

مفهوم الجرائم المعلوماتية وتحدياتها التشريعية في فلسطين

إعداد

نبيل محمود فريد أبو الرب

إشراف

د. أنور جاتم

قدمت هذه الأطروحة استكمالاً لمتطلبات الحصول على درجة الماجستير في القانون العام
بكلية الدراسات العليا، في جامعة النجاح الوطنية، نابلس - فلسطين.

2018

مفهوم الجرائم المعلوماتية وتحدياتها التشريعية في فلسطين

إعداد

نبيل محمود فريد أبو الرب

نوقشت هذه الأطروحة بتاريخ 2018/1/18م، وأجيزت.

أعضاء لجنة المناقشة

التوقيع

1. د. أنور جاتم / مشرفاً ورئيساً

2. د. رائد طه / ممتحناً خارجياً

3. د. عبد اللطيف ربابعة / ممتحناً داخلياً

الإهداء

أقدم هذا الجهد العلمي

إلى رمز الحنان أُمي ...

إلى رمز العزة والشموخ أبي ...

إلى سندي وقوتي إخواني وأخواتي ...

إلى من تركوا بصمة جميلة في حياتي أصدقائي ...

إلى كل من علمني وخاصةً أساتذتي في جامعة النجاح الوطنية ...

الشكر والتقدير

أقدم الشكر والعرفان إلى الدكتور أنور جانم المشرف على هذه الرسالة، على ما قدمه لي من توجهات علمية حكيمة ومثمرة طيلة مدة إعداد هذه الرسالة.

كما أتقدم بجزيل الشكر إلى أعضاء لجنة المناقشة.

الدكتور رائد طه ممتحناً خارجياً والدكتور عبد اللطيف ربابعة ممتحناً داخلياً.

وأشكر مجلس القضاء الأعلى والنيابة العامة وجهاز الشرطة الفلسطينية على تعاونهم في إجراء المقابلات وتقديم البيانات والمعلومات القيمة.

الإقرار

أنا الموقع أدناه، مقدم الرسالة التي تحمل العنوان:

مفهوم الجرائم المعلوماتية وتحدياتها التشريعية في فلسطين

أقر بأن ما اشتملت عليه هذه الرسالة إنما هو نتاج جهدي الخاص، باستثناء ما تمت الإشارة إليه حيث ما أن هذه الرسالة كاملة، أو أي جزء منها لم يقدم من قبل لنيل أي درجة أو لقب علمي أو بحث لدى أي مؤسسة تعليمية أو بحثية أخرى.

Declaration

The work provided in this thesis, unless otherwise referenced, is the researcher's own work, and has not been submitted elsewhere for any other degree or qualification.

Student's name:

أسم الطالب:

Signature

التوقيع:

Date:

التاريخ:

فهرس المحتويات

الصفحة	الموضوع
ج	الإهداء
د	الشكر والتقدير
هـ	الإقرار
ط	فهرس الجداول
ك	فهرس الأشكال
ل	فهرس الملاحق
م	الملخص
1	المقدمة
10	الفصل الأول: ماهية الجريمة المعلوماتية
10	المبحث الأول: مفهوم الجريمة المعلوماتية
11	المطلب الأول: تعريف الجريمة المعلوماتية
11	الفرع الأول: وفقا لوسيلة ارتكاب الجريمة
12	الفرع الثاني: وفقا لمحل أو موضوع الجريمة
13	الفرع الثالث: وفقا لمعرفة الفاعل بتقنية المعلومات
13	الفرع الرابع: وفقا لمعايير متعددة
15	المطلب الثاني: خصائص الجريمة المعلوماتية
15	الفرع الأول: عابرة للحدود والدول
16	الفرع الثاني: صعوبة الإثبات والاكتشاف
17	الفرع الثالث: سهولة الارتكاب
17	الفرع الرابع: جرائم مغرية للمجرمين
18	الفرع الخامس: ترتكب بتعاون أكثر من شخص
18	المطلب الثالث: تقسيمات الجرائم المعلوماتية
19	الفرع الأول: منظمة التعاون الاقتصادي والتنمية
20	الفرع الثاني: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات
22	الفرع الثالث: الاتفاقية الدولية لمكافحة الجرائم المعلوماتية بودابست 2001
23	الفرع الرابع: المجلس الأوروبي
24	الفرع الخامس: التقسيم الفرنسي

25	الفرع السادس: التقسيم الأمريكي
27	المبحث الثاني: أركان الجريمة المعلوماتية وأطرافها
27	المطلب الأول: أركان الجريمة المعلوماتية
28	الفرع الأول: الركن المادي
30	الفرع الثاني: الركن المعنوي
31	المطلب الثاني: أطراف الجريمة المعلوماتية
32	الفرع الأول: الفاعل
34	الفرع الثاني: المجني عليه
34	المطلب الثالث: المسؤولية الجزائية لمرتكبي الجرائم المعلوماتية
40	الفصل الثاني: الجرائم المعلوماتية وتحدياتها
41	المبحث الأول: الواقع القانوني للجرائم المعلوماتية في فلسطين قبل صدور القرار بقانون بشأن الجرائم الإلكترونية
42	المطلب الأول: تشريعات مختلفة في مكافحة الجرائم الإلكترونية
42	الفرع الأول: قانون العقوبات الأردني رقم 16 لسنة 1960
45	الفرع الثاني: قانون رقم 3 لسنة 1996 بشأن الاتصالات السلكية واللاسلكية
45	الفرع الثالث: القرار بقانون رقم (15) لسنة 2009 بشأن الهيئة الفلسطينية لتنظيم قطاع الاتصالات
46	الفرع الرابع: قانون المعاملات الإلكترونية رقم 15 لسنة 2017
47	المطلب الثاني: القرار بقانون بشأن الجرائم الإلكترونية رقم 16 لسنة 2017
47	الفرع الأول: من الناحية الموضوعية
48	أولاً: جرائم تقع بواسطة الكترونية
54	ثانياً: جرائم تقع على النظام الإلكتروني
58	ثالثاً: أحكام عامة
63	الفرع الثاني: من الناحية الإجرائية
63	أولاً: دور جهاز الشرطة
68	ثانياً: دور النيابة العامة
73	ثالثاً: دور القضاء
74	الفرع الثالث: ملاحظات عامة حول القرار بقانون بشأن الجرائم الإلكترونية رقم 16 لسنة 2017

78	المبحث الثاني: التحديات التشريعية ودور المؤسسات في الوقاية من الجرائم المعلوماتية وواقعها في فلسطين
79	المطلب الأول: التحديات التي تواجه المشرع الفلسطيني في ملاحقة مرتكبي الجرائم المعلوماتية
79	الفرع الأول: وضع استراتيجية تشريعية فلسطينية
80	الفرع الثاني: تحديات قانونية
81	الفرع الثالث: تطبيق القانون وإنفاذ قرارات المحاكم
82	الفرع الرابع: مواكبة التطورات الإقليمية والدولية
82	الفرع الخامس: تعزيز المشاركة المجتمعية
84	المطلب الثاني: دور المؤسسات في الوقاية من الجرائم المعلوماتية ومكافحتها
84	الفرع الأول: المجلس التشريعي
84	الفرع الثاني: المؤسسة الأمنية
85	الفرع الثالث: المؤسسات الإعلامية
85	الفرع الرابع: المؤسسات الدينية
86	الفرع الخامس: الأسرة
86	الفرع السادس: المؤسسات التعليمية والثقافية
87	الفصل الثالث: إجراءات الدراسة والتحليل الإحصائي
120	النتائج
121	التوصيات
122	المصادر والمراجع
130	الملاحق
b	Abstract

فهرس الجداول

الرقم	الجداول	الصفحة
جدول (1)	عدد القضايا الواردة للنيابة العامة المتعلقة بالجرائم المعلوماتية "الإلكترونية" للعام 2016	71
جدول (2)	نتائج معامل كرونباخ الفا (Cronbach Alpha) باستخدام برنامج SPSS	88
جدول (3)	توزيع أفراد عينة الدراسة تبعاً لمتغيرات الدراسة المستقلة	90
جدول (4)	نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين متغير التعرض لجريمة الكترونية ومتغير الجنس	106
جدول (5)	نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين متغير التعرض لجريمة الكترونية ومتغير مكان السكن	107
جدول (6)	نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين متغير التعرض لجريمة الكترونية ومتغير العمر	108
جدول (7)	نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين متغير التعرض لجريمة الكترونية ومتغير المستوى العلمي	109
جدول (8)	نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين بين متغير المعرفة عن القرار بقانون بشأن الجرائم الإلكترونية ومتغير الجنس	110
جدول (9)	نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين بين متغير المعرفة عن القرار بقانون بشأن الجرائم الإلكترونية ومتغير مكان السكن	111
جدول (10)	نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين متغير المعرفة عن القرار بقانون بشأن الجرائم الإلكترونية ومتغير العمر	112
جدول (11)	نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين بين متغير المعرفة عن القرار بقانون بشأن الجرائم الإلكترونية ومتغير المستوى العلمي	113
جدول (12)	نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين الاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية ومتغير الجنس	115

116	نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين الاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية ومتغير مكان السكن	جدول (13)
117	نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين الاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية ومتغير العمر	جدول (14)
119	نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين الاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية ومتغير المستوى العلمي	جدول (15)

فهرس الأشكال

الرقم	الشكل	الصفحة
شكل (1)	أعداد الشكاوى المقدمة لدى وحدة الجرائم الإلكترونية في جهاز الشرطة الفلسطيني للأعوام 2013 حتى 14.8.2017	66
شكل (2)	تصنيف الجرائم الإلكترونية الواردة إلى وحدة الجرائم الإلكترونية في جهاز الشرطة الفلسطيني حسب نوعها وعددها للعام 2016	67
شكل (3)	عدد الشكاوى حول مرتكبي الجرائم الإلكترونية التي وصلت للنيابة العامة في الأعوام 2014 و 2015 و 2016	70
شكل (4)	عدد القضايا الواردة للنيابة العامة المتعلقة بالجرائم المعلوماتية "الإلكترونية" للعام 2016	71
شكل (5)	مدى تعرض أفراد العينة إلى جريمة الكترونية	92
شكل (6)	عدد المرات التي تعرض فيها أفراد العينة لجريمة الكترونية	94
شكل (7)	نوع الجريمة الإلكترونية التي تعرض لها أفراد العينة	95
شكل (8)	تقديم الشكاوى لدى الجهات المختصة	96
شكل (9)	الجهات التي قدمت إليها الشكاوى	97
شكل (10)	مدى رضا أفراد العينة عن نتائج الشكاوى	98
شكل (11)	الأسباب التي حالت دون تقديم الشكاوى من قبل أفراد العينة لدى الجهات المختصة ضد مرتكبي الجرائم الإلكترونية	99
شكل (12)	مدى معرفة أفراد العينة بالقرار بقانون بشأن الجرائم الإلكترونية	100
شكل (13)	رأي أفراد العينة بالقرار بقانون بشأن الجرائم الإلكترونية	101
شكل (14)	مدى استعداد أفراد العينة لتقديم شكاوى لدى الجهات المختصة ضد مرتكبي الجرائم الإلكترونية بعد صدور القرار بقانون بشأن الجرائم الإلكترونية	103
شكل (15)	الإجراءات الواجب اتخاذها حسب أفراد العينة للحد من الجرائم الإلكترونية في فلسطين	104

فهرس الملاحق

الرقم	الملحق	الصفحة
ملحق (1)	أسئلة الاستبيان وتحليلها	130
ملحق (2)	استبانة الدراسة	145

مفهوم الجرائم المعلوماتية وتحدياتها التشريعية في فلسطين

إعداد

نبيل محمود فريد أبو الرب

إشراف

د. أنور جاتم

الملخص

هدفت هذه الدراسة إلى تحليل ظاهرة الجرائم الإلكترونية وتحدياتها التشريعية في فلسطين من خلال التعريف بماهية الجريمة المعلوماتية، ودراسة مدى ملائمة التشريعات والقوانين الفلسطينية السارية والتحديات التي تواجه المشرع الفلسطيني للحد منها، وتبيان آليات ملاحقة مرتكبيها من قبل الشرطة والنيابة العامة والقضاء، ودراسة واقعها في فلسطين، كما هدفت الدراسة إلى المساهمة في نشر الوعي والثقافة القانونية حول مخاطر الجريمة المعلوماتية بين أفراد المجتمع الفلسطيني.

خلصت الدراسة إلى وجود صعوبات موضوعية وإجرائية في تحديد مفهوم واكتشاف وإثبات الجرائم المعلوماتية، وفراغ القوانين الجزائية القائمة من إجراءات البحث والتحري وجمع الأدلة وتفتيشها وضبطها. الجرائم الإلكترونية ظاهرة انتشرت في فلسطين وبشكل متزايد في ظل الاعتماد على القوانين العادية (التقليدية) التي لا تلبي الحد الأدنى من متطلبات مكافحتها والحد منها، وجاء القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية لسد الفراغ القانوني بهذا الخصوص دون إصدار لائحته التنفيذية والذي لا زال يُثير جدلاً واسعاً حول بنوده ومدى ملائمته للواقع الفلسطيني للوقاية والحد من الجرائم الإلكترونية وردع مرتكبيها. توصلت الدراسة إلى وجود ضعف في مؤسسة العمل على ملاحقة مرتكبي الجرائم المعلوماتية في ظل نقص الموظفين المؤهلين وغياب الأدلة الإجرائية لدى جهاز الشرطة والنيابة العامة حول آلية تقديم الشكاوى وأساليب التحقيق فيها لملاحقة ومتابعة مرتكبيها، ونقص الدورات التدريبية لأفراد العدالة الجنائية حول بناء الدليل الرقمي المعلوماتي وكيفية التعامل مع الوسائل التقنية الحديثة لإثبات الجريمة الإلكترونية، وحداثة تعامل القضاء الفلسطيني مع تلك الجرائم، وغياب خطة

استراتيجية وطنية للوقاية والحد من الجرائم المعلوماتية، وضعف دور المؤسسات في نشر
التوعية والثقافة القانونية حول مخاطرها.

المقدمة

أحدثت ثورة المعلومات والاتصالات تغيرات جذرية ونوعية في مختلف نظم الحياة الاقتصادية والسياسية والاجتماعية والقانونية في نهاية القرن العشرين، نتيجة الاندماج الكبير بين قطاعي تكنولوجيا المعلومات والاتصالات وما رافقها من تطورات تقنية وظهور الفضاء المعلوماتي.

تركت الثورة المعلوماتية وبسبب التقنيات العالية التي تقوم عليها والتي تتمثل في استخدام الحواسيب والشبكات المعلوماتية أثراً إيجابية على حياة الأفراد والمؤسسات والدول، حيث تعتمد مختلف القطاعات في الوقت الراهن في أداء عملها على استخدام الأنظمة المعلوماتية لما لها من ميزة في السرعة والدقة في تجميع المعلومات وتخزينها ومعالجتها ونقلها وتبادلها بين الأفراد والشركات والمؤسسات والدول، حيث أصبحت هذه الأنظمة منجماً لأسرار الدول والأشخاص السياسية والاقتصادية والمالية والأمنية¹.

أدى انتشار استخدام التقنية العالية لمنجزات الثورة المعلوماتية إلى ظهور من يسيء استخدام الأنظمة المعلوماتية واستغلالها بشكل غير مشروع تضر بمصالح الأفراد والمؤسسات والشركات والدول، وفي الفضاء المعلوماتي تكونت بيئة خصبة لظهور أنماط مستحدثة من الجرائم المعلوماتية، التي يصعب حصرها نتيجة تطور التقنيات المعلوماتية وأساليب ارتكابها كتعطيل الأجهزة وصناعة الفايروسات ونشرها، وعمليات القرصنة والاختراقات²، والاحتيايل والجرائم المالية، والإرهاب الإلكتروني، والابتزاز المعلوماتي، والحرب الإلكترونية وغيرها، وهذا يتطلب سن تشريعات وقوانين تقي وتحد وتردع مرتكبيها.

¹ المومني، عبد القادر نهلا: الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الثانية، عمان، 2010، ص13.

² العجمي، عبد الله دغش: المشكلات العلمية والقانونية للجرائم الإلكترونية "دراسة مقارنة"، رسالة ماجستير (منشورة)، جامعة الشرق الأوسط، عمان، 2014، ص11.

القانون الجنائي التقليدي لا يكفي من حيث المبدأ لمواجهة هذا الشكل الجديد من الجرائم المعلوماتية، مما استدعى تدخل الدول والحكومات عن طريق تعديل النصوص القانونية القائمة أو إصدار تشريعات وقوانين خاصة لمواجهة الجرائم المعلوماتية على المستوى الداخلي والخارجي، وتعتبر السويد أول دولة سنت تشريعات خاصة بجرائم الحاسب الآلي في عام 1973، وتبعتها الولايات المتحدة والدول الأوروبية في وضع تشريعات خاصة أو تعديل قانون العقوبات لديها بغية تجريم مرتكبي الجرائم المعلوماتية، كما بادرت العديد من الدول العربية إصدار تشريعات وقوانين خاصة لمكافحة الجرائم المعلوماتية منها: الإمارات العربية المتحدة، الكويت، البحرين، المملكة العربية السعودية، قطر، والأردن¹.

أما في فلسطين لجأت النيابة العامة والمحاكم الفلسطينية إلى تطبيق نصوص قانون رقم (3) لسنة 1996 بشأن الاتصالات السلكية واللاسلكية، ونصوص الجرائم التقليدية من قانون العقوبات الأردني رقم 16 لسنة 1960 الساري المفعول على الجرائم المعلوماتية، واللدان لا يلبيان الحد الأدنى لمكافحتها، حيث تأخذ بالقياس نصوص الجرائم العادية على الجرائم المعلوماتية بسبب عدم وجود نصوص قانونية تجرم الجرائم المعلوماتية صراحةً أو ضمناً في التشريعات والقوانين الفلسطينية قبل إصدار القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية. وهذا القياس يخالف المبدأ الأساسي في القانون الجنائي: (لا جريمة ولا عقوبة إلا بنص قانوني).

ولتحقيق متطلبات الدراسة تناول الفصل الأول مفهوم الجريمة المعلوماتية والخصائص التي تميزها عن غيرها من الجرائم وتصنيفاتها وأركانها وأطرافها والمسؤولية الجزائية لمرتكبيها، أما الفصل الثاني فقد بحث الواقع القانوني والتشريعي للجرائم المعلوماتية في فلسطين ودور جهاز الشرطة والنيابة العامة والقضاء من الناحية الموضوعية والإجرائية في ملاحقة مرتكبيها والتحديات التشريعية التي تواجه المشرع الفلسطيني في مواجهة ومكافحة الجريمة المعلوماتية

¹ الديربي، عبد العال: الجريمة الإلكترونية بين التشريع والقضاء في الدول الغربية، منشورات المركز العربي لأبحاث الفضاء الإلكتروني بتاريخ 2013/3/1، ص 1، نشر على موقع www.acronline.com.

ودور المؤسسات في الوقاية والحد منها وواقعها في فلسطين، وفي الفصل الثالث تم إجراء تحليل لاستبانة الدارسة.

أهمية الدراسة

تكمّن أهمية هذه الدراسة في التعرف على الجريمة المعلوماتية المستحدثة وسوء استغلال وسائل الاتصالات الحديثة من قبل مرتكبي الجرائم المعلوماتية، والبحث وتحليل ظاهرة الجرائم المعلوماتية وانتشارها في فلسطين وتبيان مدى خطورة تلك الجرائم، وأهمية نشر الوعي والثقافة القانونية بين أفراد المجتمع للحد من الوقوع بها، ومحاولة إيجاد الحلول للمشكلات التي تثيرها الجرائم المعلوماتية في التشريعات سارية المفعول، وكذلك استفادة الباحثين والشرطة والنيابة العامة والقضاء والمشرع الفلسطيني وأصحاب الاختصاص من نتائجها وتوصياتها.

أهداف الدراسة

تهدف هذه الدراسة إلى:

1. التعريف بالطبيعة الموضوعية للجريمة المعلوماتية.
2. دراسة واقع وتحديات الجرائم المعلوماتية في فلسطين.
3. دراسة مدى ملائمة التشريعات والقوانين سارية المفعول لمكافحة الجرائم المعلوماتية في فلسطين وآليات ملاحقة مرتكبيها.
4. المساهمة في نشر الوعي والثقافة القانونية حول مخاطر الجريمة المعلوماتية بين أفراد المجتمع الفلسطيني.

