الجريمة، أو من السّلطات في البلد أو البلدان الّتي عبر من خلالها النّشاط المجرَّم وهو في طريقه إلى الهدف، أو حيث قد توجد أدلّة الجريمة. وهناك عنصران أساسيّان للتعاون: المساعدة غير الرّسميّة من محقّق لآخر، والمساعدة الرّسميّة المتبادلة [1]. فضلًا عن أنّ المساعدة غير الرّسميّة قد تكون أسرع إنجازًا، وهي الوسيلة المفضّلة للنهج حين لا تكون هناك حاجة إلى صلاحيات إلزاميّة (أيّ أوامر تفتيش أو طلب تسليم المجرم). فهي تقوم على وجود علاقات عمل جيّدة بين أجهزة شرطة البلدان المعنيّة، وتولد نتيجة الإتصالات الّتي جرت مع الوقت، في مسار المؤتمرات وزيارات المجاملة والتّحقيقات المشتركة السّابقة.

من ناحية أخرى، فإنّ المساعدة الرّسميّة المتبادلة هي عمليّة أكثر إرهاقًا يتمّ اللّجوء اليّها عادة عملًا بترتيبات معاهدات بين البلدان المعنيّة وتشمل تبادل الوثائق الرّسميّة. وهي تشترط في الغالب الأعم أن تكون الجريمة المعنيّة على درجة معيّنة من القسوة وأن تشكّل جريمة في كل من البلدان الطّالبة والموجّه اليّها الطّلب. ويشار إلى هذا الأمر الأخير باعتباره "تجريمًا مزدوجًا".

في حين لم تعد تشكّل الجرائم المعلوماتية خطرًا على سرّية النّظم الحاسوبية أو سلامتها أو توافرها فحسب، بل تعدّت إلى أمن البنى الأساسيّة الحرجة، ومع تميّزها بالعالمية وبكونها عابرة للحدود فإن مكافحتها لا تتحقّق إلا بوجود تعاون دولي على المستوى الإجرائي الجنائي. بحيث يسمح بالإتصال المباشر

[1] بدري فيصل، **مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي**، أطروحة لنيل شهادة دكتوراه علوم تخصص (قانون عام)، جامعة الجزائر 1(بن يوسف بن خلدة)، كلية الحقوق، سنة 2018/2017– ص: 10.

بين أجهزة الشّرطة في الدّول المختلفة، وذلك بإنشاء مكاتب متخصّصة لجمع المعلومات عن مرتكبي الجرائم المتعلّقة بالإنترنت وتعميمها. لذلك أصبحت الحاجة ماسّة إلى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة وتتعاون من خلاله أجهزة الشّرطة في الدّول المختلفة، خاصّة فيما يتعلّق بتبادل المعلومات المتعلّقة بالجريمة والمجرمين والضّحايا بأقصى سرعة ممكنة، بالإضافة إلى تعقب المجرمين الفارّين من وجه العدالة وتحديد مكان الضّحايا الّذين يقعون فريسة هؤلاء.

لذلك تأسّس الأنتربول وهو أكبر منظمة شرطيّة في العالم، عام 1923، ومهمته تتمثّل في تقديم المساعدة إلى أجهزة إنفاذ القانون في بلدانه الأعضاء ال 186 لمكافحة جميع أشكال الإجرام عبر الوطني، حيث له بنى تحتية متطوّرة للإسناد الفنّيّ والميدانيّ، وذلك عبر تمكين قوى الشّرطة في سائر أنحاء العالم من مواجهة التّحديات الإجرامية المتنامية في القرن الحادي والعشرين. وتركّز المنظمة إهتمامها في ستة مجالات إجرامية أعطتها الأوّلويّة هي الفساد، المخدرات والإجرام المنظّم، الإجرام المآليّ والمرتبط بالتكنولوجيا المتقدّمة، المجرمون الفارّون، تهديد السّلامة العامّة والإرهاب، والإتجار في البشر [1]. يقوم الإنتربول بعمليّة ملاحقة مجرمي المعلوماتية عامّة وشبكة الإنترنت خاصّة، عن طريق تعقّب الأدلّة الرقميّة وضبطها، والقيام بعمليّة التّفتيش العابر للحدود لمكونات الحاسب الآليّ المنطقيّة والأنظمة المعلوماتية وشبكات الإتصال بحثًا عمّا قد تحويه من أدلّة وبراهين على إرتكاب الجريمة المعلوماتية، كلّها أمور تستدعي القيام ببعض العمليّات الشّرطية والفنّيّة والأمنيّة المشتركة، وهي من شأنها صقل مهارات وخبرات القائمين على مكافحة تلك الجرائم، وبالتّاليّ وضع حدّ لها. وعلى غرار هذه المنظمة، أنشأ المجلس الأوروبي في لكسمبورج عام 1991م شرطة أوربية لتكون همزة وصل بين أجهزة الشّرطة الوطنيّة في الدّول المنظّمة ولملاحقة الجناة في الجرائم العابرة للحدود ومنها بطبيعة الحال الجرائم المتعلّقة بالإنترنت. أمّا على

[1] Malcom Anderson, **Policing the world – Interpol the Politics of International Police Cooperation**, Clarendon press. Oxford, 1989, p: 168-185.

المستوى العربي نجد أن مجلس وزراء الدّاخلية العرب أنشأ المكتب العربي للشرطة الجنائية، بهدف تأمين وتنمية التّعاون بين أجهزة الشّرطة في الدّول الأعضاء في مجال مكافحة الجريمة وملاحقة المجرمين، في حدود القوانين والأنظمة المعمول بها في كل دولة. بالإضافة إلى تقديم المعونة في مجال دعم وتطوير أجهزة الشّرطة في الدّول الأعضاء.

