عمادة الدراسات العليا
جامعة القدس أبوديس

جريمة الابتزاز الإلكتروني

"دراسة مقارنة"

دعاء سليمان عبد القادر التميمي

رسالة ماجستير

القدس – فلسطين

1440هـ/2019م

جريمة الابتزاز الإلكتروني

"دراسة مقارنة"

إعداد

دعاء سليمان عبد القادر التميمي

بكالوريوس قانون من جامعة القدس/ فلسطين

إشراف: د. نبيه صالح

قدمت هذه الرّسالة استكمالًا لمتطلبات درجة الماجستير في القانون العام من كلية القانون –كلية الدّراسات العليا –جامعة القدس

1440هـ/2019م

جامعة القدس أبوديس
عمادة الدراسات العليا
برنامج القانون العام

إجازة الرسالة

جريمة الابتزاز الإلكتروني

"دراسة مقارنة"

اسم الطالبة: دعاء سليمان عبد القادر التميمي

الرقم الجامعي: 21512540

المشرف: د. نبيه صالح

نوقشت هذه الرسالة وأجيزت بتاريخ 7/7/ 2019م من أعضاء لجنة المناقشة المدرجة أسمائهم وتواقيعهم:

1- رئيس لجنة المناقشة: د. نبيه صالح التوقيع: .....

2- ممتحنا داخليا: د . فادي ربايعة التوقيع: .....

3- ممتحنا خارجيا: سامر نجم الدين التوقيع: .....

القدس – فلسطين

1440هـ/2019م

الإهداء

إلى أفضل الخلق والمرسلين إلى المعلم الأول سيدنا محمد – صلى الله عليه وسلم،

وإلى المنارات التي تضئ لنا الطريق "مدرسينا الأفاضل".

وإلى الشمعتين اللتين أضاءتا طريق حياتي بالعلم والنور:

"أبي، السيد الفاضل "سليمان التميمي"

وأمي، المربية الفاضلة " عبلة التميمي"

أسأله سبحانه أن يمدهما بطول العمر، وحسن العمل.

إلى زوجي ورفيق دربي " طلال مرقة "

إلى أبنائي وأزهار حياتي " زينة وزيد وعبد الرحمن

إلى جميع صديقاتي وزميلاتي الغاليات على قلبي

إليهم جميعاً أهدي هذا الجهد المتواضع، وأن يكون خالصاً لوجهه الكريم.

الباحثة

دعاء سليمان التميمي

إقرار

أُقر أنا معدة الرسالة أنها قدمت لجامعة القدس لنيل درجة الماجستير، وأنها نتيجة أبحاثي الخاصة باستثناء ما تم الإشارة له حيثما ورد، وأن هذه الرسالة أو أي جزء منها لم يقدم لنيل درجة عليا لأي جامعة، أو معهد آخر.

التوقيع :.....دعاء التميمي.....

اسم الطالبة: دعاء سليمان عبد القادر التميمي

التاريخ: 2019/7/7

شكر وعرفان

الحمد لله ربّ العالمين، والصلاة والسلام على خاتم الأنبياء والمرسلين، سيدنا محمد صلى الله عليه وسلم، وبعد:

الشكر لله أولًا وأخيرًا على إعانته لي في إكمال هذا الجهد المتواضع. ولمَّا كان: "من لا يشكر الناس لا يشكر الله"، فإنه لا بد من القول إنه قد تفضّل عليّ كثيرون بالمساعدة والعون، وأودُّ أن أتقدّم لهم بجزيل الشكر والعرفان. وأخصّ بالذكر:

أستاذي الفاضل الدكتور/ نبيه صالح، والذي تفضّل بالإشراف على هذه الرسالة، فبفضل الله عز وجل، ثم بجهده المتواصل، وتوجيهاته السديدة، ورحابة صدره، تمّ إنجاز هذه الرسالة، فله مني كل الشكر والتقدير.

الأستاذين الفاضلين: الدكتور / فادي ربايعه ، والدكتور / سامر نجم الدين ؛ لتفضّلهما بقبول مناقشة رسالتي.

كما أتقدّم بالشكل الجزيل لكل من ساعدني من الأصدقاء والإخوان، الذين شجعوني ووقفوا إلى جانبي.

وختامًا، فإنَّ ما كان في هذه الرسالة من صواب وسداد فبتوفيق من الله عز وجل، وما كان فيها من خطأ أو نقص أو نسيان فمني ومن الشيطان.

والسلام عليكم ورحمة الله وبركاته

الباحثة

دعاء سليمان التميمي

الملخص

هدفت هذه الدراسة إلى تسليط الضوء على جريمة الابتزاز الإلكتروني في القانون الفلسطيني دراسة مقارنة مع كل من القانون المصري والقانون الأردني.

وبينت الدراسة أنّ جريمة الابتزاز الإلكتروني تعتبر من أخطر الجرائم المعلوماتية وأكثرها تعقيداً، وذلك بسبب وجود العديد من التجاوزات التي تعدت على خصوصيات الغير دون وجه حق، كما أنّ هذه الجرائم تختلف من دولة إلى أخرى حسب البيئة التي نشأت بها هذه الجرائم، حيث قارنت الدراسة بين كل من القانون الفلسطيني والقانون المصري والقانون الأردني في تعاطيه معَ مثل هذه الجرائم، مما كان له أفضل الأثر في إثراء الدراسة، كما أنّ هذه الجرائم يصعب الكشف عنها وتعقبها، خاصةً أنها ليس لها أثر مادي من جهة، وَضْعُ الخبرة لدى ذوي التحقيق القضائي من جهة، وَضْعُف التعاون الدولي في مكافحة هذه الجريمة من جهة أخرى.

وقد تم تقسيم الدراسة إلى فصلين إضافة إلى فصلٍ تمهيديّ تطرَّق إلى الإطار العام للدراسة، وخاتمة للدراسة؛ حيث تطرق الفصل الأول إلى دراسة ماهية جرائم الابتزاز الإلكتروني، حيث بيَّن المبحثُ الأول موضوع جرائم الابتزاز الإلكتروني من خلال مفهومها وأركانها وأنواعها ودوافعها، وذلك حتى يتم الكشف عن هذه الجريمة قبل تطبيقها على القانون الفلسطيني وعلى كلاً من القانونين المصري والأردني، أما المبحث الثاني فقد وضَّح طرق التحقيق والإثبات في جرائم الابتزاز الإلكتروني وآثارها على الفرد وعلى المجتمع بأكمله، أما الفصل الثاني فقد أبرز موضوع جريمة الابتزاز الإلكتروني في القانون الفلسطيني (دراسة مقارنة مع القانونين المصري والأردني)، حيث وضح المبحث الأول جريمة الابتزاز الإلكتروني في القانون الفلسطيني (عقوبتها وصعوبات الكشف عنها) من خلال دراسة الجريمة كخلفية عامة في الأراضي الفلسطينية، ثم التطرق إلى عقوباتها كما بينها المشرع الفلسطيني، والصعوبات التي تواجه السلطات في الكشف عنها، أما المبحث الثاني فقد ناقش جريمة الابتزاز الإلكتروني في القانونين المصري والأردني، وذلك من خلال دراسة جريمة الابتزاز في كل من القانون المصري والعقوبة المقررة لها، وأيضًا في القانون الأردني وعقوبتها، كما تم توضيح أوجه الشبه والاختلاف بين عقوبة جريمة الابتزاز الإلكتروني في كل من القانون الفلسطيني والقانونين المصري والأردني.

وقد استخدمت الباحثة في دراستها عدة مناهج ونظريات للوصول إلى مشكلة الدراسة، حيث تحتمل الدراسة مناهج ونظريات عدة مثل: المنهج الوصفي الاستقرائي الذي يقوم على أساس تحديد خصائص

المشكلة ووصف طبيعتها وأسبابها، ومن ثم تحليلها لمعالجة المسؤولية الجنائية عن جرائم الابتزاز الإلكتروني في كل من النظام الفلسطيني والمصري والأردني. كما استخدمت أيضًا المنهج المقارن من خلال المقارنة بين بعض الأنظمة والقوانين التي تتابع هذا النوع من الجرائم، ومعرفة حدود هذه الجرائم لدى كل نظام من هذه الأنظمة. وذلك باستخدام المنهج التحليلي وبعض المصادر والمراجع الأصيلة للحصول على المعلومات، والنتائج المطلوبة.

وخلصت الدراسة إلى عدة نتائج منها: أن جرائم الابتزاز الإلكتروني تعتبر من أخطر الجرائم التي تدمر منظومة القيم والأخلاق لدى المجتمع، أيضًا لاقت قوانين الجرائم الإلكترونية في فلسطين ومصر والأردن انتقادات حادة بحجة أنها تمس حرية الرأي والتعبير، خاصة وأن المشرّع في هذه الدول كان قد تصدى بكل قوة لمرتكبي هذه الجرائم. أيضًا هناك مشكلات عديدة تواجه أجهزة الدولة في إثبات هذه الجريمة لاعتبارات عديدة، وأخيرًا يمكن القول إن الجهود الدولية لمكافحة جريمة الابتزاز الإلكترونية لم تكن على المستوى المطلوب منها، خاصة في ظل قلة خبرة وعدم وجود معرفة لمواجهة مثل هذه الجرائم بالصورة السليمة التي يمكنها أن تحد منها.

كما أوصت الباحثة بعدة توصيات منها: ضرورة قيام المشرّع العربي بصورة عامة والفلسطيني والمصري والأردني بصورة خاصة بوضع نصوص قانونية خاصة بجريمة الابتزاز الإلكتروني كونها من الجرائم الخطيرة التي لم ينتبه لها الكثير من المشرعين إلا بعبارات عابرة فقط. كما أوصت المشرع الفلسطيني والأردني والمصري بوضع بعض الجرائم التي لم ينص عليها ضمن قوانين الجرائم لديهم كالمضايقات والتحرش في نطاق المواقع الإلكترونية والملاحقة الإلكترونية والتشهير وغير ذلك من الأفعال التي لم ينص عليها أي قانون للجرائم الإلكترونية لديهم. وأخيرًا أوصت الباحثة بضرورة تدريب المحققين القضائيين والنيابة العامة على طرق الإثبات وجمع الأدلة والتعامل مع الجرائم الإلكترونية.

The Crime of Cyber Extortion

" Comparative Study "

Prepared by : Doaa Suliman Abd Alqader Altamimi

Supervised by: Dr.Nabih Saleh

Abstract

This study aimed to spot the light on the electronic blackmail crime in the Palestinian law compared to both of Egyptian and Jordan law.

The study indicated that the electronic blackmail is among the most dangerous and complicated information crimes because of many abuses which has unduly exceeded the other privacy. These crimes differ from state to another based on the environment where they have arose. The study compared between the three laws (Palestinian , Egyptian and Jordan) in their dealing with these crimes . The thing that has enriched the study. As well as, these crimes can't be detected and tracked down easily as it doesn't have any material effect, the judicial investigators are inexperience, and the international cooperation doesn’t strong enough to fight this crime. The study has been divided into two chapters in addition to the introductory chapter which addressed the theoretical background and the study conclusion;

The first chapter studied the nature of electronic blackmail crimes as the first subsection addressed the concept, elements, kinds, and motivations of the electronic crimes in order to discover this crime before applying it on the Palestinian, Egyptian and Jordan laws. While the second subsection showed the evidence and investigation ways of the electronic blackmail crimes and its effects on the individual and the society as a whole.

As for the second chapter, it showed the topic of electronic blackmail in the Palestinian law (a comparative study with the Egyptian and Jordan law) in which the first subsection clarified the crime of electronic blackmail in the Palestinian law (its penalty and difficulties to detect it) through studying the crime with a general background in the Palestinian law and then addressing its penalty as the Palestinian legislator clarified and the difficulties which authorities face to detect it. The second subsection discussed the electronic blackmail in both Jordan and Egyptian laws by studying the crime of each law and the prescribed penalty for it. As well as, the similarities and differences between the penalty in the Palestinian law and the penalty in the Jordan and Egyptian law were clarified.

The researcher used many approaches and theories to get the study problem such as the objective descriptive approach which bases on problem characterization, its nature description, and its reasons. Then, analyzing it to address the criminal responsibility of the electronic blackmail in each of Palestinian, Jordan and Egyptian system. The researcher used also the comparative approach through the comparison between the systems and laws which follow this kind of crimes. The analytical approach is used to know the crimes limits at every system of these systems, some of resources and references to get information and the needed results.

The study results revealed that the electronic blackmail crimes is one of the most dangerous crimes that ruin the value and ethics system of society. The Palestinian electronic laws faced great criticisms claiming that it affects the freedom of opinion and expression but the legislator addressed forcefully these criticisms. In addition, the state organs face problems of proof this crime due to several considerations. Finally, it can be said that the international efforts to combat the electronic blackmail crimes were not at the

required level particularly in the presence of inexperience and lack of knowledge to face these crimes in the right-way that limits its happening.

المقدمة

شهد النصف الثاني من القرن العشرين ثورة تكنولوجية هائلة في مجال التقنية والاتصالات والصناعات، حيث بات العالم يعتمد على التكنولوجيا بصورة كبيرة على كل من المستوى الرسمي والشخصي، خاصة في مجال تخزين المعلومات وتبادلها بين الحكومات والأفراد والشركات، وأصبح قياس مدى تقدم أي دولة بمدى تطور التقنيات التي تمتلكها، إلا أن هذه التقنيات شأنها كشأن أي منتج آخر له آثاره السلبية، وقد يستخدم كوسيلة هدم لا وسيلة بناء من قبل الخارجين عن القانون والأنظمة من ضعفاء النفوس والعابثين لتحقيق مآربهم المشبوهة؛ حيث ساعدهم على ذلك صعوبة التوصل لمرتكبي هذا النوع من الجرائم، وفي مقدمة هذه الجرائم جرائم الابتزاز الإلكتروني، والتي انتشرت بصورة كبيرة في الآونة الأخيرة في كثير من دول العالم[1].

لقد صاحب ثورة التطور التكنولوجي في مجال الأجهزة الإلكترونية المختلفة من أجهزة التصوير والاتصالات بكافة أشكالها، وما صاحبها من انتشار واسع في المتاجر والأسواق العالمية، وقد ظهر بموازاة ذلك الرغبة الشديدة من كافة طبقات المجتمع في اقتنائها، والاستفادة منها، ومن ثم استخدامها بكل ما فيها من إيجابيات وسلبيات، دون مراعاة لحرمة أو حدود، فكانت سبيلاً للعقاب والهلاك [2].

يعد الابتزاز الإلكتروني في أغلب القوانين لدول العالم أحد أشكال الجريمة الإلكترونية التي أرقت مستخدمي التكنولوجيا، وذلك بسبب وجود العديد من التجاوزات التي تعدت على خصوصياتهم وبياناتهم الشخصية، إلى جانب صورهم وما يتعلق بحياتهم الخاصة وأدت إلى فضحهم على الملأ، حيث تطورت هذه الجرائم حتى كادت تظهر بصورة كبيرة أكثر من وقوعها على الأرض، لِظَنِّ البعض أنه لا رقابة ولا متابعة، وبالتالي هو بعيد عن رقابة الدولة، بالرغم من التحذيرات المستمرة من الوقوع

([1])سامي مرزوق المطيري، المسؤولية الجنائية عن الابتزاز الإلكتروني في النظام السعودي (دراسة مقارنة)، رسالة ماجستير غير منشورة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2015: ص4.

([2]) نورة بنت عبد الله المطلق، ابتزاز الفتيات: أحكامه وعقوبته في الفقه الإسلامي، كلية الشريعة، جامعة الإمام محمد بن سعود الإسلامية، د.ت: ص1.

في مثل هذه الجرائم، وبالتالي فإنَّ الكثير لا يزال ضحية لمخاطر اجتماعية وأخلاقية كبيرة يتسبب بها أفراد متمرسون في النصب والاحتيال[3].

أما الحالة الفلسطينية فإن فلسطين ظلت لسنوات عديدة تعاني من إشكاليات قانونية في المجال الجنائي تقوم على ازدواجية قوانين العقوبات المطبقة بين شطر الوطن من ناحية، وبين قدم هذه القوانين من ناحية أخرى، كما أن واقع الجرائم الإلكترونية وملاحقتها في فلسطين يعتبر حالة مختلفة عن مثيلاتها في الدول الأخرى، وذلك بسبب وقوع دولة فلسطين تحت الاحتلال الإسرائيلي الذي يسيطر على الأرض والسماء والفضاء الإلكتروني لفلسطين سيطرة تامة، ما يعطي شكلاً خاصاً عند ملاحقة هذه الجرائم [4].

وقد وجدت الباحثة أهمية وخطورة هذا النوع من الجرائم والتي لم يتم التطرق إليه بصورة شاملة ومحددة من خلال الدراسات الأخرى، وما ينتج عن هذا النوع من الجرائم خلل اجتماعي كبير وارتفاع معدل الجريمة داخل المجتمعات العربية خاصة المجتمع الفلسطيني والأردني والمصري، وهي مجتمعات محافظة لم تعرف مثل هذه الجرائم قبل ذلك، حيث سيتم دراسة جرائم الابتزاز الإلكتروني في نظام مكافحة الجرائم المعلوماتية بمقارنة بين عدة أنظمة مثل الفلسطيني والأردني والمصري.

أهمية الدراسة:

تتضح أهمية هذه الدراسة من خلال النتائج التي يمكن أن تتوصل إليها، خاصة في ظل قيام السلطات بجهود كبيرة في العديد من المجتمعات للحد من هذه الجرائم، وذلك نظراً لما يمثله هذا الموضوع من أهمية بالغة هي ما دفعت الباحثة لاختياره كموضوع للدراسة الحالية، كما تنبع أهمية هذه الدراسة من خلال إمكانية قيامها بتنبيه الأفراد المستخدمين لهذه التقنيات للمخاطر السلبية في استخدام تلك الأجهزة، وأخذ الحيطة والحذر من اختراق أجهزتهم والوصول لمعلوماتهم الشخصية، وبالتالي سيكونون في واجهة الابتزاز. كما أن أهمية هذه الدراسة تتضح من خلال قيامها بالمقارنة بين عدة قوانين لإبراز هذا النوع من الجرائم التي يمكن أن تعمل على التعاون بين الدول للحد من هذه الجرائم، وهذه المواضيع هي نادرة ولم يسبق للباحثين القيام بالبحث في مثل هذه المواضيع بصورة رئيسة، كما يمكن لإثارة هذه الموضوعات أن تنبه الشركات والدول وأجهزة الدولة لمعرفة الإيجابيات والسلبيات لاستخدام

([3])هنادي كرسوع، الابتزاز الإلكتروني بين الواقع والشرع والقانون، موقع الشرطة الفلسطينية، 2016/7/4، للتفاصيل:
http://www.police.ps/ar/include/plugins/news/news.php?action=s&id=7969

([4]) عبد الفتاح ربعي، ومحمد فهاد الشلالدة، الجرائم الالكترونية في دولة فلسطين المحتلة في ضوء التشريعات الوطنية والدولية، بحث مقدم إلى المؤتمر العلمي الحادي عشر لكلية القانون في جامعة جرش حول الجرائم الالكترونية، والذي عقد من 5-2015/5/7، 15 نيسان 2015: ص6-7

هذه التقنيات الحديثة ومعرفة السمات الخاصة بهذه الجرائم التي تعدت وتخطت حدود الكثير من الدول.

كما تبرز أهمية الدراسة من خلال إلقاء الضوء على المسئولية الجنائية على جرائم الابتزاز الالكتروني، والتي انتشرت بصورة لم يسبق لها مثيل في الآونة الأخرة في العديد من الدول. كذلك إبراز خطورة هذه الجريمة التي ظهرت نتيجة العولمة وما صاحبها من انفجار علمي وتقني هائل، مما دفع الباحثة لاختيار هذا الموضوع. وأخيراً فإن هذا النوع من الدراسات يمكن أن يعود بالفائدة على العاملين بالحقل القضائي من ناحية، والباحثين في هذا المجال من ناحية ثانية، وإثراء المكتبة العربية من ناحية ثالثة.

الدراسات السابقة:

دراسة المطيري، سامي مرزوق (2015)، وهي بعنوان "المسؤولية الجنائية عن الابتزاز الإلكتروني في النظام السعودي (دراسة مقارنة)"، وهي رسالة ماجستير غير منشورة من جامعة نايف العربية للعلوم الأمنية، الرياض، وتتكون الدراسة من مقدمة إضافة إلى أربعة فصول، تحدث الباحث في الفصل الأول عن ماهية جرائم الابتزاز الإلكتروني من حيث ماهيته وخصائصه. أما الفصل الثاني فتطرق إلى الإثبات والتحقيق في جرائم الابتزاز الإلكتروني، وأبرز الفصل الثالث العقوبات المترتبة على الابتزاز الإلكتروني في النظام السعودي والمصري، وقد توصل الباحث في الفصل الرابع إلى عدة نتائج وتوصيات هامة.

دراسة الحميدي، هشام بن عبد العزيز (2011)، وهي بعنوان "دور هيئة الأمر بالمعروف والنهي عن المنكر في الحد من جرائم الابتزاز ضد الفتيات في المملكة العربية السعودية"، وهي رسالة ماجستير غير منشورة من جامعة نايف بن عبد العزيز للعلوم الأمنة، الرياض، وتكونت الدراسة من مقدمة وأربعة فصول، تناول الفصل الأول الخلفية النظرية للدراسة، أما الفصل الثاني فقد تطرق إلى الإجراءات المنهجية للدراسة، وبحث الفصل الثالث في عرض النتائج التي قامت بها الدراسة، واستعرض الفصل الرابع نتائج الدراسة وتوصياتها.

دراسة المطيري، طارق بن عبد الرزاق، وهي بعنوان "الأحكام الخاصة بجريمة الابتزاز المقررة في نظام مكافحة جرائم المعلوماتية السعودي "دراسة مقارنة"، وهي رسالة ماجستير من جامعة الإمام محمد بن سعود الإسلامية، السعودية، وتكونت الدراسة من فصل تمهيدي وثلاثة فصول إضافة إلى خاتمة، حيث تطرق الفصل الأول إلى جريمة الابتزاز أركانها وأنواعها، وبين الفصل الثاني آثار جريمة

الابتزاز، أما الفصل الثالث فقد استعرض عقوبة جريمة الابتزاز، ثم انتهت الدراسة بخاتمة ونتائج وتوصيات.

دراسة الشمراني، محمد بن علي (2011)، وهي بعنوان "ظاهرة الابتزاز في المجتمع السعودي من وجهة نظر العاملين في الضبط الجنائي"، وهي دراسة ماجستير غير منشورة من جامعة نايف للعلوم الأمنية، حيث أجريت الدراسة على عدد من الضباط العاملين بشرطة منطقة الرياض، وتوصلت الدراسة لعدد هام من النتائج والتوصيات.

التعليق على الدراسات السابقة:

تتفق أغلب هذه الدراسات مع هذه الدراسة من خلال الحديث عن ماهية مفهوم الابتزاز وشرح أركانه وصوره وطرق الحد منه، إضافة إلى إبراز دور الدولة في محاربة هذا النوع من الجرائم.

أما هذه الدراسات فتختلف عن هذه الدراسة من حيث إن دراستي تطرقت لجرائم الابتزاز الإلكتروني في القانون الفلسطيني ومقارنته بالقانون المصري والأردني، وهو ما لم تتطرق إليه الدراسات السابقة، أو بمعنى آخر هناك شح واضح في المصادر التي تتحدث عنها دراستي.

إشكالية البحث:

تتمثل إشكالية البحث في العدد الكبير لجرائم الابتزاز الالكتروني والذي تخطى الحكومات والدول والهيئات الدولية، وذلك نتيجة زيادة عدد مستخدمي التقنيات الالكترونية نتيجة التطور الهائل في تكنولوجيا الاتصال، حيث شكلت هذه الجرائم مخالفات تؤسس لمسئولية الفاعل جنائياً حسب الأنظمة والقوانين لكل دولة، حيث يحتاج الباحث لتحديد العقوبة وما يتصل بها من مسئوليات تجاه الجاني، وهي تحتاج إلى تفسير وتحديد وتوضيح.

كما يبرز تساؤل حول **كيف واجه المشرّع الجزائي جريمة الابتزاز الالكتروني؟** حيث أن العديد من القوانين ومنها القانون الفلسطيني والأردني والمصري وغيرها قد حدد عقوبات رادعة لكل ما يتصل بوسائل الاتصال والتكنولوجيا، خاصة جرائم الابتزاز الالكتروني، فالعديد من المواد في القانون الفلسطيني قد بينت تلك العقوبات منها المادة 15 من قانون الجرائم الالكترونية المعدل رقم 10 لعام 2018م، ومن ثم المواد 22 وما بعدها، والتي حددت مقدار العقوبة التي تقع على كل من يستخدم الوسائل التكنولوجية في عمليات غير مشروعة.

لكن التساؤل الهام الذي تطرحه الدراسة أيضاً بقول هل هذا القانون كافياً للتصدي لكل حالات الابتزاز الالكتروني، أم أن تحقيق ذلك أصبح صعباً في ظل وجود تطور هائل في وسائل الاتصال، والذي قد يصعب على الأجهزة المعنية ملاحقة هذه الجرائم المتكررة.

ويتفرع من هذا السؤال عدة تساؤلات فرعية منها:

ما مفهوم جرائم الابتزاز الإلكتروني وأنواعها وأركانها؟، ما طرق التحقيق والإثبات في جرائم الابتزاز الإلكتروني؟، ما طبيعة جريمة الابتزاز الإلكتروني في القانون الفلسطيني؟، ما وجه المقارنة بين جريمة الابتزاز الإلكتروني في كلا القانونين الأردني والمصري؟

أهداف الدراسة:

تهدف الدراسة إلى ما يلي:

1- الكشف عن جرائم الابتزاز الإلكتروني من حيث مفهومها وأركانها وأنواعها وغير ذلك من القضايا.

2- توضيح طرق الإثبات والتحقيق في جرائم الابتزاز الإلكتروني.

3- توضيح جريمة الابتزاز الإلكتروني من خلال التعرف عليها في القانون الفلسطيني.

4- بيان جريمة الابتزاز الإلكتروني في كلا القانونين الأردني والمصري.

حدود الدراسة:

1- **الحدود الموضوعية/** وهي دراسة موضوع "جريمة الابتزاز الالكتروني" دراسة مقارنة.

2- **الحدود المكانية/** سوف تتطرق الدراسة إلى موضوع الابتزاز الالكتروني في كل من القانون الفلسطيني والقانون المصري والقانون الأردني.

3- **الحدود الزمانية/** منذ بروز القوانين الخاصة بجريمة الابتزاز الالكتروني في كل من الدول سالفة الذكر وتطور هذه القوانين وتعديلها حتى اليوم.

منهجية الدراسة:

اتبعت الباحثة في دراستها عدة مناهج ونظريات للوصول إلى مشكلة الدراسة، حيث تحتمل الدراسة مناهج ونظريات عدة مثل: **المنهج الوصفي الاستقرائي** الذي يقوم على أساس تحديد خصائص

المشكلة ووصف طبيعتها وأسبابها، ومن ثم تحليلها لمعالجة المسؤولية الجنائية عن جرائم الابتزاز الإلكتروني في كلٍّ من النظام الفلسطيني والمصري والأردني.

كما استخدمت الباحثة أيضاً **المنهج التحليلي** بشقيه الاستنباطي والاستقرائي للوصول إلى النتائج.

كما استخدمت **المنهج المقارن** من خلال المقارنة بين بعض الأنظمة والقوانين التي تتابع هذا النوع من الجرائم، ومعرفة حدود هذه الجرائم لدى كل نظام من هذه الأنظمة.

الفصل الأول

الأحكام العامة لجرائم الابتزاز الإلكتروني

يميل العديد من الأشخاص لاستغلال المخترعات العلمية وما تقدمه من وسائل متقدمة في ارتكاب العديد من الجرائم التقليدية مستغلين الإمكانيات الهائلة لهذه المخترعات، أو يقوموا بأنفسهم باستحداث صور إجرامية جديدة ترتبط بهذه التقنيات بصورة كبيرة، والتي تصبح بدورها محلاً للإجرام أو وسيلة لارتكابها، وقد تزايدت معدلات هذه الجرائم في العقدين الأخيرين بصفة خاصة، بصورة أدت إلى بروز ظاهرة إجرامية تعرف بالإجرام المعلوماتي [5].

لهذا يشهد العالم منذ منتصف القرن العشرين ثورة جديدة، اصطلح على تسميتها بالثورة المعلوماتية، وذلك إشارة إلى دور المعلومات البارز في هذا الوقت، والذي بالرغم من الدور الإيجابي الذي لعبته هذه الثورة، إلا أن الانعكاسات السلبية عليها أصبحت واضحة وبارزة، حيث تغيرت أنماط الجريمة، فلم تعد الاعتداءات تستهدف النفس والمال فقط، بل طالت المعلومات، وهو ما عرف على الساحة الدولية بإجرام "ذوي الياقات البيضاء"*، حيث يستطيع بموجبه المجرمون العصريون ارتكاب أبشع الجرائم، ليس فقط دون إراقة دماء، ولكن أيضًا بدون الانتقال من أماكنهم، وهذا النوع من الجرائم ليس مقصوراً على منطقة معينة، أو دولة معينة، لكنها مشكلة عالمية[6].

([5]) محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، محور القانون الجنائي، دبي، الإمارات العربية المتحدة، 26-2003/4/28: ص19.

* مصطلح أطلقه سذرلاند عام 1930م، حيث وصف فيه الأفعال الجرمية للأغنياء، وعرف ارتباط الجريمة بنزعة الشخص والمنزلة الاجتماعية العالية والرتبة المهنية، ويرى سذرلاند أن هؤلاء ينشغلون في عمليات تآمر عندما يستغلون وظائفهم في تحقيق مصالحهم الشخصية عن طريق الأعمال غير الشرعية من غير اعتبار للقانون. للتفاصيل أنظر: شيرين الياس دبابنة، جرائم بطاقات الائتمان في الأردن: دراسة وصفية استطلاعية، رسالة ماجستير غير منشورة، جامعة مؤتة، الأردن، 2005: ص22.

([6]) مليكة عطوي، الجريمة المعلوماتية، مجلة حوليات جامعة الجزائر، العدد 21، يونيو 2012: ص8.

كما تعدّ الجريمة الإلكترونية من أهم التحديات التي تواجه الدول والجهات المعنية بإنفاذ القانون في العصر الحديث، لا سيّما أنها جريمة قد تكون عابرة لحدود الدول بل والقارات؛ ذلك لأن أدواتها هي شبكة المعلومات الدولية (الإنترنت وتطبيقاتها المتمثلة في البريد الإلكتروني ومواقع التواصل الاجتماعي، وتجري عبر أجهزة الحواسيب أو باستخدام الهواتف الذكية الحديثة، ومن ناحية أخرى يرجع الخبراء والمؤرخون تاريخ الجريمة الإلكترونية إلى بداية استخدام الإنترنت تقريبًا، والذي بدأت معه عمليات القرصنة والتهكير والسرقات الإلكترونية والابتزاز الإلكتروني والاحتيال الإلكتروني بطرق متعددة، وقد تعرّضت الشبكات المعلوماتية لكبرى المؤسسات الدولية بالاختراق والتهكير والابتزاز الإلكتروني. وقد أدركت العديد من الدول منذ البداية خطورة الجريمة الإلكترونية، وبالتالي أولت الجهود الدولية والإقليمية لمحاربتها سواء على الصعيد الداخلي أم الخارجي[7].

لهذا أشارت الأمم المتحدة في المدونة الصادرة عنها بشأن الجريمة المعلوماتية، إلى الخلاف الواقع بين الخبراء حول ماهية العناصر المكونة لجرائم الكمبيوتر أو حتى المتعلقة بالكمبيوتر ولعل ذلك ما يفسر عدم التوصل إلى تعريف متفق علية دوليًا لهذه المصطلحات وإن كان هؤلاء قد اتفقوا ضمنيا على وجود ظاهرة تتزايد بمعدلات عالمية لتلك الجرائم[8].

أما جريمة الابتزاز الإلكتروني فتعتبر من الجرائم المعلوماتية التي تشكل آفة من آفات العصر، والتي أفرزها التطور الهائل في تقنية المعلومات، ومع أن هذه الوسائل لها من الفوائد ما لا يعد ولا يحصى، فإن لها من الآثار السلبية ما يستدعي أن يتداعى أهل الاختصاص سواء في المجال الشرعي أم مجال الضبط الجنائي أم مجال تقنية المعلومات، للمساهمة في محاصرة هذه المشكلة سواء بالوقاية من الوقوع في هذه المشكلة، أم مكافحة هذه الجريمة والوقوف مع الجهات الأمنية في رصد هذه الظاهرة، أم تأهيل من وقع في هذه الجريمة من خلال برامج التأهيل في الجهات المختصة[9].

أما الأراضي الفلسطينية فلم يكن بها قانونًا متخصصاً يعالج ارتكاب هذه الجرائم، حتى أصدر الرئيس الفلسطيني محمود عباس القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية بتاريخ

([7]) ياسر محمد، الجريمة الإلكترونية.. إرهاب يتحدى الدول بالتكنولوجيا المتطورة، صحيفة العرب القطرية، 2018/6/23.

([8]) الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، مركز هردو لدعم التعبير الرقمي، القاهرة، 2014: ص7.

([9]) عبد الرحمن السند، جريمة الابتزاز، الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر، السعودية، ط1، 2018: ص9-10.

2018/4/29م، والمنشور في العدد الممتاز رقم (16) من الوقائع الفلسطينية، والذي جاء لسد حالة الفراغ التشريعي في مجال الجرائم الإلكترونية، وبذات الوقت للحد من هذه الجرائم وخطورتها والتي ازدادت في الأعوام الأخيرة نتيجة التقدم التكنولوجي الهائل، كما جاء أيضاً لعدم ترك مرتكبي هذه الجرائم دون ملاحقة قانونية، وهنا نلاحظ أن المشرع الفلسطيني قد استخدم مصطلح الجرائم الإلكترونية في عنوان القرار بقانون المذكور، وإن مصطلح الجرائم المعلوماتية هو الذي نحبذ استخدامه كونه مصطلح شامل لكافة الجرائم المعلوماتية حيث إن الاتفاقية العربية قد اتبعت هذا النهج، وجاءت بعنوان الاتفاقية العربية بشأن مكافحة تقنية المعلومات وكذلك الحال بالنسبة لغالبية التشريعات العربية المقارنة وكذلك الاتفاقية الأوروبية "بودابست "للجرائم المعلوماتية، وهي اتفاقية تم توقيعها عام 2001م من خلال العديد من الدول الأوروبية، وصادق عليها المجلس الأوروبي، وذلك بهدف مكافحة الجريمة المعلوماتية[10].

لهذا سوف يتم التطرق في هذا الفصل لماهية جرائم الابتزاز الإلكتروني، حيث سيتم من خلال المبحث الأول إبراز مفهوم جريمة الابتزاز الإلكتروني من خلال التعرف على بعض التعريفات المختلفة لهذه الجريمة الجديدة، ومن ثم توضيح أركان هذه الجريمة وأنواعها وخصائصها التي تدفع الشخص لارتكاب مثل هذه الجريمة. أما المبحث الثاني فسنتناول فيه طرق التحقيق والإثبات في جرائم الابتزاز الإلكتروني، من خلال بيان كيفية إثبات هذه الجريمة من ناحية، ومن ثم آثار هذه الجريمة على الفرد والمجتمع، حيث إن هذه الجريمة لها تأثيرات سلبية واضحة تمس الفرد والمجتمع على حد سواء.

المبحث الأول: جرائم الابتزاز الإلكتروني (مفهومها وأركانها وأنواعها وخصائصها)

لم يكن التمييز بين مصطلحات الجرائم الإلكترونية خاصة الابتزاز الإلكتروني واضحًا ومتيسرًا في بداية شيوع هذه الظاهرة، أما في ظل تطور هذه الظاهرة ومحاولة الفقهاء تحديد مفهوم وأركان وأنماط الجرائم المعلوماتية، أصبح البعض يستخدم اصطلاح جرائم الكمبيوتر للدلالة على الأفعال التي يكون الكمبيوتر فيها هدفًا للجريمة، أما اصطلاح الجرائم المرتبطة بالكمبيوتر فهي تلك الجرائم التي يكون فيها الكمبيوتر وسيلة لارتكاب الجريمة كالاحتيال والنصب والابتزاز ونحو ذلك[11]، ومن ذلك اصطلاح

([10]) أحمد براك، وعبد القادر جرادة، الجرائم الإلكترونية في التشريع الفلسطيني: دراسة تحليلية تأصيلية مقارنة، دار الشروق، القاهرة، ط1، 2018: ص6.

([11]) أيمن عبد الله فكري، الجرائم المعلوماتية: دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد، السعودية، ط1، 2014: ص88.

الابتزاز الإلكتروني الذي ظهر مؤخرًا والتي سيتم التطرق لمفهومه وأركانه وما إلى ذلك في هذا المبحث.

المطلب الأول/ جريمة الابتزاز الإلكتروني (مفهومها وأركانها)

قبل التطرق لمفهوم جريمة الابتزاز الإلكتروني يقتضي التعرف على الحاسب الآلي الذي يعد محور العالم الافتراضي ومسرح الجريمة التي يستخدمها الجناة في جرائم الابتزاز الإلكتروني. حيث يعرف الحاسوب بأنه/ جهاز لمعالجة البيانات والمعلومات بعمليات حسابية ومنطقية بصفة آلية ودون تدخل بشري، أثناء التشغيل وعادة ما يعمل بالترقيم الثنائي*. ويتكون الحاسب الآلي من: وحدات إدخال، وحدات معالجة، وحدات إخراج، برامج تشغيل، لغات برمجة، البرامج المساعدة، وبرامج التطبيقات[12].

أما المشرّع الفلسطيني فلم يتطرق لمفهوم الجريمة الإلكترونية بصورة واضحة، حيث إن هذه الجريمة تعتبر من الجرائم المستحدثة على الساحة الفلسطينية، كما أن الفقه والقضاء الفلسطيني لم يتطرق إلى تعريف الجريمة الإلكترونية بصفة عامة، وجريمة الابتزاز الإلكتروني بصفة خاصة [13].

وتعد الشبكة العالمية "الإنترنت" أكثر المجالات التي تستخدم فيها أجهزة الحاسب الآلي والهواتف الذكية، ويعتبر الحاسب امتدادًا للعالم الافتراضي الذي ترتكب فيه جريمة الابتزاز الإلكتروني، وهذا الإنترنت هو لغة العصر والمستقبل، وظهور مجتمع الإنترنت الجديد قد فرض نفسه على كل المجتمعات، فأجهزة الحاسب الآلي التي تستخدم الإنترنت هي مسرح لارتكاب جريمة الابتزاز الإلكتروني، ولا يمكن ارتكابها في مكان آخر، وهو ما يميزها عن جرائم الابتزاز العادية التقليدية، وجعلها تختلف عنها في مفهومها وأركانها وأنواعها المتطورة[14].

---

* الترقيم الثنائي أو ما يسمى بالأساس2 والذي يستخدم لتحديد المنطق (صح- غلط، أو صواب- خطأ، أو شغال- بطال، أو مفتوح- مقفول ..إلخ)، وهذا الترقيم في الحاسب يتكون من رقمين الصفر والواحد فقط. للتفاصيل:
أحمد محمد شامي ، سيد حسب الله، الموسوعة العربية لمصطلحات علوم المكتبات والمعلومات والحاسبات، المكتبة الأكاديمية، القاهرة، المجلد1، ط1، 1998: ص295.

([12])المطيري، مرجع سابق: ص22.

([13]) يوسف خليل العفيفي، الجرائم الإلكترونية في التشريع الفلسطيني: دراسة تحليلية مقارنة، رسالة ماجستير غير منشورة، الجامعة الإسلامية، غزة، 2013: ص7.

([14]) المطيري، مرجع سابق: ص24-25

الفرع الأول: مفهوم جريمة الابتزاز:

تعرَف جريمة الابتزاز لغة: مأخوذ من الثلاثي بزز، يقال: بزَّ الشيء يبزه بزًا اغتصبه، والبز السَّلب، وابتززت الشيء: استلبته، ومنه المثل: من عزَّ بزّ، أي من غلب سلب[15].

قال ابن الأثير: "ففي حديث أبي عبيدة أنه ستكون نبوة ورحمة ثم كذا وكذا، ثم يكون بزيزي وأخذ أموال بغير حق"، البزيزي –بكسر الباء وتشديد الزاي الأولى والقصر–: السلب والتغلب. من بزه ثيابه وابتزه إذ سلبه إياها [16].

أما المعنى الاصطلاحي فقد: وردت كلمة ابتزاز في هذا عبارات متعددة منها[17]:
محاولة تحصيل مكاسب مادية أو معنوية من شخص أو أشخاص طبيعي أو اعتباري بالإكراه بالتهديد بفضح سر من وقع عليه الابتزاز.
استغلال القوة مقابل ضعف إنسان آخر سواء أكان هذا الضعف مؤقتًا أم دائمًا.
محاولة للإكراه وسلب الإرادة والحرية لإيقاع الأذى الجسدي أو المعنوي على الضحايا عن طريق وسائل يتفنن الجاني في استخدامها لتحقيق جرائمه الأخلاقية أو المادية أو كليهما معًا.

ويمكن تعريف الابتزاز أيضًا بأنه: الحصول على معلومات سرية أو صور شخصية أو مواد فيلمية تخص الضحية واستغلالها لأغراض مالية أو القيام بأعمال غير مشروعة. ويتمثل ذلك في عدة صور مثل تهديد بعض الفتيات بنشر صورهن على الشبكة العنكبوتية "الإنترنت" أو في مواقع التواصل الاجتماعي، أو إبلاغ ذويهن –مما قد يلحق الضرر بهن–إذا لم يستجبن لمطالب المبتز السلوكية أو المالية [18].

([15]) صالح بن عبد الله بن حميد، الابتزاز: المفهوم والواقع، بحث منشور ضمن بحوث ندوة الابتزاز: المفهوم– الأسباب– العلاج، مركز باحثات لدراسات المرأة بالتعاون مع قسم الثقافة الاسلامية بجامعة الملك سعود، السعودية، 1432هـ: ص14.

([16]) السند، مرجع سابق: ص15.

([17]) بن حميد، المرجع سابق: ص14.

([18]) السند، مرجع سابق: ص16.

أما لفظة "الابتزاز" فقد استعملها العلماء في كتاباتهم قديمًا وحديثًا، ولم يكن هذا المصطلح يختلف في معناه القديم عن المعنى المعاصر، فجميعها تهدف إلى مفهوم واحد [19].

لهذا يمكن القول إن جريمة الابتزاز الإلكتروني هي أسلوب من أساليب الضغط والإكراه على المجني عليه يمارسه الجاني لتحقيق مقاصده الإجرامية، وإلا سيقوم بنشر المعلومات التي يحتفظ بها على الملأ، فيجد المجني عليه نفسه مرغمًا على تنفيذ تهديدات الجاني كما يصبح مسلوب الحرية والإرادة تفاديًا للتشهير والفضيحة، وهي صورة من الصور القبيحة التي تحملها نفس الجاني وفيها من الدناءة والوضاعة ما تشمئز منه النفوس السليمة، خاصة حينما يستغل ثقة شخص استأمنه، أو يصل إلى أسرار الآخرين باختراق أجهزتهم والتعدي على حياتهم الخاصة، ثم يبدأ بالضغط والإكراه وممارسة قوته أمام الضحية، والتي لا تجد مخرجًا سوى القبول بطلبات الجاني، وهنا تكون الضحية سبباً في استمرار الابتزاز لخشيتها من إبلاغ ذويها مما تتعرض له من تهديد وخوف وتعرضها للابتزاز النفسي والجسدي[20].

حيث أن المشرِّعَ الفلسطيني قد أولى من خلال قانون الجرائم الإلكترونية جلَّ اهتمامه في حماية حق السر أو انتهاك لخصوصية الأفراد أو ابتزازهم، وذلك من خلال فرض عقوبات رادعة عليهم، وذلك لأن لكل حق حرمه، وحرمة الحق تعني الحماية القانونية المقررة لهذا الحق، فالتفتيش بما يتضمن من إجراءات إنما يعد انتهاكًا قضائيًا لحرمة الحياة الخاصة التي تعد مستودعًا للاحتفاظ بالأسرار [21].

أما قانون العقوبات الفلسطيني لسنة 1936م يرى أن الابتزاز أو التهديد يتم ب: "قيام الجاني بتهديد المجني عليه بهدم مسكنه أو إيقاع الضرر بذلك المنزل، أو تهديده بإلحاق الأذى بذاته أو النيل من سمعته أو الإضرار بماله أو بتهديده بإلحاق الأذى بشخص ينتمي إليه أو النيل من سمعته"[22]. أما في قانون العقوبات رقم 16 لسنة 1960م والمطبق في المحافظات الشمالية فتنص العديد من مواده على أنه يكون التهديد إما من خلال التوعد بجناية بإجراء عمل أو الامتناع عن عمل أو التوعد بجناية مشافهة أو التهديد بجناية عقوبتها أقل من الأشغال الشاقة 15 سنة، أو التهديد بجنحة أو التهديد

([19]) محمد بن جرير الطبري، التبصير في معالم الدين، تحقيق: علي بن عبد العزيز بن علي الشبل، دار العاصمة، السعودية، ط1، 1996: ص157.

([20]) المطيري، مرجع سابق: ص27-28.

([21]) طارق محمد طميزة، التفتيش المعلوماتي في النظام القانوني الفلسطيني والمقارن، رسالة دكتوراه غير منشورة، جامعة أسيوط، مصر، 2018: ص34.

([22]) المادة 100 من قانون العقوبات رقم 74 لسنة 1936م المطبق في المحافظات الجنوبية.

بإنزال ضرر غير محق[23]، كما نصت المادة 414 منه على أنه: "يعاقب بالحبس لا أقل من ثلاثة أشهر بالغرامة لا أقل من عشرة دنانير كل من أقدم بالتهديد أو باستعمال العنف لاجتلاب نفع غير مشروع له أو لغيره على: (1) اغتصاب توقيع أو أي صك يتضمن تعهداً أو إبراء أو حوالة هذا الصك أو تغييره أو إتلافه. (2) تحرير ورقة أو بصمة أو توقيع أو ختم أو علامة أخرى على صك كي يستطاع فيما بعد تحويله أو تغييره أو استعماله كصك ذي قيمة. وتفرض عقوبة الأشغال الشاقة المؤقتة إذا كان الفاعل حاملاً سلاحاً هدد به المجني عليه". أما المادة 415 فقد نصت على أنه: "كل من هدد شخصاً بفضح أمر أو إفشائه أو الإخبار عنه وكان من شأنه أن ينال من قدر هذا الشخص أو من شرفه أو من قدر أحد أقاربه أو شرفه لكي يحمله على جلب منفعة غير مشروعة له أو لغيره عوقب بالحبس من أسبوع إلى سنتين وبالغرامة من خمسة دنانير إلى خمسين ديناراً"[24]. وفي مجال الجرائم الإلكترونية نظم القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية والمنشور في العدد الممتاز رقم (16) من الوقائع الفلسطينية بتاريخ 2018/05/03 هذا الأمر، حيث نص على إنه: "كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في تهديد شخص آخر أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان هذا الفعل أو الامتناع مشروعًا يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني ولا تزيد على ألف دينار أردني أو بكلتا العقوبتين"[25].

لهذا يمكننا تعريف جريمة الابتزاز الإلكتروني بأنها: "حصول الجاني على معلومات وسجلات ومستندات تتعلق بالضحية، ويقوم بتهديده بكشفها وفضحه والتشهير به في حال لم يستجب لطلباته، مما يؤثر على الضحية نفسيًا فيستجيب للجاني ويستجيب لرغباته ويبقى أسيرًا لها".

الفرع الثاني: أركان جريمة الابتزاز:

الأصل أن كل جريمة تتكون من ركنين الركن المادي والركن المعنوي وإذ تخلف أحدهما اعتبر الفعل غير مجرم كما تطلب القانون لبعض الجرائم قصداً خاصاً، حيث تتكون جريمة الابتزاز الالكتروني من ركنين أساسيين هما الركن المادي، والركن المعنوي.

([23]) المواد 350-351-352-353-354 من قانون العقوبات رقم 16 لسنة 1960م والمطبق في المحافظات الشمالية.

([24]) المواد 414-415 من قانون العقوبات رقم 16 لسنة 1960م والمطبق في المحافظات الشمالية.

([25]) المادة 15 من القرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية.

الركن المادي

يمكن تعريف الركن المادي بأنه: فعل ظاهري يبرز الجريمة ويعطيها وجودها وكيانها في الخارج.
كما يعرف بأنه وقوع فعل أو امتناع عن فعل حرمه القانون بما يجعل الجريمة تبرز إلى الوجود تامة كانت أو ناقصة.

فلا بدَّ من القيام بفعل مادي محسوس أو الامتناع عن القيام بفعل مادي يعاقب عليه القانون لتكون لدينا جريمة ابتزاز.

فجريمة الابتزاز لا تقع بمجرد وجود نية الجريمة، بل لا بد من فعل شيء مادي نشعر ونحس به، وهذا الفعل هو الركن المادي الذي يعتبر شرطًا أساسيًا لاعتبار الجريمة تامة[26].

ويعد السلوك أو الفعل المادي هو القاسم المشترك بين جميع الجرائم، وهو العنصر الأول من عناصر الجريمة الالكترونية، ويجب أن يكون الموضوع الذي يقع عليه السلوك محل حماية من قبل المشرِّع، وأن يكون مجرَّم بنص القانون، ويجب أن يترتب على هذا السلوك نتيجة إجرامية، وهو العنصر الثاني للركن المادي للجريمة، وهو الأثر الذي يتركه السلوك الإجرامي سواء أكان فعلاً أم تركاً في العالم الخارجي وذلك طبقاً للمفهوم المادي، أما المفهوم القانوني فهو الضرر الذي يصيب المصلحة التي يحميها الشارع، أما العنصر الثالث فهو العلاقة السببية بين السلوك سواء أكان فعلًا أم امتناعًا وبين النتيجة الإجرامية، بمعنى آخر لولا السلوك فعلًا أم امتناعًا ما كانت لتحدث النتيجة الإجرامية[27].

يمكن القول إنه عندما يتوفر الركن المادي في جريمة الابتزاز الإلكتروني أو الجرائم الإلكترونية بصفة عامة يجب أن تتواجد بيئة رقمية تتمثل في جهاز إلكتروني مثل الحاسب الآلي أو هاتف محمول، وأن يكون الجهاز الإلكتروني متصل بشبكة الإنترنت في الجرائم المتصلة بالإنترنت، فبدون ما ذكر لا يمكننا مباشرة السلوك الإجرامي، ولا نكون بصدد جريمة إلكترونية، فوجود الجهاز الإلكتروني يعتبر من أهم عناصر الجريمة الإلكترونية [28].

([26]) المطيري، مرجع سابق: ص37.

([27]) عبد القادر جرادة، مبادئ قانون العقوبات الفلسطيني، المجلد الأول، مكتبة آفاق، غزة، 2010: ص138 وما بعدها.

([28]) العفيفي، مرجع سابق: ص51

اكتفى المشرّع الفلسطيني بالسلوك أو النشاط الإجرامي كي يتحقق الركن المادي لجريمة الابتزاز الإلكتروني دون النظر إلى النتيجة الإجرامية وعلاقة السببية، فيكفى مباشرة المجرم لسلوكه الإجرامي للقول بإن الركن المادي للجريمة قد اكتمل، لكن في المقابل هناك بعض الجرائم تتطلب تحقق النتيجة الإجرامية لاكتمال الركن المادي بها؛ حيث نص القانون الفلسطيني في ذلك على أنه: "لا عبرة للنتيجة التي كان القصد أن يؤدي إليها ارتكاب فعل أو ترك إلا إذا ورد نص صريح على أن نية الوصول إلى تلك النتيجة تؤلف عنصرًا من عناصر الجرم الذي يتكون كله أو بعضه من ذلك الفعل أو الترك"[29].

لهذا يمكننا القول أن جريمة الابتزاز الالكتروني إنما هي جريمة شكلية، فبمجرد أن يقوم الجاني بالسلوك المكون لهذه الجريمة فإنها تصبح جريمة تامة، ومن ثم لا شروع في مثل هذه الجريمة.

وبطبيعة الحال ليست كل جريمة تستلزم وجود أعمال تحضيرية، وفي الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في جرائم الابتزاز الإلكتروني، إلا أنه في مجال تكنولوجيا المعلومات الأمر يختلف بعض الشيء. فشراء برامج اختراق، ومعدات لفك الشفرات وكلمات المرور، وحيازة صور دعارة للأطفال مثل هذه الأشياء تمثل جريمة في حد ذاتها، وبالتالي فهذا ينطبق على جريمة الابتزاز، والتي يمكن أن تستلزم مواد تحضيرية من خلال شراء البرامج والمعدات للدخول إلى الحاسب الآلي وابتزاز المجني عليه. وتثير مسألة النتيجة الإجرامية في جرائم الإنترنت مشاكل عدة، فعلى سبيل المثال مكان وزمان تحقق النتيجة الإجرامية، فلو قام أحد المجرمين في أمريكا اللاتينية باختراق جهاز خادم Server البنوك في الإمارات، وهذا الخادم موجود في الصين فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم؟ أو توقيت بلد البنك المسروق؟ أو توقيت الجهاز الخادم في الصين؟ وتثير أيضًا إشكاليات القانون الواجب التطبيق في هذا الشأن. حيث إن هناك بعد دولي في هذا المجال [30].

حيث تشير المادة (15) من قانون الجرائم الإلكترونية الفلسطيني لعام 2017م بأن: "كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في تهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه يعاقب بالحبس أو بغرامة لا تقل عن ألفي دينار أردني ولا تزيد عن خمسة آلاف دينار أو بالعقوبتين كليهما". كما تبرز المادة نفسها بأنه: "إذا كان التهديد بارتكاب جناية أو بإسناد أمور خادشة للشرف أو الاعتبار، يعاقب بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن ألفي

([29]) المادة 2/11 من قانون العقوبات الفلسطيني رقم 74 لعام 1936.

([30]) محمد على قطب، الجرائم المعلوماتية وطرق مواجهتها الجزء الثاني، الأكاديمية الملكية للشرطة، وزارة الداخلية، مملكة البحرين، مارس 2010: ص2.

دينار ولا تزيد عن خمسة آلاف دينار أو ما يعادلهما بالعملة المتداولة قانوناً [31]. اما المادة 15 من قانون الجرائم الالكترونية رقم 10 المعدل لسنة 2018م والمنشور في العدد الممتاز رقم (16) من الوقائع الفلسطينية بتاريخ 2018/05/03، فتنص على: "1- كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في تهديد شخص آخر أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان هذا الفعل أو الامتناع مشروعاً، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 2- إذا كان التهديد بارتكاب جناية أو بإسناد أمور خادشة للشرف أو الاعتبار، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً[32].

يمكن القول إن الركن المادي يتحقق في هذه الجريمة بالدخول إلى مجموعة أو بعض نظم المعالجة الآلية للمعطيات عن طريق الاحتيال، ويقصد بالدخول الدخول إلى محتويات الجهاز ذاته أي إجراء اتصال مباشر بالنظام بالطرق الفنية اللازمة لذلك، وعليه يمكن القول إن جريمة الدخول المنصوص عليها تعتبر من الجرائم الوقتية وليست من الجرائم المستمرة.

ويرى بعض الفقهاء أن الدخول إلى النظام قد يكون له عدة صور منها على سبيل المثال لا الحصر حصان طروادة، والذي يعني قيام الشخص بإدخال برنامج داخل الجهاز بحيث يقتصر دوره على التجسس بتسجيل نظام ترميز دخول المشتركين الأمر الذي يتيح له إمكانية الاحتفاظ على هذه المعلومات، وقد يتم الدخول بواسطة التقلص، أي استغلال ضعف الرقابة الداخلية للدخول إلى الجهاز[33].

إن أكثر الجرائم التي تتسبب بخسائر مادية جسيمة هي جرائم السرقة الإلكترونية، وإن أغلب هذه الجرائم ترتكب عبر اختراق مواقع البنوك لسرقة الحسابات البنكية، أو الحصول على بيانات العملاء في هذه الشركات، وكل ما يشمل الحصول على معلومات وبيانات ومستندات دون الحصول على إذن من صاحب المحل الإلكتروني، فذلك يكفي لقيام الركن المادي لجريمة السرقة الإلكترونية، وفي جريمة الإتلاف الإلكترونية هناك عدة طرق ووسائل قد ينتهجها المجرم الإلكتروني في ارتكاب جريمته، إما

([31]) المادة 15 من قنون الجرائم الإلكترونية الفلسطيني رقم 16 الصادر سنة 2017م.

([32]) المادة 15 من قنون الجرائم الإلكترونية الفلسطيني رقم 10 المعدل، والصادر سنة 2018م.

([33]) أمل المرشدي، الجرائم المعلوماتية، موقع محاماة نت، نشر بتاريخ 2016/7/17، للتفاصيل:
https://www.mohamah.net/law

عن طريق إتلاف البيانات الأساسية لقاعدة البيانات الخاصة بالمحل الإلكتروني، أو عن طريق الاتصال عن بعد والدخول لبرامج الحاسب الآلي وإتلاف البرامج والبيانات والمعلومات، أو عن طريق إرسال برامج فايروس لتدمير البيانات والمعلومات تلقائياً[34].

الركن المعنوي

الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، وقد تنقل المشرع الأمريكي في تحديد الركن المعنوي للجريمة بين مبدأ الإرادة ومبدأ العلم. فهو تارة يستخدم الإرادة كما هو الشأن في قانون العلامات التجارية في القانون الفيدرالي الأمريكي، وأحيانا أخري اخذ بالعلم كما في قانون مكافحة الاستنساخ الأمريكي.

برزت تلك المشكلة في قضية موريس الذي كان متهما في قضية دخول غير مصرَّح به علي جهاز حاسب فيدرالي وقد دفع محامي موريس على انتفاء الركن المعنوي، الأمر الذي جعل المحكمة تقول: "هل يلزم أن يقوم الادعاء بإثبات القصد الجنائي في جريمة الدخول غير المصرَّح به، بحيث تثبت نية المتهم في الولوج إلى حاسب فيدرالي، ثم يلزم إثبات نية المتهم في تحدي الحظر الوارد على استخدام نظم المعلومات في الحاسب وتحقيق الخسائر، ومثل هذا الأمر يستدعي التوصل إلى تحديد أركان جريمة الدخول دون تصريح". وبذلك ذهبت المحكمة إلى تبني معيارين هنا هما الإرادة بالدخول غير المصرَّح به، وكذا معيار العلم بالحظر الوارد على استخدام نظم معلومات فيدرالية دون تصريح [35]، ويتوفر القصد الجنائي في حق الجاني في ثلاث حالات هي:

الأولى: إذا كان الجاني يتوقع أو يريد أن يترتب على فعله أو امتناعه حدوث الضرر أو وقوع الخطر الذي حدث والذي يعلق عليه القانون وجود جريمة.

الثانية: إذا نجم عن الفعل أو الامتناع ضرر أو خطر أكثر جسامة مما كان يقصده الفاعل، وهي حالة جواز القصد الذي ينص عليها القانون صراحة على إمكان ارتكابها بهذا الوصف، وهنا يتوافر القصد المتعدي.

([34]) ناير جميل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، الاسكندرية، 2012: ص71.

([35]) فؤاد جمال، جرائم الحاسبات والإنترنت، الجرائم المعلوماتية، مركز المعلومات ودعم اتخاذ القرار، مارس ٢٠٠٥: ص27 وما بعدها.

الثالثة: الحالات التي يعزي فيها القانون الفعل إلى الفاعل نتيجة لفعله أو امتناعه، أي حالات يفترض فيها القانون توافر القصد الجنائي لدى الجاني افتراضًا، وهو مستمد من أنه طالما أنَّ النتيجة الجسيمة التي تحققت نشأت عن فعل الجاني، فمقتضى ذلك أن هذا الفعل كان صحيحًا لإحداثها، ولكونه كذلك فإن الجاني يجب أن يتحمل نتائجه، توقعها أو لم يتوقعها وهنا يتوافر القصد الاحتمالي وهو عبارة عن توقع النتيجة الاجرامية وقبولها ومن ثم المضي قدماً في سبيل ارتكاب الفعل أو السلوك المؤدي إليها[36].

يمكن القول إن الركن المعنوي إذا توفر في جرائم الابتزاز الإلكتروني، فإن ذلك يعد من الأمور الهامة في تحديد طبيعة السلوك المرتكب وتكييفه لتحديد النصوص التي يلزم تطبيقها، إذ إنه وبدون الركن المعنوي لن يكون هناك سوى جريمة واحدة هي جريمة الدخول أو الولوج غير المشروع، فمثلًا إن التمييز بين جريمة الدخول غير المشروع على نظام المعالجة الآلية للبيانات وبين جريمة تجاوز الصلاحيات في الدخول على مثل هذا النظام يعد تمييزًا دقيقًا. ففي جريمة تجاوز صلاحية الدخول فإنه يلزم لتوافرها أن يكون هناك صلاحية للدخول على نظام ما، على أن تتوافر في النظام أنظمة ليس من حقه الدخول إليها، فيقوم المذكور بالدخول إليها، فإذا دخل على هذه الأنظمة فإنه سيقع عليه جريمة واحدة وهي الدخول على الأنظمة التي منع من الدخول إليها وبالتالي يعاقب على جريمة واحدة، وهي الدخول على الأنظمة بطريقة غير مشروعة، دون أن يعاقب على الجريمة الأخرى وهي ابتزاز أصحاب تلك الأجهزة [37].

إن المجرم الإلكتروني يتوجه من أجل ارتكاب فعل غير مشروع أو غير مسموح مع علم هذا المجرم بأركان الجريمة، وبالرغم من أن بعض المخترقين يبررون أفعالهم بأنهم مجرد فضوليين وأنهم قد تسللوا صدفة، فلا انتفاء العلم كركن للقصد الجنائي*، حيث كان يجب عليهم أن يتراجعوا بمجرد دخولهم ولا يستمروا في الاطلاع على أسرار الأفراد والمؤسسات، لأن جميع المجرمين والأشخاص الذين يرتكبون هذه الأفعال يتمتعون بمهارات عقلية ومعرفية كبيرة تصل في كثير من الأحيان إلى حد العبقرية. فالقصد الجنائي متوافر في غالبية الجرائم الإلكترونية ولكن هذا لا يمنع أن هناك بعض الجرائم

([36]) عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية: دراسة مقارنة، رسالة ماجستير غير منشورة، جامعة الشرق الأوسط، الأردن، 2014.: ص30.

([37]) المرجع السابق: ص30.

* يمكن تعريف القصد الجنائي بأنه: "إرادة الفعل المكون للجريمة، وإرادة نتيجته التي يتمثل فيها الاعتداء على الحق الذي يحميه القانون، وإرادة كل واقعة تحدد دلالة الفعل الإجرامية وتعد جزءاً من ماديات الجريمة"، للتفاصيل:
عثمان يحيى أبو مسامح، الأركان العامة لجريمة التخابر في التشريع الفلسطيني مقارنة بالتشريع المصري والأردني: دراسة تحليلية مقارنة، مجلة جيل الدراسات المقارنة العدد7، يونيو 2018: ص78.

الإلكترونية تتطلب أن تتوافر فيها القصد الجنائي الخاص مثل جرائم تشويه السمعة عبر الإنترنت. أما جرائم نشر الفيروسات عبر الشبكة فهي تتوفر على القصد الجنائي الخاص*، فالمجرم يهدف إلى تعطيل عمل الشبكة وفي جميع الحالات المشرِّع هو من يختص بتحديد الحالات التي يشترط فيها توافر القصد الجنائي الخاص[38].