مشكلة الدراسة

أحدث ظهور الجرائم المعلوماتية تحديات جمة في مواجهة النظام القانوني القائم وخاصة قانون العقوبات في مختلف دول العالم ومنها فلسطين، هذا الواقع الجديد دعا فقهاء القانون البحث في كفاية القوانين سارية المفعول ونصوصها التقليدية لمواجهة الجرائم المعلوماتية وضرورة استحداث تشريعات وقوانين ونصوص خاصة قادرة على احتوائها ومراعاة طبيعتها وخصوصيتها تكفل الحد من هذه الجرائم وإصلاح المجرم المعلوماتي وردعه.

تعتبر الجرائم المعلوماتية ظاهرة حديثة في فلسطين ظهرت مع تنامي وتزايد استخدام الوسائل الإلكترونية الحديثة وبخاصة الشبكة المعلوماتية وأجهزة الحاسوب والهاتف المحمول، حيث أظهرت أرقام وإحصائيات رسمية صادرة عن جهاز الشرطة الفلسطينية والنيابة العامة ازدياد ظاهرة الجرائم المعلوماتية خلال السنوات الأخيرة في فلسطين، في ظل غياب قانون عقوبات خاص وعصري يردع مرتكبي هذه الجرائم، ونتيجة لتعطل المجلس التشريعي الفلسطيني عن أعماله وبخاصة إصدار التشريعات والقوانين، بقيت المحاكم الفلسطينية تطبق قانون العقوبات الأردني لسنة 1960 الساري المفعول وقانون رقم (3) لسنة 1996 بشأن الاتصالات السلكية واللاسلكية على الجرائم المعلوماتية والذي لا تكفي نصوصه لردع المجرم المعلوماتي. هذا الواقع دفع أصحاب العلاقة إعداد مسودة قانون الجرائم الإلكترونية الذي تم إقراره من قبل رئيس دولة فلسطين تحت عنوان قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية والذي أثار ويثير جدلاً قانونياً واسعاً من قبل أصحاب الاختصاص ومؤسسات المجتمع المدني حول بنوده وأحكامه وبخاصة عدم وجود اللائحة التفسيرية لهذا القرار بقانون.

تتمثل الإشكالية الرئيسية لهذه الدراسة في معرفة الوضع القانوني للجرائم الإلكترونية وتحدياتها في فلسطين، ويتفرع عنها الأسئلة التالية:

- ✓ ما هي الطبيعة الموضوعية للجريمة المعلوماتية؟
- ✓ ما دور الشرطة والنيابة العامة والقضاء في ملاحقة مرتكبيها؟
- ✓ ما دور المؤسسات في الوقاية والحد منها في فلسطين؟

فرضيات الدراسة

تقوم هذه الدراسة على الفرضيات التالية:

1. لا يوجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متغير (التعرض لجريمة الكترونية) والمتغيرات الديموغرافية (الجنس، مكان السكن، العمر، المستوى العلمي)، أي أن متغيرات مستقلة.

2. لا يوجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متغير (المعرفة عن القرار بقانون بشأن الجرائم الإلكترونية) والمتغيرات الديموغرافية (الجنس، مكان السكن، العمر، المستوى العلمي)، أي أن متغيرات مستقلة.

3. لا يوجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متغير (الاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية) والمتغيرات الديموغرافية (الجنس، مكان السكن، العمر، المستوى العلمي)، أي أن متغيرات مستقلة.

محددات الدراسة

ركزت هذه الدراسة في البحث عن الجرائم المعلوماتية في فلسطين من 2013 وحتى العام 2017، والتحديات التي تواجه المشرع والشرطة والنيابة العامة والقضاء الفلسطيني في مواجهتها، وفيما يتعلق بالدراسة التطبيقية فقد تمت ما بين الثامن عشر والرابع والعشرون من شهر آب من العام 2017.

منهج الدراسة

استخدم الباحث المنهج الوصفي والتحليل الكمي في الدراسة مع التركيز على النصوص القانونية والأحكام القضائية لتحقيق أهداف الدراسة وذلك من خلال دراسة البيانات الثانوية والأولية من خلال المقابلات مع جهاز الشرطة والنيابة العامة والقضاء وكذلك الاستبانة التي تم تصميمها

ونشرها على موقع جوجل فورم (Google Forms) وتعميمها على العديد من المواقع الإلكترونية في فلسطين بحيث أصبحت متاحة لكل فرد يمتلك المعرفة الفنية والإمكانية والرغبة للوصول إليها وتعبئتها.

صعوبات الدراسة

واجه الباحث العديد من الصعوبات تمثلت في ندرة الأبحاث والدراسات العلمية حول الجرائم الإلكترونية في فلسطين وخاصة المتعلقة بالقرار بقانون بشأن الجرائم الإلكترونية رقم 16 لسنة 2017، وكذلك غياب الإحصائيات حول الأحكام القضائية المتعلقة بالجرائم الإلكترونية، وصعوبة الوصول إلى المعلومات التفصيلية الخاصة بالجرائم المعلوماتية بسبب خصوصيتها وارتفاع درجة سريتها إلى جانب حداثة موضوع الجرائم الإلكترونية.

الدراسات السابقة

1. رسالة ماجستير بعنوان (المشكلات العلمية والقانونية للجرائم الإلكترونية "دراسة مقارنة")، عبد الله دغش العجمي، جامعة الشرق الأوسط: عمان/ المملكة الأردنية الهاشمية، 2014.

جاءت هذه الدراسة لبيان طبيعة المشكلات الموضوعية والإجرائية التي تثيرها الجرائم الإلكترونية على المستوى التشريعي والعملي ووضع الحلول التشريعية لمواجهتها، فالمرجع الأردني جرم وعاقب على ارتكاب الجرائم الإلكترونية بموجب قانون جرائم أنظمة المعلومات المؤقت رقم 30 لسنة 2010، بخلاف المشرع الكويتي الذي لم يسن قانوناً خاصاً بالجرائم الإلكترونية، ولا بإجراء أي تعديل على القوانين التي تعالج هذه الجرائم. خرج الباحث بعدد من النتائج ومن أهمها: إن القواعد التقليدية في التشريع الجزائي الكويتي غير كافية لمواجهة تلك الجرائم وما تثيره من إشكاليات، ويركز على المشرع الكويتي الإسراع بسن قانون خاص بالجرائم الإلكترونية لمواجهة تلك التحديات والمشكلات الموضوعية والإجرائية للجرائم الإلكترونية.

2.دراسة بعنوان "جرائم الكمبيوتر والإنترنت في التشريع الفلسطيني"، د. عبد الكريم خالد الشامي، ديوان الفتوى والتشريع: رام الله/ فلسطين، 2010.

تناول هذه الدراسة جرائم الكمبيوتر والإنترنت في التشريع الفلسطيني حيث تتطرق إلى مشروع قانون العقوبات الفلسطيني ومشروع قانون الإنترنت والمعلوماتية الفلسطيني. خلص الباحث إلى ضرورة الإسراع في إقرار وإصدار مشروعات القوانين المتعلقة بجرائم الكمبيوتر والإنترنت والمعلوماتية، وتعزيز التعاون الفلسطيني العربي الدولي المشترك لمكافحه هذه الجرائم.

3.رسالة دكتوراه بعنوان "السياسة الجنائية في مواجهة جرائم الإنترنت "دراسة مقارنة"، حسين بن سعيد الغافري، جامعة عين شمس: القاهرة/ جمهورية مصر العربية، 2009.

تناول الباحث الأحكام الموضوعية للجرائم المتعلقة بالإنترنت وهي جرائم القذف والسب، وجرائم الاعتداء على حرمة الحياة الخاصة والجرائم المخلة بالآداب العامة، وجرائم غسل الأموال وجرائم القرصنة وجرائم التجسس والتنصت على البيانات والمعلومات من خلال شبكة الإنترنت، وجريمة إتلاف وتدمير البيانات والمعطيات بواسطة شبكة الإنترنت، وتطرق إلى الجهود العربية والإقليمية والدولية في مواجهة جرائم الإنترنت. وخلص الباحث إلى عدة نتائج منها: وضع تشريع عربي موحد لمكافحة جرائم الإنترنت والحد منها نتيجة وجود فراغ قانوني لمواجهة لتلك الجرائم.

4.رسالة ماجستير بعنوان "الجرائم المعلوماتية"، الجامعة الأردنية، عمان/ المملكة الأردنية الهاشمية، نهلا المومني، 2010.

تعنى هذه الدراسة بتسليط الضوء على الجريمة المعلوماتية وتحديدًا جرائم الحاسوب والإنترنت باعتبارها جرائم حديثة، والبحث في مدى إمكانية انطباق النصوص التقليدية في قانون العقوبات الأردني على الجرائم المعلوماتية المستحدثة، حيث وجدت الباحثة عدة عقبات تحول دون تطبيق النصوص التقليدية على الجرائم المعلوماتية باعتبار نصوص قانون العقوبات وضعت ابتداءً لحماية الأموال المادية ذات الكيان المادي الملموس ولم توضع لحماية الأموال المعنوية

كالملومات، وان مبدأ شرعية الجرائم والعقوبات (لا جريمة ولا عقوبة إلا بنص صريح) الذي لا يجيز التوسع في قياس النصوص الجزائية وبالتالي يشكل عائقاً أمام إمكانية إدراج الجرائم المعلوماتية ضمن النصوص التقليدية في قانون العقوبات الأردني. وقد توصلت الباحثة إلى عدة توصيات منها: ضرورة تدخل المشرع الجزائي الأردني من أجل تعديل واستحداث النصوص الجزائية حتى تكفل الحماية الجزائية المعلوماتية، وإلى ضرورة تأهيل جهات الشرطة والادعاء العام والقضاء من أجل القدرة على التعامل مع هذه الجرائم، وضرورة التعاون الدولي من أجل مواجهة تلك الجرائم للحد منها ومكافحتها.

5. رسالة دكتوراه بعنوان "جرائم نظم المعلومات" دراسة مقارنة"، أيمن عبد الله فكرى، جامعة المنصورة: المنصورة/ جمهورية مصر العربية، 2007.

هدف البحث إلى دراسة الطرق المختلفة لمواجهة جرائم نظم المعلومات من خلال دراسة الوضع الحالي في التشريع الجنائي المصري وملاءمة تلك التشريعات والقوانين في مواجهة تلك الجرائم، وتناول فيها أحكام عامة في جرائم نظم المعلومات، وتطرق إلى تقسيمات جرائم نظم المعلومات (التقسيم الفقهي، تقسيم Ulrich Sieber، تقسيم Martin Vasik، التقسيم الأمريكي، والجهود الأوروبية في تقسيم جرائم نظم المعلومات)، وتحدث عن الحماية الجنائية للخصوصية المعلوماتية في التشريعات المقارنة (فرنسي، أمريكي، وبعض التشريعات العربية) وخلص إلى نتيجة: مراجعة القوانين القائمة في التشريع المصري لتعديل بعض نصوصها وإصدار قانون خاص بالجرائم المعلوماتية، وإنشاء جهات قانونياً مختصة "قانونياً وتقنياً" في تطبيقه.

ركزت الدراسات السابقة في بحث وتحليل الأحكام العامة "الموضوعية والإجرائية" للجرائم المعلوماتية باعتبارها جرائم مستحدثة، وعن مدى إمكانية تطبيق النصوص التقليدية عليها، وتناولت العديد من الإجراءات الواجب على الدول اتباعها للوقاية والحد من هذه الجرائم أهمها مراجعة واستحداث القوانين الجزائية القائمة والإسراع في سن قوانين جديد لمكافحة جرائم تقنية المعلومات.

وتتميز هذه الدراسة في تحليل التحديات القانونية التي تواجه المؤسسة الأمنية والقضائية في أداء مهامها في ملاحقة ومتابعة مرتكبي الجرائم المعلوماتية والحد منها، وتبيان الواقع القانوني للجرائم الإلكترونية قبل وبعد إصدار القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، ومدى انتشارها وخطورتها، والمساهمة في نشر الوعي والثقافة القانونية بين أفراد المجتمع الفلسطيني حول تلك الجرائم. ومن أجل الإجابة على تساؤلات الدراسة تم استخدام استبانة لاستطلاع رأي الشارع الفلسطيني بهذا الخصوص وتحليلها كمياً.

الفصل الأول

ماهية الجريمة المعلوماتية

تعتبر الجرائم المعلوماتية جرائم مستحدثة، لارتباطها بالتطور والنقد التكنولوجي الحديث، حيث كان هنالك اتجاهات متعددة في تعريفها، كما أنها تتميز عن الجرائم الأخرى بمجموعة من الخصائص، وجاءت بنمط جديد من المجرمين يطلق عليهم بمصطلح (مجرمي المعلوماتية)¹. قسم هذا الفصل إلى مبحثين: تناول المبحث الأول مفهومها، وأهم الخصائص التي تميزها عن غيرها من الجرائم، بالإضافة إلى تقسيمات نظم جرائم المعلومات، ويتضمن المبحث الثاني أركانها (الركن المادي، الركن المعنوي)، وأطرافها (الفاعل والمجني عليه)، والمسؤولية الجزائية لمرتكبيها.

المبحث الأول: مفهوم الجريمة المعلوماتية

أحدث التطور الهائل والمتسارع في مجال صناعة الحاسوب واستخدام برامجه ظهور أنواع وأساليب متعددة لارتكاب الجرائم المعلوماتية، ونظراً لطبيعة هذه الجرائم وصعوبة اكتشافها، يصعب تقدير حجم الخسائر الناجمة عنها، وتكتسب دراسة الجرائم المعلوماتية أهمية خاصة حيث أصبحت المجتمعات تعتمد اعتماداً رئيسياً على الحاسب الآلي والبرامج المحوسبة والمعلومات، وإيجاد الأساليب المتقدمة في مجال مكافحتها والتصدي لها².

ظهر في الستينات مصطلح أمن الحواسيب (Computers Security) من أجل حماية الحاسوب ذاته ومنع الاعتداء عليه³، في حين تركز الاهتمام في السبعينيات على أمن البيانات (Data Security) وذلك باستخدام كلمة سر (Password) خاصة بالمستخدم من أجل حمايتها وعدم السماح للغير بالاطلاع عليها، وفي الثمانينات والتسعينات، تحولت إلى حماية المعلومات ويطلق عليها مرحلة أمن المعلومات (Information Security)، وعرفت الشركة الأمريكية

¹ المومني، عبد القادر نهلا: مرجع سابق، ص45.

² العجمي، عبد الله دغش: مرجع سابق، ص1.

³ الصغير، جميل عبد الباقي: الجرائم الناشئة عن استخدام الحاسب الآلي، الكتاب الأول، دار النهضة العربية، الطبعة الأولى، 1992. ص26.

أي بي أم (IBM) أمن المعلومات بأنها "حماية البيانات من حوادث التحوير أو التدمير أو كشف المعلومات بدون تخويل"¹ ومع دخول الألفية الثالثة يدور الحديث عن أمن المعرفة (Knowledge Security)² نتيجة الانتشار الواسع للحواسيب وتبادل المعلومات السريع وتطور الحاسبات الآلية الجيل السادس. لذلك يتناول هذا المبحث تعريف الجريمة المعلوماتية في المطلب الأول، وخصائصها في المطلب الثاني، وتقسيماتها في المطلب الثالث.

المطلب الأول: تعريف الجريمة المعلوماتية

تشمل الجرائم المعلوماتية الجرائم التي يقع الاعتداء فيها على مكونات الحاسب الآلي والجرائم التي يكون فيها الحاسب الآلي موضوعاً للجريمة. وتختلف هذه المفاهيم باختلاف المعايير فمنها تقوم على معيار وسيلة ارتكابها أو موضوع الجريمة ومحلها أو معرفة فاعلها بالتقنيات التكنولوجية أو معايير متعددة بحيث تبرز موضوع الجريمة وأشكالها والعناصر التي تتصل بوسائل ارتكابها أو بيئة ارتكابها أو صفات مرتكبها³. ويمكن تصنيفها في أربعة اتجاهات فقهية هي:

الاتجاه الأول: وفقاً لوسيلة ارتكاب الجريمة

يعتمد مؤيدو هذا الاتجاه في تعريفهم للجرائم المعلوماتية إلى وسيلة ارتكاب الجريمة، فيشترط ارتكابها بواسطة الحاسب الآلي. ويعرفها (Tiedemann) بأنها "كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي"⁴، وعرفها توم فور يستر في كتابه قصة ثورة تقنية المعلومات بأنها "فعل إجرامي يتم باستخدام الحاسوب كأداة رئيسية"⁵.

¹ البياتي، هلال عبود: الوسائل الفنية لحماية البرامج ودور التشريعات في حماية المعلومات، بحث منشور في مجلة أبحاث الحاسوب، المجلد الأول، العدد 1، تصدر عن الأمانة العامة لاتحاد مجالس البحث العلمي العربي، 1996. ص 37.

² عابنة، محمود أحمد: جرائم الحاسوب وأبعادها الدولية، عمان، دار الثقافة، 2009. ص 13.

³ فكرى، أيمن عبد الله: جرائم نظم المعلومات - دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2007. ص 83.

⁴ رستم، هشام محمد: ورقة عمل بعنوان جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة، مجلة الدراسات القانونية، تصدرها كلية الحقوق بجامعة أسيوط، العدد السابع عشر، 1995. ص 110.

⁵ فوريستر، توم: قصة ثورة تقنية المعلومات، الطبعة الأولى، ترجمة ونشر مركز الكتب الأردني، عمان، 1989. ص 399.

تبين من التعريفات السابقة أنها اشترطت ارتباط السلوك غير المشروع باستخدام الحاسب الآلي لاعتبارها جرائم معلوماتية. ومع عدم إنكار أهمية دور الحاسب الآلي في ارتكابها إلا أن الاستناد في التعريف إلى وسيلة ارتكاب الجريمة تعرض إلى العديد من الانتقادات الفقهية، لأن القانون الجنائي يهتم بالفعل أو النشاط غير المشروع الذي يقوم به الجاني ولا يهتم بوسيلة ارتكاب الجريمة، بالإضافة إلى بناء هذا التعريف على معيار واحد الذي لم يكن محل اعتبار لدى المشرع الجزائي عند التجريم وإنما التكيف القانوني للجريمة وتوافر أركانها هي محل اعتبار عند تطبيق النص القانوني.

الاتجاه الثاني: وفقاً لمحل أو موضوع الجريمة

يستند هذا الاتجاه في تعريفها إلى وجوب أن يكون الحاسب الآلي هو محل الجريمة، فيشترط الاعتداء على الحاسب أو على نظامه. ويمثل هذا الاتجاه روزنبلات Rosenblatt الذي عرفها بأنها "نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو الوصول أو التي تحول عن طريقه"¹ وتعرض هذا التعريف إلى الانتقاد حيث اعتبر بدايةً أن جرائم الحاسب الآلي من الجرائم المحصورة ضمن نشاط معين يتفق مع مبدأ الشرعية الجنائية، إلا أنه توسع في النشاط غير المشروع المتعلق بالمعلومات عبر الحاسب وترك مجالاً واسعاً للاجتهاد والتفسير وهذا يتعارض مع مبدأ المشروعية في تحديد السلوك الإجرامي، بالإضافة إلى تبني معيار موضوعي أدى إلى ظهور مفاهيم عامة لا تحدد الأفعال المرتبطة بجرائم الحاسوب بشكل دقيق.

وعرفت قشوق بأنها "كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقلها" وعرفها خبراء منظمة التعاون الاقتصادي والتنمية بأنها "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و / أو نقلها"² فهذه الجرائم تقع على الحاسب الآلي وبرامجه ومكوناته. من وصف هذين التعريفين بالعمومية

¹ يونس، عرب: دليل أمن المعلومات والخصوصية، الجزء الأول، جرائم الكمبيوتر والإنترنت ، ط1 ، اتحاد المصارف العربية، 2002، ص213.

² قشوق، هدى حامد: جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، 1992، ص5.

والشمولية والمرونة إلا أنه يوسع نطاق التجريم إلى الأفعال الأخلاقية التي تخرج عن التجريم وفقاً للقوانين الجنائية. وتتبنى هذا المفهوم الألماني Ulrich Sieber، الذي يعتمد على وصف السلوك واتصاله بالمعالجة الآلي للبيانات أو نقلها.