يتجلّى التّعاون الدّولي لمكافحة الجرائم المعلوماتية في أشكال ثلاثة، التّعاون الأمني الدّولي، التّعاون القضائي والتّعاون الدّولي بشأن تسليم المجرمين. حيث يعرف التّعاون الأمني الدّولي بأنّه تبادل العون والمساعدة وتضافر الجهود المشتركة بين طرفين دوليين أو أكثر، لتحقيق نفع أو خدمة أو مصلحة مشتركة في مجال التّصدي لمخاطر الإجرام وما يرتبط به من مجالات أخرى، مثل مجال العدالة الجزائيّة، مجال الأمن، أو لتخطّي مشكلات الحدود والسّيادة الّتي يتعرّض لها هذا الإجرام [1] . كما يشمل التّعاون الأمني الدّولي مجالات مختلفة، كالمجال الشّرطي، المجال القانوني، والمجال القضائي. ومرد ذلك أنّ تحقيق الأمن يتطلّب تنفيذ إجراءات تتعلّق بتلك المجالات مجتمعة. عدا عن أنّ التعاون الأمني الدّولي يمثّل بين أجهزة الشّرطة الجنائية المخصّصة لمكافحة الجرائم المعلوماتية في الدّول أحد الوسائل الهامة الّتي يمكن من خلالها منع الجرائم المعلوماتية أو إنخفاضها. وتؤكد التّحقيقات في الجرائم عامّة – والمعلوماتية خاصّة على أهمّية التعاون الأمني الدّولي، حيث يستحيل على الدّولة بمفردها القضاء على هذه الجرائم الدّوليّة العابرة للحدود.

بالإضافة، فإن الدّور الفعلي للتعاون الأمني الدّولي لمكافحة جرائم المعلوماتية يتحقّق بالتّنسيق المستمر بين المؤسّسات الأمنيّة بآليّاتها المختلفة، تناول ظاهرة الإجرام المعلوماتي بشكل علمي وتوفير

[1] د. عادل عبد العال إبراهيم خراشي، **إشكاليّات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها**، كلية الشريعة والقانون بالقاهرة، سنة 2018 – ص: 188.

المعلومات الإحصائية والبيانات اللازمة، سواء ما يتعلّق بالجريمة أو ما يتعلّق بمرتكبيها[1]. فضلًا عن الضّحايا الّذين يقعون فريسة هؤلاء المجرمين، وتحديد سبل التعاون في مجال التّدريب والتّعاون التّقنيّ وذلك عبر تحديد مدوّنة دوليّة تتضمّن توحيد المعايير والأركان القانونية الّتي تقوم عليها هذه الجرائم.

بينما التّعاون القضائي الدّولي فيعرّف على أنّه كلّ إجراء قضائي تقوم به دولة من شأنها تسهيل مهمّة المحاكمة في دولة أخرى بصدد جريمة من الجرائم [2]. فيتحقق التّعاون القضائي في خطوات ثلاث، أوّلها الطّلب الّذي تقدّمه الدّولة صاحبة الإختصاص الجنائي بالمحاكمة، فيخضع هذا الطّلب لقانون الدّولة الطّالبة وفي نطاق الإتّفاقية الّتي تعقدها مع الدّولة الّتي تقدّم المساعدة. أمّا الخطوة الثّانية فتتمثّل في فحص الطّلب المقدّم من الدّولة الطّالبة إلى الدّولة الّتي ستقدّم المساعدة، ويتمّ ذلك عن طريق التّحقّق من إعتبار الواقعة المطلوب تحقيقها تعدّ جريمة وفقًا لقانون الدّولة الطّالبة، في ضوء مدى إختصاص الدّولة المطلوب منها بإجابة هذا الطّلب، وفقًا لنصوص الإتّفاقية الّتي تعقدها مع الدّولة الطّالبة. بينما الخطوة الثّالثة والأخيرة، هي تنفيذ المساعدة القضائية وتتمّ وفقًا لقواعد الدّولة المطلوب منها، حيث يتمّ تنفيذ الإجراء وفقًا لقانون الدّولة الّتي تنفّذه [3].

من صور التّعاون القضائي الدّولي لمكافحة جرائم المعلوماتية، تبادل المعلومات بين سلطة قضائية وطنيّة وأخرى أجنبيّة مع حضور الشّهود والخبراء من دولة إلى أخرى، والإنابة القضائية الدّوليّة. بحيث يتمّ ذلك بطلب إتّخاذ إجراء قضائي من إجراءات الدّعوى الجنائية، تتقدّم به الدّولة الطّالبة إلى الدّولة المطلوب إليها لضرورة ذلك للفصل في مسألة معروضة على السّلطة القضائية في الدّولة الطّالبة ويتعذّر عليها القيام بها بنفسها.

---

[1] د. عادل عبد العال إبراهيم خراشي، **إشكاليّات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها**، المرجع السابق نفسه، ص: 192-193.

[2] د. عادل عبد العال إبراهيم خراشي، **إشكاليّات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها**، المرجع السابق نفسه، ص:201-202.

[3] بدري فيصل، **مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي**، المرجع السابق نفسه، ص 62.

أمّا التعاون الدّولي لتسليم المجرمين، فيعرّف على أنّه الإجراء الّتي تسلّم به دولة، إستنادًا إلى معاهد أو تأسيسًا على المعاملة بالمثل عادة، إلى دولة أخرى شخصًا تطلبه الدّولة الأخيرة لإتهامه أو لأنّه محكوم عليه بعقوبة جنائية [1]. إذ يقوم مبدأ تسليم المجرمين على أساس أنّ الدّولة الّتي يتواجد على إقليمها المتّهم بإرتكاب إحدى الجرائم العابرة للحدود مثل جرائم الإنترنت، عليها أن تقوم بمحاكمته إذا كان تشريعها يسمح بذلك، وإلاّ عليها أن تقوم بتسليمه لمحاكمته بمعرفة دولة أخرى مختصّة، وذلك إمّا حسب القانون أو وجود إتفاقية إسترداد بين البلدان. ويشترط في التّسليم أن يكون هناك تجريم مزدوج من الدّولة المطلوب منها الإسترداد والدّولة الطّالبة للإسترداد، كما أن يشكّل الفعل جريمة من الجرائم الجائز بشأنها التّسليم.