بناءً على ما سبق فإن القصد الجنائي يعتبر صورة الإرادة لتحقيق الركن المعنوي، وهو يقوم على عنصرين مهمين هما: **العلم** ويقصد به علم الجاني بنتيجة جريمته والوقائع المتصلة بها والعلم بموضوع الجريمة، فالأصل علم الجاني بكل العناصر التي تساهم في ارتكاب جريمة الابتزاز الإلكتروني سواء أكانت مادية أم معنوية. أما العنصر الآخر فهو **الإرادة** ويقصد بها القوة النفسية والنشاط النفسي الموجَّه لتحقيق هدف معين بوسيلة معينة، والإرادة هي المحرك للسلوك الإجرامي، ففي الابتزاز الإلكتروني يجب أن تتجه الإرادة إلى أمرين هما: الحصول على معلومات سرية للضحية، وقيامه بالابتزاز للحصول على المال أو المتعة الجنسية، كما أن الإرادة تنقسم إلى قسمين هما إرادة الفعل وإرادة النتيجة، فالأولى تكون لمساءلة الجاني عن فعلته، والثانية تقوم على النتيجة التي جناها الجاني من هذه الفعلة كالحصول على المال أو إشباع الرغبة[39].

وبالتالي يجب أن يكون الجاني متمتعًا بإرادة حرة واعية حال ارتكابه الجريمة، دون إجبار أو إكراه من أحد كي يقوم بارتكاب هذه الجريمة، ويكون حينها قد ارتكب جريمته وهو يتمتع بحرية الاختيار والتمييز، فلا يمكن أن ينسب السلوك معنويًا لمن لم يكن لديه القدرة على الاختيار أو التمييز ساعة ارتكاب الجريمة، وهذه الإرادة يتبعها تحمل المسؤولية القانونية والجزائية على كافة الأفعال المخالفة للقانون والتي يرتكبها الجاني [40].

---

* قد يتطلب القانون في بعض الجرائم أن يتوافر لدى الجاني إرادة تحقيق غاية معينة من الجريمة، فلا يكتفي بمجرد تحقق غرض الجاني كما في القصد الجنائي العام، بل يذهب إلى أكثر من ذلك فيتغلغل إلى نوايا الجاني ويعتدّ بالغاية التي دفعته إلى ارتكاب الجريمة، كما لا يختلف القصد الخاص عن القصد العام من حيث العناصر التي تكوّن كلا منها، فطبيعتهما واحدة تقوم على توافر ذات العناصر أي عنصري: العلم والإرادة، لكن موضوع العلم والإرادة في القصد الخاص أكثر تحديداً وكثافة منه في القصد العام. للتفاصيل:
عبد الله سليمان: شرح قانون العقوبات الجزائري (القسم العام/ الجريمة)، ديوان المطبوعات الجامعية، الجزائر، 1998: ص 262 ،263 ، 264.

([38]) أمل المرشدي، أركان الجريمة الإلكترونية في التشريع الجزائري، موقع محاماة نت، نشر بتاريخ 2017/1/7، للتفاصيل:

https://www.mohamah.net/law

([39]) المطيري، مرجع سابق: ص41 وما بعدها.

([40]) أمين محمد نوفل، قانون العقوبات العام، كلية الشرطة الفلسطينية، غزة، د.ت: ص8.

أما المشرّع الفلسطيني فقد حاول جاهدًا إبراز أهمية توفر الركن المعنوي في جريمة الابتزاز الإلكتروني، حيث بيّن أهمية المحاولة التي تسبق تنفيذ الجريمة، فقد نص القانون الفلسطيني على أنه: "يعتبر الشخص بأنه حاول ارتكاب الجرم إذا ما شرع في تنفيذ نيته على ارتكاب ذلك الجرم باستعمال وسائل تؤدي إلى وقوعه، وأظهر نيته هذه بفعل من الأفعال الظاهرة، ولكنه لم يتمكن من تنفيذ نيته إلى حد إيقاع الجرم"[41].

كما تناول قانون العقوبات الفلسطيني هذه الجرائم من نشأته عام 1960م، لكنه لم يشر إلى وسائل الاتصال الحديثة نظرًا لِقِدَمِه، لكنَّه في المقابل نصّ صراحة على تجريم ارتكاب جرائم القدح والذم والتشهير والسرقة والانتحال والاحتيال وغيرها، وهذه الجرائم ذاتها يتم ممارستها بصورة واسعة عن طريق الوسائل الإلكترونية، ومن هذه العقوبات ما يلي [42]:

أبرزت المادة 213 أن من ثبت انتحاله اسم غيره في تحقيق قضائي أو محاكمة قضائية يعاقب بالحبس من شهر إلى سنة، وهنا نحن بصدد جريمة الابتزاز الالكتروني.

أوضحت المادة 348 أنه يعاقب بالحبس مدة لا تتجاوز أسبوع أو غرامة لا تتجاوز عشرة دنانير من تسلل بواسطة الكسر أو العنف على الأشخاص إلى أماكن تخص الغير وليست مباحة للجمهور، أو مكث فيها على الرغم من رغبة من له الحق في إقصائه عنها، ولا يلاحق المجرم إلا من خلال شكوى الفريق المتضرر.

كما نصت المادة 416 على معاقبة كل من استعمل دون وجه حق شيئًا يخص غيره بصورة تلحق به ضررًا دون أن يكون قاصدًا اختلاس ذلك الشيء، بالحبس حتى ستة أشهر، وبالغرامة حتى عشرين دينارًا أو بإحدى هاتين العقوبتين، أيضاً المادة 415 من قانون العقوبات الأردني المطبق بالضفة الغربية والمتعلق بالابتزاز التقليدي، والتي تنص على: "كل من هدد شخصاً بفضح أمر أو إفشاء أو الإخبار عنه، وكان من شأنه أن ينال من قدر هذا الشخص أو من شرفه لكي يحمله على جلب منفعة غير مشروعة له أو لغيره عوقب بالحبس من اسبوعين إلى سنتين وبالغرامة من خمسة دنانير إلى خمسين ديناراً".

([41]) المادة 1/30 من قانون العقوبات الفلسطيني رقم 74 سنة 1936.

([42]) خاص معهد أبحاث السياسات الاقتصادية "ماس"، دراسة نقدية للإطار القانوني للجرائم الإلكترونية في الأراضي الفلسطينية، القدس، 2012: ص18.

أيضًا نصت المادة 445 على معاقبة كل من ثبت إلحاقه ضررًا بمال غيره المنقول باختياره، وبناءً على شكوى المتضرر، بالحبس لمدة لا تتجاوز سنة أو غرامة لا تتجاوز خمسين دينارًا أو بكلتا العقوبتين، وأن تنازل المشتكي يُسقط دعوى الحق العام.

أما القرار بقانون رقم (10) لسنة 2018م والمنشور في العدد الممتاز رقم (16) من الوقائع الفلسطينية بتاريخ 2018/05/03 بشأن الجرائم الإلكترونية فقد اهتم بإبراز الركن المعنوي الذي يسبق الفعل الإجرامي، فقد نص في مادته الخامسة عشر على: " كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في تهديد شخص آخر أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان هذا الفعل أو الامتناع مشروعاً، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 2. إذا كان التهديد بارتكاب جناية أو بإسناد أمور خادشة للشرف أو الاعتبار، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً"[43].

كذلك نصت المادة 22 من القرار ذاته على أنه: "1. يحظر التدخل التعسفي أو غير القانوني في خصوصيات أي شخص أو في شؤون أسرته أو بيته أو مراسلاته. 2. كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات بقصد نشر أخبار أو صور أو تسجيلات صوتية أو مرئية، سواء كانت مباشرة أو مسجلة، تتصل بالتدخل غير القانوني في الحياة الخاصة أو العائلية للأفراد، ولو كانت صحيحة، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين"[44].

من خلال ما سبق يتضح أن توفر الركن المعنوي في جريمة الابتزاز الإلكتروني يعتبر من الأمور الهامة التي لا يمكن الاستغناء عنها في إثبات وجود الجريمة، أو في طبيعة السلوك الإجرامي المرتكب، إذ إنه بدون وجود الركن المعنوي لن يكون هناك جريمة مكتملة، أي بمعنى أن جريمة الابتزاز الالكتروني لا تقع بطريق الخطأ، أي لا تكون من الجرائم غير المقصودة.

---

[43] المادة 15 من قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية.

[44] المادة 22 من قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية.

كما يمكن القول إن قانون العقوبات الفلسطيني لعام 1960م قد قام بتجريم العديد من الجرائم التي يمكن أن تحدث من خلال الوسائل الإلكترونية الحديثة على الرغم من قدم القانون، وذلك بأن العديد من الجرائم تحدث في كل وقت مع اختلاف الوسيلة المرتكبة في الجريمة.

المطلب الثاني: أنواع وخصائص جريمة الابتزاز الإلكتروني.

نظراً لما شهدته البشرية في السنوات الأخيرة من تطور هائل في وسائل الاتصال والتواصل ناتجة عن استخدام الشبكة العنكبوتية "الإنترنت"، وظهور وسائل التواصل الاجتماعي كالإنستغرام، الفيس بوك، التويتر والسناب تشات وغيره الكثير من البرامج، حيث باتت هذه الوسائل تستخدم بين الكبير والصغير، بين المميز وغير المميز، ما نتج عنها تطور ملحوظ لهذه الجريمة كنتيجة لأي تطور آخر، ما جعل هناك أنواع وخصائص اختلفت من وقت لآخر نتيجة السرعة في هذا التطور واختلاف جرائم الابتزاز عن السابق.

حيث سيتم التعرض في هذا المطلب لأنواع وخصائص جريمة الابتزاز الالكتروني، وذلك كما يلي:

الفرع الأول: أنواع جريمة الابتزاز الإلكتروني

نظراً لتزايد نسب ارتكاب جريمة الابتزاز الالكتروني في الآونة الأخيرة، لا سيما وإن لهذه الجريمة خصوصية تختلف عن بقية الجرائم التقليدية، ووسائل وطرق تنفذ بها، الأمر الذي أدى إلى تشعبها وتفرّع أنواعها، والتي تتعلق بالأنواع طبقاً لشخصية المجني عليه، وتبعاً لوسائله، وتبعاً للهدف المرجو منه، وهكذا.

أولاً: أنواع جريمة الابتزاز طبقًا لشخصية المجني عليه (المبتز)

الشخصية الاعتبارية (المعنوية)

يمكن تعريف جريمة الابتزاز بحق الشخصية الاعتبارية بأنه: "نوع من جرائم الابتزاز الإلكتروني تكون فيها الفئة المستهدفة كضحية هي الحكومات والشركات والمؤسسات ذات الشخصية المعنوية، وذلك حيث تتم جريمة الابتزاز عن طريق الحصول على معلومات سرية خاصة بالضحية كمؤسسة أو شركة أو وزارة حكومية، والتهديد بالإعلان عن هذه المعلومات ونشرها للآخرين[45].

([45]) المطيري، مرجع سابق: ص48.

يعتبر هذا الفرع من الجرائم الإلكترونية أشدها خطورة وتأثيرًا وأكثرها حدوثًا وتحقيقًا للخسائر للأفراد والمؤسسات على حد سواء. ويشمل هذا الفرع الأنشطة التي تتضمن تعديل أو محو أو سرقة أو إتلاف أو تعطيل العمل للمعلومات وقواعد البيانات الموجودة بصورة إلكترونية على الحواسب الآلية المتصلة أو غير المتصلة بشبكات المعلومات، أو مجرد محاولة الدخول بطريقة غير مشروعة عليها، وأبسط تلك الأنشطة هو الدخول لأنظمة المعلومات وقواعد البيانات بصورة غير مشروعة والخروج دون إحداث أي تأثير سلبي عليها، ويقوم بذلك النوع من الأنشطة ما يطلق عليهم ذوي الياقات البيضاء، والذين يقومون بالدخول بطريقة غير مشروعة على أنظمة الحاسب أو شبكات المعلومات أو مواقع الإنترنت مستغلين بعض الثغرات في تلك النظم مخترقين بذلك سياسات وإجراءات أمن المعلومات التي يقوم بها مديرو تلك الأنظمة، وكما ذكرنا فإن وصول شخص غير مصرح له وإمكانية دخوله إلى حجرة الحواسب المركزية بالمؤسسة ثم خروجه دون إحداث أي أضرار يعتبر خرقًا لسياسة وإجراءات أمن المعلومات بتلك المؤسسة [46].

تجدر الإشارة إلى أن كل حالات السرقة والاحتيال التي تتم عن طريق تزوير البيانات إلكترونياً، إنما نجد أننا أمام حالة من حالات تعدد الجرائم، ويتحقق فيها التعدد المعنوي للجرائم خاصة مثل التلاعب الذي يتم بالأرصدة المصرفية، لأن عمليات التحويل غير المشروعة تتم عن طريق تعديل في البيانات والأسماء، أو تعديل في البرامج المعلوماتية المعالجة لهذه البيانات، مما يترتب عليه تحويلات مالية غير مشروعة، ما يوجب تطبيق أحكام التعدد المعنوي والارتباط بين الجرائم [47].

يمكن القول من خلال ما سبق إن هذا النوع من الابتزاز يعتبر من أخطر الأنواع، حيث إن سرقة وابتزاز المؤسسات والحكومات بمستندات وأوراق رسمية يمكن أن يعَرِّض هذه المؤسسات والحكومات لخطر عظيم، خاصةً أن هذه الأوراق تعتبر مهمة جدًا لهذه المؤسسات ومن غير المعقول أن يقوم أحد من خارج هذه المؤسسات بالاطلاع عليها، كما أن نشرها يمكن أن يكون انتكاسة لهذه المؤسسات.

الرجال (الشخص الطبيعي)

يمكن أن يكون الرجل مجنيًا عليه في جريمة الابتزاز الإلكتروني لعدد من الأسباب، فقد يكون ميسور الحال وعرضة للابتزاز من بعض النساء اللواتي يقمن بهذا العمل بدافع الحصول على الأموال عن

([46]) قطب، مرجع سابق: ص6.

([47]) العجمي، مرجع سابق: ص57-58.

طريق المواقع الإلكترونية، حيث تقوم بابتزازه بنشر صور أو مقاطع مصورة لتهديد مركزه، مما يدفعه للقبول بتقديم التنازلات كي لا تسوء سمعته، كما قد يكون الرجل عرضة لجرائم الابتزاز بشكل عام بسبب أسرار في مجال عمله، أو عائلته، أو أي معلومات بشكل عام يرى الرجل الضحية أنَّ الإفصاح عنها ونشرها يؤذي شرفه وسمعته ويضعضع مركزه بين عشيرته[48].

لقد قام مرتكبو الجرائم الإلكترونية بتكثيف نشاطاتهم في الفترة الأخيرة باستهداف فئة الرجال، حيث إن الأمر بدا مُمَنهجًا ومدروسًا من قبل عصابات دولية تقيم في دول أخرى، حيث يتم الاستهداف لهؤلاء الذكور ممن يشغلون مناصب مهمة ومرموقة في عدد من المؤسسات ويحاولون الإيقاع بهم، حيث يتم استدراج الضحية عبر قيام أحد الأشخاص بانتحال صفة فتاة، تقوم بالتواصل مع الضحية عبر فيسبوك أو تويتر، وبعد ذلك تطلب منه محادثتها بالفيديو عبر سكايب، وبعد إيهام الضحايا بأن الطرف الجديد الذي يرغب بالتواصل معهم، هي فتاة جميلة بسن المراهقة، يقوم المبتز بتسجيل هذه المحادثة بطريقة أو بأخرى وليبتز المجني عليه بنشر صورهم على حساباتهم الشخصية على فيس بوك بعد اختراقها ما لم يعطوه أموالًا ليمتنع عن ذلك[49].

يلجأ هؤلاء المجرمين إلى إثارة الخوف والهلع لدى المجني عليهم والضحايا، خاصة بعد قيامه بتحميل مقطع الفيديو على شبكة اليوتيوب أو فيسبوك مباشرة فور الانتهاء من تسجيلها، وإرسال الروابط إلى الضحية، وإبلاغه بأن الفيديو مجمَّد إلى أن يدفع المبلغ المطلوب، وإلا سوف يتم نشره للعموم ومن ثم إرساله إلى قائمة أصدقائه عبر شبكة فيسبوك وتويتر ووسائل التواصل الاجتماعية الأخرى، وهو ما يجعل العديد من الضحايا يوافقون على شروط المجرم بسهولة [50].

النساء

يعتبر ابتزاز النساء من أكثر أنواع الابتزاز انتشارًا وشيوعًا، حيث يتحكم في هذا النوع غالبًا الرغبات الجنسية، حيث يطلب المبتز من الضحية إشباع رغباته الجنسية، وذلك من خلال تهديدها بفضحها، حيث يتمكن من إخضاع الضحية لإرادته، كما أنه قد يطلب من الضحية ممارسة الجنس معه أو مع أصدقاءه، وذلك مع تصاعد نغمة التهديد بفضح أمر الضحية بين الأسرة والأهل والرفاق بنشر صور إباحية لها على شبكة الإنترنت، حيث يتنوع هذا الابتزاز ليشمل ابتزاز المرأة من محارمها، أو ابتزازها

([48]) داليا عبد العزيز، المسؤولية الجنائية عن جريمة الابتزاز الإلكتروني في النظام السعودي دراسة مقارنة، مجلة جيل الأبحاث القانونية المعمقة العدد 25، مايو 2018: ص36.

([49]) خاص صحيفة البيان الإماراتية، تحذير من تنامي ظاهرة الابتزاز الإلكتروني للرجال في الشرق الأوسط، 24 فبراير 2015.

([50]) المرجع السابق.

من رؤساء العمل لديها، كذلك ابتزازها من قبل الباعة في الأسواق بهدف تخفيض قيمة السلع مقابل إقامة علاقة معهم، كذلك ابتزاز النساء عن طريق الهاتف بمحادثة المرأة ومن ثم تسجيل مكالمات لها معه وتهديدها بالقيام بعدة أفعال مقابل عدم نشره للمكالمة، وترضخ النساء لذلك حتى تقع في الفاحشة[51].

كما أن التنوع يشمل الابتزاز الإلكتروني عن طريق محادثات الشات، حيث يقوم الشاب بالتعرف على الفتاة عن طريق الشات أو الماسنجر، بالصوت والصورة ويقوم بتصويرها عن طريق محادثته معها، خاصة إذا طلب منها تصوير جسدها ومن ثم يلتقط صور لها، ثم يقايضها بين نشر تلك الصور أو مقابلتها ما يجعلها ترضخ له. أيضًا هناك ابتزاز الفقراء أصحاب الدخل المحدود والعاملين في المنازل، كذلك ابتزاز الفتيات الهاربات من ذويهن حيث يتم اصطيادهن في الأسواق لممارسة الدعارة بعد ابتزازهن بإعادتهن إلى أهاليهن، وابتزاز النساء من قبل بعض متمرسي الرقية، أيضًا ابتزاز النساء من قبل السحرة والمشعوذين. حيث اعتبر هذا النوع من الابتزاز الموجه للنساء بشكل خاص أكثر الأنواع شيوعًا، نظرًا للتطور العلمي والتكنولوجي الهائل الذي ساعد على انتشار هذا النوع من الجرائم عبر التقنيات الاتصالية المتطورة، وضعف الرقابة الأسرية [52].

تعتبر جرائم الابتزاز الإلكتروني الخاصة بالنساء نموذجًا مثاليًا للجريمة، ويرجع ذلك غالبًا بأنه يكون تهديد المبتز للمرأة بصور فاضحة أو محادثات خادشه للحياء، أو عرض مرئي لعلاقة غير شرعية جمعت ما بين المبتز وضحيته، والمبتز يمكن أن يكون قد خطط لجريمته قبل الجريمة، حيث سرعان ما تتجاوب الضحية مع شروط وتهديدات المبتز، وذلك منعًا للعار الذي يمكن أن يلحق بها وبعائلتها إذا ما رفضت طلب الجاني، خاصة إذا ما كان سبب الابتزاز علاقة غير مشروعة ينظر لها المجتمع بالتحريم والرفض والاستهجان [53]

الأطفال

هناك القليل من التشريعات والقوانين من أعطى تعريفًا محددًا للأطفال أو الأحداث، وذلك بسبب اختلاف تحديد سن التمييز وسن الرشد، بسبب العوامل الطبيعية والاجتماعية والثقافية الخاصة بكل مجتمع وتفرده، فالحدث في الأنظمة الخاصة بالأحداث في المملكة العربية السعودية، هو من بلغ

([51]) محمد بن منصور آل النمر، دور تقنية المعلومات في مكافحة جرائم الابتزاز، رسالة ماجستير غير منشورة، جامعة نايف للعلوم الأمنية، الرياض، 2013: ص44-45.

([52]) المرجع السابق: ص46-47.

([53]) المطلق، مرجع سابق: ص10.

الخامسة عشر من عمره ولم يبلغ الثامنة عشر، ويعد الحدث راشدًا ببلوغه الثامنة عشر من العمر، كما تكثر جرائم ابتزاز الأطفال، وذلك حيث يقوم المبتز بالضغط على الحدث بتهديده بنشر صور أو تسجيل مرئي أو محادثات على مواقع الدردشة، أو غيرها، عن واقعة يكون من شأنها تحقير المجني عليه عند أهله ومجتمعه، كما أنَّ الطفل ضحية سهلة لجرائم الابتزاز الإلكتروني، وذلك لسهولة انزلاقه في الجريمة، ولقلة خبرته، فالأحداث والأطفال من أكثر الفئات اتصالًا بالتكنولوجيا ووسائل التواصل الاجتماعي وأكثر بسبب شغفهم به، ورغبتهم في التجربة، حيث باتت تشكل حيزًا كبيرًا من يومهم. مما يسهل انزلاقهم في الجريمة [54].

أما القانون الفلسطيني فقد قام بتعريف الحدث في قانون رقم 4 لسنة 2016 بشأن حماية الأحداث بأنه: "الطفل الذي لم يتجاوز سنه (18) سنة ميلادية كاملة وقت ارتكابه فعلاً مجرماً، أو عند وجوده في إحدى حالات التعرض للانحراف، ويحدد سن الحدث بوثيقة رسمية، فإذا ثبت عدم وجودها يُقدر سنه بواسطة خبير تعينه المحكمة أو نيابة الأحداث حسب مقتضى الحال"[55].

أما قانون الطفل الفلسطيني رقم 7 لسنة 2004م فقد اهتم بتعريف الطفل، حيث أورد في مادته الأولى تعريفاً للطفل بأنه: " الطفل هو كل إنسان لم يتم الثامنة عشرة من عمره"[56].

اعتبر القانون الفلسطيني ابتزاز الأطفال جريمة يعاقب عليها بصورة أشد من الجرائم الأخرى، حيث أفرد المشرّع الفلسطيني في القانون الفلسطيني المعدل رقم (10) لسنة 2018م والمنشور في العدد الممتاز رقم (16) من الوقائع الفلسطينية بتاريخ 2018/05/03، أكثر من مادة لإبراز عقوبة على كل من يقوم بهذا الفعل سواءً أكان بالحبس، أم بدفع غرامة مالية، لما لهذه الشريحة من أهمية في المجتمع، وما يمكن أن يكون لهذه الجريمة من عواقب سواء أكان على الطفل أم على المجتمع ككل، حيث نصت المادة (16) البند رقم (2) على أن: " كل من أرسل أو نشر عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات قصدًا كل ما هو مسموع أو مقروء أو مرئي يتضمن أعمالًا إباحية لمن لم يكمل الثامنة عشر سنة ميلادية أو تتعلق بالاستغلال الجنسي لهم، يعاقب

([54]) عبد العزيز، مرجع سابق: ص35.

[55] المادة الأولى من قرار بقانون رقم 4 لسنة 2016 بشأن حماية الأحداث.

[56] المادة الأولى من قانون الطفل الفلسطيني رقم 7 لسنة 2004م

بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا، أو بكلتا العقوبتين"[57].

كما نصت المادة (16) البند رقم (3) على أن: " كل من قام قصدًا باستخدام الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في إنشاء أو إعداد أو حفظ أو معالجة أو عرض أو طباعة أو نشر أو ترويج أنشطة أو أعمال إباحية لغايات التأثير على من لم يكمل الثامنة عشر سنة ميلادية أو من ذوي الإعاقة، يعاقب بالحبس مدة لا تقل عن سنتين، أو بغرامة لا تقل عن ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا، أو بكلتا العقوبتين"[58].

حيث يعتبر استغلال وابتزاز الأحداث والأطفال من أخطر أنواع الابتزاز، حيث إن العديد من القوانين الدولية قد ضاعفت عقوبة ابتزاز الحدث، مع العديد من المطالبات والتحذيرات من استخدام الأطفال في هذه الجريمة، فمثلًا حذر مركز مكافحة استغلال الأطفال وحمايتهم على الإنترنت في بريطانيا من أنّ المئات من الأطفال البريطانيين يجري ابتزازهم للقيام بممارسات جنسية على شبكة الإنترنت، وقال مركز مكافحة استغلال الأطفال وحمايتهم على الإنترنت إنه من خلال 12 قضية ظهرت على مدى عامين، تعرض 424 طفلًا للابتزاز بهذه الطريقة، وكان من بينهم 184 طفلًا في بريطانيا. وقال نائب المدير التنفيذي للمركز أندي بيكر إن هذه الانتهاكات "تصاعدت بشكل سريع حقا"، وأضاف لراديو بي بي سي أن الأمر يمكن أن يستغرق أربع دقائق فقط ليتحول الحوار من مجرد التحية وسؤال الطفل إذا كان يرغب بالتعري إلى إيذاء الطفل لنفسه، وهو ما يمكن أن يتحول لجريمة ابتزاز في النهاية [59].

([57]) المادة 16 البند2 من قرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية، صحيفة الوقائع الفلسطينية، العدد16 ، 2018/5/3: ص15.

([58]) المادة 16 البند3 من قرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية، صحيفة الوقائع الفلسطينية، العدد16 ، 2018/5/3: ص15.

([59]) خاص موقع bbc عربي، "ابتزاز مئات الأطفال في بريطانيا" عبر الإنترنت، 21 سبتمبر/ أيلول 2013، للتفاصيل:

http://www.bbc.com/arabic/worldnews/2013/09/130920_cyber_blackmail_childeren

ثانياً: أنواع جريمة الابتزاز طبقًا لوسائله

1- وسائل مادية

وهي الوسائل التي تتضمن ابتزاز المجني عليه مادياً مثل: تصوير محادثات الماسنجر أو صور خاصة بالضحية أو رسائل غرامية بينهما، ثم يبدأ الجاني بالقيام بتهديد الضحية بتلك الوسائل المادية عن طريق [60]:

1- فضحها أمام أهلها وأقاربها بتلك الصور والرسائل.

2- تهديدها بنشر صورها أو رسائلها الغرامية على وسائل التواصل الاجتماعي.

3- تهديد المجني عليها بإيصال صورها إلى أهلها وولي أمرها وهي في وضع مشين كالتعري أو وقت فعل الفاحشة معها أو غير ذلك.

كما يمكن أن يكون التهديد والابتزاز بارتكاب الجريمة واضحًا وصريحًا، كما يمكن أن يكون غامضًا مثل إرسال خنجر يقطر دمًا أو جمجمة وعظم، أو إغماد خنجر في باب منزل المجني عليه، أو وضع مواد ملتهبة حول بيته، أو إرسال رسومات له حول ما سبق، وقد يكون التهديد كتابة أو بواسطة شخص ثالث، فالتهديد والوعيد بشَرٍّ يصيب المجني عليه بالخوف والفزع الذي يحمله على تلبية طلبات الجاني، كما يمكن أن يوجه التهديد للمجني عليه مباشرة عن طريق زوجته أو قريب له، كما يعتبر جريمة ابتزاز كل من امتنع عن إنقاذ شخص يحتاج إلى إنقاذ أو الامتناع عن تقديم المساعدة لأي شخص، فإذا تحققت النتيجة الإجرامية بناء على التهديد فإنه يلزم أن تتوفر علاقة السببية بين التهديد والتسليم، فإذا لم يحدث التهديد هذا الأثر وتم التسليم أو تحقيق المنفعة نتيجة لاعتبارات أخرى لا تتعلق بالابتزاز انقطعت علاقة السببية ووقف نشاط الجاني عند حدِّ الشروع في جريمة الابتزاز[61].

تتمثل الوسائل المادية في هذه الجريمة بالعمل بتصرف مادي يصدر عن الفاعل الأمر الذي يتطلب مشاهدة أو إدراك هذا التصرف من الغير، وهو ما يشار إليه بمصطلح العلانية، حيث إن أكثر هذه الجرائم هي جرائم الذم والقدح والتشهير حيث ترتكب هذه الأفعال بطريقة كتابية أو صور أو سمعية، وهو يمثل اعتداء على الحياة الخاصة وحرمتها، ومن صورها الاعتداء على معلومات خاصة بالمحامين أو الأطباء أو المحاسبين أو غيرهم، وتتم بالاطلاع على البيانات الخاصة بهم وتسجيلها وابتزازهم بها [62].

([60]) آل النمر، مرجع سابق: ص66-67.

([61]) علي أحمد القاعدي، الجرائم المتعلقة بجريمة اختطاف الأفراد والممتلكات، مجلة جامعة الناصر، العدد 3، يونيو 2014: ص297-298.

([62]) العفيفي، مرجع سابق: ص25-26.

2- وسائل معنوية

تعتبر جريمة الابتزاز من الجرائم المربكة للضحية ولأهله، حيث يعتبر الابتزاز عملية تهديد وترهيب للضحية بنشر صور أو مواد فيلمية أو تسريب معلومات سرية تخص الضحية، مقابل دفع مبالغ مالية أو استغلال الضحية لفعل أمر ما، وتصاحب هذا التهديد حالة نفسية تؤثر على تفكيره، حتى لو لم يتم نشر هذه المواد، فإن المجني عليه يشعر وكأن المواد سيتم نشرها في أي وقت [63].

كما أن هذا النوع من الابتزاز هو محاولة للحصول على مكاسب مادية أو معنوية عن طريق الإكراه المعنوي للضحية، وذلك بالتهديد بكشف أسرار أو معلومات خاصة، والابتزاز بهذه الصورة يمتد ليشمل جميع القطاعات فنجد ما يسمى بالابتزاز السياسي والابتزاز العاطفي والابتزاز الإلكتروني، والابتزاز الإلكتروني هو الابتزاز الذي يتم باستخدام الإمكانيات التكنولوجية الحديثة ضد ضحايا أغلبهم من النساء لابتزازهم ماديًا أو جنسيًا. وفي المجتمع المصري مثلًا نجد أن الضحية تنصاع في أغلب الأحوال لطلبات المُبتز خوفًا من الفضيحة، وخاصة أنّ المحاكمات تكون علنية وأنّ الأحكام يسْهل نقضها وبالتالي نجاة الجاني من العقوبة، وذلك لقيام القاضي بالقياس على مواد أخرى في القانون حتى يجد عقوبة مناسبة للجاني، وهو الأمر الذي يمنعه القانون "حيث إنه لا جريمة و لا عقوبة إلا بنص"[64].

ثالثاً: أنواع جريمة الابتزاز طبقًا للدافع المرجو منه

1- دافع مادي

يعد الدافع المادي من أهم وأكثر الدوافع التي تحرك الجاني لاقتراف الجريمة الإلكترونية "الابتزاز"، خاصة أن الربح الكبير والذي يمكن تحقيقه من خلالها يدفع بالمجرم المعلوماتي إلى تطوير نفسه حتى يواكب كل حديث يطرأ على التقنية المعلوماتية[65]، ويقتنص الفرص ويسعى إلى الاحتراف حتى يحقق أعلى المكاسب وبأقل جهد دون أن يترك أثرًا وراءه، فكثير من حالات الغش المعلن عنها تكون بدافع

([63]) عمار محمد، 9 طرق للتعامل مع الابتزاز الإلكتروني، موقع صحيفة الشرق، 2017/8/10، للتفاصيل: https://www.al-sharq.com/opinion/10/08/2017/9

([64]) محمود رجب فتح الله، جريمة الابتزاز في القانون المصري، موقع الحوار المتمدن، 2018/10/19، للتفاصيل: http://www.m.ahewar.org/s.asp?aid=615334&r=0

([65]) جعفر حسن الطائي، جرائم تكنولوجيا المعلومات وآليات الحد منها، بحث منشور في الأمانة العامة للمكتبة المركزية، جامعة ديالي، العراق،2015/11/4: ص420.

الاختلاس، فالرغبة في الثراء والربح المادي عادة ما تواجهها صعوبات بالغة لتحقيقها بالطرق القانونية والمقبولة اجتماعيًا، لذلك يلجأ بعض الأفراد إلى الجرائم الإلكترونية وتحديدًا جريمة الابتزاز الإلكتروني، حيث إن المجتمع أكبر، وسهولة التنفيذ ووفرة المردود وقلة الخطورة، إضافة إلى إمكانية محو الدليل، وتوفر الوسائل التقنية التي تعرقل الوصول للجاني[66].

يمكن القول إن الهدف الأساسي للابتزاز الإلكتروني غالبًا ما يكون هدفه ماديًا بطريقة بحتة، فحتى في الحالات التي تتعلق بالابتزاز الجنسي فإن الهدف قد يكون ماديًا، وذلك بأن المبتز قد يقوم بطلب أموالًا من الضحية سواء أكان هذا الضحية رجلًا أم امرأةً أو من المؤسسات، فيعمل على مقايضة الرجل أو المرأة أو المؤسسة بدفع مبالغ مالية أو منقولات عينية مقابل عدم إفشاء أسرارهم، وقد يكون الابتزاز المادي من خلال إجبار المرأة على التنازل عن حق من حقوقها من خلال سوء معاملتها وتعمد إهانتها، لكي تطلب الطلاق مقابل التنازل عن متعلقاتها أو نفقتها أو غير ذلك، وكثيراً ما تتعرض لهذا النوع من الابتزاز كل من المطلقات أو المعلقات ومن على شاكلتهن[67].

لهذا تستند أكثر جرائم الابتزاز الإلكتروني إلى الطمع الذي يطغي على كثير من الجناة في سبيل إشباع رغباته في الحصول على المال، حيث يضع العديد من الخبراء والمختصين أن أكثر من 43% من حالات الغش والابتزاز المعلن عنها قد بوشرت من أجل الحصول على المال، ووفقًا لهذه الدراسات فإن القطاع المالي يعد أكثر عرضة من غيره من القطاعات للاستهداف من قبل جرائم الحاسب الآلي[68].

وبالتالي ترجع كثير من جرائم الابتزاز الإلكتروني إلى الرغبة في تحقيق أرباح ومكاسب مادية كاستخدام شبكة الإنترنت للإعلان عن صفقات تجارية غير مشروعة كصفقات المخدرات والاتجار بالبشر وقد ورد في بحث أعده هشام بشير المستشار الإعلامي للجمعية المصرية لمكافحة جرائم الإنترنت أنَّ عصابات الإجرام المنظم* استغلت التكنولوجيا الحديثة في تيسير شؤون الاتجار في البشر

([66]) ياسمينة بونعارة، الجريمة الإلكترونية، جامعة الأمير عبد القادر للعلوم الإسلامية، الجزائر، د.ت: ص11.

([67])آل النمر، مرجع سابق: ص48.

([68]) سميرة معاشي، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني، الجزائر، العدد السابع، د.ت: ص283.

* هي مجموعة منظمة من ثلاثة أشخاص أو أكثر، تقوم لفترة من الزمن، ويعمل أفرادها باتفاق بهدف ارتكاب أي جريمة أو أكثر، من أجل الحصول على منافع مالية أو مادية أياً كان نوعها، سواء بصورة مباشرة أو غير مباشرة. لمزيد من التفاصيل انظر:

المادة 1 من الفصل الأول من قرار بقانون رقم 20 لسنة 2015 بشأن مكافحة عسيل الأموال وتمويل الإرهاب.

حيث إن الاتجار بالبشر عبر الإنترنت هو تجارة إلكترونية حيث إن تعريف التجارة الإلكترونية هي تلك التعاملات التي تتم إلكترونياً عبر شبكة المعلومات العالمية "الإنترنت"[69].

لقد اهتم المشرّع الفلسطيني بإبراز عقوبة جرائم الابتزاز والسرقة بدافع مادي، حيث وضّح ذلك في المادة 4/12 من قانون الجرائم الإلكترونية رقم 16 لعام 2017م بأنه: "كل من استخدم الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في الحصول على أموال أو بيانات أو ما تتيحه من خدمات، يعاقب بالحبس لمدة لا تقل عن سنة أو بغرامة لا تقل عن ألف دينار ولا تزيد عن خمسة آلاف دينار أردني أو بالعقوبتين كليهما"[70]. كما نصت المادة 13 والمادة 14 من نفس القانون على عقوبة بحق من يقوم بسرقة أو ابتزاز أشخاص على الشبكة الإلكترونية بدافع مادي، سواء أكانت العقوبة بالحبس لمدة لا تقل عن سنة أو غرامة لا تقل ألي دينار ولا تزيد عن خمسة آلاف دينار، أو بكلا العقوبتين[71].

هناك ارتباط وثيق بين جريمة الابتزاز بدافع مادي وبين جريمة الاختطاف، حيث تتضح تلك الصورة من خلال قيام الجناة بخطف شخص سواء أكان طفلًا أم امرأة أو رجلًا، وذلك للحصول على فدية مالية من والده أو من يهمه أمره مقابل إطلاق سراحه، أو في صورة احتجاز الرهائن بعد جريمة الاختطاف بهدف ابتزاز السلطات العامة أو التأثير عليها في أداء عملها [72].
عادة ما تكون هذه الفئة معدومة الضمير، وهم على استعداد لارتكاب أي نوع من الجرائم، طالما أنها تجلب لهم المال، وهم عادة ما يكونوا أذكياء جدًا ومنظمين ويعرفون كيفية الهروب من وكالات إنفاذ القانون، وهؤلاء الجناة يرتكبون الجرائم الخطيرة في سبيل الحصول على الأموال، وهو ما يشكل تهديدًا كبيرًا للمجتمع [73].
من خلال ما سبق يمكن القول إن الدافع المادي يعتبر أهم وأقوى الدوافع التي تقف خلف جرائم الابتزاز الإلكتروني، حيث يعمل الجناة على تحقيق ربح مادي كبير، من خلال قيامهم بعمليات

([69]) الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مسابقة جائزة الأمير نايف بن عبدالعزيز للبحوث الأمنية لعام 2015م، مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة، سلطنة عمان، 2016: ص29.

([70]) المادة 4/12 من قانون الجرائم الإلكترونية الفلسطيني رقم 16 لعام 2017.

([71]) أنظر المادة 13 والمادة 14 من قانون الجرائم الإلكترونية الفلسطيني رقم 16 لعام 2017.

([72]) علي أحمد القاعدي، مرجع سابق: ص299.

([73]) ذياب موسى البداينة، الجرائم الإلكترونية: المفهوم والأسباب، ورقة مقدمة للمؤتمر العلمي بعنوان: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، وذلك خلال الفترة من 7-1435/11/9هـ الموافق 2-2014/9/4م، كلية العلوم الاستراتيجية، عمان، الأردن، 2014: ص21.

الابتزاز عبر الحاسوب، حيث إن تأثير المال على النفوس من شأنه أن يجعل هؤلاء الجناة يقومون بالعديد من الجرائم الإلكترونية في سبيل الحصول على أكبر كمٍّ من الأموال.

2- دافع جنسي

وتشمل هذه الجرائم جرائم جنسية وممارسات غير أخلاقية والمواقع والقوائم البريدية الإباحية، ثم يندرج تحت هذا البند جرائم ارتياد المواقع الإباحية، والشراء منها أو الاشتراك بها أو إنشائها، والتي تشكِّل بدورها قضية عالمية، أما القوائم البريدية فتختص بتبادل الصور والأفلام الجنسية على العناوين البريدية مجانًا، وتكون بعيدة عن المتابعة الأمنية، أما المواقع الإباحية فيكون الهدف منها الربح المادي، ويستوجب على متصفحها دفع المال مقابل الاستفادة من خدمات هذه المواقع، ويتطلب كلاهما الاتصال المباشر بشبكة الإنترنت، وتتيح هذه الشبكة أفضل الوسائل لتوزيع الصور الفاضحة والأفلام الخالعة بشكل علني فاضح يقتحم على الجميع بيتهم وخصوصياتهم، وكل مستخدم للإنترنت معرض للتأثر بما يتم عرضه على الإنترنت والذي لا يعترف بأي حدود مما يشكل خطرًا حقيقيًا للابتزاز غير شبكة الإنترنت، كما يوجد على شبكة الإنترنت آلاف المواقع الإباحية التي تروج لمثل هذه الأفعال[74].

أما القانون الأساسي الفلسطيني فقد اهتم بإظهار التعويض اللازم لكل من وقع عليه ضرر التدخل في حياته الخاصة، أو يقوم بابتزاز مستخدمي الشبكات الإلكترونية بدوافع جنسية أو غير ذلك، حيث نص القانون الفلسطيني في مادته رقم 32 على أنَّ: "كل اعتداء على أي من الحريات الشخصية أو حرمة الحياة الخاصة للإنسان وغيرها من الحقوق والحريات العامة التي يكفلها القانون الأساسي أو القانون، جريمة لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم، وتضمن السلطة الوطنية تعويضًا عادلًا لمن وقع عليه الضرر"[75].

حيث يقوم بعض الجناة بارتكاب الجريمة عبر شبكة المعلومات العالمية وتقنية المعلومات بصورة عامة يتركز الدافع من ورائها غالبًا في صورة ابتزاز أو تهديد أو تشهير بدافع جنسي، سواء بأن يقوم بسرقة صور للفتيات لإشباع غرائزه، أو مقايضة هؤلاء الفتيات مقابل الحصول منهن على أموال مقابل عدم نشرها، وهذا ما أكدته أيضاً المادة 22 من القرار بقانون رقم 10 لسنة 2018، والمنشور في العدد الممتاز رقم (16) من الوقائع الفلسطينية بتاريخ 2018/05/03، إذ نصت على: "1- يحظر

([74]) علي جبار الحسيناوي، جرائم الحاسوب والإنترنت، دار اليازوري العلمية للنشر والتوزيع، عمان، 2009: ص77.

([75]) المادة رقم 32 من القانون الأساسي الفلسطيني المعدل لعام 2005.

التدخل التعسفي أو غير القانوني في خصوصيات أي شخص أو في شؤون أسرته أو بيته أو مراسلاته. 2- كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات بقصد نشر أخبار أو صور أو تسجيلات صوتية أو مرئية، سواء كانت مباشرة أو مسجلة، تتصل بالتدخل غير القانوني في الحياة الخاصة أو العائلية للأفراد، ولو كانت صحيحة، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين"[76]، حيث يعد مثل هذا العمل من قبيل الاعتداء على الحق في الخصوصية للأفراد، وقد يقوم الجاني بالسطو على البريد الإلكتروني لفتيات، والاستيلاء غير المشروع على صورهن الشخصية وتعمد نشرها على موقع خاص بشبكة الإنترنت مع مجموعة الصور الإباحية، وكما يمكن أن تكون هذه الجرائم غير مباشرة وتتمثل في الحصول على البيانات والمعلومات الخاصة بتلك الجهات أو الأشخاص لاستخدامها فيما بعد في ارتكاب جرائم مباشرة[77].

أيضًا هناك جريمة ابتزاز جنسي مرتبطة بدعارة الأطفال، وتوفير محتويات جنسية متعلقة بالأطفال، وذلك من خلال الاتصال الجنسي بالأطفال عن طريق قيام الطفل القاصر بتصرفات جنسية وعرضها على مواقع، أو ظهور أي شخص باتصال أو بتصرفات جنسية مع طفل قاصر، أيضًا الصور الواقعية التي تمثل أو تُظهر قاصرًا يقوم بتصرف جنسي، وقد تم تعريف القاصر عند كثير من الدول بالطفل الذي لم يبلغ سن الثامنة عشرة [78]. كذلك الحدث تم تحديد سنه في العديد من الدول خاصة القانون الفلسطيني بأنه الطفل الذي لم يتجاوز سنه الثامنة عشرة سنة ميلادية وقت وقوع الجريمة[79].

هناك فئات عديدة ومتزايدة تستخدم مواقع انترنت تبث مواد إعلانية بذيئة بوساطة الشبكة، فهذه الصناعة تعد من أكثر الصناعات عبر الإنترنت انتشارًا، أما المواقع الإباحية فلا تعد ولا تحصى، أما الفئة الأكثر استخداماً لهذه المضامين هي الأطفال، فالقصر والأطفال يعدون من أكثر الشرائح استخدامًا لهذه المواقع، فدخولهم لها يتم إما مصادفة أو رغمًا عنهم، أو بإيعاز من أقرانهم على سبيل الفضول، فالقصر يستخدمون الإنترنت بمعدل 12%، ومنهم يمضي أكثر من ثلاث ساعات على الإنترنت، و87% منهم وقعوا في محتويات سيئة خلال تنقلهم عبر الإنترنت، فالصور والأفلام

([76]) المادة رقم 22 من قانون الجرائم الالكترونية رقم 10 المعدل لسنة 2018.

([77]) القاعدي، مرجع سابق: ص29.

([78]) وليد طه، التنظيم التشريعي للجرائم الإلكترونية في اتفاقية بودابست، وزارة العدل، مصر، د.ت: ص24.

[79] المادة رقم 1 من الفصل الأول من قرار بقانون رقم 4 لسنة 2016 بشأن حماية الأحداث.

الإباحية التي تتضمن أطفالًا هي شكل خاص وخطير من الاستغلال الجنسي للأطفال والذي يتخذ مدى عالمي مع تطور استعمال الشبكات الرقمية[80].

لهذا تبدأ جريمة الابتزاز بدافع جنسي عند قيام عملية تبادل الصور الشخصية والمحادثات لمن تكون معه علاقة غير شرعية، سواء أكان ذلك عن طريق اتصال هاتفي أم في غرف المحادثات في الشبكة العنكبوتية، أم عن طريق برامج المراسلة الفورية "الماسنجر"، أو برامج المحادثة في الهواتف النقالة[81]، وهذا السبب تساهم فيه المرأة بشكل كبير من خلال تساهلها في إقامة العلاقات، ومنح الطرف الآخر فرصة لابتزازها بمنحه صورها، أو السماح له بلقائها، مما يسهل عملية التصوير والتسجيل المرئي والصوتي، ما ينتج عنه قيامه بابتزازها للحصول على أموال من ناحية أو لإشباع رغباته الجنسية من ناحية أخرى، وقد يتطور الأمر لابتزاز الشاب للفتاة ويهددها لأجل أن تمكنه من ممارسة الفاحشة، أو مقدماتها[82].

كما تشمل الجرائم الجنسية جرائم ارتياد المواقع الإباحية للشراء منها أو الاشتراك فيها، أو للانضمام للقوائم الإباحية لتبادل الأفلام والصور منها، وكل ما يندرج تحت أعمال الدعارة أو الاستغلال الجنسي للأطفال من ناحية أو الابتزاز الجنسي للنساء أو الأطفال على حد سواء من ناحية أخرى [83].

ومثال ذلك مثلاً لو قام شخص برفع شكوى ضد آخر اتهمه فيها بتهديده من خلال حساب على موقع الفيس بوك بنشر صور خاصة لزوجته، إذا لم يدفع له مبلغاً من المال وهو ما كان مقداره أربعة آلاف دينار أردني، ونتيجة إلى ذلك وبتتبع هذا الموضوع تبين أن صاحب هذا الحساب هو شخص صاحب محل صيانة أجهزة حاسوب، حث كان قد قام المشتكي بإجراء صيانة لجهاز الحاسوب لهذا الشخص الذي قام باسترجاع ونسخ جميع البيانات والصور العائدة له، وقام بابتزازه وأثناء التحقيق معه اعترف بجريمته، ومن ثم قدم للقضاء.

أما المشرع المصري فقد نص في المادة 25 من قانون جرائم تقنية المعلومات رقم 175 لسنة 2018 والمنشور في الجريدة الرسمية العدد 32 مكرر (ج) بتاريخ 14 / 8 / 2018م على أن: "يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه،

([80]) مريم، أحمد مسعود، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون 04/09، رسالة ماجستير غير منشورة، جامعة قاصدي مرباح- ورقلة، الجزائر2013: ص28.

([81]) عبد العزيز جايز الفقيري، الابتزاز الداء والدواء، شبكة الألوكة، د.ت: ص4-5.

([82])المطلق، مرجع سابق: ص10-11-12.

([83])الحسيناوي، مرجع سابق: ص104.

أو بإحدى هاتين العقوبتين، كل من اعتدى على أي من المبادئ أو القيم الاسرية في المجتمع المصري، أو انتهك حرمة الحياه الخاصة أو ارسل بكثافة العديد من الرسائل الاليكترونية لشخص معين دون موافقته، أو منح بيانات إلى نظام أو موقع الكتروني لترويج السلع أو الخدمات دون موافقته أو بالقيام بالنشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، لمعلومات أو اخبار أو صور وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة ام غير صحيحة"[84]، وقد حرص المشرع المصري على المحافظة على كيان الأسرة وعلى المبادئ والأخلاق المتعارف عليها والسائدة بوجه عام في المجتمع، حيث تقوم الأسرة على مجموعة من المبادئ والقيم التي ينبغي احترامها وعد الخروج عليها أو مخالفتها.

أما في قطاع غزة فقد قامت الحكومة الفلسطينية بحجب جميع المواقع الإباحية، حيث أصدر وزير الاتصالات وتكنولوجيا المعلومات قرارًا وزاريًّا رقم 2012/33 والذي تضمن فيه الأمر بحجب كافة المواقع الإلكترونية المخلة بالآداب، مع إلزام مزودي الإنترنت بتطبيق مواد هذا القرار، الأمر الذي يعمل على حماية المجتمع ومستخدمي الإنترنت من الدخول إلى مثل هذه المواقع المشبوهة [85].

يتضح للباحثة مما سبق أن الجرائم الجنسية التي تمس بالأشخاص بصورة مباشرة من أخطر الجرائم الإلكترونية، وهي من أكثر الجرائم التي تنتشر على الإنترنت، فالبيئة التي تنشأ بها تساعد على انتشارها بصورة كبيرة، خاصة بسبب بعد الجاني عن الضحية من ناحية، وسرعة تنفيذ هذه الجريمة من ناحية أخرى، ومن ناحية ثانية يفضِّل الجناة ارتكاب هذه الجريمة عبر الإنترنت بسبب صعوبة اكتشاف أمرهم، وبعدهم عن أيدي العدالة، خاصة جريمة الابتزاز الجنسي بنشر الصور الجنسية أو تصوير الفتيات وابتزازهن وغير ذلك.

([84]) المادة 25 من قانون جرائم تقنية المعلومات المصري رقم 175 لسنة 2018م.

([85]) العفيفي، مرجع سابق: ص27.

رابعاً: أنواع جريمة الابتزاز الإلكتروني تبعاً للهدف المرجو منه

1- الابتزاز السياسي

يعتبر الابتزاز السياسي أخطر أنواع الابتزاز، والذي يتأتى بالضغط المباشر والغير مباشر الذي يمارسه الأشخاص أو المؤسسات السياسية في موقع ما، ضد مسؤولين أو أشخاص أو كيانات أخرى، بهدف الحصول على امتيازات سياسية معينة[86].

يقوم الابتزاز كونه سلوكاً على التهديد بكشف معلومات معينة عن شخص ما، أو فعل شيء للإضرار أو تشويه سمعة الشخص المهدد، وذلك إذا رفض الاستجابة إلى بعض الطلبات، حيث يمكن أن تكون هذه المعلومات في العادة محرجة أو ذات طبيعة مدمرة اجتماعياً. كما أن للابتزاز عدة أنواع وأشكال، حيث تتنوع هذه الأشكال في مدى حدتها ودرجتها، فعلى الصعيد السياسي، يمكن الحديث عن دولاً قوية تبتز دولاً أخرى أقل نفوذاً سواء اقتصادياً أو عسكرياً لتحظى بمكتسبات معينة أو لتحقيق مصالحها وأطماعها سواء المحلية أو الإقليمية أو الدولية، أو حتى لفرض أيدولوجيتها على غيرها من الدول، كما كشف التاريخ عن حالات ابتزاز لسياسيين وأصحاب نفوذ عالمياً من خلال انتهاك حياتهم الشخصية لإجبارهم على اتخاذ قرارات وإجراءات تصب في مصلحة الجهة المبتزة لهم[87].

إن من أخطر أنواع الابتزاز السياسي ذلك الذي يقع ضد أحد المسئولين السياسيين بهدف ابتزازه، كما حصل مع وزير الشؤون الداخلية في جنوب أفريقيا، "مالوسي جيجابا"، الذي تم تسريب لقطات جنسية خاصة له بعد اختراق هاتفه، وإنه تعرض للابتزاز لهذا السبب عندما كان يتولى منصب وزير المالية[88].

كما كشفت تسيبي ليفني، وزيرة الخارجية الإسرائيلية السابقة، والتي كانت تعمل في جهاز المخابرات "الموساد" أنها مارست الجنس "من أجل إسرائيل" وانها مستعدة لتكرار ذلك لو اقتضت الضرورة، كما

([86]) ناجي الغزي، الابتزاز السياسي.. واللعب بالورقة الطائفية، مجلة الحوار المتمدن، العدد 2911، 2010/2/8.

([87]) محمد حازم أبو رمضان، "الابتزاز" وباء متفشٍّ في العالم المعاصر، موقع الجزيرة نت، 2018/2/23، للتفاصيل:

https://blogs.aljazeera.net/blogs/2018/2/23

([88]) خاص موقع الخبر الأول، ابتزاز وزير في جنوب أفريقيا بفيديو جنسي، 2018/10/28، للتفاصيل:
https://read07.com/193872.html

أكدت في مقابلة نشرتها مجلة التايمز عن تفاصيل فترة عملها في جهاز "الموساد" الإسرائيلي وطبيعة المهام منها ممارسة الجنس بهدف الحصول على معلومات، والإيقاع بعلماء وشخصيات سياسية عربية وعالمية. حيث تفاخرت "ليفني" بأعمالها التي هدفت للقيام بعمليات خاصة كإسقاط شخصيات هامة عن طريق إيقاعهم في عمليات جنسية ومن ثم ابتزازهم لتقديم تنازلات سياسية تصب لصالح الموساد". ومارست "ليفني" أنشطتها في العديد من الدول الأوروبية للإيقاع بشخصيات سياسية وعلماء في العالم وبعض الدول العربية[89].

لقد اهتمت العديد من التشريعات بموضوع التهديد السياسي، حيث فرضت عقوبات مشددة على من يقوم بابتزاز من هذا النوع، فقد نصت المادة (9) من قانون الجرائم المصري: " يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن 50 ألف جنيه ولا تجاوز 200 ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمداً أو بخطأ غير عمدى وبقى بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعاً أو بريداً إلكترونياً أو حساباً خاصاً أو نظاماً معلوماتياً يدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوك لها أو يخصها. فإذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية تكون العقوبة السجن والغرامة التي لا تقل عن 100 ألف جنيه ولا تجاوز 500 ألف جنيه[90].

أما القانون الفلسطيني فقد اهتم بفرض عقوبة على من ابتز شخصاً سواء عادياً أو شخصية اعتبارية بصور أو ذم أو قدح لهدف معين فإنه يعاقب سواء بعقوبة مادية أو بالسجن، حيث نصت المادة (15) من قانون الجرائم الالكترونية رقم (10) المعدل لسنة 2018 والمنشور في العدد الممتاز رقم (16) من الوقائع الفلسطينية بتاريخ 2018/05/03، على أنه: "1- كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في تهديد شخص آخر أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان هذا الفعل أو الامتناع مشروعاً، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 2- إذا كان التهديد بارتكاب جناية أو بإسناد أمور خادشة للشرف أو الاعتبار، يعاقب

([89]) صحيفة النهار الإماراتية، تسيبي ليفني : مارست الجنس من أجل الابتزاز والقتل، 05 نوفمبر 2012.

([90]) المادة 20 من قانون مكافحة جرائم الإنترنت المصري رقم 175 لعام 2018م.

بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً[91].

يتبين مما سبق بأن العديد من القوانين كفلت حماية الحياة الخاصة للمواطنين داخل الدولة، وذلك من خلال إصدار العديد من التشريعات والقوانين التي تعاقب كل من يتعدى على هذه الحياة من خلال الابتزاز ونشر الصور أو الفضائح أو تشويه السمعة، لكنها في الوقت نفسه عملت الحكومات على تغليظ العقوبة لكل من يقوم بالتعدي على الحياة الخاصة للشخصيات الاعتبارية أو المسئولين، وهو ما عملت به العديد من القوانين ومنها القوانين الفلسطينية والمصرية والأردنية.

2- الابتزاز الاقتصادي

تتنوع أشكال الابتزاز الاقتصادي بين جماعات ضغط لا تتردد في أن تتخذ أي وسيلة في سبيل تحقيق أهدافها وفرض سياساتها أو سياسات الدول الداعمة والممولة لها على كيانات أو دول أخرى، كما لا يقتصر الابتزاز الاقتصادي على ذلك فقط؛ بل قد يتجسد الابتزاز الاقتصادي في الحياة المهنية للأفراد والعاملين في مختلف القطاعات، فعندما نرى مؤسسات وشركات وإدارات تستغل حاجة العاملين فيها لكسب قوت يومهم، بغرض إجبارهم على اتخاذ سلوكيات مشبوهة، أو التنازل عن حقوقهم، أو تعطيل وتقييد تطورهم الوظيفي، أو فرض سياسة الأمر الواقع، أو الخضوع لإجراءات عمل سلبية، أو حتى انتهاك حقوقهم العمالية التي تكفلها لهم القوانين والتشريعات الاقتصادية والدولية والإنسانية، فهذا هو إحدى أبشع صور الابتزاز[92].

وقد عاقب المشّرع الأردني كل من دخل للمواقع الالكترونية بقصد الاطلاع على بيانات يمكنها المساس بالاقتصاد الوطني بالحبس والغرامة أو بكلتا العقوبتين في آن واحد، حيث نصت الفقرة (ج) من المادة 12 من قانون الجرائم الالكترونية رقم 27 لسنة 2015 الأردني والمنشور على الصفحة 5631 من عدد الجريدة الرسمية رقم 5343 بتاريخ 2015/6/1. بأنه: "يعاقب كل من دخل قصداً إلى موقع الكتروني للاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو

([91]) المادة (15) من قانون الجرائم الالكترونية رقم (10) المعدل لسنة 2018

([92]) أبو رمضان، مرجع سابق.

العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس لمدة لا تقل عن أربعة أشهر وغرامة لا تقل عن 500 دينار"[93].

أما المشرّع الفلسطيني فقد قام بتوقيع عقوبة لكل من استخدم شبكة المعلومات في أي وسيلة تنتهي بالابتزاز أو الاستيلاء على اموال دون وجه حق، بمعاقبته سواء بعقوبة مادية أو بالسجن، حيث نصت المادة (14) من قانون الجرائم الالكترونية رقم (10) المعدل لسنة 2018 والمنشور في العدد الممتاز رقم (16) من الوقائع الفلسطينية بتاريخ 2018/05/03، على أنه: "كل من استولى عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات لنفسه أو لغيره على مال منقول أو على سند أو توقيع إلكتروني أو بيانات إنشاء توقيع إلكتروني أو منظومة إنشاء توقيع إلكتروني، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين[94].

كما يمكن أن يكون الابتزاز الاقتصادي من دولة قوية لدولة أقل قوة منها، وذلك لتمرير مخططات لديها، فمثلاً لم تتوقف محاولات أمريكا عند دعم إسرائيل في صراعها مع الفلسطينيين، حيث تحاول ممارسة الابتزاز الاقتصادي من خلال تجميد أو تقليص المساعدات المالية المقدمة للسلطة الفلسطينية التي تعاني من أزمات وعجز في الميزانية العامة لها. وقد أعلنت وزارة الخارجية الأميركية أكثر من مرة، أن الإدارة الأمريكية قرّرت إلغاء إرسال ملايين الدولارات من المساعدات المخصّصة للفلسطينيين في الضفة الغربية وقطاع غزة، وأن هذه الأموال ستذهب الآن إلى مشاريع ذات أولوية كبرى في أماكن أخرى"، حيث أن تقليص المساعدات المقدم للسلطة هي ضغوطات اقتصادية جديدة لانتزاع مواقف سياسية[95].

([93]) الفقرة (ج) من المادة 12 من قانون الجرائم الالكترونية رقم 27 لسنة 2015

([94]) المادة (14) من قانون الجرائم الالكترونية رقم (10) المعدل لسنة 2018

([95]) فلسطين عبد الكريم، وقف المساعدات الأمريكية .. ابتزاز سياسي وضغوطات اقتصادية، وكالة الرأي الفلسطينية للإعلام، 2018/8/25، للتفاصيل:

http://alray.ps/ar/post/184063

يتبين ما سبق بأن الابتزاز الاقتصادي تتعدد مآربه وتتفرع أنواعه، حيث أن هذه الابتزاز عادة ما يتخطى الأفراد ليشمل الدول فيما بينها، خاصة الدول الغنية والفقيرة، أما الأفراد فقد كفلت القوانين المحلية والدولية لهم عدم المساس بهم وتعريض حياتهم المالية أو الاقتصادية للخطر من خلال ابتزازهم، وهو ما جعل هذه الدول تفرض عقوبات رادعة على من ينتهك تلك الحالة، أما الدول فيما بينها فقد انتشرت بشكل واسع خاصة أن الابتزاز الاقتصاد قد ارتبط بصورة كبيرة بالابتزاز السياسي، وهو ما نلمسه من خلال قيام الدول المانحة بابتزاز الدول الضعيفة كفلسطين أو غيرها بوقف مساعدتها لها إذا امتنعت عن تمرير قرارات سياسية تفرضها عليها هذه الدول.

3- الابتزاز الوظيفي

يعتبر الابتزاز الوظيفي أحد أوجه استغلال النفوذ في الوظيفة على نحو غير مشروع، حيث اعتبرت بعض الدول الاستغلال او الابتزاز الوظيفي نوع من الرشوة، واعتبره البعض الآخر مستقلاً عن الرشوة، والبعض اعتبره جنحة، والبعض الآخر اعتبروه جناية، كما أن الابتزاز الوظيفي تعاني منه الدول النامية بصورة أشد، وقد أصدرت الأمم المتحدة اتفاقية مكافحة الفساد، حيث تحدثت المادة 19 منها عن استغلال الوظائف حيث نصت على أنه: "تنظر كل دولة طرف في اعتماد ما قد يلزم من تدابير تشريعية وتدابير أخرى لكي تجرّم تعمد موظف عمومي إساءة استغلال وظائفه أو موقعه، أي قيامه أو عدم قيامه بفعل ما، لدى الاضطلاع بوظائفه، بغرض الحصول على مزية غير مستحقة لصالحه هو أو لصالح شخص آخر أو كيان آخر، مما يشكل انتهاكاً للقوانين"[96].

يظهر الابتزاز واستغلال النفوذ الوظيفي عندما يرغب الشخص في الوصول إلى موقع ما، وهو يعلم أنه ليس من حقه، فيلجأ لأساليب لا تخضع للنظام لتحقيق ما يريد، فيسعى لتشويه الآخرين او ابتزازهم بطرق عديدة بغرض إقصائهم، ويضطر أيضاً للرشوة والمجاملة، كما يمكنه أن يسعى لتحقيق مكاسب مادية يعتقد أنها من حقه، بعكس ما يمليه عليه النظام، فتغيب القيم والمعايير الأخلاقية، وتتلاشى النظم والقوانين التي يتضح فيها مبدأ الثواب والعقاب، وغياب الثقة بالذات والمجتمع[97].

([96]) المادة 19 من اتفاقية الأمم المتحدة لمكافحة الفساد رقم 4/58 لسنة 2003.

([97]) سمير محمد سعيد أبو شمس، استغلال النفوذ الوظيفي في ظل التشريعات الفلسطينية وأثره على التنمية السياسية، رسالة ماجستير غير منشورة، جامعة النجاح الوطنية، نابلس، 2011: ص13-14.