الاتجاه الثالث: وفقاً لوجوب معرفة الفاعل بتقنية المعلومات

يستند أنصار هذا الاتجاه إلى معيار شخصي متعلق بالفاعل، بأن يكون فاعل هذه الجرائم على الإلمام والدراية والمعرفة بتقنية المعلومات واستخدام الحاسوب لاعتبارها جرائم معلومات. وعرفها ديفيد تومبسون David Thompson بأنها " أي جريمة يكون متطلباً لاعترافها أن تتوافر لدى فاعلها معرفة تقنية بالحاسب الآلي"، وكذلك ستين سكيولبيرج Stein Schiolberg الذي عرف جرائم الحاسب بأنها " أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه والتحقيق فيه وملاحقته قضائياً". وقد عرفت وزارة العدل الأمريكية ضمن دراسة أجرتها عام 1979 بأنها " أي جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها"¹

حددت هذه المفاهيم وحصرت الجريمة المعلوماتية في الحالات التي تتطلب فيها معرفة الفاعل بالتقنية المعلوماتية وقت ارتكابها، ولم يبين طبيعة الأفعال غير المشروعة مما يتطلب البحث في الظروف الخاصة بالجاني، وإن تقنية الحاسب الآلي هي جوهر ومحور السلوك الإجرامي.

الاتجاه الرابع: وفقاً لمعايير متعددة

يتبنى هذا الاتجاه تعريفات متعددة تُبنى على أكثر من معيار ومن ضمنها، تعريف منظمة التعاون الاقتصادي والتنمية (OCDE) حول الغش المعلوماتي عام 1982، حيث تم تعريف الجريمة المعلوماتية بأنها " كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية، يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"² يعد هذا

¹ رستم، هشام: الجرائم المعلوماتية أصول التحقيق الجنائي التقني، مجلة الأمن والقانون، دبي، كلية الشرطة، 1999. ص110.

² الشوا، سامي محمد: ثورة المعلومات وانعكاساتها على قانون العقوبات، ط2، دار النهضة العربية، القاهرة، 1994. ص32.

التعريف واسع وشامل يحيط بظاهرة الجرائم المعلوماتية، ويعبر عن الطابع التقني مع إمكانية التعامل مع التطورات التقنية الحديثة. وايد الفقه المصري هذا التعريف لاستبعاده أشكال التجريم التي يكون دور الحاسب الآلي فيها ثانوياً أو عارضاً، وانتقد هذا التعريف نتيجة إدراجه الأموال المادية لأن هذه الأموال لا تحتاج إلى قانون جديد، وإنما يمكن حمايتها بموجب قوانين العقوبات التقليدية.

وعرفها الفرنسي ماس (Mass) بأنها " الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلومات التقنية بعرض تحقيق ربح"، وبتعريف الخبير الأمريكي دون باركر Done.B.Barke أنها " أي فعل إجرامي أياً كانت صلاته بتقنية المعلومات، يلحق بالمجني عليه خسارة أو ربحاً يحققه الفاعل"¹. ويتبن من التعريفين السابقين ربطهما بين الجريمة وغايتها من أجل وقوعها، فجعل استخدام الحاسب الآلي فيها وسيلة رئيسية لارتكابها، بالإضافة إلى إظهار غاية الفاعل لتحقيق مكاسبه، ويؤدي هذا الربط بتحقيق الشروع أو وجود خسارة إلى توسيع نطاق العقاب.

حاولت هذه الاتجاهات تحديد مفهوم الجرائم المعلوماتية من خلال موضوع الجريمة ووسيلة ارتكابها وصفات مرتكبها، إلا أنه من الصعوبة وضع تعريفاً محدداً نتيجة التطور والتقدم التكنولوجي المتسارع الذي أدى إلى ظهور أشكال جديدة من هذه الجرائم، وتتنوع واختلاف وسائل ارتكابها، وخشية من حصر نطاق التجريم في إطار أفعال معينة، وكذلك صعوبة حصر الطبيعة التقنية لجرائم المعلومات في إطار قانوني واحد، ولوجود بعد دولي للجريمة المعلوماتية، وهذا المنهج اتبعه المشرع الأردني في قانون الجرائم الإلكترونية رقم 27 لسنة 2015 وكذلك المشرع الإماراتي في القانون رقم 5 لسنة 2012 وتعديلاته في شأن جرائم تقنية المعلومات، مما يستوجب صياغتها في مفهوم شامل ومتفق عليه. وخلق القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية من تحديد مفهومها مما قد يتطلب تعديل نص المادة الأولى بإضافة تعريف جامع لها لتحديد عناصرها الرئيسية.

¹ المومني، نهلا عبد القادر: الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الثانية، عمان، 2008. ص48.

تأسياً على ما تقدم يمكن تعريف الجريمة المعلوماتية بأنها: "أي فعل غير مشروع يقوم به الجاني بواسطة الحاسب الآلي أو الشبكة المعلوماتية وأنظمة المعلومات أو أية وسيلة تقنية، ويلحق ضرراً بالمجني عليه مع توافر المعرفة التقنية لدى الفاعل"

ويرجع السبب في اختيار هذا التعريف لأنه يستند على تحديد معالم الجريمة المعلوماتية وعناصرها الأساسية، التي تشتمل على صورتين جريمة ارتكبت بواسطة الوسائل الإلكترونية مثل الدم والقذح عبر الإنترنت، وجريمة محلها أنظمة تقنية المعلومات بما فيها المعلومات وبرامج وبيانات، وشمل على طبيعة السلوك ومحل الاعتداء وارتباط السلوك بموضوع الاعتداء بواسطة استخدام تقنية المعلومات.

المطلب الثاني: خصائص الجريمة المعلوماتية

تتميز الجرائم المعلوماتية بمجموعة من الخصائص تتمثل في كونها عابرة للحدود، صعوبة الإثبات، سهولة الارتكاب، مغرية لمرتكبيها، وترتكب بواسطة أكثر من شخص.

الفرع الأول: جرائم عابرة للحدود والدول

أحدث التقدم التكنولوجي والمعلوماتي في العصر الحديث، ظهوراً شبكات معلومات لا تعترف بالحدود الجغرافية والسياسية بين الدول، حيث أصبح من السهولة تبادل المعلومات بين أنظمة متعددة في دول مختلفة، ومع انتشار الشبكة المعلوماتية (الإنترنت)، أصبحت بيئة خصبة لارتكابها، "وغالباً ترتكب هذه الجريمة في دولة معينة، والمجني عليه في دولة أخرى، وقد يكون الضرر الناتج عنها في مكان آخر"¹، وبناء على ذلك أصبحت الجرائم المعلوماتية نمطاً جديداً من الجرائم العابرة للحدود والدول. وتثير العديد من الإشكاليات تكمن في تحديد الدولة صاحبة الاختصاص القضائي بهذه الجرائم، وتحديد القانون الواجب التطبيق، بالإضافة إلى إجراءات الملاحقة القضائية. وهذا يتطلب التعاون الدولي والتنسيق بين الدول كإبرام المعاهدات

¹ الشوا، سامي: جرائم الحاسب الآلي والجرائم الأخرى المرتبطة بوسائل الاتصال الحديثة، ترجمة سامي الشوا، 1993.

والاتفاقيات الدولية، سن قوانين داخلية ملائمة من أجل مواجهة مكافحة مجرمو المعلوماتية وتقديمهم للعدالة، وحماية المجتمع المحلي والدولي من نتائج وأثار هذه الجرائم¹.

من الأمثلة على الجرائم عابرة للحدود وذات بعد دولي، قضية مرض نقص المناعة (الإيدز) عام 1989 وتتلخص وقائع هذه القضية قيام أحد الأشخاص بتوزيع ونشر عدد كبير من النسخ الخاصة بأحد البرامج الذي هدف في ظاهره إلى إعطاء بعض النصائح الخاصة بهذا المرض، إلا أن حقيقة هذا البرنامج يحتوي على فيروس حصان طروادة، يترتب على تشغيله تعطيل جهاز الحاسوب ثم تظهر عبارة على الشاشة يطلب فيها الفاعل إرسال مبلغ مالي على عنوان معين من أجل حصول المجني عليه مضاد فايروسات².

الفرع الثاني: جرائم صعبة الإثبات والاكتشاف

تتميز هذه الجرائم بصعوبة اكتشافها وإثباتها نتيجة عدم تركها لأي أثر خارجي ملموس التي تمكن الجاني من ارتكابها في دول مختلفة، وقدرة الجاني على تدمير الدليل وإخفاءه بسهولة في أقل من ثانية. كمسح البرامج أو وضع رموز وكلمات سرية لتشفير المعلومات والبيانات، مما يصعب على أجهزة التحقيق والملاحقة في الوصول إلى الدليل الرقمي لإدانة المجرم المعلوماتي³، حيث تشير الدراسات إن ما يتم اكتشافه من جرائم المعلومات يصل إلى نسبة 1% والذي يتم الإبلاغ عنه من هذه النسبة لا يكاد يصل إلى 5% فقط. ويشكل حرص المؤسسات والجهات التي تتعرض لتلك الجرائم عدم إبلاغ السلطات المختصة أو الكشف عنها خوفاً من هز كيانه وتفتتها، وتقتصر على اتخاذ إجراءات إدارية داخلية من أجل المحافظة على سمعتها ومكانتها⁴.

¹ د. Ulrich Sieber، جرائم الكمبيوتر والجرائم الأخرى في مجال المعلومات، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي (ترجمة سامي الشوا)، دار النهضة العربية، القاهرة، 1993، ص 58.

² قوره، نائلة: جرائم الحاسب الآلي الاقتصادية، دار النهضة العربية، القاهرة، 2004، ص 48.

³ الصغير، جميل عبد الباقي: مرجع سابق، ص 17.

⁴ القطاونة، مصعب: الإجراءات الجنائية الخاصة في الجرائم المعلوماتية، بحث مقدم لشبكة قانوني الأردن، 2010.

لا تساعد الوسائل والمعاينة التقليدية على إثبات هذه الجرائم نظراً لاختلاف طبيعتها عن الجريمة التقليدية، فالجريمة التقليدية تنتج آثار مادية تكشف عن الجريمة، أما الجرائم المعلوماتية فيصعب تحديد الأثر المادي واكتشافه، ويحتاج إلى فترة زمنية طويلة، مما يمنح الجاني فرصة تغير أو إتلاف الأثر المادي فيصيب الشك في الأدلة الناتجة عن معاينتها¹. كما تم توضيحه سابقاً.

الفرع الثالث: سهولة الارتكاب

تمتاز هذه الجرائم عن غيرها من الجرائم التقليدية باعتبارها جرائم هادئة بطبيعتها (Soft Crime) وبسهولة ارتكابها، أي أنها لا تحتاج إلى أي وقت أو ممارسة العنف أو أي مجهود عضلي، كما هو الحال في الجرائم التقليدية كالقتل أو الكسر والخلع في جرائم السرقة. بل يشترط لارتكابها توافر الحاسب الآلي وشبكة المعلومات (الإنترنت)، ومعرفة الفاعل بتقنية المعلومات والوسيلة المناسبة لارتكاب الجريمة، وتعزيز معرفته وقدراته في التعامل مع هذه الشبكة وبرامجها، للقيام بجرائم مختلفة كاختراق خصوصيات الغير والتجسس والتحويل الإلكتروني غير المشروع².

الفرع الرابع: جرائم مغرية للمجرمين

تعتبر الجرائم المعلوماتية جرائم مغرية للمجرمين لسرعة تنفيذها ومع إمكانية تنفيذها عن بُعد دون الحاجة للتواجد في مسرح الجريمة، ولضخامة المكاسب المادية والمعنوية التي قد يحققها الجاني من ارتكابه لهذه الجرائم، وترجع أسباب ذلك نتيجة لاستغلال التقدم التكنولوجي الحديث، وغياب النصوص العقابية القانونية الرادعة، مما أدى إلى ظهور أشكال وأنماط جديدة لهذه الجرائم³.

¹ المومني، عبد القادر نهلا: مرجع سابق، ص 56.

² الزعبي، وآخرون: جرائم تقنية نظم المعلومات الإلكترونية - دراسة مقارنة، دار الثقافة، عمان، الطبعة الثانية، 2014. ص 97.

³ إبراهيم، خالد ممدوح: الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط1، 2009. ص 78.

الفرع الخامس: جرائم ترتكب عادةً بتعاون أكثر من شخص

تتميز الجرائم المعلوماتية بتعاون أكثر من شخص على ارتكابها، ومن يقوم بإخراج الجريمة إلى حيز الوجود الخارجي، غالباً أشخاص متخصصون فنياً في مجال تقنية المعلومات والإنترنت لتشكيل النشاط الجرمي، وبالتعاون مع شخص آخر من حوله أو من خارج مكان عمل المجني عليها لتغطية وإخفاء عمليات التحويل والتلاعب. ويعد إخراج هذه الجريمة إلى الوجود الخارجي عملاً سلبياً، لأنه يدل على من يعلم بوقوع الجريمة تسهياً لإتمامها، وقد يكون تدخلاً إيجابياً يتمثل في تقديم مساعدة فنية أو مادية¹.

كما تتميز بأنها تقع أثناء عملية معالجة البيانات سواءً عند مرحلة إدخال البيانات أو معالجتها أو إخراجها، بالإضافة إلى المعطيات الخاصة بالحاسب الآلي، وفي حال تخلف هذا الشرط تنتفي هذه الجريمة ولا يمكن البحث في قيام أركانها. والى خطورتها على حياة الأشخاص والمؤسسات الاقتصادية والأمنية والسياسية².

تثير هذه الجرائم احتمالية تعدد الوصف القانوني لمحلها، يظهر محلها على شكل مادي وتكون عبارة عن معلومات مخزنة على الدعائم الإلكترونية، وعلى صورة غير مادية (معنوية) للمعلومات التي تنتقل أو موجودة فعلاً على النظام المعلوماتي، وسواءً كانت على شكل مادي أو غير مادي، فإنها تخضع لأكثر من نص قانوني، في حال اعتبارها مصنفاً أدبية تثير تعدد الأوصاف القانونية على نفس المحل³.

المطلب الثالث: تقسيمات الجرائم المعلوماتية

تختلف وجهات النظر الفقهية والقانونية حول تصنيفها، فهناك العديد من الجهود الدولية والإقليمية التي ساهمت وأبرزت في مجال تقسيم هذه الجرائم من أجل تعزيز التعاون الدولي في مكافحة هذه الجرائم والعمل على توحيد القواعد الموضوعية والإجرائية وتوحيد القوانين الجنائية

¹ الشوا، سامي: ثورة المعلومات وانعكاساتها على قانون العقوبات، القاهرة، دار النهضة العربية، 1994. ص 46.

² أبراهيم، خالد ممدوح، مرجع سابق: ص 86 – 88.

³ العجمي، عبدالله دغش: مرجع سابق، ص 25.

لمكافحتها باعتبارها جرائم عابرة للحدود فيقع السلوك في دولة وقد تقع نتائجه في دولة أخرى، ومن هذه التصنيفات تصنيفها وفق منظمة التعاون الاقتصادي والتنمية، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، والاتفاقية الدولية لمكافحة الجريمة المعلوماتية بودابست لسنة 2001، والتقسيم الأوروبي، والفرنسي والأمريكي.

الفرع الأول: تصنيف الجرائم المعلوماتية وفق منظمة التعاون الاقتصادي والتنمية

اهتمت هذه المنظمة بالجريمة المعلوماتية من خلال إقامة العديد من المؤتمرات والاجتماعات المتعلقة بمشاكل هذه الجرائم من النواحي الاقتصادية منذ عام 1977، من خلال حماية الخصوصية من التهديد المعلوماتي لها، واشتملت على قواعد وتوصيات استرشادية للدول الأعضاء في تشريعاتها الداخلية فيما يتعلق بحماية البيانات ذات الطبيعة الشخصية، وفرضت عقوبات في حال مخالفة هذه القواعد، ومن هذه القواعد تحديد غرض جمع البيانات والمعلومات واستخدامها لهذا الغرض، حق الأفراد في الوصول إلى البيانات والمعلومات الخاصة بهم وتعديلها، ومساءلة ومحاسبة الأشخاص المكلف في التعامل مع البيانات الشخصية¹. وفي عام 1985 شكلت لجنة لدراسة الجريمة المعلوماتية لدى الدول الأعضاء بالمنظمة، حيث أصدرت هذه اللجنة تقريرها عام 1986 بعنوان جرائم الحاسب الآلي، أوصت فيه بضرورة مواجهة المشكلات الناجمة عن الجريمة المعلوماتية في قوانينها الداخلية²، وبينت الأفعال التي تعتبر جرائم معلوماتية وهي:

- إدخال معلومات إلى نظام الحاسب الآلي أو تعديل أو محو معلومات موجودة بشكل غير مشروع، وذلك بنية تحويل الأموال أو الممتلكات التي تمثلها المعلومات.

¹ فكري، أيمن عبد الله: مرجع سابق، ص 126.

² كانت الدول المشاركة في الاجتماعات هي النمسا، بلجيكا، كندا، فلندا، فرنسا، ألمانيا، إيطاليا، السويد، سويسرا، إنجلترا، أمريكا.

- إدخال معلومات إلى نظام الحاسب الآلي أو شبكة المعلومات أو تعديل أو محو معلومات موجودة فعلياً أو اعتراض النظام المعلوماتي بهدف إعاقة ومنع صاحبه من أداء وظيفته ومنفعته.

- الاستغلال التجاري لبرامج الحاسب الآلي، كالحصول غير المشروع على المعلومات وبيعها بالأسواق لتشكل انتهاكاً لحقوق مالكيها.

- الدخول أو الاعتراض غير المصرح به لنظام الحاسب الآلي بشكل عمدي من أجل ارتكاب جريمة أو تمهيداً لها أو لارتكاب جريمة أخرى.

- الاستعمال غير المشروع لنظام الحاسب الآلي.

أن منظمة التعاون الاقتصادي والتنمية اتجهت للاهتمام بحماية أنظمة الحاسب الآلي وشبكات المعلومات، وأصدرت العديد من التوصيات والإجراءات الأمنية من أجل حماية المعلومات والمشكلات الناتجة عن هذه الجرائم في القوانين الداخلية للدول الأعضاء¹.

الفرع الثاني: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

أبرمت هذه الاتفاقية من أجل تعزيز وتدعيم التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات لدرء أخطارها وحفاظاً على أمن ومصالح دولها وسلامة مجتمعاتها وأفرادها²، وتضمنت العديد من المصطلحات وحالات تطبيقها، وإلزام الدول الأعضاء بتطبيق أحكامها بما لا يتعارض مع سيادة الدول³.

¹ قوره، نائلة: مرجع سابق، ص 255 - ص 257.

² حررت هذه الاتفاقية باللغة العربية بمدينة القاهرة في 15/1/1432 هجري الموافق 21/12/2010 من أصل واحد مودع بالأمانة العامة لجامعة الدول العربية (الأمانة الفنية لمجلس وزراء العدل العرب)، ونسخة مطابقة للأصل تسلم للأمانة العامة لمجلس وزراء الداخلية العرب، وتسلم كذلك نسخة مطابقة للأصل لكل دولة من الدول الأطراف. وتسري هذه الاتفاقية بعد مضي ثلاثين يوماً من تاريخ إيداع وثائق التصديق عليها أو قبولها أو إقرارها من سبع دول عربية وهي (الأردن، الإمارات العربية المتحدة، السودان، فلسطين، قطر، الكويت) بموجب الفقرة (3) من الأحكام الختامية للاتفاقية.

الأمانة العامة لجامعة الدول العربية - إدارة الشؤون القانونية - الشبكة القانونية العربية www.arablegalnet.org

³ المواد 2 و3 و4 من الاتفاقية المشار إليها.

صنفت هذه الاتفاقية في الفصل الثاني منها الأفعال التي تعد جرائم معلوماتية، وألزمت الدول الأعضاء على تجريمها في تشريعاتها وأنظمتها الداخلية ومن هذه الأفعال:

- جرائم الدخول والاعتراض غير المشروع للمعلومات والاعتداء على سلامة البيانات وإساءة استخدام الوسائل التقنية¹.

- الجرائم المتعلقة بتقنية أنظمة المعلومات: التزوير، الاحتيال، الجرائم الإباحية والجرائم المرتبطة بها كالمقامرة والاستغلال الجنسي، الاعتداء على حرمة الحياة الخاصة، والجرائم المنظمة والإرهاب المرتكب بواسطة تقنية المعلومات، والجرائم المتعلقة بانتهاك حق المؤلف والاستخدام غير المشروع لأدوات الدفع الإلكترونية².