لكن ما يؤخذ على التعاون الدّولي اليوم هو عدم فعاليّته في الدّول النّامية أو الدّول الّتي لم تتمرّس النّظم المعلوماتية، والّتي تفتقد إلى أجهزة حمائية أمام أيّ تعرّض إلكتروني يمكن أن يصيبها. بالإضافة إلى عدم وجود مجموعات بشرية فاعلة ورسميّة متخصّصة في هذه التّقنيّة الحديثة. أيضًا فإنّ التعاون الدّولي غيّب الإهتمام بشكل أساسي لضحيّة الإجرام المعلوماتي الّذي لا يقف عند بلد ولا على أشخاص ولا على عدديّة معيّنة. بل يمكن أن يتمّ إختيارضحاياه وفقًا لآليّات تتعلّق بالجريمة وأهدافها، فيصبح هذا الإجرام عابرًا للحدود ويصيب ضحايا في بلدان مختلفة ومتنوّعة في هجمة إلكترونية واحدة. فبالرّغم من توجّه التّعاون الدّولي لمكافحة الجريمة المعلوماتية وإلقاء القبض على مجرميها، فإنّ مسألة ضّحايا هذا الإجرام تشكّل إشكاليّة قانونية وإجتماعيّة، دونهما لا تتحقّق العدالة الجزائية.

[1] د. جنان فايز الخوري، **الجرائم الإقتصادية الدّوليّة والجرائم المنظمة العابرة للحدود**، المرجع السابق نفسه، ص: 419.

الخاتمة

يعتبر الإجرام المعلوماتي من أكبر السّلبيات الّتي خلفتها الثّورة الرّقمية، هذا الإجرام الّذي يصعب حتّى الآن الإتفاق على تعريف موحّد له والمتميّز عن الإجرام التّقليدي بعدّة خصائص، لعلّ أهمّها طابعه العابر للحدود وإنفراده بخاصّية الإجرام الناعم الّذي لا يحتاج لإستخدام العنف عند إرتكابه. وبنشأة هذه الظاهرة الإجرامية ترتّب عنها بروز طائفة جديدة من المجرمين، الّذين يمتازون بالذّكاء، الخبرة والمهارة لإستعمال التّقنيّة المعلوماتية من جهة. بالإضافة إلى بروز طائفة جديدة من الضّحايا الّذين يقعون فريسة هؤلاء المجرمين، نتيجة ضعفهم في إستعمال التّقنيّة المعلوماتية وقلّة إحترازهم وخبرتهم في الولوج إلى البرامج والمواقع الحاسوبية المختلفة.

هذا النمط الجديد من المجرمين والضّحايا الّذي إنبثق عن الإجرام المعلوماتي، والّذي يعتبر من الجرائم الحديثة، أحدث نقصًا في علم الإجرام الّذي كان يدرس أطراف الجريمة بوجهها التّقليدي. لذلك كان من الضّروري التّطرّق إلى كل من مجرم وضحية الإجرام المعلوماتي على ضوء علم الإجرام، الّذي يساعد على تأسيس آليّة تمكّن من التّصدّي ومواجهة هذه الظاهرة الإجرامية، خصوصًا مقابل ما تطرحه هذه الأخيرة من تحدّيات على المستوى القانوني والعملي، وعلى مستوى طريقة تنفيذها من قبل المجرمين القائمة على التّخطيط والتّنظيم والدّقة، وصعوبة معرفة المتضرّرين منها.

ومع تغيّر البيئة الجرمية في الإجرام المعلوماتي من بيئة تقليدية واقعية إلى بيئة معلوماتية إفتراضية، والتّطوّر الحاصل على مستوى شخصيّة كلّ من المجرم والضّحيّة المعلوماتيين، طرأ بدوره تبدّل على مستوى السلوك الجرمي الّذي يرتكبه المجرم والّذي يقع على الضّحيّة. حيث ظهر نوعان من السلوك الإجرامي المرتكب في البيئة المعلوماتية، الأول هو السلوك الجرمي المرتكب بواسطة التّقنيّة المعلوماتية، أمّا الثّاني فهو السلوك الجرمي المرتكب على تكنولوجيا المعلومات بحدّ ذاتها.

بفعل هذا السلوك الجرمي المتطوّر والجديد في السّاحة الجرمية، كانت وضعيّة المجرم والضّحيّة المعلوماتيين ملتبسة من ناحية فهمنا لكلّ منهما، الطريقة المتّبعة لإرتكاب الإجرام المعلوماتي والآليّة

المبتكرة لإختيار الضّحايا فيه. فكان لا بُدّ من إجراء تصنيف قانوني وعملي لكلّ منهما، إستنادًا لنوع الأعمال الجرمية المرتكبة في البيئة المعلوماتية. فتنوّع المجرمون المعلوماتيون بين محترفين وغير محترفين، كما شهدنا على بروز ضحايا على مستوى عالي كالمؤسّسات الماليّة والشّركات المصرفية وحتّى الدّولة، الّتي كانت في السّياسة العقابية التّقليدية وقبل ظهور الإجرام الحديث وخصوصًا الإجرام المعلوماتي، هي الحامي للسيادة والجهة المعنية في تطبيق القوانين والأنظمة.

هذا النموذج الحديث من الإجرام، كان له وقعه على المسؤوليّة الجزائية الّتي يرتّبها القانون على كلّ من المسؤولين عن الجريمة الجزائية ويُنزل بهم العقوبات المقرّرة قانونًا. فبالرّغم من وجود دراسات سابقة تعالج المسؤوليّة الجزائية في الإجرام المعلوماتي، إلاّ أنّه كان من الضّروري التّطرّق إلى بعض أوجه هذه المسؤوليّة الّتي تمثّل إشكاليّات لم تعالج بعد في النّظام القانوني أو على مستوى الفقه. تلك الإشكاليّات المرتبطة بشكل أو بآخر بالمجرم المعلوماتي كونها تترتّب عليه، كما تعني الضّحيّة لأنّها هي الجهة المتضرّرة من الجريمة، وإلقاء المسؤوليّة الجزائية على المجرمين المعلوماتين هو نوع من الحماية لها.