وقد قامت العديد من السلطات والتشريعات بمحاولة الحد من هذه الجريمة، وهي استغلال النفوذ عن طريق الابتزاز الوظيفي أو غيره من الجرائم، حيث نصت المادة 19 من قانون الكسب غير المشروع رقم 1 لسنة 2005 في بندها الأول على: "كل موظف عام علم بكسب غير مشروع أن يبلغ الهيئة بذلك". حيث يعني ذلك أن إعطاء المعلومات السليمة عن مستغلي نفوذهم أو عن طريق الرشاوي أو الابتزاز الوظيفي يمكن أن يتم الحد منهم عن طريق هذه المعلومات التي وجب أن تكون إجبارية، وأن يعاقب كل من يتستر عليهم[98].

من جانب آخر قد يواجه الموظف، سواء العامل في قطاع خاص او حكومي بعض العقبات التي يمكن أن تعترض طريقه، ولكن يظل اصعبها ذلك الذي تواجهه الموظفة من تحرش بغرض التقرب الجنسي او العاطفي من مسؤولها. حيث أن هذه الأفعال انتشرت وتكررت مع عشرات الموظفات وفي بلدان عديدة جلّها من الدول النامية والعربية بشكل خاص، حيث أن عدم الإفصاح عنها يكمن في الخوف من نتيجة ذلك، خاصة مع تعرضها لشيء من الابتزاز، وهو ما يمكن أن يطلق عليه "الابتزاز الوظيفي" الذي يهدد به المدير بأنها لن تحصل على التقدير الذي تستحقه إن فكرت برفضه او حتى بالتحدث عن أي من تلك التحرشات[99].

يمكن القول بأنه تتعدد أنواع وأشكال الابتزاز الوظيفي من خلال استغلال النفوذ والقيام بابتزاز شخص بطريقة غير قانونية لحمله على الرضوخ لمطالب الجاني، حيث يمكنها أن تطال الأفراد ذوي الوظائف العامة في الدولة، كما يمكنها أن تمس الموظفين في الشركات والوظائف الخاصة، ولكن أخطرها هو ابتزاز النساء من خلال حملهنّ على الرضوخ لمطالب الجاني كي لا يتم التعرض لهم من خلال الفصل الوظيفي أو الضرر في وظيفتها، وهذا النوع ينتشر بصورة واضحة في الدول، والتي حاولت جاهدة الحد منه عن طريق إصدار تشريعات وقوانين لمعاقبة مستغلي مناصبهم لتحقيق هذه المآرب غير القانونية.

([98]) المرجع السابق: ص34.

([99]) خاص موقع القبس الالكتروني، الابتزاز الوظيفي، 7 أبريل 2006، للتفاصيل:

/https://alqabas.com/178755

الفرع الثاني: خصائص جريمة الابتزاز الإلكتروني

تختلف جريمة الابتزاز الإلكتروني عن الجريمة التقليدية من عدة اتجاهات، فجريمة الابتزاز الإلكتروني لم تظهر وتنتشر إلا في عصر الحاسب الآلي والإنترنت، وكون هذا النوع من الجرائم يعتبر حديثًا ومتطورًا فإن له خصائص تميزه عن غيره من الجرائم التقليدية، وهذه الخصائص يمكننا أن نستخرجها من خلال التعريفات التي قام الباحث بسردها في بداية البحث.
نظراً لارتباط جريمة الابتزاز الإلكتروني بجهاز الحاسوب، وشبكة الإنترنت بصفة عامة، ووسائل التواصل الاجتماعي بصفة خاصة، فقد أضفى ذلك عليها مجموعة من الخصائص المميزة لها عن خصائص الجريمة العادية التقليدية، ومن خصائص جريمة الابتزاز الإلكتروني ما يلي:

أولاً: جريمة عابرة للحدود (عالمية الجريمة): حيث يطلق على هذا النوع من الجرائم أيضًا "جرائم غير وطنية"، وهي التي تقع بين أكثر من دولة، بمعنى أنها لا تعترف بالحدود الجغرافية للدول كجرائم تبييض الأموال، والمخدرات، والإتجار بالبشر وغيرها. أما في عصر الحاسب الآلي، ومع انتشار شبكة الاتصالات العالمية، أمكن ربط أعداد هائلة من الحواسيب عبر العالم بهذه الشبكة بحيث يغدو أمر التنقل والاتصال فيما بينهم أمرًا سهلًا طالما تم تحديد عنوان المرسل إليه، أو أمكن معرفة كلمة السر، سواء تم ذلك بطريقة مشروعةً أو غير مشروعة، وفي هذه البيئة يمكن وصف جريمة الابتزاز الإلكتروني بأنها جرائم عابرة للدول، إذ كثيرًا ما يكون الجاني في بلد والمجني عليه في بلد آخر، وعليه فإن هذه الجرائم تعتبر عابرة للحدود الوطنية أو الإقليمية أو القارية، وبالتالي تظهر الحاجة للتعاون الدولي في مجال مكافحة هذه الجرائم، حيث إن جهود الإنتربول الدولي في مكافحة هذه الجريمة يمكن أن تشكل نقطة انطلاق للحد من هذه الجرائم[100].

تعتبر جريمة نقص المناعة المكتسبة "الإيدز"، والتي حدثت عام 1989م مثالًا على ذلك، حيث تتلخص وقائع هذه الجريمة في قيام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج التي تهدف ظاهرياً للوقاية من مرض الإيدز، لكنها في الحقيقة عبارة عن برنامج يحتوي فايروس خطير يترتب على تشغيله تعطيل لنظام الحاسوب بأكمله، ثم تظهر على الشاشة عبارة يطلب فيها الفاعل مبلغ مالي يرسل على عنوان معين مقابل حصول المتضرر على برنامج مضاد للفايروس، وقد تم إلقاء القبض على المتهم "جوزيف بوب" في أوهايو بالولايات المتحدة الأمريكية وتم تسليمه للمملكة

([100]) ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية: دراسة تأصيلية تطبيقية، رسالة ماجستير غير منشورة، إشراف دكتور جلال الدين محمد صالح، جامعة نايف العربية للعوم الأمنية، الرياض، 2012: ص23.

المتحدة بطلب منها باعتبار أن فعل الإرسال تم في إقليمها، وتم توجيه إحدى عشرة تهمة ابتزاز للمتهم في دول مختلفة[101].

أما التحقيق في هذا النوع من الجرائم فيتطلب القيام بإجراءات وأعمال للتحقيق خارج حدود البلد، مثل: تفتيش المواقع الإلكترونية أو تفتيش المواقع الإلكترونية المادية؛ وذلك للعثور على البيانات أو المعلومات، أو إلقاء القبض على المطلوبين، أو معاينة مسرح الجريمة، وكل هذه الأعمال تحتاج إلى تعاون ملموس على المستوى الدولي للحد من هذه الجرائم أو محاولة التقليل منها [102].

وقد نتج عن طبيعة جريمة الابتزاز الإلكتروني بأنها عابرة للحدود العديد من المشاكل حول تحديد الدولة ذات الاختصاص القضائي بهذه الجريمة، وكذلك حول القانون الواجب تطبيقه، إضافة إلى الإشكاليات المتعلقة بإجراءات الملاحقة القضائية وإجراءات الإثبات، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود تجعل إمكانية التحري والتنسيق أمرًا صعبًا وشاقًا ومشتتًا للجهات الأمنية والقضائية [103].

من الممكن أن تكون جريمة الابتزاز الإلكتروني جريمة داخلية أو جريمة دولية: أما الداخلية فهي عندما تقع داخل إقليم دولة معينة. وتكون دولية عندما تتعلق بالقانون الدولي، أي عندما يكون أحد أطرافها شخصًا دوليًا، على نحو ما حدث في التجسس الذي قامت به الولايات المتحدة الأمريكية عندما انتهكت أنظمة أعداءها الحاسوبية، وذلك بواسطة أسلحة معلوماتية فتاكة، أثناء القصف الجوي للحلف الأطلسي في كوسوفو. أيضًا يمكن أن تكون هذه الجريمة ذات بعد دولي، إذا اتفق المجتمع الدولي بأن جريمة معينة يمكن أن تشكل خطرًا على كل دولة، أو عندما ترتكب الجريمة داخل دولة معينة إلا أنها تمتد خارج إقليم الدولة مثل: جريمة ترويج المخدرات عبر الإنترنت [104].

يتضح مما سبق أن الجريمة الإلكترونية قد أزالت كافة الحدود الجغرافية لها، خاصة أن الشبكة العنكبوتية قد جعلت العالم كله قرية صغيرة يسهل التواصل بين الأفراد في الدول، وهو ما جعل الجريمة الإلكترونية عابرة للحدود، ومن هنا فإن أغلب الجرائم الإلكترونية ترتكب عبر الإنترنت فيكون المجرم في دولة والمجني عليه في دولة أخرى.

([101]) مريم، مرجع سابق: ص11.

([102]) العفيفي، مرجع سابق: ص16.

([103]) المطيري، مرجع سابق: ص54.

([104]) طارق الخن، جرائم المعلوماتية، الجامعة الافتراضية السورية، دمشق، 2018: ص12.

ثانياً: تتصف بالإغراء والنعومة للمجرمين/ فإذا كانت الجريمة بصورتها التقليدية تحتاج في الأغلب إلى مجهود عضلي كجرائم السرقة والاغتصاب والقتل، فإن الجريمة الإلكترونية لا تحتاج إلى أدنى مجهود عضلي، بل تحتاج إلى إعمال الذهن والعقل والتفكير المدروس القائم على معرفة جيدة بتقنيات الحاسب الآلي، ولذا كان الشرط الأساسي في المجرم توافر العلم بكيفية عمل الحاسب الآلي وآلية تشغيله، إضافة إلى الإحاطة ببعض البرامج التشغيلية[105].

أما الإغراءات التي تجذب المجرمين نحو جريمة الابتزاز الإلكتروني وغيرها من هذه الجرائم فتتمثل في أنها جرائم سريعة التنفيذ، إذ غالبًا ما يتمثل الركن المادي فيها باستخدام جهاز حاسوب، مع إمكانية تنفيذ ذلك عن بعد، دون اشتراط الوجود في مسرح الجريمة. أيضًا ضخامة الفوائد والمكاسب التي يستطيع الجاني تحقيقها باقتراف مثل هذه الجريمة دون جهد يذكر، ودون مخافة من انكشاف أمره، كما أن الجرائم الإلكترونية بصفة عامة وجريمة الابتزاز الإلكتروني بصفة خاصة يمكن اعتبارها بمثابة إغراء كبير للمجرمين، لاستغلال التكنولوجيا الحديثة، بغية اقتراف الجرائم بصورها المتعددة، خصوصًا عندما يكون الجاني موظفًا في شركة تعتمد الحاسب الآلي في عملها، إذ يكون لديه كافة المعلومات اللازمة لتحقيق اختراقات متعددة ومتتالية لأنظمة الحاسب الآلي في الشركة، مما ينتج عنه تحقيق أرباح طائلة، ومكاسب عديدة[106].

فمن الأمثلة على هذا الصنف من المجرمين Hacker croll والذي استجوب في العام 2009 بعد قرصنته حسابات Twitter خاصة حساب الرئيس باراك أوباما، وقد قبضت الشرطة على هذا الشاب بسبب النصب عبر الشبكة، والتي جنى من خلالها 15 ألف يورو، وحكم عليه خمسة أشهر حبس مع إيقاف التنفيذ[107].

وبالتالي فنظرًا للصفات التي تتمتع بها هذه الجريمة باعتبارها إحدى أهم الجرائم الإلكترونية في هذا العصر، ومن ثم ظهور الصعوبات التي تثار عند محاولة الكشف عنها أو البدء بملاحقتها محليًا ودوليًا، وما ينتج عن هذه الصعوبات من إغراءات للجناة بصعوبة الكشف عنهم وملاحقتهم، وسهولة

([105]) مصطفى سليمان أبكر، جرائم الحاسوب وأساليب مواجهتها، مجلة الأمن والحياة، العدد 210، 1420هـ: ص47.

([106]) آل ثنيان، مرجع سابق: ص22-23.

([107]) مريم، مرجع سابق: ص13.

جني أرباح مادية طائلة من وراء هذه الجريمة، ما جعل هذه الجرائم تستهوي الكثيرين لسهولتها وكثرة مكاسبها [108].

يتضح مما سبق أن الجريمة الإلكترونية بأنه مغرية للجناة، خاصة لسهولة ارتكابها دون مجهود، مع وجود الكثير من الأموال التي يمكن أن يحصل عليها الجاني من خلال القيام بجريمته، كذلك فإن هذه الجرائم سريعة التنفيذ ولا تتطلب سوى ضغط مفتاح معين لتنفيذها.

ثالثاً: صعوبة اكتشاف جريمة الابتزاز الإلكتروني وإثباتها/ حيث إن جريمة الابتزاز لا تحتاج إلى أي عنف أو سفك للدماء، أو آثار اقتحام لسرقة الأموال، وإنما هي أرقام وبيانات تتغير أو تمحى تماماً من السجلات المخزنة في الذاكرة، ولأن هذه الجرائم في الغالب لا تترك أي أثر خارجي مرئي، فإنها تكون صعبة في الإثبات، ومما يزيد من صعوبة إثبات هذه الجرائم ارتكابها عادة في الخفاء، وعدم وجود أي أثر كتابي لما يجري خلال تنفيذها من عمليات أو أفعال إجرامية، حيث يتم بالنبضات الإلكترونية نقل المعلومات، إضافة إلى إحجام الضحايا عن الإبلاغ عن هذه الجرائم تجنبًا للإساءة إلى السمعة وهز الثقة، فضلًا عن إمكانية تدمير المعلومات التي يمكن استخدامها كدليل للإثبات في مدة لا تزيد عن ثانية واحدة. إضافة إلى عدم ملائمة الأدلة التقليدية في القانون الجنائي في إثباتها، ومن ثم يلزم البحث عن أدلة جديدة ناتجة من ذات الحاسب، ومن ثم تبدأ صعوبات البحث عن الدليل وجمع هذا الدليل، وتبدأ مشكلات قبوله إن وجد، ومدى مصداقيته على إثبات وقائع الجريمة[109].
ومما جعل الجرائم الإلكترونية بصفة عامة وجريمة الابتزاز بصفة خاصة صعبة الاكتشاف والإثبات، البعد الجغرافي بين الجاني والمجني عليه، واستخدام الجاني وسائل فنية حديثة في جرمه، كما أن هذه الجرائم تستخدم في وقت سريع، ويتم محوها في وقت أسرع، كما أنه لا يوجد خبرة كافية لدى ضباط التحقيق في مثل هذه الجرائم من ناحية التحقيق والبحث عن الأدلة والتحفظ عليها، ومن صعوبات إثبات هذه الجرائم عدم اقتناع القضاة بكثير من الجرائم المستحدثة في هذا الشأن. حيث تعد سمة عدم القدرة على إثبات هذه الجريمة من السمات التي تميز جريمة الابتزاز الإلكتروني عن غيرها، حيث انتشرت مكاتب تقوم بأعمال الابتزاز والقرصنة والسرقة، من خلالها يقوم بعض الأشخاص باستئجار محترفين لسرقة بينات وملفات الشركات الكبرى دون اكتشاف أمرهم أو الإثبات عليهم [110].

([108])العجمي، مرجع سابق: ص22.

([109]) سمية فتحي السيد، الجريمة المعلوماتية، المؤتمر العلمي العاشر لقسم المكتبات والوثائق والمعلومات، كلية الآداب، جامعة القاهرة، 15-16 مايو 2013: ص6-7.

([110]) العفيفي، مرجع سابق: ص16-17.

يتبين مما سبق أن الجرائم الإلكترونية خاصة جريمة الابتزاز الإلكتروني لا يمكنها أن تترك آثار مادية وراءها بصورة يستطيع المختصون كشفها والقبض عليهم، وبالتالي فهذه الجريمة نظيفة لا تترك دماء أو قتل أو اعتداء، حيث إن هذه الجريمة ترتكب ويتم محو آثارها في ثواني معدودة، وبالتالي فإن هذه الخاصية من السمات التي تتميز بها الجريمة الإلكترونية عن غيرها من الجرائم.

رابعاً: خصوصية مجرمي المعلومات/ حيث إن المجرم الذي يقترف جريمة الابتزاز الإلكتروني يتسم بخصائص معينة تميزه عن المجرم التقليدي، فإذا كانت الجرائم التقليدية لا أثر فيها للمستويين العلمي والمعرفي للمجرم في عملية ارتكاب جريمته، فإن الأمر يختلف بالنسبة للجرائم المعلوماتية، فهي جرائم فنية تقنية في الغالب الأعم، ومن يرتكبها عادة يكون من ذوي الاختصاص في تقنية المعلومات، أو على الأقل شخص لديه حد أدني من المعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الإنترنت، فعلى سبيل المثال تتطلب الجرائم الإلكترونية ذات الطابع الاقتصادي مثل التحويل الإلكتروني غير المشروع للأموال مهارة وقدرة فنية تقنية عالية جدًا من قبل مرتكبيها، كذلك فإن البواعث على ارتكاب المجرم المعلوماتي لهذا النوع من الإجرام المعلوماتي قد تكون مختلفة عن بواعث ارتكاب الجرائم من قبل المجرم التقليدي[111].

وقد تم تصنيف مجرمي الابتزاز الإلكتروني أو الجرائم الإلكترونية إلى عدة أصناف وهي: المخترقون مثل **الهاكرز** الذين يعدون بارعين في استخدام الحاسب الآلي ولديهم فضول في استخدام حسابات الآخرين بطرق غير مشروعة، وهم متطفلون وغير مرحب بهم. **والمحترفون** وهم الأكثر خطورة بين مجرمي الإنترنت، حيث يهدف بعضهم إلى الحصول على الكسب المادي غير المشروع، والبعض الآخر من أجل تحقيق مكاسب سياسية وإبراز وجهات نظرهم أو أفكارهم. أما النوع الثالث وهم **الحاقدون** الذين ليس لديهم أي أهداف للجريمة ولا يسعون لمكاسب سياسية أو مادية، لكنهم يتحركون بدافع الرغبة في الانتقام والتأثر كالأمور الطائفية[112].

لهذا يتبين للباحثة من خلال ما سبق أن مجرمي الإنترنت خاصة الذين يقومون بعملية الابتزاز الإلكتروني لهم مميزات وسمات تميزهم عن غيرهم من المجرمين، فهم يمتازون بالذكاء من ناحية، والاحتراف في التعامل مع الأجهزة الإلكترونية من ناحية ثانية، والحقد والكره للمجني عليهم من ناحية ثالثة.

([111]) تركي بن عبد الرحمن المويشير، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، جامعة نايف العربية للعلوم الامنية، الرياض، ط1، 2012: ص25.

([112]) العجمي، مرجع سابق: ص21-22.

خامساً: جريمة الابتزاز تتم بتعاون أكثر من شخص/ حيث تتميز الجريمة الإلكترونية بصفة عامة بأنها تتم بتعاون أكثر من شخص على ارتكابها إضرارًا بالجهة المجني عليها، وغالبًا ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والإنترنت يقوم بالجانب الفني من المشروع الإجرامي، وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه، أما الاشتراك في إخراج الجريمة الإلكترونية إلى حيز الوجود قد يكون اشتراكًا سلبيًا وهو الذي يترجم بالصمت من جانب من يعلم بوقوع الجريمة في محاولة منه لتسهيل إتمامها، وقد يكون اشتراكًا إيجابيًا وهو غالبًا كذلك يتمثل في مساعدة فنية أو مادية[113].

يمكن القول من خلال ما سبق إن هذه الجريمة لا يمكن لشخص واحد فقط القيام بها، كونها تتم في مراحل مختلفة، فتقنيات الحواسيب لا يمكن لشخص واحد أن يكون على علم ودراية بكافة جوانب الحاسوب وشبكة الإنترنت، وبالتالي فإن الاشتراك بين أكثر من شخص في هذه الجريمة يمكن أن يكون له آثار إيجابية في نجاح الجريمة.

تعتبر الجريمة الإلكترونية من أشد الجرائم فتكًا بالإنسان، خاصة أنها تتم في بيئة غامضة وصعبة الوصول إليها، لذلك فإن العديد من دول العالم غير قادرة على إعاقتها وكبح جماحها، كونها عابرة للدول من ناحية، وتحتاج لمهارة ودقة فائقة للوصول إليها، لذلك تتضافر الجهود الدولية والإقليمية للحد منها.

لم يعرّف المشرع الفلسطيني الجريمة الإلكترونية بصورة واضحة، بسبب حداثة هذه الجريمة على الساحة الفلسطينية، لكنه أعطى اهتمامه لحماية حق السر أو انتهاك خصوصية الأفراد، وفرض عليهم عقوبات رادعة. وفي الوقت نفسه ومع ظهور قانون الجرائم الإلكترونية الفلسطيني رقم 10 لسنة 2018م اهتم المشّرع الفلسطيني بهذه الجريمة وتوعد من قام باستخدام الشبكة الإلكترونية استخدامًا ينافي القانون في ابتزاز شخص أو تهديده بالحبس والغرامة المالية أو بكلتا العقوبتين.

لقد اهتم المشرع الفلسطيني خاصة والأردني والمصري بصفة عامة بإبراز العقوبة التي تترتب على الابتزاز الإلكتروني سواء أكان هذا الابتزاز ماديًا أم جنسيًا أو ابتزازًا بهدف الحصول على الوثائق والمستندات، وفرض عقوبات رادعة عليها وهو ما جعل العديد من مؤسسات المجتمع المدني ترفض هذا القانون.

([113]) المويشير، المرجع السابق: ص35.

أيضًا تختلف جريمة الابتزاز الإلكتروني عن غيرها من الجرائم التقليدية كونها تتم عن طريق جهاز الحاسوب وأنها تعتبر عابرة للحدود من ناحية، وتتصف بالإغراء والنعومة للمجرمين من ناحية أخرى، وصعوبة اكتشافها من ناحية ثالثة، وخصوصية مجرميها من ناحية رابعة، وأنها تتم بتعاون بين شخص وآخر، وهو ما تفتقده الجرائم العادية.

الفرع الثالث: الآثار المترتبة على جريمة الابتزاز الإلكتروني على الفرد والمجتمع.

تعتبر قضية الابتزاز من الجرائم الخطيرة، التي لها آثار سلبية على كل من الفرد والمجتمع، وتتطلب الحكمة في التعامل والمعالجة والتثبت من الحقائق والأدلة، قبل التسرع في إصدار التهم والعقوبات، حيث يوجد هنالك قضايا ابتزاز قد لا تكون المرأة طرفًا فيها، من خلال حصول الجاني على صورها دون علمها بطريقة أو بأخرى بقصد ابتزازها، ومن أهم الآثار التي تتركها جريمة الابتزاز على الفرد والمجتمع [114]:

أولاً/ الآثار المترتبة على جريمة الابتزاز الإلكتروني على الفرد

1. الصدمات والاضطرابات النفسية التي قد تتعرض لها المبتزة، يتَّضح أنها قد تعاني من اضطرابات عصبية كالقلق النفسي، الخوف، الاكتئاب، أو قد تعاني من اضطرابات التكيف الاجتماعي بأن تميل إلى العزلة الاجتماعية والخوف من مواجهة الناس، وقد تدخل في بعض الاضطرابات الشخصية كالشخصية العدوانية أو المضادة للمجتمع.
2. يتحول المجني عليه لأسير لا يستطيع أن يتحكم في قراراته ولا سلوكياته، بل هو رهن إشارة للمبتز أينما حلّ وارتحل.

3. يترك الابتزاز العاطفي أثرًا كبيرًا في نفسية المرأة وشخصيتها وقد يحتاج إلى سنوات من العلاج النفسي المستمر بعد إبعادها عن الطرف الذي يمارس الابتزاز وانخفاض تقدير الذات وذلك سيؤثر على الضحية في كل شيء بعد ذلك.

4. أن جريمة الابتزاز عندما تقع على الشخص فإنه يمكنه أن يخسر الكثير من أمواله في سبيل الخلاص من تهديدات المبتز إليه، وبالتالي فإنه ذلك من شأنه يكون له تأثير اقتصادي كبير عليه.

([114]) نوال بنت عبدالعزيز العيد، الابتزاز: المفهوم ، الأسباب ، العلاج، موقع الكاتبة الرسمي، نشر بتاريخ 5 جمادي الأول 1435هـ، للتفاصيل:

http://nawalaleid.com/cnt/lib/768

5. يمكن أن تكون جريمة الابتزاز الالكتروني دافعاً لارتكاب جرائم عديدة بدافع الأخلاق والشرف كالقتل، حيث أن ابتزاز الفتيات وتطور الأمر لقضايا أخلاقية يمكن أن يدفع بالأهل للانتقام من ابنتهم وقتلها جراء ارتكابها ذلك الفعل.

6. يمكن لجريمة الابتزاز إذا تم اكتشافها وانتشارها في المجتمع أن تعمل على تشويه سمعة الشخص المبتز، خاصة لو كانت امرأة وليس رجلاً، وهو ما يمكن أن ينتج عنها ابتعاد الناس عنها، وعدم الزواج منها، خاصة وأن المجتمع الشرقي يتأثر كثيراً بهذه الجرائم خاصة الأخلاقية منها.

7. أن جريمة الابتزاز الالكتروني لها آثاراً وانعكاسات على نفسية الضحية واستقرار أسرتها، ما يؤدي إليه من تفكك أسري وشيوع الخيانة والاستغلال، ما يفضي الى نشر الجريمة وهدم شخصيات الضحايا، ونشر الأمراض النفسية والجنسية بين الاشخاص.

ثانياً/ الآثار المترتبة على جريمة الابتزاز الإلكتروني على المجتمع والمؤسسات

1. نشر الجريمة في المجتمع فكم من عورة لمسلمة أو مسلم تناقلها بعض ضعفاء النفوس في الأعراض ونشروها في أوساط المجتمع.
2. يمكن للمؤسسات التي تتعرض للابتزاز أن ينتج عنه العديد من الآثار كالاطلاع على معلومات سرية لصفقة أو مناقصة أو أمور تسويقية خاصة والاستفادة منه، العبث بمخازن المعلومات الخاصة بالشركة بحذفها أو تعديلها أو تعطيل الوصول إليها، وسرقة الأموال، أيضاً الغش في المعاملات الالكترونية كالتغيير في المبيعات، وعمليات الاحتيال، والابتزاز، واختراق الموقع الإلكتروني الخاص بالشركة.
3. خلخلة الجانب الاجتماعي للمجتمع بما تحدثه من حالات طلاق وعنوسة، وبما تحدثه من مشكلات اجتماعية بين الأسر.
4. التمادي في الظلم والطغيان؛ فالذي يحاول الابتزاز لن يتوقف، وسيستمر في طريقه من ابتزاز للأعراض وانتهاك للخصوصيات، وذلك سيؤثر سلبًا في المجتمع، وسيزيد من الجريمة إذا لم يتم ردعه، وهذا هو الدور الذي تقوم الجهات المختصة به من خلال حفظ الأمن والاستقرار، وصيانة الأعراض، وتعقب هؤلاء المفسدين والقبض عليهم وإحالتهم إلى الجهات المختصة.

ترى الحكومة الفلسطينية أنَّ هناك حاجةً ماسة إلى وجود قانون للجرائم الإلكترونية في الأراضي الفلسطينية، لا سيَّما في ظل الانتشار الكبير لوسائل الاتصال عبر الإنترنت، والذي رافقه حالات إخلال بالسلوك العام والتحريض، حيث أشار رامي الحسيني المستشار القانوني للحكومة الفلسطينية إلى أنَّ أهمية هذا القانون تكمن في سد الفراغ القانوني الهائل المتعلق بالجرائم الإلكترونية، لا سيَّما

التي تتزايد بشكل ملحوظ، وأن وجود هذا القانون يهدف بالأساس إلى معاقبة من يسيئون استخدام التكنولوجيا وتقنيات المعلومات، وبيَّن أنّ هذا القانون يراعي الاتفاقيات والقوانين الدولية والتشريعات الفلسطينية[115].

إنَّ الخسائر الناتجة عن جرائم الابتزاز الإلكتروني لا يمكن حصرها، سواء أكانت خسائر مالية أم جنسية أم ما يقدمه المجني عليه من تنازلات لإرضاء المبتز وضمان عدم افتضاح أمره، فهذه الجريمة تتسبب في ضياع المستقبل الاجتماعي للضحية وتؤدي للمزيد من معاناته داخل محيط الأسرة والمجتمع، كما تقل فرص الضحية إن كانت امرأة في الزواج خشية افتضاح أمرها عند زوجها، أو بسبب علم الآخرين بما تعرضت له فيعرضون عنها، كما يتسبب في العزلة وعدم التعامل مع الآخرين بسبب الشعور بالخجل وضعف الثقة بالنفس وتأنيب الضمير، مما يسبب لها أمراض نفسية، وقد يزداد الانحراف الأخلاقي لدى المرأة وتصبح غير مبالية بما تفعل، وتصبح الجريمة لديها فرصة للانتقام من نفسها ومن ذويها ومن المجتمع بأكمله[116].

كما أن الابتزاز بتسبب في كثير من الانحرافات الجنسية والإباحية والوقوع في وحل الانحرافات التي يرفضها المجتمع. وتزداد نسبة الطلاق بسبب اكتشاف العديد من الفضائح والتشهير بالضحية، مما يتسبب في هدم أسرة من المجتمع بما فيها من أطفال وضياع تلك الأسرة، ويعيش الأطفال في بيئة غير صحية من الناحية الأخلاقية، مما ينتج عنه جيل غير سوي ويخلق اضطرابات داخل المجتمع[117]، كما يمتد تأثير جرائم الابتزاز الإلكتروني ليشمل تهديدا لنظام القيم الموجود داخل المجتمع، وتدمير المنظومة الأخلاقية فيه، كما تهتز معايير الأخلاق الحميدة بما تشمله من كرم وشجاعة وبر وإحسان، ونبذ الأخلاق السيئة من كراهية وحقد وبخل وغيبة وانتهاك لحق الآخرين، خاصة إذا كانت هذه الجرائم تقوم في المجتمعات المُحافظة، مما ينتج عنه انتشار للرذيلة والإباحية بين أفراد المجتمع والتأثير على النسيج الاجتماعي للمجتمع، وهدم القيم الفاضلة التي بناها المجتمع في سنوات طويلة[118].

([115]) محمد الهندي، نفاذ قانون الجرائم الإلكترونية الفلسطيني: المجتمع المدني وانكفاء الدور، ورقة بحثية قدمت إلى البرنامج التدريبي "إعداد السياسات العامة والتفكير الاستراتيجي"، مركز مسارات، 2018/3/27: ص11.

([116]) المطيري، مرجع سابق: ص58.

([117]) المرجع السابق: ص58.

([118]) ذياب البداينة، جرائم الحاسب الآلي والإنترنت، بحث منشور في الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، تونس، ١٤٢٤هـ، ص١١٢.

يتضح مما سبق أن الجرائم الإلكترونية لها آثار جانبية سلبية على الفرد والمجتمع على حد سواء، فانتشار هذه الجرائم في المجتمع العربي المحافظ ينعكس عليه، وذلك من خلال التأثير على النسيج الاجتماعي بصورة كبيرة، كما أن هذه الجرائم تعمل على تفتيت المجتمع سواء أكان على مستوى النساء أم الأطفال أم الشباب أم الشيوخ، فالخسائر التي تنتج عن هذه الجرائم لا يمكن وصفها أو وقفها؛ حيث إن انتشار الحواسيب والشبكة العنكبوتية في كل بيت تسبب بانتشار الآثار السلبية بين أفراد المجتمع وانعكس بصورة سلبية على عادات وتقاليد المجتمع.

المبحث الثاني: طرق التحقيق والإثبات في جرائم الابتزاز الإلكتروني

إنّ الهدف الأساسيّ الذي تسعى إلى تحقيقه أجهزة العدالة في المجتمع من ناحية الجريمة، هو عنصر الإثبات لكي يُصار إلى تحقيق العدالة، ونظريّة الإثبات في القانون تقوم على عدّة مبادئ صاغها فقهاء القانون لمساعدة السلطات المختصة للاستعانة بها في القضايا الجزائية المعروضة عليهم، وبالتالي وجود قواعد تحدّد للقاضي الطريق الذي يسلكه في تتبع النزاع، والحكم في نهاية المطاف. ومثل هذه المبادئ تؤدّي إلى عدم ازدواج الأحكام القضائية في القضايا المتشابهة، بسبب عشوائية القاضي في انتقاء وسائل وعناصر إثبات دون أخرى، وحريته في الاقتناع الوجدانيّ مبنية على شروط معينة، وبالتالي تحقيق العدالة النسبية للجميع، لأن العدالة المطلقة هي تلك العدالة الموجودة في السّماء [119].

وجريمة الابتزاز الإلكتروني مثلها مثل أي نوع من الجرائم التقليدية الأخرى تمر بمراحل الاستدلال والتحقيق الجنائي الابتدائي، والتي تحتاج إلى بحث المحقق عن الدليل المثبت لوقوع الجريمة في الحاسب الآلي وما شابه من الهواتف الذكية، ومن ثم ربط تلك الأدلة التي عثر عليها بالأشخاص الذين ارتكبوا تلك الجرائم تمهيدًا لتقديمهم للعدالة، وإلا اعتبر عمله ناقصًا، ويترتب على هذه الأدلة التي عثر عليها في جرائم الابتزاز الإلكتروني داخل أجهزة الحاسب الآلي التحقيق مع المتهمين بتلك الجرائم ومواجهتهم بالأدلة التي عثر عليها، وبالتالي التحقيق للوصول إلى أعلى درجات العدالة لكل من الجاني والمجني عليه، أما الدليل فهو الوسيلة التي يستعين بها المحقق للوصول إلى الحقيقة التي يسعى إليها، وكل ما يتعلق بالوقائع المطروحة عليه لتطبيق حكم القانون عليها، فبدون هذا الدليل لا تثبت الجريمة ولا يمكن إسنادها إلى متهم وبالتالي لن يطبق قانون العقوبات[120].

([119]) آمال عبد الرحمن حسن، الأدلة العلمية الحديثة ودورها في الإثبات الجنائي، رسالة ماجستير غير منشورة، جامعة الشرق الأوسط، عمان، 2012: ص12.

([120]) المطيري، مرجع سابق: ص61.

كما أدى التطور العلمي والتكنولوجي الحديث إلى إنتاج أجهزة مراقبة ووسائل حديثة ذات تقنية عالية في الإثبات والتحقيق، والواقع أن استخدام أجهزة المراقبة لا تقتصر على أجهزة التصنت الت تلتقط الأحاديث السلكية واللاسلكية، بل امتدت بقدرتها الفائقة للالتقاط المكالمات التي تتم بطريق الانترنت، كما أنه بات من السهل التقاط صور الأشخاص عن بعد وبدقة عالية، وهو الأمر الذي أفقد الإنسان حريته وخصوصيته، أما هذه الوسائل فيجب أن لا تمس الحرية الفردية، أما إذا كانت تمس بالحرية الفردية فإنه وجب على القاضي استبعادها كوسيلة إثبات في المواد الجنائية[121].

كما نص القانون الإجرائي الفلسطيني على من يخول بصفة الضبطية القضائية، حيث أقر إنه: "يكون من مأموري الضبط القضائي:

1. مدير الشرطة ونوابه ومساعدوه ومديرو شرطة المحافظات والإدارات العامة.
2. ضباط الشرطة، كل في دائرة اختصاصه.
3. رؤساء المراكب البحرية والجوية
4. الموظفون الذين خولوا صلاحيات الضبط القضائي بموجب القانون [122].

المطلب الأول: طرق التحقيق في جرائم الابتزاز الإلكتروني:

يشرع رجال الضبط الجنائي ورجال التحقيق بمجرد وقوع الجريمة بجمع الاستدلالات بغرض إقامة الدليل، والبحث عن الجاني، كما أن التحقيق في جرائم الابتزاز الإلكتروني مختلف عن غيره من الجرائم، خاصة مع وجود العديد من العقبات التي ظهرت نتيجة التطور في هذه الجريمة بسبب التطور الهائل في تكنولوجيا الاتصال، حيث أن المحقق في هذه الجريمة بالذات يحتاج إلى خبرة في التعامل مع أدلة الجريمة الرقمية، وهو ما يبرز صعوبات تكتنف التحقيق والإثبات في جريمة الابتزاز الإلكتروني وسيتم تناول هذا الموضوع في فرعين كالتالي:

التحقيق الجنائي عبارة عن فحص جهاز الجاني أو المشتبه به من قبل المحققين، فمثلًا إذا تمت جريمة عن طريق الحاسوب أو الأجهزة الذكية المختلفة، فيأتي المحقق المتخصص ليفحص ما به وذلك باستخدام أدوات خاصة ودراسات سابقة وكل ما هو ممكن والهدف منها لجمع الأدلة المطلوبة؛

([121]) زاهر خالد صباح، دور الوسائل العلمية الحديثة في الإثبات الجنائي في فلسطين، رسالة ماجستير غير منشورة، جامعة القدس، أبو ديس، فلسطين، 2017: ص57.

([122]) المادة رقم 21 من قانون الإجراءات الجزائية الفلسطيني رقم 3 لعام 2001م، والمنشور في العدد 38 من الجريدة الرسمية.

لكي تُعطى للنيابة أثناء عملية التحقيق. أما عملية التحقيق الجنائي الرقمي ليست مقتصرة فقط على الأجهزة الإلكترونية أو أدلة ملموسة، بل من الممكن أن تكون أيضًا عملية تتبع لبعض الأدلة والأمور التي تم إجراؤها أثناء عملية الاختراق أو بعد عملية الاختراق من خلال تحليل ملفات النظام وتتبع أثاره والحركات التي قام بها أو يقوم بها في نفس اللحظة وهذه الأمور جميعها تفيد في عملية التحقيق الجنائي الرقمي ليس فقط لمعرفة الجاني بل لمعرفة نقاط ضعف الموقع لديه من خلال تحليل الحركات التي قام بها المخترق أثناء عملية الاختراق [123].

في حال وجود أي إشعار يدل على وجود عمليات اختراق سواء من خلال مراقبتك الدورية لملفات أو من خلال متابعة الإشعارات الناتجة عن الجدار الناري الموجود على السيرفر مثلًا، وسوف يحاول البرنامج تحديد الأيبيهات التي حاولت التخمين والدخول على السيرفر من جهة وأيضًا سوف يحاول المحققون الجنائيون أن يلقوا نظرة على ملفات اكس لكي يحللوا الحركات التي قام بها المخترق على تطبيق الويب الخاص بهم وسوف يحاولوا معرفة الطرق التي حاول المخترق للدخول للموقع من خلالها [124].

يختلف التحقيق في جرائم الابتزاز الإلكتروني عن التحقيق في الجرائم الأخرى للابتزاز، حيث إن المحقق سيحتاج إلى خبرة في التعامل مع الأدلة الرقمية التي بحوزته وكيفية تفنيدها، ليعرف الكيفية التي تمت بها ارتكاب الجريمة، وأخذ التصور الصحيح لها ومواجهة المتهم بما يتوفر من أدلة تدينه بالعمل الجرمي، وضمان عدم مراوغته أثناء التحقيق ليصل في النهاية لاكتشاف الحقيقة التي يبحث عنها، إما بإدانة المتهم بالتهمة المنسوبة إليه أو بتبرأته من هذه التهمة [125].

إنّ المحقق الناجح هو من يحافظ على سير مراحل التحقيق بكل سرية لمصلحة التحقيق ولضمان تحقيق العدالة والكشف عن الحقيقة، وذلك حتى لا يتم التأثير على الشهود، أو حتى من ناحية المتهمين الذين يحاولون أثناء سير عملية التحقيق من الاختفاء أو الهروب أو إخفاء بعض آثار الجريمة، كذلك حفاظًا على سمعة المتهم وضمان عدم فضيحته إذا ما لم يثبت الجريمة عليه، أما سرية التحقيق فإنها تبقى دون إعلان إلى أن تنتهي التحقيقات جميعها، وتتصرف سلطة التحقيق في الدعوى المنظورة أمامهم، ويكون نطاق السرية على من لم يكن طرفًا في الدعوى الجنائية حيث يحق

([123])منى كامل تركي، التحقيق الجنائي في الجرائم الإلكترونية، نشر بتاريخ 10 ابريل 2016، للتفاصيل:
https://amday55.blogspot.com/2016/04/blog-post.html

([124]) تركي، المرجع السابق.

([125]) المطيري، مرجع سابق: ص93.

لأطراف الدعوى الاطلاع على التحقيق؛ حيث إن غالبية القوانين تجعل من سرية هذه التحقيقات عاملًا مهمًا في سير التحقيق، وكل من يقوم بإفشاء أسرار التحقيق يعرض نفسه للمسائلة القانونية[126].

وقد اهتم المشرع الفلسطيني بموضوع سرية البيانات والتحقيقات في أكثر من موضع، فمثلاً تبين المادة 46 من قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية والمنشور في العدد الممتاز رقم (16) من الوقائع الفلسطينية بتاريخ 2018/05/03، بأنه: "كل من أفشى سرية الإجراءات المنصوص عليها في هذا القرار بقانون، في غير الأحوال المصرح بها قانوناً، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين".

والثابت أنّ الدعوى الجزائية تمر بمرحلتين، مرحلة التحقيق ومرحلة المحاكمة، وتمر عملية التحقيق بمرحلتين أيضًا، مرحلة التحقيق الأولي ومرحلة التحقيق الابتدائي. فالمرحلة الأولى وهي مرحلة جمع الاستدلالات التي يباشرها أعضاء الضبط القضائي، والمرحلة الثانية تدخل في اختصاص قاضي التحقيق، أو عضو النيابة العامة، وإننا نؤيد الرأي أو الاتجاه الذي يقسم التحقيق إلى: **تحقيق أولي** والذي يناط به رجال الضبطية القضائية. **وتحقيق ابتدائي** ويناط به رجال القضاء، وهذا الأخير يقسم إلى تحقيق ابتدائي من اختصاص قاضي التحقيق وتحقيق نهائي ويكون في مرحلة المحاكمة من طرف قضاة الحكم. وفي كل جميع أنواع التحقيق هذه، يكون للقائمين عليه من ضبطية قضائية وقضاة، صلاحية ممارسة إجراءات البحث والتحري المحددة [127].

وقد حرص القانون الفلسطيني على ضمان سير الدعوى الجزائية بكل حيادية ونزاهة، حيث أوكل مهمة التحقيق الابتدائي إلى النيابة العامة، كونها تتسم بالشفافية والموضوعية في التحقيق، ولاكتساب هذه السلطة الخبرة الواسعة للموازنة بين حقوق الأفراد، وقدرتها على بناء قراراتها على الأدلة التي تتحراها لتقديم المتهمين إلى القضاء ليقول كلمته الأخيرة بهم [128].

([126]) خليفة كندر، عبد الله حسين، ضمانات المتهم في مرحلة التحقيق الابتدائي في قانون الاجراءات الجنائية، دار النهضة العربية، بيروت، ط1، 2002: ص154.

([127]) نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير غير منشورة، إشراف زرارة صالحي الواسعة، جامعة الحاج لخضر، الجزائر، 2012-2013: ص102.

([128]) جرادة، مرجع سابق: ص420.

إن التحقيق في جرائم الابتزاز الإلكتروني تحكمه نفس القواعد التي تحكم قواعد التحقيق في أي جريمة أخرى، أما وجه الخلاف فإنه يجب أن يكون المحقق في جريمة الابتزاز الإلكتروني ملمًا ومؤهلًا للتعامل معَ مقتضيات الجريمة من أجهزة إلكترونية وأدلة رقمية وأيضًا مصطلحات الجريمة، خاصة إذا كان المجرم في جريمة الابتزاز الإلكتروني ذكيا وله دراية بالتكنولوجيا [129].

كما اهتم المشرّع الفلسطيني بإجراءات التحقيق لضمان سيرها، حيث نصت المادة 34 فقرة 2 من قرار بقانون رقم 10 لسنة 2018 (المعدَّل) بشأن الجرائم الإلكترونية والمنشور في العدد الممتاز رقم (16) من الوقائع الفلسطينية بتاريخ 2018/05/03، أنه: "للنائب العام أو أحد مساعديه أن يأمر بالجمع والتزويد الفوري لأي بيانات، بما فيها حركة الاتصالات أو معلومات إلكترونية أو بيانات مرور أو معلومات المشترك التي يراها لازمة لمصلحة التحقيقات لغايات الفقرة 1 من هذه المادة باستعمال الوسائل الفنية المناسبة، والاستعانة بذلك عند الاقتضاء بمزودي الخدمات أو حسب الخدمة التي يقدمها"[130].

كما أن القانون الفلسطيني قد جعل من مصادرة الأجهزة إحدى أهم الإجراءات الرادعة لانتشار الجريمة، بل إنه أحد العلاجات التي يمكن أن تحد من هذه الجريمة، حيث أوصى المشرّع الفلسطيني بضرورة مصادرة أي أجهزة تم استخدامها في جريمة الابتزاز الإلكتروني، فقد نصت المادة 50 فقرة 2 بأنه: "دون الإخلال بالعقوبات المنصوص عليها في هذا القرار بقانون، وحقوق الغير حسن النية، على المحكمة أن تصدر قراراً يتضمن الآتي: ... 2- مصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القرار بقانون أو الأموال المتحصلة منها، على أن تكون إزالة المخالفة على نفقة الفاعل"[131].

وعليه فإنه يمكن القول إن إجراءات البحث والتحري عن الجرائم هي من صلاحيات جهات التحقيق سواء أكان أوليًا أم ابتدائيًا، ومن المفهوم فإن إجراءات البحث والتحري التي يباشرها رجال الضبط القضائي تصب في إطار التحقيق الأولي، بينما هذه الإجراءات عندما يباشرها قاضي التحقيق تعتبر تحقيقًا ابتدائيًا، وإذا كان التحقيق عموما يعتمد على ذكاء المحقق وفطنته وقوة ملاحظته وسرعة البديهة لديه، وأن يحاول بكل الجهد الممكن أن يقوم بالتحقيق في الجريمة ومتابعتها والبحث فيها وفي الأدلة والتنقيب عنها وصولاً لإظهار الحقيقة؛ فإن التحقيق في البيئة الإلكترونية يستوجب بالإضافة

([129]) عبد العزيز، مرجع سابق: ص53.
([130]) المادة 34 فقرة 2 من قرار بقانون رقم 10 لسنة 2018 (المعدل) بشأن الجرائم الإلكترونية.
([131]) المادة 50 فقرة 2 من قرار بقانون رقم 10 لسنة 2018 (المعدل) بشأن الجرائم الإلكترونية.

إلى كل هذا تطويرًا لأساليبه وتكليف جهات مختصة لممارسته من أجل مواكبة حركة الجريمة وتطور أساليب ارتكابها في هذه البيئة[132].

لقد تطورت وسائل التحقيق الجنائي في عصر المعلوماتية تطورًا ملموسًا يواكب حركة الجريمة وتطور أساليب ارتكابها، فبعد أنْ كان الطابع المميز لوسائل التحقيق العنف والتعذيب للوصول إلى الدليل، أصبحت المرحلة العلمية الحديثة القائمة على الاستعانة بالأساليب العلمية واستخدام شبكة الإنترنت هي الصفة المميزة والغالبة. ومرد ذلك حدوث طفرة علمية في مجال تكنولوجيا المعلومات والاتصالات واستخدام الوسائط الإلكترونية في شتى مجالات الحياة، فكلما اكتشف العلم شيئًا حديثًا وجد هذا الاكتشاف طريقه إلى مجال الإثبات الجنائي والتدليل [133].

وتبعًا لذلك فإنه من البديهي أن تظهر أنماط جديدة من الجرائم لم تكن معهودة في السابق، وهذا ليس قاصرًا على أسباب التقدم التقني فقط بل يحدث دومًا وبصفة مستمرة، فالمجرم والجريمة في تقدم وتجدد مستمر، فمجرم الأمس ليس كمجرم اليوم وبالتالي فجريمة الأمس ليست كجريمة اليوم. ولا شك ظهور أنماط جديدة من الجرائم لم تكن مألوفة من السابق ونحن لا نزال في بداية عصر الانفجار المعلوماتي، يعنى توقع ظهور المزيد والمزيد من هذه الأنماط الجديدة، والذي يتوجب معها تحديث الأنظمة والتعليمات والجهات الأمنية المختصة بمعالجة القضايا الناتجة عن ظهور هذه الأنماط الجديدة، وهو ما يستتبع تطوير أسلوب التحقيق فيها[134].

من خلال ما سبق تشير الباحثة إلى خصوصية الجرائم المتعلقة بالحاسب الآلي بصورة تستدعي بأن يتم تطوير أساليب التحقيق الجنائي وإجراءاته بصورة تتلاءم مع هذه الخصوصية، وحيث يتمكن رجل الشرطة، والمحقق من كشف الجريمة، والتعرف على مرتكبيها بالسرعة والدقة اللازمين.

ولتحقيق ذلك يجب من ناحية تدريب الكوادر التي تباشر التحريات والتحقيقات مع الاستعانة بذوي الخبرة الفنية المتميزة في هذا المجال، فضلاً عن تطوير الإجراءات الجنائية، لتحقيق الغرض المطلوب، وهو ما بدأت التشريعات منذ بضع سنوات في تحقيقه.

([132]) سعيداني، مرجع سابق: ص103.

([133]) خالد ممدوح، مبادئ التحقيق في الجرائم المعلوماتية، موقع كنانة أونلاين، نشر بتاريخ 2009/1/26، للتفاصيل: http://kenanaonline.com/users/KhaledMamdouh/posts/81536

([134]) المرجع السابق.

المطلب الثاني: طرق الإثبات في جرائم الابتزاز الإلكتروني:

قاد التطور التقني والتكنولوجي في جرائم الابتزاز الإلكتروني والحواسيب إلى تغيير واضح في مفهوم الإثبات وجمع الأدلة من حيث طرق هذا الجمع والبحث عن الأدلة الرقمية واستخلاصها والتحفظ عليها، ما أدى إلى ضرورة وجود خبير تقني ينضم إلى فريق عمل إثبات هذه الجرائم كالطبيب الشرعي وخبير البصمات وغير ذلك. وبالتالي فإن الإثبات في جريمة الابتزاز الإلكتروني يعتمد على ثوابت وأسس واحدة يستخدمها المختصون في جمع الأدلة، فهي تحتاج إلى المعاينة والتفتيش واستخراج الأدلة المتعلقة بالجريمة وتقديمها لجهات الاختصاص لاستكمال إجراءات التحقيق ومن ثم المحاكمة [135].

أولاً: المعاينة:

ويقصد بها الانتقال إلى الأماكن التي وقعت بها الجريمة، أي إلى مسرح الجريمة، وذلك لإثبات حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة عن الجريمة ومرتكبيها، وبالتالي وجب على السلطات المختصة بإجراء المعاينة بالانتقال إلى أماكن وقوع الجريمة فور ارتكابها، حتى لا يكون هناك فارق زمني طويل بين وقوع الجريمة وإجراء المعاينة التي تسمح للجاني بإجراء تغيير أو إزالة كل أو بعض الآثار المادية للجريمة، والتي يمكن أن تساعد في التنقيب عن الحقيقة، وحتى لا يقع الشك في الدليل المستنبط منه [136].

تتضح أهمية المعاينة في كونها تقوم بإحاطة صورة شاملة لموقع الجريمة لجهة التحقيق والمحاكمة، وبكل ما يحتويه من تفصيلات، سواء أتعلقت بمكانه أم وصفه من الداخل، أم الآثار الموجودة به، وهذا حتى يتسنى لضباط الشرطة القضائية والقضاة وضع تصور لكيفية وقوع الجريمة واستخلاص بعض الأدلة من المادة التي تم جمعها. وباعتبار المعاينة من أهم إجراءات التحقيق الجنائي فإن أهميتها تتجسد سواء من الناحية القانونية أو العملية، فمن الناحية القانونية تبدو أهميتها من عدة اتجاهات منها تأكيد وقوع الجريمة أو نفيها، صدق أقوال الواقعة، ركن الخطأ أو العمد فيها، تحديد الوصف القانوني لها، كما تساعد القاضي في تكوين قناعته؛ أمَّا من الناحية العملية فهي تساعد

([135]) المطيري، مرجع سابق: ص63 وما بعدها.

([136]) عمرو حسين عباس، أدلة الإثبات الجنائي والجرائم الإلكترونية (المعلوماتية)، بحث مقدم إلى المؤتمر الإقليمي الثاني حول تحديات تطبيق الملكية الفكرية في الوطن العربي، خلال الفترة من 26-2008/4/27، مقر جامعة الدول العربية، ص16.

المحقق على تحديد وقت ارتكاب الواقعة الإجرامية، ومعرفة علاقة الجاني بالمجني عليه، وتحديد الأسلوب الإجرامي الذي استعان به الجاني[137].

والمعاينة في مجال كشف غموض الجريمة المعلوماتية خاصة جريمة الابتزاز الإلكتروني لا تتمتع بنفس الدرجة من الأهمية التي تلعبها في مجال الجريمة التقليدية، ومرد ذلك أن هناك تقريبًا مسرحًا للجريمة التقليدية، والتي يتمكن من خلالها الباحث والمحقق الجنائي التنقيب عن الواقعة عن طريق معاينة الآثار المادية التي خلفها ارتكاب الجريمة والتحفظ على الأشياء التي لها علاقة بالواقعة الإجرامية، بينما لا توجد عادة مسرح للجريمة المعلوماتية باعتبار مكان الإدارة هو العالم الافتراضي أو عالم الفضاء الإلكتروني Cyber Space والذي يكون عادة الموقع أو المكتب الذي توجد فيه مكونات الحاسب الآلي المادية، والمعنوية، والتي تكون محلا للجريمة أو أدلتها وهي تتمثل في الأجهزة والأنظمة والبرامج، إذا فالانتقال للمعاينة في الجريمة المعلوماتية لا يكون إلى العالم المادي بل إلى العالم الافتراضي[138]. ويتم بمراحل عديدة من خلال تجميع المعلومات المخزنة، ومن ثم المراقبة، وأخيرًا ضبط الأجهزة وفحصها[139].

تعتبر المعاينة إجراءً تحقيقيًا متروكًا لتقدير المحقق حسب مصلحة القضية سواء طالب بها الخصوم أم لم يطلبوها، إلا في حالة واحدة أوجب فيها القانون الانتقال الفوري إلى محل الواقعة وهي في حالة إخطارها بجناية متلبس بها، وذلك لإثبات حالة الأماكن ووصفها وصفًا دقيقًا، وبيان حالة الأشخاص والأفراد والأشياء وكل ما يلزم حالته. كما أنه لا يجوز للمحقق في إجراء المعاينة ندب أحد رجال الضبط الجنائي للقيام بهذا الإجراء، أما في قضايا الجنح والقضايا غير المتلبس بها فيكون الانتقال والمعاينة أمرًا تقديره للمحقق حسب ما يراه في مصلحة التحقيق. كما أنه وبالرغم من أهمية المعاينة في الجرائم التقليدية، إلا أنَّ هذه الأهمية تقلُّ في الجرائم الإلكترونية خاصة جريمة الابتزاز الإلكتروني، وذلك بسبب قلة الآثار المادية التي يخلفها الجاني عند ارتكابه للجريمة، وذلك لطول الفترة الزمنية بين ارتكاب الجريمة واكتشافها، مما يجعل الجاني يتلاعب بالأدلة والآثار لطمس معالم جريمته[140].

([137]) زهية معمش، ونسيمة غانم، الإثبات الجنائي في الجرائم المعلوماتية، رسالة ماجستير غير منشورة، إشراف محمد بن فردية، جامعة عبد الرحمن ميرة، الجزائر، 2012-2013: ص7-8.

([138]) معمش، المرجع السابق: ص8.

([139]) Orin S. Kerr* DIGITAL EVIDENCE AND THE NEW CRIMINAL PROCEDURE، COLUMBIA LAW REVIEW {Vol .105-279}، P 285

([140]) المطيري، مرجع سابق: ص71 وما بعدها.

كما قد تكون المعاينة إجراء استدلال وتحري، وبالتالي لا تتوقف طبيعتها على صفة الشخص الذي يقوم بها، بل على مدى ما يقتضيه إجراءها من مساس بحقوق الأشخاص وحرياتهم، فإذا تمت المعاينة في مكان عام كانت إجراء استدلالي، وإذا تمت أو اقتضت دخول مسكن له حرمة خاصة كانت عبارة عن إجراء تحقيق.

نص المشرّع الفلسطيني وفق قانون الإجراءات الجزائية رقم 3 بسنة 2001م والمنشور في العدد 38 من الجريدة الرسمية على أنه: "وفقًا لأحكام القانون على مأموري الضبط القيام بما يلي: 2-إجراء الكشف والمعاينة والحصول على الإيضاحات اللازمة لتسهيل التحقيق"[141]، كذلك المشرّع الأردني أولى عملية المعاينة اهتمامًا خاصًا في قانون أصول المحاكمات الجزائية الأردني رقم 9 لسنة 1961م، حيث نص على أنه: "إذا وقع جرم مشهود يجب على المدعي العام أن ينتقل في الحال إلى مسرح الجريمة"[142].

أما عند إجراء عملية المعاينة بعد وقوع الجريمة مباشرة يجب مراعاة عدة ضوابط وهي: تصوير الحاسب والأجهزة الطرفية المتصلة به، على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة، أيضًا يجب إخطار الفريق الذي سيتولى المعاينة قبل موعدها بوقتٍ كافٍ حتى يستعد من الناحية الفنية والعملية لوضع خطة مناسبة للعملية، كذلك إعداد خطة المعاينة موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها بدقة، أيضًا ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء المقارنة والتحليل عند عرضها على المحكمة، كذلك التحفظ على سلة المهملات من الأوراق الملقاة أو الممزقة والشرائط والأقراص الممغنطة وفحصها ورفع البصمات ذات الصلة بالجريمة، أيضًا التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة، كذلك يجب أن تقتصر المعاينة على الباحثين والمحققين أصحاب الكفاءة العلمية والخبرة الفنية، وأخيرًا يجب أن تتم الإجراءات وفق مبدأ المشروعية وفي إطار ما تنص عليه القوانين الجنائية[143].

([141]) المادة 22 فقرة 2 من قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001م.

([142]) المادة 29 فقرة 1 من قانون أصول المحاكمات الجزائية الأردني رقم 9 لسنة 1961م.

([143]) عبد الغني فرغلي، ومحمد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية: دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، والذي عقد في الفترة من 12-2007/11/14م، جامعة نايف العربية للعلوم الأمنية، الرياض: ص17-18.

تتم المعاينة في جريمة الابتزاز الإلكتروني كأي جريمة معلوماتية يتم الانتقال فيها إلى العالم الافتراضي الذي تعيش فيه الأدلة الرقمية من طرف رجال الأمن المعلوماتي والذي يستخدم طريقتين في البحث والتحري: **أولهما:** تقصي الحقائق والآثار، وهي أكثر ما يشكل هاجسًا لدى محترفي الإجرام المعلوماتي ومحترفي الأجهزة، حيث نجد أول نصيحة في المواقع الخاصة بالمحترفين "قم بمسح آثارك"، فإذا لم يتم إخفاء الآثار التي تدل على هويته سيتم التعرف عليه بسهولة. **وثانيهما:** حماية مسرح الجريمة، حيث يسعى رجال الأمن المعلوماتي لحماية مسرح الجريمة المعلوماتية من أي تغيير حتى تختفي الآثار التي تدل على شخصية الجاني [144].

يتبين للباحثة من خلال ما سبق أن المعاينة تعتبر من أهم إجراءات التحقيق فهي تسهّل مهمة المحقق بالوقوف السريع والمباشر على مكان الجريمة، وبذلك يتمكن من تصور مكان الجريمة وسماع الشهود الموجودين قبل مغادرتهم المكان، ويقف حائلًا دون الجاني أو المتهم أو حتى المجني عليه أو ذويهم من التأثير على الشهود أو محاولة طمس معالم الجريمة وتلفيق أدلتها.

ثانياً: التفتيش

وهو إجراء من إجراءات التحقيق تختص به سلطة التحقيق بصفة أصلية ويجوز استثناءً لرجال الضبط القضائي متى كانت لهم الصفة، فالتفتيش فيه إباحة قانونية لانتهاك خصوصية فرد، فهو يعد أقسى الصلاحيات التي تمارسها الجهات العدلية في الدولة ضد المواطنين، والتفتيش بحد ذاته ليس غاية، لكنه وسيلة للبحث في مستودع سر الشخص عن دليل يرتبط بجريمة مرتكبة، أما جرائم الابتزاز الإلكتروني فهي ترتكب في عالم الإنترنت وعلى المستوى المحلي والدولي، مما يثير عدة مشكلات منها تتبع الاتصالات الإلكترونية عن طريق جهات التحقيق لإقامة الدليل على مرتكب الجريمة، ويلزم ليكون التفتيش قانونيًا أن تكون الجريمة على درجة عالية من الخطورة مع وجود البحث والتفتيش بالإضافة إلى تحديد الإذن[145].

لهذا فإن المشرع الفلسطيني لم يخصص نصاً تشريعياً لتعريف التفتيش، إنما اكتفى بالنص على أن التفتيش إنما هو عمل من أعمال التحقيق فقط، مما دفع كل من الفقه والقضاء إلى تعريف التفتيش،

([144]) المطيري، مرجع سابق: ص75.

([145]) أبو الوفا محمد أبو الوفا، المواجهة الإجرائية للجرائم المعلوماتية، ندوة بعنوان: جرائم تقنية المعلومات في ظل القانون الاتحادي رقم "2" لسنة 2006م، جامعة الامارات العربية المتحدة، دولة الامارات العربية المتحدة، ص13.

لهذا فإن التفتيش إما أن يكون عن المكونات المادية للحاسب الآلي، وإما أن يكون عن المكونات المعنوية مثل البيانات والمعلومات.

بما أن التفتيش يعتبر من إجراءات التحقيق الابتدائي الخطيرة التي تمس الحرية الشخصية، وينتهك مستودع سر الإنسان وراحته وهدوءه، كان لا بد من وضع شروط وضوابط لتنظيم التفتيش لضمان عدم التجاوز على حرية الأفراد وحرمة منازلهم، وهذه الشروط هي [146]:

أولاً–الشروط الموضوعية لتفتيش النظام المعلوماتي، والتي تنحصر في عدة أسباب كوجود سبب مباشر لتفتيش النظام المعلوماتي، فلا بد أن يكون التفتيش مشروعًا. أيضًا يجب تحديد محل التفتيش كشخص أو منزل أو غير ذلك.
ثانياً–الشروط والضوابط الشكلية لتفتيش الحاسب الآلي/ وهذه الضوابط يجب مراعاتها عند ممارسة هذا الإجراء وذلك صونًا للحريات الفردية من التعسف أو الانحراف في استخدام السلطة، ومن هذه الضوابط أن يكون الأمر بالتفتيش مسببًا؛ أي أن تكون هناك أدلة على وجود جريمة في المكان أو في حالة الضبط. أيضًا أن يكون الإذن بالتفتيش مكتوبًا. واشتراط التوقيع ممن أصدر الإذن وإثبات تاريخه. أيضًا تحديد نوع الجريمة ومحل التفتيش. كذلك تحديد مدة الإذن بالتفتيش ونطاقه. وأخيرًا تحرير محضر بتفتيش نظم الحاسب الآلي.

لهذا جاء القانون الفلسطيني وأشار على أن [147]:

- للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة.
- يجب أن يكون أمر التفتيش مسببًا ومحددًا، ويجوز تجديده أكثر من مرة ما دامت مبررات هذا الإجراء قائمة.
- إذا أسفر التفتيش في الفقرة 2 من هذه المادة عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة يتعين على مأموري الضبط القضائي تنظيم محضر بالمضبوطات وعرضها على النيابة العامة لاتخاذ ما يلزم بشأنها.

([146]) عادل عبدالله خميس المعمري، التفتيش في الجرائم المعلوماتية، بحث منشور، مجلة الفكر الشرطي، المجلد 22، العدد86، مركز بحوث الشرطة، الأمارات العربية المتحدة، 2013: ص12 وما بعدها.
([147]) المادة 33 من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية.

- لوكيل النيابة أن يأذن بالنفاذ المباشر لمأموري الضبط القضائي أو من يستعينون بهم من أهل الخبرة إلى أي وسيلة من وسائل تكنولوجيا المعلومات وإجراء التفتيش فيها بقصد الحصول على البيانات أو المعلومات.
- يشترط في مأمور الضبط القضائي أن يكون مؤهلًا للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية.