كما أشارت هذه الاتفاقية في المواد 18 - 21 إلى الشروع والاشتراك في الجرائم التقنية، والمسؤولية الجزائية للأشخاص الطبيعية والمعنوية، والتدابير والعقوبات الجنائية والمالية، بالإضافة إلى حالات تشديد العقوبات على مرتكبي الجرائم التقليدية بواسطة تقنية أنظمة المعلومات³، وبين الفصل الثالث من ذات الاتفاقية الأحكام الإجرائية التي يجب أن تتبناها الدول الأعضاء لتحديد الصلاحيات والإجراءات في تشريعاتها وأنظمتها الداخلية وهي التحفظ العاجل على البيانات المخزنة في أنظمة المعلومات وجمعها والكشف عنها جزئياً وتفتيشها وضبطها واعتراضها وتسليمها⁴. واحتوى الفصل الرابع على إجراءات التعاون القانوني والقضائي كتسليم المجرمين وتبادل المعلومات وتتبع المستخدمين والوصول إلى المعلومات عبر الحدود⁵.

¹ المواد 5 - 9 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

² المواد 10 - 18 من الاتفاقية المشار إليها.

³ المواد 18 - 21 من الاتفاقية المشار إليها.

⁴ المواد 22 - 29 من الاتفاقية المشار إليها.

⁵ المواد 30 - 43 من الاتفاقية المشار إليها.

يلاحظ بأن هذه الاتفاقية لم تحدد مفهوم الجريمة المعلوماتية، ولم تجرم كافة أنواع المساهمة الجنائية مما يتطلب إعادة صياغة هذه النصوص لتشمل مفهومها وكافة أنواع المساهمة الجرمية وكافة صور الشروع في الجريمة ويشمل كافة الأعمال التحضيرية لهذا الجرائم.

الفرع الثالث: الاتفاقية الدولية لمكافحة الجريمة المعلوماتية بودابست 2001

وقعت هذه الاتفاقية عام 2001 من قبل 26 دولة، لمواجهة خطورة الجرائم المعلوماتية في ظل مجتمع المعرفة وثورة المعلومات، وتعد هذه أول معاهدة دولية في مجال مكافحة الجرائم المعلوماتية ناتجة عن التعاون الدولي والقانوني بين الدول¹، واستندت على الميثاق الدولي لحماية الحقوق المدنية والسياسية عام 1966، ومعاهدة التعاون الدولي في مجال مكافحة الجرائم المعلوماتية الصادرة عن الأمم المتحدة، ومنظمة التعاون الاقتصادي والتنمية OECD ومجموعة G8 والتوصية الأوروبية رقم 10/85، والتوصية رقم 2/88، و9/89 و13/95². تضمنت هذه الاتفاقية 48 مادة ووزعت جرائم نظم المعلومات إلى أربعة أقسام كما يلي³:

1. جرائم ضد السرية وسلامة البيانات والنظام المعلوماتي وتشمل الدخول غير المشروع عليها الاعتراض غير القانوني، الاعتداء على سلامة البيانات والنظام، وإساءة استخدام الحاسب الآلي.
2. الجرائم المعلوماتية المتعلقة بالحاسب الآلي وتضم الغش المعلوماتي والاحتيال المعلوماتي.

¹ فكري، أيمن عبدالله: مرجع سابق، ص 129.

² إن هذه الاتفاقية تنطلق من أحكام اتفاقية مجلس أوربا لعام ١٩٨١ بشأن الحماية من مخاطر المعالجة الآلية للبيانات الشخصية، ومن اتفاقية الأمم المتحدة لعام 1989 بشأن حقوق الطفل واتفاقية منظمة العمل الدولية لعام 1999 بشأن عمالة الأطفال، وتنطلق أيضاً من جهود دولية وإقليمية وتحديداً أنشطة الأمم المتحدة ومنظمة التعاون الاقتصادي والتنمية (OECD) والاتحاد الأوروبي ومجموعة الدول الصناعية، كما تعتمد الاتفاقية على ما تم إقراره من أدلة إرشادية وتوصيات تشريعية منذ عام ١٩٨٥ وتوصيات عام ١٩٨٨ بشأن القرصنة والحقوق المجاورة وتوجيهات عام 1995 المتعلقة بمشكلات القانون الإجرائي المتصلة بتقنيات المعلومات، انظر إلى غايب، محروس نصار: الجريمة المعلوماتية، المعهد التقني، الأنبار، 2011/5/3، ص 20. وصادقت عليها فلسطين بموجب مرسوم رئاسي رقم 9 لسنة 2011 الصادر عن رئيس دولة فلسطين بتاريخ 2011/6/27.

³ الزعبي، وآخرون: مرجع سابق، ص 97 - ص 98.

3. الجرائم المتعلقة بالمحتوى وتشمل جميع الجرائم الإباحية والجنسية والجرائم المخلة بالآداب العامة والأخلاق.

4. الجرائم المتعلقة بحقوق الملكية الفكرية وتشمل كافة الاعتداءات على الملكية الفكرية، كالاغتداء على حق المؤلف وقرصنة البرامج.

أكدت هذه الاتفاقية على عناصر أساسية ثلاثة وهي: اتخاذ تدابير تشريعية موضوعية "نصوص التجريم" لمكافحة الجرائم المعلوماتية والحد من مخاطرها، وفرض قواعد إجرائية ملائمة في البحث والتحري والتحقيق والضبط والمحاكمة حول هذه الجرائم، وركزت على أهمية التعاون الدولي في مكافحة الجرائم المعلوماتية¹.

الفرع الرابع: التقسيم الخاص بالمجلس الأوروبي

اهتم المجلس الأوروبي بالمعلومات ومشكلاتها في بداية السبعينيات من القرن الماضي من خلال حماية البيانات الشخصية من الاعتداءات عليها، ووقع على اتفاقية خاصة بحماية إساءة استخدام البيانات المعالجة إلكترونياً في عام 1981، وبدأ الاهتمام بالجريمة المعلوماتية في المؤتمر الثاني عشر لرؤساء معاهد العلوم الجنائية عام 1976، وصدر عنه توصية رقم 12/81 وأقرها المجلس الأوروبي عام 1981 والتي تضمنت تعريف جرائم الحاسب الآلي ضمن نطاق جرائم اقتصادية، جرائم سرقة المعلومات، التجسس المعلوماتي، العبث في البيانات والمعلومات المعالجة تقنياً².

في عام 1989 قامت اللجنة الأوروبية بدراسة مشاكلها خلال سنوات 1985 - 1989، وأصدرت تقريراً يحتوي على مجموعة من الإرشادات من أجل مكافحتها تحت رقم 9/89، وتضمن هذا التقرير مجموعة من الأفعال التي تعد جرائم معلوماتية على نحو أفعال أساسية وتشمل: الاحتيال المعلوماتي والتزوير المعلوماتي والإتلاف المعلوماتي، والاعتراض غير

¹ غايب، محروس نصار: مرجع سابق، ص 20.

² فكري، أيمن عبد الله: مرجع سابق، ص 128.

المشروع للحاسب الآلي، وإعاقة النظام المعلوماتي عن أداء عمله ووظيفته، والدخول غير المشروع للنظام المعلوماتي، والنسخ غير المشروع لبرامج الحاسب. وتشمل الأفعال الاختيارية: تعديل البيانات أو البرامج الموجودة على الحاسب الآلي دون إتلافها، والتجسس المعلوماتي، والاستعمال غير المشروع لنظام الحاسب الآلي. كما اشترطت هذه اللجنة لاعتبارها جريمة معلوماتية أن تتوفر الشروط التالية: وقوع ضرر جسيم، ومعرفة الفاعل بتقنية المعلومات، وارتباط وظيفي بين الفاعل ومحل النشاط الإجرامي المتمثل في المعلومات المعالجة تقنيا¹.

كما أصدر المجلس الأوروبي في العام 2000 اتفاقية شاملة تتعلق بجرائم الحاسب الآلي عن الدول الأعضاء، تناولت مفهوم نظام الحاسب الآلي، والإجراءات الواجب اتخاذها على المستوى الداخلي بإضافة قوانين حول جرائم الاعتراض غير المشروع، وتناولت التزوير والاحتيال المرتبط بالحاسب الآلي، وحقوق النسخ والاعتداءات المتعلقة بها، وإلى المسؤولية والمساهمة والعقوبات، بالإضافة إلى تنظيم الإجراءات كتحقيقات ومصادرة المعلومات المخزنة على الحواسيب، وتضمنت مبادئ التعاون الدولي في جمع الأدلة والإجراءات والتشريعات، وأشارت في مقدمتها إلى وضع تشريعات لحماية المجتمعات وتعزيز التعاون الدولي نتيجة تزايد هذه الجرائم والمشاكل التي تواجه قانون الإجراءات الجزائية².

الفرع الخامس: التقسيم الفرنسي

تمثل هذا التقسيم بالقانون رقم 88/19 وفق المعلومات والنظام المعلوماتي وهي الدخول غير المشروع أو إتلاف معلومات أو إعاقة وتعطيل لنظام معالجة البيانات الإلكتروني، وتزوير شهادة برمجة من أجل استخدامها³. ويعاقب المشرع الفرنسي على المساهمة الجنائية والشروع في هذه الجرائم. فإن المشرع الفرنسي استخدم في قانون العقوبات الحديث إطار موسع لمفهوم التزوير،

¹ قوره، نائلة: مرجع سابق، ص 260-262.

² الزعبي، وآخرون: مرجع سابق، ص 98.

³ رمضان، مدحت عبد الحليم: الحماية الجنائية للتجارة الإلكترونية - دراسة مقارنة، دار النهضة العربية، 1994. ص45.

وحذف المواد الخاصة بالتزوير في وثائق البرمجة واستخدامها، لعل غاية المشرع الفرنسي إدخال التزوير المعلوماتي ضمن مجال جرائم التزوير التقليدية¹.

تناول المشرع الفرنسي في قانون العقوبات الحديث 19/ 88 جريمة الإلتاف المعلوماتي في المادة 323 وفرض عقوبة الحبس لمدة سنتين وبغرامة 30000 يورو لمن يدخل بطريق الغش أو التدليس على نظام لمعالجة البيانات أو الاتصال بطريقة غير مشروعة، وفي حال ترتب على ذلك الغاء أو تعديل النظام أو البيانات الموجودة عوقب بالحبس لمدة 3 سنوات وبغرامة 45000 يورو². ويستخلص من هذا النص بان المشرع الفرنسي قام بحماية النظام المعلوماتي والمعلومات الموجودة فيه.

وقد طبقت محكمة النقض الفرنسية هذه المادة على حالة قيام أحد الأشخاص بتعديل أو محو معلومات تتعلق باللوائح الداخلية بإحدى الشركات عن طريق العمد، وقد أقرت المحكمة بانه ليس من الضروري إجراء هذه التعديلات أو الإلغاءات من قبل شخص ليس له الحق في الدخول إلى النظام، ولا يشترط توافر نية الإضرار لدى الجاني³. وطبقت محكمة جناح باريس هذه المادة على الجاني الذي استعمل برامج Siffer الإلكترونية لتحويل أموال من حسابات الغير إلى حسابه الخاص بطرق غير مشروعة⁴.

الفرع السادس: التقسيم الأمريكي

قبل صدور التشريعات الأمريكية الخاصة بجرائم الحاسب الآلي، كان القضاء الأمريكي يطبق نصوص العقوبات التقليدية على الجرائم المعلوماتية، ونتيجة التقدم التكنولوجي وعجز القوانين التقليدية عن مواجهة هذه الجرائم، صدر قانون جرائم الحاسب الآلي الفيدرالي عام 1984 وتم تعديله عامي 1986 و1994، واطلق عليه قانون الاحتيال وإساءة استخدام الحاسب الآلي، وفي

¹ رمضان، مدحت عبد الحليم: مرجع سابق، ص 50.

² فكري، أيمن عبد الله: مرجع سابق، ص 250 - 251.

³ قشقوش، هدى: الإلتاف العمدي لبرامج وبيانات الحاسب الإلكتروني، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، في الفترة 1-3 مايو، 2000 . ص 20.

⁴ رستم، هشام: مرجع سابق، ص 323.

عام 1996 وقع الرئيس الأمريكي قانون الاتصالات، الذي قيد حرية الاطلاع على المواد الإباحية عبر الإنترنت، وفي عام 1997 تم توقيع قانون السرقة غير الإلكترونية لحماية حقوق الطبع والعلامات التجارية¹.

اعتمد التقسيم الأمريكي لهذه الجرائم على الدراسات والأبحاث الأمريكية، وعلى مشروعات القوانين ذات العلاقة من أجل تعزيز الانسجام والملائمة بين هذه القوانين، ومثل هذا التقسيم مشروع القانون النموذجي لجرائم نظم المعلومات عام 1999 الذي وضع من قبل خبراء أكاديميين أمريكيين، ويتضمن²:

- جرائم تستهدف الأشخاص وتنقسم إلى جرائم جنسية وتشمل استخدام الإنترنت لنشر معلومات وصور جنسية غير مشروعة، وجرائم غير جنسية كالتحريض على الانتحار والتحرش الجنسي عبر شبكات الاتصال.

- جرائم الاختراق والإتلاف كالدخول غير المشروع لسرقة الملكية والبيانات وإنشاء البرامج والفايروسات الضارة وبثها عبر الشبكات.

- جرائم الاحتيال والسرقة مثل استخدام الحاسب الآلي للحصول على البطاقات المالية والائتمانية وسرقة معلومات الحاسب الآلي، وجرائم التزوير كتزوير الوثائق والبريد الإلكتروني، وجرائم ضد الأخلاق والآداب وتشمل ترويج المقامرة والكحول عبر استخدام الإنترنت.

- جرائم ضد الحكومات وتشمل هذه جرائم تهدد السلامة العامة والإرهاب الإلكتروني.

ومن الأمثلة على هذه الجرائم قضية الأمريكي Robert Morris في نهاية عام 1988، الذي استخدم حاسبه أثناء دراسته للدكتوراه في جامعة هارفارد في تصميم وتطوير برنامج فايروس الدودة، ثم قام بنشره وتشغيله على شبكة الإنترنت في الولايات المتحدة الأمريكية مما أدى إلى تعطيل أنظمة الكمبيوتر والمواقع العسكرية ومراكز البحوث الطبية والجامعات، وتراوحت

¹ رمضان، مدحت عبد الحليم: مرجع سابق، ص 45.

² فكري، أيمن عبد الله: مرجع سابق، ص 131 - 137.

تكاليف إصلاح هذه الإضرار ما بين 2000 - 53000 دولار، وقد تم محاكمته على جريمة الدخول العمدي إلى جهاز الحاسب الآلي الفيدرالي التي أدت إلى تخريب أو تدمير المعلومات الموجودة فعلياً عليه، ودفع Morris بعدم وجود نية الإضرار لديه، ولكن رفضت المحكمة دفعه بقولها لا يشترط أن تتجه النية إلى تحقيق الضرر بل يكفي أن تتجه النية إلى الدخول غير المشروع على نظام حاسب فيدرالي، وحكم عليه بوضعه تحت المراقبة لمدة 3 سنوات وعمل خدمة مجتمعية لمدة 400 ساعة وبغرامة عشرة آلاف وخمسمائة دولار¹.

تختلف هذه التصنيفات وفقاً للمعايير والأسس الذي استندت إليها كل فئة، فمنهم يصنفها إلى جرائم ترتكب على النظام المعلوماتي أو ترتكب بواسطته، وتصنف وفق أسلوب أو دافع ارتكابها أو تعدد محلها، ولم تتطرق هذه التقسيمات إلى خصائص هذه الجرائم وحق المعتدى عليه، إلا أنها تناولت بعض المواضيع المتعلقة بها، وخلصت إلى اعتبارها جرائم مستحدثة، تقع على النظام المعلوماتي والمعلومات باستخدام وسائل التقنيات التكنولوجية، وإن الجرائم ذات الطبيعة المادية تدخل في إطار الجرائم التقليدية ولا تندرج ضمن نطاقها.

المبحث الثاني: أركان الجريمة المعلوماتية وأطرافها

تعد أركان الجريمة العناصر الأساسية لقيام أي جريمة وبدونها تنفي وجودها، وتحتاج لوجود فاعل ومجني عليه ومحل الجريمة، ولكنها تختلف باختلاف الفاعل وقدراته وطبيعة السلوك الإجرامي ومسرح الجريمة، وتخضع هذه الجريمة إلى طبيعة قانونية واحدة ترتكز على محل الجريمة وهو مكونات الحاسوب وأنظمة المعلومات واستخدام الحاسب الآلي كوسيلة لارتكابها².

المطلب الأول: أركان الجريمة المعلوماتية

تقوم على ثلاثة أركان وهي: الركن الشرعي: هو صفة عدم مشروعية الفعل وقاعدة التجريم والعقاب، الركن المادي: هو إخراج ماديات الجريمة إلى حيز الوجود الخارجي، والركن

¹ د. يونس عرب: جرائم الكمبيوتر والإنترنت المعنى والخصائص والصور واستراتيجية المواجهة القانونية. والى أيمن عبد الله فكرى، مرجع سابق، ص 168 - 173.

² الزعبي، وآخرون: مرجع سابق، ص 43.

المعنوي: هو نية وإرادة ارتكاب الفعل سواء بصورة عمدية أو عن طريق الخطأ، وسيتم البحث في ركنها المادي والمعنوي على فرعين¹:

الفرع الأول: الركن المادي

يُثير طبيعة الركن المادي في الجرائم المعلوماتية مشكلة عملية حقيقية، تكمن في أن مفهوم أو مناط التجريم يقع على إساءة استخدام النظام الإلكتروني أو الدخول إليه بطريقة غير المشروع، ويكون لذلك الاستعمال أو الدخول غير المشروع إظهار الأثر المادي². ويرتبط السلوك الإجرامي فيها بالمعلومات المخزنة والموجودة فعلاً على الحاسب الآلي أو المعلومات التي يتم إدخالها للحاسب الآلي، وقد يتحقق السلوك الإجرامي بمجرد كبسة زر على الحاسب الآلي، فيتم تدمير نظام المعلومات، أو حصول تزوير، أو السرقة عن طريق الدخول إلى أنظمة أرصدة العملاء والزيائن لدى البنوك، أو إساءة استعمال بطاقات الائتمان³.

إن السلوك الإجرامي في الجرائم التقليدية يختلف عنه بالجريمة المعلوماتية، ففي الجرائم التقليدية يمكن مشاهدته والتأكد منه كالقتل والسرقة، أما في الجرائم المعلوماتية فمن الصعب رؤيته، لأنها ترتكب بسرعة فائقة بواسطة معلومات عبر نظام الحاسب الآلي. حيث يتطلب السلوك المادي فيها وجود حاسب إلى واتصال بشبكة الإنترنت وبيئة رقمية (معلومات)، ويشترط معرفة بداية هذا النشاط والشروع فيه ونتيجته، فعلى سبيل المثال يقوم الجاني بتحضير حاسب إلى لتحقيق نتيجة الجريمة، ثم يبدأ بإعداد أو تحميل برامج الاختراق، أو إنشاء صفحات تحتوي على مواد مخلة بالآداب العامة كالصور الإباحية أو برامج فيروسات من أجل تحميلها على الجهاز المضيف⁴.

¹ الجبور، محمد: الوسيط في قانون العقوبات - القسم العام، دار وائل عمان، ط1، ص59.

² العجمي، عبدالله دغش: مرجع سابق، ص26-27.

³ معاشي، سميرة: ماهية الجرائم المعلوماتية، بحث منشور في مجلة المنتدى القانوني، العدد السابع، جامعة محمد خضير بسكرة، الجزائر، 2011، ص280.

⁴ حجازي، عبد الفتاح: مرجع سابق، ص113.

يلاحظ أن بعض الجرائم لا تستوجب القيام بأعمال تحضيرية، وغالباً يصعب الفصل بين الأعمال التحضيرية والبدء في النشاط الإجرامي في جرائم الكمبيوتر والإنترنت، حتى ولو لم يكن القانون يعاقب عن الأعمال التحضيرية، ولكن يختلف الأمر في مجال تقنية المعلومات، فشراء برامج الاختراق ومعدات لفك الشيفرات وكلمات السر تمثل في حد ذاتها جريمة يعاقب عليها القانون¹.