لذلك ظهر نوع آخر من المساهمة الجرمية وذلك مع ظهور الإجرام المعلوماتي، والّتي تنطبق نوعًا ما على الإجرام الحديث بكافة أشكاله وأهمّها كان بروز المسؤوليّة الجماعية عن الإجرام المعلوماتي المنظّم، ومسؤوليّة المجرم الأصلي والمجرم التّقني المنفّذ.

وبفعل خصوصية الإجرام المعلوماتي، كان للضحية نصيب في المسؤوليّة الجزائية، حيث برزت في بعض السّاحات الجرمية إمّا كضحية لها دور مساهم في إرتكاب الإجرام بحقها والّذي أثّر بشكل مباشر على المسؤوليّة الجزائية للمجرم إنتقاصا. وإمّا خطأ الضّحيّة عن الإجرام المعلوماتي الواقع عليه والّذي دحضنا من خلاله أيّ تأثير لها على المسؤوليّة الجزائية.

لكن في الوقت نفسه لم تسلم المسؤوليّة الجزائية من تأثيرات الإجرام المعلوماتي عليها، حيث برزت العديد من الإشكاليّات المؤثّرة فيها، إمّا بشكل مباشر على مستوى القواعد الإجرائية كالمسائل الّتي تعترض

أعمال الملاحقة والتّحقيق والإثبات والإختصاص، أو على مستوى وضعيّة الحدث المعلوماتي المنحرف عليها من جهة مقابلة الذّكاء بالوعي والإرادة، ممّا يستتبع إلقاء المسؤوليّة الجزائية عليه كالرّاشد نفسه والّذي بيّنا عدم صحته، أو على مستوى عدم ملاءمة قانون الأحداث اللّبناني للجرائم المرتكبة من الحدث المعلوماتي المنحرف.

ولم ينتهِ الإجرام المعلوماتي عند تعرّضه للمسؤوليّة الجزائية، إنّما برزت الغاية إلى إعادة النّظر في سياسة الجزاء العقابي التّقليدي الّذي كان قائمًا على العقوبات المانعة والمقيّدة للحرّية، بالإضافة إلى بعض التّدابير الإحترازية الّتي تتلاءم مع طبيعة الجرائم التّقليدية. فظهر خلال هذه الدّراسة الحاجة الملحّة إلى عقوبات وتدابير أكثر فعاليّة في تحقيق العدالة الجزائية، وفي نفس الوقت تتناسب مع الإجرام المعلوماتي. فكان للعقوبات الماليّة كالمصادرة والغرامة، الأثر البالغ في معاقبة المجرمين عن أفعالهم الجرمية دون الإستغناء عن العقوبات التّقليديّة الّتي يجب أن تأتي في المرحلة الثانوية. وكذلك الأمر بالنّسبة إلى التّدابير الإحترازية، حيث بيّنا بعض التّدابير المستحدثة والفعّالة في الحدّ من الخطورة الإجرامية كحجر إستعمال الوسائل الإلكترونية وغيرها.

وإذا كان الجزاء العقابي هو أداة لمعاقبة المجرمين أو الحدّ من إجرامهم المتفلّت، فإنّه لا بُدّ من أن يكون مقرونًا بضمانات لضحايا الإجرام المعلوماتي، والّتي يتمثّل أهمّها في سرية المعلومات إمّا بالنّسبة إلى المعلومات الّتي وقعت عليها الأعمال الجرمية، أو المعلومات الإلكترونية الشّخصيّة الخاصّة بالضّحيّة. بالإضافة إلى الحق في التّعويض عن الجرم المعلوماتي المرتكب، والّذي يصطدم عادة بعدم معرفة المجرم المعلوماتي وإلقاء القبض عليه.

بناءً على كل ما سبق ذكره وجرّاء كلّ ما يعترض ماهية كل من مجرم وضحية الإجرام المعلوماتي من إشكاليّات قانونية وعمليّة، كانت الوقاية من هذا الإجرام عبر تقنيّات الأمان وإستراتيجيات التوعية محطّة مساعدة لتجنّب الوقوع في بئر الإجرام المعلوماتي، الّذي إن كان قد وقع يكون التّصدّي له أمرًا واجبًا عبر

القوانين اللّبنانية، وخصوصًا قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي اللّبناني الّذي يحتاج إلى تضافر الجهود المحلّية كما الدّولية، عبر تعاون دولي يصب إهتمامه على مكافحة الإجرام المعلوماتي بأنجح الوسائل.

ختامًا إنّ الإجرام المعلوماتي، والتّطوّر الحاصل على مستوى أطراف هذا الإجرام، وما شهدناه من إشكاليّات تعترضهما بيّن لنا ضرورة دراسة هذه الظاهرة الإجرامية بمختلف أشكالها وأبعادها. بحيث وضعت وفسّرت وبنت مفهومًا أوليًّا لكلّ من المجرم والضّحيّة المعلوماتيين، الّذي يساعدنا أكثر على فهم طبيعة الإجرام المعلوماتي وطريقة حصوله، آليّة الوقاية منه والتّصدّي له محقّقين غاية علم الإجرام في دراسة كل من مجرم وضحية الإجرام المعلوماتي.