يتضح للباحثة من خلال ما سبق أنّ التفتيش يعتبر من أخطر الحقوق التي منحت للمُحقِّق وذلك لمساسها بالحريات التي تكفلتها الدساتير عادة، ولذا نجد المشرِّع يضع لها ضوابط عديدة سواء فيما يتعلق بالسلطة التي تباشره أم تأذن بمباشرتِه والأحوال التي تجوز فيها مباشرته وشروط اتخاذ هذا الإجراء بما يمثل ضمانات الحرية الفردية أو حرمة المسكن. وتكمن الفكرة الأساسية للتفتيش في إباحة انتهاك الحق في الخصوصية طالما أن هناك مبررًا في القانون لهذا الانتهاك، لذا فهو يعد من بين أقصى الصلاحيات التي قد تمارسها الدولة ضد المواطن ويعد أحد مظاهر تقييد الحريات الإنسانية التي ساهمت التشريعات الأساسية في دعم المحافظة عليها.

ثالثاً: سماع شهادة الشهود

يمكن القول أن شهادة الشاهد في الحقل المعلوماتي الخاص بهذه الجريمة يعتبر من أهم العوامل التي يمكنها الوصول للحقيقة مهما كانت شهادته قليلة أو غير كافية، فالشاهد يقول ما يعلمه، كما أنَّ الشاهد يعلم الكثير وجزء مما يعلم واقع ضمن إطار الخصوصية والسرية، حيث إن التنظيم القانوني للقواعد الإجرائية والإثباتية في الدعاوى المعتمدة على أدلة معلوماتية أو تتصل بعوالم التقنية والإلكترونيات يجب إعادة توصيفها قانونًا، بل وتنظيمها بشكل لا يضع الشاهد موضع المساءلة ولا يحرم القضاء فرصة الإفادة من شهادة الشاهد في أنّ الحقيقة التي تتوقف في أحيان كثيرة على ما يعلمه الشاهد بالخبرة النظرية لا ما يعلمه بالواقع من حقائق رآها أو سمعها أو نقلت له[148].

وقد نصت المادة رقم 80 من قانون الإجراءات الجزائية الفلسطيني رقم 3 لعام 2001 والمنشور في العدد 38 من الجريدة الرسمية على أنه: "يدلي الشهود بأقوالهم فرادى أمام وكيل النيابة بعد حلف

([148]) خاص موقع محاماة نت، لمحة قانونية على الإثبات في الجرائم الإلكترونية، موقع محاماة نت، نشر بتاريخ 2016/12/22، للتفاصيل:

https://www.mohamah.net/law

اليمين بحضور كاتب التحقيق، ويحرر محضر بإفادتهم والأسئلة الموجهة إليهم"[149]، حيث إن هذا الشاهد هو طرف محايد في الدعوى الجزائية، كما أن للمحقق أن يستمع إلى شهادة أي شاهد يحضر للمحكمة للإدلاء بشهادته من تلقاء نفسه [150].

من ناحية أخرى يجب على مأموري الضبط القضائي عدم إجبار الشاهد على حلف اليمين عند سماع أقواله، كونهم غير مخولين بذلك، فالجهة المخولة بتحليف الشاهد اليمين هي النيابة العامة والمحكمة فقط دون سواهما، وهذا ما أكَّده القانون الفلسطيني، وجعل سماع أقوال الشهود أمام مأموري الضبط القضائي دون حلف اليمين [151].

يعتبر الشاهد في جرائم الابتزاز الإلكتروني هو الفني صاحب الخبرة والمتخصص في تقنية الحاسب الآلي والشبكات، والذي تكون لديه معلومات جوهرية وهامة لازمة للدخول في نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق التنقيب عن أدلة الجريمة داخله، ويطلق على هذا الشاهد "المعلوماتي"، ويجب عليه تقديم كل المعلومات المهمة والجوهرية في كشف الحقيقة وأن يكون رجل الضبط الجنائي والمحقق لديهما الخبرة الكافية في أدلة الحاسب الآلي، وهذا الشاهد المعلوماتي يكون إما مكلفًا من قبل إحدى جهات التحقيق الأصلية ممثلة بهيئة التحقيق والادعاء العام، أو بناءً على أمر المحكمة، وفي كلا الحالتين يعد الأمر الصادر أمرًا قضائيًا، وفي حال قيام الفني بمباشرة عمله دون وجود الأمر القضائي فإن ما ينتج عن عمله من دليل يعد دليلًا غير مشروع، ويحق للمحكمة أن لا تأخذ به [152].

أما الشاهد الفني فلا يجوز له أن يلجأ إلى استخدام أساليب غير مشروعة للقيام بإنجاز عمله، بل يجب أن يكون أداء مهمته داخل الأطر المشروعة التي يحددها القانون، أما هذا الشاهد فإنه ينتمي إلى إحدى الفئات التالية: **أولهم** القائمون على تشغيل الحاسب الآلي وهم المسؤولون عن تشغيل الحاسب الآلي والمعدات المتصلة به، ويجب أن يكون لديهم خبرة في تشغيل الجهاز، واستخدام لوحة المفاتيح في إدخال البيانات بالإضافة إلى معلومات عن قواعد كتابة البرامج. **وثانيهم** المبرمجون وهم أشخاص متخصصون في كتابة أوامر البرامج وهم كاتبو برامج التطبيق وكاتبو برامج النظم. **وثالثهم** المحللون وهم أشخاص يحللون الخطوات وجمع بيانات نظام معين ودراستها وتحليلها لوحدات واستنتاج

([149]) المادة رقم 80 من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001م.
([150]) العفيفي، مرجع سابق: ص125.
([151]) المادة رقم 22/2 من قانون الإجراءات الجزائية الفلسطيني رقم 3 لعام 2001م.
([152]) المطيري، مرجع سابق: ص82-83.

العلاقات الوظيفية من تلك الوحدات. **ورابعهم** مهندسو الصيانة والاتصالات وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب وشبكاته. **وخامسهم** مديرو النظم وهم الذين توكل إليهم أعمال الإدارة في النظم المعلوماتية [153].

يتبين للباحثة بناءً على ما سبق بأن شهادة الشهود يمكن أن تكون إحدى منابع وأصول الدليل، وهي من أهم طرق الإثبات لجميع الجرائم خاصة الجرائم الالكترونية منها، فلا يحكم بهما إلا بإقرار أو شهادة بعد توافر شروطهما وضوابطهما الشرعية، ويشترط في الشاهد أن يكون أهلًا للشهادة ومع ذلك قد تتوافر فيه شروط الأهلية ويمنع من أداء الشهادة لوجود سبب من أسباب عدم الصلاحية.

وهكذا تعتبر جريمة الابتزاز الإلكتروني كباقي الجرائم التقليدية التي تمر بمراحل الإثبات والتحقيق لتأكيد حدوثها، حيث تحتاج إلى بحث المحقق عن الدليل المادي والمعنوي والمرور بمراحل الاستدلال والتحقيق الجنائي الكامل، إذا اختفت إحدى هذه الطرق اعتُبر العمل ناقصًا، فبدون هذا الدليل لا تثبت الجريمة ولا يمكن إسنادها إلى متهم؛ وبالتالي لن يطبق قانون العقوبات.

كما أنَّ طُرُقَ الإثبات في جرائم الابتزاز الإلكتروني عديدة وموجودة في كافة الجرائم التقليدية، لكنها تختلف بعض الشيء كون هذه الجرائم تتم بواسطة الحاسب الآلي وهي بالتالي أكثر تعقيدًا من الجرائم العادية التقليدية، لكنها تمر بعدة طرق منها المعاينة وهي الانتقال للمكان التي وقعت به الجريمة، وأيضًا التفتيش، وهو غاية وليس وسيلة وذلك للبحث في مستودع سر الشخص عن دليل يرتبط بالجريمة المرتكبة، كذلك سماع شهادة الشهود.

كما تمر القضية بعدة مراحل مثل: مرحلة التحقيق ومرحلة المحاكمة، أما مرحلة التحقيق تمر بمرحلتين هما: مرحلة التحقيق الابتدائي ومرحلة التحقيق القضائي، حيث حرص القانون الفلسطيني على تتبع تلك الإجراءات لضمان سير الدعوى بكل حيادية وشفافية، فقد تطورت الآن أساليب التحقيق من الضرب والتعذيب إلى استخدام الوسائل العلمية في التحقيق. مثل استثمار الحركات العصبية والضمادات والمناورة والمراقبة والوعد بمكافأة وغيرها.

وتعتبر قضية الابتزاز من الجرائم الخطيرة التي تمس الفرد والمجتمع على حد سواء، وتتطلب الحكمة في التعامل معها قبل التسرع بإصدار الأحكام والتهم، حيث تترك آثار قاسية على الفرد والمجتمع من

([153]) المرجع السابق: ص83.

خلال خلخلة الجانب الاجتماعي للمجتمع، والصدمات النفسية التي تتركها على الأفراد، والتمادي في الظلم والطغيان من قبل المجرمين في ابتزازهم، كما يتحول المجني عليه لأسير لرغبات الجناة. وبالتالي الخسائر الناجمة عن الابتزاز لا يمكن حصرها سواء أكانت مادية أم معنوية وهو ما يتطلب الوقوف عنده.

الفصل الثاني

عقوبة جريمة الابتزاز الإلكتروني في القانون الفلسطيني وصعوبة الكشف عنها: دراسة مقارنة مع القانونين المصري والأردني

مقدمة

تتم جريمة الابتزاز عادة عن طريق استخدام شخص وسائل وبرامج التواصل الإلكتروني، من أجل ارتكاب جريمة معينة لإلحاق الضرر والأذى بسمعة وكرامة أحد الأشخاص الذين تم استدراجهم من خلال تلك المواقع أو غيرها، حيث يستخدم المجرم تلك الوسائل التكنولوجية من أجل الاستحواذ على بعض المحتويات والمواد، سواء أكانت صوراً أم فيديوهات أم وثائق مختلفة تخص الضحية، سواء من خلال التسلل غير المشروع إليها، أم الحصول عليها بناء على ثقة الضحية، إلا أنه يستغل تلك الثقة وبدأ التهديد بنشر تلك المحتويات دون وجه حق، وقد تستخدم العصابات عدة طرق للإيقاع بالضحايا والحصول على محتويات وصور، ومن ثَم تهديد الضحية وابتزازه للحصول على مبالغ مالية، وقد يتم أيضًا الوصول إلى الضحية من خلال التسلل غير المشروع إلى جهاز الحاسوب أو الهاتف الشخصي، أو مثلًا قد يتم الابتزاز إذا ما فقد الهاتف وداخله محتويات خاصة، لهذا تعدّ جرائم الابتزاز كثيرة وأنواعها متعددة، ويشار إلى أنّ الجريمة الإلكترونية أصبحت شائعة في المجتمعات العربية خاصة المجتمع الفلسطيني والمصري والأردني محل الدراسة، وذلك بعد تطور التكنولوجيا في السنوات الأخيرة[154].

لهذا يتم التطرق في هذا الفصل إلى جريمة الابتزاز الإلكتروني في القانون الفلسطيني: دراسة مقارنة مع القانونين المصري والأردني، حيث سيتم من خلال المبحث الأول إبراز جريمة الابتزاز الإلكتروني في القانون الفلسطيني (عقوبتها وصعوبات الكشف عنها)، وذلك من خلال التعرف على قانون الجرائم الإلكترونية الفلسطيني (خلفية عامة). وتحديد عقوبات جريمة الابتزاز الإلكتروني في القانون الفلسطيني والصعوبات التي تواجه السلطات في الكشف عنها. أما المبحث الثاني فسوف نستعرض جريمة الابتزاز الإلكتروني في القانونين المصري والأردني، من خلال بيان جريمة الابتزاز الإلكتروني

([154]) ياسر محمد، الجريمة الإلكترونية.. إرهاب يتحدى الدول بالتكنولوجيا المتطورة، مرجع سابق.

في القانونين الأردني والمصري والعقوبة المقررة لها. كذلك التعرف على أوجه الاتفاق والاختلاف بين عقوبة جريمة الابتزاز الإلكتروني في كلٍّ من القانون الفلسطيني والقانونين المصري والأردني.

المبحث الأول: عقوبة جريمة الابتزاز الإلكتروني في القانون الفلسطيني (عقوبتها وصعوبات الكشف عنها)

على الرغم من الفوائد العديدة للتقنيات التكنولوجية الحديثة، إلا أنه لا يكاد يخلو من الضرر الذي يقع على مستخدمي هذه التقنيات، حيث تنتشر جرائم عديدة تختص بالابتزاز الالكتروني كالسرقة والتهديد والجرائم الجنسية والمادية وغيرها، ما يجعل مجرمي هذه التقنيات تحت الطائلة القانونية، فقد قام المشرع الفلسطيني بتوقيع عقوبات عديدة بحق هؤلاء المجرمين، منها ما يتعلق بالحبس لعقوبات متعددة، ومنها ما يتعلق بالغرامة المالية، وذلك لردع هؤلاء المجرمين عن القيام بمثل هذه الجرائم.

المطلب الأول: قانون الجرائم الإلكترونية الفلسطيني (خلفية عامة):

يعد التطور الكبير في تكنولوجيا المعلومات والاتصالات وظهور الشبكة العالمية "الإنترنت" أحد أهم مميزات العصر الحالي، حيث كان له العديد من الآثار الإيجابية في عدة جوانب مختلفة، فقد ساهم بشكل عام في تطور وتغيير نمط حياة الأفراد والمجتمعات، ولكن في المقابل كان لهذا التطور التكنولوجي الكبير العديد من الآثار السلبية الجانبية على حياة الناس والشركات والمؤسسات والدول أيضًا، وقد تمثل ذلك في استغلال الإنترنت والوسائل الإلكترونية لممارسة جريمة الابتزاز الإلكتروني بكافة تصنيفاتها، وهو ما جعل الجرائم الإلكترونية تظهر إلى الوجود، والتي يراها الخبراء بأنها الابن غير الشرعي للتكنولوجيا، والتي انتشرت بشكل واسع بحكم التزامن بين ثورة التكنولوجيا المعلوماتية والعولمة[155].

لهذا أجمع العديد من الأطراف ذات الصلة بهذا الموضوع بأنه الجرائم الإلكترونية ومنها جريمة الابتزاز الإلكتروني منتشرة في الأراضي الفلسطينية بصورة واضحة، وأن انتشارها بدأ منذ عدة سنوات، وبسبب عدم وجود قانون يحدد أنواع وعقوبات الجرائم الإلكترونية في السابق، كان من الصعب إيجاد بيانات رسمية موثوقة حول عدد الجرائم وأنواعها في الأراضي الفلسطينية، لكنه تبين أنه يوجد الكثير من الجرائم الإلكترونية في الأراضي الفلسطينية، وهذا بدوره يرجع إلى أن هذه الجرائم كان يتم تصنيفها

([155]) محمد خليفة، دراسة نقدية للإطار القانوني للجرائم الإلكترونية في الأراضي الفلسطينية، معهد أبحاث السياسات الاقتصادية "ماس"، رام الله، 2012: ص1.

تحت بند الجرائم الأخرى التي يوجد نصوص قانونية تجرمها وتضع عقوبة رادعة لها، فعلى سبيل المثال فإن جرائم التشهير على الإنترنت تصنف تحت بند جرائم القدح والذم، ومن الصعوبة بمكان معرفة عدد الجرائم الإلكترونية أو إعادة تصنيفها دون وجود القانون الذي يحدد ماهيتها وأنواعها والعقوبات المتعلقة بها[156].

اعتبرت الحكومة الفلسطينية أن هناك حاجة ماسة وقوية إلى وجود قانون للجرائم الإلكترونية، لا سيما في ظل الانتشار الواسع لوسائل الاتصال عبر الإنترنت، والذي رافقته حالات إخلال بالسلوك العام والتحريض والابتزاز عبر الإنترنت، وفي هذا السياق أشار المستشار القانوني للحكومة الفلسطينية "رامي الحسيني" بأنه: "تكمن أهمية القانون في سد الفراغ القانوني الهائل المتعلق بالجرائم الإلكترونية، لا سيما أنها تتزايد بشكل ملحوظ، وأن هذا القانون يهدف بالأساس إلى معاقبة من يسيئون استخدام التقنية، وأكد أن القانون يراعي الاتفاقيات الدولية والقوانين والتشريعات الفلسطينية[157].

صادق الرئيس محمود عباس بتاريخ 2017/6/24م على قرار بقانون الجرائم الإلكترونية المحال إليه من الحكومة بتاريخ 2017/6/20م، ونشر في الجريدة الفلسطينية "الوقائع الفلسطينية" في عددها الصادر بتاريخ 2017/7/9م، حيث نص القرار بقانون في مادته (61) على أن يجري العمل به اعتبارًا من تاريخ نشره في الجريدة الرسمية [158].

يتبين لنا مما سبق أن الحاجة كانت ماسة لإصدار قانون للحد من جريمة الابتزاز الإلكتروني في فلسطين، لما لهذا القانون من أهمية في الحد من مثل هذه الجرائم، خاصة بعد انتشارها بصورة ملفتة في الآونة الأخيرة، وعجز الحكومات عن التصدي لها مما استوجب العمل على سن قانون يحد من هذه الجرائم.

الفرع الأول: ردود الفعل الرسمية الفلسطينية بعد صدور القانون

جاءت ردود الحكومة الفلسطينية سريعة إثر صدور هذا القانون، حيث شدد الناطق باسم الشرطة الفلسطينية "لؤي زريقات على أن القرار جاء ليعالج الجرائم الإلكترونية التي ارتفعت معدلاتها في الأراضي الفلسطينية خلال السنوات الأخيرة، ففي عام 2015م بلغ عدد تلك الجرائم 502، وفي العام

([156]) المرجع السابق: ص5.

([157])الهندي، مرجع سابق: ص12.

([158]) عصام عابدين، جهود مؤسسة الحق في مواجهة قرار بقانون الجرائم الإلكترونية، مؤسسة الحق، رام الله، 2018: ص5.

2016 بلغ العدد 1327، وحتى منتصف العام 2017م تلقت الشرطة الفلسطينية 850 بلاغ عن الجريمة الإلكترونية، كما أكد زريقات أن جهاز الشرطة أسس وحدة مكافحة الجريمة الإلكترونية ضمن نطاق عمل إدارة المباحث العامة، وتم تزويدها بضباط متخصصين وإمكانيات لازمة من أجل متابعة هذه القضايا، وفي اللحظة التي تصل فيها الشكوى تتحرك الوحدة وتبدأ بإجراءات البحث، إضافة إلى أن الشرطة تقوم بدور توعوي في الجامعات والمدارس ومع الأهل، ومن خلال رسائل ونشرات توعوية وأفلام قصيرة لتوضيح الاستخدام الآمن للإنترنت[159].

كما أشار الدكتور عبد الكريم شبير بأن هذا القانون بالرغم من مساوئه القليلة ومنها أنه صدر في ظل الانقسام الفلسطيني، لكنه تمتع بالعديد من الإيجابيات ومنها أنه قام بردع كل من تسول له نفسه الإساءة للآخرين عبر مواقع التواصل الاجتماعي سواء أكان عن طريق القذف أم التشهير أم السب أم الابتزاز وغيرها، كما أن هذا القانون يضع حدًا للجرائم سواء الخاصة أو العامة، وسواء أكان على مستوى مرتكب الجريمة أم من تسول له نفسه بارتكاب جريمة جديدة، حيث تابع أيضًا بالقول بأن تصنيف هذه الجرائم وتكييفها ترجع للمحكمة التي تقرر ما يناسب الوقائع والأسباب المنسوبة لكل شخص، حسب طبيعة الجريمة والظروف الموجودة في قطاع غزة والضفة الغربية، ومكان وزمان ارتكاب الجريمة[160].

ومن ناحية أخرى أكدت كل من وزارة العدل الفلسطينية ومجلس الوزراء الفلسطيني أن قانون الجرائم الالكترونية الفلسطيني يلبي حاجة مجتمعية وطنية فلسطينية، خاصة بعد انتشار العديد من الجرائم في الآونة الأخيرة أهمها جرائم الابتزاز الإلكتروني، مما أضر بالنسيج الوطني الفلسطيني، حيث رأت كل من وزارة العدل ومجلس الوزراء أن هذا القانون يعمل على سد الفراغ التشريعي الهائل المتعلق بالجرائم الإلكترونية، كون قانون العقوبات المطبق سواء في قطاع غزة أم في الضفة الغربية لا يراعي التطورات التكنولوجية التي حصلت، وقد وفر هذا القانون الحماية اللازمة للمواطنين، من خلال تغليظ العقوبة على المجرم بما يصون الحرمات، وأكدوا أنَّ هذا القانون يراعي الاتفاقيات الدولية والقوانين والتشريعات الفلسطينية كافة[161].

([159]) أسامة الكحلوت، ما هو قانون الجرائم الإلكترونية؟، موقع دنيا الوطن، 2017/7/18، للتفاصيل:
https://www.alwatanvoice.com/arabic/news/2017/07/18/1068272.html

([160]) المرجع السابق.

([161]) المرجع السابق.

لهذا يتبين لنا مما سبق أن الردود الرسمية لإصدار هذا القانون كانت إيجابية، حيث أكد العديد من المسؤولين الفلسطينيين أن هذا القانون جاء ليلبي الحاجة الماسة لإصدار مثل هذه القوانين نظرًا لانتشار جريمة الابتزاز الإلكتروني بصورة كبيرة، مما أضر بالنسيج الوطني الفلسطيني، وعمل على تفكك المجتمع، كما أنه أحدث حالة فراغ تشريعي واضحة من جراء عدم وجود قانون يحمي الضحايا الذين يتساقطون بصورة كبيرة جرَّاءَ عدم وجود رادع للجناة.

الفرع الثاني: موقف المؤسسات المحلية والدولية من قانون الجرائم الالكترونية

منذ صدور القرار بقانون رقم (16) لسنة 2017م بشأن الجرائم الإلكترونية الصادر في تموز/ يوليو 2017م، تابعت الهيئات والمؤسسات المحلية والدولية عن كثب كافة الإجراءات والأحداث وردود الأفعال التي أعقبت صدور هذا القانون، حيث عبرت الهيئة المستقلة لحقوق الإنسان "ديوان المظالم" كإحدى المؤسسات المحلية التي تعمل في مجال حقوق الإنسان عن خشيتها وقلقها البالغ من القرار بصدور القانون، وذلك لما تضمنه –حسب تعبيرها– من أحكام ما من شأنها أن تشكّل تهديدًا خطيرًا للحق في حرية الرأي والتعبير، والحق في الخصوصية، وحرمة الحياة الخاصة للمواطنين، حيث طالبت ومعها العديد من مؤسسات المجتمع المدني بالعمل على تعديله بما يعزز من حقوق المواطنين وحرياتهم الأساسية، وبما ينسجم مع القانون الأساسي ومع التزامات دولة فلسطين على الصعيد الدولي، وقد شاركت الهيئة برفقة العديد من المؤسسات المحلية والدولة العاملة في فلسطين في العديد من جلسات الحوار مع الجهات الرسمية بهدف الوصول إلى تعديلات جوهرية على القرار، على نحو يوازن بين مكافحة الجرائم الإلكترونية وحماية الحقوق والحريات الأساسية للمواطنين[162].

من خلال مراجعتنا لقانون الجرائم الإلكترونية الفلسطيني لسنة 2017م يرى المركز الفلسطيني لحقوق الإنسان في دراسة أعدها أن المشرع الفلسطيني لم يلتزم بالمعايير الدولية المتعلقة بالحق في حرية التعبير، والحدود المتعلقة بصلاحية الدولة في فرض قيود عليها استنادًا للمعايير المختلفة وأهمها الأمن القومي، ويؤكد المركز أنّ القانون قد خالف التزامات فلسطين بموجب الفقرة (3) من المادة (19) من العهد الدولي للحقوق المدنية والسياسية، والتي تنص على أنه: "تستتبع ممارسة الحقوق المنصوص عليها في الفقرة 2 من هذه المادة واجبات ومسؤوليات خاصة. وعلى ذلك يجوز إخضاعها لبعض القيود ولكن شريطة أن تكون محددة بنص القانون وأن تكون ضرورية: (أ) لاحترام حقوق الآخرين أو سمعتهم، (ب) لحماية الأمن القومي أو النظام العام أو الصحة العامة أو الآداب العامة.

([162]) خاص الهيئة المستقلة لحقوق الإنسان "ديوان المظالم"، مذكرة قانونية: حول القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية، الهيئة المستقلة لحقوق الإنسان، 2018/5/20: ص1.

حيث وتفسير هذه الفقرة يوجد في العديد من المواثيق الدولية، أبرزها التعليق العام رقم (34) الصادر عن لجنة حقوق الإنسان، والإعلان المشترك الخاص بحرية التعبير والإنترنت لسنة 2011م، ومبادئ جوهانسبرج المتعلقة بالأمن القومي، وحرية التعبير والوصول للمعلومات لسنة 1996م، وقرار الجمعية العامة بإنشاء ثقافة عالمية لأمن الفضاء الإلكتروني لسنة 2003م[163]. حيث أجاز المشرع الفلسطيني حجب المواقع أو الروابط التي تهدد الأمن القومي أو السلم الأهلي أو النظام العام أو الآداب العامة، وبالتالي لها أن تطلب الإذن بحجب المواقع كليًا أو جزئيًا [164]، وهو ما اعتبرته هذه المؤسسات طمسًا لحرية التعبير.

من ناحية أخرى يقارن المركز الفلسطيني بين القانون الفلسطيني للجرائم الإلكترونية مع نصوص التجريم في بعض القوانين العربية مثل: القانون الكويتي والمصري والأردني، حيث يوضح أيضًا أن المشرع الفلسطيني قد أسهب في تنظيم الجرائم الإلكترونية بخلاف القانون الكويتي والمصري والأردني، حيث جاء القانون الفلسطيني لسنة 2017م في 61 مادة، التي تناولت الكثير من صور الاستخدام التي اعتبرها القانون غير مشروعة، وبالتالي اعتُبر القانون الفلسطيني أكثر تشددًا من القوانين الأخرى، حيث انتقى القانون الفلسطيني أسوأ النصوص والمصطلحات غير المنضبطة من القانون المصري وغيره من القوانين العربية، كما يرى المركز أن القانون الفلسطيني تميز بضعف الصياغات وعدم انضباط التجريم، بحيث يمكن من خلال القانون تجريم أفعال مشروعة بطبيعتها، مما يدلل على عدم الدقة والتسرع في وضع القانون[165]. وقد تم تعديل القانون الفلسطيني للجرائم الالكترونية سنة 2018م والمنشور في العدد الممتاز رقم (16) من الوقائع الفلسطينية بتاريخ 2018/05/03، ليصبح 57 مادة.

([163]) خاص المركز الفلسطيني لحقوق الإنسان، مراجعة لقانون الجرائم الإلكترونية الفلسطينية لسنة 2017 في ضوء المعايير الدولية لحرية التعبير، المركز الفلسطيني لحقوق الإنسان، أغسطس 2017: ص22.

([164]) المادة 39 من القرار بقانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية. حيث تنص المادة على أنه: "لجهات التحري والضبط المختصة إذا ما رصدت قيام مواقع إلكترونية مستضافة داخل الدولة أو خارجها، بوضع أية عبارات، أو أرقام، أو صور، أو أفلام، أو أية مواد دعائية، أو غيرها، من شانها تهديد الأمن القومي، أو السلم الأهلي، أو النظام العام، أو الآداب العامة أن تعرض محضراً بذلك على النائب العام أو أحد مساعديه، وتطلب الإذن بحجب الموقع أو المواقع الإلكترونية، أو حجب بعض روابطها من العرض.

يقدم النائب العام أو أحد مساعديه طلب الإذن لمحكمة الصلح خلال 24 ساعة مشفوعاً بمذكرة برأيه، وتصدر المحكمة قرارها في الطلب، في ذات يوم عرضه عليها إما بالقبول أو بالرفض".

([165]) خاص المركز الفلسطيني لحقوق الإنسان، مراجعة لقانون الجرائم الإلكترونية الفلسطينية لسنة 2017 في ضوء المعايير الدولية لحرية التعبير، مرجع سابق: ص23.

وجد القانون الفلسطيني للجرائم الإلكترونية الكثير من الاستهجان لدى المؤسسات المحلية التي رأت فيه مساسًا بالحريات العامة وخصوصية المواطنين، حيث صدرت ورقة تعبر عن موقف مركز الميزان لحقوق الإنسان بتاريخ 2017/9/12م، طالب بها بوقف العمل بهذا القانون، والعمل على تعديله بما ينسجم مع التزامات دولة فلسطين الناشئة عن الاتفاقيات التعاقدية لحقوق الإنسان، والعمل من أجل أي تعديل وبغض النظر عن مشروعيته القانونية والدستورية، منسجمًا مع نص وروح القانون الأساسي، مع الحفاظ على ضبط المصطلحات والألفاظ بما يحول دون احتمالها أكثر من وجه، وجعلها أداة قمع بيد السلطة للحريات المدنية والسياسية، والقرار رقم (68/167) الذي اعتمدته الجمعية العامة للأمم المتحدة في كانون الأول/ ديسمبر 2013م، بشأن عدم جواز التدخل في استخدام الأفراد للفضاء الإلكتروني[166].

لهذا يمكن القول بناء على ما سبق أن هذا القانون لاقى معارضة واسعة من عدة قطاعات خاصة داخل وخارج الأراضي الفلسطينية، خاصة مؤسسات المجتمع المدني التي رأت في هذا القانون فرصة كبيرة لتكميم الأفواه ومصادرة حرية الرأي والتعبير، وذلك من خلال إصدار عدة مواد داخل هذا القانون تعمل على تكميم أفواه المصلحين ورواد المواقع الإلكترونية، مما جعلهم يطالبون بتغيير العديد من مواده حتى يوافقوا عليه.

المطلب الثاني: عقوبات جريمة الابتزاز الإلكتروني في القانون الفلسطيني والصعوبات التي تواجه السلطات في الكشف عنها.

تواجه مجرمي الابتزاز الالكتروني عقوبات مشددة حسب القانون الفلسطيني، والذي استطاع أن يضع حدوداً وضوابطاً للحد من انتشار مثل هذه الجرائم التي تهدد أمن المجتمع وسلامته، حيث قام بوضع عدة مواد يمكن أن تصل عقوبة مجرمي الابتزاز إلى الحبس لعدة سنوات، أو غرامة كبيرة، وهو ما جعل العديد من القانونيين يعتبر هذا القانون بمثابة ردع لهؤلاء المجرمين.

الفرع الأول: عقوبات جريمة الابتزاز الإلكتروني في القانون الفلسطيني

لم يكن يوجد في فلسطين تشريعًا يكافح الجرائم الإلكترونية أو الجرائم التقليدية التي ترتكب بوسائل إلكترونية، حيث كان هناك حالة من الفراغ التشريعي في فلسطين بهذا الخصوص، إلى أن أصدر الرئيس محمود عباس رئيس دولة فلسطين القرار بقانون رقم (10) لسنة 2018م، والمنشور في العدد

([166]) خاص مركز الميزان لحقوق الإنسان، ورقة موقف حول التشريع الإلكتروني ومدى مراعاة الحقوق والحريات العامة، مركز الميزان لحقوق الإنسان، 2017: ص4

الممتاز رقم (16) من الوقائع الفلسطينية بتاريخ 2018/05/03، بشأن الجرائم الإلكترونية، والذي جاء لسد حالة الفراغ التشريعي في مجال الجرائم الإلكترونية، وبذات الوقت للحد من هذه الجرائم وخطورتها التي ازدادت في الآونة الأخيرة نتيجة التقدم التكنولوجي الهائل، كما أنه جاء أيضًا عدم ترك مرتكبي الجرائم الإلكترونية دون ملاحقة قانونية[167].

عند البحث عن النصوص والتشريعات العربية عمومًا تجاه جرائم الابتزاز الإلكتروني بصفة خاصة، والجرائم المعلوماتية بصفة عامة نجد أنّ هناك فراغًا تشريعيًا كبيرًا، حيث إن الغالبية من الدول العربية تفتقر إلى قانون لتجريم الجرائم المعلوماتية، لكن في الوقت ذاته هناك دول عربية قد تصدت لهذه الظاهرة بقوانين مستقلة[168]. ومن هذه الدول دولة فلسطين التي قامت بإقرار قانون لتجريم الجرائم الإلكترونية في العام 2017م، ومن ثم تم تعديله بقرار قانون رقم 10 لسنة 2018م، والمنشور في العدد الممتاز رقم (16) من الوقائع الفلسطينية بتاريخ 2018/05/03، وذلك بعد خروج أصوات تشجب وتدين هذا القانون الذي يمنع الحريات وبالتالي الاعتداء عليها.

لهذا وضع المشرع الفلسطيني عقوبات متباينة لكل جريمة إلكترونية، مع ملاحظة أنه عرّف الحبس بأنه وضع المحكوم عليه بحكم قضائي أحد سجون الدولة مدة تتراوح من أسبوع إلى ثلاث سنوات، في حين عرّف السجن بأنه وضع المحكوم عليه بحكم قضائي في أحد سجون الدولة مدة تتراوح بين ثلاث سنوات إلى خمس عشرة سنة [169].

ومع ذلك لم يضع القانون الفلسطيني تعريفًا محددًا للابتزاز أو التهديد، تاركًا مهمة تحديد الجزاء للفقهاء ولتقدير القضاء، حيث يمكن تعريف التهديد أو الابتزاز بأنه: "كل سلوك من شأنه بث الرعب أو الخوف في نفس شخص آخر من خطر يراد إيقاعه بشخصه أو بماله أو بشخص أو مال آخر يعنيه أمره، وباختصار يقصد به "الوعيد بالشر". هذه الجريمة تعني توجيه عبارة أو ما في حكمها إلى المجني عليه قصدًا يكون من شأنه إحداث الخوف في نفسيته [170].

([167]) براك، وجرادة، مرجع سابق: ص6.

([168]) خليل يوسف جندي، المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني: دراسة مقارنة، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركرك، العراق، المجلد7، العدد26، 2018: ص107.

([169]) المادة (1) من القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية.

([170]) براك، وجرادة، المرجع السابق: ص139.

لقد أثرت تكنولوجيا المعلومات على حق الحياة الخاصة للأفراد بفعل ما أتاحته من قدرات عالية على جمع ومعالجة وتبادل البيانات الشخصية في بيئتها، مما خلق مخاطر جديدة لتكنولوجيا المعلومات تهدد الحق في الخصوصية، هذا الابتزاز والتهديد تطلَّب معايير تشريعية وعقوبات رادعة منطلقة من حقوق جديدة تعرف بـ :"الخصوصية في البيئة الرقمية"، كما وأثرت تكنولوجيا المعلومات أيضًا على القواعد الموضوعية والإجراءات للقانون الجنائي فيما يتعلق بحماية المعلومات وأمن نظمها، وذلك لجهة التعامل مع الأنماط المستجدة من الجرائم الإلكترونية، ومع الوسائل الجديدة لارتكاب الأفعال إجرامية تقليدية في بيئة الكومبيوتر والإنترنت[171]. حيث يستطيع الشخص بواسطة التقنيات الحديثة الوصول إلى أي مكان يرغب فيه وفي أي زمان، وذلك عبر الإبحار في الشبكة المعلوماتية والتفاعل مع من يشاء دون قيود [172].

لم يغفل القانون رقم 3 لسنة 1996م بشأن الاتصالات السلكية واللاسلكية هذه الجريمة، لكنه ألغى العديد من المواد ضمنًا بعد صدور القرار بقانون رقم 15 لسنة 2009م بشأن الهيئة الفلسطينية لتنظيم قطاع الاتصالات، خاصة وأن العقوبات التي جاءت في القرار بقانون رقم 15 لسنة 2009م كانت أشد من تلك العقوبات التي جاءت في قانون رقم 3 لسنة 1996م، حيث جاءت المادة 93 بعقوبة الحبس من أسبوع إلى ستة أشهر أو الغرامة التي لا تزيد عن 1000 دينار لكل من أقدم على كتم رسالة عليه نقلها بواسطة شبكات الاتصال إلى شخص آخر أو رفض نقل رسائل منه أو أفشى رسالة أو عبث بالبينات المتعلقة بأحد المشتركين بما في ذلك أرقام الهواتف غير المعلنة والرسائل المرسلة أو المستقبلة[173].

وقد اهتم القانون الفلسطيني المعروف بـ "قانون رقم 15 لسنة 2009 بشأن الهيئة الفلسطينية لتنظيم قطاع الاتصالات" بتجريم بعض الأفعال المتعلقة بهذا الشأن، حيث نص القانون في العديد من مواده على عقوبة تلك الأفعال، من خلال عقوبة بالسجن أو عقوبة مالية تراوحت ما بين 200 دينار، و5000 دينار، حيث حددت المادة 52 من هذا القرار بقانون عقوبة نشر أو إشاعة مضمون أي اتصال بواسطة شبكة اتصالات أو رسالة هاتفية اطلع عليها بحكم وظيفته أو سجلها دون سند قانوني بالحبس من شهر إلى سنة، أو غرامة تتراوح بين 200–1200 دينار [174].

([171]) أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكومبيوتر والإنترنت، ط1، مكتبة الوفاء القانونية، الإسكندرية، 2011: ص285.

([172]) المادة (1) من القرار بقانون الجرائم الإلكترونية الفلسطيني رقم (10) لسنة 2018م.

([173]) المادة 93 من القانون رقم 3 لسنة 1996م بشأن الاتصالات السلكية واللاسلكية.

([174]) المادة 52 من قانون رقم 15 لسنة 2009 بشأن الهيئة الفلسطينية لتنظيم قطاع الاتصالات.

كما جاءت المادة 57 من هذا القرار بقانون أشد عقوبة تجاه كل من أقدم عبر وسائل الاتصالات على توجيه رسائل التهديد أو الإهانة أو الرسائل المنافية للآداب أو نقل خبر كاذب بقصد إثارة الفزع بعقوبة الحبس من شهر إلى ثلاث سنوات، وغرامة مالية لا تقل عن مائتي دينار [175]، كما نصت المادة 58 من هذا القرار بقانون على عقوبة اعتراض أو شطب محتويات الرسائل عبر شبكات الاتصالات أو قام بتشجيع غيره على هذا الفعل بالحبس من شهر واحد إلى ستة أشهر، أو غرامة من 200 إلى 1000 دينار [176].

أيضًا نظم القرار بقانون رقم (10) لسنة 2018م والمنشور في العدد الممتاز رقم (16) من الوقائع الفلسطينية بتاريخ 2018/05/03، في مادته رقم (15) بشأن الجرائم الإلكترونية من ناحية الابتزاز والتهديد، حيث نص على أنه: "كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في تهديد شخص آخر أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان هذا الفعل أو الامتناع مشروعًا يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني ولا تزيد على ألف دينار أردني أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين. وإذا كان التهديد بارتكاب جناية أو بإسناد أمور خادشه للحياء أو الشرف أو الاعتبار، يعاقب بالحبس لمدة لا تقل عن سنة أو بغرامة لا تقل عن مائتي دينار أردني ولا تزيد عن ثلاثة آلاف دينار أردني أو ما يعادلها بالعملات المتداولة قانونًا"[177].

لطالما راقبت السلطات الإسرائيلية عن كثب النشاط الفلسطيني عبر الإنترنت، من خلال سياسات الرقابة الجماعية لتقصّي الدعوات إلى المقاومة أو العنف، فضلاً عن استقصاء المعلومات التي يمكن استخدامها لإرغام الفلسطينيين على التعاون مع قوات الأمن الإسرائيلية. ويُستخدم مصطلح "إسقاط" بشكل شائع بين الفلسطينيين عند الإشارة إلى المُمارسات التي تقوم بها وحدات الاستخبارات الإسرائيلية مستخدمة معلومات أو صورًا يتمّ جمعها بهدف ابتزاز الفلسطينيين من أجل التعاون مع القوات الإسرائيلية، وقد تحدّث جنود سابقون في جيش الدفاع الإسرائيلي عن هذا الأسلوب، وهم يشيرون إلى أن وحدات الاستخبارات تنتهك حقوق الأفراد دون مُبرّر، وفي بعض الأحيان تبتزّ الأفراد لإرغامهم

([175]) المادة 57 من قانون رقم 15 لسنة 2009 بشأن الهيئة الفلسطينية لتنظيم قطاع الاتصالات.
([176]) المادة 58 من قانون رقم 15 لسنة 2009 بشأن الهيئة الفلسطينية لتنظيم قطاع الاتصالات.
([177]) براك، وجرادة، مرجع سابق: ص140.

على التعاون. وبسبب الموقف السلبي من المجتمع تجاه التوجهات الجنسية لدى البعض؛ فإن الجماعات ذات الميول المثلية جنسيًا هي الأكثر عرضة لهذا الابتزاز من أجل الـ "إسقاط"[178].

يمكن القول إن قانون الجرائم الإلكترونية رغم الاعتراضات الكثيرة على بعض نصوصه التي تحدُّ من حرية التعبير ولتضمنه نصوصًا فضفاضة، إلا أنه قد يشكل أداة رادعة للمبتزين والتمكن من الحفاظ على النسيج الاجتماعي من مثل هذا النوع من الجرائم الذي تزايد بشكل كبير خلال السنوات الأخيرة، إذ إن الأرقام لدى الشرطة الفلسطينية تؤكد تضاعف مثل هذا النوع من الجرائم عدة مرات من العام 2013 حتى صدور قانون الجرائم الإلكترونية عام 2017م. حيث أشار المستشار القانوني الدكتور علاء بني فضل بقوله: "يتضح من نص المادة 1/15 من القرار بقانون رقم 16 لسنة 2017 أن المشرّع عاقب على جريمة الابتزاز الإلكتروني بعقوبة الحبس أو الغرامة أو الاثنتين معًا؛ حيث إن ذلك يصب بالمصلحة العامة كون الجرائم الإلكترونية أسهل على المجرم ارتكابها، ولتمثل مثل هذه العقوبة رادعًا أمام المجرمين، لكن الحد من هذه الظاهرة يعتمد على التطبيق الفعلي لهذا القانون في المحاكم الفلسطينية"[179].

كما يهدف المتورطون في جرائم الابتزاز الإلكتروني إلى الحصول على المال، أو إلى جر الضحايا لعلاقات جنسية، أو توريطهم في شباك التعامل مع أجهزة الاحتلال الإسرائيلي، وذلك من خلال التهديد بنشر صور شخصية، أو نشر محادثات مكتوبة أو مكالمة صوتية، وقد يتم الحصول على هذه الصور والمحادثات من خلال اختراق الحسابات، وليس من خلال حوارات مباشرة، وذلك وفقًا للتحقيقات التي أجرتها الجهات المختصة في قضايا الابتزاز الإلكتروني. وبحسب قانون العقوبات الفلسطيني، رقم 3 لسنة 2009م معدل لقانون العقوبات رقم 74 لسنة 1936م المطبق في قطاع غزة، فقد حددت المادة رقم 3 عقوبة الحبس لمدة لا تزيد عن سنة، لكل من اقتحم نظامًا لمعلومات حاسوب خاص بغيره أو بقي فيه دون وجه مشروع، إضافة لغرامة لا تتجاوز ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا، أو بإحدى هاتين العقوبتين. وإذا نتج عن ذلك تعطيل تشغيل النظام أو محو المعلومات التي يحتوي عليها أو تعديلها، تكون العقوبة الحبس، وبغرامة لا تتجاوز ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونًا، أو بإحدى هاتين العقوبتين [180].

([178]) كيارا عياد، الأمن الرقمي لمراقبة من؟ قانون الجرائم الإلكترونية في فلسطين، ورقة عمل قدمت لمبادرة الإصلاح العربي: بدائل سياسات، تشرين الأول/ أكتوبر 2018: ص3.

([179]) مجد عقل، تفاقم ظاهرة الابتزاز الإلكتروني، هل يحلها قانون الجرائم الإلكترونية؟، موقع بيرزيت أونلاين، 2018/2/26، للتفاصيل http://online.birzeit.edu/articles/Article/445/ar

([180]) آلاء البرعي، الابتزاز الإلكتروني: "الشاباك" وباحثون عن الجنس والمال، موقع صوت الترا فلسطين، 2017/12/2، للتفاصيل: https://ultrapal.ultrasawt.com

لقد حرص المشرع الفلسطيني من خلال القانون بشأن الجرائم الإلكترونية خاصة جريمة الابتزاز الإلكتروني على معاقبة كل من يدخل بغير حق أو قام بانتهاك خصوصية الآخرين بأي وسيلة كانت، ويظهر ذلك من خلال المادة (4) من هذا القرار بقانون 2017 التي نصت على أنه[181]:
كل من دخل عمدًا من دون وجه حق بأي وسيلة موقعًا إلكترونيًا، أو نظامًا معلوماتيًا، أو شبكة معلوماتية، ووسيلة تقنية المعلومات، أو جزء منها، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك، يعاقب بالحبس، أو بغرامة لا تقل عن 200 دينار أردني، ولا تزيد عن ألف دينار أردني، أو العقوبتين كلتيهما.

إذا ارتكب الفعل المحدد في الفقرة (1) من هذه المادة على البيانات الحكومية، يعاقب بالحبس لمدة لا تقل عن ستة شهور أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد عن ألف دينار أردني، أو بالعقوبتين كليهما.

إذا ترتب على الدخول إلغاء أو حذف أو إضافة أو إفشاء أو إتلاف أو تغيير أو نقل أو إلحاق ضرر بالمستخدمين أو المستفيدين أو تغيير الموقع الإلكتروني أو انتحال شخصية، أو القائم على إدارته يعاقب بالحبس لمدة لا تتجاوز خمس سنوات وبالغرامة لا تقل عن ألف دينار ولا تزيد عن خمسة آلاف دينار.

إذا ارتكب الفعل المحدد في الفقرة (3) من هذه المادة على البيانات الحكومية، يعاقب بالأشغال الشاقة المؤبدة مدة لا تقل عن خمس سنوات وبغرامة لا تقل عن خمسة آلاف دينار أردني، ولا تزيد عن عشرة آلاف دينار أردني، أو بالعقوبتين كليهما.

لذلك يمكن القول إنه لا يشترط أن يكون لدى مرتكب جريمة التهديد والابتزاز الإلكتروني نية تحقيق الفعل المهدد بارتكابه؛ لأن التهديد جريمة قائمة بذاتها ويعاقب عليها القانون بسبب ما تحدثه من رعب في نفس الشخص المهدد، وإكراهه تحت وطأة التهديد التأثير في نفس المجني عليه، وأن يكون الجاني عالمًا بما يمكن أن يحدثه ذلك التهديد، أما بالنسبة للإرادة يتعين أن يثبت أن الجاني قد أراد العبارات

([181]) طميزة، مرجع سابق: ص302.

التي صدرت عنه، وأراد إبلاغها إلى المجني عليه وأراد أن تنتج تأثيرها على نفسيته، وليس من عناصر التهديد أن تتوافر لدى الجاني نية تنفيذ الأمر الذي هدد به[182].

أما فيما يتعلق بالعقوبة فقد نص الشارع على أن العقوبة تتضمن العديد من الأشخاص منهم[183]:

– كل من هدَّد أو ابتزَّ شخصًا بهدم مسكنه أو إيقاع الضرر بذلك المسكن قاصدًا بذلك تخويف الشخص أو ابتزازه أو إزعاجه.

– كل من أطلق عيارًا ناريًا أو ارتكب فعلًا من الأفعال الأخرى التي تكدر صوف الطمأنينة العامة قاصدًا بذلك تهديد أو ابتزاز أو إرعاب شخص يقيم في مسكن.

– كل من هدد شخصًا آخر بإلحاق الأذى بذاته أو بالنيل من سمعته أو بالإضرار بماله أو هدده بإلحاق الأذى بشخص ينتمي إليه أو النيل من سمعته قاصدًا بذلك حمله على القيام بفعل لا يفرض عليه القانون القيام به أو إغفال القيام بفعل يخوله القانون حق القيام به، يعد أنه ارتكب جنحة.

فضلاً عن ذلك قد تقع جرائم الابتزاز الإلكتروني على أسرار ومعلومات عن طريق اختراقها وتكون لتلك المعلومات والأسرار قيمة اقتصادية، الأمر الذي قد يسبب خسائر باهظة في الأموال والجهد الأمر الذي قد يؤدي إلى ابتزاز المجني عليه من قبل الجاني، خاصة أننا اليوم أمام انتشار واسع للحاسب الآلي، والذي لم يعد استخدامه مقتصرًا على المؤسسات المالية والاقتصادية والتجارية والشركات، بل أصبح في متناول أيدي الأفراد حتى في مدارسهم ومنازلهم، مما يتيح للجميع الاتصال به بصورة أو بأخرى، لا شكَّ أن الحاسب الحالي قد يكون مشروعًا أو غير مشروع[184].

يمكن القول إن هناك العديد من حالات الابتزاز التي وقعت في الأراضي الفلسطينية في الآونة الأخيرة، والتي لم يتهاون القانون في التصدي لها، حيث قضت محكمة صلح جنين المأذونة بإجراء المحاكمة وإصداره في القضية الموسومة بـ التهديد باستعمال الشبكة الإلكترونية أو إحدى وسائل التواصل خلافًا للمادة 15 ف1 من قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، حيث إن المتهم أسندت له تهمة التهديد باستخدام الشبكة الإلكترونية خلافًا للمادة 15 ف1، ومع إنكار المذنب بالتهمة المنسوبة إليه، ومع مراجعة ملفات القضية وجدت المحكمة أن المتهم اعترف بالتهم المنسوبة إليه، وقد قررت المحكمة إدانة المتهم بالتهمة المنسوبة إليه وهي التهديد باستعمال الشبكة

([182]) براك، وجرادة، مرجع سابق: ص142.

([183]) المادة (100) من قانون العقوبات رقم (74) المطبق في المحافظات الجنوبية.

([184]) محمد حماد الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر والتوزيع، عمان، الأردن،ط2، د.ت: ص156.

الإلكترونية خلافًا للمادة 15 ف1، والحكم بحبسه لمدة ثلاثة أشهر، وللمصالحة وإسقاط الحق الشخصي تحويل الحبس لغرامة بواقع نصف دينار عن كل يوم حبس(انظر الملحق رقم 1)*.

يتبين مما سبق أن المشرع الفلسطيني وضع في قانون الجرائم الإلكترونية العديد من المواد التي يمكنها أن تعمل على ردع الجناة في ارتكاب مثل هذه الجرائم، فقد شرع العديد من النصوص التي تعمل على الحد من عمليات الابتزاز الإلكتروني من ناحية والمس بحياة الأشخاص الشخصية والخاصة من ناحية ثانية، وجريمة التهديد والوعيد من ناحية أخرى، حيث تباينت العقوبات ما بين الحبس والغرامة، لذلك كان لفرض هذه العقوبات أثره الواضح في التقليل من حجم الجريمة.

الفرع الثاني: الصعوبات التي تواجه السلطات في الكشف عنها.

أولًا: حق الإنسان في الخصوصية.

مع تطور وسائل الاتصال، واستخدام أجهزة الكومبيوتر في هذا المجال، أصبحت المعلومات تتداول على الشبكات بشكل متزايد بحيث أصبح من الممكن إجراء عمليات تقاطع المعلومات بسرعة وفعالية، لا شك بأن لهذا التطور فوائده وحسناته، ولكن مساوئه لا سيما إذا ما تعلق الأمر بمعلومات تمس حياة الأفراد الخاصة، وقد بدأ الوعي لخطورة الكومبيوتر على حرمة الحياة الخاصة منذ سنوات عديدة، فتعالت صيحات العديد من الدول لإصدار قوانين تتعلق بحرمة الحياة الخاصة للمواطنين وحمايتها من مخاطر المعلوماتية [185].

لهذا يمكن القول إن موضوع الحرية الفردية للأشخاص تتعلق بمسألة إفشاء البيانات الإسمية بين دوائر الدولة، فانقسم الفقه الجزائي بين مؤيد ومعارض حول هذه المسألة، فمنهم من يصبغ صفة المشروعية على أنظمة دوائر الدولة في تبادل المعلومات المتعلقة بالأفراد انطلاقًا من فكرة ضبط أجهزة الدولة الحكومية وتحسين مستوى الإدارة، وضبط نفقات الدولة، أما الاتجاه الآخر فيعارض هذه الفكرة ويستند في ذلك للخوف من إمكانية المساس بالحرية الشخصية للأفراد واستغلال المقارنة بين البيانات لتحقيق أغراض غير تلك التي أعلن عنها، والتي تتمثل في النهاية بأنها عدوانًا على الحياة الخاصة للأفراد[186].

* والذي يشير إلى قرار محكمة بشأن إدانة متهم بتهمة التهديد باستعمال الشبكة الإلكترونية خلافًا للمادة 15 ف1.

([185]) الحسيناوي، مرجع سابق: ص64-65.

([186]) المرجع السابق: ص68.

كما اهتم المشرّع الفلسطيني بالحياة الخاصة للمواطنين، وذلك من خلال تجريم كل من يمس هذه الحياة بعقوبات مشددة لتكون رادعًا لهم بعد ذلك، حيث نصت المادة 22 فقرة 1 من قانون الجرائم الفلسطيني رقم 10 معدل لعام 2018م والمنشور في العدد الممتاز رقم (16) من الوقائع الفلسطينية بتاريخ 2018/05/03، على أنه: "يحظر التدخل التعسفي أو غير القانوني في خصوصيات أي شخص أو في شؤون أسرته أو بيته أو مراسلاته". أيضًا نصت الفقرة 2 من المادة ذاتها على أنه: "كل من أنشأ موقعًا أو تطبيقًا أو حسابًا إلكترونيًا أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات بقصد نشر أخبار أو صور أو تسجيلات صوتية أو مرئية، سواء أكانت مباشرة أم مسجلة تتصل بالتدخل غير القانوني في الحياة الخاصة أو العائلية للأفراد، ولو كانت صحيحة، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار، ولا تزيد عن ثلاثة آلاف دينار، أو ما يعادلها بالعملية المتداولة قانونًا، أو بكلتا العقوبتين [187].

يمكن القول إن هذا الحق الذي يملكه الشخص يمكن أن يؤدي إلى عدم تمكن السلطات المختصة من كشف الجريمة بسبب عدم وجود الحق لهم في التفتيش بسبب الحرمة الشخصية للأفراد، وبالتالي عدم قدرتهم على تحديد الجاني.

كما يتبين مما سبق أن المشرّع الفلسطيني لم يغفل هذا الموضوع، حيث إنه قام بتجريم كل من ينتهك الخصوصية للإنسان والمواطن، حيث فرض على أي شخص يقوم بانتهاكها غرامة مالية أو الحبس أو كلا العقوبتين، وهو ما يؤكد اهتمام القانون بحرمة الحياة الخاصة للأفراد.

وهنا نجد أن المشرع الفلسطيني قد جرّم المساس بحرمة الحياة الخاصة حرصاً على المبادئ التالية[188]:

1- الحفاظ على كيان الأسرة، ومن ثم الحفاظ على المبادئ والأخلاق المتعارف عليها.
2- الحد من تأثير شبكة الانترنت ووسائل تقنية المعلومات على المجتمع والحفاظ في نفس الوقت على الأسرة التي تعد إحدى مكونات المجتمع الأساسية.
3- احترام حرمة الحياة الخاصة والعائلية.

([187]) المادة 22 من قانون الجرائم الإلكترونية المعدل رقم 10 لسنة 2018م.

([188]) محمد علي سويلم، شرح قانون جرائم تقنية المعلومات رقم 175 لسنة 2018، دار المطبوعات الجامعية، القاهرة، ط1، 2019: ص389.

ثانيًا: نقص الخبرة الفنية لدى جهات التحقيق

من الصعوبات التي تواجه عملية استخلاص الدليل في الجريمة المعلوماتية نقص الخبرة لدى رجال الضبط القضائي أو أجهزة الأمن بصفة عامة، وكذلك لدى أجهزة العدالة الجنائية ممثله في سلطات الاتهام والتحقيق الجنائي، وذلك فيما يتعلق بثقافة الحاسب الآلي وكيفية التعامل معها، وذلك على الأقل في البلدان العربية، نظراً لان تجربة الاعتماد على الحاسب الآلي وتقنياته وانتشارها في هذه البلدان جاء متأخراً عن أوربا والولايات المتحدة، فقد أثبتت الوقائع بأن بعضاً من أعضاء الضبط القضائي قد أعانوا مجرمي المعلوماتية على ارتكاب جرائمهم عن جهل ومن دون قصد، بدلًا من ضبطهم وذلك بالنظر لعدم امتلاكهم المعرفة اللازمة للتعرف على مثل هذه الجرائم ووسائل ارتكابها[189].

إن المشكلة هي أن مأموري الضبط القائمين بالفعل وسلطات التحقيق الجنائي تنقصها الخبرة في الجريمة المعلوماتية، وأن اكتشاف هذه الجرائم والتوصل إلى فاعليها وملاحقتهم قضائيًا، لا يتطلب فقط الإلمام بأصول البحث الجنائي أو قواعد التحقيق القانونية، ولكن يجب الإلمام بأصول التحقيق الجنائي الفني في الجرائم التقليدية فضلًا عن مهارات خاصة تسمح باستيعاب تقنيات الحاسب الآلي من حيث برامجه، أنظمته، طبيعة الجريمة الواقعة عليه ومفرداتها، من احتيال الإلكتروني والقرصنة والاختراق والحماية، وكيفية كسر جدار الحماية وفيروسات الكومبيوتر، ونظم استعمال ومعلومات دولية وغيرها من مصطلحات يمكنه عن طريقها التعامل مع هذه الجريمة المتفردة في خصوصيتها، وكذلك التعامل مع المجرم المعلوماتي وهو مجرم ذات طبيعة خاصة يتعين فهم كيفية التعامل معه، ويزيد من التحدي الذي تواجهه أجهزة العدالة الجنائية في جرائم الحاسب الآلي وجرائم الإنترنت، أنَّ الجناة في هذه الجرائم لهم المفردات والمصطلحات الخاصة بهم، لدرجه أنهم يطلقون على أنفسهم اسم (النخبة) بدعوى أنهم الأكثر معرفة بأسرار الحاسب الآلي ولغاته المتميزة، ويطلق على رجال الشرطة والنيابة والقضاء صفة الضعفاء[190].

على الرغم من قلة الخبرة والنقص في الأمور الفنية التي يجب أن يكون العاملون في هذا المال مؤهلين بما فيه الكفاية للتعامل مع هذه القضايا، إلا أن المشرّع الفلسطيني اهتم بهذه الناحية، حيث

([189]) محمد الأمين البشري، التحقيق في الجرائم المستحدثة، ط1، الرياض، 2004: ص107.

([190]) جاسم خريبط خلف، صعوبات الدليل الجنائي في الجرائم المعلوماتية، قسم القانون، كلية شط العرب الجامعة، العراق، د.ت: ص23.

بين ضرورة أن يكون ذو الاختصاص مؤهلًا وذا خبرة كافية، وقد بينت المادة 32 فقرة 4 على ضرورة الاستعانة بأهل الخبرة في المعاينة والتفتيش وغير ذلك من الأمور، حيث نصت المادة على أنه: "لوكيل النيابة أن يأذن بالنفاذ المباشر لمأموري الضبط القضائي أو من يستعينون بهم من أهل الخبرة إلى أي وسيلة من وسائل تكنولوجيا المعلومات، وإجراء التفتيش فيها بقصد الحصول على البيانات أو المعلومات". أيضًا أوضحت الفقرة 5 من نفس المادة على أنه: "يشترط في مأمور الضبط القضائي أن يكون مؤهلًا للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية"[191].

حيث نرى أن جهات البحث والتحري التي يقوم بها رجال الضابطة القضائية مقبلين على الانتقال من مرحلة التعامل مع الأدلة المادية الملموسة إلى مرحلة التعامل مع الأدلة الرقمية الالكترونية، والتي انتشرت في جميع أنحاء العالم الافتراضي مجهولة المصادر، مما دفع عطوفة النائب العام إلى استحداث نيابة أطلق عليها نيابة الجرائم الالكترونية، مكانها مقر النيابة العامة في مدينة رام الله[192].

يمكن القول إن هذه المشكلة تنتشر بصورة كبيرة لدى جهات التحقيق في الدول العربية، وهو الأمر الذي يتطلب القيام بدورات عديدة ومكثفة للحصول على الخبرة الفنية في عمليات التحقيق.
كما أن القانون الفلسطيني لم يغفل هذا الجانب، حيث اهتم بضرورة وجود الخبرة الفنية والتأهيل الكافي للعاملين في هذا الحقل، وذلك كي يكونوا على استعداد كامل للتعامل مع هذه القضايا المعقدة.

ثالثًا: عدم ظهور الدليل المادي

إن أغلب الآثار المتخلفة عن هذه الجرائم هي آثار إلكترونية، وهذه الآثار بدوها إنما هي عبارة عن نبضات إلكترونية غير مرئية بالعين المجردة، فهي تصل في حجمها وشكلها ومكان تواجدها إلى درجة شبه منعدمة بحيث إنه لا يمكن رؤيتها إلا من خلال الاستعانة بأجهزة ووسائل تقنية تظهرها للعيان (193)، فضخامة حجم وكم البيانات والملفات الإلكترونية التي تتواجد في البيئة الإلكترونية تصعّب من إمكانية تحديد الملفات والبيانات الإلكترونية المجرمة، من بين ذلك الكم الهائل لفصلها عن تلك البريئة منها، وتؤدي في الغالب إلى اصطدام مهمة الاكتشاف بحق الأفراد في الخصوصية الشخصية، كما أن البيئة المعلوماتية غالبًا ما تكون مؤلفة من شبكات منتشرة في كافة أرجاء المعمورة ومرتبطة

([191]) المادة 32 من قانون الجرائم الإلكترونية المعدل رقم 10 لسنة 2018م.
([192]) محمد علي سويلم، مكافحة الجرائم الالكترونية، دار المطبوعات الجامعية، القاهرة، ط1، 2019: ص591.
([193]) إبراهيم محمد منصور، الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية، دار النهضة العربية، القاهرة، 2002: ص191.

ببعضها البعض عن طريق شبكة الإنترنت ، بحيث تتيح الفرصة أمام مجرمي المعلوماتية للولوج عن بعد إلى البيانات الإلكترونية المخزونة في أية بقعة من بقاع العالم[194].

ولصعوبة استخلاص الدليل في مثل هذه الجريمة يرى المختصون في جرائم الحاسب الآلي أن هذا الجهاز وما يقع علية من جرائم معلوماتية يعد تحديًا هائلًا لرجال الأمن، ذلك أن رجل الأمن غير المتخصص والذي انحصرت معلوماته في جرائم قانون العقوبات بصورته التقليدية من قتل وضرب وسرقة لن يكون قادراً على التعامل مع الجريمة المعلوماتية التي تقع بطريقة تقنية عالية وإذا كانت المصادفة من الأمور التي يعول عليها في كشف الجريمة المعلوماتية، فإنّ وجود أجهزة الرقابة أو التدقيق داخل جهة الإدارة، سواء أكانت حكومية، أم خاصة أم شركة من الشركات، سوف يؤدي إلى كشف وقوع هذه الجريمة، ومن ثم إظهار الدليل الخفي الذي تتسم به مثل هذه الجرائم، شريطة أن يكون الجهاز الذي يتولى هذه الرقابة ذا تخصص وخبرة عالية في التعامل مع أجهزة الحاسب الآلي وبرامجها، وعالمً بأحداثها وطرق التعامل معها، سيما وأن المجرم في هذه الجريمة لدية الخبرة الفنية والمعرفة الكافية التي تمكنه من اقتراف جريمته[195].