يُثير النشاط أو السلوك المادي في الجريمة المعلوماتية العديد من التساؤلات التي تتعلق في بداية ارتكاب الجريمة أو الشروع فيها، فارتكاب الجريمة عبر الإنترنت يحتاج إلى جهد تقني، وبدونه لا يستطيع الشخص الاتصال بشبكة الإنترنت سواءً كان بهدف ارتكاب جريمة أم لمجرد التصفح، ويشكل هذا السلوك المنطق التقني الذي يجعل الجريمة عبر الإنترنت ذات طابع موحد. لذلك يُعتبر الدفع أمام محكمة الموضوع، بعدم وجود قدرات تقنية لدى الفاعل وقت ارتكابها من الدفع الموضوعية الجوهرية، التي يُلزم المحكمة الرد عليه بشكل مفصل والا اعتبر حُكمها معيباً في التسبب والتعليل، مما يستوجب نقضه².

كما تظهر عدة إشكاليات في النتيجة الإجرامية في الجرائم المعلوماتية، فمثلاً مكان تحديد مكان وزمان تحقق نتيجة الجريمة، فإذا قام أحد المجرمين في المانيا بسرقة أحد البنوك في الأردن عبر جهاز الخادم الموجود في الصين، فكيف يمكن معرفة وقت حدوث الجريمة، هل هو توقيت بلد الجاني أو بلد المجني عليه أو وقت جهاز الخادم، وتبرز أيضاً إشكالية ما هو القانون الواجب التطبيق في هذه الحالة لوجود بعد دولي³. ولكي يتوافر ركنها المادي يشترط حصول النتيجة الإجرامية لارتباطها بالسلوك الإجرامي من خلال إثبات العلاقة السببية بين الفعل والنتيجة.

¹ العجمي، عبدالله دغش: مرجع سابق، ص 28.

² إبراهيم، خالد ممدوح: مرجع سابق، ص 100.

³ مطر، كامل: الجريمة الإلكترونية، ورقة عمل مقدمة إلى المؤتمر الأول لمكافحة الجرائم الإلكترونية في فلسطين، جامعة النجاح الوطنية، نيسان، 2016، ص 17.

الفرع الثاني: الركن المعنوي

يمثل الركن المعنوي الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، ويتضمن مقومات المسؤولية الجنائية من علم وإرادة أثمة وقصد جرمي مع حق الدولة في إيقاع العقوبات. لذلك عرف محمود نجيب حسني الركن المعنوي بأنه " العلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، وهذه العلاقة هي محل الجريمة التي تستوجب العقاب، وتوجيه لوم قانون من أجل معاقبته"¹ ويتوفر القصد الجنائي لدى الجاني في ثلاثة حالات وهي: إذا ترتب على فعل الجاني أو امتناعه حدوث ضرر أو خطر ليشكل جريمة وفق القانون، وإذا نتج عن فعل الجاني أو امتناعه ضرر أو خطر جسيم أكثر مما يقصده الفاعل، والحالات التي افترض فيها القانون توافر القصد الجنائي لدى الجاني نتيجة فعله أو امتناعه، وهو مستمد من النتيجة الجرمية التي حققها الفاعل².

إن توافر الركن المعنوي في الجرائم المعلوماتية من الأمور الأساسية الواجبة لتحديد طبيعة السلوك المرتكب وتكييفه، من أجل تحديد النصوص القانونية الواجبة التطبيق، وفي حال عدم توفر الركن المعنوي، يصبح أمام جريمة أخرى وهي جريمة الدخول غير المشروع، بحيث يقوم الشخص بالدخول إلى نظام معين، ولا يملك صلاحيات الدخول عليه³.

لم يستقر القضاء بشكل عام والأمريكي بشكل خاص على حالات معينة بالنسبة لبعض الجرائم التي ترتكب باستخدام الإنترنت، فيما إذا كانت تتطلب قصداً عاماً أو قصداً خاصاً، ففي جريمة التهديد عبر البريد الإلكتروني يكفي توفر القصد العام ولا يمنع من تطلب قصد جنائي خاص فيها، ويستدل على سلوكه الشخصي من الظروف المحيطة بالجريمة⁴.

¹ حسني، محمود نجيب: النظرية العامة للقصد الجنائي، دار النهضة العربية، ط2، 1981. ص90.

² الجبور، محمد، مرجع سابق، ص238 وما بعدها.

³ موسى، مصطفى محمد: دليل التحري عبر شبكة الإنترنت، دار الكتب القانونية، مصر، 2010، ص 143.

⁴ إبراهيم، خالد ممدوح: مرجع سابق، ص109.

يلاحظ أن المشرع الأمريكي من أجل تحديد الركن المعنوي يأخذ بمبدأ العلم ومبدأ الإرادة كما في قانون العلامات التجارية في القانون الفيدرالي الأمريكي، وأحياناً يأخذ بالعلم كما في قانون مكافحة الاستساح الأمريكي. برزت تلك المشكلة في قضية موريس الذي كان متهماً في قضية دخول غير مصرح به على 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 المصرح 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 خسائر، ومثل هذا الأمر يستدعي التوصل إلى تحديد أركان جريمة الدخول دون تصريح"¹. وبذلك ذهبت المحكمة إلى تبني معيارين هنا هما الإرادة بالدخول غير المصرح به، وإذا معيار العلم بالحظر الوارد على استخدام نظم معلومات فيدرالية دون تصريح.

أما القضاء الفرنسي فيشترط توافر سوء النية في حالة وجود اعتداء على البريد الإلكتروني، وبالتالي فإن هذه الجرائم لا تدخل حيز التطبيق إذا لم يتوفر سوء النية وإرادة الإضرار. كذلك الحال لدى المشرع البريطاني، فالركن المعنوي يتطلب أن تتجه أرادة الجاني نحو الدخول إلى البيانات والمعلومات المخزنة على الحاسب الآلي². ويتوفر الركن المعنوي في الجرائم المعلوماتية في حال قيام أحد القراصنة بنسخ برامج كمبيوتر من موقع على شبكة الإنترنت، والقيام بفك شيفرة الموقع وتدميره للحصول على معلومات وبرامج بغية إلحاق الضرر على الشركة³.

المطلب الثاني: أطراف الجريمة المعلوماتية

تحتاج هذه الجرائم كغيرها من الجرائم وجود طرفين فاعل ومجني عليه، لكنهم يختلفون عن أطراف الجرائم التقليدية، وسوف يتم تناول ذلك في فرعين، الفاعل والمجني عليه، ودرس المطلب الثالث المسؤولية الجزائية لمرتكبي الجرائم المعلوماتية.

¹ مطر، كامل: مرجع سابق، ص18.

² موسى، مصطفى محمد: دليل البحث والتحري عبر شبكة الإنترنت، دار الكتب القانونية، مصر، 2010. ص143.

³ الرواشدة، وآخرون: مكافحة الجريمة المعلوماتية بالتجريم والعقاب، المجلة الأردنية في القانون والعلوم السياسية، جامعة مؤتة، الأردن، المجلد (1)، العدد (3)، ص128 وما بعدها.

الفرع الأول: الفاعل

يلعب الفاعل الدور الرئيسي في إبراز العناصر المكونة للجريمة أو الأفعال التي يساهم في تنفيذها، التي تخرج المظهر الخارجي للجريمة، ويشكل هذا السلوك وما يرتبط به ركناً مادياً في جرائم تقنية المعلومات، وعلى سبيل المثال ما ورد بقانون حق المؤلف الأردني، بيع برامج وأنظمة الحاسوب المقلدة أو نسخاً عنها شريطة علمه بأنه مقلد باي طريقة كانت، وكل من يستعمله بصورة غير شرعية يعتبر فاعل أصلي. أما القانون الأمريكي أعتبر الفاعل في جرائم الغش والاحتيال باستعمال الحاسوب هو كل شخص يصل بمعرفته وقدرته دون تفويض، أو تجاوز حدود التفويض الممنوح له، وحصل على معلومات وبيانات سرية¹.

يختلف الجاني في الجرائم المعلوماتية عن الجاني في الجرائم التقليدية، فالجريمة المعلوماتية تُرتكب من قبل أفراد يتمتعون بمستوى كاف من المعرفة والخبرة والذكاء في مجال آليات عمل الحاسب الآلي واستخدام تقنية المعلومات، بالإضافة إلى تحقق الشروط العامة وهي السلوك والعلم والإرادة، وقد أطلق عليه البعض بمصطلح المجرم المعلوماتي أو المجرم الإلكتروني².

ويمتاز فاعلها بعدد من الصفات والخصائص، وهي: يتمتع بالمهارة والمعرفة والذكاء استخدام الحاسوب وتقنية المعلومات وشبكات الإنترنت، كما أنه إنسان اجتماعي محل ثقة في مجال عمله، ويبرر ارتكابه جريمته باعتبارها أفعال أخلاقية ومشروعة³، ويصنف المجرم المعلوماتي على النحو التالي:

1. المخترقون: مثل الهاكرز، وهم أشخاص يجيدون استخدام الحاسب الآلي ويحاولون الدخول إلى شبكات الإنترنت نتيجة التباعد الجغرافي، وهم الأقل خطورة لا تتوفر لديهم أعمال الحقد أو التخريب، ويرتكبون المخالفات دون قصد أو نية الإضرار، من أجل التحدي بينهم وإثبات الذات، وغالباً يكون أعمارهم في سن المراهقة. ويقتصر دورهم بالاطلاع على البيانات والمعلومات،

¹ المناعسة، وآخرون: مرجع سابق، ص 84-85.

² دغش، عبد الله العجمي: مرجع سابق، ص 32.

³ المومني، نهلا عبد القادر: مرجع سابق، ص 77-81.

وتصبح الخطورة في حال نشر هذه المعلومات على شبكات الإنترنت. ومن أمثلتها قيام فتاة تبلغ 14 سنة باختراق نظام معلومات البنّاجون، وشخص آخر لا يتجاوز 17 سنة اخترق حواسيب وبرامج بعض المؤسسات في أوروبا¹.

2. المحترفون: تعد هذه الفئة الأكثر خطورة بين مجرمي المعلومات، ويتمتعون بقدرات وخبرات متخصصة في مجال تكنولوجيا المعلومات، تهدف إلى تحقيق مكاسب مادية غير مشروعة كالاستيلاء على أموال الغير عبر الإنترنت، والانتقام والى تحقيق أهداف سياسية ونشر وجهات النظر الفكرية، وان معظمهم غالباً تتراوح أعمارهم ما بين 25-40 عام، وتمتاز هذه الفئة بالذكاء الشديد لأنها لا تحتاج إلى جهد عضلي مثل الجرائم التقليدية بل إلى جهد فكري وتقني للتعامل مع الحاسب الآلي وبرامجه، ولديهم طابع التحدي بقدرتهم على اختراق أنظمة حماية برامج وبيانات ومعلومات المؤسسات².

3. الحاقدون: وهم الذين لا يسعون إلى تحقيق أهداف الجريمة، ولا تحقيق أي مكاسب مادية أو سياسية وليس لإثبات قدراتهم ومهاراتهم، وإنما يتحركون من أجل الانتقام والثأر من صاحب العمل معهم أو نتيجة تصرف الإدارة مع الموظفين فيها، لا يتميز هؤلاء بالمعرفة التقنية، وغالباً يقومون بأعمالهم من خلال نشر الفيروسات والبرامج الضارة وتخريب النظام أو إتلافه أو تعطيله، وهم أقل خطورة من غيرهم³.

إضافة إلى تنوع دوافع وبواعث ارتكابها والتي تتمثل فيما يلي: دافع مادي لتحقيق المكاسب المالية كالنصب والاحتيال الإلكتروني على المؤسسات المالية كالبنوك وشركات التأمين، وكذلك التعلم على أنظمة تقنية المعلومات واختراق الشبكات الإلكترونية للحصول على معلومات. ومن أجل إثبات الذات من خلال التحدي وإثبات قدرته في اختراق الأنظمة المعلوماتية. والانتقام من الأشخاص أو المؤسسات أو بعض الأنظمة السياسية في الدول⁴. ودوافع أخرى تتمثل في

¹ قوره، نائلة: مرجع سابق، ص 178.

² مصطفى، سليمان أبكر: جرائم الحاسوب وأساليب مواجهتها، مجلة الأمن والحياة، 2010. ص 48.

³ فكري، أيمن عبد الله: مرجع سابق، ص 111.

⁴ الشوا، سامي: مرجع سابق، ص 52.

مجالات المنافسة السياسية والاقتصادية والعسكرية، مثل قيام بعض القراصنة من داخل روسيا باختراق أنظمة الحواسيب والشبكات المعلوماتية التابعة لوكالة ناسا الفضائية والمنتمى للاقتصادي العالمي (دافوس) بسويسرا¹.

الفرع الثاني: المجني عليه

تقع هذه الجرائم على الشخص الطبيعي والمعنوي، وغالباً تقع على الأشخاص المعنوية مثل الشركات الصناعية الكبرى وشركات التأمين والمؤسسات المالية كالبنوك، التي تعتمد في عملها على الحاسب الآلي وتقنية المعلومات. وشهدت لوس أنجلوس أشهر الجرائم عندما قام أحد موظفي شركات التأمين بإنشاء عملاء مؤمن عليهم وهميين باستخدام نظامها التقني والمعلوماتي، وتم بيع نحو 46000 بوليصة تأمين إلى شركة مقابلة. وتنتشر هذه الجرائم في الدول النامية على شكل انتهاك حقوق المؤلف كعرض أو بيع برامج مقلدة. وأخطر التي تقع على الجهات العسكرية والأمنية من خلال عمليات التجسس ورصد البيانات وتهريبها. يكون دور المجني عليه (الضحية) في هذه الجرائم دوراً سلبياً، فمنهم لا يريد الكشف عن الاعتداءات التي لحقت بأنظمتهم التقنية والمعلوماتية وعدم إبلاغ الجهات الأمنية والقضائية، حرصاً على سمعتهم وحماية مركزهم المالي ومن أجل المحافظة على ثقة العملاء بهم، وإذا اكتشفت هذه الجرائم غالباً تكون عن طريق الصدفة². وإذا كان المجني على طفلاً يعاقب الفاعل بالأشغال الشاقة المؤقتة بمدة لا تقل عن 5 سنوات ولو لم تقع الجريمة فعلاً، وفق نص المادة 29³.

المطلب الثالث: المسؤولية الجزائية لمرتكبي الجرائم المعلوماتية

تتناول المسؤولية الجزائية لمرتكبي الجرائم المعلوماتية للفاعل، والشريك، والمتدخل، والمحرض، بالإضافة إلى المسؤولية الجزائية لمزودي خدمة الإنترنت والمستضيف في الجرائم المعلوماتية، وتقوم المسؤولية الجزائية على من يقوم بتحقيق الركن المادي للفعل المجرم بموجب

¹ هلاي عبد اللاه، أحمد: الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، القاهرة، دار النهضة العربية، 2000. ص24.

² الزعبي، مرجع سابق، ص82.

³ المادة 29 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية.

القواعد والنصوص الجزائية، فأساس المسؤولية الجزائية عنصري الوعي والإرادة أي الإدراك وحرية الاختيار، ويتساوى الشخص الطبيعي والمعنوي في هذه المسؤولية إلا أنه يختلف في طبيعة العقوبة المفروضة عليهم فاذا كان فاعلها شخص معنوي يفرض عليه غرامة¹.

1. مسؤولية (الفاعل، الشريك، المتدخل، المحرض)

تفرض المسؤولية الجزائية في جرائم المعلومات على أساس دور الشخص الذي يرتكب الفعل الإجرامي، فقد يكون السلوك ناتج عن مساهمة آخرين مع الفاعل الأصلي، وشركاء آخرون، وقد يستعين الفاعل بآخر فيصبح متدخلًا. فالشريك يقوم بفعل أو أكثر يدخل في نطاق الركن المادي للجريمة، مثل الاحتيال عبر شبكة الإنترنت وبيع برامج مقلدة، فيتم مسألتة مع الفاعل بعد إثبات الحالة النفسية والذهنية بينهم وعلمه وإرادته في إتمام الجريمة. ونظراً لطبيعة السلوك الجرمي فيحتاج إلى استخدام وسائل تقنية متعددة مع عدة أشخاص. ويلعب الشريك دوراً رئيسياً في تحقيق الجريمة ونتائجها وحسن تنفيذها. أما المتدخل يكون دوره ثانوياً ولا يدخل في نطاق الأفعال التنفيذية المكونة للجريمة، ولا يعتبر فعله مجرم، ويكون التدخل في الجنايات والجنح وفق نص المادة 2/80 من قانون العقوبات الأردني، فمثلاً استخدام مبرمج لمعلوماته حول الشبكات المعلوماتية لمساعدة الجناة لاقتحام برامج الحاسب الآلي وتدميره أو إتلافها يعتبر متدخلًا، ما دام فعله انطبق عليه وصف المساعدة بإرشاداته الخادمة لارتكاب جريمة، مما يقتصر حالات تدخل الجرائم المعلوماتية على حالات التدخل للجرائم التقليدية، وهذا يتطلب احتواء صور أخرى استناداً إلى دور الفاعل والمساهمين وأدوات الجريمة الوسائل التقنية وأنظمة المعلومات والسلوك المعنوي أساس التجريم².

¹ سلامة، محمد أبو بكر: موسوعة جرائم المعلومات، منشأة المعارف الإسكندرية، 2006، ص 20.

² المناعسة، والزعبي: مرجع سابق، ص 84، ص 86. (انظر إلى المادة 80 من قانون العقوبات الأردني رقم 16 لسنة 1960).

يقتصر دور **المحرض** في المراحل السابقة لارتكاب الجريمة، لإظهار الجريمة إلى حيز الوجود، وأشار قانون العقوبات الأردني إلى التحريض على ارتكاب جناية أو جنحة، ولم يشر إلى نصوص خاصة بالاشتراك الجرمي والمساهمة في الجرائم المعلوماتية، وبالتالي يتم تطبيق القواعد العامة الواردة في قانون العقوبات¹. وفرضت المادة 28 ضعف العقوبة المقررة في التشريع الأصلي حال ارتكاب أو الاشتراك أو التحريض على ارتكابها بقصد ارتكاب جريمة معاقب عليها بموجب تشريعات نافذة. ويعاقب المحرض على ارتكاب هذه الجرائم بثلاثي الحد الأقصى لعقوبة الفاعل الأصلي².

2. المسؤولية الجزائية لمزود خدمة الإنترنت

نصت المادة 1 و2 من اتفاقية بودابست لسنة 2001 بشأن جرائم الإنترنت على تعريف المزود، وهو كل شخص يمكن المستخدمين على الاتصال باستخدام أنظمة الحاسب الآلي أو قيامه بمعالجة البيانات وتخزينها نيابة عن المستخدمين، ويقتصر دوره على إيصال المشتركين إلى شبكة الإنترنت باستخدام الوسائل التقنية. وليس مراقبة محتويات المعلومات وسلوك مستخدمي الإنترنت³.

تختلف وسائل الوصول إلى الإنترنت فقد تكون عن طريق IDSL، Dial up وغيرها، ولكن في جميع الحالات يشترط وجود خادم server، وتثير مسألة اعتبار مزود الخدمة فاعلاً أصلياً في هذه الجرائم العديد من الآراء حول اعتبار مزود خدمة الإنترنت مسؤولاً عن هذه الجرائم، فمنهم من يرى بعدم مسؤولية المزود، لأنه لا يملك القدرة على التحكم في مضمون المعلومات المخزنة ولا يملك وسائل فنية لمراقبتها⁴، ويرى اتجاه آخر بوجود المسؤولية الجزائية عليه وفقاً للمسؤولية المتتابعة لعلمه السابق بما يعلن وينشر على الشبكات، ويصعب تطبيق هذا الرأي لأن

¹ المناعسة، مرجع سابق، ص 83-88.

² المادة 28 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية.

³ انظر تفصيل ذلك: أ.د. هلال عبد الله أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية (معلقاً عليها)، دار النهضة العربية، الطبعة الأولى، القاهرة، 2007، ص 47.

⁴ حسين، محمد عبد الطاهر: المسؤولية القانونية في مجال شبكات الإنترنت، 2002. دار النهضة العربية، القاهرة، ص 38.