المقترحات

- إن البحث في شخصية مجرم وضحية الإجرام المعلوماتي يقتضي فهمًا أكثر للإجرام المعلوماتي وليس فقط التركيز على الجريمة المعلوماتية المنصوص عنها قانونا وذلك لأنه بفعل التطور التكنولوجي السريع في النظم المعلوماتية تطورت بدورها السلوكيات الجرمية للمجرمين المعلوماتيين، فأصبح الإجرام المعلوماتي بعضه مجرم وبعضه الآخر غير معاقب عليه قانونا مما يؤثر بشكل أو بآخر على فهم ماهية كل من مجرم وضحية الإجرام المعلوماتي.
- ضرورة إستحداث دراسات خاصة عن ضحايا جرائم العصر الحديث وخصوصا ضحايا الإجرام المعلوماتي، وسن قوانين تتلاءم مع وضعهم وإقرار ضمانات تمكنهم من الإلتجاء للقضاء دون خوف أو تردد.
- إعادة النظر في أحكام المسؤولية الجزائية بما يتناسب مع جرائم المعلوماتية، والبحث بجدية في مسؤولية الضحية عن مساهمتها في إرتكاب الإجرام المعلوماتي عليها.
- تطوير أحكام المساهمة الجرمية الفردية بما يتلاءم مع الصور الجديدة للإسهام الجرمي في الإجرام المعلوماتي بالنسبة لكل من المجرم والضحية، وإضافة نوع جديد من المساهمة الجرمية ألا وهي المساهمة الجماعية عن الإجرام المرتكب من الجماعات الإجرامية المنظمة.
- وضع آلية عملية منصوص عنها قانونا تحدد كيفية عمل مكتب مكافحة جرائم المعلوماتية التابع لمؤسسة قوى الأمن الداخلي، والتشدد بالرقابة القضائية على هذا الفرع.
- الإهتمام الكبير بالعقوبات المالية خصوصا المصادرة والغرامة لما يمثلانه من دور رادع في جرائم العصر الحديث وخصوصا الإجرام المعلوماتي.
- تطوير قانون حماية الأحداث المنحرفين او المعرضين للخطر، رقم 422، 6 حزيران 2002، لتلاؤمِه مع وضع الأحداث المعلوماتيين المنحرفين.
- تطوير قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي اللبناني رقم 81، عدد 45 تاريخ 18 تشرين الأول 2018، بما يتناسب مع التطور الذي شهده الإجرام المعلوماتي، حيث ان القانون الموجود يتلاءم مع الجيل الثالث من التطور التكنولوجي في حين أننا أصبحنا في الجيل السابع من هذا التطور.

المراجع باللّغة العربية:

1- أوتاني، (صفاء)، الأستاذ، (سوزان)، **عدم ملائمة قانون الأحداث السوري لإنحراف الأحداث المعلوماتي**، مجلة جامعة البعث، المجلد 40، العدد 5، 2018.

2- الأشقر، (منى)، جبور، (محمود عارف)، **القانون والإنترنت (تحدي التكيف والضبط)**، المنشورات الحقوقية صادر، 2008.

3- الخوري، (جنان)، **الجرائم الإقتصادية الدّولية والجرائم المنظّمة العابرة للحدود**، المنشورات الحقوقية، صادر، 2009.

4- الشاذلي، (فتوح)، عفيفي، (عفيف كامل)، **جرائم الحاسوب وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة**، منشورات الحلبي الحقوقية، 2007.

5- العجمي، (عبد الله دغش)، **المشكلات العملية والقانوينة للجرائم الإلكترونية**، دراسة مقارنة، جامعة الشرق الأوسط، 2014.

6- الغريب، (إنتصار نوري)، **فيروسات الحاسوب**، دار الراتب الجامعية، بيروت، 1994.

7- الغول، (حسين محمد)، **جرائم شبكة الإنترنت والمسؤوليّة الجزاءية الناشئة عنها، دراسة مقارنة**، مكتبة بدران الحقوقية، سنة 2005.

9- الفاضل، (محمد)، **التعاون الدولي في مكافحة الإجرام**، 1966.

10- الفيل، (علي عدنان)، **الإجرام الإلكتروني، دراسة مقارنة**، جامعة الموصل، كلية الحقوق، منشورات زين الحقوقية، 2011.

11- بلوط، (محمد)، فقيه، (ناريمان)، **الجرائم عند النساء**، 2003/2002.

12- جعفر، (علي عبود)، **جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة (دراسة مقارنة)**، منشورات زين الحقوقية، 2013.

13- خراشي، (عادل عبد العال إبراهيم)، **إشكاليّات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها**، كلية الشريعة والقانون بالقاهرة، 2018.

14- سالم، (محمد علي)، هجيج، (حسون عبيد)، **الجريمة المعلوماتية**، كلية القانون جامعة بابل، مجلة جامعة بابل، العلوم الإنسانية، المجلد 14 العدد 2، 2007.

15- شحادة، (زينات طلعت)، **الأعمال الجرمية الّتي تستهدف الانظمة المعلوماتية**، المنشورات الحقوقية صادر، 2009.

17- شومان، (نمر)، **التكنولوجيا الجرمية الحديثة وأهميتها في الإثبات الجنائي**، دراسة في الحقوق، 2011.

18- عالية، (سمير)، **مبادئ علم الإجرام والعقاب والسّياسة الجزائية، أسباب الإجرام ومكافحته جزائيًا**، منشورات الحلبي الحقوقية، 2019.

19- عالية، (سمير)، عالية، (هيثم سمير)، **الوسيط في شرح قانون العقوبات، القسم العام، دراسة مقارنة**، المؤسسة الجامعية للدراسات والنشر والتوزيع، 2010.

20- عبد الرؤوف الحق، (محمد طارق)، **جريمة الإحتيال عبر الإنترنت، الأحكام الموضوعية والأحكام الإجرائية**، منشورات الحلبي الحقوقية، 2011.

21- عرب، (يونس)، **جرائم الحاسوب والإنترنت**، الجزء الأول، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، إتحاد المصارف العربية، 2002.

22- عفيفي، (عفيفي)، **جرائم الحاسوب وحقوق المؤلف والمصنفات الفنية ودور الشرطو والقانون**، دراسة مقارنة، منشورات
الحلبي الحقوقية، بيروت، 2003.

23- عيسى، (طوني ميشال)، **التنظيم القانوني لشبكة الإنترنت – دراسة مقارنة في ضوء القوانين الوضعية والإتفاقيات الدّوليّة**، صادر، الطبعة الأولى، 2001.

24- قشقوش، (هدى)، **جرائم الحاسب الإلكتروني في التشريع المقارن**، دار النهضة العربية، القاهرة، 1992، ص:167.