يرجع السبب في افتقاد الآثار التقليدية لجريمة الابتزاز الإلكتروني إلى أن هناك بعض العمليات التي يتم إدخال بياناتها مباشرة في جهاز الحاسب الآلي، دون أن يتوقف ذلك على وثائق أو مستندات يتم النقل منها، كما لو كان البرنامج معدًا ومخزنًا على جهاز الحاسب. وبالتالي الوسيلة التي ترتكب بها الجريمة الإلكترونية توضع ضمن قالب غير تقليدي، نظرًا لأن ارتكابها يتم عن طريق نقل المعلومات على شكل نبضات إلكترونية غير مرئية تنساب عبر أجزاء الحاسب الآلي. وتستفيد الكيانات الإجرامية من مادية الآثار، والمعالم التي يمكن الاستدلال من خلالها على وقوع جريمة مادية، ونسبتها إلى شخص أو أشخاص محددين[196].

لهذا يمكن القول بناء على ما سبق أن اختفاء آثار الدليل المادي يمكن أن يؤدي إلى صعوبة تحديد الجناة، حيث إن الجرائم الإلكترونية تستخدم من خلال الحاسب الآلي وهو ما يؤدي إلى إمكانية حذف الآثار المادية التي يمكن العثور عليها على جهاز الكومبيوتر من صور وبيانات وأفلام وغير ذلك من مستندات.

([194]) خلف، مرجع سابق: ص9.

([195]) المرجع السابق: ص9-10.

([196]) نسرين فوزي اللواتي، صعوبات اكتشاف "الجريمة الإلكترونية"، موقع لغة العصر، 2017/12/10، للتفاصيل: http://aitmag.ahram.org.eg/News/86864.aspx

وهذا يدعونا إلى القول أن مفهوم الدليل الرقمي إنما يقتصر على ما يتم استخراجه من الحاسب الآلي ومن غيره من الأدلة مثل الهاتف وآلات التصوير وغيرها من الأدلة والأجهزة الرقمية التي تعتمد على التقنية الرقمية في تشغيلها بحيث تكون مصدراً للدليل الالكتروني[197].

رابعًا: ضعف التعاون الدولي في مواجهة الجريمة المعلوماتية

إن غياب سياسة التعاون الدولي والتنسيق بين الدول في مقاومة الجريمة المعلوماتية يقابله في ذات الوقت تعاون واضح بين محترفي الإجرام المعلوماتي، ففضلًا عن البرامج التي يستعين بها القراصنة في أنشطتهم الإجرامية ، فإنهم يتعاونون فيما بينهم ويتبادلون النصائح والخبرات فيما يتعلق بأنشطتهم مما يزيد من فاعلية وخطورة هجومهم وخصوصًا في ظل قصور وعدم فاعلية سياسة الدفاع الخاصة والمنفردة ضد الجريمة المعلوماتية[198].

ما زال التعاون الدولي لمكافحة الجرائم المعلوماتية على وجه العموم دون المستوى المطلوب، وذلك لعدم وجود اتفاقية دولية صادرة عن الأمم المتحدة في مكافحة هذا النوع من الجرائم، أما على المستوى الإقليمي فهنالك عدد من الاتفاقيات الدولية مثل اتفاقية بودابست لمكافحة الجرائم المعلوماتية والتي صدرت بتاريخ 2001/11/23، وهي خاصة لدول الاتحاد الأوروبي، وفي الإطار العربي صدرت عن جامعة الدول العربية اتفاقية حديثة عن مكافحة الجرائم المعلوماتية سميت "الاتفاقية العربية لمكافحة جرائم المعلومات"، حيث وافق على الاتفاقية مجلس وزراء الداخلية العرب بتاريخ 2010/12/21م، ودخلت حيز التنفيذ في 2011/2/7م بعد مصادقة الدول الأطراف عليها، وتعد هذه الاتفاقية نقطة تحول في التعاون العربي لمكافحة هذه الجرائم[199].

يمكن القول إنه يجب أن يتم تعاون دولي حثيث لمكافحة الجريمة الإلكترونية خاصة في عصر المعلومات التي تنتشر به المعلومة من ناحية ويقابلها الجريمة من ناحية أخرى، مما سيكون من الأولى التنسيق والتعاون بين الدول للحد من انتشار هذه الجرائم.

([197]) ميسون خلف حمد الحمداني، مشروعية الأدلة الالكترونية في الإثبات الجنائي، مجلة كلية الحقوق، جامعة النهرين، العراق، المجلد 18، العدد2، كانون الثاني لسنة 2016: ص196.

([198]) خلف، المرجع السابق: ص14.

([199]) الحوامدة، مرجع سابق: ص29.

أما الحالة الفلسطينية فهي مختلفة عن الحالات الأخرى مع نظيراتها في الدول العربية، فمن أهم الصعوبات التي تواجهها في الكشف عن هذه الجرائم الشرائح الإسرائيلية المشفرة، والتي يصعب كشفها والتعامل معها، حيث تطرق الأستاذ مالك الوحيدي وكيل نيابة في محافظة الخليل في مقابلة مع الباحثة للإجابة من جانب استخدام المتهم للشرائح الإسرائيلية، الذي بين أنها تعتبر من ضمن استخدام الشرائح للشركات التابعة للشبكات الأجنبية التي تم النص عليها في قانون الاتصالات السلكية واللاسلكية الفلسطيني رقم 3 لسنة1996 في المادة 90 الفقرة الأولى منه إضافة إلى التعليمات الصادرة عن وزارة الاتصالات الفلسطينية بهذا الخصوص ، أما بالنسبة للجانب الأردني تعتبر شبكات أجنبية عن فلسطين ولكن يوجد اتفاق بين الجانب الأردني والجانب الفلسطيني، ولا تعتبر حيازة الشريحة الأردنية جريمة حتى لو استخدمت في الابتزاز الإلكتروني، أما بالنسبة للجانب الإسرائيلي لا يوجد أي تعاون بينهم وبين الجانب الفلسطيني، فيتم عن طريق رجال الضابطة الجمركية أثناء قيامهم بالجولات التفتيشية للمحلات الخلوية بضبط الشرائح وتحرير المحضر وإحالتها إلى النيابة العامة، بعد ذلك يتم عرض هذه الشرائح على مديرية الاتصالات الفلسطينية لتقوم بتزويد النيابة العامة بتقرير يبين لها منشأ هذه الشرائح، حتى يتم التحقيق مع حائزها وإحالته إلى المحكمة[200].

فهذه الشرائح الإسرائيلية بالإضافة إلى الضرر الذي يلحق بالاقتصاد الوطني الفلسطيني من جراء استخدام شرائح تعود إلى شركات غير مسجلة بالأراضي الفلسطينية أصبحت تستخدم كأداة في تنفيذ الجرائم الإلكترونية حيث يقوم المتهم بابتزاز وتخويف وإثارة الرعب والفزع للمجني عليه ومن ثم صعوبة الوصول إليه وذلك لأنها تخرج من دائرة السيطرة الأمنية الفلسطينية. تتم ملاحقة المتهم ليس لحيازته الشريحة الإسرائيلية لأن النص في المادة 90 من القانون نفسه لا يعتبر حيازة الشريحة الإسرائيلية من قبل المواطنين جريمة يعاقب عليها القانون وهذا يعتبر نقصًا تشريعيا، على المشرع الفلسطيني تعديله حتى يسهل عمل النيابة العامة في إلقاء القبض على من يحوز مثل هذه الشرائح واستخدامها كأداة في حصول الجريمة وصعوبة ملاحقته.

فقضايا الابتزاز الإلكتروني التي تستخدم فيها عادة الشرائح الإسرائيلية لا يمكن التوصل إلى نتيجة في التحقيق وذلك لغياب التعاون الأمني من الجانب الإسرائيلي. إضافة إلى ذلك تحدث الأستاذ مالك الوحيدي أن الإتجار في مثل هذه الشرائح وتزويدها ببطاقات شحن، يعتبر جريمة استنادًا للمادة 90 من القانون نفسه [201]

([200]) ابراهيم أبو كامش، فضاء الانترنت في فلسطين تنخره السرقة والابتزاز والاحتيال والتشهير، صحيفة حياة وسوق، السنة الثانية، العدد 56، 2012/6/2: ص2.
([201]) المرجع السابق: ص2.

الفرع الثالث: نموذج تطبيقي لاستخدام قانون الجرائم الإلكترونية الفلسطيني المعدل لسنة 2018م.

القضية الأولى: قضية ابتزاز إلكتروني (انظر ملحق رقم"2")*

موضوع القضية: النيابة العامة تتمكن من الحصول على إدانة في قضية ابتزاز إلكتروني

فحوى القضية: أدانت محكمة صلح بيت لحم بهيئة القاضي سلام عقيل، واستنادًا إلى البيانات التي قدمتها النيابة العامة بحق المتهم (و.ق) بتهمة استعمال الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في تهديد شخص أو ابتزازه خلافًا لأحكام المادة 15/1 من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وحكمت عليه بالحبس لمدة سنة.

وجاء الحكم بناءً على المرافعات الخطية التي قدمتها نيابة بيت لحم أمام المحكمة ممثلة بوكيل النيابة العامة في نيابة بيت لحم الأستاذة نورة براهمة.

التاريخ: 2018/9/5

المكان/ رام الله

التحليل:

عند النظر إلى القضية يلاحظ أنها مرتبطة ارتباطًا وثيقًا بالجرائم الإلكترونية بصفة عامة، وجريمة الابتزاز الإلكتروني على وجه الخصوص، وذلك من خلال تناولها لتهمة الدخول غير المشروع لموقع إلكتروني، وتهديد وابتزاز رواده، حيث بينت هذه القضية نشاط المتهم الإجرامي الذي استخدم به التقنية الإلكترونية بصورة مباشرة كوسيلة لتنفيذ فعله الإجرامي، ونجد أيضًا من خلال النظر إلى هذه القضية توفر الركن المادي والمعنوي للجريمة، حيث يتمثل الركن المادي بوجود حساب للمتهم استطاع الدخول عن طريقه للشبكة الإلكترونية، وتم تهديد الضحية من خلال ذلك وابتزازه، وهو ما انطبق على المتهم وتوافر ذلك الشرط وانطبق مع الركن المادي للجريمة الإلكترونية. كما يمكن أن يتوفر الركن المعنوي للجريمة من خلال الإرهاب والخوف الذي عاد على الضحية جراء ابتزازه.

كما تعتبر المرافعات الخطية التي تدين المتهم هي أقوى أدلة الإثبات، كون الإقرار صادر عن الشخص الذي عليه الحق، وفي هذا دليل على استعداده لقبول الحكم وأداء الحق، كما توفرت صحة الإقرار الخطي بالمتهم، حيث إنه شخص بالغ عاقل مُمَيِّز ومعلوم. وقد توافرت هذه الشروط في المتهم الذي اعترف خطيًا بارتكابه جريمة الاختراق الإلكتروني ومن ثم الابتزاز للضحية.

* والذي يشير إلى صورة عن صحة النيابة العامة بشأن قضية ابتزاز إلكتروني.

كما تتوفر في القضية الأدلة والقرائن التي تدل على إثبات الجريمة وهي كالتالي:

ما ورد في تقرير النيابة العامة من وجود إدانة واضحة وكاملة للمتهم بتوارد عدد من الأدلة التي قدمتها النيابة والتي أدت لحبسه سنة.

ما قدمته النيابة من مرافعات خطية رسمية تثبت تورط المتهم في الولوج إلى الحاسب الآلي وابتزازه للضحية.

ونتيجة لما سبق فقد انتهى التحقيق إلى توجيه الاتهام للجاني بمخالفة أحكام المادة 15/1 من القرار بقانون رقم 10 لسنة 2018م والمنشور في العدد الممتاز رقم (16) من الوقائع الفلسطينية بتاريخ 2018/05/03، بشأن الجرائم الإلكترونية، وقيامه بالدخول غير المشروع لموقع إلكتروني وابتزاز رواده، ولذلك ينطبق على المتهم العقوبة المقررة عليه وهي السجن لمدة عام.

ومن خلال ما تقدم ومناقشة جريمة الابتزاز الإلكتروني، قد أوضحت المادة الخامسة عشر من قرار بقانون رقم (16) لسنة 2017م بشأن الجرائم الإلكترونية الفلسطيني: أنَّ كلَّ من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في تهديد شخص آخر أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان هذا الفعل أو الامتناع مشروعًا، يعاقب بالحبس أو بغرامة لا تقل عن ألفي دينار أردني ولا تزيد عن خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما. وهذا ما ينطبق على القضية، كون المدَّعى عليه قام بالاعتراف باختراقه للبريد الإلكتروني للمدعِي، ثم قام بابتزازه بأي فعل سواء بنشر صور أو سرقة معلومات أو تهديد أو غير ذلك، وفي هذه الحالة يجوز التعزير والحكم طبقًا لرؤية القاضي.

وهكذا تنتشر جريمة الابتزاز الإلكتروني في الأراضي الفلسطينية بصورة واضحة، حيث بدأ انتشارها منذ عدة سنوات، مما جعل المشرّع الفلسطيني يقوم بسن قانون يجرّمها، حيث اعتبرت الحكومة الفلسطينية أن هناك حاجة ماسة لوجود مثل هذا القانون، خاصة في ظل الانتشار الواسع لوسائل الاعلام وما رافقها من اختلال منظومة القيم والأخلاق مما استوجب سن قانون للحد من انتشار هذه الجريمة بين أفراد المجتمع.

كانت الردود الرسمية الفلسطينية إثر سَنِّ قانون الجرائم الإلكترونية الفلسطيني لسنة 2017م لتؤكد أنَّ مثل هذه القوانين كفيلة للحد من هذه الجريمة، خاصة أن عدد جرائم الابتزاز الإلكتروني في السنوات

الأخيرة في الأراضي الفلسطينية تجاوز المئات، مما استوجب سن هذا القانون الذي يمكنه الوقف أو التقليل من هذه الظاهرة، ويلبي الحاجة المجتمعية في مثل هذا القانون.
وعلى الرغم من ذلك واجه هذا القانون معارضة شرسة من مؤسسات المجتمع المدني من ناحية والمؤسسات والأحزاب السياسية المتعددة من ناحية أخرى، وذلك بحجة أنَّ مثل هذا القانون يحدُّ من حرية الرأي والتعبير في الأراضي الفلسطينية، حيث طالبت العديد من هذه المؤسسات بتعديل القانون انطلاقًا من أنَّ الكثير من مواده التي يحتوي عليها تؤكد على القمع وتكتيم الأفواه.

ومع زيادة الأصوات المطالبة بتعديل هذا القانون، صدر قانون معدل للجرائم الإلكترونية في العام 2018م وصادق عليه الرئيس الفلسطيني محمود عباس، حيث جاء هذا القانون لتعديل بعض النقاط محل الخلاف والتي ثارت حولها التصريحات والخلافات، وقد صدر قرار بقانون رقم 10 معدل لسنة 2018م ليجُبَّ ما قبله، وليؤكدَ على تجريم كل من تسول له نفسه بالتلاعب بالأمن وحياة المواطنين وحرمتهم عن طريق سوء استخدام الوسائل التكنولوجية.

فرض القانون الفلسطيني الذي صادق عليه الرئيس محمود عباس والمختص بالجرائم الإلكترونية الكثير من العقوبات الرادعة بحق من تسول له نفسه بارتكاب هذه الجرائم، وقد تراوحت هذه العقوبات بين السجن من ثلاثة أشهر إلى خمس سنوات، وأيضًا غرامات مالية بحق الجناة وصلت إلى ألفي دينار أردني، كما أن المادة 15 من قانون الجرائم الإلكترونية المعدل لعام 2018م والمنشور في العدد الممتاز رقم (16) من الوقائع الفلسطينية بتاريخ 2018/05/03، قد حدد عقوبة جريمة الابتزاز الإلكتروني بغرامة مالية لا تقل عن 200 دينار أردني ولا تزيد عن ألف دينار أردني أو ما يعادلها بالعملة المتداولة قانونًا أو بكلتا العقوبتين، أو بالحبس مدة لا تقل عن سنة. وهو ما يؤكد أن هذه العقوبات يمكنها أن تحدَّ من هذه الجريمة التي انتشرت بصورة واسعة. كما واجهت السلطات المختصة في التحقيق في هذه الجرائم عدة صعوبات في الكشف عن هذه الجريمة منها: حق الإنسان في الخصوصية، ونقص الخبرة الفنية لدى جهات التحقيق، وعدم ظهور الدليل المادي، وضعف التعاون الدولي في مواجهة الجريمة المعلوماتية وغيرها.

المبحث الثاني: جريمة الابتزاز الإلكتروني في القانونين المصري والأردني

اهتمت العديد من التشريعات في الدول العربية بالجرائم الالكترونية نظراً للتطور الهائل في وسائل التكنولوجيا الحديثة في السنوات الأخيرة، حيث قامت هذه الدول بتشريع عدة قوانين تجرّم استخدام هذه الوسائل بطرق غير مشروعة، فقد انتشرت العديد من الجرائم الالكترونية في هذه الدول مما جعلها تعمل على الحد من هذه الجرائم بتشريع قوانين رادعة، ومن هذه الجرائم جريمة الابتزاز الالكتروني التي انتشرت بصورة غير مسبوقة في الأعوام الأخيرة، مما جعل بعض الدول ومنها الأردن ومصر تلجأ لسن قوانين للحد منها، حيث يمكننا التعرف على هذه القوانين في الأردن ومصر من خلال الدراسة.

المطلب الأول: جريمة الابتزاز الإلكتروني في القانونين المصري والأردني والعقوبة المقررة لها:

لقد قرر كل من القانون المصري والقانون الأردني عقوبات متباينة على مرتكبي جرائم الابتزاز الالكتروني، على الرغم من أن كلاهما لم يتطرق صراحة لمصطلح ابتزاز الكتروني، برغم أن القانون الأردني قد نص صراحة في بعض المواد على عقوبة الابتزاز الالكتروني، أما القانون المصري فلم ينص صراحة على مصطلح ابتزاز، حيث استعاض عنه بكلمة تهديد وغيرها من المصطلحات، وفي هذه الدراسة سوف يتم التطرق لجريمة الابتزاز في كل من القانونين المصري والأردني وعقوبة كل منهما.

الفرع الأول: جريمة الابتزاز في القانون المصري والعقوبة المقررة لها:

أولاً: جريمة الابتزاز الإلكتروني في القانون المصري (خلفية عامة):

أصدر الرئيس المصري عبد الفتاح السيسي، 14 أغسطس/آب 2018م، قرارًا جمهوريًا رقم 175، بالتصديق على قانون "مكافحة جرائم تقنية المعلومات"، والمنشور في الجريدة الرسمية العدد 32 مكرر (ج) بتاريخ 14 / 8 / 2018، كأول تشريع مصري، يخاطب الجرائم التي تتم عبر شبكة الإنترنت، حيث عرف القانون المكون من 45 مادة، تقنية المعلومات بأنها أي وسيلة أو مجموعة وسائل مترابطة أو غير مترابطة تستخدم لتخزين، واسترجاع، وترتيب، وتنظيم، ومعالجة، وتطوير، وتبادل المعلومات أو البيانات، ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة سلكيًا أو لاسلكيًا.

وأعطى القانون لجهات التحقيق المختصة، سلطة حجب المواقع، متى قامت أدلة على قيام موقع يبث من داخل الدولة أو خارجها، بوضع أية عبارات أو صور أو أفلام، أو أية مواد دعائية أو ما في حكمها، تشكل تهديدًا للأمن القومي [202].

وحدد القانون التزامات وواجبات مقدم الخدمة؛ في حفظ وتخزين سجل النظام المعلوماتي أو أي وسيلة لتقنية المعلومات لمدة 180 يومًا متصلة، إلى جانب المحافظة على سرية البيانات التي تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة، ويشمل ذلك البيانات الشخصية لأيٍّ من مستخدمي خدمته، أو أية بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التي يدخل عليها هؤلاء المستخدمون أو الأشخاص والجهات التي يتواصلون معها، وتأمين البيانات والمعلومات بما يحافظ على سريتها وعدم اختراقها أو تلفها. وتضمن القانون 29 عقوبة تتراوح بين السجن من 3 شهور وحتى 5 سنوات، والغرامة التي تبدأ بـ 10 آلاف جنيه وحتى 20 مليون جنيه [203].

وكشف أمين سر لجنة حقوق الإنسان في جمهورية مصر العربية "شريف الورداني"، أنه تم ضبط قرابة 200 ألف حالة تحرش منذ 2016، وحتى عام 2018م، منها 50 حالة ابتزاز جنسي على مواقع التواصل الاجتماعي كل 10 أيام بحسب إحصائيات وزارة الداخلية. حيث إن الجناة أصبحوا يلجؤون لمواقع التواصل الاجتماعي لاصطياد الضحية باستخدام أسماء وحسابات وهمية، وفى كثير من الأحيان يتطور الأمر إلى حد الابتزاز والتشهير، مطالبًا بتطبيق القانون عليهم وتوعية الفتيات بكيفية التعامل مع هذا الفضاء الإلكتروني، وفقًا لقانون "مكافحة الجرائم الإلكترونية" الذي لم يغفل مثل هذه الجرائم، ويعاقب بالحبس مدة لا تقل عن 6 أشهر، وغرامة لا تقل عن 3 آلاف جنيه، ولا تزيد على 5 آلاف جنيه، أو بإحدى هاتين العقوبتين كل من تعرض للغير في مكان عام أو خاص أو مطروق بإتيان أمور أو إيحاءات أو تلميحات جنسية أو إباحية سواء أكان بالإشارة أم بالقول أم بالفعل بأية وسيلة بما في ذلك وسائل الاتصالات السلكية أو اللاسلكية، وفقًا لقانون العقوبات المصري[204].

يعتبر وجود قانون ينظم التعاملات الإلكترونية ويعاقب على الجرائم المرتكبة بالإنترنت أمرًا بديهيًا لا غنى عنه، ولكن لما لهذا القانون من أهمية وعلاقة مباشرة بحرية الرأي والتعبير والنشر التي يكفلها

([202]) الرئيس المصري يصدر قرارا بشأن جرائم الإنترنت، موقع sputnik عربي، 2018/8/18، للتفاصيل: https://arabic.sputniknews.com

([203]) المرجع السابق.

([204]) خاص صحيفة المصري اليوم، نائب: 50 حالة ابتزاز جنسي كل 10 أيام على مواقع التواصل الاجتماعي، موقع صحيفة المصري اليوم، 19-06-2018، للتفاصيل:
https://www.almasryalyoum.com/news/details/1301069

الدستور المصري بموجب المواد 65، 70، 71 ينبغي على المشرع اتخاذ الحيطة اللازمة في سن هذا التشريع حتى لا ينتقص القانون من هذه الحريات أو يقيدها، لهذا فالدراسة بصدد مناقشة وتحليل مشروع قانون مكافحة الجريمة الإلكترونية المصري أمام مجلس النواب لوضع اليد على مواطن الضعف في هذا المشروع وما يجب تعديله قبل إقراره حتى يؤدي الدور المنوط به دون المساس بالحريات، وحتى لا يصبح امتدادًا لسلسلة من التشريعات التي صدرت قبل هذا القانون وتضمنت ثغورًا على تلك الحريات والانتقاص منها وتسببت في العديد من الأزمات. وفي نفس الوقت يتضمن هذا القانون عددًا من النقاط الإيجابية والتي ينص عليها القانون المصري لأول مرة في مثل هذه الجرائم (205).

وقد خصصت وزارة الداخلية المصرية الرقم المجاني للإبلاغ عن أي جريمة ابتزاز تصادف الفتيات أو الشبان، حيث بينت أنه يجب الاحتفاظ بالرسائل التي تحتوي على السب أو القذف ثم التوجه إلى قسم شرطة الاتصالات التابع له وتقديم بلاغ بالواقعة وإثبات نص هذه الرسائل بالمحضر، وإن أمكن طباعة صورة لهذه الرسائل وإثبات رقم الهاتف الذي وردت منه هذه الرسائل، وسيجري إحالة المحضر إلى النيابة المختصة والتي تصدر قرارها بالاستعلام عن رقم الهاتف المبلغ عنه لمعرفة اسم مالك هذه الرقم وبياناته. ولابد أن يقدم البلاغ في خلال ثلاثة أشهر، طبقًا لنص المادة 3 من قانون الإجراءات الجنائية، والتي تنص على أنه: "لا يجوز أن ترفع الدعوى الجنائية إلا بناء على شكوى شفهية أو كتابية من المجني عليه أو من وكيله الخاص، إلى النيابة العامة أو إلى أحد مأموري الضبط القضائي في الجرائم المنصوص عليها في المواد في قانون العقوبات، وكذلك في الأحوال الأخرى التي ينص عليها القانون، ولا تقبل الشكوى بعد ثلاثة أشهر من يوم علم المجني عليه بالجريمة وبمرتكبها ما لم ينص القانون على خلاف ذلك [206].

لهذا يجب القول إن الحاجة الماسة لوقف جرائم الابتزاز الإلكتروني التي انتشرت في مصر كانت الدافع الكبير وراء تنظيم وإصدار هذا القانون الذي بدأ بتأدية دوره المنوط به في مكافحة الجرائم الإلكترونية التي أضرت بقيم وأخلاق وعادات المجتمع المصري، وأصبحت داءً انتشر في كافة أنحاء الجمهورية مما استلزم من المشرّع المصري إصدار مثل هذا القانون.

([205]) أحمد رجب، قراءة لمشروع قانون مكافحة الجريمة الإلكترونية: تحليل للإشكاليات القانونية بالمشروع وتأثيرها على الحريات، المركز المصري لدراسات السياسة العامة، مصر، مايو 2016: ص3.

([206]) اميمة سعيد، لحالات التهديد والابتزاز الإلكتروني.. خطوات تقديم شكوى لمباحث الإنترنت، موقع صحيفة الوطن الإلكترونية،2018/12/9، للتفاصيل: https://www.elwatannews.com/news/details/3855054

ثانياً: العقوبة المقررة لجريمة الابتزاز الإلكتروني في القانون المصري

بعد موافقة مجلس النواب المصري على مشروع القرار الذي قدمته الحكومة بشأن مكافحة جرائم تقنيات المعلومات، أصبح هذا القانون هو الأول من نوعه في مصر في هذا المجال، وقد نص القانون على فرض عقوبات رادعة تصل إلى السجن أو الغرامة المالية الباهظة ضد مستخدمي الإنترنت والشركات مقدمة الخدمة في حال إساءة استخدامها ومخالفة القانون، حيث يكلف القانون رئيس المحكمة الجنائية المختصة بإصدار أوامر بضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات، وتتبعها في أي مكان، أو نظام، أو برنامج، أو دعامة إلكترونية، أو حاسب تكون موجودة فيه، ويتم تسليمها للجهة المنفذة للأمر، في حال كان لذلك فائدة في إثبات ارتكاب جريمة تستلزم العقوبة بمقتضى أحكام هذا القانون، كما تتضمن تلك الأوامر البحث والتفتيش، والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقًا لغرض الضبط، وكذلك أمر مقدم الخدمة بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتي أو جهاز تقني، موجودة تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمي خدمته، وحركة الاتصالات التي تمت على ذلك النظام أو الجهاز التقني أو في نطاقه[207].

نظرًا لخطورة جريمة الابتزاز الإلكتروني، والتي تتمثل ابتداءً بالعالمية من خلال شبكات الاتصال والتواصل وسهولة التخلص منها وتأثيرها الكبير والواسع على أمن الوطن والمواطن، حرص المشرّع المصري أيضًا على تضمين قانون مكافحة جرائم تقنية المعلومات لسنة 2018م والمنشور في الجريدة الرسمية العدد 32 مكرر (ج) بتاريخ 14 / 8 / 2018 نصوصًا تضمن ملاحقة مرتكبي هذه الجرائم، وهو الأمر الذي تم النص عليه في القانون المصري المشار إليه أعلاه في المادة الثالثة منه أن: "مع عدم الإخلال بأحكام الباب الأول من الكتاب الأول من قانون العقوبات، تسري أحكام هذا القانون على كلِّ من ارتكب خارج جمهورية مصر العربية من غير المصريين جريمة من الجرائم المنصوص عليها من هذا القانون، متى كان الفعل معاقبًا عليه في الدولة التي وقع بها تحت أي وصف قانوني، وذلك في أي من الأحوال الآتية: 1- إذا ارتكبت هذه الجريمة على متن أي وسيلة من وسائل الجوي أو البري أو المائي، وكانت مسجلة لدى جمهورية مصر العربية أو تحمل علمها. 2-إذا كان المجني عليهم أو أحدهم مصريًا. 3-إذا تم الإعداد للجريمة أو التوجيه أو التخطيط أو تمويلها في جمهورية مصر العربية. 4-إذا ارتكب الجريمة بواسطة جماعة إجرامية في أكثر من دولة من بينها جمهورية مصر العربية. 5-إذا كان من شأن الجريمة إلحاق أي ضرر بأي من مواطني جمهورية مصر العربية

([207]) عبدالبصير حسن، مجلس النواب المصري يقر قانون مكافحة الجريمة الإلكترونية، موقع بي بي سي عربي، القاهرة، 7 يونيو/ حزيران 2018، للتفاصيل: http://www.bbc.com/arabic/middleeast-44396471

أو المقيمين بها. 6-إذا وُجد مرتكب جريمة في جمهورية مصر العربية بعد ارتكابها ولم يتم تسليمه [208].

كما اهتم المشرّع المصري بتطبيق العقوبة على مرتكبي هذه الجريمة، حيث بيَّن في المادة الرابعة عشر من القانون سالف الذكر أنه: "يعاقب بالحبس مدة لا تقل عن 6 أشهر وبغرامة لا تقل عن 30 ألف جنيه ولا تجاوز 50 ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتي مستخدِمًا حقًا مخولًا له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول."[209].

كما فرض المشّرع المصري عقوبات رادعة لكل من يقوم بالاعتداء على حرمة الأشخاص الخاصة، ويقوم بتهديدهم وابتزازهم، فقد وضحت المادة (25) من هذا القانون على أن: "يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا يتجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعتدى على أيٍّ من المبادئ أو القيم الأسرية في المجتمع المصري، أو انتهك حرمة الحياة الخاصة أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات إلى نظام أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقته أو بالقيام بالنشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، لمعلومات أو أخبار أو صور وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء أكانت المعلومات المنشورة صحيحة أم غير صحيحة"[210].

وعن مسألة العقوبة في جرائم القذف والسب، يمكن القول: "إنه من المقرر بنص المادة 306 من قانون العقوبات المعدلة بالقانون رقم 95 لسنة 1996م "كل سب لا يشتمل على إسناد واقعة معينة بل يتضمن بأي وجه من الوجوه خدشًا للشرف أو الاعتبار يعاقب عليه في الأحوال المبينة بالمادة 171 بالحبس مدة لا تجاوز سنة وغرامة لا تقل عن ألف جنيه ولا تزيد عن خمسة آلاف جنيه أو إحدى هاتين العقوبتين"[211].

كما تنص المادة 308 من ذات القانون على أنه: "إذا تضمن العيب أو الإهانة أو القذف أو السب الذي ارتكب بإحدى الطرق المبينة في المادة "171" طعنًا في عرض الأفراد أو خدشًا لسمعة العائلات تكون العقوبة الحبس والغرامة معًا في الحدود المبينة في المواد (179، 181، 182، 303، 306،

([208]) طميزة، مرجع سابق: ص15.

([209]) المادة رقم (14) من قانون مكافحة جرائم تقنية المعلومات المصري لسنة 2018م.

([210]) المادة رقم (25) من قانون مكافحة جرائم تقنية المعلومات المصري لسنة 2018م.

([211]) المادة 306 من قانون العقوبات المصري المعدلة بالقانون رقم 95 لسنة 1996.

307) على ألَّا تقلَّ الغرامة في حالة النشر في إحدى الجرائد أو المطبوعات عن نصف الحد الأقصى وألا يقل الحبس عن ستة شهور"[212] (للتفاصيل انظر الملحق رقم 3)*.

كما فرض المشّرع المصري عقوبات رادعة بحق كل من يقوم بابتزاز غيره أو ربط محتويات منافية للآداب بشخصية فرد معين، حيث نص ذلك في المادة (26) من القانون ذاته بأنه : "يعاقب بالحبس مدة لا تقل عن سنتين ولا تجاوز خمس سنوات وبغرامة لا تقل عن مائة ألف جنيه لا تجاوز 300 ألف جنيه أو بإحدى العقوبتين كل من تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها بمحتوى مُنافٍ للآداب العامة أو لإظهارها بطريقة من شانها المساس باعتباره أو شرفه"[213].

وفي حادثة شهدتها منطقة المقطّم في مصر جريمة بشعة حين أقدم شاب على قتل أبيه، وبرر جريمته أمام النيابة بأن والده كان يصور مقاطع فيديو لوالدته أثناء معاشرتها، وعندما انفصلا عن بعضهما هددها بنشر المقاطع على يوتيوب إذا لم تتنازل عن المؤخر وبعض الممتلكات الخاصة بها، وهو ما فتح الطريق أمام المشرّع المصري لتغليظ العقوبة على مرتكبي هذا النزع من الابتزاز، كون توقف هذه الجريمة يستتبعه توقف جرائم أخرى كالقتل والسرقة والزنا وغيرها [214]

كما أن وزارة الداخلية المصرية قد اهتمت بهذا النوع من الجرائم، حيث إنَّه وفي واقعة جديد تم تبليغ الإدارة العامة لتكنولوجيا المعلومات من المدعوة/ ريم م. ع–مقيمة بمنطقة المرج بالقاهرة، بتضررها من مستخدم هاتف محمول "محدد". لقيامه بإرسال رسائل للهاتف الخاص بها عبر تطبيق "واتس آب" تتضمن صور خاصة بها بملابس منزلية وعبارات تهديد وابتزاز بطلب تصوير نفسها صور ومقاطع فيديو عارية مقابل عدم نشر الصور المشار إليها.

بالفحص أسفرت الجهود أن وراء ارتكاب الواقعة المدعو/حسام م. ص–مواليد 1995، عامل زراعي ومقيم بمحافظة البحيرة. وعقب تقنين الإجراءات والتنسيق مع قطاع الأمن العام ومديرية أمن البحيرة تم استهداف المذكور وضبطه بمحل إقامته، وبالتفتيش تبين قيامه باستخدام برامج اختراق، واستيلائه من

([212]) المادة 171 من قانون العقوبات المصري المعدلة بالقانون رقم 95 لسنة 1996.

* وهو يشير إلى شرح المواد المذكورة أعلاه من خلال قرار محكمة مصرية بخصوص قضية قذف وتشهير في الصحف والجرائد.

([213]) المادة رقم (26) من قانون مكافحة جرائم تقنية المعلومات المصري لسنة 2018م.

([214]) الدستور تفتح ملف الابتزاز العاطفي في مصر، موقع صحيفة الدستور، 18 فبراير 2017، للتفاصيل: https://www.dostor.org/1310954

خلالها على (1003) حسابات لأشخاص آخرين عبر موقع "فيس بوك" وكذا وجود تطبيق يستخدم في إنشاء وتمرير أرقام هواتف محمولة دولية وهمية تستعمل في تطبيقات المحادثات المختلفة بغرض صعوبة رصده أو التوصل إليه. وبمواجهة المتهم المذكور اعترف بارتكاب الواقعة وعديد من الوقائع المماثلة، وذلك بغرض ابتزاز أصحاب تلك الحسابات للاستفادة منهم ماديًا، وقد تم اتخاذ الإجراءات القانونية اللازمة حيال الواقعة [215].

يتبين مما سبق أنَ المشرع المصري فرض عقوبات شديدة على كل من تسول له نفسه ارتكاب جناية ابتزاز إلكتروني أو أي جريمة معلوماتية، حيث إنه قام بفرض عقوبات قاسية للحد من ارتكاب هذه الجريمة تراوحت ما بين السجن لفترة تصل إلى خمس سنوات، إلى الغرامة المالية التي تخطت في بعض الأحيان 200 ألف جنيه مصري، وبالتالي إنَّ الجمع ما بين السجن والغرامة المالية من شأنه أن يعمل على ردع الجاني عن ارتكاب جريمته.

الفرع الثاني: جريمة الابتزاز في القانون الأردني والعقوبة المقررة لها

لقد اهتم المشرع الأردني بجريمة الابتزاز الالكتروني، وقام بتجريم كل من تسول له نفسه بالقيام بمثل هذه الجرائم أو نشرها بين أفراد المجتمع، لما لهذه الجرائم من خطورة على الفرد والمجتمع والسلامة العامة والأمن الوطني، وهو ما جعل المملكة الأردنية تعمل على إصدار قانون لتجريم مرتكبي هذه الجرائم.

أولاً: جريمة الابتزاز الإلكتروني في القانون الأردني (خلفية عامة)

تعتبر الأردن من الدول العربية المتقدمة التي تكافح كافة أنواع الجرائم وتفرض لها عقوبات قاسية بحق مرتكبيها، وذلك تبعًا للجريمة المرتكبة ومدى خطورتها وموقعها بين الجرائم، ومدى تأثيرها على المجتمع، لهذا تعد الأردن من الدول المتطورة نسبيًا والتي جاء في قوانينها ما يكفل ويحمي الأشخاص الذين يتعرضون إلى ابتزاز وتهديد، وأيضًا معاقبة المجرم، فهو تسلسل يهدف الى الحفاظ على أمن وكيان المجتمع، فكثير من المجرمين يعتقدون أن العقاب لن يطالهم أولًا لعدم وجود قوانين عربية صارمة، وعدم تعاون الدول في إلقاء القبض على المجرمين أو لنوع الجريمة المخفي الذي يعتمد على إرهاب الضحية، وبث الرعب في داخله، وبالتالي لن يتجرأ في التواصل مع الجهات المختصة، لكن يفاجئ الكثير من المجرمين وبمجرد الإبلاغ عنهم، أنهم أصبحوا في قبضة العدالة، وبالتالي أحالتهم

[215] خاص موقع وزارة الداخلية المصرية، ضبط أحد الأشخاص لقيامه بالاستيلاء على عدد كبير من الحسابات على موقع فيس بوك، والاستيلاء على البيانات واستغلالها في ابتزازهم مادياً، 2019/3/7، للتفاصيل:
https://moi.gov.eg/News/GetDetails?newsId=e6b41437-bbdb-41db-be72-b376040a0407

إلى جهات تنفيذ القانون لإيقاع العقوبة الرادعة بحقهم، تطبيقاً لما نصت عليه نصوص القوانين المنظمة لتلك المسائل[216].

لهذا نرى أن الابتزاز أو التهديد إنما يتمثل بالاستغلال غير المشروع للأسرار الشخصية أو الحياة الخاصة للأفراد، ومن ثم يشكل اعتداءً عليها، وفي هذه الحالة يستغل الجاني ما يحصل عليه من معلومات وأسرار لها علاقة بالحياة الخاصة للمجني عليه أو الضحية، وذلك من أجل تحقيق منافع ومكاسب مادية ومعنوية، وذلك بتهديد الشخص صاحب هذه الأسرار عن طريق إفشائها في حالة عدم تحقيق أو إجابة طلبه[217].

ونشير إلى أن فعل التهديد أو الابتزاز إنما يتحقق إما بطريق القول المباشر أو غير المباشر للشخص الضحية صاخب المعلومات السرية الخاصة أو يتحقق فعل التهديد أو الابتزاز بالكتابة في أية صورة خاصة كالرسائل الالكترونية، إضافة إلى ذلك حتى يتحقق فعل الابتزاز أو التهديد يجب أن يؤدي إلى إفشاء هذه الأسرار الخاصة للضحية إلى الرهبة والخوف لديه، مما يؤدي إلى الإضرار به سواء من الناحية المادية أو الناحية المعنوية. وأخيراً يشترط لتحقيق فعل الابتزاز أو التهديد أن يكون الهدف من هذا الابتزاز والتهديد هو الحصول على منفعة غير مشروعة، في حين إذا كان الهدف هو الحصول على منفعة مشروعة مثل استيفاء دين له في ذمة المهدد، فإن فعل الابتزاز أو التهديد لا يقع في مثل هذه الحالة، إنما يعاقب القانون في هذه الحالة على جريمة استيفاء الحق بالذات[218].

لهذا تتمثل الجرائم الإلكترونية بصورة عامة وجرائم الابتزاز الإلكتروني بشكل خاص، والمنتشرة بكثرة في جرائم الذم والقذف والابتزاز، حيث يرتكب الجاني عن طريق جهاز الحاسب الآلي أو الهاتف المحمول، وذلك كإرسال رسائل نصية بها عبارات تلصق صفة سيئة بالمجني عليه، أو تشبيهه بحيوان، أو ابتزازه بصفات سيئة، وقد ترتكب هذه الجريمة بإرسال ملفات صوتية أو صور أو غيرها من الوسائل الإلكترونية الحديثة بهدف ابتزاز المجني عليه[219].

بالرجوع إلى جرائم أنظمة المعلومات الأردني والتي تتعلق كثير منها بالابتزاز سواء أكان المالي أم الجنسي أم الأخلاقي أم غير ذلك، يمكن القول إن المشرّع الأردني أحسن حينما تدخل وحسم الجدل

([216]) عقوبة جريمة الابتزاز في المملكة الأردنية الهاشمية، موقع مكافحة الابتزاز والتهديد الإلكتروني، 2016/10/13، للتفاصيل: https://www.antiextortion.net

([217]) أسامة المناعسة، وجلال الزعبي، وصايل الهواوشة، جرائم الحاسب الآلي والانترنت، دار وائل للنشر، عمان، ط1، 2001: ص226.

([218]) المرجع السابق: ص226.

([219]) يوسف حسن يوسف، الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، القاهرة، ط1، 2011: ص206.

الفقهي في طبيعة الجرائم الإلكترونية، إذ إنَّه عالج صورًا متعددة من هذه الجرائم، وحدد لها عقوبات رادعة ومنها: الجرائم المتعلقة بالحياة الخاصة للمواطنين كجريمة التقاط أو اعتراض أو التصنت على المرسل من خلال النظام الإلكتروني أو الابتزاز الجنسي في المادة (5) من القانون الأردني الخاص بالجرائم الإلكترونية لعام 2015م والتي تنص على أنه: "يعاقب كل من قام قصدًا بالتقاط أو باعتراض أو بالتنصت أو شطب محتويات على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) الف دينار"، كذلك عالج جريمة نشر أعمال إباحية تتعلق بالاستغلال الجنسي لمن لم يكمل الثامنة عشرة من العمر، أو ترويج هذه الأعمال بمقتضى المادة (8) من نفس القانون والتي تنص على أنه: "تضاعف العقوبة على الجرائم المنصوص عليها في المواد من (3) إلى (6) من هذا القانون بحق كل من قام بارتكاب أي منها بسبب تأديته وظيفته أو عمله أو باستغلال أي منهما"، كذلك ترويج جريمة الدعارة بموجب المادة (9) من ذات القانون، والتي تنص على أنه: " أ- يعاقب كل من ارسل أو نشر عن طريق نظام معلومات أو الشبكة المعلوماتية قصدًا كل ما هو مسموع أو مقروء أو مرئي يتضمن أعمالًا إباحية وتتعلق بالاستغلال الجنسي لمن لم يكمل الثامنة عشر من العمر بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (300) ثلاثمائة دينار ولا تزيد على (5000) خمسة آلاف دينار. ب- يعاقب كل من قام قصدًا باستخدام نظام معلومات أو الشبكة المعلوماتية في إنشاء أو إعداد أو حفظ أو معالجة أو عرض أو طباعة أو نشر أو ترويج أنشطة أو أعمال إباحية لغايات التأثير على من لم يكمل الثامنة عشر من العمر أو من هو معوق نفسيًا أو عقليًا، أو توجيهه أو تحريضه على ارتكاب جريمة، بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن (1000) ألف دينار ولا تزيد على (5000) خمسة آلاف دينار. ج- يعاقب كل من قام قصدًا باستخدام نظام معلومات أو الشبكة المعلوماتية لغايات استغلال من لم يكمل الثامنة عشر من العمر أو من هو معوق نفسيًا أو عقليًا، في الدعارة أو الأعمال الإباحية بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن (5000) خمسة آلاف دينار ولا تزيد على (15000) خمسة عشر ألف دينار.، كذلك القيام بأعمال إرهابية أو دعم لجماعة أو تنظيم أو تمويل جمعية إرهابية بموجب المادة (10) من نفس القانون، كذلك الاطلاع على البيانات والمعلومات غير المتاحة للجمهور والتي تمس الأمن القومي واستغلالها في عملية الابتزاز وذلك بموجب المادة (11) من القانون ذاته والتي تنص على أنه: "يعاقب كل من قام قصدًا بإرسال أو إعادة إرسال أو نشر بيانات أو معلومات عن طريق الشبكة المعلوماتية أو الموقع الإلكتروني أو أي نظام معلومات تنطوي على ذم أو قدح أو تحقير أي

شخص بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن (100) مائة دينار ولا تزيد على (2000) ألفي دينار[220].

لهذا كانت الأردن وما زالت من أكثر الدول التي تعمل على تنظيم حرية المواطن وتجرّم من يمس حرمته الشخصية سواء أكان بالتهديد والابتزاز أم الذم والقدح والشتم وغير ذلك، حيث إن وزارة الداخلية الأردنية تتواصل مع المواطنين بصفة دائمة لاستقبال الشكاوي عن جرائم الابتزاز التي يمكن أن يعاني منها بعض المواطنين من خلال التشهير بهم أو ابتزازهم المالي والسياسي والجنسي وغير ذلك، ما يدفع هؤلاء المواطنين بالتوجه بالشكوى لوزارة الداخلية التي تعمل على وقف هذه التهديدات، وتقوم بتغليظ العقوبة على من يقوم بهذه الأفعال (للتوضيح: انظر الملحق رقم 4)*.

يمكن القول إن المملكة الأردنية الهاشمية كانت وما زالت من أوائل الدول العربية التي اهتمت بمكافحة الجريمة الإلكترونية بصورة عامة، وجريمة الابتزاز الإلكتروني بصفة خاصة، حيث لمست الأردن ما لهذه الجرائم من أضرار يمكنها أن تمس الحياة الخاصة للأفراد من ناحية، والمجتمع بأكمله من ناحية أخرى، وهو ما استلزمها إصدار قانون الجرائم الإلكترونية لعام 2015م ليكون بمثابة الرادع لارتكاب مثل هذه الجرائم.

ثانياً: العقوبة المقررة لجريمة الابتزاز الإلكتروني في القانون الأردني

لا يوجد في الأردن قوانين خاصة لحماية الحياة الخاصة للأفراد، وإنما هناك مجموعة من النصوص القانونية المتناثرة التي تنتشر في قانون العقوبات وقانون أصول المحاكمات الجزائية، ففي قانون العقوبات رقم (16) لسنة 1960م وتعديلاته، ورد بنص المادة (355) عقوبة من يقوم بابتزاز وإفشاء أسرار تحصَّل عليها بحكم وظيفته أو إبقائها في حيازته بعد انتهاء عمله حيث نصت المادة على أنه: "يعاقب بالحبس مدة لا تزيد على ثلاث سنوات كل من:

- حصل بحكم وظيفته أو مركزه الرسمي على أسرار رسمية وأباح هذه الأسرار لمن ليس له صلاحية الاطلاع عليها أو إلى من لا تتطلب طبيعة وظيفته ذلك الاطلاع وفقًا للمصلحة العامة.
- كان يقوم بوظيفة رسمية أو خدمة حكومية واستبقى بحيازته وثائق سرية أو رسومًا أو مخططات أو نماذج أو نسخًا منها دون أن يكون له حق الاحتفاظ بها أو دون أن تقضي ذلك طبيعة وظيفته.
- كان بحكم مهنته على علم بسر وأفشاه دون سبب مشروع.

([220]) العجمي، مرجع سابق: ص18-19.

* وهو يشير إلى شكوى بخصوص تشهير وقذف وإثارة النعرات الطائفية خلافاً لقانون الجرائم الالكترونية الأردني.

وكذلك ورد بنص المادة (356) من ذلك القانون عقوبة من كان يعمل بمصلحة البرق والبريد ويقوم بالاطلاع على الرسائل والاستماع إلى المحادثات الهاتفية، حيث نصت المادة المذكورة على أنه:" 1- يعاقب بالحبس من شهر إلى سنة كل شخص ملحق بمصلحة البرق والبريد يسيء استعمال وظيفته هذه بأن يطَّلع على رسالة مظروفه أو يتلف أو يختلس إحدى الرسائل أو يفضي بمضمونها إلى غير المرسل إليه، 2-ويعاقب بالحبس مدة ستة أشهر أو بالغرامة حتى عشرين دينارًا من كان ملحقًا بمصلحة الهاتف وأفشى مخابرة هاتفية اطلع عليها بحكم وظيفته أو عمله [221].

أما في قانون أصول المحاكمات الجزائية الأردني رقم (9) لسنة 1961م وتعديلاته وردت عدة مواد قانونية تنظم عملية القبض على المتهم وتفتيش بيته أو تفتيشه شخصيًا واستجوابه بهدف عدم المساس بحريته الشخصية وحياته الخاصة، وذلك ضمن المادة 348 مكررة [222].

لقد نظمت الأردن النصوص والقوانين التي تعاقب على جريمة الابتزاز الإلكتروني في قانون العقوبات الأردني، حيث نصت المادة 415 من قانون العقوبات على أن: "كل من هدد شخصًا بفضح أمر أو إفشائه أو الإخبار عنه، وكان من شأنه أن ينال من قدر هذا الشخص أو من شرفه أو من قدر أحد أقاربه أو شرفه لكي يحمله على جلب منفعة غير مشروعة له، أو لغيره، عوقب بالحبس من ثلاثة أشهر إلى سنتين وبالغرامة من خمسين ديناراً إلى مائتي دينار "[223].

كما أن المشرع الأردني أصدر قانون جرائم أنظمة المعلومات المؤقت رقم (30) لسنة 2010م، حيث أورد جرائم إلكترونية تتعلق بالخصوصية، وبشكل خاص بالنسبة للشخصيات العامة أو البيانات المتصلة بالحياة الخاصة والتي تشمل جرائم الابتزاز الإلكتروني، والاعتداء على المعطيات السرية أو الخاصة، وجرائم الاعتداء على البيانات الشخصية المتعلقة بالحياة الخاصة وغيرها [224]. حيث تنص المادة 3 من قانون جرائم أنظمة المعلومات المؤقت رقم 30 لسنة 2010م على أنه: " أ -كل من دخل قصدًا موقعًا إلكترونيًا أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح يعاقب بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أو بغرامة لا تقل عن

([221]) العجمي، مرجع سابق: ص43.

([222]) المرجع السابق: ص43

([223]) المادة (415) من قانون العقوبات الأردني رقم 1960/16 وجميع تعديلاته، والمعدل بآخر قانون رقم 2011/8.

([224]) المادة (3) والمادة (5) من قانون جرائم أنظمة المعلومات الأردني، وانظر أيضًا: المادة (76) من قانون الاتصالات الأردني رقم (13) لسنة 1995م.

(100) مائة دينار ولا تزيد على (200) مائتي دينار أو بكلتا العقوبتين. ب –إذا كان الدخول المنصوص عليه في الفقرة أ من هذه المادة بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل نظام معلومات أو تغيير موقع الكرتوني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار أو بكلتا العقوبتين.

أيضًا جرّم المشرع الأردني أفعال التنصت أو التقاط أو اعتراض الرسائل، فكل من يتنصت لأي رسائل عن طريق شبكة المعلومات أو أجهزة الحاسوب أو يلتقطها أو يعترضها دون تصريح يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد عن سنة أو بغرامة لا تقل عن 200 دينار ولا تزيد عن 1000 دينار أو بكلتا العقوبتين، حيث نصت المادة 5 من قانون جرائم أنظمة المعلومات الأردني رقم 30 لعام 2010 بأنه: "كل من قام قصدًا دون سبب مشروع بالتقاط أو باعتراض أو بالتصنت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على سنة أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار أو بكلتا هاتين العقوبتين"[225].

إنَّ من أهم خصائص الجرم المعلوماتي، والتي تميزه عن غيره من الجرائم الأخرى أنه يتميز بالتكرار، حيث يعود العديد من المجرمين المعلوماتيين إلى تكرار ارتكاب هذا النوع من الجرائم المستحدثة خاصة الابتزاز الإلكتروني، إما لاهتمامهم بالاطلاع على المعلومات وكشف الأسرار، أو حصولهم على المكاسب المادية جراء ارتكابهم هذه الجرائم، أو إضرارًا بالغير، حيث نجد إن تكرار الجرائم المعلوماتية ومنها جريمة الابتزاز الإلكتروني اعتبره التشريع الأردني الخاص بمكافحة الجرائم الإلكترونية ظرفًا مشددًا، حيث نصت المادة (16) من قانون الجرائم الإلكترونية رقم (27) لسنة 2015م على ما يلي: "تضاعف العقوبة المنصوص عليها في هذا القانون في حال تكرار أي من الجرائم المنصوص عليها فيه"[226].

بعد استعراض النصوص لقانون الجرائم الإلكترونية الأردني رقم (27) لسنة 2015م والمنشور على الصفحة 5631 من عدد الجريدة الرسمية رقم 5343 بتاريخ 2015/6/1. نجد أن المشرع الأردني قد

([225]) المادة (5) من قانون جرائم أنظمة المعلومات الأردني رقم 30 لسنة 2010.

([226]) الحوامدة، مرجع سابق: ص13.

عالج جميع الأفعال الناتجة عن الجرائم الإلكترونية بمنهج شمولي، حيث لم يترك المشرع الأردني فعلًا له علاقة بالجرائم الإلكترونية، إلا وعالجه بالتجريم والعقاب، ومن هذه الأفعال فعل الإرسال أو النشر عن طريق نظام المعلومات أو الشبكات المعلوماتية بوسائل الإعلام المقروءة والمرئية والمسموعة، بحيث يتضمن أفعالًا إباحية أو تتعلق بالاستغلال الجنسي أو الابتزاز الإلكتروني بكافة أشكاله أو الترويج للدعارة أو ذم أو قدح أو تحقير أي شخص[227].

أما المادة 14 من قانون الجرائم الالكترونية الأردني رقم 27 لسنة 2015 والمنشور على الصفحة 5631 من عدد الجريدة الرسمية رقم 5343 بتاريخ 2015/6/1. فقد نصت: "يعاقب كل من قام قصداً بالاشتراك أو التدخل أو التحريض على ارتكاب أي من الجرائم المنصوص عليها في هذا القانون بالعقوبة المحددة فيه لمرتكبيها"، أما المادة 15 من هذا القانون المذكور فقد نصت: "كل من ارتكب أي جريمة معاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتية أو أي نظام معلومات أو موقع الكتروني أو اشترك أو تدخل أو حرض على ارتكابها، يعاقب بالعقوبة المنصوص عليها في ذلك التشريع"[228].

اكتفى المشرِّع الأردني لقيام جريمة الابتزاز الإلكتروني أو أي جريمة إلكترونية أخرى وجود السلوك الجنائي، دون النظر إلى النتيجة الإجرامية التي كان يبتغيها الجاني، إلا إذا كانت الجريمة تتطلب تحقق نتيجة معينة، وهو ما نص عليه المشرّع الأردني في المادة رقم (65) من قانون العقوبات الأردني رقم 16 لسنة 1960م، حيث نص على أن: "لا عبرة للنتيجة إذا كان القصد أن يؤدى إليها ارتكاب فعل إلا إذا ورد نص صريح على أن نية الوصول إلى تلك النتيجة تؤلف عنصرًا من عناصر الجرم الذي يتكون كله أو بعضه من ذلك الفعل"[229].

يتبين مما سبق أن المشرّع الأردني فرض عقوبات شديدة على كل من يقوم بالمساس بحياة الآخرين الشخصية، أو يعمل على ابتزازهم سواء أكان بقضايا مادية أم جنسية أم غير ذلك، حيث فرض عليهم غرامات مالية إضافة إلى السجن، وبالتالي يمكن القول إن مثل تلك الإجراءات والعقوبات يمكن أن تكون رادعًا لهم.

([227]) المرجع السابق: ص16.

([228]) المادة 14و 15 من قانون الجرائم الالكترونية الأردني رقم 27 لسنة 2015.

([229]) المادة (65) من قانون العقوبات الأردني رقم (16) لعام 1960.

المطلب الثاني: أوجه الاتفاق والاختلاف بين عقوبة جريمة الابتزاز الإلكتروني في كل من القانون الفلسطيني والقانونين المصري والأردني.

الفرع الأول: أوجه الاتفاق في أحكام العقوبة بين القانون الفلسطيني وكلا القانونين الأردني والمصري:

بعد الاطلاع على ما سبق من قوانين الجرائم الإلكترونية لدى كل من فلسطين ومصر والأردن، تبين وجود عدد من عناصر الاتفاق لدى القوانين الثلاثة جميعها، حيث تتمثل تلك العناصر في الآتي:

اتفقت القوانين جميعها على حرمة الحياة الخاصة لدى الأفراد، كذلك حماية الآداب والأخلاق العامة للمجتمع وعدم السماح لأحد بالمساس بها، حيث ورد في المادة 15 من قانون رقم 16 لسنة 2017م، والمعدل بقانون رقم 10 لسنة 2018م، والمنشور في العدد الممتاز رقم (16) من الوقائع الفلسطينية بتاريخ 2018/05/03، بشأن الجرائم الإلكترونية في فلسطين على أن: "كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في تهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان هذا الفعل أو الامتناع مشروعًا، يعاقب بالحبس أو بالغرامة التي لا تقل عن ألفي دينار أردني ولا تزيد عن خمسة آلاف دينار أردني أو بالعقوبتين كليهما". كما ورد في قانون تقنية المعلومات الأردني لسنة 2010م ما نصه: "المحافظة على سرية البيانات التي تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمرٍ مسبب من إحدى الجهات القضائية المختصة – ويشمل ذلك البيانات الشخصية لأى من مستخدمي خدمته أو أي بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التي يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التي يتواصلون معها" وهذا جاء في أكثر من مادة من القانون مثل المادة 10، 11، 12... أما المشرّع الأردني فقد أورد في قانون الجرائم الإلكترونية رقم 27 لسنة 2015م والمنشور على الصفحة 5631 من عدد الجريدة الرسمية رقم 5343 بتاريخ 2015/6/1. بقوله: "يعاقب كل من قام قصدًا بالتقاط أو باعتراض أو بالتنصت أو أعاق أو حور أو شطب محتويات على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار".

كما لا يمكن إنكار الجهد المبذول من قبل المشرّع المصري وصولًا إلى قانون مكافحة جرائم تقنية المعلومات، وخروجه إلى التطبيق والنفاذ، وما تضمنه من نصوص تجريميه وقيامه على الموازنة ما بين الخطوط العامة للمسؤولية عن الجرائم بصفة عامة وانتهاء الاعتماد على ما تضمنته النصوص

المتناثرة في القانون المصري من أحكام موضوعية وإجرائية للمسؤولية الجنائية عن جرائم تقنية المعلومات لعام 2018م. والمنشور في الجريدة الرسمية العدد 32 مكرر (ج) بتاريخ 14 / 8 / 2018 حيث أشارت عدة مواد منها المادة 2 من قانون تقنية المعلومات المصري على ضرورة: "المحافظة على سرية البيانات التي تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة – ويشمل ذلك البيانات الشخصية لأى من مستخدمي خدمته أو أي بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التي يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التي يتواصلون معها[230].

وبالتالي يعد الابتزاز الإلكتروني تعديًا سافرًا على حياة الآخرين الشخصية، وأنَّ الحصول على معلومات وأسرار تتعلق بهم شخصيًا لا يرغبون بها قد يؤدي إلى السجن أو الغرامة، كون هذه الجرائم وسيلة لانتهاك الآداب العامة والتحريض على الفجور.

أن جميع القوانين السابقة قد قامت بإيقاع عقوبة السجن بفترات متفاوتة، حيث إن هذه العقوبات يمكنها أن تؤدي في النهاية إلى إحجام الجاني عن القيام بجريمته، حيث إن بعض مواد هذه القوانين بدأت بمعاقبة الجاني عدة أشهر في السجن، وبعضها وصلت فترة سجنه لخمس سنوات، حيث إن هذا الفارق يدل على مدى جسامة الجرم الذي ارتكبه عن طريق المواقع الإلكترونية. كذلك اتفقت هذه القوانين أيضًا على معاقبة الجاني بغرامات مالية تصل إلى مبالغ كبيرة، وذلك كي يرتدع الجاني بصورة أكبر، وهو الأمر الذي من شأنه أن يقلل من نسبة هذه الجرائم.
فقد نصت المادة (25) من القانون المصري سالف الذكر على أنه: " يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعتدى على أي من المبادئ أو القيم الأسرية في المجتمع المصري، أو انتهك حرمة الحياه الخاصة أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات إلى نظام أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقته أو بالقيام بالنشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، لمعلومات أو أخبار أو صور وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء أكانت المعلومات المنشورة صحيحة أم غير صحيحة". أما قانون جرائم تقنية المعلومات الأردني لسنة 2015 والمنشور على الصفحة 5631 من عدد الجريدة الرسمية رقم 5343 بتاريخ 2015/6/1. قد تطرق لذلك من خلال المادة رقم (12) بما نصه: "يعاقب كل من دخل قصدًا دون تصريح أو بما يخالف أو يجاوز التصريح إلى الشبكة

([230]) المادة 2 من قانون تقنية المعلومات المصري لسنة 2018م.

المعلوماتية أو نظام معلومات بأي وسيلة كانت بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (5000) خمسة آلاف دينار". كما أن المادة (16) من قانون الجرائم الإلكترونية الفلسطيني لعام 2017 قد وضحت ذلك بنص: "كل من أنتج ما من شأنه المساس بالآداب العامة أو أعد شيئًا أو أرسله أو خزنه بقصد الابتزاز والاستغلال، أو التوزيع أو العرض على غيره على الشبكة الإلكترونية، أو إحدى وسائل المعلومات يعاقب بالحبس لمدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار ولا تزيد عن خمسة آلاف دينار أو بالعقوبتين كليهما". في حين نصت المادة (15) من قانون الجرائم الالكترونية رقم 10 لسنة 2018 والمنشور في العدد الممتاز رقم (16) من الوقائع الفلسطينية بتاريخ 2018/05/03، على أن: "1- كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في تهديد شخص آخر أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان هذا الفعل أو الامتناع مشروعاً، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 2- إذا كان التهديد بارتكاب جناية أو بإسناد أمور خادشة للشرف أو الاعتبار، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً".

يمكن لأي من الدول سالفة الذكر أن تقوم بمصادرة الأجهزة والأموال المتحَصَّل عليها والمستخدمة في نطاق الابتزاز الإلكتروني كما نصت عليه تلك القوانين، حيث نصَّ القانون المصري على هذا الشيء، كما نصَّ عليه القانون الأردني والفلسطيني، وهذا الأمر من شأنه الحد من هذه الجريمة وردعها. قد نص المشرّع الفلسطيني في المادة (34) من قانون الجرائم الفلسطيني لسنة 2017م على أنه: "للنيابة العامة حق الحصول على الأجهزة أو الأدوات أو الوسائل أو البيانات أو المعلومات الإلكترونية أو بيانات المرور أو البيانات المتعلقة بحركات الاتصالات أو بمستعمليها أو بمعلومات المحتوى ذات الصلة بالجريمة الإلكترونية". كما وضحت الفقرة (ج) من المادة (13) من قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015: "للمحكمة المختصة الحكم بمصادرة الأجهزة والأدوات والوسائل والمواد وتوقيف أو تعطيل عمل أي نظام معلومات أو موقع إلكتروني مستخدم في ارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون ومصادرة الأموال المتحصلة من تلك الجرائم والحكم بإزالة المخالفة على نفقة الفاعل". أما المادة (38) من الفصل الثامن من قانون جرائم تقنية المعلومات المصري لسنة 2018 قد بينت أنه: "مع عدم الإخلال بحقوق الغير حسن النية، على المحكمة في حالة الحكم بالإدانة في أي جريمة من الجرائم المنصوص عليها في هذا القانون، أن تقضي بمصادرة

الأدوات والآلات والمعدات والأجهزة مما لا يجوز حيازتها قانونًا، أو غيرها مما يكون قد استخدم في ارتكاب الجريمة، أو سهّل أو ساهم في ارتكابها".