مزود الخدمة لا يملك وسائل فنية وقانونية لمراقبة المعلومات المنشورة على الشبكات، فيما يرى آخرون مساءلته جزائياً لامتلاكه وسائل فنية تمنع من دخوله إلى هذه المواقع وتمنع نشر المحتويات التي تتعارض مع الأنظمة والقوانين، تواجه صعوبة في تطبيق العلم المسبق لأسباب فنية وقانونية لعدم وجود إمكانية مراجعة مضمون المعلومات قبل نشرها، وعدم اختصاص مزود الخدمة بممارسة الرقابة التوجيهية على ما يتم نشره¹.

وذهب القضاء الفرنسي في حال قيام مستخدم الشبكة بنشر رسائل غير مشروعة، لا تقوم المسؤولية الجزائية على مقدم خدمات الإنترنت، نتيجة عدد المستخدمين وحجم الرسائل الهائلة المتداولة². وفرض المشرع التونسي التزامات على مزودي المعلومات من أجل المحافظة على خصوصية وسرية المعلومات وفي حال مخالفتها يترتب عليها سحب ترخيص أو إيقاف نشاط مزود خدمات المصادقة الإلكترونية بالإضافة إلى الغرامات المالية، ونص المشرع البحريني على المسؤولية الجزائية للشخص الاعتباري وموظفيه أو من يتصرف بصفته أو الشخص الطبيعي، في حال قيامهم بالمساس بصحة وسلامة المعلومات والبيانات الشخصية، ويعاقب قانون إمارة دبي على الأفعال غير المشروعة حال ارتكابها من الشخص الاعتباري أو شخص يتصرف بصفته³. وفي فلسطين نص المشرع في المادة 30 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية على " إذا ارتكبت باسم الشخص المعنوي أو لحسابه أحد الجرائم المنصوص عليها في هذا القرار بقانون يعاقب بالغرامة التي لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني والمحكمة أن تقضي بحرمان الشخص المعنوي من مباشرة نشاطه لمدة أقصاها خمس سنوات أو تقضي بحله وذلك مع عدم الإخلال بالمسؤولية الجنائية للشخص الطبيعي التابع له"⁴، يحتوي هذا النص على غرامات مالية وتدابير احترازية مشددة دون الأخذ بعين الاعتبار طبيعة الجرائم ومدى جسامتها، وان المادة 36 من قانون العقوبات النافذ اشترطت ارتكاب جنائية أو جنحة لا تقل عقوبتها عن سنتين لإمكانية وقف

¹ جميل، عبد الباقي: مرجع سابق، ص 119.

² حجازي، عبد الفتاح: مرجع سابق، ص 15.

³ فكري، أيمن عبد الله: مرجع سابق، ص 763 – 769.

⁴ المادة 30 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية.

الهيئة المعنية عن عملها، وان حرمان الشخص المعنوي من ممارسة نشاطه أو حله يكون بموجب حكم قضائي نهائي إعمالاً لمبدأ الضرورة والتناسبية¹. وهذا ما يجب أن يأخذ به المشرع الفلسطيني. كما يعاقب كل من يستخدم الوسائل والأنظمة الإلكترونية لتجاوز الحجب المفروض على المواقع بالحبس مدة لا تقل عن ثلاثة شهور وبغرامة لا تقل عن خمسمائة دينار أردني ولا تزيد عن ألف دينار استناداً لنص المادة 31 من ذات القرار بقانون². وجود هذا النص يشكل مخالفة للمعايير الدولية التي لا تجيز الحجب وقد يستغل من أجل تقييد الحق في الوصول للمعلومة، ويجب على المشرع ذكر التقنيات والبرامج الحديثة التي تسهل إمكانية تجاوز الحجب المفروض على المواقع الإلكترونية³.

لم يتناول المشرع الفلسطيني في القرار بقانون بشأن الجرائم الإلكترونية آليه التعامل مع مزود خدمة الإنترنت الإسرائيلي الذي يمثل الإشكالية الحقيقية وصعوبة الكشف عن مرتكبيها لسيطرة الاحتلال الإسرائيلي على الفضاء الإلكتروني الفلسطيني. وبالتالي يجب على المشرع الفلسطيني وضع قوانين تتبنى إجراءات وعقوبات صارمة حول مزود الخدمة الإسرائيلي والحد من تداول الشرائح الإسرائيلية غير المرخصة.

3. المسؤولية الجزائية إلى المستضيف

وهي الشركات التي تستضيف وتنشئ صفحات ومواقع إنترنت على خادمها (server) مقابل أجر معين، ويكون فيها العميل (صاحب الموقع) على شكل مستأجر لمساحة محدودة من خادم الشركة تمكنه من كتابة وتخزين المعلومات ونشرها للغير، ويكون مقدم الخدمة على شكل مؤجر.

¹ ملاحظات مؤسسة الحق على القرار بقانون بشأن الجرائم الإلكترونية رقم 16 لسنة 2017، بتاريخ 2017/10/2، رام الله، ص6.

² المادة 31 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية.

³ ملاحظات مؤسسة الحق على القرار بقانون بشأن الجرائم الإلكترونية رقم 16 لسنة 2017، بتاريخ 2017/10/2، رام الله، ص13.

تختلف الآراء حول المسؤولية الجنائية فمنهم من اتجه بعدم وجود مسؤولية جنائية على المستضيف استناداً لطبيعة عمله الفني وهو احتواء المعلومات وتخزينها لاطلاع الغير عليها، ولا يسمح لهم بالسيطرة على مضمون المعلومات، وبالتالي تنتفي المسؤولية الجنائية والمدنية، وهذا ما أخذ به المشرع الفرنسي في القانون رقم 719 لسنة 2000 وتعديلاته. ويرى الاتجاه الآخر بوجود مسؤولية جنائية على المستضيف لاستطاعته رفض مضمون المعلومات غير المشروعة. ومنهم من يساءله على أساس الأحكام العامة للمساهمة الجنائية، في حال ثبوت علمه باستضافته معلومات غير مشروعة، ويساءل على أساس المسؤولية المتتابة لعدم قدرته على مراقبة مضمون المعلومات¹.

قد يصعب تطبيق الأحكام العامة نظراً لصعوبة إثبات العلم بمضمون المعلومات، ولا يمكن تطبيق المسؤولية المتتابة لصعوبة مراقبة المضمون وهي قاعدة استثنائية على القاعدة الأصلية للمسؤولية الجنائية، ويتلخص من أحكام القضاء بقيام مسؤولية المستضيف على تبنى معيار العلم، فتقوم هذه المسؤولية إذا كان يعلم بالجريمة ولم يقم بإجراءات لإيقافها.

¹ الصغير، جميل عبد الباقي: الإنترنت والقانون الجنائي، دار النهضة العربية، 2001. ص 132 – 134.

الفصل الثاني

الجرائم المعلوماتية وتحدياتها

تعتبر الجرائم الإلكترونية ظاهرة حديثة في فلسطين ظهرت مع انتشار وتزايد استخدام الوسائل الإلكترونية الحديثة وبخاصة الشبكة المعلوماتية وأجهزة الحاسوب والهاتف المحمول، مهد هذا الواقع الجديد في فلسطين لبيئة خصبه وسهلة لارتكابها وانتشارها في ظل غياب القوانين والعقوبات الرادعة لمرتكبيها.

خلت مختلف القوانين السارية في الضفة الغربية وقطاع غزة قبل منتصف العام 2017 من نصوص قانونية تحدد الأفعال التي تشكل الجرائم المعلوماتية. أدى هذا الفراغ القانوني إلى زيادة انتشارها وفق الإحصائيات الصادرة عن النيابة العامة الفلسطينية وجهاز الشرطة الفلسطينية، مما استوجب إصدار قرار بقانون بشأن الجرائم الإلكترونية لسنة 2017 للحد من هذه الظاهرة وملاحقة مرتكبيها في المجتمع الفلسطيني.

لتحقيق أهداف هذه الدراسة قسم هذا الفصل إلى مبحثين، يتناول المبحث الأول الواقع القانوني للجرائم المعلوماتية في فلسطين قبل صدور القرار بقانون بشأن الجرائم الإلكترونية، يبحث المطلب الأول تشريعات مختلفة في مكافحة الجرائم الإلكترونية، أما المطلب الثاني يدرس القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية من الناحية الموضوعية والإجرائية مركزاً على دور الشرطة والنيابة العامة والمحاكم الفلسطينية في ملاحقة مرتكبي الجرائم الإلكترونية. ويتناول المبحث الثاني مطلبين، يشتمل المطلب الأول على التحديات التي تواجه المشرع الفلسطيني في مجال الجرائم المعلوماتية، أما المطلب الثاني يبحث دور المؤسسات في الوقاية منها ومكافحتها.

المبحث الأول: الواقع القانوني للجرائم المعلوماتية في فلسطين قبل صدور القرار بقانون بشأن الجرائم الإلكترونية

تختلف التشريعات والقوانين السارية المفعول في دولة فلسطين، ففي الضفة الغربية يطبق قانون العقوبات الأردني رقم 16 لسنة 1960، وفي قطاع غزة يطبق قانون العقوبات الفلسطيني "الانتدابي" رقم 74 لسنة 1936، التي لا تحتوي على أي نصوص قانونية تتعلق بالجرائم التقنية. في العام 2003 أقر المجلس التشريعي الفلسطيني مشروع قانون العقوبات الفلسطيني بالقراءة الأولى حيث شمل هذا المشروع على العديد من النصوص القانونية التي عالجت جرائم الحاسب الآلي والإنترنت ولم يتم إقرار مشروع قانون العقوبات حتى الآن.

قبل نشر القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية بتاريخ 2017/7/9، كانت ملاحقة مرتكبي هذه الجرائم تتم بتطبيق النصوص التقليدية من قانون العقوبات الأردني رقم 16 لسنة 1960 على الجرائم الإلكترونية، والقانون رقم 3 لسنة 1996 بشأن الاتصالات السلكية واللاسلكية، بالإضافة إلى القرار بقانون رقم (15) لسنة 2009 بشأن الهيئة الفلسطينية لتنظيم قطاع الاتصالات¹، وقانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 وتعديلاته. التي تعجز عن ملاحقة وردع مرتكبيها ومكافحتها. وبسبب غياب النصوص القانونية التي تجرم وتحد وتكافح من هذه الجرائم. وتعطل المجلس التشريعي عن أعماله بما فيها تشريع القوانين ومراجعتها في ظل الانقسام، دفع هذا الواقع رئيس دولة فلسطين بموجب صلاحياته الدستورية وفق أحكام المادة 43 من القانون الأساسي الفلسطيني لسنة 2005 وتعديلاته، إلى إصدار قرار بقانون بشأن الجرائم الإلكترونية رقم 16 لسنة 2017، لمواجهة هذه الظاهرة في المجتمع الفلسطيني وليحد ويردع مرتكبيها، متماشياً مع الالتزامات المترتبة على دولة فلسطين نتيجة الانضمام والتوقيع على المعاهدات الدولية والإقليمية ذات العلاقة، ومنها اتفاقية بودابست لعام 2001، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات والتي تم التوقيع عليها بتاريخ

¹ الشلادة، محمد فهاد ربيعي، عبد الفتاح أمين، الجرائم الإلكترونية في دولة فلسطين المحتلة في ضوء التشريعات الوطنية والدولية، بحث مقدم إلى المؤتمر العلمي الحادي عشر لكلية القانون في جامعة جرش حول الجرائم المعلوماتية من 2015/5/7-5، نيسان 2015، ص8.

2010/12/21 وصادقت عليها دولة فلسطين بتاريخ 2013/5/21¹. تناول هذا المبحث في المطلب الأول تشريعات مختلفة في مكافحة الجرائم الإلكترونية، ويدرس المطلب الثاني القرار بقانون بشأن الجرائم الإلكترونية رقم 16 لسنة 2017 من الناحية الموضوعية والإجرائية.

المطلب الأول: تشريعات مختلفة في مكافحة الجرائم الإلكترونية

مع اتساع العالم الفضائي الإلكتروني والتكنولوجي الذي جعل العالم بمثابة قرية كونية، أصبحت الجرائم المعلوماتية ظاهرة جديدة في المجتمع الفلسطيني بسبب زيادة وانتشار استخدام الأنظمة التقنية الحديثة، وسوء استخدامها واستغلالها من قبل الأفراد والمؤسسات. يتناول هذا المطلب النصوص القانونية التي تتحدث عن الجرائم المعلوماتية في مختلف التشريعات السارية المفعول في فلسطين وشمل قانون العقوبات الأردني رقم 16 لسنة 1960 في الفرع الأول، وقانون رقم 3 لسنة 1996 بشأن الاتصالات السلكية واللاسلكية في الفرع الثاني، والقرار بقانون رقم 15 لسنة 2009 بشأن الهيئة الفلسطينية لتنظيم قطاع الاتصالات في الفرع الثالث، والقرار بقانون رقم 15 لسنة 2017 بشأن المعاملات الإلكترونية في الفرع الرابع.

الفرع الأول: قانون العقوبات الأردني رقم 16 لسنة 1960

عالج المشرع الأردني في قانون العقوبات الجرائم التقليدية ولم يشير إلى الجرائم المستحدثة بمختلف صورها، حيث عالج المواد 339 - 416 جريمة السرقة وعرفها بأخذ مال الغير منقول دون رضاه، واستناداً إلى هذا المفهوم يتمثل الركن المادي لهذه الجريمة بفعل الأخذ ومحلها مال منقول مملوك للغير وركنها المعنوي نية التملك²، وهذا النص لا يخلق إشكالية التطبيق في حال سرقة المكونات المادية للتقنيات كالبرامج لكنها تثار في حالة قيام الفاعل بالحصول على المعلومات المخزنة داخل الأنظمة المعلوماتية بغير وجه حق، وبناءً عليه فإن سرقة المعلومات لا تدخل ضمن نطاق هذا النص.

¹ قائمة الدول العربية الموقعة والمصادقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الأمانة العامة لجامعة الدول العربية، إدارة الشؤون القانونية، الشبكة القانونية العربية www.arablegalnet.org.

² قشقوش، هدى: مرجع سابق: ص 63. أنظر إلى المادة 399 من قانون العقوبات الأردني.

كما نص المشرع الجزائي الأردني في المادة 416 على جريمة استعمال أشياء الغير دون وجه حق حيث تتجه نية الفاعل نحو استعمال مال مادي منقول مملوك للغير دون موافقة مالكه أو حائزه دون تملكه، ومن خلال استعراض أركانها يكون أمام نص تقليدي يشترط أن يكون محل الجريمة مال مادي، وبما أن الخدمات المعلوماتية لا تتمتع بكيان مادي ملموس، وان يقوم الفاعل بإخراج الشيء من حيازة المجني عليه وإدخاله في حيازته لاستعماله، وهذا الأمر لا يتحقق في حالة الاستعمال غير المصرح به للنظام المعلوماتي، وأشار المشرع الأردني في المادة 445 من قانون العقوبات إلى جريمة الإتلاف، فهي جريمة عمدية تؤدي إلى إتلاف مال منقول مملوك للغير من شأنه الحاق الضرر، ويستفاد من ذلك عدم إمكانية انطباق هذا النص على جريمة الإتلاف المعلوماتي باعتبار الأموال المعنوية لا تتجسد في كيان مادي ملموس، فقد يقع الإتلاف على المكونات المادية للأنظمة المعلوماتية وقد يقع على مكوناته المعنوية (المعلومات)، ويجب توفير حماية للمعلومات من فعل الإتلاف بإضافة نصوص تراعي خصوصية مختلف المعلومات بخلاف قانون العقوبات¹.

عالج قانون العقوبات جريمة التزوير التقليدية في المادة 260 واستناداً لهذا النص تقوم أركانها على فعل تحريف مغير للحقيقة مع توافر الضرر المحتمل والقصد الجنائي العام العلم والإرادة والقصد الجنائي الخاص نية استعمال المستند المزور، واستناداً لذلك فإن التزوير وفق هذا النص يجب أن يقع في محرر مكتوب، ولم يتطرق إلى التزوير المعلوماتي كالتلاعب بالمعلومات أو إدخالها بشكل غير صحيح أو تعديلها أو محوها لتغيير الحقائق داخل الأنظمة المعلوماتية²، وبالتالي لا يمكن تطبيق نصوص جريمة التزوير التقليدية على واقعة تغيير حقائق المعلومات المعالجة تقنياً والكترونياً قبل اتخاذها شكل المحرر والمستند الإلكتروني، لأنها تفتقد إلى صفة المحرر مما يستدعي تجاوز هذا القصور في النص الجزائي لتجريم التزوير المعلوماتي ومعاقبة فاعله.

¹ المناعسة، وآخرون: مرجع سابق: ص 110 ... أنظر إلى المواد 416 و 445 ما قانون العقوبات الأردني.

² قورة، نائلة: مرجع سابق: ص 72 ... أنظر إلى المادة 260 من قانون العقوبات الأردني.

لم ينص قانون العقوبات على تجريم الدخول غير المصرح به أو غير المشروع باستخدام الوسائل التقنية إلى النظام المعلوماتي، ولم يجرم البقاء غير المصرح به أو تواجد الفاعل داخل الأنظمة المعلوماتية دون موافقة صاحبها، ولم ينص على تجريم انتهاك الحياة الخاصة عبر الأنظمة التقنية والمعلوماتية كجمع البيانات أو تخزينها أو إفشاؤها أو إساءة استعمالها على نحو غير مشروع أو الاعتداء على سرية الاتصالات والمراسلات، لكنه أشار في المواد 355 - 357 إلى جريمة إفشاء الأسرار الرسمية والمهنية¹، ويستفاد من هذه النصوص بأن الحماية المقررة بموجبها وتحتصر إطار التجريم في المعلومات السرية والرسمية والمهنية التي حصل عليها الفاعل بحكم وظيفته، ولا تشمل صور الانتهاكات الخصوصية للأفراد باستخدام الوسائل التكنولوجية، مما يستوجب وضع الحماية القانونية لخصوصية الأفراد.

نصت المادة 417 من قانون العقوبات على جريمة الاحتيال التقليدية ولم ينص على وسائل الاحتيال المعلوماتية كتغيير أو إعاقة أو التلاعب بالمعلومات والبيانات والبرامج أثناء عملية إدخالها أو إخراجها أو استعمال شيفرات غير صحيحة للدخول إلى أنظمة تقنية مدفوعة الأجر، ومن خلال استعراض ركنها المادي المتمثل في النشاط الإيجابي باستخدام الطرق والوسائل الاحتيالية لإيهام المجني عليه بمشروع كاذب وحدوث النتيجة أي تسليم المال إلى الجاني وتوفر العلاقة السببية بين الفعل والنتيجة مع علم الجاني بعناصر جريمة الاحتيال واتجاه إرادته لتحقيق النتيجة ونية التملك، وقد بين المشرع الأردني جريمة التجسس في المواد 124 - 126 ولم يتناول جرائم التجسس المعلوماتي رغم خطورتها².

يتضح مما سبق عجز انطباق هذه النصوص على الجرائم المستحدثة، ومن أهم الأسباب التي تحول دون تطبيق نصوص القوانين التقليدية على الجرائم المعلوماتية تتمثل في كونها وضعت قبل ظهور وتبلور الجرائم المعلوماتية، حيث أن المبدأ الأساسي الذي يحكم القانون الجنائي هو مبدأ شرعية الجرائم والعقوبات حيث "لا جريمة ولا عقوبة إلا بنص قانوني"، أضف إلى ذلك عدم جواز التوسع في تفسير النصوص الجزائية.

¹ المومني، نهلا: مرجع سابق: ص 155 - 185. .. أنظر إلى المواد 355 - 357 من قانون العقوبات الأردني.

² المومني، نهلا: مرجع سابق، ص 207 - 209. أنظر إلى المواد 124 - 126 و 417 من قانون العقوبات الأردني.

واكب المشرع الأردني التطورات الناتجة عن ثورة المعلومات والاتصالات وما رافقها من ظهور جرائم مستحدثة بإصدار قانون الجرائم الإلكترونية رقم 27 لسنة 2015، في حين استمر تطبيق قانون العقوبات الأردني رقم 16 لسنة 1960 في المحاكم الفلسطينية والذي لا يلبي الحد الأدنى لملاحقة ومكافحة وردع مرتكبي الجرائم الإلكترونية.