25- قورة، (نائلة عادل محمد فريد)، **جرائم الحاسب الآليّ الاقتصادية، دراسة نظرية وتطبيقية**، منشورات الحلبي الحقوقية، 2005.

26- قورة، (نائلة عادل محمد فريد)، **جرائم الحاسب الآليّ الاقتصادية، دراسة نظرية وتطبيقية**، منشورات الحلبي الحقوقية، 2006.

27- منصوري، (نديم)، **سوسيولوجيا الإنترنت**، منتدى المعارف، 2004.

28- هجيج، (حسنّن عثيذ)، غازي، (صفاء كاظى)، **آثار جريمة قرصنة البريد الإلكتروني**، جامعة القادسية، مجلة القادسية للقانون والعلوم السياسية، العدد الثاني، المجلد السابع، كانون الأول 2016.

القوانين:

1- قانون أصول المحاكمات الجزائية اللّبناني.

2- قانون العقوبات اللّبناني.

3- قانون المعاملات الإلكترونية والبيانات ذات الطّابع الشّخصي، رقم 81، السنة 158، العدد 45، الخميس في 18 تشرين الأول 2018.

4- قانون حماية الأحداث المنحرفين أو المعرضين للخطر، رقم 422، 6 حزيران 2002.

المؤلفات المعرّبة:

1- أتنغوف، (كيم)، **الملاحة في الشبكة العنكبوتية**، الدار العربية للعلوم ناشرون، 2015.

2- آيكن، (ماري)، **التأثير السيبراني**، الدار العربية للعلوم ناشرون، 2017.

3- توماس، (طوم)، **الخطوة الأولى نحو أمان الشبكات**، الدار العربية للعلوم، 2004.

4- موراي، (أندرو)، ويفر، (فينسنت)، **دليل سيمانتك الى أمن الإنترنت في المنزل**، الدار العربية للعلوم، 2006.

الدّراسات البحثية:

1- العجمي، (خالد حسين المهان)، **جريمة الحاسوب والإنترنت في القانون الكويتي والمقارن**، أطروحة لنيل شهادة الدكتوراه اللبنانية في الحقوق، 2011.

2- العجمي، (عبد الله دغش)، **المشكلات العملية والقانونية للجرائم الإلكترونية (دراسة مقارنة)**، مذكرة مقدمة لنيل شهادة الماجستير في القانون العام، إشراف د. أحمد اللويزي، جامعة الشرق الأوسط، 2014، ص: 34.

3- آل ثنيان، (ثنيان ناصر)، **إثبات الجريمة الإلكترونية**، رسالة مقدمة للحصول على شهادة الماجستير، جامعة نايف العربية
للعلوم الأمنية، سنة 2012.

4- بوزيد، (مختارية)، ماهية الجريمة الإلكترونية، **كتاب أعمال ملتقى آليّات مكافحة الجرائم الإلكترونية في التّشريع الجزائري**
المعقد في الجزائري العاصمة يوم 29 مارس 2017.

5- شريفة، (بن غذفة)، صليحة، (القص)، **دراسة قانونية حول الجريمة الإلكترونية الممارسة ضد المرأة على صفحات الإنترنت وطرق محاربتها**، جامعة سطيف 2 الجزائر، 2017.

6- صالح، (بن منصور)، أنيسة، (كوش)، **السلوك الإجرامي للمجرم المعلوماتي**، مذكرة لنيل شهادة الماستر في الحقوق، جامعة عبد الرحمان ميرة، سنة 2015/2014.

7- فقيه، (هانيا محمد علي)، **حماية الحق في الخصوصية المعلوماتية**، دراسة تحليلية لواقع الحماية وتحديات العصر، الجامعة اللّبنانية، مركز الدراسات والأبحاث في المعلوماتية القانونية، 2018/1/22.

8- فيصل، (بدري)، **مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي**، أطروحة لنيل شهادة دكتوراه علوم تخصص (قانون عام)، جامعة الجزائر 1(بن يوسف بن خلدة)، كلية الحقوق، سنة 2018/2017.

9- كرابيج، (طاهر جمال الدين)، **الجريمة المعلوماتية، دراسة بحثية**، الجمهورية العربية السورية، العام الدراسي 2010 /2011.

10- موايعية، (ريمة)، **النظام القانوني للمصادرة**، مذكرة مكملة لمتطلبات نيل شهادة الماستر، جامعة العربي التبسي، سنة 2016/2015.

11- نعيم، (سعيداني)، **آليّات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية (علوم جنائية)، إشراف د. زرارة صالحي الواسعة، جامعة الحاج لخضر، باتنة، 2013.

المؤتمرات:

1- د. محمد مرياتي، **أمن تقنيّة المعلومات**، مدينة الملك عبد العزيز للعلوم والتّقنيّة، المنظّمة العربية للترجمة، 2012.

2- سيد طنطاوى محمد سيد، **الجريمة المعلوماتية – الصّعوبات الّتي تواجه التّعاون الوطني والدّولي وكيفيّة مكافحتها**، المركز الدّيمقراطي العربي، 2018.

3- د. نمديلي رحيمة، **خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة - أعمال المؤتمر الدّولي الرّابع عشر في الجرائم الإلكترونية**، جامعة محمد لمين دباغين سطيف 2 الجزائر، 2017.

4- حيى بن محمد أبو مغايضا، **لأبعاد الإستراتيجية في مواجهة الجريمة الإلكترونية**، أكاديمية نايف للعلوم الأمنيّة، مؤتمر الجرائم المعلوماتية، 2009.

الأمم المتّحدة:

الأمم المتحدة، الإعلان العالمي الخاص بالمبادئ الأساسيّة لتوفير العدالة لضحايا الجريمة وإستعمال السّلطة، قرار رقم 401434، تاريخ 1985/11/29.

المراجع باللّغة الأجنبية:

1- Alajami, (Abed Alah Daghesh), **The Practical and Legal Problems of Cybercrime**, **a comparative study**, middle east university, 2014.