لما تقدم وجدنا هذه التشريعات الثلاث قد عاقبت على جريمة الابتزاز الالكتروني بالعقوبات التالية:

1- العقوبة الأصلية وتتمثل في هذه التشريعات بالعقوبة السالبة للحرية وهي عقوبة الحبس والسجن أو الأشغال الشاقة، إضافة إلى عقوبة الغرامة الجنائية.

2- العقوبة التكميلية، حث نرى أنها تتمثل في المصادرة الجوازية، حيث تكون المصادرة حينئذ عقوبة تكميلية إضافة للعقوبة الأصلية، إضافة لذلك فإن هذه المصادرة قد تكون تدبيراً احترازياً خاصة إذا كان الشيء محل المصادرة لا يجوز حيازته بموجب القانون.

وفي نفس الوقت نرى أن هناك العديد من الظروف المشددة التي من شأنها أن تشدد عقوبة الجرائم الالكترونية، فمثلاً نرى أن قانون الجرائم الالكترونية الاردني رقم 27 لسنة 2015م يرى أن ظرف العود من شأنه أن يشدد العقوبة، ويضاعفها في حالة تكرار ارتكاب أياً من الجرائم الالكترونية. كما نصت المادة 16 من هذا القانون: " تضاعف العقوبة المنصوص عليها في هذا القانون في حال تكرار أي من الجرائم المنصوص عليها فيه".

أما قانون تقنية المعلومات المصري رقم 175 لسنة 2018م والمنشور في الجريدة الرسمية العدد 32 مكرر (ج) بتاريخ 14 / 8 / 2018 فقد نصت المادة 34 على أنه: " إذا وقعت أي جريمة من الجرائم المنصوص عليها فى هذا القانون بغرض الاخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر، أو الاضرار بالأمن القومي للبلاد أو بمركزها الاقتصادي أو منع أو عرقلة ممارسة السلطات العامة لأعمالها، أو تعطيل احكام الدستور أو القوانين أو اللوائح أو الاضرار بالوحدة الوطنية والسلام الاجتماعي تكون العقوبة السجن المشدد"، أما المادة 39 من نفس القانون فتنص على: " للمحكمة إذا قضت بالإدانة على أحد الموظفين العموميين، لارتكابه جريمة من الجرائم المنصوص عليها في هذا القانون، أثناء وبسبب تأديته لوظيفته، أن تقضى بعزله مؤقتاً من وظيفته، إلا في الحالات المشار اليها في المادة (35) من هذا القانون فيكون العزل وجوبياً"

أما القرار بقانون رقم 10 لسنة 2018 والمنشور في العدد الممتاز رقم (16) من الوقائع الفلسطينية بتاريخ 2018/05/03، بشأن الجرائم الالكترونية الفلسطيني فقد نصت المادة 27 على أنه: "كل موظف ارتكب أياً من الجرائم المنصوص عليها في هذا القرار بقانون، مستغلاً صلاحياته وسلطاته أثناء تأدية عمله، أو بسببه أو سهل ذلك لغيره، تزيد العقوبة بمقدار الثلث. 2. كل من ارتكب، من

موظفي مزودي الخدمة، أياً من الجرائم المنصوص عليها في هذا القرار بقانون، أثناء تأدية عمله أو بسببه أو سهل ذلك لغيره، تزيد العقوبة بمقدار الثلثين".

ونري أن من أهم العقوبات التبعية في قانون مكافحة الجرائم الالكترونية المصري ما نصت عليه المادة 39 من القانون رقم 175 لسنة 2018م، والمنشور في الجريدة الرسمية العدد 32 مكرر (ج) بتاريخ 2018/8/14 إذ قصت بالإدانة على أحد الموظفين العموميين لارتكابه جريمة من الجرائم المنصوص عليها في هذا القانون أثناء وبسبب تأديته لوظيفته أن تقضي بعزله من وظيفته مؤقتاً إلا الحالات المشار إليها في المادة 34 من هذا القانون فيكون العزل وجوبياً.

حيث أن العزل حسب المادة المذكورة أعلاه هو عزل جوازي وهو الأصل في حالة الحكم بالإدانة على أحد الموظفين العموميين لارتكابه جريمة من الجرائم الالكترونية أثناء وبسبب تأديته لوظيفته، والعزل وضع له القانون حد أدنى سنة واحدة، وحد أقصى ست سنوات، ثم العزل الوجوبي وهذا يتوافر في حالة الظرف المشدد والمنصوص عليه في المادة 34 من هذا القانون، حيث أن العزل في هذه الحالة يكون عبارة عن عقوبة تبعية تلحق كل عقوبة جنائية منصوص عليها في المادة 25 من قانون العقوبات المصري، وفي هذه الحالة يكون العزل عبارة عن عقوبة تبعية مؤبدة.

يتبين للباحثة مما سبق أن النظام الفلسطيني والمصري والأردني قد اتفقوا جميعًا على تجريم الابتزاز الإلكتروني بصورة مطلقة، كما أنهم وفروا الحماية اللازمة للأشخاص الآخرين والحرص على عدم انتهاك أي شخص لحياتهم الخاصة، وقد فرضت غرامات باهظة وعالية إضافة إلى السجن لفترات طويلة لكل من يقوم بعملية الابتزاز الإلكتروني أو إفشاء حياة الآخرين الخاصة، ومن ناحية أخرى لم ينص القانون المصري على جريمة الابتزاز الإلكتروني صراحة، لكنه ذكر عوضًا عنها جريمة إفشاء الأسرار والتصنت وغيرها مما يمكن اعتباره كأحد الوجوه الأخرى لجريمة الابتزاز الإلكتروني.

الفرع الثاني: أوجه الاختلاف في أحكام العقوبة بين القانون الفلسطيني وكلا القانونين الأردني والمصري:

يمكن للباحثة استخلاص عدة أوجه للاختلاف بين كل من القانون الفلسطيني والقانون الأردني والقانون المصري، ومن هذه الاختلافات ما يلي:

1- أن عقوبة إفشاء الأسرار أو التصنت أو الابتزاز الإلكتروني لم تكن موحدة ضمن هذه القوانين، فقد حددها القانون المصري بمدة لا تتجاوز خمس سنوات، أما جريمة الابتزاز في القانون الفلسطيني

لم يتم تحديد مدة الحبس، أما المشرع الأردني فكانت المدة لا تزيد عن سنة ولا تقل عن ثلاثة أشهر، وهذا يعني أن التقديرات تكون من القاضي وليست محكومة بفترة معينة. وهذا يعني اختلاف في مقدار العقوبة، حيث اعتبرها المشرع المصري جناية، في حين اعتبرها كل من المشرع الأردني والفلسطيني جنحة عقوبتها الحبس.

2- أن الابتزاز الإلكتروني جاء في القانون الفلسطيني صريحًا بدرجة كبيرة بلفظ الابتزاز، أما القانون الأردني قد كان فضفاضًا نوعًا ما في هذا اللفظ واستعاض عنه بلفظ إفشاء أسرار أو تصنت أو غيره، وفي القانون المصري لم ترد كلمة ابتزاز ولكنها استعيض عنها بكلمات أخرى بديلًا عنها اعتبرها الفقهاء يمكن أن تحل مكانها.

3- أن القانون الفلسطيني يمكن اعتباره قانونًا من نوع خاصًا لا يقارن بالقوانين الأخرى كالقانون المصري والقانون الأردني، حيث إنه جاء في ظل احتلال، وبالتالي يمكن أن ينعكس ابتزاز إلكتروني من قبل أجهزة المخابرات الإسرائيلية للفلسطينيين من منطلقات ابتزازات جنسية أو أخلاقية أو مالية، وبالتالي فإن هذا القانون يعمل بوضعية خاصة جدًا تميزه عن باقي القوانين الأخرى. حيث ازدادت في الفترة الأخيرة جرائم الابتزاز الإلكتروني التي تمارسها السلطات الإسرائيلية بهدف إيقاع الفلسطينيين من ذوي النفوس الضعيفة في شرك العمالة والتعاون مع الاحتلال، وهذا الإيقاع يتم من خلال صور أو فيديوهات مخلة بالآداب أو أفلام مسيئة أو ابتزاز مالي من خلاله يقوم الإسرائيليون بالتهديد بفضح الضحية أو التعاون معهم، حيث إن هنالك من يتم ابتزازه سريعًا يلجأ لهم مما يوقعه في شرك العمالة دون أن يعلم. وهو ما يجعل القانون الفلسطيني ذا وضعية خاصة لا تقارن بالقوانين الأخرى.

4- أن القانون الفلسطيني بخلاف القانون المصري والأردني واجه حملة شرسة من الانتقادات بسبب منعه ومحاربته لحرية الرأي والتعبير، حيث إن عنصر الاختلاف بين القانون الفلسطيني وكلا القانونين – برغم من أن القانون الأردني والمصري حاربا حرية الرأي والتعبير–أن القانون الفلسطيني صدر في ظل وجود احتلال يهيمن على الأرض ويصادر كافة أشكال الحريات في الأراضي الفلسطينية، وبالتالي كان هذا الخلل واضحًا منذ البداية.

بالنسبة لمصادرة الأموال والمنقولات والمعلومات التي قام الجاني بجلبها من الضحية، فقد كان المشرِّع الفلسطيني قد وضح على أنَّ للنيابة حق إصدار قرار بالمصادرة وهو أمر غير إلزامي، وكذا في القانون الأردني الذي أجاز للمحكمة فعل ذلك متى رأت أن هذه المصادرة يمكنها أن تخدم القضية وأيضًا هذا الفعل يعتبر غير إلزامي، أما القانون المصري فقد ألزم المحكمة بمصادرة جميع المنقولات المادية والمعنوية سواء أكان ذلك يخدم القضية أم لا، وبالتالي إن القانون المصري في هذه النقطة يعتبر إلزاميًا وليس تشاوريًا.

إن المصادرة لا تكون إلزامية "وجوبية" إلا في حالة إن كانت عبارة عن تدبير احترازي، حيث أن محل المصادرة يكون محله عبارة عن شيء منقول لا يجوز حيازته قانوناً، في حين إذا كانت المصادرة عقوبة تكميلية فإنها تكون حينها مصادرة جوازية. وهذا ما أخذ به كل من المشرع الأردني والفلسطيني.

وهكذا اهتمت كلٌّ من جمهورية مصر العربية والأردن بضرورة إصدار قانون يمنع ارتكاب جرائم الابتزاز الإلكتروني لما لها من خطورة كبيرة على الفرد والمجتمع من ناحية، وعلى الأمن القومي لكلا البلدين من ناحية أخرى، حيث أصدر الرئيس المصري عبد الفتاح السيسي قانون مكافحة جرائم تقنيات المعلومات رقم 175 لسنة 2018م والذي اعتبر أول تشريع مصري لهذا الغرض.

كما أن هذا القانون قرر عقوبات رادعة لمرتكبي جرائم المعلومات بصورة عامة وجرائم الابتزاز الإلكتروني بصورة خاصة لما لهذه الجرائم من خطورة على المجتمع، حيث يتأثر بها المواطن بصورة بارزة، مما جعل المشرّع المصري يهتم بتطبيق العقوبة الرادعة سواء أكان بالحبس أم بالغرامة المالية وهو الأمر الذي سينعكس على المواطنين في الحد من هذه الجريمة.
كما كانت الأردن من أوائل الدول العربية المتقدمة التي تكافح من أجل الحد من جرائم الابتزاز الإلكتروني، وذلك بسبب فطنتها لما لهذه الجرائم من خطورة على أمنها وسلامة مجتمعها، حيث فرضت عقوبات قاسية بحق الجناة الذين يرتكبون مثل هذه الجرائم، حيث نص قانون الجرائم الالكترونية الأردني رقم 27 لسنة 2015م في العديد من مواده على ضرورة حبس أو تغريم الجاني حتى يتوقف تمامًا عن ارتكابه مثل هذه الجرائم الخطيرة والمنافية للأخلاق والقانون.

كما أن هناك حالات اتفاق واختلاف بين القوانين العربية التي تهتم بمكافحة جرائم الابتزاز الإلكتروني، فالقانون الفلسطيني يتفق مع القانون الأردني والمصري من عدة نواحي وهي المصير المشترك والأخلاق والآداب المشتركة والدين والعقيدة وبالتالي ستكون بعض البنود مشتركة ومتطابقة، أما البيئات المختلفة وبعض العوامل الأخرى التي تتعلق بعادات المجتمع هنا أو هنا تحتم على المشرّع في كل بلد من هذه البلاد وضع بعض مواد القوانين بصورة تختلف مع البلد الآخر كي يواكب البيئة التي تعيش بها هذه المجتمعات.

الخاتمة

لقد حاولت من خلال هذه الدراسة معالجة موضوعاً هاماً وحساساً سواء على الصعيد العملي أو التشريعي، حيث عرضت الباحثة في دراستها من خلال الفصل التمهيدي الذي تناول أدبيات الدراسة وأبرز مشكلة الدراسة وتساؤلاتها وأهميتها العلمية وأهدافها التي سعيت جاهدة لإبرازها.

كما تطرق الفصل الأول من هذه الدراسة إلى ماهية جرائم الابتزاز الإلكتروني، وذلك بالحديث عن مفهوم جرائم الابتزاز الإلكتروني وأركانه وأنواعه ودوافعه، كذلك إبراز أهم طرق الإثبات والتحقيق في جرائم الابتزاز الإلكتروني وبيان آثارها على المجتمع وعلى الفرد.

وقد بين الفصل الثاني من الدراسة جريمة الابتزاز الإلكتروني في القانون الفلسطيني ومقارنته مع القانون المصري والقانون الأردني، وذلك من خلال توضيح وبيان قانون الجرائم الفلسطيني والعقوبات التي تطرق لها من ناحية جريمة الابتزاز الإلكتروني والصعوبات التي تواجه السلطات في الكشف عن هذه الجرائم، كما أوضح أيضًا هذا الفصل جريمة الابتزاز الإلكتروني في كل من القانون المصري والقانون الأردني وأوجه الاتفاق والاختلال فبين عقوبة جريمة الابتزاز الإلكتروني في كل من القانون الفلسطيني مقارنة مع القانون المصري والأردني.

وبناءً على ذلك وبعد الوصول لنتائج وتوصيات الدراسة، رأت الباحثة أن هذه الدراسة يمكن أن يكون لها امتداد لدراسات مستقبلية لباحثين آخرين، خاصة ما يتعلق بموضوعات إجراءات المحاكمة، وكذلك موضوع جرائم اختراق حرمة الغير، والحرية الشخصية، وجرائم التهديد وغيرها من الجرائم التي لم يخض أحد من الباحثين في هذه المجالات قبل ذلك، وبالتالي يمكن أن يؤسس هذا البحث للكتابة عن هذه الموضوعات مستقبلاً.

نتائج الدراسة وتوصياتها

أولاً: نتائج الدراسة:

توصلت في هذه الدراسة لعدة نتائج منها:

1- تعتبر جرائم الابتزاز الإلكتروني إحدى أخطر الجرائم التي تدمر منظمة القيم والاخلاق في المجتمع، بخلاف مساسها بالأمن القومي لأي دولة.
2- أن هناك مشكلات عديدة تواجه أجهزة الدولة في إثبات هذه الجريمة لاعتبارات عديدة.
3- لاقى قانون الجرائم الإلكترونية الفلسطيني انتقادات واسعة من المجتمع المدني ومراكز حقوق الإنسان، والذين رأوا أن هذا القانون يمس بحرية التعبير والرأي خاصة للصحفيين منهم.
4- لم يأت هذا القانون سواء قانون سنة 2017م أو المعدل منه لسنة 2018م على إبراز مفهوم التفتيش عن المعلومات، على الرغم من تطرق قانون الإجراءات الجزائية لبيان مدلول التفتيش بصورة الأولية، لهذا تم تقديم معلومات عن مفهوم التفتيش وطرقه في الابتزاز الالكتروني.
5- أن العديد من المواد خاصة المادة 33 و 34 من قانون الجرائم الالكترونية قد بينت أنه لا مانع من الدخول إلى الحاسب الآلي وتفتيشه وإظهار آثار الجريمة. خاصة مع وجود إذن من المشرع الفلسطيني لوكيل النيابة بالنفاذ المباشر إلى وسائل تكنولوجيا المعلومات وإجراء التفتيش بها بقصد الحصول على البيانات والمعلومات.
6- أن الأساليب التكنولوجية المنتشرة في المنطقة العربية خاصة مصر والأردن بشكل عام، والأراضي الفلسطينية بشكل خاص قد تطورت وواكبت التحديث في استخدام هذه البرامج والوسائل، ما يجعل المهمة أكبر على السلطات داخل الدولة في مواكبة هذا التطور.
7- أنه تم تحديد المسئوليات والواجبات التي يجب أن يلتزم بها مزود خدمات الإنترنت بخصوص الجرائم الإلكترونية عامة والابتزاز الإلكتروني بصفة خاصة، وذلك من خلال تزويد جهات التحقيق بالبيانات اللازمة للمشتركين، في إطار التعاون مع الجهات المختصة بناء على قانون الجرائم الإلكترونية في مواده 32 و 42.
8- أن المشّرع الأردني تصدى لجرائم المعلومات بإصداره قانون خاص للجرائم الإلكترونية سنة 2010، و2015م من خلالهما فرض عقوبات قاسية على كل من تسول له نفسه استخدام التكنولوجيا بطرق غير قانونية.
9- أن المشرع المصري أيضًا حاول متأخراً في عام 2015م إصدار قانون خاص بالمعلومات، حيث حاول التصدي لهذه الظاهرة التي استشرت في المجتمع، وفرض قوانين صارمة على مرتكبيها.

10- بالرغم من قيام العديد من الدول العربية خاصة مصر والأردن وفلسطين بفرض قوانين تجرّم كل من يستخدم التكنولوجيا بطرق ملتوية وغير قانونية، إلا أن ذلك لم يحد من الجريمة بالقدر المطلوب، بل بقيت منتشرة.

11- أن بعض بنود هذه القوانين تعتبر فضفاضة ولم تتطرق لطرق الابتزاز بصورة صحيحة وهذا الأمر يمكن أن يؤدي إلى أن يجعل هذا القانون غير صالح لتطبيقه على كثير من الحالات.

12- أن الجهود الدولية لمكافحة جريمة الابتزاز الإلكترونية لم تكن على المستوى المطلوب منها، خاصة في ظل قلة خبرة وعدم وجود معرفة لمواجهة مثل هذه الجرائم بالصورة السليمة التي يمكنها أن تحد من هذه الجرائم.

ثانياً: توصيات الدراسة:

توصي الدراسة بما يلي:

1- نوصي بضرورة الاستفادة من القوانين الأجنبية في تحديد صور الجرائم الإلكترونية وعقوبتها، وتعديل قوانين الجرائم بحيث يستجيب للتطورات التي تحصل في مجال التكنولوجيا والثورة المعلوماتية.

2- نوصي المشرّع العربي بصورة عامة والفلسطيني والمصري والأردني بصفة خاصة بوضع مواد قانونية خاصة بجريمة الابتزاز الإلكتروني كونها من الجرائم الخطيرة التي لم ينتبه لها الكثير من المشرعون إلا بعبارات عابرة فقط.

3- نوصي المشرع الفلسطيني والأردني والمصري بوضع بعض الجرائم التي لم ينص عليها ضمن قوانين الجرائم لديهم كالمضايقات والتحرش في نطاق المواقع الإلكترونية والملاحقة الإلكترونية والتشهير وغير ذلك من الأفعال التي لم ينص عليها أي قانون جرائم الإلكترونية لديهم.

4- ضرورة وجود جهاز خاص بالجرائم الإلكترونية في كل دولة يكون مدرباً على أحدث المستويات، كون هذا النوع من الجرائم يعتبر من أخطر الجرائم على الإطلاق، وأن الكشف عنه يعتبر بالغ الصعوبة.

5- نظراً لخصوصية الحالة الفلسطينية التي ترزح تحت احتلال من عشرات السنوات، فقد يجعل هذا من الضروري تحديد مسئوليات وواجبات مزودي هذه الخدمات للجمهور، وذلك في إطار التعاون بينهم وبين السلطات المختصة كي لا تخرج الأمور عن نطاقها.

6- ضرورة تدريب المحققين القضائيين والنيابة العامة على طرق الإثبات وجمع الدلائل والتعامل مع الجرائم الإلكترونية بسبب نقص الخبرة لديهم وعدم معرفتهم في كيفية التعامل مع هذه الجرائم.

7- نوصي بتأهيل وتدريب رجال الشرطة وكذلك رجال الضبط القضائي والقضاة على التعامل وفهم هذا النوع من الجرائم الالكترونية التي تحتاج إلى خبرة فنية عالية، وذلك لملائمة هذا النوع من الأدلة في الإثبات.

8- أما على الصعيد الدولي نوصي بتعزيز التعاون والتنسيق مع المؤسسات الدولية والمعنية بمواجهة هذه المشكلة وخاصة الانتربول، ومن ثم الانضمام إلى الاتفاقيات الدولية الخاصة بمكافحة الجرائم المعلوماتية.

9- نوصي بتحسين تدابير الأمن والوقاية المتعلقة بالحاسوب، وذلك مع مراعاة حماية الحق في الحياة الخاصة، ومن ثم احترام حقوق الإنسان وحرياته الأساسية.

10- نوصي ببث الوعي والثقافة لدى المواطنين والعاملين في الجهاز القضائي، وكذلك أجهزة تنفيذ القوانين، وكذلك الوعي بأهمية مكافحة الجرائم الالكترونية.

المصادر والمراجع

أولاً: القوانين .

1- قانون الإجراءات الجزائية الفلسطيني رقم 3 لعام 2001م.
2- القانون الأساسي الفلسطيني المعدل لعام 2005.
3- قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015.
4- قانون الجرائم الإلكترونية الفلسطيني رقم 16 الصادر سنة 2017م.
5- قانون العقوبات رقم 16 لسنة 1960م والمطبق في المحافظات الشمالية.
6- قانون العقوبات رقم 74 لسنة 1936م المطبق في المحافظات الجنوبية.
7- قانون رقم 10 لسنة 2018م بشأن الجرائم الإلكترونية.
8- قانون رقم 15 لسنة 2009 بشأن الهيئة الفلسطينية لتنظيم قطاع الاتصالات.
9- قانون رقم 15 لسنة 2009 بشأن الهيئة الفلسطينية لتنظيم قطاع الاتصالات.
10- القانون رقم 3 لسنة 1996م بشأن الاتصالات السلكية واللاسلكية.
11- قانون مكافحة جرائم تقنية المعلومات المصري لسنة 2015.
12- قانون مكافحة جرائم تقنية المعلومات المصري لسنة 2018.
13- قانون تقنية المعلومات الأردني رقم 30 لسنة 2010.

الكتب العربية

1- إبراهيم محمد منصور، **الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية**، دار النهضة العربية، القاهرة، 2002.
2- أحمد براك، وعبد القادر جرادة، **الجرائم الإلكترونية في التشريع الفلسطيني: دراسة تحليلية تأصيلية مقارنة**، دار الشروق، القاهرة، ط1، 2018.
3- أحمد محمد شامي ، سيد حسب الله، **الموسوعة العربية لمصطلحات علوم المكتبات والمعلومات والحاسبات**، المكتبة الأكاديمية، القاهرة، المجلد1، ط1، 1998.
4- أمير فرج يوسف، **الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكومبيوتر والإنترنت**، ط1، مكتبة الوفاء القانونية، الإسكندرية، 2011

5- أمين محمد نوفل، **قانون العقوبات العام**، كلية الشرطة الفلسطينية، غزة، د.ت.

6- أيمن عبد الله فكري، **الجرائم المعلوماتية: دراسة مقارنة في التشريعات العربية والأجنبية**، مكتبة القانون والاقتصاد، السعودية، ط1، 2014.

7- تركي بن عبد الرحمن المويشير، **بناء أنموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته**، جامعة نايف العربية للعلوم الامنية، الرياض، ط1، 2012.

8- خليفة كندر، **عبد الله حسين، ضمانات المتهم في مرحلة التحقيق الابتدائي في قانون الاجراءات الجنائية**، دار النهضة العربية، بيروت، ط1، 2002.

9- ذياب البداينة، **جرائم الحاسب الآلي والإنترنت**، بحث منشور في الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، تونس، ١٤٢٤هـ.

10- طارق الخن، **جرائم المعلوماتية**، الجامعة الافتراضية السورية، دمشق، 2018.

11- عبد الرحمن السند، **جريمة الابتزاز**، الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر، السعودية، ط1، 2018.

12- عبد العزيز جايز الفقيري، **الابتزاز الداء والدواء**، شبكة الألوكة، د.ت.

13- عبد القادر جرادة، **مبادئ قانون العقوبات الفلسطيني**، المجلد الأول، مكتبة آفاق، غزة، 2010.

14- عبد القادر جرادة، **موسوعة الإجراءات الجزائية في التشريع الفلسطيني**، المجلد، مكتبة آفاق، غزة، عدد بئر السبع، 2009

15- عصام عابدين، **جهود مؤسسة الحق في مواجهة قرار بقانون الجرائم الإلكترونية**، مؤسسة الحق، رام الله، 2018.

16- علي جبار الحسيناوي، **جرائم الحاسوب والإنترنت**، دار اليازوري العلمية للنشر والتوزيع، عمان، 2009.

17- محمد الأمين البشري، التحقيق في الجرائم المستحدثة، ط1، الرياض، 2004.

18- محمد بن جرير الطبري، **التبصير في معالم الدين**، تحقيق: علي بن عبد العزيز بن علي الشبل، دار العاصمة، السعودية، ط1، 1996.

19- محمد حماد الهيتي، **التكنولوجيا الحديثة والقانون الجنائي**، دار الثقافة للنشر والتوزيع، عمان، الأردن،ط2، د.ت.

20- محمد خليفة، **دراسة نقدية للإطار القانوني للجرائم الإلكترونية في الأراضي الفلسطينية**، معهد أبحاث السياسات الاقتصادية "ماس"، رام الله، 2012.

21- ناير جميل عمر، **الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية**، دار الجامعة الجديدة، الاسكندرية، 2012.

22- نورة بنت عبد الله المطلق، **ابتزاز الفتيات: أحكامه وعقوبته في الفقه الإسلامي**، كلية الشريعة، جامعة الإمام محمد بن سعود الإسلامية، السعودية، د.ت.

23- وليد طه، **التنظيم التشريعي للجرائم الإلكترونية في اتفاقية بودابست**، وزارة العدل، مصر، د.ت.

24- ياسمينة بو نعارة، **الجريمة الإلكترونية**، جامعة الأمير عبد القادر للعلوم الإسلامية، الجزائر، د.ت.

25- يوسف حسن يوسف، **الجرائم الدولية للإنترنت**، المركز القومي للإصدارات القانونية، القاهرة، ط1، 2011.

ثانياً: الرسائل العلمية

1- أحمد مسعود مريم، **آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون 04/09**، رسالة ماجستير غير منشورة، جامعة قاصدي مرباح- ورقلة، الجزائر، 2013.

2- آمال عبد الرحمن حسن، **الأدلة العلمية الحديثة ودورها في الإثبات الجنائي**، رسالة ماجستير غير منشورة، إشراف دكتور محمد الجبور، جامعة الشرق الأوسط، عمان، 2012.

3- ثنيان ناصر آل ثنيان، **إثبات الجريمة الإلكترونية: دراسة تأصيلية تطبيقية**، رسالة ماجستير غير منشورة، إشراف دكتور جلال الدين محمد صالح، جامعة نايف العربية للعوم الأمنية، الرياض، 2012.

4- زهية معمش، ونسيمة غانم، **الإثبات الجنائي في الجرائم المعلوماتية**، رسالة ماجستير غير منشورة، إشراف محمد بن فردية، جامعة عبد الرحمن ميرة، الجزائر، 2012-2013.

5- سامي مرزوق المطيري، **المسؤولية الجنائية عن الابتزاز الإلكتروني في النظام السعودي: دراسة مقارنة**، رسالة ماجستير غير منشورة، إشراف عبد الفتاح باباه باباه، جامعة نايف العربية للعوم الأمنية، الرياض، 2015.

6- سمير أسعد أبو شمس، **استغلال النفوذ الوظيفي في ظل التشريعات الفلسطينية وأثره على التنمية السياسية**، رسالة ماجستير غير منشورة، جامعة النجاح الوطنية، نابلس، 2011.

7- شيرين الياس دبابنة، **جرائم بطاقات الائتمان في الأردن: دراسة وصفية استطلاعية**، رسالة ماجستير غير منشورة، جامعة مؤتة، الأردن، 2005.

8- طارق محمد طميزة، **التفتيش المعلوماتي في النظام القانوني الفلسطيني والمقارن**، رسالة دكتوراه غير منشورة، جامعة أسيوط، مصر، 2018

9- عبد الله دغش العجمي، **المشكلات العملية والقانونية للجرائم الإلكترونية: دراسة مقارنة**، رسالة ماجستير غير منشورة، إشراف الدكتور أحمد اللوزي، جامعة الشرق الأوسط، الأردن، 2014.

10- محمد بن منصور آل النمر، **دور تقنية المعلومات في مكافحة جرائم الابتزاز**، رسالة ماجستير غير منشورة، إشراف: لواء د. حسن بن أحمد الشهري، جامعة نايف العربية للعلوم الأمنية، الرياض، 2013.

11- نعيم سعيداني، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، رسالة ماجستير غير منشورة، إشراف زرارة صالحي الواسعة، جامعة الحاج لخضر، الجزائر، 2012-2013.

12- يوسف خليل العفيفي، **الجرائم الإلكترونية في التشريع الفلسطيني: دراسة تحليلية مقارنة**، رسالة ماجستير غير منشورة، إشراف دكتور أيمن عبد العال، الجامعة الإسلامية، غزة، 2013.

ثالثاً: المجلات والأبحاث

1- أحمد رجب، **قراءة لمشروع قانون مكافحة الجريمة الإلكترونية: تحليل للإشكاليات القانونية بالمشروع وتأثيرها على الحريات**، المركز المصري لدراسات السياسة العامة، مصر، مايو 2016.

2- جاسم خريبط خلف، **صعوبات الدليل الجنائي في الجرائم المعلوماتية**، قسم القانون، كلية شط العرب الجامعة، العراق، د.ت.

3- **الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها**، مسابقة جائزة الأمير نايف بن عبدالعزيز للبحوث الأمنية لعام 2015م، مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة، سلطنة عمان، 2016.

4- **الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي**، مركز هردو لدعم التعبير الرقمي، القاهرة، 2014.

5- جعفر حسن الطائي، **جرائم تكنولوجيا المعلومات وآليات الحد منها**، بحث منشور في الأمانة العامة للمكتبة المركزية، جامعة ديالي، العراق،2015/11/4.

6- خليل يوسف جندي، **المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني: دراسة مقارنة**، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد7، العدد26، 2018.

7- داليا عبد العزيز، **المسؤولية الجنائية عن جريمة الابتزاز الإلكتروني في النظام السعودي دراسة مقارنة**، مجلة جيل الأبحاث القانونية المعمقة العدد 25، مايو 2018.

8- ذياب البداينة، **جرائم الحاسب الآلي والإنترنت، بحث منشور في الظواهر الإجرامية المستحدثة وسبل مواجهتها**، أكاديمية نايف العربية للعلوم الأمنية، تونس، ١٤٢٤هـ

9- سميرة معاشي، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني، الجزائر، العدد السابع، د.ت.

10- صالح بن عبد الله بن حميد، **الابتزاز: المفهوم والواقع**، بحث منشور ضمن بحوث ندوة الابتزاز: المفهوم- الأسباب- العلاج، مركز باحثات لدراسات المرأة بالتعاون مع قسم الثقافة الاسلامية بجامعة الملك سعود، السعودية، 1432هـ.

11- عادل عبدالله خميس المعمري، **التفتيش في الجرائم المعلوماتية**، بحث منشور، مجلة الفكر الشرطي، المجلد 22، العدد86، مركز بحوث الشرطة، الأمارات العربية المتحدة، 2013.

12- عثمان يحيى أبو مسامح، **الأركان العامة لجريمة التخابر في التشريع الفلسطيني مقارنة بالتشريع المصري والأردني: دراسة تحليلية مقارنة**، مجلة جيل الدراسات المقارنة العدد7، يونيو 2018.

13- علي أحمد القاعدي، **الجرائم المتعلقة بجريمة اختطاف الأفراد والممتلكات "الاغتصاب- الابتزاز": دراسة فقهية مقارنة بقانوني الجرائم والعقوبات اليمني والمصري**، مجلة جامعة الناصر، العدد الثالث، يناير- يونيو 2014.

14- فؤاد جمال، **جرائم الحاسبات والإنترنت، الجرائم المعلوماتية**، مركز المعلومات ودعم اتخاذ القرار، مارس ٢٠٠٥.

15- لورنس سعيد الحوامدة، **الجرائم المعلوماتية أركانها وآلية مكافحتها: دراسة تحليلية مقارنة**، مجلة الميزان الإسلامية والقانونية، جامعة العلوم الإسلامية العالمية، الأردن، 2016-2017.

16- مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة (2016) "**الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها**"، مسابقة جائزة الأمير نايف بن عبد العزيز للبحوث الأمنية لعام 2015م، سلطنة عمان.

17- محمد الهندي، **نفاذ قانون الجرائم الإلكترونية الفلسطيني: المجتمع المدني وانكفاء الدور**، ورقة بحثية قدمت إلى البرنامج التدريبي "إعداد السياسات العامة والتفكير الاستراتيجي"، مركز مسارات، 2018/3/27.

18- محمد على قطب، **الجرائم المعلوماتية وطرق مواجهتها الجزء الثاني**، الأكاديمية الملكية للشرطة، وزارة الداخلية، مملكة البحرين، مارس 2010.

19- مصطفى سليمان أبكر، **جرائم الحاسوب وأساليب مواجهتها**، مجلة الأمن والحياة، العدد 210، 1420هـ.

20- مليكة عطوي، **الجريمة المعلوماتية**، مجلة حوليات جامعة الجزائر، العدد 21، يونيو 2012.

21- ناجي الغزي، **الابتزاز السياسي.. واللعب بالورقة الطائفية**، مجلة الحوار المتمدن، العدد 2911، 2010.

رابعاً: المؤتمرات والندوات العلمية

1- أبو الوفا محمد أبو الوفا، **المواجهة الإجرائية للجرائم المعلوماتية، ندوة بعنوان: جرائم تقنية المعلومات في ظل القانون الاتحادي رقم "2" لسنة 2006م**، جامعة الامارات العربية المتحدة، دولة الامارات العربية المتحدة.

2- ذياب موسى البداينة، **الجرائم الإلكترونية: المفهوم والأسباب**، ورقة مقدمة للمؤتمر العلمي بعنوان: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، وذلك خلال الفترة من 7-1435/11/9هـ الموافق 2-2014/9/4م، كلية العلوم الاستراتيجية، عمان، الأردن، 2014.

3- سمية فتحي السيد، **الجريمة المعلوماتية**، المؤتمر العلمي العاشر لقسم المكتبات والوثائق والمعلومات، كلية الآداب، جامعة القاهرة، 15-16 مايو 2013.

4- صالح بن عبد الله بن حميد، **الابتزاز: المفهوم والواقع**، بحث منشور ضمن بحوث ندوة الابتزاز: المفهوم- الأسباب- العلاج، مركز باحثات لدراسات المرأة بالتعاون مع قسم الثقافة الاسلامية بجامعة الملك سعود، السعودية، 1432هـ.

5- عبد الغني فرغلي، ومحمد المسماري، **الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية: دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي**، والذي عقد في الفترة من 12-2007/11/14م، جامعة نايف العربية للعلوم الأمنية، الرياض.

6- عمرو حسين عباس، **أدلة الإثبات الجنائي والجرائم الإلكترونية (المعلوماتية)**، بحث مقدم إلى المؤتمر الإقليمي الثاني حول تحديات تطبيق الملكية الفكرية في الوطن العربي، خلال الفترة من 26-2008/4/27، مقر جامعة الدول العربية.

7- محمد أبو العلا عقيدة، **التحقيق وجمع الأدلة ي مجال الجرائم الإلكترونية**، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، محور القانون الجنائي، دبي، الإمارات العربية المتحدة، 26-2003/4/28.

خامساً: أوراق العمل

1- إبراهيم سليمان الهويمل، **جرائم ابتزاز الفتيات وطرق اكتشافها والتحقيق فيها**، ورقة عمل مقدمة للملتقى العلمي حول الجرائم المعلوماتية التي نظمته هيئة التحقيق والادعاء العام وجامعة نايف العربية للعلوم الأمنية في الفترة 23-1430/10/25هـ، جامعة نايف للعوم العربية والأمنية، 2009.

2- خاص المركز الفلسطيني لحقوق الإنسان، **مراجعة لقانون الجرائم الإلكترونية الفلسطينية لسنة 2017 في ضوء المعايير الدولية لحرية التعبير**، المركز الفلسطيني لحقوق الإنسان، أغسطس 2017.

3- خاص الهيئة المستقلة لحقوق الإنسان "ديوان المظالم"، **مذكرة قانونية: حول القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية**، الهيئة المستقلة لحقوق الإنسان، 2018/5/20.

4- خاص مركز الميزان لحقوق الإنسان، **ورقة موقف حول التشريع الإلكتروني ومدى مراعاة الحقوق والحريات العامة**، مركز الميزان لحقوق الإنسان، 2017.

5- كيارا عياد، **الأمن الرقمي لمراقبة من؟ قانون الجرائم الإلكترونية في فلسطين**، ورقة عمل قدمت لمبادرة الإصلاح العربي: بدائل سياسات، تشرين الأول/ أكتوبر 2018

سادساً: الصحف

1- ابراهيم أبو كامش، **فضاء الانترنت في فلسطين تنخره السرقة والابتزاز والاحتيال والتشهير**، صحيفة حياة وسوق، السنة الثانية، العدد 56، 2012/6/2

2- خاص صحيفة البيان الإماراتية، **تحذير من تنامي ظاهرة الابتزاز الإلكتروني للرجال في الشرق الأوسط**، 24 فبراير 2015.

3- صحيفة النهار الإماراتية (2012)، **تسيبي ليفني : مارست الجنس من أجل الابتزاز والقتل**، 05 نوفمبر 2012.

4- ياسر محمد، **الجريمة الإلكترونية.. إرهاب يتحدى الدول بالتكنولوجيا المتطورة**، صحيفة العرب القطرية، 2018/6/23.

سادساً: المواقع الإلكترونية

1- نوال بنت عبدالعزيز العيد، **الابتزاز: المفهوم ، الأسباب ، العلاج**، موقع الكاتبة الرسمي، 5 جمادي الأول 1435هـ، للتفاصيل:

http://nawalaleid.com/cnt/lib/768

2- خالد ممدوح، **مبادئ التحقيق في الجرائم المعلوماتية**، موقع كنانة أونلاين، 2009/1/26، للتفاصيل:

http://kenanaonline.com/users/KhaledMamdouh/posts/81536

3- منى كامل تركي، **التحقيق الجنائي في الجرائم الإلكترونية**، 10 ابريل 2016، للتفاصيل:

https://amday55.blogspot.com/2016/04/blog-post.html

4- خاص موقع محاماة نت، **لمحة قانونية على الإثبات في الجرائم الإلكترونية**، موقع محاماة نت، 2016/12/22، للتفاصيل:

https://www.mohamah.net/law

5- أمل المرشدي، **أركان الجريمة الإلكترونية في التشريع الجزائري**، موقع محاماة نت، 2017/1/7، للتفاصيل:

https://www.mohamah.net/law

6- كرسوع، هنادي، **الابتزاز الإلكتروني بين الواقع والشرع والقانون**، موقع الشرطة الفلسطينية، 2016/7/4، للتفاصيل:

http://www.police.ps/ar/include/plugins/news/news.php?action=s&id=7969

7- أمل المرشدي، **الجرائم المعلوماتية**، موقع محاماة نت، نشر بتاريخ 2016/7/17، للتفاصيل:

https://www.mohamah.net/law

8- خاص موقع محاماة نت، **لمحة قانونية على الإثبات في الجرائم الإلكترونية**، موقع محاماة نت، نشر بتاريخ 2016/12/22، للتفاصيل:

https://www.mohamah.net/law

9- خالد ممدوح، **مبادئ التحقيق في الجرائم المعلوماتية**، موقع كنانة أونلاين، نشر بتاريخ 2009/1/26، للتفاصيل:

http://kenanaonline.com/users/KhaledMamdouh/posts/81536

10- نوال بنت عبدالعزيز العيد، **الابتزاز: المفهوم ، الأسباب ، العلاج**، موقع الكاتبة الرسمي، نشر بتاريخ 5 جمادي الأول 1435هـ، للتفاصيل:

http://nawalaleid.com/cnt/lib/768

11- أسامة الكحلوت، **ما هو قانون الجرائم الإلكترونية؟**، موقع دنيا الوطن، 2017/7/18، للتفاصيل:

https://www.alwatanvoice.com/arabic/news/2017/07/18/1068272.html

12- مجد عقل، **تفاقم ظاهرة الابتزاز الإلكتروني، هل يحلها قانون الجرائم الإلكترونية؟**، موقع بيرزيت أونلاين، 2018/2/26، للتفاصيل:

http://online.birzeit.edu/articles/Article/445/ar

13- آلاء البرعي، **الابتزاز الإلكتروني: "الشاباك" وباحثون عن الجنس والمال**، موقع صوت الترا فلسطين، 2017/12/2، للتفاصيل:

https://ultrapal.ultrasawt.com

14- نسرين فوزي اللواتي، **صعوبات اكتشاف "الجريمة الإلكترونية"**، موقع لغة العصر، 2017/12/10، للتفاصيل:

http://aitmag.ahram.org.eg/News/86864.aspx

15- **الرئيس المصري يصدر قرارا بشأن جرائم الإنترنت**، موقع sputnik عربي، 2018/8/18، للتفاصيل:

https://arabic.sputniknews.com

16- عبدالبصير حسن، **مجلس النواب المصري يقر قانون مكافحة الجريمة الإلكترونية**، موقع بي بي سي عربي، القاهرة، 7 يونيو/ حزيران 2018، للتفاصيل:

http://www.bbc.com/arabic/middleeast-44396471

17- **عقوبة جريمة الابتزاز في المملكة الأردنية الهاشمية**، موقع مكافحة الابتزاز والتهديد الإلكتروني، 2016/10/13، للتفاصيل:

https://www.antiextortion.net

18- خاص موقع bbc عربي، "**ابتزاز مئات الأطفال في بريطانيا**" **عبر الإنترنت**، 21 سبتمبر/ أيلول 2013، للتفاصيل:

http://www.bbc.com/arabic/worldnews/2013/09/130920_cyber_blackmail_children

19- عمار محمد، **9 طرق للتعامل مع الابتزاز الإلكتروني**، موقع صحيفة الشرق، 2017/8/10، للتفاصيل:

https://www.al-sharq.com/opinion/10/08/2017/9

20- محمود رجب فتح الله، **جريمة الابتزاز في القانون المصري**، موقع الحوار المتمدن، 2018/10/19، للتفاصيل:

http://www.m.ahewar.org/s.asp?aid=615334&r=0

21- خاص صحيفة المصري اليوم، **نائب: 50 حالة ابتزاز جنسي كل 10 أيام على مواقع التواصل الاجتماعي**، موقع صحيفة المصري اليوم، 19-06-2018، للتفاصيل:

https://www.almasryalyoum.com/news/details/1301069

22- اميمة سعيد، **لحالات التهديد والابتزاز الإلكتروني.. خطوات تقديم شكوى لمباحث الإنترنت**، موقع صحيفة الوطن الإلكترونية،2018/12/9، للتفاصيل:

https://www.elwatannews.com/news/details/3855054

23- الدستور تفتح **ملف الابتزاز العاطفي في مصر**، موقع صحيفة الدستور، 18 فبراير 2017، للتفاصيل:

https://www.dostor.org/1310954

24- خاص موقع وزارة الداخلية المصرية، **ضبط أحد الأشخاص لقيامه بالاستيلاء على عدد كبير من الحسابات على موقع فيس بوك، والاستيلاء على البيانات واستغلالها في ابتزازهم مادياً**، 2019/3/7، للتفاصيل:

https://moi.gov.eg/News/GetDetails?newsId=e6b41437-bbdb-41db-be72-b376040a0407

25- محمد حازم أبو رمضان، "**الابتزاز**" **وباء متفشٍّ في العالم المعاصر**، موقع الجزيرة نت، 2018/2/23، للتفاصيل:

https://blogs.aljazeera.net/blogs/2018/2/23

26- خاص موقع الخبر الأول، **ابتزاز وزير في جنوب أفريقيا بفيديو جنسي**، 2018/10/28، للتفاصيل:

https://read07.com/193872.html

27- فلسطين عبد الكريم، **وقف المساعدات الأمريكية .. ابتزاز سياسي وضغوطات اقتصادية**، وكالة الرأي الفلسطينية للإعلام، 2018/8/25، للتفاصيل:

http://alray.ps/ar/post/184063

28- خاص موقع القبس الالكتروني، **الابتزاز الوظيفي**، 7 أبريل 2006، للتفاصيل:

/https://alqabas.com/178755

سادساً: المراجع الأجنبية

1- Orin S. Kerr* **DIGITAL EVIDENCE AND THE NEW CRIMINAL PROCEDURE**، COLUMBIA LAW REVIEW {Vol .105-279}.

الملاحق:

ملحق رقم (1): قرار محكمة بشأن إدانة متهم بتهمة التهديد باستعمال الشبكة الإلكترونية خلافًا للمادة 15 ف1،

دولة فلسطين
السلطة القضائية

الحكم

الصادر عن محكمة صلح جنين المنعقدة بإجراء المحاكمة وإصدارة
باسم الشعب العربي الفلسطيني

في الدعوى رقم: 2018 / 1170 صح
اسم القاضي: [redacted]
كاتب الجلسة: [redacted]
المدعي/ة: 1- [redacted]
2- [redacted]
المتهم/ة: 1- [redacted]
التهمة/التهم: التهديد باستعمال الشبكة الإلكترونية او احدى وسائل تكنولوجيا المعلومات خلافا للمادة 15 ف 1 من قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية

الوقائع: أسندت النيابة العامة للمتهم [redacted] تهمة التهديد باستعمال الشبكة الإلكترونية او احدى وسائل تكنولوجيا المعلومات خلافا للمادة 15 ف 1 من قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية
الإجراءات: بالمحاكمة العلنية وبجلسة 2018/4/26 قيدت على المتهم التهمة المسندة إليه فأجاب بأنه غير مذنب وبجلسة 2018/06/24 صرح المتهم بأنه يعود عن اقراره السابق وانه مذنب وطلب من المحكمة الرحمة وبذات الجلسة قدمت النيابة العامة بينتها المسرة د/1 وبعد انتهاء من البدء التحقيقي بكامل محتوياته وبه حصلت النيابة العامة بينتها وصرح المتهم بأنه لا يرغب الإدلاء بإفادة وليس لديه شهود دفاع وتراجع كيل النيابة مذكرة ادانة المتهم بالتهمة المسندة اليه وبمطالبته حسب الاصول والقانون وليس المتهم من المحكمة اتخاذ الأسباب المخففة والتقديرية بحقه وختمت إجراءات المحاكمة بتلاوة الحكم الذي علة.

المحكمة

بالتدقيق في ملف هذه الدعوى وفي البينات المقدمة فيها من قبل النيابة العامة والمتمثلة في المبرز د/1 الملف التحقيقي بكافة محتوياته تجد المحكمة ان المتهم اعترف بالتهم المسندة اليه اعترافا واضحا وصريحا بما اسند اليه و التطابق للواقع والذي قنعت به المحكمة و الذي توفرت فيه جميع الشروط المنصوص عليها في المادة 214 من قانون الاجراءات الجزائية رقم 3 لسنة 2001 حيث اجاب في مجرى رده على التهم بالإجابة الآتية "... مذنب وادعو بفضل الرحمة ..." و الذي تاييد بالبينة المقدمة و المتمثلة في المبرز د/1 و الذي لم يعترض عليه المتهم و الذي جاء واضحا بصحيحا ما اسند للمتهم وبذلك الاعتراف الامر الذي يستوجب

ادانته بالتهم المسندة اليه

وعليه

تقرر المحكمة وعملا بأحكام الفقرة الثانية من المادة 274 من قانون الاجراءات الجزائية رقم 3 لسنة 2001 إدانة المتهم [redacted] بالتهمة المسندة إليه وهي التهديد باستعمال الشبكة الإلكترونية او احدى وسائل تكنولوجيا المعلومات خلافا للمادة 15 ف 1 من قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية والحكم عليه بالحبس لمدة ثلاثة شهور والمصادرة وإسقاط الحق الشخصي تحويل الحبس لعقوبة بواقع نصف دينار أردني عن كل يوم حبس
حكما حضوريا قابلا للاستئناف صدر وتلي علنا باسم الشعب العربي الفلسطيني وافهم في 2018/06/24

القاضي

ملحق رقم (2) صورة عن صحة النيابة العامة بشأن قضية الابتزاز الإلكتروني

النيابة العامة
لدولة فلسطين

ممارسة العدالة الجنائية

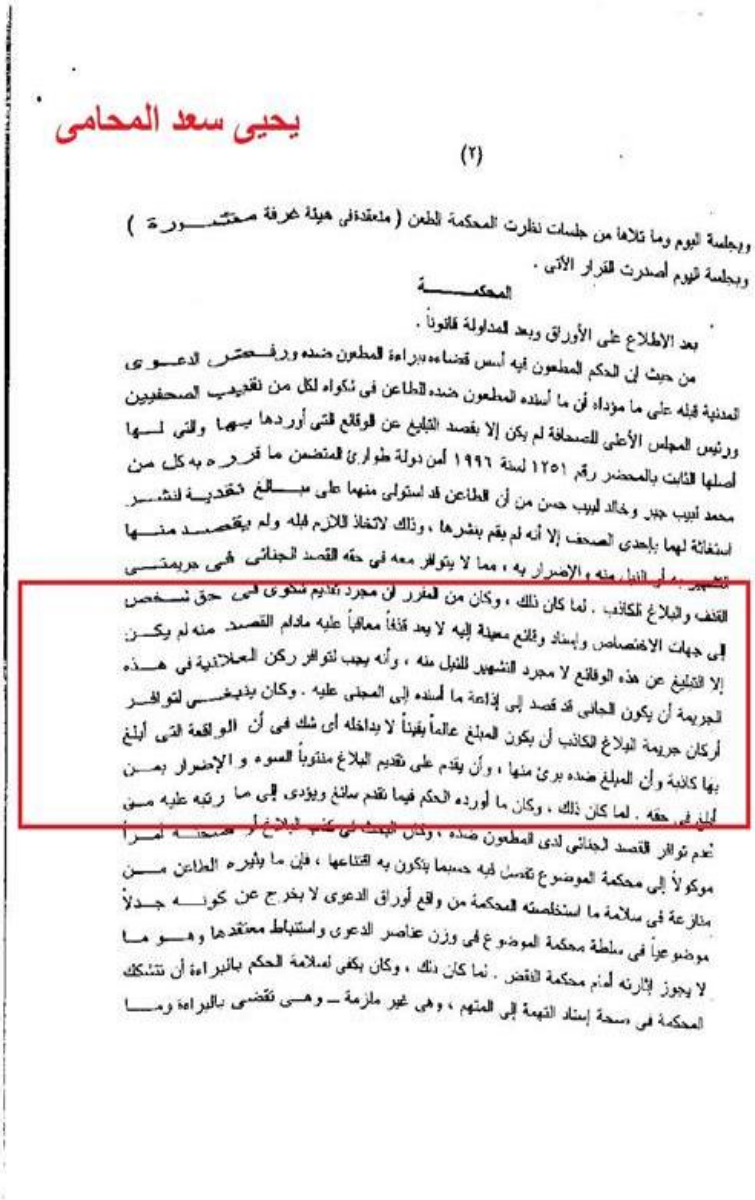
النيابة العامة تتمكن من الحصول على ادانه في قضية ابتزاز إلكتروني

أدانت محكمة صلح بيت لحم بهيئة القاضي سلام عقيل ، واستنادا إلى البينات التي قدمتها النيابة العامة بحق المتهم (و.ق) بتهمة استعمال الشبكة الالكترونية أو إحدى وسائل تكنولوجيا المعلومات في تهديد شخص أو ابتزازه خلافا لإحكام المادة 15/1 من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وحكمت عليه بالحبس مدة سنة.

وجاء الحكم بناء على المرافعات الخطية التي قدمتها نيابة بيت لحم أمام المحكمة ممثلة بوكيل النيابة العامة في نيابة بيت لحم الأستاذة نوره براهمة

التاريخ:- 05/09/2018
المكان:- رام الله

ملحق رقم (3): قرار محكمة بخصوص قضية قذف وتشهير في الصحف والمجلات



يحيى سعد المحامى

(٢)

وبجلسة اليوم وما تلاها من جلسات نظرت المحكمة الطعن (منعقدة في هيئة غرفة مشـــورة) وبجلسة اليوم أصدرت القرار الآتي .

المحكمـــــة

بعد الاطلاع على الأوراق وبعد المداولة قانوناً .

من حيث إن الحكم المطعون فيه أسس قضاءه برءاءة المطعون ضده ورفـض الدعـوى المدنية قبله على ما مؤداه أن ما أسنده المطعون ضده للطاعن في شكواه لكل من نقيب الصحفيين ورئيس المجلس الأعلى للصحافة لم يكن إلا بقصد التبليغ عن الوقائع التي أوردها بهما والتي لـها أصلها الثابت بالمحضر رقم ١٢٥١ لسنة ١٩٩٦ أمن دولة طوارئ المتضمن ما قرره به كل من محمد أديب جبر وخالد أديب حسن من أن الطاعن قد استولى منهما على مبـالغ نقدية لنشـر استغاثة لهما بإحدى الصحف إلا أنه لم يقم بنشرها ، وذلك لاتخاذ اللازم قبله ولم يقصـد منـها تشهير به أو النيل منه والإضرار به ، مما لا يتوافر معه في حقه القصد الجنائي في جريمتـي القذف والبلاغ الكاذب . لما كان ذلك ، وكان من المقرر أن مجرد تقديم شكوى إلى حق شـخص إلى جهات الاختصاص وإسناد وقائع معينة إليه لا يعد قذفاً معاقباً عليه مادام القصد منه لم يكـن إلا التبليغ عن هذه الوقائع لا مجرد التشهير للنيل منه ، وأنه يجب لتوافر ركن العلانية في هـذه الجريمة أن يكون الجاني قد قصد إلى إذاعة ما أسنده إلى المجني عليه . وكان يذيغـي لتوافـر أركان جريمة البلاغ الكاذب أن يكون المبلغ عالماً يقيناً لا يداخله أي شك في أن الواقعة التي أبلغ بها كاذبة وأن المبلغ ضده بريء منها ، وأن يقدم على تقديم البلاغ متوياً السوء و الإضرار بمـن أبلغ في حقه . لما كان ذلك ، وكان ما أورده الحكم فيما تقدم سائغ ويؤدي إلى ما رتبه عليه مـن عدم توافر القصد الجنائي لدى المطعون ضده ، وكان البحث في كذب البلاغ أو صحتـه أمـراً موكولاً إلى محكمة الموضوع تقدير فيه حسبما يتكون به اقتناعها ، فإن ما يثيره الطاعن مـن منازعة في سلامة ما استخلصته المحكمة من واقع أوراق الدعوى لا يخرج عن كونـه جـدلاً موضوعياً في سلطة محكمة الموضوع في وزن عناصر الدعوى واستنباط معتقدها وهـو مـا لا يجوز إثارته أمام محكمة النقض . لما كان ذلك ، وكان يكفي لسلامة الحكم بالبراءة أن تشكك المحكمة في صحة إسناد التهمة إلى المتهم ، وهي غير ملزمة – وهـي تقضي بالبراءة ومـا

(٣)

ويترتب على ذلك من رفض الدعوى المدنية ــ بأن ترد على كل دليل من أدلة الاتهام لأن في إغفال التحدث عنه ما يفيد حتماً أنها أطرحته ولم تر فيه ما تطمئن معه إلى الحكم بالإدانة متى كانت قد أحاطت بالدعوى عن بصر وبصيرة ــ كمال هو الحال في الدعوى المطروحة ــ ومن ثم فلا يعيب الحكم عدم تصديه لما قد يكون المدعي بالحقوق المدنية قد ساقه من قرائن تشير إلى ثبوت الاتهام مادمت المحكمة قد قطعت في أصل الواقعة وتشككت في ثبوت التهمة على المتهم ، ومن ثم فإن ما يثيره الطاعن في هذا الصدد ينحل إلى جدل في تقدير أدلة الدعوى مما لا يجوز إثارته أمام محكمة النقض . لما كان ما تقدم ، فإن الطعن برمته يكون على غير أساس مفصحاً عن عدم قبوله موضوعاً مع مصادرة الكفالة وإلزام الطاعن المصاريف المدنية .

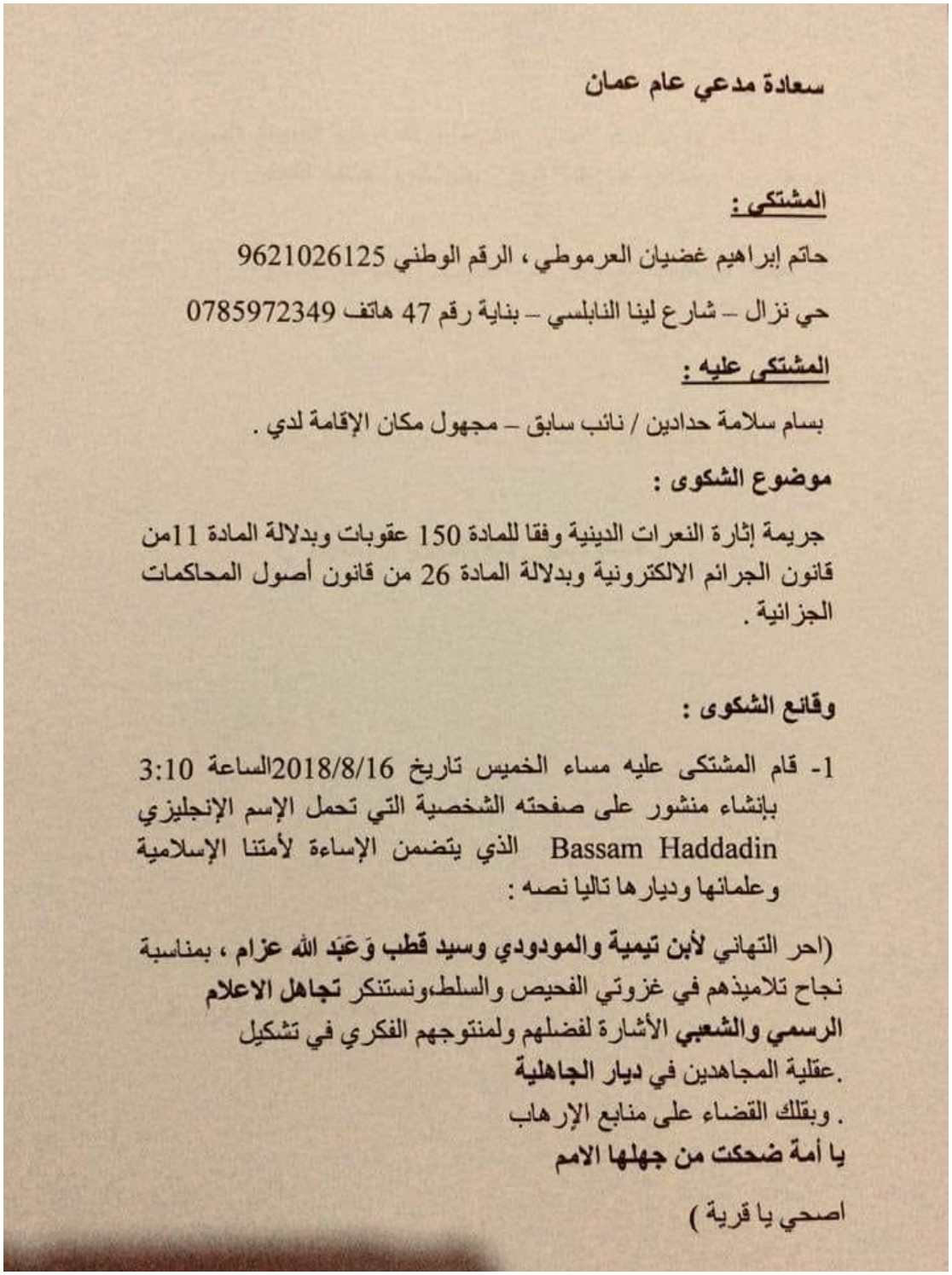
لذلك

أمرت الغرفة عدم قبول الطعن مع مصادرة الكفالة وإلزام الطاعن المصاريف المدنية .

أمين السر

نائب رئيس المحكمة

ملحق رقم (4): شكوى بخصوص حادثة قذف وإثارة للنعرات الطائفية خلافاً لقانون الجرائم الالكترونية الأردني:



سعادة مدعي عام عمان

المشتكي :

حاتم إبراهيم غضيان العرموطي ، الرقم الوطني 9621026125

حي نزال – شارع لينا النابلسي – بناية رقم 47 هاتف 0785972349

المشتكى عليه :

بسام سلامة حدادين / نائب سابق – مجهول مكان الإقامة لدي .

موضوع الشكوى :

جريمة إثارة النعرات الدينية وفقا للمادة 150 عقوبات وبدلالة المادة 11من قانون الجرائم الالكترونية وبدلالة المادة 26 من قانون أصول المحاكمات الجزائية .

وقائع الشكوى :

1- قام المشتكى عليه مساء الخميس تاريخ 2018/8/16الساعة 3:10 بإنشاء منشور على صفحته الشخصية التي تحمل الإسم الإنجليزي Bassam Haddadin الذي يتضمن الإساءة لأمتنا الإسلامية وعلمائها وديارها تاليا نصه :

(احر التهاني **لأبن تيمية والمودودي وسيد قطب وَعَبَد الله عزام** ، بمناسبة نجاح تلاميذهم في غزوتي الفحيص والسلط،ونستنكر **تجاهل الاعلام الرسمي والشعبي** الأشارة لفضلهم ولمنتوجهم الفكري في تشكيل .عقلية المجاهدين في **ديار الجاهلية** . وبقلك القضاء على منابع الإرهاب **يا أمة ضحكت من جهلها الامم**

اصحي يا قرية)

ملحق رقم (5): قانون رقم (10) المعدل لسنة 2018 للجرائم الإلكترونية في فلسطين

قرار بقانون رقم (10) لسنة 2018م
بشأن الجرائم الإلكترونية

رئيس دولة فلسطين

رئيس اللجنة التنفيذية لمنظمة التحرير الفلسطينية

استناداً لأحكام القانون الأساسي المعدل لسنة 2003م وتعديلاته، لا سيما أحكام المادة (43) منه،

وبعد الاطلاع على أحكام قانون العقوبات رقم (74) لسنة 1936م وتعديلاته، الساري في المحافظات الجنوبية،

والاطلاع على أحكام قانون العقوبات رقم (16) لسنة 1960م وتعديلاته، الساري في المحافظات الشمالية،

وعلى أحكام قانون الاتصالات السلكية واللاسلكية رقم (3) لسنة 1996م،

وعلى أحكام قانون الإجراءات الجزائية رقم (3) لسنة 2001م وتعديلاته،

وعلى أحكام القرار بقانون رقم (18) لسنة 2015م، بشأن مكافحة المخدرات والمؤثرات العقلية،

وعلى أحكام القرار بقانون رقم (20) لسنة 2015م، بشأن مكافحة غسل الأموال وتمويل الإرهاب وتعديلاته،

وعلى أحكام القرار بقانون رقم (6) لسنة 2017م، بشأن تنظيم نقل وزراعة الأعضاء البشرية،

وعلى أحكام القرار بقانون رقم (15) لسنة 2017م، بشأن المعاملات الإلكترونية،

وعلى أحكام القرار بقانون رقم (16) لسنة 2017م، بشأن الجرائم الإلكترونية،

وبناءً على تنسيب مجلس الوزراء بتاريخ 2018/04/17م،

وعلى الصلاحيات المخولة لنا،

وتحقيقاً للمصلحة العامة،

وباسم الشعب العربي الفلسطيني،

أصدرنا القرار بقانون الآتي:

مادة (1)

يكون للكلمات والعبارات الواردة في هذا القرار بقانون المعاني المخصصة لها أدناه، ما لم تدل القرينة على خلاف ذلك:

الوزارة: وزارة الاتصالات وتكنولوجيا المعلومات.