الفرع الثاني: قانون رقم 3 لسنة 1996 بشأن الاتصالات السلكية واللاسلكية¹

تناول هذا القانون نصوص قانونية محدودة تشير في مضمونها إلى بعض أنواع الجرائم الإلكترونية، وكانت هذه النصوص الوحيدة التي تسعف النيابة العامة والقاضي الجزائي الفلسطيني في ملاحقة مرتكبي هذه الجرائم قبل صدور القرار بقانون بشأن الجرائم الإلكترونية. حيث نصت المادة 91 منه على جريمة التهديد أو الإهانة بأي وسيلة من وسائل الاتصالات وفرض عقوبة الحبس أو الغرامة، وفي حال ارتكابها من قبل مزود الخدمة يعاقب بإلغاء أو سحب ترخيصه² ففي حال ارتكاب المتهم فعل التهديد والإهانة عبر الهاتف خلافاً لهذا النص يعاقب بالحبس وجعل مدة الحبس سلطة تقديرية لقاضي الموضوع وفي حال وجود مصلحة وأسقاط حق شخصي تقرر المحكمة تحويل مدة الحبس إلى غرامة بواقع نصف دينار عن كل يوم³، وهذه العقوبة سواء الحبس أو الغرامة لا تحقق الردع لمرتكبيها مما دفع المشرع الفلسطيني إلى استحداث قانون عصري يتناسب مع تطور تلك الجرائم.

الفرع الثالث: القرار بقانون رقم (15) لسنة 2009 بشأن الهيئة الفلسطينية لتنظيم قطاع الاتصالات

جاء هذا القرار بقانون بمجموعة من النصوص القانونية التي تبين الأفعال المجرمة التي تقع على شبكة الاتصالات، حيث نصت المادة 52 على جريمة نشر وإشاعة الاتصالات المتحصل

¹ صدر هذا قانون في مدينة غزة بتاريخ 1996/1/18، عن الرئيس ياسر عرفات، وقد تم نشره في جريدة الوقائع الفلسطينية في العدد 12، صفحة 7، بتاريخ 1996/4/23م، والذي بدء العمل به بعد ثلاثين يوماً من تاريخ نشره بموجب المادة 105 منه.

² المادة 91 من ذات القانون المشار اليه.

³ الحكم الصادر في الدعوى الجزائية 2016/1542 بتاريخ 2017/9/18، صلح نابلس.

عليها بحكم الوظيفة بدون مسوغ قانوني، وحددت المادة 57 من هذا القرار بقانون جريمة التهديد والإهانة بأي وسيلة تقنية، كذلك نصت المادة 58 على الاعتراض أو إعاقة أو تغيير وشطب محتويات الرسائل المرسلة بواسطة شبكات الاتصالات¹. جرمت هذه النصوص العديد من الأفعال كالتهديد أو الإهانة أو الاعتراض على الرسائل ومحتوياتها من خلال شبكة الإنترنت والاتصال، وفرض عقوبة الحبس ما بين شهر إلى سنة أو غرامة مالية 200 - 1200 دينار إلا أن هذه العقوبات لا تتناسب مع طبيعة الفعل المرتكب مما يتطلب إعادة النظر بها لتحقيق ردع مرتكبيها².

الفرع الرابع: قرار بقانون رقم 15 لسنة 2017 بشأن المعاملات الإلكترونية

جاء هذا القرار بقانون انسجاماً مع رؤية الحكومة الفلسطينية الارتقاء بالخدمات العامة وتقديمها إلكترونياً في دولة فلسطين بهدف تنظيم وتسهيل المعاملات الإلكترونية من خلال إرساء وتطوير البنية القانونية والأنظمة واللوائح والمعايير الخاصة بتطبيق المعاملات الإلكترونية محلياً ودولياً بالإضافة إلى المنع والحد من حالات الاحتيال والتزوير في المراسلات والمعاملات الإلكترونية. تناول القرار بقانون مهام واختصاصات وزارة الاتصالات وتكنولوجيا المعلومات، والأثار القانونية المترتبة على المعاملات الإلكترونية وطرق حمايتها، والسندات الإلكترونية، والتحويل الإلكتروني للأموال، والتوقيع الإلكتروني، والتوقيعات الإلكترونية الأجنبية، والجرائم والعقوبات³.

منح هذا القرار بقانون وزارة الاتصالات صلاحيات إغلاق مراكز تقديم خدمات المصادقة الإلكترونية أو التوقيع الإلكتروني أو إلغاء رخصتها أو بإيقافها لمدة محدودة حال مخالفتها شروط الترخيص أو القانون. ويعاقب المرخص له في حال عدم إخطار الوزارة بأي تغيير في

¹ المادة 52 و57 و58 من القرار بقانون المشار اليه.

² صدر هذا القرار بقانون في مدينة رام الله بتاريخ 2009/6/4، عن الرئيس محمود عباس، وقد تم نشره في جريدة الوقائع الفلسطينية في العدد 82، صفحة 6، بتاريخ 2009/8/22م، والذي بدء العمل به من تاريخ نشره بموجب أحكام المادة 67 منه.

³ قرار بقانون رقم 15 لسنة 2017 بشأن المعاملات الإلكترونية، الصادر في مدينة رام الله عن رئيس دولة فلسطين بتاريخ 2017/6/15، منشور في الجريدة الرسمية الفلسطينية، ممتاز عدد 14، بتاريخ 2017/7/9، ص2.

البيانات المقدمة لحصوله على رخصة تقديم الخدمات الإلكترونية وفرض عقوبة على كل من قدم بشكل متعمد بيانات غير صحيحة للحصول على رخصة تقديم خدمات الكترونية¹.

المطلب الثاني: القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية

يعتبر هذا القانون حاجة أساسية وضرورية للمجتمع الفلسطيني في ظل التغيرات التكنولوجية وتطورها، ونتيجة للالتزامات المترتبة على دولة فلسطين بعد انضمامها إلى الاتفاقيات الدولية والإقليمية حول الجرائم المعلوماتية التي حثت الدول الأعضاء على اتخاذ تدابير تشريعية لإصدار قانون الجرائم الإلكترونية، حيث صادق رئيس دولة فلسطين على قرار بقانون بشأن الجرائم الإلكترونية رقم 16 لسنة 2017 بتاريخ 2017/6/24 وأصبح هذا القرار ساري المفعول بتاريخ نشره 2017/7/9². وفي الفرع الأول من هذا المطلب تم تناول القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية من الناحية الموضوعية، أما الفرع الثاني فتناول الجرائم الإلكترونية من الناحية الإجرائية، وفي الفرع الثالث تم إجمال الملاحظات حول القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية.

الفرع الأول: الناحية الموضوعية

سيتم دراسة القرار بقانون من الناحية الموضوعية، هناك نوعين من الجرائم: جرائم تقع بواسطة الوسائل الإلكترونية وهي جرائم أمن دولة، جرائم واقعة على الأشخاص، وجرائم تقع على الأموال، وجرائم مخلة بالآداب العامة، إضافة إلى جرائم تقع على النظام الإلكتروني أو الحاسب الآلي منها جرائم متعلقة بأنظمة البيانات والاعتداء عليها وجرائم التزوير الإلكتروني والبيانات الكاذبة.

¹ قرار بقانون رقم 15 لسنة 2017 بشأن المعاملات الإلكترونية، الصادر في مدينة رام الله عن رئيس دولة فلسطين بتاريخ 2017/6/15، منشور في الجريدة الرسمية الفلسطينية، ممتاز عدد 14، بتاريخ 2017/7/9. ص 2.

² قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، الصادر في مدينة رام الله عن رئيس دولة فلسطين بتاريخ 2017/6/24، منشور في الجريدة الرسمية الفلسطينية، ممتاز عدد 14، بتاريخ 2017/7/9. ص 15.

أولاً: جرائم تقع بواسطة الكترونية

تختلف الجرائم المعلوماتية باختلاف طبيعتها فمنها جرائم أموال، أو أشخاص، أو أمن دولة، أو جرائم مخلة بالنقطة والآداب العامة، أو جرائم متعلقة بالاعتداء على البيانات وأنظمتها، وجرائم التزوير الإلكتروني والبيانات الكاذبة، ويرجع هذا الاختلاف إلى محل السلوك الإجرامي ووسيلة ارتكابها.

1. جرائم أمن دولة

يُعد استخدام التقدم التكنولوجي الحديث ومختلف شبكات الاتصال، بيئة ملائمة لوقوع هذه الجرائم عبر الوسائل الإلكترونية المختلفة، سواءً جرائم تمس أمن الدولة الداخلي أو الخارجي وذلك من خلال استخدام أجهزة الحاسب الآلي وشبكات الإنترنت¹. نصت المادة 20 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية على " 1. كل من أنشأ موقعاً إلكترونياً 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 كليهما 2. كل من روج 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 كليهما 3. إذا كان الفعل الوارد في الفقرتين (1،2) من هذه المادة في حالة الطوارئ تضاعف العقوبة المقررة له " 2، احتوى هذا النص على مصطلحات فضفاضة تمنح احتمالية أوجه التفسير والتأويل خلافاً لمبدأ شرعية الجرائم والعقوبات، وقد تشكل اعتداءً أو تقييد على الحقوق والحريات العامة من خلال تأويل تلك المصطلحات وفرض عقوبات شديدة لا تتناسب مع طبيعة الفعل المرتكب، وأشار إلى إحدى الحالات التي استخدم فيها هذا النص وهي اعتقال خمسة من الصحفيين وتوقيفهم من قبل النيابة العامة وتمديد توقيفهم من قبل

¹ منصور، محمد حسين: المسؤولية الإلكترونية، دار النهضة العربية، القاهرة، ط 2، 2004. ص148.

² المادة 20 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية.

القضاء الفلسطيني، ويلاحظ بأن هذه الجرائم لا تندرج تحت اطار الجرائم الإلكترونية في اتفاقية بودابست¹، وبناء على الالتزامات المترتبة على دولة فلسطين بموجب هذه الاتفاقية وحماية للحقوق والحريات العامة يجب إعادة صياغة هذا النص أو توضيح هذه المصطلحات لعدم فرض القيود على حرية التعبير عن الرأي وفقاً للمعايير الدولية.

نصت المادة 21 على "كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات بقصد الإساءة أو سب إحدى المقدسات أو الشعائر المقرر للأديان أو إحدى 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 كليهما"². استخدام هذا النص مصطلح شامل وعام "الإساءة للمقدسات والشعائر الدينية" وقد يشكل تقييد على حرية التعبير في حالة انتقاد الأديان وعلماء الدين الذي لم يرد في اتفاقية بودابست الخاصة بالجرائم الإلكترونية، ويخالف ما نصت عليه لجنة لحقوق الإنسان في تعليقها العام رقم 34 فقرة 48 بعدم جواز حظر حالات انتقاد رجال الدين أو التعليق على المذاهب الدينية أو المبادئ العقائدية أو المعاقبة عليها³. مما يتطلب إعادة النظر بذلك المصطلح من خلال تحديد مفهومه وتفسيره وفق إرادة المشرع.

نصت المادة 24 على "كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً 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

¹ ملاحظات مؤسسة الحق على القرار بقانون بشأن الجرائم الإلكترونية رقم 16 لسنة 2017، بتاريخ 2017/10/2، رام الله، ص 10.

² المادة 21 من القرار بقانون المشار اليه.

³ ملاحظات مؤسسة الحق على القرار بقانون بشأن الجرائم الإلكترونية رقم 16 لسنة 2017، بتاريخ 2017/10/2، رام الله، ص 11.

الأف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً¹. استخدام هذا النص مصطلح "إثارة النعرات العنصرية" وقد لا يصلح وضعه في النصوص الجزائية لاعتباره قيداً على حرية التعبير واستخدامه في اعتقال الصحفيين والمواطنين بسبب آرائهم، كما فرض ذات النص عقوبات جزائية مشددة لا تتناسب مع طبيعة الفعل المرتكب، يلاحظ بان هذا الفعل يخرج عن إطار الجرائم الإلكترونية ولا يندرج ضمن القيود الواردة في المادة 19 من العهد الدولي الخاص بالحقوق المدنية والسياسية². مما يتطلب إعادة صياغة هذا النص بما ينسجم مع الاتفاقيات والمعاهدات الإقليمية والدولية التي تعتبر دولة فلسطين عضواً فيها.

2. جرائم واقعة على الأشخاص

تقع هذه الجرائم على الأشخاص بوصفهم محلاً للجريمة، بواسطة النظام الإلكتروني عبر أدواته المختلفة وشبكات الاتصال المحلية والدولية³. نصت المادة 15 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية على "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 مشروعاً يعاقب بالحبس أو بغرامة لا تقل عن ألفي دينار أردني ولا تزيد عن خمسة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً². وإذا كان التهديد بارتكاب جناية أو بإسناد أمور خادشه للشرف أو الاعتبار يعاقب بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن ألفي دينار أردني ولا تزيد عن خمسة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً⁴، لم يوضح هذا النص ما المقصود بمصطلح "الابتزاز والتهديد" فقد يكون هنالك تهديد بالقتل وهي جناية أو الإيذاء التي تعد من قبيل الجنيح⁵، وجاءت الفقرة الثانية بنطاق واسع في التجريم غير المبرر كالتهديد بإسناد أمور خادشه للشرف أو الاعتبار، وفرض

¹ المادة 24 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية.

² ملاحظات مؤسسة الحق على القرار بقانون بشأن الجرائم الإلكترونية رقم 16 لسنة 2017، بتاريخ 2017/10/2، رام الله، ص4 و ص 12.

³ المناعسة، والزعبي، مرجع سابق، ص90.

⁴ المادة 15 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية.

⁵ ملاحظات مؤسسة الحق على القرار بقانون بشأن الجرائم الإلكترونية رقم 16 لسنة 2017، بتاريخ 2017/10/2، رام الله، ص9.

عقوبات مشددة وهي الأشغال الشاقة المؤقتة كما استخدم عقوبات جنائية وجنحوية في ذات النص¹، وهذا يستدعي إضافة تعريف لتوضيح المصطلحات المذكورة بهذا النص خشية الخروج عن فلسفة المشرع من التجريم.

نصت المادة 22 من ذات القرار بقانون على "كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً 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 كانت مباشرة أو مسجلة تتصل بحرمة الحياة الخاصة أو العائلية للأفراد ولو كانت صحيحة أو تعدى بالذم أو القبح أو التحقير أو التشهير بالآخرين وإلحاق الضرر بهم يعاقب بالحبس مدة لا تقل عن سنتين أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد على خمسة آلاف دينار أردني أو بالعقوبتين كليهما"²، يستخدم هذا النص مصطلح فضفاض الاعتداء على القيم والمبادئ الأسرية قد يقيد حرية التعبير، ولم يفرق بين جرائم القبح والذم الواقعة على الشخصيات العامة والأشخاص العاديين إذا ورد بحسن نية، إضافة على ذلك أكدت لجنة المعنية بحقوق الإنسان على نزع صفة التجريم عن التشهير (الذم والقبح) في القوانين الجنائية في تعليقها العام رقم 34 فقرة 47³، مما ينبغي الاستعاضة عن هذا النص بنصوص قانونية مدنية حول التشهير (التعويض المدني).

3. جرائم واقعة على الأموال

ساهم التقدم التكنولوجي في إيجاد طرق جديدة لارتكاب الجرائم المعلوماتية في مختلف مجالات القطاعات الحياتية ومنها الأموال⁴، حيث تقع جرائم الأموال باستخدام النظام المعلوماتي كأداة أو

¹ مذكرة قانونية حول القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، الهيئة المستقلة لحقوق الإنسان، ص5.

² المادة 22 من القرار بقانون المشار اليه.

³ ملاحظات مؤسسة الحق على القرار بقانون بشأن الجرائم الإلكترونية رقم 16 لسنة 2017، بتاريخ 2017/10/2، رام الله، ص11.

⁴ السراج، عبود: قانون العقوبات الاقتصادي، ط7، دمشق، 1998، ص11.

وسيلة مثل جرائم السرقة والاحتيال¹، وتزيف العملة أو التزوير في المستندات الرسمية أو الاختلاس². ونصت المادة 13 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية على "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 ولا تزيد عن خمسة آلاف دينار أردني أو بالعقوبتين كليهما"³، تشدد هذا النص في العقوبات المفروضة وهي الأشغال الشاقة المؤقتة خلافاً لما ورد في جريمة السرقة في قانون العقوبات التي يمكن أن تكون جنائية إذا ارتكبت بظروف مشددة ويمكن أن تكون جنحة، بالإضافة إلى التوسع في إطار التجريم وربطها بأداة الجريمة بما لا يتناسب مع طبيعة الفعل المرتكب، ويخالف القواعد العامة في قانون العقوبات بإدراجه عقوبة الغرامة الجنحية مع العقوبة الجنائية⁴.

نصت المادة 18 من ذات القرار بقانون على "دون الإخلال بالحكام الواردة في قرار بقانون مكافحة غسل الأموال وتمويل الإرهاب كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات بقصد ارتكاب جريمة غسل الأموال وتمويل الإرهاب يعاقب بالأشغال الشاقة المؤقتة 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 قانوناً"⁵، تعاقب هذه المادة على القصد وهو الركن المعنوي للجريمة الذي يصعب إثباته عملياً في الجرائم الإلكترونية دون استكمال العناصر المكونة للركن المادي والتي تتمثل في وقوع النشاط الجرمي وحصول النتيجة الإجرامية والعلاقة السببية، ويستنتج من ذلك بفرض العقوبة دون استكمال عناصر وأركان الجريمة⁶. ويتطلب ذلك إعادة صياغة هذا

¹ قشقوش، هدى: مرجع السابق، ص 51 – 52.

² الهيتمي، محمد حماد مرهج، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة، عمان، ط1، ص46.

³ المادة 13 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية.

⁴ مذكرة قانونية حول القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، الهيئة المستقلة لحقوق الإنسان، ص5.

⁵ المادة 18 القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية.

⁶ ملاحظات مؤسسة الحق على القرار بقانون بشأن الجرائم الإلكترونية رقم 16 لسنة 2017، بتاريخ 2017/10/2، رام الله، ص2.

النص بما يتناسب مع فرض العقوبة عند تحقق كافة العناصر المكونة للجريمة بشقيها الركن المادي والمعنوي.

4. جرائم مخلة بالآداب العامة

سهل استخدام الوسائل التقنية الحديثة ارتكاب الجرائم المعلوماتية المخلة بالآداب العامة وذلك مثل جرائم تزوير، انتحال الشخصية والتهديد والابتزاز ونشر وترويج الأفكار من شأنها الإخلال بالنظام والآداب العامة¹. نصت المادة 16 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية على "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 كليهما 2. كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً 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 لا تقل عن ألف دينار أردني ولا تزيد عن خمسة آلاف دينار أردني أو بالعقوبتين كليهما 3. إذا كان الفعل المحدد في الفقرة 1 و2 من هذه المادة موجهاً 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 قانوناً 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 قانوناً"²، قد يشكل إساءة تطبيق هذا النص انتهاكاً للحرية الشخصية والحقوق والحريات العامة من خلال إدراج حالات حرية الرأي والتعبير في إطار التجريم ضمن

¹ حجازي، عبد الفتاح بيومي: الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، ط1، ص59.

² المادة 16 القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية.

مصطلح "الآداب العامة"، علماً أن اتفاقية بودابست قد حصرت نطاق التجريم الماسة باستغلال الأطفال في المواد الإباحية وهذا ما اتبعه المشرع الأردني في قانون الجرائم الإلكترونية رقم 27 لسنة 2015¹، وبناء على ذلك يفضل عدم وضع هذا النص في الجرائم الإلكترونية لخطورته على الحقوق والحريات العامة أو قيام المشرع الفلسطيني بتحديد مفهوم الآداب العامة لكي لا يساء استخدام ذلك النص في التطبيق العملي.

ثانياً: جرائم تقع على النظام الإلكتروني

جرائم واقعة على النظام المعلوماتي بمكوناته المادية أو المعنوية، فالجرائم التي تقع على مكوناته المادية عندما يكون أجهزة الحاسب الآلي أو الشبكة المعلوماتية محلاً للجريمة، وتتحقق نتيجة القيام بأعمال مادية تخرج حيازة الحاسوب من ماله لإدخاله في حيازة شخص آخر وهي²:

1. جرائم متعلقة بأنظمة البيانات والاعتداء عليها

نصت المادة 4 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية على "1. كل من دخل عمداً وبدون 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 كليهما 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 كليهما 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

¹ ملاحظات مؤسسة الحق على القرار بقانون بشأن الجرائم الإلكترونية رقم 16 لسنة 2017، بتاريخ 2017/10/2، رام الله، ص10.

² المناعسة، والزعبي: مرجع سابق، ص89.