2- Anderson, (Malcom), **Policing the world - Interpol the Politics of International Police Cooperation,** Clarendon press. Oxford, 1989.

3- Bainbridge, (David), **Introduction To Computer Law**, forth edition, logman, 2000.

4- Becker, (Jay), **The Investigation Of Computer Crime**, 1980.

5- Cornwall, (Hugo), **Datatheft – Computer Fraud – Industrailespionage and Information Crime**, Heinemann, London, McGraw Hill, 1992.

6- Caelli, (William), Longley, (Dennis), Shain, (Michael), **Information Security For Managers,** Macmillan Publishers ltd, 1989.

7- Eaton, (John), Smithers, (Jeremy), **This is I.T.: Manager's Guide To Information Tech-nology**, philipi allan, 1982.

8- Johnson, (David), **Electromnic Privacy**, stodder, Canada, 1997.

9- Ribeyne, (Cédric), **La victim de l'infraction pénale, Nouveaité**, (Thémes et comer-ciales), edition, 2016, Dalloz.

10- Leukfeldt, (Eric Rutger), **Big Five Personality Traits of Cybercrime Victims**, Re searchGate, 2017.

11- Ngo, (Fawn T.), Paternoster, (Raymond), **Cybercrime Victimization- An examination**

of Individual and Situational level factors, International Journal of Cyber Criminology, Vol 5 Issue 1 January, July 2011.

12- Pignoux, (Nathalie), **La ré paration des victimes d'infraction pénales**, edition l'harmattan, 2008, collection sciences criminelles.

13- Ryan, (Kaitlyn N.), Curwen, (Tracey), **Cyber-Victimized Students- Incidence, Impact, and Intervention**, October-December 2013.

14- Schjolberg, (Stein), **Computers and Penal Legislation: a study of the legal politics of a new technology**, universitetsforlaget, oslo, 1983.

المواقع الإلكترونية:

1- جلال الجنيدي، الجرائم الإلكترونية وطرق الوقاية منها، مدونات جزيرة
الجرائم-الإلكترونية-وطرق-الوقاية-منها/2018/7/24/https://blogs.aljazeera.net/blogs

2- د. حميد بن ناصر الحجري، ضحايا الجريمة قبل وبعد وقوعها، شرطة عمان
https://www.rop.gov.om/media/arabic/articledetails.aspx?articleid=35

3- برنامج دفاعكم، دور الضّحيّة في إرتكاب الجريمة، مجرّد نظرية أم واقع يستوجب المراجعة، قناة النّهار
https://www.youtube.com/watch?v=ZpiMOPZn5sI

4- رياض هاني بهار، قانون الجرائم المعلوماتية والمجرم المعلوماتي والعقوبات البديلة، موقع كتابات الإلكتروني،
/قانون-الجرائم-المعلوماتية-والمجرم-ال/2019/04/25/https://kitabat.com

5- غادة الحلايقة، مفهوم الذكاء، موقع موضوع -17/ يوليو/ 2018،
مفهوم_الذكاء/https://mawdoo3.com

6- د. علي مشيك، الوعي البشري ظاهرة تاريخية (فكر)، موقع تحولات، 2017/1/17،
http://www.tahawolat.net/MagazineArticleDetails.aspx?Id=1131

7- غيدة فرنجية، المفكرة القانونية، مكتب مكافحة الجرائم المعلوماتية، رقابة غير منظمة على المساحات الإلكترونية،
2013/12/3، https://www.legal-agenda.com/article.php?id=594

فهرس المحتويات

الإهداء **1**
ملخص تصميم الرّسالة **2**
مقدمة **3**

القسم الأوّل: ماهيّة المجرم والضّحيّة المعلوماتيين **8**

الباب الأوّل: المجرم المعلوماتي **10**

الفصل الأوّل: تطوّر شخصيّة المجرم في الإجرام المعلوماتي **11**
المطلب الأوّل: مفهوم مجرم المعلوماتية **11**
النّبذة الأولى: تعريف مجرم المعلوماتي 12
النّبذة الثّانية: صفات مجرم المعلوماتية 15
السّمات المشتركة بين المجرمين المعلوماتيين 16
سمات الجماعة المعلوماتية الإجرامية 18

المطلب الثّاني: السّلوك الجرمي للمجرمين المعلوماتيين **21**
النّبذة الأولى: السّلوك الجرمي المرتكب بواسطة تقنيّة المعلومات 22
أوّلًا: السّلوك الجرمي المعلوماتي الواقع على الأموال 22
1. الإحتيال المعلوماتي 23
2. الجرائم الواقعة على بطاقات الدّفع الإلكترونية 23
ثانيًا: السّلوك الجرمي المعلوماتي الواقع على حرمة الحياة الخاصّة 24
1. القدح والذّم 25
2. إنتحال الشخصيّة والتّعدي على البيانات ذات الطّابع الشخصي 25
3. إستغلال القاصرين في المواد الإباحية الإبتزازية 26
النّبذة الثّانية: السّلوك الجرمي الواقع على تكنولوجيا المعلومات 27
أوّلًا: السّلوك الجرمي المعلوماتي الواقع على المنتجات المعلوماتية غير المادّية 27
1. جرائم التّعدي على نظم المعالجة الآليّة للبيانات 27
1.1 الدّخول غير المشرّع لنظام المعلومات 28
2.1 البقاء غير المصرّح به في النّظام المعلوماتي 28
2. جرم الإعتداء العمدي على نظم المعالجة الآليّة 28

3. جرائم التّعدي على برامج الحاسب الآلي 28

ثانياً: السّلوك الجرمي المستهدف للمعلومات داخل الأنظمة المعلوماتية 29
1. سرقة المال المعلوماتية 30
2. جريمة الإتلاف المعلوماتي 30
3. التزوير المعلوماتي 31