الوزير: وزير الاتصالات وتكنولوجيا المعلومات.

معالجة البيانات: إجراء أو تنفيذ عملية أو مجموعة عمليات على البيانات، سواء تعلقت بأفراد أو خلافه، بما في ذلك جمع تلك البيانات أو استلامها أو تسجيلها أو تخزينها أو تعديلها أو نقلها أو استرجاعها أو محوها أو نشرها، أو إعادة نشر بيانات أو حجب الوصول إليها، أو إيقاف عمل الأجهزة أو إلغاؤها أو تعديل محتوياتها.

تكنولوجيا المعلومات: أي وسيلة إلكترونية مغناطيسية بصرية كهروكيميائية، أو أي وسيلة أخرى، سواء أكانت مادية أم غير مادية، أو مجموعة وسائل مترابطة أو غير مترابطة، تستخدم لمعالجة البيانات وأداء المنطق والحساب أو الوظائف التخزينية، وتشمل أي قدرة تخزين بيانات أو اتصالات تتعلق أو تعمل بالاقتران مع مثل هذه الوسيلة.

البيانات والمعلومات الإلكترونية: كل ما يمكن تخزينه أو معالجته أو إنشاؤه أو توريده أو نقله باستخدام تكنولوجيا المعلومات، بوجه خاص الكتابة أو الصور أو الصوت أو الأرقام أو الحروف أو الرموز أو الإشارات، وغيرها.

الشبكة الإلكترونية: ارتباط بين أكثر من وسيلة لتكنولوجيا المعلومات للحصول على المعلومات وتبادلها، بما في ذلك الشبكات الخاصة أو العامة أو الشبكة العالمية (الإنترنت).

السجل الإلكتروني: مجموعة المعلومات التي تشكل بمجملها وصفاً لحالة تتعلق بشخص أو شيء ما، والتي يتم إنشاؤها أو إرسالها أو تسلمها أو تخزينها بوسائل إلكترونية.

المستند الإلكتروني: السجل الإلكتروني الذي يصدر باستخدام إحدى وسائل تكنولوجيا المعلومات، يتم إنشاؤه أو تخزينه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة تكنولوجيا المعلومات على وسيط مادي أو على أي وسيط إلكتروني آخر، ويكون قابلاً للاسترجاع بشكل يمكن فهمه.

الموقع الإلكتروني: مكان إتاحة المعلومات أو الخدمات على الشبكة الإلكترونية من خلال عنوان محدد.

الشخص: الشخص الطبيعي أو المعنوي.

التطبيق الإلكتروني: برنامج إلكتروني مصمم لأداء مهمة محددة بشكل مباشر للمستخدم أو لبرنامج إلكتروني آخر، يستخدم من خلال وسائل تكنولوجيا المعلومات أو ما في حكمها.

بيانات المرور: أي بيانات أو معلومات إلكترونية تنشأ عن طريق تكنولوجيا المعلومات تبين مصدر الإرسال، والوجهة المرسل إليها، والطريق الذي سلكه، ووقته، وتاريخه، وحجمه، ومدته، ونوع خدمة الاتصال.

كلمة السر: كل ما يستخدم للولوج لنظم تكنولوجيا المعلومات، وما في حكمها، للتأكد من هويته، وهي جزء من بيانات المرور، وتشمل الرموز وبصمة العين أو الوجه أو الأصبع أو ما في حكمها.

وسيلة التعامل الإلكتروني: البطاقة الإلكترونية التي تحتوي على شريط ممغنط أو شريحة ذكية أو ما في حكمها من تكنولوجيا المعلومات أو تطبيق إلكتروني، تحتوي هذه الوسيلة على بيانات أو معلومات إلكترونية تصدرها الجهات المرخصة بذلك.

البيانات الحكومية: البيانات الخاصة بالدولة والهيئات والمؤسسات العامة أو الشركات التابعة لها.

التشفير: تحويل بيانات إلكترونية إلى شكل يستحيل به قراءتها وفهمها دون إعادتها إلى هيئتها الأصلية.

الشفرة: مفتاح أو مفاتيح سرية خاصة، لشخص أو لجهة معينة تستخدم لتشفير البيانات الحاسوبية بالأرقام والحروف والرموز والبصمات أو ما في حكمها.

الالتقاط: مشاهدة البيانات أو المعلومات أو الحصول عليها.

الاختراق: الدخول غير المصرح به أو غير المشروع لنظم تكنولوجيا المعلومات أو الشبكة الإلكترونية.

التوقيع الإلكتروني: بيانات إلكترونية مضافة أو ملحقة أو مرتبطة بمعاملة إلكترونية، ولها طابع يسمح بتحديد هوية الشخص الذي وقعها، ويميزه عن غيره بغرض الموافقة على مضمون المعاملة.
أداة التوقيع: برنامج يستعمل لإنشاء توقيع إلكتروني على معاملة.
الشهادة: شهادة التصديق الإلكترونية التي تصدرها الوزارة أو الجهة المفوضة من قبلها لإثبات العلاقة والارتباط بين الموقع وبيانات التوقيع الإلكتروني.
مزود الخدمة: أي شخص يقدم لمستخدمي الخدمة الخاصة به القدرة على الاتصال عن طريق تكنولوجيا المعلومات، أو أي شخص آخر يقوم بمعالجة أو تخزين أو استضافة بيانات الحاسوب نيابة عن أي خدمة إلكترونية أو مستخدمي هذه الخدمة.
الإتلاف: تدمير البرامج الإلكترونية، سواء أكان كلياً أم جزئياً، أو جعلها على نحو غير صالحة للاستعمال.
معلومات المشترك: المعلومات الموجودة لدى مزود الخدمة والمتعلقة بمشتركي الخدمات حول نوع خدمة الاتصالات المستخدمة، والشروط الفنية، وفترة الخدمة، وهوية المشترك، وعنوانه البريدي أو الجغرافي أو هاتفه، ومعلومات الدفع المتوفرة بناءً على اتفاق أو تركيب الخدمة، وأي معلومات أخرى عن موقع تركيب معدات الاتصال بناءً على اتفاق الخدمة.
الموظف: كل من يعمل في القطاع العام أو الخاص أو المؤسسات الخاصة أو الهيئات المحلية والأهلية أو الجمعيات أو الشركات الخاصة التي تساهم بها الدولة، وكل من هو في حكمهم.
الحبس: وضع المحكوم عليه بحكم قضائي في أحد سجون الدولة مدة تتراوح بين أسبوع إلى ثلاث سنوات.
السجن: وضع المحكوم عليه بحكم قضائي في أحد سجون الدولة مدة تتراوح بين ثلاث سنوات إلى خمس عشرة سنة.

مادة (2)

1. تطبق أحكام هذا القرار بقانون على أي من الجرائم المنصوص عليها فيه، إذا ارتكبت كلياً أو جزئياً داخل فلسطين أو خارجها، أو امتد أثرها داخل فلسطين، سواء كان الفاعل أصلياً أم شريكاً أم محرضاً أم متدخلاً، على أن تكون الجرائم معاقباً عليها خارج فلسطين، مع مراعاة المبادئ العامة الواردة في قانون العقوبات النافذ.
2. يجوز ملاحقة كل من يرتكب خارج فلسطين، إحدى الجرائم المنصوص عليها في هذا القرار بقانون في إحدى الحالات الآتية:
   أ. إذا ارتكبت من مواطن فلسطيني.
   ب. إذا ارتكبت ضد أطراف أو مصالح فلسطينية.
   ج. إذا ارتكبت ضد أطراف أو مصالح أجنبية من قبل أجنبي أو شخص عديم الجنسية محل إقامته المعتاد داخل فلسطين، أو من قبل أجنبي أو شخص عديم الجنسية وجد بالأراضي الفلسطينية، ولم تتوافر في شأنه شروط التسليم القانونية.

مادة (3)

1. تنشأ وحدة متخصصة في جهاز الشرطة وقوى الأمن من مأموري الضبط القضائي تسمى "وحدة الجرائم الإلكترونية"، وتتولى النيابة العامة الإشراف القضائي عليها، كل في دائرة اختصاصه.
2. تتولى المحاكم النظامية والنيابة العامة، وفقاً لاختصاصاتهما، النظر في دعاوى الجرائم الإلكترونية.

مادة (4)

1. كل من دخل عمداً دون وجه حق بأي وسيلة موقعاً إلكترونياً أو نظاماً أو شبكة إلكترونية أو وسيلة تكنولوجيا معلومات أو جزء منها أو تجاوز الدخول المصرح به أو استمر في التواجد بها بعد علمه بذلك، يعاقب بالحبس، أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.
2. إذا ارتكب الفعل المذكور في الفقرة (1) من هذه المادة، على البيانات الحكومية، يعاقب بالحبس لمدة لا تقل عن ستة أشهر، أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألفي دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.
3. إذا ترتب على الدخول إلغاء بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي أو حذفها أو إضافتها أو إفشاؤها أو إتلافها أو تغييرها أو نقلها أو التقاطها أو نسخها أو نشرها أو إعادة نشرها أو ألحق ضرراً بالمستخدمين أو المستفيدين، أو تغيير الموقع الإلكتروني أو إلغاؤه أو تعديل محتوياته أو شغل عنوانه أو تصميماته أو طريقة استخدامه، أو انتحال شخصية مالكه أو القائم على إدارته، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.
4. إذا ارتكب الفعل المذكور في الفقرة (3) من هذه المادة على البيانات الحكومية، يعاقب بالسجن مدة لا تزيد على خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (5)

كل من أعاق أو عطل الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات بأي وسيلة كانت عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

مادة (6)

كل من أنتج أو أدخل عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، ما من شأنه إيقافها عن العمل أو تعطيلها أو إتلاف البرامج أو حذفها أو تعديلها، يعاقب بالسجن مدة لا تزيد على خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (7)

كل من التقط ما هو مرسل عن طريق الشبكة أو إحدى وسائل تكنولوجيا المعلومات أو سجله أو اعترضه أو تنصت عمداً دون وجه حق، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

مادة (8)

1. كل من قام عمداً بفك بيانات مشفرة في غير الأحوال المصرح بها قانوناً، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.
2. كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية أو أداة إنشاء التوقيع الإلكتروني المتعلقة بتوقيع شخص غيره، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.
3. كل من ارتكب جريمة باستخدام أي من الوسائل المذكورة في الفقرة (2) من هذه المادة، يعاقب بالسجن وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (9)

1. كل من ينتفع دون وجه حق بخدمات الاتصال عن طريق إحدى وسائل تكنولوجيا المعلومات أو ما في حكمها، يعاقب بالحبس مدة لا تقل عن ستة أشهر، أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.
2. إذا كان الانتفاع في الفقرة (1) من هذه المادة بقصد الربح، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

مادة (10)

كل من قام عمداً، عبر استخدام الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، بإنشاء أو نشر شهادة غير صحيحة أو قدم بيانات غير صحيحة عن هويته إلى الجهات المختصة بموجب القوانين الخاصة بإصدار الشهادات بغرض طلب استصدار شهادة أو إلغائها أو إيقافها، يعاقب بالحبس وبغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (11)

1. كل من زور مستنداً إلكترونياً رسمياً من مستندات الدولة أو الهيئات أو المؤسسات العامة معترفاً به قانوناً في نظام معلوماتي، يعاقب بالسجن مدة لا تقل عن خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.
2. إذا وقع التزوير، فيما عدا ذلك من المستندات، وكان من شأن ذلك إحداث ضرر، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.
3. كل من استعمل المستند المزور مع علمه بتزويره يعاقب بالعقوبة المقررة لجريمة استعمال السند المزور وفق قانون العقوبات النافذ.
4. كل من زور أو تلاعب بتوقيع أو أداة أو أنظمة توقيع إلكترونية رسمية، سواء تم ذلك باصطناعه أو إتلافه أو تعييبه أو تعديله أو تحويره، أو بأي طريقة أخرى تؤدي إلى تغيير الحقيقة في بياناته أو معلوماته، يعاقب بالسجن مدة لا تقل عن خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.
5. إذا وقع التزوير أو التلاعب فيما عدا ذلك من التواقيع الإلكترونية المذكورة في الفقرة (4) من هذه المادة، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.
6. كل من أنشأ بيانات توقيع أو أداة نظام توقيع إلكتروني رسمي أو للهيئات أو للمؤسسات العامة لا يحق له الحصول عليه، مستخدماً في ذلك معلومات أو بيانات كاذبة أو خاطئة، أو تواطأ مع غيره في إنشاء ذلك، يعاقب بالسجن مدة لا تقل عن خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.
7. إذا وقع الإنشاء فيما عدا ذلك من التواقيع الإلكترونية المذكورة في الفقرة (6) من هذه المادة، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد عن ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

مادة (12)

1. كل من استخدم الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في الوصول، دون وجه حق، إلى أرقام أو بيانات وسيلة التعامل الإلكترونية أو التلاعب فيها، يعاقب بالحبس مدة لا تقل عن ستة أشهر، أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.
2. كل من زور وسيلة تعامل إلكترونية بأي وسيلة كانت، أو صنع أو حاز بدون ترخيص أجهزة أو مواد تستخدم في إصدار أو تزوير بطاقة التعامل الإلكتروني، يعاقب بالعقوبة ذاتها المنصوص عليها في الفقرة (1) من هذه المادة.

3. كل من استخدم أو سهل استخدام وسيلة تعامل إلكترونية مزورة مع علمه بذلك أو قبل وسيلة تعامل إلكترونية غير سارية أو مزورة أو مسروقة مع علمه بذلك، يعاقب بالعقوبة ذاتها المنصوص عليها في الفقرة (1) من هذه المادة.
4. إذا تم ارتكاب الأفعال المنصوص عليها في أحكام هذه المادة بقصد الحصول على أموال أو بيانات غيره أو ما تتيحه من خدمات، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.
5. كل من استولى لنفسه أو لغيره على مال الغير بموجب الأحكام الواردة في هذه المادة، يعاقب بالحبس مدة لا تقل عن سنتين، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

مادة (13)

كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في سرقة أموال أو اختلاسها، يعاقب بالسجن أو بغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

مادة (14)

كل من استولى عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات لنفسه أو لغيره على مال منقول أو على سند أو توقيع إلكتروني أو بيانات إنشاء توقيع إلكتروني أو منظومة إنشاء توقيع إلكتروني، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

مادة (15)

1. كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في تهديد شخص آخر أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان هذا الفعل أو الامتناع مشروعاً، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.
2. إذا كان التهديد بارتكاب جناية أو بإسناد أمور خادشة للشرف أو الاعتبار، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (16)

1. كل من أرسل عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات قصداً كل ما هو مسموع أو مقروء أو مرئي يتضمن أعمالاً إباحية لمن هم فوق الثامنة عشر سنة ميلادية دون رضاه، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، ولا تزيد على سنتين، أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.
2. كل من أرسل أو نشر عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات قصداً كل ما هو مسموع أو مقروء أو مرئي يتضمن أعمالاً إباحية لمن لم يكمل الثامنة عشر سنة ميلادية أو تتعلق بالاستغلال الجنسي لهم، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.
3. كل من قام قصداً باستخدام الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في إنشاء أو إعداد أو حفظ أو معالجة أو عرض أو طباعة أو نشر أو ترويج أنشطة أو أعمال إباحية لغايات التأثير على من لم يكمل الثامنة عشر سنة ميلادية أو من هو من ذوي الإعاقة، يعاقب بالحبس مدة لا تقل عن سنتين، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة، أو بكلتا العقوبتين.

مادة (17)

دون الإخلال بالأحكام الواردة في القرار بقانون بشأن تنظيم نقل وزراعة الأعضاء البشرية النافذ، يعاقب كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، بقصد الاتجار في البشر أو الأعضاء البشرية أو تسهيل التعامل فيه، بالسجن مدة لا تزيد على سبع سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (18)

دون الإخلال بالأحكام الواردة في القرار بقانون بشأن مكافحة غسل الأموال وتمويل الإرهاب النافذ، يعاقب كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو إحدى وسائل تكنولوجيا المعلومات بقصد:
1. القيام بارتكاب جريمة غسل الأموال بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.
2. القيام بارتكاب جريمة تمويل الإرهاب بالسجن أو بغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

مادة (19)

دون الإخلال بالأحكام الواردة في القرار بقانون بشأن مكافحة المخدرات والمؤثرات العقلية النافذ، يعاقب كل من أنشأ أو نشر موقعاً على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، بقصد الاتجار أو الترويج للمخدرات أو المؤثرات العقلية، أو ما في حكمها، أو سهل التعامل فيها، أو بيع أو شرح أو عرض طرق إنتاج المواد المخدرة، بالسجن مدة لا تقل عن عشر سنوات، أو بغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

مادة (20)

كل من انتهك حق من حقوق الملكية الفكرية أو الأدبية أو الصناعية وفقاً للتشريعات النافذة، عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، يعاقب بالحبس مدة لا تزيد على ستة أشهر، أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

مادة (21)

1. لكل إنسان حق التعبير عن رأيه بالقول أو الكتابة أو التصوير أو غير ذلك من وسائل التعبير والنشر وفقاً للقانون.
2. حرية الإبداع الفني والأدبي مكفولة، ولا يجوز رفع أو تحريك الدعاوى لوقف أو مصادرة الأعمال الفنية والأدبية والفكرية أو ضد مبدعيها إلا بأمر قضائي، ولا توقع عقوبة سالبة للحرية أو التوقيف الاحتياطي في الجرائم التي ترتكب بسبب علانية المنتج الفني أو الأدبي أو الفكري.
3. حرية الصحافة والطباعة والنشر الورقي والمرئي والمسموع والإلكتروني مكفولة، وللفلسطينيين من أشخاص طبيعية أو اعتبارية عامة أو خاصة، حق ملكية وإصدار الصحف، وإنشاء وسائل الإعلام المرئية والمسموعة ووسائط الإعلام الرقمي وفقاً للقانون.
4. لا يجوز فرض قيود على الصحافة أو مصادرتها أو وقفها أو إنذارها أو إلغاؤها إلا وفقاً للقانون، وبموجب حكم قضائي.

مادة (22)

1. يحظر التدخل التعسفي أو غير القانوني في خصوصيات أي شخص أو في شؤون أسرته أو بيته أو مراسلاته.
2. كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات بقصد نشر أخبار أو صور أو تسجيلات صوتية أو مرئية، سواء كانت مباشرة أو مسجلة، تتصل بالتدخل غير القانوني في الحياة الخاصة أو العائلية للأفراد، ولو كانت صحيحة، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

مادة (23)

كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، بقصد إدارة مشروع مقامرة أو تسهيله أو تشجيعه أو الترويج له أو عرض ألعاب مقامرة، يعاقب بالحبس مدة لا تقل عن ستة أشهر، أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

مادة (24)

كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، بقصد عرض أي كلمات مكتوبة أو سلوكيات من شأنها أن تؤدي إلى إثارة الكراهية العنصرية أو الدينية أو التمييز العنصري بحق فئة معينة بسبب انتمائها العرقي أو المذهبي أو اللون أو الشكل أو بسبب الإعاقة، يعاقب بالحبس مدة لا تزيد عن سنة، أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

مادة (25)

كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، من شأنه التسويه أو التبرير لأعمال إبادة جماعية أو جرائم ضد الإنسانية نصت عليها المواثيق والقوانين الدولية أو المساعدة قصداً أو التحريض على ارتكاب جرائم ضد الإنسانية، يعاقب بالسجن مدة لا تقل عن عشر سنوات.

مادة (26)

كل من حاز بغرض الاستخدام جهازاً أو برنامجاً أو أي بيانات إلكترونية معدة أو كلمة سر أو ترميز دخول أو قدمها أو أنتجها أو وزعها أو استوردها أو صدرها أو روج لها، وذلك بغرض اقتراف أي من الجرائم المنصوص عليها في هذا القرار بقانون، يعاقب بالسجن مدة لا تزيد على خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (27)

1. كل موظف ارتكب أياً من الجرائم المنصوص عليها في هذا القرار بقانون، مستغلاً صلاحياته وسلطاته أثناء تأدية عمله، أو بسببه أو سهل ذلك لغيره، تزيد العقوبة بمقدار الثلث.
2. كل من ارتكب، من موظفي مزودي الخدمة، أياً من الجرائم المنصوص عليها في هذا القرار بقانون، أثناء تأدية عمله أو بسببه أو سهل ذلك لغيره، تزيد العقوبة بمقدار الثلثين.

مادة (28)

كل من حرض أو ساعد أو اتفق مع غيره على ارتكاب جريمة من الجرائم المنصوص عليها بموجب أحكام هذا القرار بقانون، بأي وسيلة إلكترونية، ووقعت الجريمة بناءً على هذا التحريض أو المساعدة أو الاتفاق، يعاقب بالعقوبات المقررة لفاعلها الأصلي.

مادة (29)

إذا ارتكب، باسم الشخص المعنوي أو لحسابه، إحدى الجرائم المنصوص عليها في هذا القرار بقانون، يعاقب بغرامة لا تقل عن خمسة آلاف دينار أردني، ولا تزيد على عشرة آلاف دينار أردني، وللمحكمة أن تقضي بحرمان الشخص المعنوي من مباشرة نشاطه لمدة أقصاها خمس سنوات أو أن تقضي بحله في حال كانت الجريمة معاقب عليها بالحبس لمدة لا تقل عن سنة، وذلك مع عدم الإخلال بالمسؤولية الجنائية للشخص الطبيعي التابع له.

مادة (30)

كل من نشر قصداً معلومات عن موقع إلكتروني محجوب بموجب أحكام المادة (39) من هذا القرار بقانون، باستخدام أنظمة أو موقع أو تطبيق إلكتروني، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

مادة (31)

يلتزم مزود الخدمة، وفقاً للإجراءات القانونية المقررة بالآتي:

1. تزويد الجهات المختصة بمعلومات المشترك التي تساعد في كشف الحقيقة، بناءً على طلب النيابة أو المحكمة المختصة.
2. حجب رابط أو محتوى أو تطبيق على الشبكة الإلكترونية بناءً على الأوامر الصادرة إليها من الجهات القضائية، مع مراعاة الإجراءات الواردة في المادة (39) من هذا القرار بقانون.
3. الاحتفاظ بمعلومات المشترك لمدة لا تقل عن ثلاث سنوات لغايات ما ورد في الفقرة (1) من هذه المادة.
4. التعاون ومساعدة الجهات المختصة وبناءً على قرار قاضي المحكمة المختصة في جمع أو تسجيل المعلومات أو البيانات الإلكترونية والاحتفاظ المؤقت بها.

مادة (32)

1. للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة.
2. يجب أن يكون أمر التفتيش مسبباً ومحدداً، ويجوز تجديده أكثر من مرة، ما دامت مبررات هذا الإجراء قائمة.
3. إذا أسفر التفتيش في الفقرة (2) من هذه المادة، عن ضبط أجهزة أو أدوات أو وسائل ذات صلة

بالجريمة، يتعين على مأموري الضبط القضائي تنظيم محضر بالمضبوطات، وعرضها على النيابة العامة لاتخاذ ما يلزم بشأنها.

4. لوكيل النيابة أن يأذن بالنفاذ المباشر لمأموري الضبط القضائي أو من يستعينون بهم من أهل الخبرة إلى أي وسيلة من وسائل تكنولوجيا المعلومات، وإجراء التفتيش فيها بقصد الحصول على البيانات أو المعلومات.

5. يشترط في مأمور الضبط القضائي أن يكون مؤهلاً للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية.

مادة (33)

1. للنيابة العامة الحصول على الأجهزة أو الأدوات أو الوسائل أو البيانات أو المعلومات الإلكترونية أو بيانات المرور أو البيانات المتعلقة بحركة الاتصالات أو بمستعمليها أو معلومات المشترك ذات الصلة بالجريمة الإلكترونية.

2. للنيابة العامة الإذن بالضبط والتحفظ على كامل نظام المعلومات أو جزء منه أو أي وسيلة من وسائل تكنولوجيا المعلومات التي من شأنها أن تساعد على كشف الحقيقة.

3. إذا لم يكن الضبط والتحفظ على نظام المعلومات ضرورياً أو تعذر إجراؤه، تنسخ البيانات أو المعلومات التي لها علاقة بالجريمة والبيانات التي تؤمن قراءتها وفهمها على وسيلة من وسائل تكنولوجيا المعلومات.

4. إذا استحال إجراء الضبط والتحفظ بصفة فعلية، يتعين حفاظاً على أدلة الجريمة استعمال كافة الوسائل المناسبة لمنع الوصول والنفاذ إلى البيانات المخزنة بنظام المعلومات.

5. تتخذ الاحتياطات الضرورية للحفاظ على سلامة المضبوط المتحفظ عليه، بما في ذلك الوسائل الفنية لحماية محتواها.

6. تحرر قدر الإمكان قائمة بالمضبوط المتحفظ عليه بحضور المتهم أو من وجد لديه المضبوط المتحفظ عليه، ويحرر تقرير بذلك، ويحفظ المضبوط المتحفظ عليه حسب الحالة في ظرف أو مغلف مختوم، ويكتب عليه ورقة مع بيان تاريخ التحفظ وساعته وعدد المحاضر والقضية.

مادة (34)

1. لقاضي الصلح أن يأذن للنائب العام أو أحد مساعديه بمراقبة الاتصالات والمحادثات الإلكترونية، وتسجيلها، والتعامل معها للبحث عن الدليل المتعلق بجناية أو جنحة يعاقب عليها بالحبس مدة لا تقل عن سنة، وذلك لمدة خمسة عشر يوماً قابلة للتجديد لمرة واحدة، بناءً على توافر دلائل جدية، وعلى من قام بالتفتيش أو المراقبة أو التسجيل أن ينظم محضراً بذلك يقدمه إلى النيابة العامة.

2. للنائب العام أو أحد مساعديه أن يأمر بالجمع والتزويد الفوري لأي بيانات، بما فيها حركة الاتصالات أو معلومات إلكترونية أو بيانات مرور أو معلومات المشترك التي يراها لازمة لمصلحة التحقيقات لغايات الفقرة (1) من هذه المادة، باستعمال الوسائل الفنية المناسبة، والاستعانة بذلك عند الاقتضاء بمزودي الخدمات، حسب نوع الخدمة التي يقدمها.

مادة (35)

على الجهات المختصة اتخاذ التدابير والإجراءات الكفيلة بالحفاظ على سلامة الأجهزة أو الأدوات أو وسائل تكنولوجيا المعلومات أو الأنظمة الإلكترونية أو البيانات أو المعلومات الإلكترونية وخصوصيتها محل التحفظ، إلى حين صدور قرار من الجهات القضائية ذات العلاقة بشأنها.

مادة (36)

1. للمحكمة المختصة أن تأذن بالاعتراض الفوري لمحتوى اتصالات، وتسجيلها أو نسخها بناءً على طلب من قبل النائب العام أو أحد مساعديه، ويتضمن قرار المحكمة جميع العناصر التي من شأنها التعريف بالاتصالات موضوع طلب الاعتراض والأفعال الموجبة له، ومدته.
2. تكون مدة الاعتراض في الفقرة (1) من هذه المادة، لا تزيد على ثلاثة أشهر من بداية تاريخ الشروع الفعلي في إنجازه، قابلة للتمديد مرة واحدة فقط.
3. يتعين على الجهة المكلفة بتنفيذ إذن الاعتراض إعلام النيابة العامة بالتاريخ الفعلي لانطلاق عملية الاعتراض، والتنسيق معها بخصوص اتخاذ التدابير اللازمة لحسن سيرها.

مادة (37)

يعتبر الدليل الناتج بأي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الإلكترونية أو البيانات والمعلومات الإلكترونية من أدلة الإثبات.

مادة (38)

تعتبر الأدلة المتحصل عليها بمعرفة الجهة المختصة أو جهات التحقيق من دول أخرى، من أدلة الإثبات، طالما أن الحصول عليها قد تم وفقاً للإجراءات القانونية والقضائية للتعاون الدولي.

مادة (39)

1. لجهات التحري والضبط المختصة، إذا ما رصدت قيام مواقع إلكترونية مستضافة داخل الدولة أو خارجها، يوضع أي عبارات أو أرقام أو صور أو أفلام أو أي مواد دعائية أو غيرها، من شأنها تهديد الأمن القومي أو النظام العام أو الآداب العامة، أن تعرض محضراً بذلك على النائب العام أو أحد مساعديه، وتطلب الإذن بحجب الموقع أو المواقع الإلكترونية أو حجب بعض روابطها من العرض.
2. يقدم النائب العام أو أحد مساعديه طلب الإذن لمحكمة الصلح خلال (24) ساعة، مشفوعاً بمذكرة برأيه، وتصدر المحكمة قرارها في الطلب، في ذات يوم عرضه عليها إما بالقبول أو بالرفض، على ألا تزيد مدة الحجب على ستة أشهر، ما لم تجدد المدة وفقاً للإجراءات المنصوص عليها في هذه المادة.

مادة (40)

فيما عدا الالتزامات المهنية المنصوص عليها في القانون، لا يجوز الاستناد إلى أسرار المهنة أو مقتضياتها للامتناع عن تقديم المعلومات أو الوثائق التي تطلب وفقاً لأحكام القانون.

مادة (41)

تلتزم أجهزة الدولة ومؤسساتها وهيئاتها والجهات والشركات التابعة لها بالآتي:

1. اتخاذ التدابير الأمنية الوقائية اللازمة لحماية أنظمتها المعلوماتية، ومواقعها الإلكترونية، وشبكاتها المعلوماتية، والبيانات والمعلومات الإلكترونية الخاصة بها.
2. الإسراع في إبلاغ الجهة المختصة عن أي جريمة منصوص عليها في هذا القرار بقانون، فور اكتشافها أو اكتشاف أي محاولة للالتقاط أو الاعتراض أو التنصت بشكل غير مشروع، وتزويد الجهة المختصة بجميع المعلومات لكشف الحقيقة.
3. الاحتفاظ ببيانات تكنولوجيا المعلومات، ومعلومات المشترك لمدة لا تقل عن (120) يوماً، وتزويد الجهة المختصة بتلك البيانات.
4. التعاون مع الجهة المختصة لتنفيذ اختصاصاتها.

مادة (42)

1. تعمل الجهات المختصة على تيسير التعاون مع نظيراتها في البلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصادق عليها، أو طبق مبدأ المعاملة بالمثل، بقصد الإسراع في تبادل المعلومات، بما من شأنه أن يكفل الإنذار المبكر بجرائم أنظمة المعلومات والاتصال، وتفادي ارتكابها، والمساعدة على التحقيق فيها، وتتبع مرتكبيها.
2. يتوقف التعاون المشار إليه في الفقرة السابقة على التزام الدولة الأجنبية المعنية بالحفاظ على سرية المعلومات المحالة إليها، والتزامها بعدم إحالتها إلى طرف آخر أو استغلالها لأغراض أخرى غير مكافحة الجرائم المعينة بهذا القرار بقانون.

مادة (43)

1. يتعين على الجهات المختصة أن تقدم العون للجهات النظيرة في الدول الأخرى، لأغراض تقديم المساعدة القانونية المتبادلة، وتسليم المجرمين في التحقيقات والإجراءات الجنائية المرتبطة بالجرائم المنصوص عليها في هذا القرار بقانون، وفقاً للقواعد التي يقررها قانون الإجراءات الجزائية النافذ والاتفاقيات الثنائية أو متعددة الأطراف التي تكون الدولة طرفاً فيها، أو بمبدأ المعاملة بالمثل، وذلك بما لا يتعارض مع أحكام هذا القرار بقانون أو أي قانون آخر.
2. لا ينفذ طلب المساعدة القانونية أو طلب تسليم المجرمين، استناداً إلى أحكام هذا القرار بقانون، إلا إذا كانت قوانين الدولة الطالبة وقوانين الدولة تعاقب على الجريمة موضوع الطلب أو على جريمة مماثلة، وتعتبر ازدواجية التجريم مستوفاة، بغض النظر عما إذا كانت قوانين الدولة الطالبة تدرج الجريمة في فئة الجرائم ذاتها أو تستخدم في تسمية الجريمة المصطلح ذاته المستخدم في الدولة، بشرط أن يكون الفعل موضوع الطلب مجرماً بمقتضى قوانين الدولة الطالبة.

مادة (44)

مع عدم الإخلال بأي عقوبة أشد، ينص عليها قانون العقوبات الساري أو أي قانون آخر، يعاقب مرتكبو الجرائم المعاقب عليها بموجب أحكام هذا القرار بقانون، بالعقوبات المنصوص عليها فيه.

مادة (45)

كل من ارتكب فعلاً يشكل جريمة بموجب أي تشريع نافذ باستخدام الشبكة الإلكترونية أو بإحدى وسائل تكنولوجيا المعلومات، أو اشترك فيها أو تدخل فيها أو حرض على ارتكابها، ولم ينص عليها في هذا القرار بقانون، يعاقب بالعقوبة ذاتها المقررة لتلك الجريمة في ذلك التشريع.

مادة (46)

كل من أفشى سرية الإجراءات المنصوص عليها في هذا القرار بقانون، في غير الأحوال المصرح بها قانوناً، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

مادة (47)

كل من أقدم على العبث بأدلة قضائية معلوماتية أو أقدم على إتلافها أو إخفائها أو التعديل فيها أو محوها، يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (48)

يعاقب من يشترك بطريق الاتفاق أو التحريض أو المساعدة أو التدخل في ارتكاب جناية أو جنحة معاقب عليها بموجب أحكام هذا القرار بقانون، بالعقوبات ذاتها المقررة للفاعل الأصلي، وإن لم تقع الجريمة يعاقب بنصف العقوبة.

مادة (49)

يعد مرتكباً جريمة الشروع كل من شرع في ارتكاب جناية أو جنحة من الجرائم المنصوص عليها في هذا القرار بقانون، ويعاقب بنصف العقوبة المقررة لها.

مادة (50)

دون الإخلال بالعقوبات المنصوص عليها في هذا القرار بقانون، وحقوق الغير حسن النية، على المحكمة أن تصدر قراراً يتضمن الآتي:

1. مدة إغلاق المحل، وحجب الموقع الإلكتروني الذي ارتكبت فيه أو بواسطته تلك الجرائم بحسب الأحوال.
2. مصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القرار بقانون أو الأموال المتحصلة منها، على أن تكون إزالة المخالفة على نفقة الفاعل.

مادة (51)

تضاعف العقوبة المنصوص عليها في هذا القرار بقانون في حال تكرار الجاني أياً من الجرائم المنصوص عليها فيه، سواء ارتكبت في فلسطين أو خارجها، وتعتبر الأحكام الأجنبية سابقة في التكرار بحق الجاني.

مادة (52)

تضاعف العقوبة المقررة للجرائم المعاقب عليها بموجب أحكام هذا القرار بقانون، في أي من الحالات الآتية:

1. إذا وقعت الجريمة على موقع أو نظام معلوماتي أو بيانات أو أرقام أو حروف أو شفرات أو صور يدار بمعرفة الدولة أو أحد الأشخاص المعنوية العامة أو مملوك لها أو يخصها، بما في ذلك الهيئات المحلية.
2. ارتكاب الجاني الجريمة من خلال عصابة منظمة.
3. التغرير أو استغلال من لم يكمل الثامنة عشر سنة ميلادية.
4. إذا وقعت الجريمة على نظام معلومات أو موقع إلكتروني أو شبكة معلوماتية تتعلق بتحويل الأموال أو بتقديم خدمات الدفع أو التقاص أو التسويات أو أي من الخدمات المصرفية المقدمة من البنوك والشركات المالية.

مادة (53)

يعفى من العقوبات المنصوص عليها في هذا القرار بقانون، كل من بادر من الجناة بإبلاغ السلطات المختصة بأي معلومات عن الجريمة وعن الأشخاص المشتركين فيها، وذلك قبل علم السلطات بها وقبل وقوع الضرر، ويجوز للمحكمة أن تقضي بوقف تنفيذ العقوبة إذا حصل الإبلاغ بعد علم السلطات المختصة، وأدى إلى ضبط باقي الجناة.

مادة (54)

تتولى الوزارة وفقاً لاختصاصها تقديم الدعم والمساعدة الفنية لجهات إنفاذ القانون، ويعتبر موظفو الوزارة المعينون من قبل الوزير مأموري ضبط قضائي لغايات تنفيذ أحكام هذا القرار بقانون.

مادة (55)

1. يلغى القرار بقانون رقم (16) لسنة 2017م، بشأن الجرائم الإلكترونية.
2. يلغى كل ما يتعارض مع أحكام هذا القرار بقانون.

مادة (56)

يعرض هذا القرار بقانون على المجلس التشريعي في أول جلسة يعقدها لإقراره.

مادة (57)

على الجهات المختصة كافة، كل فيما يخصه، تنفيذ أحكام هذا القرار بقانون، ويعمل به من تاريخ نشره في الجريدة الرسمية.

صدر في مدينة رام الله بتاريخ: 2018/04/29 ميلادية
الموافق: 13/شعبان/1439 هجرية

محـــمود عـــباس
رئيـــــــس دولـــــــة فلسطـــــــين
رئيس اللجنة التنفيذية لمنظمة التحرير الفلسطينية

الملحق رقم (8): قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015

المادة 1

يسمى هذا القانون (قانون الجرائم الإلكترونية لسنة 2015) ويعمل به من تاريخ نشره في الجريدة الرسمية.

المادة 2

يكون للكلمات والعبارات التالية حيثما وردت في هذا القانون المعاني المخصصة لها أدناه ما لم تدل القرينة على غير ذلك-:

نظام المعلومات: مجموعة البرامج والأدوات المعدة لإنشاء البيانات أو المعلومات الكترونيا، أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو إدارتها أو عرضها بالوسائل الإلكترونية.

البيانات: الأرقام أو الحروف أو الرموز أو الأشكال أو الأصوات أو الصور أو الرسومات التي ليس لها دلالة بذاتها.

المعلومات: البيانات التي تمت معالجتها واصبح لها دلالة.

الشبكة المعلوماتية: ارتباط بين اكثر من نظام معلومات لإتاحة البيانات والمعلومات والحصول عليها.

الموقع الإلكتروني: حيز لإتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد.

التصريح: الإذن الممنوح من صاحب العلاقة إلى شخص أو اكثر أو للجمهور للدخول إلى أو استخدام نظام المعلومات أو الشبكة المعلوماتية بقصد الاطلاع أو الغاء أو حذف أو إضافة أو تغيير أو إعادة نشر بيانات أو معلومات أو حجب الوصول اليها أو إيقاف عمل الأجهزة أو تغيير موقع الكتروني أو الغائه أو تعديل محتوياته.

البرامج: مجموعة من الأوامر والتعليمات الفنية المعدة لإنجاز مهمة قابلة للتنفيذ باستخدام انظمة المعلومات.

المادة 3

أ- يعاقب كل من دخل قصداً إلى الشبكة المعلوماتية أو نظام معلومات باي وسيلة دون تصريح أو بما يخالف أو يجأوز التصريح، بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة اشهر أو بغرامة لا تقل عن (100) مائة دينار ولا تزيد على (200) مائتي دينار أو بكلتا هاتين العقوبتين.

ب- اذا كان الدخول المنصوص عليه في الفقرة)أ) من هذه المادة لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل الشبكة المعلوماتية أو نظام معلومات الشبكة المعلوماتية فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنة وبغرامة لا تقل عن (200 (مائتي دينار ولا تزيد على (1000) الف دينار.

ج- يعاقب كل من دخل قصداً إلى موقع الكتروني لتغييره أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) الف دينار.

المادة 4

يعاقب كل من ادخل أو نشر أو استخدم قصداً برنامجا عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ أو التقاط أو تمكين الآخرين من الاطلاع على بيانات أو معلومات أو إعاقة أو تشويش أو إيقاف أو تعطيل عمل نظام معلومات أو الوصول اليه أو تغيير موقع الكتروني أو الغائه أو إتلافه أو تعديل محتوياته أو اشغاله أو انتحال صفته أو انتحال شخصية مالكه دون تصريح أو بما يجأوز أو يخالف التصريح بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) الف دينار.

المادة 5

يعاقب كل من قام قصداً بالتقاط أو باعتراض أو بالتنصت أو اعاق أو حور أو شطب محتويات على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) الف دينار.

المادة 6

يعاقب كل من حصل قصدا دون تصريح عن طريق الشبكة المعلوماتية أو أي نظام معلومات على بيانات أو معلومات تتعلق ببطاقات الائتمان أو بالبيانات أو بالمعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية بالحبس مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (2000)الفي دينار.

المادة 7

يعاقب كل من قام بأحد الأفعال المنصوص عليها في المواد (3) و(4) و(5) و(6) من هذا القانون إذا وقعت على نظام معلومات أو موقع الكتروني أو شبكة معلوماتية تتعلق بتحويل الأموال، أو بتقديم خدمات الدفع أو التقاص أو

التسويات أو باي من الخدمات المصرفية المقدمة من البنوك والشركات المالية بالأشغال الشاقة المؤقتة مدة لا تقل عن خمس سنوات وبغرامة لا تقل عن (5000) خمسة آلاف دينار ولا تزيد عن (15000 (خمسة عشر الف دينار.

المادة 8

تضاعف العقوبة على الجرائم المنصوص عليها في المواد من (3) إلى (6) من هذا القانون بحق كل من قام بارتكاب أي منها بسبب تأديته وظيفته أو عمله أو باستغلال أي منهما

المادة 9

أ- يعاقب كل من ارسل أو نشر عن طريق نظام معلومات أو الشبكة المعلوماتية قصداً كل ما هو مسموع أو مقروء أو مرئي يتضمن أعمالا إباحية وتتعلق بالاستغلال الجنسي لمن لم يكمل الثامنة عشرة من العمر بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (300) ثلاثمائة دينار ولا تزيد على (5000) خمسة الاف دينار.

ب- يعاقب كل من قام قصداً باستخدام نظام معلومات أو الشبكة المعلوماتية في إنشاء أو إعداد أو حفظ أو معالجة أو عرض أو طباعة أو نشر أو ترويج أنشطة أو أعمال إباحية لغايات التأثير على من لم يكمل الثامنة عشرة من العمر أو من هو معوق نفسيا أو عقليا، أو توجيهه أو تحريضه على ارتكاب جريمة، بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن (1000)الف دينار ولا تزيد على (5000) خمسة الاف دينار.

ج- يعاقب كل من قام قصداً باستخدام نظام معلومات أو الشبكة المعلوماتية لغايات استغلال من لم يكمل الثامنة عشرة من العمر أو من هو معوق نفسيا أو عقليا، في الدعارة أو الأعمال الإباحية بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن (5000) خمسة الاف دينار ولا تزيد على (15000) خمسة عشر الف دينار.

المادة 10

يعاقب كل من استخدم الشبكة المعلوماتية أو أي نظام معلومات أو أنشأ موقعا الكترونيا للتسهيل أو الترويج للدعارة بالحبس مدة لا تقل عن ستة اشهر وبغرامة لا تقل عن (300) ثلاثمائة دينار ولا تزيد على (5000) خمسة الاف دينار.

المادة 11

يعاقب كل من قام قصدا بإرسال أو إعادة إرسال أو نشر بيانات أو معلومات عن طريق الشبكة المعلوماتية أو الموقع الإلكتروني أو أي نظام معلومات تنطوي على ذم أو قدح أو تحقير أي شخص بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن (100) مائة دينار ولا تزيد على (2000) الفي دينار.

المادة 12

أ- يعاقب كل من دخل قصداً دون تصريح أو بما يخالف أو يجأوز التصريح إلى الشبكة المعلوماتية أو نظام معلومات باي وسيلة كانت بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس مدة لا تقل عن أربعة اشهر وبغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (5000) خمسة الاف دينار.

ب- اذا كان الدخول المشار اليه في الفقرة)أ) من هذه المادة، بقصد الغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها أو إفشائها، فيعاقب الفاعل بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن (1000) الف دينار ولا تزيد على (5000) خمسة الاف دينار.

ج- يعاقب كل من دخل قصداً إلى موقع الكتروني للاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس بالأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس مدة لا تقل عن أربعة اشهر وبغرامة لا تقل عن (500) خمسمائة دينار.

د- اذا كان الدخول المشار اليه في الفقرة)ج) من هذه المادة لإلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها، فيعاقب الفاعل بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن (1000) الف دينار ولا تزيد على (5000) خمسة آلاف دينار.

المادة 13

أ- مع مراعاة الشروط والأحكام المقررة في التشريعات النافذة ومراعاة حقوق المشتكى عليه الشخصية، يجوز لموظفي الضابطة العدلية، بعد الحصول على اذن من المدعي العام المختص أو من المحكمة المختصة، الدخول إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم، وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضرا بذلك ويقدمه إلى المدعي العام المختص.

ب- مع مراعاة الفقرة (أ) من هذه المادة ومراعاة حقوق الآخرين ذوي النية الحسنة، وباستثناء المرخص لهم وفق أحكام قانون الاتصالات ممن لم يشتركوا باي جريمة منصوص عليها في هذا القانون، يجوز لموظفي الضابطة العدلية ضبط الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل المستخدمة لارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون والأموال المتحصلة منها والتحفظ على المعلومات والبيانات المتعلقة بارتكاب أي منها.

ج- للمحكمة المختصة الحكم بمصادرة الأجهزة والأدوات والوسائل والمواد وتوقيف أو تعطيل عمل أي نظام معلومات أو موقع الكتروني مستخدم في ارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون ومصادرة الأموال المتحصلة من تلك الجرائم والحكم بإزالة المخالفة على نفقة الفاعل.

المادة 14

يعاقب كل من قام قصداً بالاشتراك أو التدخل أو التحريض على ارتكاب أي من الجرائم المنصوص عليها في هذا القانون بالعقوبة المحددة فيه لمرتكبيها.

المادة 15

كل من ارتكب أي جريمة معاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتية أو أي نظام معلومات أو موقع الكتروني أو اشترك أو تدخل أو حرض على ارتكابها، يعاقب بالعقوبة المنصوص عليها في ذلك التشريع.

المادة 16

تضاعف العقوبة المنصوص عليها في هذا القانون في حال تكرار أي من الجرائم المنصوص عليها فيه.

المادة 17

تقام دعوى الحق العام والحق الشخصي على المشتكى عليه أمام المحاكم الأردنية اذا ارتكبت أي من الجرائم المنصوص عليها في هذا القانون باستخدام أنظمة معلومات داخل المملكة أو الحقت أضرارا باي من مصالحها أو بأحد المقيمين فيها أو ترتبت أثار الجريمة فيها، كليا أو جزئيا، أو ارتكبت من احد الأشخاص المقيمين فيها.

المادة 18

رئيس الوزراء والوزراء مكلفون بتنفيذ أحكام هذا القانون.

4/5/2015

ملحق رقم (9): قانون الجرائم الإلكترونية الفلسطيني رقم 16 لسنة 2017م

عدد ممتاز (14) الوقائع الفلسطينية 2017/7/9

البيانات الإلكترونية: كل ما يمكن تخزينه أو معالجته أو إنشاؤه أو نقله باستخدام تكنولوجيا المعلومات، بوجه خاص الكتابة، أو الصور، أو الصوت، أو الأرقام، أو الحروف، أو الرموز، أو الإشارات، وغيرها.

المعلومات الإلكترونية: أية معلومات يمكن تخزينها ومعالجتها وتوريدها ونقلها بوسائل تكنولوجيا المعلومات بوجه خاص بالكتابة، أو الصور، أو الصوت، أو الأرقام، أو الحروف، أو الرموز، أو الإشارات، وغيرها.

الشبكة الإلكترونية: هي ارتباط بين أكثر من وسيلة لتكنولوجيا المعلومات للحصول على المعلومات وتبادلها بما في ذلك الشبكات الخاصة أو العامة أو الشبكة العالمية (الإنترنت).

السجل الإلكتروني: مجموعة المعلومات التي تشكل بمجملها وصفاً لحالة تتعلق بشخص أو شيء ما، والتي يتم إنشاؤها، أو إرسالها، أو تسلمها، أو تخزينها بوسائل إلكترونية.

المستند الإلكتروني: هو السجل الإلكتروني الذي يصدر باستخدام إحدى وسائل تكنولوجيا المعلومات، يتم إنشاؤه أو تخزينه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة تكنولوجيا المعلومات على وسيط مادي أو على أي وسيط إلكتروني آخر، ويكون قابلاً للاسترجاع بشكل يمكن فهمه.

الموقع الإلكتروني: هو مكان إتاحة المعلومات أو الخدمات على الشبكة الإلكترونية من خلال عنوان محدد.

الشخص: الشخص الطبيعي أو المعنوي.

التطبيق الإلكتروني: هو برنامج إلكتروني مصمم لأداء مهمة محددة بشكل مباشر للمستخدم أو لبرنامج إلكتروني آخر، يستخدم من خلال وسائل تكنولوجيا المعلومات أو ما في حكمها.

بيانات المرور: أية بيانات أو معلومات إلكترونية تنشأ عن طريق تكنولوجيا المعلومات تبين مصدر الإرسال والوجهة المرسل إليها، والطريق الذي سلكه، ووقته، وتاريخه، وحجمه، ومدته ونوع خدمة الاتصال.

كلمة السر: هي كل ما يستخدم للولوج لنظم تكنولوجيا المعلومات وما في حكمها للتأكد من هويته وهي جزء من بيانات المرور، وتشمل الرموز وبصمة العين أو الوجه أو الأصبع أو ما في حكمها.

وسيلة التعامل الإلكتروني: هي البطاقة الإلكترونية التي تحتوي على شريط ممغنط أو شريحة ذكية أو ما في حكمها من تكنولوجيا المعلومات أو تطبيق إلكتروني، تحتوي هذه الوسيلة على بيانات أو معلومات إلكترونية تصدرها الجهات المرخصة بذلك.

البيانات الحكومية: يشمل ذلك بيانات الدولة والهيئات والمؤسسات العامة أو الشركات التابعة لها.

التشفير: هو تحويل بيانات إلكترونية إلى شكل يستحيل به قراءتها وفهمها دون إعادتها إلى هيئتها الأصلية.

الشفرة: هي مفتاح، أو مفاتيح سرية خاصة، لشخص أو لجهة معينة تستخدم لتشفير البيانات الحاسوبية بالأرقام والحروف والرموز أو ما في حكمها.

الالتقاط: مشاهدة البيانات أو المعلومات أو الحصول عليها.

الاختراق: هو الدخول غير المصرح به أو غير المشروع لنظم تكنولوجيا المعلومات أو الشبكة الإلكترونية.

التوقيع الإلكتروني: بيانات إلكترونية مضافة أو ملحقة أو مرتبطة بمعاملة إلكترونية، ولها طابع يسمح بتحديد هوية الشخص الذي وقعها ويميزه عن غيره بغرض الموافقة على مضمون المعاملة.
اداة التوقيع: هي برنامج يستعمل لإنشاء توقيع إلكتروني على معاملة.
الشهادة: شهادة التصديق الإلكترونية التي تصدرها الوزارة أو الجهة المفوضة من قبلها لإثبات العلاقة والارتباط بين الموقع وبيانات التوقيع الإلكتروني.
مزود الخدمة: هو أي شخص يقدم لمستخدمي الخدمة الخاصة به القدرة على الاتصال عن طريق تكنولوجيا المعلومات، أو اي شخص آخر يقوم بمعالجة أو تخزين أو استضافة بيانات الحاسوب نيابة عن أية خدمة إلكترونية أو مستخدمي هذه الخدمة.
الإتلاف: هو تدمير البرامج الإلكترونية سواء أكان كلياً أم جزئياً، أو جعلها على نحو غير صالحة للاستعمال.
معلومات المشترك: أية معلومات موجودة لدى مزود الخدمة والمتعلقة بمشتركي الخدمات بما في ذلك:
- نوع خدمة الاتصالات المستخدمة والشروط الفنية وفترة الخدمة.
- هوية المشترك وعنوانه البريدي أو الجغرافي أو هاتفه، ومعلومات الدفع المتوفرة بناءً على اتفاق أو تركيب الخدمة.
- أية معلومات أخرى عن موقع تركيب معدات الاتصال بناءً على اتفاق الخدمة.

الموظف: كل من يعمل في القطاع العام، أو الخاص، أو المؤسسات الخاصة، أو الهيئات المحلية والأهلية، أو الجمعيات، أو الشركات الخاصة التي تساهم بها الدولة، وكل من هو في حكمهم.

مادة (2)

1. تطبق أحكام هذا القرار بقانون على أي من الجرائم المنصوص عليها فيه، إذا ارتكبت كلياً أو جزئياً داخل فلسطين أو خارجها، أو امتد أثرها داخل فلسطين، سواء أكان الفاعل أصلياً، أم شريكاً، أم محرضاً، أم متدخلاً، على أن تكون الجرائم معاقباً عليها خارج فلسطين مع مراعاة المبادئ العامة الواردة في قانون العقوبات النافذ.
2. يجوز ملاحقة كل من يرتكب خارج فلسطين إحدى الجرائم المنصوص عليها بهذا القرار بقانون في إحدى الحالات الآتية:
   أ. إذا ارتكبت من مواطن فلسطيني.
   ب. إذا ارتكبت ضد أطراف أو مصالح فلسطينية.
   ج. إذا ارتكبت ضد أطراف أو مصالح أجنبية من قبل أجنبي أو شخص عديم الجنسية يوجد محل إقامته المعتاد داخل فلسطين، أو من قبل أجنبي أو شخص عديم الجنسية وجد في الأراضي الفلسطينية، ولم تتوافر في شأنه شروط التسليم القانونية.

مادة (3)

1. تنشأ وحدة متخصصة في الجرائم الإلكترونية في الأجهزة الشرطية وقوى الأمن على أن تتمتع بصفة الضابطة القضائية، وتتولى النيابة العامة الإشراف على مأموري الضبط القضائي كل في دائرة اختصاصه.

2. تتولى المحاكم النظامية والنيابة العامة، وفقاً لاختصاصاتهما، بالنظر في دعاوى الجرائم الإلكترونية.

مادة (4)

1. كل من دخل عمداً دون وجه حق بأية وسيلة موقعاً إلكترونياً، أو نظاماً، أو شبكة إلكترونية، أو وسيلة تكنولوجيا معلومات، أو جزء منها، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني ولا تزيد على ألف دينار أردني أو بالعقوبتين كلتيهما.
2. إذا ارتكب الفعل المحدد في الفقرة (1) من هذه المادة على البيانات الحكومية، يعاقب بالحبس لمدة لا تقل عن ستة شهور أو بغرامة لا تقل عن مائتي دينار أردني ولا تزيد على ألف دينار أردني أو بالعقوبتين كلتيهما.
3. إذا ترتب على الدخول إلغاء بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي، أو حذفها، أو إضافتها، أو إفشاؤها، أو إتلافها، أو تدميرها، أو تغييرها، أو نقلها، أو التقاطها، أو نسخها، أو نشرها، أو إعادة نشرها، أو ألحق ضرراً بالمستخدمين أو المستفيدين، أو تغيير الموقع الإلكتروني، أو إلغاؤه، أو تعديل محتوياته، أو شغل عنوانه أو تصميماته أو طريقة استخدامه، أو انتحال شخصية مالكه أو القائم على إدارته، يعاقب بالأشغال الشاقة المؤقتة مدة لا تزيد على خمس سنوات، وبغرامة لا تقل عن ألف دينار أردني، ولا تزيد عن خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.
4. إذا ارتكب الفعل المحدد في الفقرة (3) من هذه المادة على البيانات الحكومية، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن خمس سنوات وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (5)

كل من أعاق أو عطل الوصول إلى الخدمة، أو الدخول إلى الأجهزة، أو البرامج أو مصادر البيانات، أو المعلومات، بأية وسيلة كانت عن طريق الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني ولا تزيد على ألف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً، أو بالعقوبتين كلتيهما.

مادة (6)

كل من أنتج أو أدخل عن طريق الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، ما من شأنه إيقافها عن العمل، أو تعطيلها، أو تدمير البرامج، أو حذفها، أو اتلافها، أو تعديلها، يعاقب بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن خمسة آلاف دينار أردني، ولا تزيد على عشرة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (7)

كل من التقط ما هو مرسل عن طريق الشبكة، أو إحدى وسائل تكنولوجيا المعلومات، أو سجله، أو اعترضه، أو تنصت عمداً دون وجه حق، يعاقب بالحبس، أو بالغرامة التي لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني أو بالعقوبتين كلتيهما.

مادة (8)

1. كل من قام عمداً بفك بيانات مشفرة في غير الأحوال المصرح بها قانوناً، يعاقب بالحبس أو بالغرامة التي لا تقل عن ألف دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.
2. كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية، أو أداة إنشاء التوقيع الإلكتروني المتعلقة بتوقيع شخص غيره، يعاقب بالحبس أو بالغرامة التي لا تقل عن ألفي دينار أردني ولا تزيد عن خمسة آلاف دينار أردني أو بالعقوبتين كلتيهما.
3. كل من ارتكب جريمة باستخدام أي من المذكور في الفقرة (2) من هذه المادة، يعاقب بالأشغال الشاقة المؤقتة وبالغرامة التي لا تقل عن ألفي دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (9)

1. كل من ينتفع دون وجه حق بخدمات الاتصال عن طريق إحدى وسائل تكنولوجيا المعلومات أو ما في حكمها، يعاقب بالحبس مدة لا تقل عن ستة شهور، أو بالغرامة التي لا تقل عن خمسمائة دينار أردني ولا تزيد عن ثلاثة آلاف دينار أردني، أو بالعقوبتين كلتيهما.
2. إذا كان الانتفاع المحدد في الفقرة (1) من هذه المادة بقصد الربح، يعاقب بالحبس مدة لا تقل عن سنة، أو بالغرامة التي لا تقل عن ألف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

مادة (10)

كل من قام عمداً بإنشاء أو نشر شهادة غير صحيحة، أو قدم بيانات غير صحيحة عن هويته إلى الجهات المختصة بموجب القوانين الخاصة بإصدار الشهادات بغرض طلب استصدار شهادة، أو إلغائها أو إيقافها، يعاقب بالحبس وبالغرامة التي لا تقل عن مائتي دينار أردني ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (11)

1. كل من زور مستنداً إلكترونياً رسمياً من مستندات الدولة، أو الهيئات والمؤسسات العامة، معترفاً به قانوناً في نظام معلوماتي، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن خمس سنوات وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد عن عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

2. إذا وقع التزوير فيما عدا ذلك من المستندات، وكان من شأن ذلك إحداث ضرر يعاقب بالحبس أو بالغرامة التي لا تقل عن خمسمائة دينار أردني ولا تزيد عن ثلاثة آلاف دينار أردني، أو بالعقوبتين كلتيهما.
3. كل من استعمل المستند المزور مع علمه بتزويره يعاقب بالعقوبة المقررة لجريمة التزوير حسب الأصول.
4. كل من زور أو تلاعب بتوقيع أو أداة أو أنظمة توقيع إلكترونية رسمية، سواء تم ذلك باصطناعه، أو إتلافه، أو تعييبه، أو تعديله، أو تحويره، أو بأية طريقة أخرى تؤدي إلى تغيير الحقيقة في بياناته، أو معلوماته، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن خمس سنوات وبالغرامة التي لا تقل عن خمسة آلاف دينار أردني، ولا تزيد عن عشرة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً.
5. إذا وقع التزوير أو التلاعب فيما عدا ذلك من التواقيع الإلكترونية في الفقرة (4) من هذه المادة، يعاقب بالحبس أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد عن ثلاثة آلاف دينار أردني، أو بالعقوبتين كلتيهما.
6. كل من أنشأ بيانات توقيع أو أداة نظام توقيع إلكتروني رسمي، أو للهيئات أو للمؤسسات العامة، لا يحق له الحصول عليه، مستخدماً في ذلك معلومات أو بيانات كاذبة أو خاطئة، أو تواطأ مع غيره في إنشاء ذلك، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن خمس سنوات وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد عن عشرة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً.
7. إذا وقع الإنشاء فيما عدا ذلك من التواقيع الإلكترونية في الفقرة (6) يعاقب بالحبس أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

مادة (12)

1. كل من استخدم الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات في الوصول دون وجه حق إلى أرقام، أو بيانات وسيلة التعامل الإلكترونية أو التلاعب فيها، يعاقب بالحبس مدة لا تقل عن ستة شهور، أو بغرامة لا تقل عن خمسمائة دينار أردني ولا تزيد على ثلاثة آلاف دينار أردني، أو بالعقوبتين كلتيهما.
2. كل من زور وسيلة تعامل إلكترونية بأية وسيلة كانت، أو صنع أو حاز بدون ترخيص أجهزة أو مواد تستخدم في إصدار أو تزوير بطاقة التعامل الإلكتروني، يعاقب بالعقوبة ذاتها المنصوص عليها في الفقرة (1) من هذه المادة.
3. كل من استخدم أو سهل استخدام وسيلة تعامل إلكترونية مزورة مع علمه بذلك، أو قبل وسيلة تعامل إلكترونية غير سارية، أو مزورة، أو مسروقة مع علمه بذلك، يعاقب بالعقوبة ذاتها المنصوص عليها في الفقرة (1) من هذه المادة.
4. إذا قصد من ذلك استخدامها في الحصول على أموال أو بيانات غيره أو ما تتيحه من خدمات، يعاقب بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد عن خمسة آلاف دينار أردني أو بالعقوبتين كلتيهما.

5. إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على مال غيره، يعاقب بالحبس مدة لا تقل عن سنتين، أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد عن خمسة آلاف دينار أردني أو بالعقوبتين كلتيهما.

مادة (13)

كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في سرقة أموال، أو اختلاسها يعاقب بالأشغال الشاقة المؤقتة، أو بغرامة لا تقل عن ألفي دينار أردني ولا تزيد عن خمسة آلاف دينار أردني أو بالعقوبتين كلتيهما.

مادة (14)

كل من توصل عن طريق الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات إلى الاستيلاء لنفسه، أو لغيره على مال منقول، أو على سند، أو توقيع إلكتروني، أو بيانات إنشاء توقيع إلكتروني، أو منظومة إنشاء توقيع إلكتروني، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب، أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه، يعاقب بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن ألفي دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

مادة (15)

1. كل من استعمل الشبكة الإلكترونية أو احدى وسائل تكنولوجيا المعلومات في تهديد شخص آخر أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان هذا الفعل أو الامتناع مشروعا، يعاقب بالحبس أو بغرامة لا تقل عن ألفي دينار أردني ولا تزيد عن خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.
2. إذا كان التهديد بارتكاب جناية أو بإسناد أمور خادشة للشرف أو الاعتبار، يعاقب بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن ألفي دينار أردني ولا تزيد عن خمسة آلاف دينار أردني، أو ما يعادلهما بالعملة المتداولة قانونا.

مادة (16)

1. كل من أنتج ما من شأنه المساس بالآداب العامة، أو أعده أو هيأه أو أرسله أو خزنه بقصد الاستغلال، أو التوزيع أو العرض على غيره عن طريق الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، أو الرسوم المتحركة، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد عن خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.
2. كل من أنشأ موقعا أو تطبيقا أو حسابا إلكترونيا، أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات؛ تدعو إلى تسهيل برامج وأفكار تروج لما من شأنه المساس بالآداب العامة، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة مالية لا تقل عن ألف دينار أردني ولا تزيد عن خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

3. إذا كان الفعل المحدد في الفقرتين (1،2) من هذه المادة موجها إلى طفل، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن سبع سنوات وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونا.
4. إذا كان محتوى الفعل الوارد في الفقرة (1) من هذه المادة طفل أو هيئة طفل أو صور محاكاة للطفل، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن سبع سنوات وبغرامة لا تقل عن خمسة آلاف دينار أردني، ولا تزيد على عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونا.

مادة (17)

كل من أنشأ موقعا أو تطبيقا أو حسابا إلكترونيا أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات بقصد الاتجار في البشر والأعضاء البشرية أو تسهيل التعامل فيه، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن عشر سنوات، وبغرامة لا تقل عشرة آلاف دينار أردني ولا تزيد على عشرين ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونا.

مادة (18)

دون الإخلال بالأحكام الواردة في قرار بقانون مكافحة غسل الأموال وتمويل الإرهاب، كل من أنشأ موقعا، أو تطبيقا أو حسابا إلكترونيا، أو نشر معلومات على الشبكة الالكترونية، أو إحدى وسائل تكنولوجيا المعلومات، بقصد ارتكاب جريمة غسل الأموال وتمويل الإرهاب، يعاقب بالأشغال الشاقة المؤقتة مده لا تقل عن عشر سنوات وبغرامة لا تقل عن عشرة ألف دينار أردني، ولا تزيد على عشرين ألف دينار أردني أو ما يعادلها بالعملة المتداولة قانونا.

مادة (19)

كل من أنشأ أو نشر موقعا على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، بقصد الاتجار أو الترويج للمخدرات أو المؤثرات العقلية، أو ما في حكمها، أو سهل التعامل فيها، أو لبيعها، أو شرح، أو عرض طرق إنتاج المواد المخدرة، يعاقب بالحبس مدة لا تقل عن عشر سنوات وبغرامة لا تقل عن عشرة آلاف دينار أردني ولا تزيد على عشرين ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونا.

مادة (20)

1. كل من أنشأ موقعا إلكترونيا، أو أداره عن طريق الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات؛ بقصد نشر أخبار من شأنها تعريض سلامة الدولة، أو نظامها العام، أو أمنها الداخلي أو الخارجي للخطر، يعاقب بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.
2. كل من روّج بأية وسيلة تلك الأخبار بالقصد ذاته أو بثها أو نشرها، يعاقب بالحبس مدة لا تزيد على سنة، أو بغرامة لا تقل عن مائتي دينار أردني ولا تزيد عن ألف دينار أردني، أو بالعقوبتين كلتيهما.

3. إذا كان الفعل الوارد في الفقرتين (1،2) من هذه المادة في حالة الطوارئ تضاعف العقوبة المقررة له.

مادة (21)

كل من أنشأ موقعا، أو تطبيقا، أو حسابا إلكترونيا، أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، بقصد الإساءة أو سب إحدى المقدسات أو الشعائر المقررة للأديان، أو أحد المعتقدات الدينية، يعاقب بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن ألفي دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

مادة (22)

كل من أنشأ موقعا، أو تطبيقا، أو حسابا إلكترونيا، أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات؛ بقصد الاعتداء على أي من المبادئ أو القيم الأسرية، من خلال نشر أخبار، أو صور، أو تسجيلات صوتية أو مرئية، سواء أكانت مباشرة أو مسجلة تتصل بحرمة الحياة الخاصة، أو العائلية للأفراد ولو كانت صحيحة، أو تعدى بالذم، أو القدح، أو التحقير أو التشهير بالآخرين وإلحاق الضرر بهم، يعاقب بالحبس مدة لا تقل عن سنتين، أو بغرامة لا تقل عن ثلاثة آلاف دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

مادة (23)

كل من أنشأ موقعا، أو تطبيقا، أو حسابا إلكترونيا، أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، بقصد إدارة مشروع مقامرة، أو تسهيله، أو تشجيعه، أو الترويج له، أو عرض ألعاب مقامرة، يعاقب بالحبس مدة لا تقل عن ستة شهور، أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

مادة (24)

كل من أنشأ موقعا، أو تطبيقا، أو حسابا إلكترونيا، أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، بقصد نشر وتوزيع معلومات تثير النعرات العنصرية، وتهدف إلى التمييز العنصري بحق فئة معينة، أو أقدم على تهديد شخص، أو تحقيره، أو التعدي عليه بسبب انتمائه العرقي أو المذهبي، أو اللون، أو الشكل، أو سبب الإعاقة، يعاقب بالأشغال الشاقة المؤقتة، وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشر آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونا.

مادة (25)

كل من أنشأ موقعا، أو تطبيقا، أو حسابا إلكترونيا، أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، من شأنه التشويه والتبرير لأعمال إبادة جماعية، أو جرائم ضد الإنسانية

نصت عليها المواثيق والقوانين الدولية، أو المساعدة قصدا، أو التحريض على ارتكاب جرائم ضد الإنسانية، يعاقب بالأشغال الشاقة المؤبدة، أو الأشغال الشاقة المؤقتة مدة لا تقل عن عشر سنوات.

مادة (26)

كل من حاز جهازا بغرض الاستخدام، أو برنامجا، أو أية بيانات إلكترونية معدة، أو كلمة سر، أو تراميز دخول، أو قدمها، أو أنتجها، أو وزعها، أو استوردها، أو صدرها، أو روّج لها، وذلك بغرض اقتراف أي من الجرائم المنصوص عليها في هذا القرار بقانون، يعاقب بالأشغال الشاقة المؤقتة مدة لا تزيد على خمس سنوات، وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونا.

مادة (27)

1. كل موظف ارتكب أيا من الجرائم المنصوص عليها في هذا القرار بقانون مستغلا صلاحياته وسلطاته في أثناء تأدية عمله، أو بسببها أو سهل ذلك لغيره، يعاقب بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو بالعقوبتين كلتيهما.
2. كل من ارتكب من موظفي مزودي الخدمة، أيا من الجرائم المنصوص عليها في هذا القرار بقانون في أثناء تأدية عمله، أو بسببها، أو سهل ذلك لغيره، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن ثلاث سنوات، أو بغرامة لا تقل عن عشرة آلاف دينار أردني ولا تزيد على عشرين ألف دينار أردني، أو بالعقوبتين كلتيهما.

مادة (28)

كل من أنشأ موقعا، أو تطبيقا، أو حسابا إلكترونيا، أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات؛ بقصد ارتكاب أية جريمة معاقب عليها بموجب أي تشريع نافذ، أو اشترك أو حرض على ارتكابها، يعاقب بضعف العقوبة المنصوص عليها في ذلك التشريع.

مادة (29)

1. كل من حرض، أو ساعد، أو اتفق مع غيره على ارتكاب جريمة من الجرائم المنصوص عليها بموجب أحكام هذا القرار بقانون بأية وسيلة إلكترونية، ووقعت الجريمة بناءً على هذا التحريض أو المساعدة، أو الاتفاق، يعاقب بثلثي الحد الأقصى للعقوبة المقررة لفاعلها.
2. إذا كان المجني عليه طفلا في الفقرة (1) من هذه المادة، يعاقب المجرم بالأشغال الشاقة المؤقتة مدة لا تقل عن خمس سنوات، وبغرامة لا تقل عن ألفي دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونا، ولو لم تقع الجريمة فعلا.

مادة (30)

إذا ارتكب، باسم الشخص المعنوي أو لحسابه، إحدى الجرائم المنصوص عليها في هذا القرار بقانون، يعاقب بالغرامة التي لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، وللمحكمة أن تقضي بحرمان الشخص المعنوي من مباشرة نشاطه لمدة أقصاها خمس سنوات، أو أن تقضي بحله وذلك مع عدم الإخلال بالمسؤولية الجنائية للشخص الطبيعي التابع له.

مادة (31)

يعاقب بالحبس مدة لا تقل عن ثلاثة شهور، وبغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألف دينار أردني كل من قام باستخدام أنظمة، أو موقع أو تطبيق إلكتروني؛ لتجاوز الحجب المفروض بموجب أحكام هذا القرار بقانون.

مادة (32)

يلتزم مزود الخدمة، وفقاً للإجراءات القانونية المقررة بالآتي:

1. تزويد الجهات المختصة بجميع البيانات والمعلومات اللازمة التي تساعد في كشف الحقيقة، بناءً على طلب النيابة أو المحكمة المختصة.
2. حجب رابط أو محتوى أو تطبيق على الشبكة الإلكترونية بناءً على الأوامر الصادرة إليها من الجهات القضائية مع مراعاة الإجراءات الواردة في المادة (40) من هذا القرار بقانون.
3. الاحتفاظ بالمعلومات عن المشترك لمدة لا تقل عن ثلاث سنوات.
4. التعاون ومساعدة الجهات المختصة، وبناءً على قرار قاضي المحكمة المختصة في جمع أو تسجيل المعلومات أو البيانات الإلكترونية والاحتفاظ المؤقت بها.

مادة (33)

1. للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة.
2. يجب أن يكون أمر التفتيش مسبباً ومحدداً، ويجوز تجديده أكثر من مرة، ما دامت مبررات هذا الإجراء قائمة.
3. إذا أسفر التفتيش المحدد في الفقرة (2) من هذه المادة عن ضبط أجهزة، أو أدوات، أو وسائل ذات صلة بالجريمة؛ يتعين على مأموري الضبط القضائي تنظيم محضر بالمضبوطات وعرضها على النيابة العامة لاتخاذ ما يلزم بشأنها.
4. لوكيل النيابة العامة أن يأذن بالنفاذ المباشر لمأموري الضبط القضائي، أو من يستعينون بهم من أهل الخبرة إلى أية وسيلة من وسائل تكنولوجيا المعلومات، وإجراء التفتيش فيها بقصد الحصول على البيانات أو المعلومات.
5. يشترط في مأمور الضبط القضائي أن يكون مؤهلاً للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية.

مادة (34)

1. للنيابة العامة الحصول على الأجهزة، أو الأدوات، أو الوسائل، أو البيانات، أو المعلومات الإلكترونية، أو بيانات المرور، أو البيانات المتعلقة بحركة الاتصالات، أو بمستعمليها أو معلومات المحتوى ذات الصلة بالجريمة الإلكترونية.
2. للنيابة العامة الإذن بالضبط والتحفظ على كامل نظام المعلومات، أو جزء منه، أو أية وسيلة من وسائل تكنولوجيا المعلومات التي من شأنها أن تساعد على كشف الحقيقة.
3. إذا لم يكن الضبط والتحفظ على نظام المعلومات ضروريا، أو تعذر إجراؤه؛ تنسخ البيانات أو المعلومات التي لها علاقة بالجريمة والبيانات التي تؤمن قراءتها وفهمها على وسيلة من وسائل تكنولوجيا المعلومات.
4. إذا استحال إجراء الضبط والتحفظ عليه بصفة فعلية؛ وحفاظا على أدلة الجريمة يتعين استعمال كافة الوسائل المناسبة؛ لمنع الوصول والنفاذ إلى البيانات المخزنة بنظام المعلومات.
5. تتخذ الاحتياطات الضرورية للحفاظ على سلامة المضبوط المتحفظ عليه بما في ذلك الوسائل الفنية لحماية محتواها.
6. تحرر قدر الإمكان قائمة بالمضبوط المتحفظ عليه بحضور المتهم، أو من وجد لديه المضبوط المتحفظ عليه، ويحرر تقرير بذلك، ويُحفظ المضبوط المتحفظ عليه حسب الحالة في ظرف، أو مغلف مختوم، وتكتب عليه ورقة مع بيان تاريخ التحفظ وساعته وعدد المحاضر والقضية.

مادة (35)

1. لقاضي الصلح أن يأذن للنيابة العامة بمراقبة الاتصالات والمحادثات الإلكترونية وتسجيلها والتعامل معها؛ للبحث عن الدليل المتعلق بالجريمة وذلك لمدة خمسة عشر يوما قابلة للتجديد لمرة واحدة، بناءً على توافر دلائل جديدة، وعلى من قام بالتفتيش أو المراقبة أو التسجيل أن ينظم محضرا بذلك يقدمه إلى النيابة العامة.
2. للنيابة العامة أن تأمر بالجمع والتزويد الفوري لأي بيانات بما فيها حركة الاتصالات، أو معلومات إلكترونية، أو بيانات مرور، أو معلومات المحتوى التي تراها لازمة لمصلحة التحقيقات، بأستعمال الوسائل الفنية المناسبة والاستعانة في ذلك عند الاقتضاء بمزودي الخدمة حسب نوع الخدمة التي يقدمها.

مادة (36)

على الجهات المختصة اتخاذ التدابير والإجراءات الكفيلة بالحفاظ على سلامة الأجهزة، أو الأدوات، أو وسائل تكنولوجيا المعلومات، أو الأنظمة الإلكترونية، أو البيانات، أو المعلومات الإلكترونية وخصوصيتها محل التحفظ، إلى حين صدور قرار من الجهات القضائية ذات العلاقة بشأنها.

مادة (37)

1. للمحكمة المختصة أن تأذن بالاعتراض الفوري لمحتوى اتصالات، وتسجيلها أو نسخها بناءً على

طلب من قبل النائب العام أو أحد مساعديه، ويتضمن قرار المحكمة جميع العناصر التي من شأنها التعريف بالاتصالات موضوع طلب الاعتراض والأفعال الموجبة له ومدته.

2. تكون مدة الاعتراض المحدد في الفقرة (1) من هذه المادة ثلاثة شهور من بداية تاريخ الشروع الفعلي في إنجازه، قابلة للتمديد مرة واحدة فقط.

3. يتعين على الجهة المكلفة بتنفيذ إذن الاعتراض إعلام النيابة العامة بالتاريخ الفعلي لانطلاق عملية الاعتراض، والتنسيق معها بخصوص اتخاذ التدابير اللازمة لحسن سيرها.

مادة (38)

لا يجوز استبعاد أي دليل ناتج عن وسيلة من وسائل تكنولوجيا المعلومات، أو أنظمة المعلومات، أو شبكات المعلومات، أو المواقع الإلكترونية، أو البيانات والمعلومات الإلكترونية، بسبب طبيعة ذلك الدليل.

مادة (39)

لا يجوز استبعاد أي من الأدلة المتحصل عليها بمعرفة الجهة المختصة أو جهات التحقيق من دول أخرى لمجرد ذلك السبب، طالما أن الحصول عليها قد تم وفقاً للإجراءات القانونية والقضائية للتعاون الدولي.

مادة (40)

1. لجهات التحري والضبط المختصة - إذا ما رصدت قيام مواقع إلكترونية مستضافة داخل الدولة أو خارجها، بوضع أية عبارات، أو أرقام، أو صور، أو أفلام، أو أية مواد دعائية، أو غيرها، من شأنها تهديد الأمن القومي، أو السلم الأهلي، أو النظام العام، أو الآداب العامة - أن تعرض محضراً بذلك على النائب العام أو أحد مساعديه، وتطلب الإذن بحجب الموقع أو المواقع الإلكترونية، أو حجب بعض روابطها من العرض.

2. يقدم النائب العام أو أحد مساعديه طلب الإذن لمحكمة الصلح خلال 24 ساعة مشفوعاً بمذكرة برأيه، وتصدر المحكمة قرارها في الطلب، في ذات يوم عرضه عليها إما بالقبول أو بالرفض.

مادة (41)

فيما عدا الالتزامات المهنية المنصوص عليها في القانون لا يجوز الاستناد إلى أسرار المهنة أو مقتضياتها؛ للامتناع عن تقديم المعلومات أو الوثائق التي تطلب وفقاً لأحكام القانون.

مادة (42)

تلتزم أجهزة الدولة ومؤسساتها وهيئاتها والجهات والشركات التابعة لها بما يلي:

1. اتخاذ التدابير الأمنية الوقائية اللازمة لحماية أنظمتها المعلوماتية، ومواقعها الإلكترونية وشبكاتها المعلوماتية، والبيانات والمعلومات الإلكترونية الخاصة بها.

2. الإسراع في إبلاغ الجهة المختصة عن أية جريمة منصوص عليها في هذا القرار بقانون فور اكتشافها أو اكتشاف أية محاولة للالتقاط، أو الاعتراض، أو التنصت بشكل غير مشروع وتزويد الجهة المختصة بجميع المعلومات لكشف الحقيقة.
3. الاحتفاظ ببيانات تكنولوجيا المعلومات ومعلومات المشترك لمدة لا تقل عن 120 يوماً وتزويد الجهة المختصة بتلك البيانات.
4. التعاون مع الجهات المختصة لتنفيذ اختصاصاتها.

مادة (43)

1. تعمل الجهات المختصة على تيسير التعاون مع نظيراتها في البلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصادق عليها، أو طبق مبدأ المعاملة بالمثل، بقصد الإسراع في تبادل المعلومات بما من شأنه أن يكفل الإنذار المبكر بجرائم أنظمة المعلومات والاتصال وتفادي ارتكابها والمساعدة على التحقيق فيها وتتبع مرتكبيها.
2. يتوقف التعاون المشار إليه بالفقرة (1) من هذه المادة على التزام الدولة الأجنبية المعنية بالحفاظ على سرية المعلومات المحالة إليها، والتزامها بعدم إحالتها إلى طرف آخر أو استغلالها لأغراض أخرى غير مكافحة الجرائم المعنية بهذا القرار بقانون.

مادة (44)

1. يتعين على الجهات المختصة أن تقدم العون للجهات النظيرة في الدول الأخرى، لأغراض تقديم المساعدة القانونية المتبادلة، وتسليم المجرمين في التحقيقات والإجراءات الجنائية المرتبطة بالجرائم المنصوص عليها في هذا القرار بقانون، وفقاً للقواعد التي يقررها قانون الإجراءات الجزائية والاتفاقيات الثنائية، أو متعددة الأطراف التي تكون الدولة طرفاً فيها، أو بمبدأ المعاملة بالمثل، وذلك بما لا يتعارض مع أحكام هذا القرار بقانون أو أي قانون آخر.
2. لا ينفذ طلب المساعدة القانونية، أو طلب تسليم المجرمين، استناداً إلى أحكام هذا القرار بقانون، إلا إذا كانت قوانين الدولة الطالبة وقوانين الدولة تعاقب على الجريمة موضوع الطلب أو على جريمة مماثلة، وتعتبر ازدواجية التجريم مستوفاة، بغض النظر عما إذا كانت قوانين الدولة الطالبة تدرج الجريمة في فئة الجرائم ذاتها، أو تستخدم في تسمية الجريمة المصطلح ذاته المستخدم في الدولة، بشرط أن يكون الفعل موضوع الطلب مجرّماً بمقتضى قوانين الدولة الطالبة.

مادة (45)

مع عدم الإخلال بأية عقوبة أشد ينص عليها قانون العقوبات النافذ، أو أي قانون آخر يعاقب مرتكبو الجرائم المعاقب عليها بموجب أحكام هذا القرار بقانون بالعقوبات المنصوص عليها فيه.

مادة (46)

كل من ارتكب فعلاً يشكل جريمة بموجب أي تشريع نافذ باستخدام الشبكة الإلكترونية أو بإحدى وسائل تكنولوجيا المعلومات، أو اشترك فيها، أو تدخل، أو حرض على ارتكابها، يعاقب بالعقوبة ذاتها المقررة لتلك الجريمة في ذلك التشريع.

مادة (47)

كل من أنشأ موقعاً على الشبكة الإلكترونية، يهدف إلى الترويج لارتكاب أية جريمة من الجرائم المنصوص عليها في قانون العقوبات، أو أي من القوانين الخاصة، يعاقب بالسجن المؤقت وبغرامة لا تقل عن خمسة آلاف دينار ولا تزيد على عشرة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (48)

كل من أفشى سرية الإجراءات المنصوص عليها في هذا القرار بقانون في غير الأحوال المصرح بها قانوناً، يعاقب بالحبس وبغرامة لا تقل عن خمسمائة دينار ولا تزيد على ثلاثة آلاف دينار أردني أو بإحدى هاتين العقوبتين.

مادة (49)

كل من أقدم على العبث بأدلة قضائية معلوماتية، أو أقدم على إتلافها، أو إخفائها، أو التعديل فيها أو محوها، يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن ألف دينار ولا تزيد على خمسة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (50)

كل من امتنع عن قصد في الإبلاغ، أو أبلغ عن قصد بشكل خاطئ عن جرائم معلوماتية، يعاقب بالحبس مدة لا تقل عن ستة شهور، وبغرامة لا تقل عن مائتي دينار ولا تزيد على ألف دينار أردني أو بإحدى هاتين العقوبتين.

مادة (51)

إذا وقعت أية جريمة من الجرائم المنصوص عليها في هذا القرار بقانون بغرض الإخلال بالنظام العام، أو تعريض سلامة المجتمع وأمنه للخطر، أو تعريض حياة المواطنين للخطر، أو منع أو عرقلة ممارسة السلطات العامة لأعمالها، أو تعطيل أحكام الدستور أو القانون الأساسي أو القوانين أو اللوائح، أو بقصد الإضرار بالوحدة الوطنية، والسلام الاجتماعي، أو ازدراء الأديان أو الاعتداء على الحقوق والحريات التي يكفلها الدستور أو القانون الأساسي، تكون العقوبة الأشغال الشاقة المؤبدة أو المؤقتة.

مادة (52)

يعاقب من يشترك بطريق الاتفاق أو التحريض، أو المساعدة، أو التدخل في ارتكاب جناية، أو جنحة

معاقب عليها بموجب أحكام هذا القرار بقانون بالعقوبات ذاتها المقررة للفاعل الأصلي، وإن لم تقع الجريمة يعاقب عليها بنصف العقوبة المقررة لها.

مادة (53)

يعد مرتكباً لجريمة الشروع كل من شرع في ارتكاب جناية أو جنحة من الجرائم المنصوص عليها، في هذا القرار بقانون ويعاقب بنصف العقوبة المقررة لها.

مادة (54)

1. دون الإخلال بالعقوبات المنصوص عليها في هذا القرار بقانون، وحقوق الغير حَسَن النية، تصدر المحكمة قراراً بمصادرة الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القرار بقانون، أو الأموال المتحصلة منها، على أن تكون إزالة المخالفة على نفقة الفاعل.
2. تصدر المحكمة قراراً بمدة إغلاق المحل وحجب الموقع الإلكتروني الذي ارتكبت فيه أو بواسطته تلك الجرائم بحسب الأحوال.

مادة (55)

تضاعف العقوبة المنصوص عليها في هذا القرار بقانون في حال تكرار الجاني أياً من الجرائم المنصوص عليها فيه سواء ارتكبت في فلسطين أم خارجها، وتعتبر الأحكام الأجنبية سابقة التكرار بحق الجاني.

مادة (56)

تضاعف العقوبة المقررة للجرائم المعاقب عليها بموجب أحكام هذا القرار بقانون في أي من الحالات الآتية:

1. إذا ارتكبها أو سهل ارتكابها موظف في مؤسسة خاصة، أو موظف عام مستغلاً صلاحياته وسلطاته في ذلك، أو من في حكمه، كما يحكم على الموظف العام بالفصل من الوظيفة في حال الإدانة.
2. إذا وقعت الجريمة على موقع، أو نظام معلوماتي، أو بيانات، أو أرقام، أو حروف، أو شفرات، أو صور يدار بمعرفة الدولة أو أحد الأشخاص المعنوية العامة أو مملوك لها أو يخصها بما في ذلك الهيئات المحلية.
3. ارتكاب الجاني الجريمة من خلال عصابة منظمة.
4. التغرير بالأحداث ومن في حكمهم واستغلالهم.
5. إذا وقعت الجريمة على نظام معلومات، أو موقع إلكتروني، أو شبكة معلوماتية تتعلق بتحويل الأموال، أو بتقديم خدمات الدفع أو التقاص، أو التسويات أو بأي من الخدمات المصرفية المقدمة من البنوك والشركات المالية.

مادة (57)

يعفى من العقوبات المنصوص عليها في هذا القرار بقانون، كل من بادر من الجناة بإبلاغ السلطات المختصة بأية معلومات عن الجريمة وعن الأشخاص المشتركين فيها، وذلك قبل علم السلطات بها وقبل وقوع الضرر، ويجوز للمحكمة أن تقتضي بوقف تنفيذ العقوبة إذا حصل الإبلاغ بعد علم السلطات المختصة وأدى إلى ضبط باقي الجناة.

مادة (58)

تتولى الوزارة وفقاً لاختصاصها تقديم الدعم والمساعدة الفنية لجهات إنفاذ القانون، ويعتبر موظفو الوزارة المعينون من قبل الوزير مأموري ضبط قضائي لغايات تنفيذ أحكام هذا القرار بقانون.

مادة (59)

يلغى كل ما يتعارض مع أحكام هذا القرار بقانون.

مادة (60)

يعرض هذا القرار بقانون على المجلس التشريعي في أول جلسة يعقدها لإقراره.

مادة (61)

على الجهات المختصة كافة، كل فيما يخصه، تنفيذ أحكام هذا القرار بقانون، ويعمل به من تاريخ نشره في الجريدة الرسمية.

صدر في مدينة رام الله بتاريخ: 2017/06/24ميلادية
الموافق: 29/رمضان/2017هجرية

محمود عباس
رئيس دولة فلسطين
رئيس اللجنة التنفيذية لمنظمة التحرير الفلسطينية

ملحق رقم (10): قانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات

قانون رقم 175 لسنة 2018
فى شأن مكافحة جرائم تقنية المعلومات

باسم الشعب

رئيس الجمهورية

قرر مجلس النواب القانون الآتى نصه، وقد أصدرناه:

الباب الأول

الأحكام العامة

تعريفات
مادة (1)

فى تطبيق أحكام هذا القانون، يُقصد بالألفاظ والعبارات التالية المعنى المبين قرين كل منهما:

الجهاز: الجهاز القومى لتنظيم الاتصالات.

الوزير المختص: الوزير المعنى بشئون الاتصالات وتكنولوجيا المعلومات.

البيانات والمعلومات الإلكترونية: كل ما يمكن إنشاؤه أو تخزينه، أو معالجته،أو تخليقه، أو نقله، أو مشاركته، أو نسخه بواسطة تقنية المعلومات؛ كالأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور والأصوات، وما فى حكمها.

بيانات شخصية: أى بيانات متعلقة بشخص طبيعى محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى.

بيانات حكومية: بيانات متعلقة بالدولة أو أحد سلطاتها، وأجهزتها أو وحداتها، أو الهيئات العامة، أو الهيئات المستقلة والأجهزة الرقابية، وغيرها من الأشخاص الاعتبارية العامة وما فى حكمها، والمتاحة على الشبكة المعلوماتية أو على أى نظام معلوماتى أو على حاسب أو ما فى حكمها.

المعالجة الإلكترونية: أى عملية إلكترونية أو تقنية تتم كليًا أو جزئيًا لكتابة أو تجميع، أو تسجيل، أو حفظ، أو تخزين، أو دمج، أو عرض، أو إرسال، أو استقبال، أو تداول، أو نشر، أو محو، أو تغيير، أو تعديل، أو استرجاع، أو استنباط للبيانات والمعلومات الإلكترونية، وذلك باستخدام أى وسيط من الوسائط أو الحاسبات أو الأجهزة الأخرى الإلكترونية أو المغناطيسية أو الضوئية أو ما يُستحدث من تقنيات أو وسائط أخرى.

تقنية المعلومات: أى وسيلة أو مجموعة وسائل مترابطة أو غير مترابطة تُستخدم لتخزين، واسترجاع، وترتيب، وتنظيم، ومعالجة، وتطوير، وتبادل المعلومات أو البيانات، ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة سلكيًا أو لاسلكيًا.

مقدم الخدمة: أى شخص طبيعى أو اعتبارى يزود المستخدمين بخدمات تقنيات المعلومات والاتصالات، ويشمل ذلك من يقوم بمعالجة أو تخزين المعلومات بذاته أومن ينوب عنه فى أى من تلك الخدمات أو تقنية المعلومات.

المستخدم: كل شخص طبيعى أو اعتبارى، يستعمل خدمات تقنية المعلومات أو يستفيد منها بأى صورة كانت.

البرنامج المعلوماتى: مجموعة الأوامر والتعليمات المعبر عنها بأية لغة أو رمز أو إشارة، والتى تتخذ أى شكل من الأشكال، ويمكن استخدامها بطريق مباشر أو غير مباشر فى حاسب آلى لأداء وظيفة أو تحقيق نتيجة سواء كانت هذه الأوامر والتعليمات فى شكلها الأصلى أو فى أى شكل آخر تظهر فيه من خلال حاسب آلى، أو نظام معلوماتى.

النظام المعلوماتى: مجموعة برامج وأدوات معدة لغرض إدارة ومعالجة البيانات والمعلومات، أو تقديم خدمة معلوماتية.

شبكة معلوماتية: مجموعة من الأجهزة أو نظم المعلومات مرتبطة معًا، ويمكنها تبادل المعلومات والاتصالات فيما بينها، ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية، والتطبيقات المستخدمة عليها.

الموقع: مجال أو مكان افتراضى له عنوان محدد على شبكة معلوماتية، يهدف إلى إتاحة البيانات والمعلومات للعامة أو الخاصة.

مدير الموقع: كل شخص مسئول عن تنظيم أو إدارة أو متابعة أو الحفاظ على موقع أو أكثر على الشبكة المعلوماتية، بما فى ذلك حقوق الوصول لمختلف المستخدمين على ذلك الموقع أو تصميمه، أو توليد وتنظيم صفحاته أو محتواه أو المسئول عنه.

الحساب الخاص: مجموعة من المعلومات الخاصة بشخص طبيعى أو اعتبارى، تخول له الحق دون غيره الدخول على الخدمات المتاحة أو استخدامها من خلال موقع أو نظام معلوماتى.

البريد الإلكترونى: وسيلة لتبادل رسائل إلكترونية على عنوان محدد، بين أكثر من شخص طبيعى أو اعتبارى، عبر شبكة معلوماتية، أو غيرها من وسائل الربط الإلكترونية، من خلال أجهزة الحاسب الآلى وما فى حكمها.

الاعتراض: مشاهدة البيانات أو المعلومات أو الحصول عليها، بغرض التنصت أو التعطيل، أو التخزين أو النسخ، أو التسجيل، أو تغيير المحتوى، أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه وذلك لأسباب غير مشروعة ودون وجه حق.

الاختراق: الدخول غير المرخص به، أو المخالف لأحكام الترخيص، أو الدخول بأى طريقة غير مشروعة، إلى نظام معلوماتى أو حاسب آلى أو شبكة معلوماتية، وما فى حكمها.

المحتوى: أى بيانات تؤدى بذاتها، أو مجتمعة مع بيانات أو معلومات أخرى إلى تكوين معلومة أو تحديد توجه أو اتجاه أو تصور أو معنى أو الإشارة إلى بيانات أخرى.

الدليل الرقمى: أى معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما فى حكمها، ويمكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة.

الخبرة: كل عمل يتصل بتقديم الاستشارات أو الفحص أو المراجعة أو التقييم أو التحليل فى مجالات تقنية المعلومات.

حركة الاتصال (بيانات المرور): بيانات ينتجها نظام معلوماتى تبين مصدر الاتصال، وجهته والوجهة المرسل منها والمرسل إليها والطريق الذى سلكه، وساعته وتاريخه وحجمه ومدته، ونوع الخدمة.

الحاسب: كل جهاز أو معدة تقنية تكون قادرة على التخزين، وأداء عمليات منطقية، أو حسابية، وتستخدم لتسجيل بيانات أو معلومات، أو تخزينها، أو تحويلها، أو تخليقها، أو استرجاعها، أو ترتيبها، أو معالجتها، أو تطويرها، أو تبادلها، أو تحليلها، أو للاتصالات.

دعامة إلكترونية: أى وسيط مادى لحفظ وتداول البيانات والمعلومات الإلكترونية ومنها الأقراص المدمجة أو الأقراص الضوئية والذاكرة الإلكترونية أو ما فى حكمها.

الأمن القومى: كل ما يتصل باستقلال واستقرار وأمن الوطن ووحدته وسلامة أراضيه، وما يتعلق بشئون رئاسة الجمهورية ومجلس الدفاع الوطنى ومجلس الأمن القومى، ووزارة الدفاع والإنتاج الحربى، ووزارة الداخلية، والمخابرات العامة، وهيئة الرقابة الإدارية، والأجهزة التابعة لتلك الجهات.

جهات الأمن القومى: رئاسة الجمهورية، ووزارة الدفاع، ووزارة الداخلية، والمخابرات العامة، وهيئة الرقابة الإدارية.

التزامات وواجبات مقدم الخدمة

مادة (2)

أولاً - مع عدم الإخلال بالأحكام الواردة بهذا القانون وقانون تنظيم الاتصالات الصادر بالقانون رقم 10 لسنه 2003، يلتزم مقدمو الخدمة بما يأتى:

1 - حفظ وتخزين سجل النظام المعلوماتى أو أى وسيلة لتقنية المعلومات لمدة مائة وثمانون يومًا متصلة. وتتمثل البيانات الواجب حفظها وتخزينها فيما يأتى:

(أ) البيانات التى تمكن من التعرف على مستخدم الخدمة.

(ب) البيانات المتعلقة بمحتوى ومضمون النظام المعلوماتى المتعامل متى كانت تحت سيطرة مقدم الخدمة.

(جـ) البيانات المتعلقة بحركة الاتصال.

(د) البيانات المتعلقة بالأجهزة الطرفية للاتصال.

(هـ) أى بيانات أخرى يصدر بتحديدها قرار من مجلس إدارة الجهاز.

2 - المحافظة على سرية البيانات التى تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة، ويشمل ذلك البيانات الشخصية لأى من مستخدمى خدمته، أو أى بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التى يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التى يتواصلون معها.

3 - تأمين البيانات والمعلومات بما يحافظ على سريتها، وعدم اختراقها أو تلفها.
ثانيًا - مع عدم الإخلال بأحكام قانون حماية المستهلك، يجب على مقدم الخدمة أن يوفر لمستخدمى خدماته ولأى جهة حكومية مختصة، بالشكل والطريقة التى يمكن الوصول إليها بصورة ميسرة ومباشرة ومستمرة، البيانات والمعلومات الآتية:

1 - اسم مقدم الخدمة وعنوانه.

2 - معلومات الاتصال المتعلقة بمقدم الخدمة، بما فى ذلك عنوان الاتصال الإلكترونى.

3 - بيانات الترخيص لتحديد هوية مقدم الخدمة، وتحديد الجهة المختصة التى يخضع لإشرافها.

4 - أى معلومات أخرى يقدر الجهاز أهميتها لحماية مستخدمى الخدمة، ويصدر بتحديدها قرار من الوزير المختص.

ثالثًا: مع مراعاة حرمة الحياة الخاصة التى يكفلها الدستور، يلتزم مقدمو الخدمة والتابعون لهم، أن يوفروا حال طلب جهات الأمن القومى ووفقًا لاحتياجاتها كافة الإمكانيات الفنية التى تتيح لتلك الجهات ممارسة اختصاصاتها وفقا للقانون.

رابعًا: يلتزم مقدمو خدمات تقنية المعلومات ووكلائهم وموزعوهم التابعون لهم المنوط بهم تسويق تلك الخدمات بالحصول على بيانات المستخدمين، ويُحظر على غيرهم القيام بذلك.

نطاق تطبيق القانون من حيث المكان

مادة (3)

مع عدم الإخلال بأحكام الباب الأول من الكتاب الأول من قانون العقوبات، تسرى أحكام هذا القانون على كل من ارتكب خارج جمهورية مصر العربية من غير المصريين جريمة من الجرائم المنصوص عليها من هذا القانون، متى كان الفعل معاقبًا عليه فى الدولة التى وقع فيها تحت أى وصف قانونى، وذلك فى أى من الأحوال الآتية:

1 - إذا ارتكبت الجريمة على متن أى وسيلة من وسائل النقل الجوى أو البرى أو المائى، وكانت مسجلة لدى جمهورية مصر العربية أو تحمل علمها.

2 - إذا كان المجنى عليهم أو أحدهم مصريًا.

3 - إذا تم الإعداد للجريمة أو التخطيط أو التوجيه أو الإشراف عليها أو تمويلها فى جمهورية مصر العربية.

4 - إذا ارتكبت الجريمة بواسطة جماعة إجرامية منظمة، تمارس أنشطة إجرامية فى أكثر من دولة من بينها جمهورية مصر العربية.

5 - إذا كان من شأن الجريمة إلحاق ضرر بأى من موطنى جمهورية مصر العربية أو المقيمين فيها، أو بأمنها أو بأى من مصالحها، فى الداخل أو الخارج.

6 - إذا وُجد مرتكب جريمة فى جمهورية مصر العربية، بعد ارتكابها ولم يتم تسليمه.

التعاون الدولى فى مجال مكافحة جرائم تقنية المعلومات

مادة (4)

تعمل السلطات المصرية المختصة على تيسير التعاون مع نظيراتها بالبلاد الأجنبية فى إطار الاتفاقيات الدولية والإقليمية والثنائية المصدق عليها، أو تطبيق مبدأ المعاملة بالمثل، بتبادل المعلومات بما من شأنه أن يكفل تفادى ارتكاب جرائم تقنيه المعلومات، والمساعدة على التحقيق فيها، وتتبع مرتكبيها.

على أن يكون المركز الوطنى للاستعداد لطوارئ الحاسب والشبكات بالجهاز هو النقطة الفنية المعتمدة فى هذا الشأن.

الباب الثانى

الأحكام والقواعد الإجرائية

مأمورو الضبط القضائي

مادة (5)

يجوز بقرار من وزير العدل بالاتفاق مع الوزير المختص منح صفة الضبطية القضائية للعاملين بالجهاز أو غيرهم ممن تحددهم جهات الأمن القومى، بالنسبة إلى الجرائم التى تقع بالمخالفة لأحكام هذا القانون والمتعلقة بأعمال وظائفهم.

الأوامر القضائية المؤقتة

مادة (6)

لجهة التحقيق المختصة، بحسب الأحوال، أن تصدر أمرًا مسببًا، لمأمورى الضبط القضائى المختصين، لمدة لا تزيد على ثلاثين يومًا قابلة للتجديد لمرة واحدة، متى كان لذلك فائدة فى ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون بواحد أو أكثر مما يأتى:

1 - ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات، وتتبعها فى أى مكان أو نظام أو برنامج أو دعامة إليكترونية أو حاسب تكون موجودة فيه.

ويتم تسليم أدلتها الرقمية للجهة مصدرة الأمر على ألا يؤثر ذلك على استمرارية النظم وتقديم الخدمة أن كان لها مقتضٍ.

2 - البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقًا لغرض الضبط.

3 - أن تأمر مقدم الخدمة بتسليم ما لدية من بيانات أو معلومات تتعلق بنظام معلوماتى أو جهاز تقنى، موجودة تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمى خدمته وحركة الاتصالات التى تمت على ذلك النظام أو الجهاز التقنى.

وفى كل الأحوال، يحب أن يكون أمر جهة التحقيق المختصة مسببًا.

ويكون استئناف الأوامر المتقدمة أمام المحكمة الجنائية المختصة منعقدة فى غرفة المشورة فى المواعيد، ووفقًا للإجراءات المقررة بقانون الإجراءات الجنائية.

الإجراءات والقرارات الصادرة فى شأن طلبات حجب المواقع

مادة (7)

لجهة التحقيق المختصة، متى قامت أدلة على قيام موقع يُبث داخل الدولة أو خارجها، بوضع أى عبارات أو أرقام أو صور أو أفلام أو أى مواد دعائية، أو ما فى حكمها بما يُعد جريمة من الجرائم المنصوص عليها بالقانون، وتشكل تهديدًا للأمن القومى أو تعرض أمن البلاد أو اقتصادها القومى للخطر، أن تأمر بحجب الموقع أو المواقع محل البث، كلما أمكن تحقيق ذلك فنيًا. وعلى جهة التحقيق عرض أمر الحجب على المحكمة المختصة منعقدة فى غرفة المشورة، خلال أربع وعشرين ساعة مشفوعًا بمذكرة برأيها. وتُصدر المحكمة قرارها فى الأمر مسببًا إما بالقبول أو بالرفض، فى مدة لا تجاوز اثنتين وسبعين ساعة من وقت عرضه عليها.

ويجوز فى حالة الاستعجال لوجود خطر حال أو ضرر وشيك الوقوع، أن تقوم جهات التحرى والضبط المختصة بإبلاغ الجهاز، ليقوم بإخطار مقدم الخدمة على الفور بالحجب المؤقت للموقع أو المحتوى أو المواقع أو الروابط المذكورة فى الفقرة الأولى من هذه المادة وفقًا لأحكامها. ويلتزم مقدم الخدمة بتنفيذ مضمون الإخطار فور وروده إليه.

وعلى جهة التحرى والضبط التى قامت بالإبلاغ أن تحرر محضرًا تثبت فيه ما تم من إجراءات وفق أحكام الفقرة السابقة يُعرض على جهات التحقيق خلال ثمانٍ وأربعين ساعة من تاريخ الإبلاغ الذى وجهته للجهاز، وتتبع فى هذا المحضر ذات الإجراءات المبينة بالفقرة الثانية من هذه المادة، وتصدر المحكمة المختصة قرارها فى هذه الحالة، أما بتأييد ما تم من إجراءات حجب أو بوقفها. فإذا لم يُعرض المحضر المشار إليه فى الفقرة السابقة فى الموعد المحدد، يعد الحجب الذى تم كأن لم يكن.
ولمحكمة الموضوع أثناء نظر الدعوى أو بناءً على طلب جهة التحقيق أو الجهاز أو ذوى الشأن أن تأمر بإنهاء القرار الصادر بالحجب أو تعديل نطاقه.

وفى جميع الأحوال، يسقط القرار الصادر بالحجب بصدور أمر بألا وجه لإقامة الدعوى الجنائية، أو بصدور حكم نهائى فيها بالبراءة.

التظلم من القرارات الصادرة فى شأن طلبات حجب المواقع

مادة (8)

لكل من صدر ضده أمر قضائى من المنصوص عليه بالمادة (7) من هذا القانون، وللنيابة العامة ولجهة التحقيق المختصة ولكل ذوى شأن، أن يتظلم منه، أو من إجراءات تنفيذه، أمام محكمة الجنايات المختصة بعد انقضاء سبعة أيام من تاريخ صدور الأمر أو من تاريخ تنفيذه بحسب الأحوال، فإذا رُفض تظلمه فله أن يتقدم بتظلم جديد كلما انقضت ثلاثة أشهر من تاريخ الحكم برفض التظلم. وفى جميع الأحوال، يكون التظلم بتقرير يودع قلم كتاب محكمة الجنايات المختصة، وعلى رئيس المحكمة أن يحدد جلسة لنظر التظلم يعلن بها المتظلم والجهاز وكل ذى شأن، وعلى المحكمة أن تفصل فى التظلم خلال مدة لا تجاوز سبعة أيام من تاريخ التقرير به.

المنع من السفر

مادة (9)

يجوز للنائب العام أو من يفوضه من المحاميين العامين الأول بنيابات الاستئناف، ولجهات التحقيق المختصة، عند الضرورة، أو عند وجود أدلة كافية على جدية الاتهام فى ارتكاب جريمة من الجرائم

المنصوص عليها فى هذا القانون أو الشروع فى ارتكابها، أن يأمر بمنع المتهم من السفر خارج البلاد أو بوضع اسمه على قوائم ترقب الوصول، بأمر مسبب لمدة محددة.

ولمن صدر ضده أمر المنع من السفر أن يتظلم من هذا الأمر أمام محكمة الجنايات المختصة خلال خمسة عشر يومًا من تاريخ علمه به، فإذا رُفض تظلمه فله أن يتقدم بتظلم جديد كلما انقضت ثلاثة أشهر من تاريخ الحكم برفض التظلم.

ويكون التظلم بتقرير يودع قلم كتاب محكمة الجنايات المختصة، وعلى رئيس المحكمة أن يحدد جلسة لنظر التظلم تُعلن بها النيابة العامة والمتظلم، وعلى المحكمة أن تفصل فى التظلم خلال مدة لا تجاوز خمسة عشر يومًا من تاريخ التقرير به، بحكم مُسبب بعد سماع أقوال المتظلم والنيابة العامة أو جهة التحقيق المختصة حسب الأحوال، ولها فى سبيل ذلك أن تتخذ ما تراه من إجراءات أو تحقيقات ترى لزومها فى هذا الشأن.

ويجوز للنيابة العامة وجهات التحقيق المختصة فى كل وقت العدول عن الأمر الصادر منها، كما يجوز لها التعديل فيه برفع الاسم من قوائم المنع من السفر أو ترقب الوصول لمدة محددة، إذا دعت الضرورة لذلك.

وفى جميع الأحوال، ينتهى المنع من السفر بمرور سنه من تاريخ صدور الأمر، أو بصدور قرار بألا وجه لإقامة الدعوى الجنائية، أو بصدور قرار نهائى فيها بالبراءة، أيهما أقرب.

الخبراء

مادة (10)

يُنشأ بالجهاز سجلان لقيد الخبراء، يُقيد بأولهما الفنيون والتقنيون العاملون بالجهاز، ويقيد بالآخر الخبراء من الفنيين والتقنيين من غير العاملين به.

وتُطبق على الخبراء فى ممارسة عملهم وتحديد التزاماتهم وحقوقهم القواعد والأحكام الخاصة بقواعد تنظيم الخبرة أمام جهات القضاء.

واستثناء من تلك القواعد، تسرى على الخبراء المقيدين بالسجل الثانى القواعد والأحكام الخاصة بالمساءلة الإدارية والتأديبية الواردة بالقانون المنظم لعملهم إن وُجد.

وتحدد اللائحة التنفيذية لهذا القانون قواعد وشروط وإجراءات القيد فى كل من السجلين.

فى الأدلة الرقمية

مادة (11)

يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط الدعامات الإلكترونية، أو النظام المعلوماتى أو من برامج الحاسب، أو من أى وسيلة لتقنية المعلومات ذات قيمة وحجية الأدلة الجنائية المادية فى الإثبات الجنائى متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية لهذا القانون.

الباب الثالث

الجرائم والعقوبات

مادة (12)

مع عدم الإخلال بأية عقوبة أشد منصوص عليها فى قانون العقوبات أو أى قانون آخر، ومراعاة أحكام قانون الطفل الصادر بالقانون رقم 12 لسنة 1996، يعاقب على الجرائم التالية بالعقوبات المبينة قرين كل جريمة.

(الفصل الأول)

الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات

جريمة الانتفاع بدون حق بخدمات الاتصالات والمعلومات وتقنيتها

مادة (13)

يُعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من انتفع بدون وجه حق عن طريق شبكة النظام المعلوماتى أو إحدى وسائل تقنية المعلومات، بخدمة اتصالات أو خدمات قنوات البث المسموع والمرئى.

جريمة الدخول غير المشروع

مادة (14)

يُعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدًا، أو دخل بخطأ غير عمدى وبقى بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتى محظور الدخول عليه.

فإذا نتج عن ذلك الدخول إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتى، تكون العقوبة الحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتى ألف جنيه، أو بإحدى هاتين العقوبتين.

جريمة تجاوز حدود الحق فى الدخول

مادة (15)

يُعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو إحدى هاتين العقوبتين، كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتى مستخدمًا حقًا مخولاً له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول.

جريمة الاعتراض غير المشروع

مادة (16)

يُعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتين وخمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعترض بدون وجه حق أى معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلى وما فى حكمها.

جريمة الاعتداء على سلامة البيانات

والمعلومات والنظم المعلوماتية

مادة (17)

يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل أو عدل مسار أو ألغى كليًا أو جزئيًا متعمدًا وبدون وجه حق البرامج والبيانات أو المعلومات المخزنة، أو المعالجة، أو المولدة أو المخلقة على أى نظام معلوماتى وما فى حكمه، أيا كانت الوسيلة التى استخدمت فى الجريمة.

جريمة الاعتداء على البريد الإلكترونى

أو المواقع أو الحسابات الخاصة

مادة (18)

يعاقب بالحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل أو أبطأ أو اخترق بريدًا إلكترونيًا أو موقعًا أو حسابًا خاصًا بآحاد الناس.

فإذا وقعت الجريمة على بريد إلكترونى أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة، تكون العقوبة الحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتى ألف جنيه، أو بإحدى هاتين العقوبتين.

جريمة الاعتداء على تصميم موقع

مادة (19)

يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل أو أبطأ أو شوَّه أو أخفى أو غيَّر تصاميم موقع خاص بشركة أو مؤسسة أو منشأة أو شخص طبيعى بغير وجه حق.

جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة

مادة (20)

يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتى ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدًا، أو دخل بخطأ غير عمدى وبقى بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعًا أو بريدًا إلكترونيًا أو حسابًا خاصًا أو نظامًا معلوماتيًا يُدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكًا لها، أو يخصها.

فإذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية، تكون العقوبة السجن، والغرامة التى لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه.

وفى جميع الأحوال، إذا ترتب على أى من الأفعال السابقة إتلاف تلك البيانات أو المعلومات أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتى أو البريد الإلكترونى، أو تدميرها أو تشويهها أو تغييرها أو تغييرها أو تصميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها، أو إلغاؤها كليًا أو جزئيًا، بأى وسيلة كانت، تكون العقوبة السجن والغرامة التى لا تقل عن مليون جنيه ولا تجاوز خمسة ملايين جنيه.

جريمة الاعتداء على سلامة الشبكة المعلوماتية

مادة (21)

يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من تسبب متعمدًا فى إيقاف شبكة معلوماتية عن العمل أو تعطيلها أو الحد من كفاءة عملها أو التشويش عليها أو إعاقتها أو اعتراض عملها أو أجرى بدون وجه حق معالجة إلكترونية للبيانات الخاصة بها.

ويعاقب كل من تسبب بخطئه فى ذلك بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن خمسون ألف جنيه ولا تجاوز مائتى ألف جنيه، أو بإحدى العقوبتين.

فإذا وقعت الجريمة على شبكة معلوماتية تخص الدولة أو أحد الأشخاص الاعتبارية العامة أو تمتلكها أو تدار بمعرفتها تكون العقوبة السجن المشدد، وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه.

البرامج والأجهزة والمعدات المستخدمة

فى ارتكاب جرائم تقنية المعلومات

مادة (22)

يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه أو بإحدى هاتين العقوبتين، كل من حاز أو أحرز أو جلب أو باع أو أتاح أو صنع أو أنتج أو استورد أو صدر أو تداول بأى صورة من صور التداول، أى أجهزة أو معدات أو أدوات أو برامج مصممة أو مطورة أو محورة أو أكواد مرور أو شفرات أو رموز أو أى بيانات مماثلة، بدون تصريح من الجهاز أو مسوغ من الواقع أو القانون، وثبت أن ذلك السلوك كان بغرض استخدام أى منها فى ارتكاب أية جريمة من المنصوص عليها فى هذا القانون أو إخفاء آثارها أو أدلتها أو ثبت ذلك الاستخدام أو التسهيل أو الإخفاء.

(الفصل الثانى)

الجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات

جرائم الاحتيال والاعتداء على بطاقات البنوك

والخدمات وأدوات الدفع الإلكترونى

مادة (23)

يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر والغرامة التى لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، فى الوصول بدون وجه حق إلى أرقام أو بيانات أو بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الالكترونية.

فإن قصد من ذلك استخدامها فى الحصول على أموال الغير أو ما تتيحه من خدمات، يعاقب بالحبس مدة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين.

وتكون العقوبة الحبس مدة لا تقل عن سنة، والغرامة التى لا تقل عن مائة ألف جنيه ولا تجاوز مائتى ألف، أو إحدى هاتين العقوبتين، إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على تلك الخدمات أو مال الغير.

الجرائم المتعلقة باصطناع المواقع

والحسابات الخاصة والبريد الإلكترونى

مادة (24)

يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز ثلاثين ألف جنيه أو بإحدى العقوبتين كل من اصطنع بريدًا إلكترونيًا أو موقعًا أو حسابًا خاصًا ونسبه زورًا إلى شخص طبيعى أو اعتبارى.

فإذا استخدم الجانى البريد أو الموقع أو الحساب الخاص المصطنع فى أمر يسئ إلى من نُسب إليه، تكون العقوبة الحبس الذى لا تقل مدته عن سنة والغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتى ألف جنيه، أو بإحدى هاتين العقوبتين.

وإذا وقعت الجريمة على أحد الأشخاص الاعتبارية العامة، تكون العقوبة السجن، والغرامة التى لا تقل عن مائة ألف جنيه، ولا تزيد على ثلاثمائة ألف جنيه.

(الفصل الثالث)

الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة

والمحتوى المعلوماتى غير المشروع

مادة (25)

يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعتدى على أى من المبادئ أو القيم الأسرية فى المجتمع المصرى، أو انتهك حرمة الحياة الخاصة أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع إلكترونى لترويج السلع أو الخدمات دون موافقته، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخبارًا أو صورًا وما فى حكمها، تنتهك خصوصية أى شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة.

مادة (26)

يعاقب بالحبس مدة لا تقل عن سنتين ولا تجاوز خمس سنوات وبغرامة لا تقل عن مائة ألف جنيه لا تجاوز ثلاثمائة ألف جنيه أو بإحدى هاتين العقوبتين كل من تعمد استعمال برنامج معلوماتى أو تقنية معلوماتية فى معالجة معطيات شخصية للغير لربطها بمحتوى منافٍ للآداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه.

(الفصل الرابع)

الجرائم المرتكبة من مدير الموقع

مادة (27)

فى غير الأحوال المنصوص عليها فى هذا القانون، يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن مائة ألف جنيه، ولا تزيد عن ثلاثمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أنشأ أو أدار أو استخدم موقعًا أو حسابًا خاصًا على شبكة معلوماتية يهدف إلى ارتكاب أو تسهيل ارتكاب جريمة معاقب عليها قانونًا.

مادة (28)

يعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن عشرين ألف ولا تجاوز مائتى ألف جنيه، أو بإحدى هاتين العقوبتين، كل مسئول عن إدارة موقع أو حساب خاص أو بريد إلكترونى أو نظام معلوماتى، إذا أخفى أو عبث بالأدلة الرقمية لإحدى الجرائم المنصوص عليها فى هذا القانون والتى وقعت على موقع أو حساب أو بريد إلكترونى بقصد إعاقة عمل الجهات الرسمية المختصة.

مادة (29)

يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن عشرين ألف ولا تجاوز مائتى ألف جنية، أو بإحدى هاتين العقوبتين كل مسئول عن إدارة الموقع أو الحساب الخاص أو البريد الإلكترونى أو النظام المعلوماتى عَرَّض أيًا منهم لإحدى الجرائم المنصوص عليها فى هذا القانون.

ويعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل مسئول عن إدارة الموقع أو الحساب الخاص أو البريد الإلكترونى أو النظام المعلوماتى تسبب بإهماله فى تَعرّض أى منهما لإحدى الجرائم المنصوص عليها فى هذا القانون، وكان ذلك بعدم اتخاذه التدابير والاحتياطيات التأمينية الواردة فى اللائحة التنفيذية لهذا القانون.

(الفصل الخامس)

المسئولية الجنائية لمقدمى الخدمة

مادة (30)

يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه، أو بإحدى هاتين العقوبتين، كل مُقدم خدمة امتنع عن تنفيذ القرار الصادر من المحكمة الجنائية المختصة بحجب أحد المواقع أو الروابط أو المحتوى المُشار إليه فى الفقرة الأولى من المادة (7) من هذا القانون. فإذا ترتب على الامتناع عن تنفيذ القرار الصادر من المحكمة، وفاة شخص أو أكثر، أو الإضرار بالأمن القومى، تكون العقوبة السجن المشدد والغرامة التى لا تقل عن ثلاثة ملايين جنيه ولا تجاوز عشرين مليون جنيه، وتقضى المحكمة فضلاً عن ذلك بإلغاء ترخيص مزاولة النشاط.

مادة (31)

يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز عشرين ألف جنيه، أو بإحدى هاتين العقوبتين، كل مقدم خدمة خالف الأحكام الواردة بالبند (2) من الفقرة أولا من المادة (2) من هذا القانون، وتتعدد عقوبة الغرامة بتعدد المجنى عليهم من مستخدمى الخدمة.

مادة (32)

يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل مقدم خدمة امتنع عن تنفيذ القرار الصادر من جهة التحقيق المختصة بتسليم ما لديه من البيانات أو المعلومات المشار إليها فى المادة (6) من هذا القانون.

مادة (33)

يعاقب بغرامة لا تقل عن خمسة ملايين جنية ولا تجاوز عشرة ملايين جنيه، كل مقدم خدمة أخل بأى من التزاماته المنصوص عليها فى البند (1) من الفقرة (أولاً) من المادة (2) من هذا القانون. وتضاعف عقوبة الغرامة فى حالة العود، وللمحكمة أن تقضى بإلغاء الترخيص.

ويعاقب بغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتى ألف جنيه، كل مقدم خدمة خالف أحكام الفقرة (ثانيًا) و(رابعًا) من المادة (2) من هذا القانون.

ويعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبالغرامة التى لا تقل عن مائتى ألف جنيه ولا تجاوز مليون جنيه، كل مقدم خدمة خالف أحكام الفقرة (ثالثًا) من المادة (2) من هذا القانون.

(الفصل السادس)

الظروف المشددة فى الجريمة

مادة (34)

إذا وقعت أى جريمة من الجرائم المنصوص عليها فى هذا القانون بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر، أو الإضرار بالأمن القومى للبلاد أو بمركزها الاقتصادى أو منع أو عرقلة ممارسة السلطات العامة لأعمالها، أو تعطيل أحكام الدستور أو القوانين أو اللوائح أو الإضرار بالوحدة الوطنية والسلام الإجتماعى تكون العقوبة السجن المشدد.

(الفصل السابع)

المسئولية الجنائية للشخص الاعتبارى

مادة (35)

يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن ثلاثين ألف جنية ولا تزيد عن مائة ألف جنية أو بإحدى هاتين العقوبتين، كل مسئول عن الإدارة الفعلية لأى شخص اعتبارى، إذا تعرض الموقع أو الحساب الخاص أو البريد الإلكترونى أو النظام المعلوماتى المخصص للكيان الذى يديره، لأى جريمة من الجرائم المنصوص عليها فى هذا القانون، ولم يبلغ بذلك الجهات المختصة وقت علمه بالجريمة.

مادة (36)

فى الأحوال التى ترتكب فيها أى من الجرائم المنصوص عليها فى هذا القانون، باسم ولحساب الشخص الاعتبارى، يعاقب المسئول عن الإدارة الفعلية إذا ثبت علمه بالجريمة أو سهل ارتكابها تحقيقا لمصلحة له أو لغيره بذات عقوبة الفاعل الأصلى.

وللمحكمة أن تقضى بإيقاف ترخيص مزاولة الشخص الاعتبار للنشاط مدة لا تزيد على سنة، ولها فى حاله العود أن تحكم بإلغاء الترخيص أو حل الشخص الاعتبارى بحسب الأحوال، ويتم نشر الحكم فى جريدتين يوميتين واسعتى الانتشار على نفقة الشخص الاعتبارى.

مادة (37)

فى تطبيق أحكام هذا القانون، لا يترتب على تقرير مسئولية الإدارة الفعلية للشخص الاعتبارى استبعاد المسئولية الجنائية للأشخاص الطبيعيين الفاعلين الأصليين أو الشركاء عن ذات الوقائع التى تقوم بها الجريمة.

(الفصل الثامن)

العقوبات التبعية

مادة (38)

مع عدم الإخلال بحقوق الغير حسن النية، على المحكمة فى حالة الحكم بالإدانة فى أى جريمة من الجرائم المنصوص عليها فى هذا القانون، أن تقضى بمصادرة الأدوات والآلات والمعدات والأجهزة مما لا يجوز حيازتها قانونا، أو غيرها مما يكون قد استخدم فى ارتكاب الجريمة، أو سهل أو ساهم فى ارتكابها.

وفى الحالات التى يتعين لمزاولة النشاط فيها الحصول على ترخيص من إحدى الجهات الحكومية، وكان الشخص الاعتبارى المدان بأى جريمة منصوص عليها فى هذا القانون لم يحصل على الترخيص فيحكم فضلاً عن العقوبات المقررة بالغلق.

مادة (39)

للمحكمة إذا قضت بالإدانة على أحد الموظفين العموميين، لارتكابه جريمة من الجرائم المنصوص عليها فى هذا القانون، أثناء وبسبب تأديته لوظيفته، أن تقضى بعزله مؤقتا من وظيفته، إلا فى الحالات المشار إليها فى المادة (34) من هذا القانون فيكون العزل وجوبيًا.

(الفصل التاسع)

الشروع والإعفاء من العقوبة

مادة (40)

يعاقب كل من شرع فى ارتكاب الجرائم المنصوص عليها بالقانون، يعاقب بما لا يجاوز نصف الحد الأقصى للعقوبة المقررة للجريمة.

مادة (41)

يعفى من العقوبات، المقررة للجرائم المنصوص عليها فى هذا القانون، كل من بادر من الجناة أو الشركاء إلى إبلاغ السلطات القضائية أو السلطات العامة بما يعلمه عنها قبل البدء فى تنفيذ الجريمة وقبل كشفها.

ويجوز للمحكمة الإعفاء من العقوبة أو التخفيف منها إذا حصل البلاغ بعد كشف الجريمة وقبل التصرف فى التحقيق فيها، إذا مكن الجانى أو الشريك فى أثناء التحقيق السلطات المختصة من القبض على مرتكبى الجريمة الآخرين، أو على ضبط الأموال موضوع الجريمة، أو أعان أثناء البحث والتحقيق على كشف الحقيقة فيها، أو على القبض على مرتكبى جريمة أخرى مماثله لهذا النوع والخطورة.

ولا يخل حكم هذه المادة، بوجوب الحكم برد المال المتحصل من الجرائم المنصوص عليها بالقانون.

الصلح والتصالح

مادة (42)

يجوز للمتهم فى أية حالة كانت عليها الدعوى الجنائية، وقبل صيرورة الحكم باتا، إثبات الصلح مع المجنى عليه أو وكيله الخاص أو خلفه العام، أمام النيابة العامة أو المحكمة المختصة بحسب الأحوال، وذلك فى الجنح المنصوص عليها فى المواد (14، 15، 16،17، 18، 19، 23، 26، 28، 30، 31) من هذا القانون.

ولا يُنتج إقرار المجنى عليه بالصلح المنصوص عليه بالفقرة السابقة أثره إلا باعتماده من الجهاز بالنسبة للجنح المنصوص عليها بالمواد (14، 17، 18، 23) من هذا القانون.

كما لا يُقبل التصالح إلا من خلال الجهاز بخصوص الجنح المنصوص عليها بالمادتين (29، 35) من هذا القانون

ولا يسقط حق المتهم فى التصالح برفع الدعوى الجنائية إلى المحكمة المختصة إذا دفع ثلثى الحد الأقصى للغرامة المقررة للجريمة أو قيمة الحد الأدنى أيهما أكثر، وذلك قبل صدور حكم نهائى فى الموضوع.

وفى جميع الأحوال، يجب على المتهم الذى يرغب فى التصالح أن يسدد قبل رفع الدعوى الجنائية مبلغًا يعادل ضعف الحد الأقصى للغرامة المقررة للجريمة. ويكون السداد إلى خزانة المحكمة المختصة أو النيابة العامة بحسب الأحوال.

ويترتب على الصلح انقضاء الدعوى الجنائية، ولا أثر للصلح على حقوق المضرور من الجريمة أو على الدعوى المدنية.

الباب الرابع

أحكام انتقالية وختامية

مادة (43)

يلتزم مقدمو الخدمة والمخاطبين بأحكام القانون والتزاماته باتخاذ الإجراءات اللازمة لتقنين أوضاعهم خلال سنة من تاريخ العمل بهذا القانون.

مادة (44)

يُصدر السيد رئيس مجلس الوزراء اللائحة التنفيذية لهذا القانون خلال ثلاثة أشهر من تاريخ العمل به.

مادة (45)

يُنشر هذا القانون فى الجريدة الرسمية، ويُعمل به من اليوم التالى لتاريخ نشره.

يُبصم هذا القانون بخاتم الدولة، ويُنفذ كقانون من قوانينها.

صدر برئاسة الجمهورية فى 3 ذى الحجة سنة 1439هـ

(الموافق 14 أغسطس سنة 2018م).

عبد الفتاح السيسى

فهرس الملاحق

فهرس المحتويات