الفصل الثّاني: تصنيف علم الإجرام للمجرمين المعلوماتيين 33

المطلب الأوّل: الدّوافع المحفّزة لإرتكاب الإجرام المعلوماتي 34

النّبذة الأولى: الدّوافع الدّاخلية للسلوك الإجرامي 34

1. الدّوافع النّفسيّة 35
2. دافع التعلّم 36

النّبذة الثّانية: الدّوافع الخارجية للسلوك الإجرامي 36

1. دافع الإنتقام 37
2. دافع التهديد 37
3. دوافع عاطفية 38
4. دوافع سياسية 38
5. دوافع إقتصادية 38

المطلب الثّاني: درجة إلمام المجرمين المعلوماتيين بالتّقنيّة المعلوماتية 40

النّبذة الأولى: المجرمون غير المحترفون 41

1. صغار المجرمين 41
2. الهاكرز (Hackerrs) 42
3. المجرم الهاوي 42

النّبذة الثّانية: المجرمون المحترفون 42

1. المخرّبون 43
2. المجرمون المتمرّسون 44
3. المتجسسون 44

فهرس المحتويات

الباب الثّاني: ضحيّة الإجرام المعلوماتي **46**

الفصل الأوّل: تطوّر شخصيّة الضّحيّة في الإجرام المعلوماتي **47**

المطلب الأوّل: مفهوم ضحيّة الإجرام المعلوماتي **48**

النّبذة الأولى: تعريف ضحيّة الإجرام المعلوماتي 49

النّبذة الثّانية: صفات ضحايا الإجرام المعلوماتي 51

1. خوض تجارب حديثة 51
2. عدم ضبط النّفس 51
3. عدم الاستقرار العاطفي 52
4. الخوف 52
5. الجهل بجرائم المعلوماتية 53
6. عدم المبالاة 53

المطلب الثّاني: إختيار ضحيّة الإجرام المعلوماتي **54**

النّبذة الأولى: هدف فرصة 55

النّبذة الثّانية: هدف خيار 56

الفصل الثّاني: تصنيف علم الإجرام لضحايا الإجرام المعلوماتي **58**

المطلب الأوّل: الشخص الطبيعي **59**

النّبذة الأولى: القاصر ضحيّة الإجرام المعلوماتي 60

النّبذة الثّانية: العنصر الأنثوي ضحيّة الإجرام المعلوماتي 61

المطلب الثّاني: الشخص المعنوي **62**

النّبذة الأولى: الشخص المعنوي الخاص 63

النّبذة الثّانية: الشخص المعنوي العام 63

القسم الثّاني: المسؤوليّة الجزائيّة للإجرام المعلوماتي بين ردع المجرمين وضمانات الضّحايا **66**

فهرس المحتويات

الباب الأوّل: أوجه المسؤوليّة الجزائية المعاصرة الّذي يطرحه الإجرام المعلوماتي 67
الفصل الأوّل: المسؤولون جزائيًا عن الإجرام المعلوماتي 68
المطلب الأوّل: المسؤوليّة الجزائية للمجرم المعلوماتي 68

النّبذة الأولى: المسؤوليّة الجماعية عن الإجرام المعلوماتي 69

النّبذة الثّانية: مسؤوليّة المجرم الأصلي الخفي والمجرم المعلوماتي التّقني المنفّذ 72

المطلب الثّاني: لجهة مسؤوليّة ضحيّة الإجرام المعلوماتي 74

النّبذة الأولى: مساهمة الضّحيّة في الإجرام المعلوماتي 75

النّبذة الثّانية: خطأ الضّحيّة عن الإجرام المعلوماتي 78

الفصل الثّاني: الإشكاليّات المؤثّرة في المسؤولية الجزائية 81
المطلب الأوّل: على مستوى القواعد الإجرائية.....82

النّبذة الأولى: الملاحقة والتحقيق 82

1. الملاحقة 83
2. التحقيق 85

النّبذة الثّانية: الإثبات الإلكتروني والإختصاص المكاني 87

1. الإثبات.....87
2. الإختصاص المكاني 88

المطلب الثّاني: المسؤولية الجزائية عن الحدث المعلوماتي المنحرف.....90

النّبذة الأولى: تأثير الذّكاء المعلوماتي للحدث على المسؤولية الجزائية 91

النّبذة الثّانية: مدى ملائمة قانون الأحداث على إنحراف الحدث المعلوماتي 95

الباب الثّاني: بين العقوبات والتدابير المناسبة وأهمّية الوقاية.....99

الفصل الأوّل: آثار المسؤوليّة الجزائية على مجرم وضحيّة الإجرام المعلوماتي 100
المطلب الأوّل: الجزاء العقابي 100

فهرس المحتويات

النّبذة الأولى: العقوبات وتدابير الإحتراز الواقعة على المجرم المعلوماتي 101

1. العقوبات الماليّة 102
1.1 المصادرة 103
2.1 الغرامة 104
2. التدابير الإحترازية 106
1.2 الحريّة المراقبة 107
2.2 الحجر بإستعمال تقنيّات المعلومات 108

النّبذة الثّانية: إستغلال الذّكاء المعلوماتي لصالح الدّول 108

المطلب الثّاني: الحقوق الملازمة لضحايا الإجرام المعلوماتي 110

النّبذة الأولى: الحق في سريّة المعلومات 111

النّبذة الثّانية: الحق في التّعويض 113

الفصل الثّاني: أساليب مكافحة السّلوك الإجرامي المعلوماتي 116

المطلب الأوّل: الوقاية من الإجرام المعلوماتي 116

النّبذة الأولى: الوقاية عبر أدوات الأمان وتقنيّاته 117

1. جدران النّار 118
2. بروتوكولات الأمان 118
3. الأمان اللّاسلكي 119

النّبذة الثّانية: الوقاية عبر إستراتيجيّات التّوعية 119

المطلب الثّاني: التصدّي للإجرام المعلوماتي 121

النّبذة الأولى: التصدّي من النّاحية القانونية 122

النّبذة الثّانية: التصدّي عبر التّعاون الدّولي 125

الخاتمة 131

المقترحات 135

المراجع 136

فهرس المحتويات 141