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 قانوناً⁴. 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 قانوناً¹. كما نصت المادة 5 على "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 كليهما"². كما نصت المادة 7 على "كل من النقط 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 كليهما"³. تناولت هذه المواد جريمة الدخول غير المشروع إلى المواقع والأنظمة المملوكة للغير أو إعاقة الوصول إليها بما فيها المواقع والبيانات الحكومية، كذلك جرمت الاعتراض أو التسجيل أو التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية دون وجه حق.

نصت المادة 6 من ذات القرار بقانون على "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 إتلافها، أو تعديلها، يعاقب بالأشغال الشاقة المؤقتة وبغرامة مالية لا تقل عن خمسة آلاف دينار أردني، ولا تزيد على عشرة آلاف دينار أردني أو ما يعادلها

¹ المادة 4 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية.

² المادة 5 من القرار بقانون المشار اليه.

³ المادة 7 من القرار بقانون المشار اليه.

بالعملة المتداولة قانوناً¹. يلاحظ بأن المشرع استخدم العقوبة الجنائية "الأشغال الشاقة المؤقتة" وعقوبة جنحوية "الغرامة" في ذات النص بشكل يتعارض مع القواعد العامة في تصنيف العقوبات، وفرض عقوبات مشددة لا تتناسب مع خطورة الفعل المرتكب استناداً لمبدأ شرعية الجرائم والعقوبات، ولم يفرق بين البرامج والأجهزة المشروعة التي يتم إنتاجها أو استخدامها في حماية الشبكات والمعلومات والبرامج غير المشروعة التي تتسبب في إتلاف أو تعطيل أو تدمير المعلومات والبيانات بطرق غير مشروعة كنشر الفيروسات الخبيثة². ويتطلب ذلك توضيح أو تفسير قصد المشرع من عبارة بصفة غير مشروعة، وإعادة النظر في العقوبات المفروضة بما تتناسب مع الفعل المرتكب وطبيعة الجريمة.

نصت المادة 8 على "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 كليهما 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 كليهما. 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 قانوناً³، ونصت المادة 9 على "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 كليهما 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

¹ المادة 6 من القرار بقانون المشار اليه.

² ملاحظات مؤسسة الحق على القرار بقانون بشأن الجرائم الإلكترونية رقم 16 لسنة 2017، بتاريخ 2017/10/2، رام الله، ص2.

³ المادة 8 من القرار بقانون المشار اليه.

تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما¹. لم يوضح المشرع الفلسطيني المقصود بعبارة "صفة غير مشروعة" وقد يتيح ذلك إلى فرض رقابة على ادوات التشفير الشخصية وإخفاء الهوية التي تستخدم لحماية الحق في الخصوصية وهذا يخالف ما قرره المفوض الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير من عدم جواز حظر أو فرض الرقابة على أدوات التشفير وإخفاء الهوية واعتبار استخدامها مكفول وفقاً للمعايير الدولية لحقوق الإنسان، كما فرض عقوبات مشددة ويخلط ما بين العقوبة الجنائية والجنحوية في ذات النص².

2. جرائم التزوير الإلكتروني والبيانات الكاذبة

نصت المادة 11 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية على "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 التوقيعات الإلكترونية في الفقرة (4) من هذه

¹ المادة 9 من القرار بقانون المشار اليه.

² ملاحظات مؤسسة الحق على القرار بقانون بشأن الجرائم الإلكترونية رقم 16 لسنة 2017، بتاريخ 2017/10/2، رام الله، ص8.

المادة، يعاقب بالحبس أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد عن ثلاثة آلاف دينار أردني، أو بالعقوبتين كليهما 5. 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 على ثلاثة آلاف دينار أردني، أو بالعقوبتين كليهما¹. عاقب هذا النص على تزوير المستندات الإلكترونية الرسمية والعرفية وتزوير التوقيعات الإلكترونية بالأشغال الشاقة (جناية) على كل من زور مستند رسمي إلكتروني من مستندات الدولة أو الهيئات والمؤسسات العامة، وفرض عقوبة جريمة التزوير الأصلية في حال استعماله للمستند المزور مع علمه بتزويره ويعد مرتكب جناية. وعاقب على تقديم بيانات كاذبة للجهات المختصة لإصدار شهادات التصديق الإلكتروني.

ثالثاً: أحكام عامة

فرض هذا القرار بقانون عقوبات متنوعة ومتشددة، ونص على المصادرة الجنائية والمساهمة والشروع في الجرائم الإلكترونية، وحالات تضاعف هذه العقوبات بحق مرتكبيها وحالات إعفائهم منها. كذلك تناول نصوص قانونية حول الحماية الإجرائية والتبليغ، بالإضافة إلى الالتزامات القانونية لمزودي خدمة الإنترنت والتعاون الدولي في مجال الجرائم الإلكترونية.

1. مدى تطبيق القانون مكانياً

استناداً إلى المادة 2 يطبق أحكام القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية على " على أي جريمة إلكترونية منصوص عليها بهذا القرار بقانون سواء ارتكبت بشكل كلي أو جزئي في فلسطين أو خارجها أو امتد أثرها داخل فلسطين، سواء كان فاعلاً أصلياً أو شريكاً أو متدخلًا أو محرضاً، شريطة أن تكون من الجرائم المعاقب عليها خارج فلسطين مع مراعاة قانون العقوبات الساري المفعول. كما أجازت ملاحقة كل شخص من خارج فلسطين يرتكب هذه الجرائم في إحدى الحالات التالية إذا ارتكبت من مواطن فلسطيني، أو ارتكبت ضد أطراف أو

¹ المادة 11 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية.

مصالح فلسطينية، أو ارتكبت ضد أطراف أو مصالح أجنبية من قبل أجنبي أو شخص عديم الجنسية ويوجد له محل إقامة معتاد في فلسطين أو وجد في فلسطين، ولم تتوافر شروط التسليم القانونية¹.

2. تنوع العقوبات باختلاف الجريمة الإلكترونية

فرض هذا القرار بقانون عقوبات متعددة على مرتكبي الجرائم الإلكترونية باستخدام أي وسيلة تقنية وتكنولوجية ضمن أحكام المواد 4 وحتى المادة 31، وجاءت هذه العقوبات متنوعة بين الغرامات المالية التي لا تقل عن 200 دينار ولا تتجاوز عن 20000 دينار والحبس بمدة لا تقل عن 6 أشهر ولا تتجاوز عقوبة الأشغال الشاقة المؤقتة أو بكلا العقوبتين، وتختلف هذه العقوبات باختلاف طبيعة ووسيلة ارتكابها.

3. فرض العقوبة الأشد حال ارتكاب أي جريمة معاقب عليها في تشريع نافذ

نصت المادة 45 على عقوبة مرتكبو الجرائم الإلكترونية بالعقوبة الأشد المنصوص عليها في قانون العقوبات النافذ أو أي قانون آخر، وعاقبت المادة 46 كل من ارتكب فعل يشكل جريمة بموجب أي تشريع نافذ باستخدام الوسائل التقنية أو اشترك أو تدخل فيها أو حرض على ارتكابها بذات العقوبة المقررة لتلك الجريمة في ذات التشريع، وبموجب المادة 47 يعاقب بالسجن المؤقت وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني لكل من أنشأ موقع الكتروني بهدف الترويج لارتكاب أية جريمة إلكترونية². تعتمد هذه النصوص على الوسيلة المستخدمة في ارتكاب الجريمة والتوسع في إطار الجرائم الإلكترونية خلافاً لما جاء في اتفاقية بودابست، وفرض عقوبات قاسية تصل إلى السجن المؤقت ودمجها مع العقوبة الجنحوية وهي الغرامة خلافاً للقواعد العامة لتصنيف قانون العقوبات³.

¹ المادة 2 من القرار بقانون المشار اليه.

² المواد 45 و46 و47 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية.

³ ملاحظات مؤسسة الحق على القرار بقانون بشأن الجرائم الإلكترونية رقم 16 لسنة 2017، بتاريخ 2017/10/2، رام الله، ص18.

4. المصادرة الجنائية

نصت المادة 54 فقرة 1 و2 على المصادرة الجنائية وإغلاق المحل أو الموقع كعقوبة ثانوية يحكم بها بجانب العقوبة الأصلية مع عدم الإخلال بحقوق الغير "حسن النية"، وجاء فيها تصدر المحكمة قرارها بالمصادرة أو بإغلاق المحل أو الموقع الإلكتروني الذي ارتكبت فيه أو بواسطته الجرائم الإلكترونية¹، فالمصادرة ترد على الوسائل الإلكترونية وبرامجها وإغلاق مواقع ارتكاب الجريمة وفق مدة تقدرها المحكمة وفق سلطتها التقديرية. وقد يمس هذا النص بالقناعة الوجدانية للقاضي ومن خلال إلزامه بمصادرة الأجهزة والوسائل أو البرامج المستخدمة وكذلك بإقفال المحل وحجب المواقع الإلكترونية².

5. المساهمة التبعية والشروع في الجرائم الإلكترونية

نصت المادة 52 و53 على المساهمة التبعية في الجريمة المعلوماتية والشروع في ارتكابها، بحيث يعاقب بعقوبة الفاعل الأصلي كل من يشترك عن طريق الاتفاق أو التحريض أو المساعدة أو التدخل في ارتكاب جنائية أو جنحة معاقب عليها بهذا القرار بقانون، وفي حال عدم وقوع الجريمة أو الشروع في ارتكابها يعاقب بنصف العقوبة المقررة لها³. يشكل هذا النص خروجاً عن القواعد العامة في الاشتراك الجرمي من حيث العقوبة المفروضة مما يتطلب مراجعتها.

6. حالات تضاعف العقوبة على مرتكبي الجرائم الإلكترونية

ذكرت المواد 55 و56 حالات تضاعف وتشديد العقوبة حال ارتكاب الجرائم الإلكترونية في فلسطين أو خارجها، وتتمثل في تكرار الجاني ارتكابها وحال ارتكابها من قبل موظف عام أو من في حكمه أو موظف خاص مستغلاً صلاحياته وسلطاته، ووقوعها على الأنظمة والمواقع

¹ المادة 54 من القرار بقانون المشار اليه.

² ملاحظات مؤسسة الحق على القرار بقانون بشأن الجرائم الإلكترونية رقم 16 لسنة 2017، بتاريخ 2017/10/2، رام الله، ص20.

³ المواد 52 و53 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية.

الإلكترونية والبيانات الحكومية، وفي حال وقوعها أثناء تقديم أي خدمة مصرفية تقدمها البنوك والشركات المالية¹.

7. الإعفاء من العقوبة

أعفى المشرع الجاني من العقوبة وفق نص المادة 57 في حال مبادرته بإبلاغ الجهات المختصة بالمعلومات حول الجريمة ومرتكبيها قبل علم السلطات المختصة بها وقبل حدوث الضرر، مع منح المحكمة السلطة الجوازية بوقف تنفيذ العقوبة حال الإبلاغ بعد علم السلطة المختصة بها وأدى ذلك إلى ضبط باقي الجناة².

8. التشدد في العقوبات

فرض عقوبات متشددة المتمثلة بالحبس بالأشغال الشاقة المؤبدة أو الموقته وغرامات مالية باهظة تصل في بعض الأحيان إلى عشرين ألف دينار، التي قد لا تتناسب مع الواقع الفلسطيني مما يتطلب إعادة النظر في العقوبات المالية لتصبح أكثر انسجاماً مع المجتمع الفلسطيني.

9. العبث بالأدلة المعلوماتية والامتناع عن التبليغ

فرضت المادة 48 على عقوبة الحبس والغرامة على كل من أفشى سرية الإجراءات المنصوص عليها في القرار بقانون بشأن الجرائم الإلكترونية في غير الأحوال المصرح بها قانوناً يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن ألف دينار ولا تزيد على خمسة آلاف دينار أردني، ونصت المادة 49 على ذات العقوبة لمن يعبث بالأدلة القضائية المعلوماتية أو قام بإتلافها أو عمل على إخفائها أو تعديلها أو محوها، وعاقبت بالحبس لمدة لا تقل عن ستة شهور وبغرامة لا تقل عن مائتي دينار ولا تزيد على ألف دينار أردني لكل من امتنع بقصد عن إبلاغ أو إبلاغ خاطئ مقصود عن جرائم الكترونية كما جاء في المادة 50³. يلاحظ غياب النصوص

¹ المواد 55 و56 من القرار بقانون المشار اليه.

² المادة 57 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية.

³ المواد 48 و49 و50 من القرار بقانون المشار اليه.

التي تحدد طبيعة وما هي الإجراءات السرية التي قد تشكل وسيلة لانتهاك الحق في الوصول إلى المعلومة مما يستوجب الإشارة إلى الإجراءات ذات الطبيعة السرية في أحكام القرار بقانون عند تعديله¹، ولم ينص على عقوبة الفصل من الوظيفة حال ارتكاب هذه الأفعال من قبل الموظف، بالإضافة إلى عدم تناسب العقوبة مع خطورة الفعل كإفشاء أسرار حرمة الحياة الخاصة بالأفراد، كما فرض هذا النص عقوبة على الامتناع عن إبلاغ حال وقوع جريمة الكترونية خلافاً للتشريعات العقابية التي لا تجرم هذا الفعل.

10. الالتزامات القانونية لمزودي خدمة الإنترنت والتعاون الدولي في الجرائم المعلوماتية

نصت المادة 32 على "الالتزامات المفروضة على مزودي خدمة الإنترنت تمثلت في تزويد الجهات المختصة بجميع البيانات والمعلومات اللازمة التي تساعد في كشف الحقيقة، بناءً على طلب النيابة أو المحكمة المختصة². 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"². كما ألزمت المادة 42 أجهزة ومؤسسات الدولة اتخاذ التدابير الأمنية الوقائية لحماية أنظمتها وبياناتها الإلكترونية، والاحتفاظ ببيانات ومعلومات المشتركين لمدة لا تقل عن 120 يوماً، منح هذا النص النيابة العامة حجب المواقع الإلكترونية في مرحلة التحقيق الابتدائي والكشف عن البيانات الشخصية المشتركين دون الحاجة إلى حكم قضائي بشكل مخالف للمعايير الدولية والحق في الخصوصية³، وهذا يوجب حصر تعريف معلومات المشتركين في المادة الأولى من القرار بقانون لتشمل المعلومات العامة مثل (نوع الخدمة ومدتها، هوية المشترك، الشروط الفنية) دون الخوض في

¹ ملاحظات مؤسسة الحق على القرار بقانون بشأن الجرائم الإلكترونية رقم 16 لسنة 2017، بتاريخ 2017/10/2، رام الله، ص19.

² المادة 32 و42 من القرار بقانون المشار اليه.

³ ملاحظات مؤسسة الحق على القرار بقانون بشأن الجرائم الإلكترونية رقم 16 لسنة 2017، بتاريخ 2017/10/2، رام الله، ص13 و ص14.

محتواها حفاظاً على خصوصية وسرية الأفراد وان يكون حجب المواقع بموجب قرار قضائي دون منح هذه الصلاحية للنياابة العامة.

كما تناولت المواد 43 و44 موضوع التعاون الفلسطيني الدولي في مجال الجرائم الإلكترونية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصادق عليها شريطة التزام الدول الأجنبية بالحفاظ على سرية المعلومات المحالة إليها وتسليم المجرمين خلال إجراءات التحقيق¹. لم يحدد هذا النص القانون الواجب التطبيق حال ارتكاب جريمة إلكترونية دولية، ولم يحدد الفترة الزمنية لحفظ المعلومات من قبل الدول الأطراف. وقد يتعارض مع المادة 28 من القانون الأساسي الفلسطيني التي لا تجيز تسليم الفلسطيني إلى أي جهة أجنبية ويجب أن تتم محاكمته داخل فلسطين².

الفرع الثاني: الناحية الإجرائية

بهدف تحقيق الأمن والاستقرار وتطبيق القانون والوقاية والحد ومكافحة الجرائم الإلكترونية في فلسطين أنيط بجهاز الشرطة الفلسطينية ملاحقة مرتبكي هذه الجرائم من خلال وحدة الجرائم الإلكترونية وكذلك بواسطة نيابة الجرائم الإلكترونية في النيابة العامة وإصدار الأحكام القضائية من خلال المحاكم.

أولاً: دور جهاز الشرطة

انطلاقاً من مهام جهاز الشرطة الفلسطيني بالحفاظ على الأمن والنظام العام وتطبيق القانون من أجل الحفاظ على سلامة أمن المجتمع وحماية الحرية الشخصية للأفراد، ودورها في بناء دولة القانون وتعزيز مبدأ سيادة القانون وفي محاربة الجريمة وضبطها، أنشئت وحدة الجرائم الإلكترونية في جهاز الشرطة لمكافحة الجرائم الإلكترونية في فلسطين³.

¹ المواد 43 و44 من القرار بقانون المشار اليه.

² المادة 28 من القانون الأساسي الفلسطيني لسنة 2003 وتعديلاته.

³ مقابلة أجراها الباحث مع مدير وحدة الجرائم الإلكترونية التابعة لإدارة المباحث في جهاز الشرطة الفلسطيني سامر الهندي بمدينة رام الله بتاريخ 14.8.2017.

1. وحدة الجرائم الإلكترونية

تشكل هذه الوحدة إحدى الوحدات الحديثة في جهاز الشرطة، حيث أنشئت بقرار من مدير عام الشرطة في النصف الثاني من العام 2013 وتتبع للمباحث العامة، وتتكون من قسم متابعة شكاوى الإنترنت ومختبر الأدلة الإلكترونية وقسم متابعة جرائم الاتصالات بالإضافة إلى قسم التوعية والإرشاد والدائرة القانونية. وعدد العاملين فيها لا يتجاوز 12 شخص وبالإضافة إلى عدد من الضباط موزعين على كافة المحافظات بواقع 2-3 في كل محافظة، وتختلف مؤهلات العاملين في الوحدة (الإدارة العامة) عن العاملين في المحافظات، فالعاملين في وحدة الجرائم الإلكترونية بالإدارة العامة معظمهم خريجي البرمجة والهندسة الإلكترونية وهندسة الحاسوب كما تضم هذه الوحدة مجموعة من الضباط المحققين (خريجو قانون)، أما العاملين في أفرع الشرطة في المحافظات فأغلبهم خريجي القانون والعلوم الشرطية. وتتنوع مؤهلاتهم العلمية وفق احتياجات جهاز الشرطة. يقدم جهاز الشرطة مجموعة من التدريبات للعاملين فيها تمثلت في مسرح الجريمة وضبط الدليل الرقمي وفحص الأدلة والمضبوطات الرقمية وآلية متابعة جرائم الاتصالات واحتياجاتها¹.

2. آلية عمل وحدة الجرائم الإلكترونية

تعمل هذه الوحدة من خلال الضباط والعاملين فيها في الأفرع والمحافظات على استقبال الشكاوى من المواطنين، ويتم التعامل مع تلك الشكاوى مباشرة حسب الأصول والقانون، أما الشكاوى التي تحتاج إلى متابعة إلكترونية متقدمة فيتم إحالتها إلى وحدة الجرائم الإلكترونية في وحدة المباحث العامة التي تقوم بدورها في البحث والتحري الإلكتروني وجمع الاستدلالات الإلكترونية بالتعاون مع وحدة الجرائم الإلكترونية في مكتب النائب العام، وبعد الوصول إلى

¹ مقابلة أجراها الباحث مع مدير وحدة الجرائم الإلكترونية التابعة لإدارة المباحث في جهاز الشرطة الفلسطيني سامر الهندي بمدينة رام الله بتاريخ 14.8.2017.

الفاعل يتم إعادة نتائج التحقيق إلى الجهة المستقبلية للشكوى ومن ثم إحالتها إلى المحكمة المختصة¹.

3. الخصوصية والسرية

وفقاً لمتطلبات القرار بقانون لا يتم متابعة أي حساب أو خدمة الكترونية إلا بوجود شكوى، ولا يتم النفاذ إلى أي جهاز مضبوط إلا بوجود مذكرة وإذن خاص من النيابة العامة بالسماح بالنفاذ المباشر لهذا الجهاز وذلك حرصاً على خصوصية المواطنين. وفيما يتعلق بالسرية في متابعة الشكاوى يوجد نظام أرشفة إلكتروني ينظم عمل الوحدة يسمح لأفرادها الاطلاع إلا على الجزء المكلف به من الشكوى فقط، ويكون لمدير الوحدة والدائرة القانونية صلاحية الإلمام بتفاصيل الشكوى².

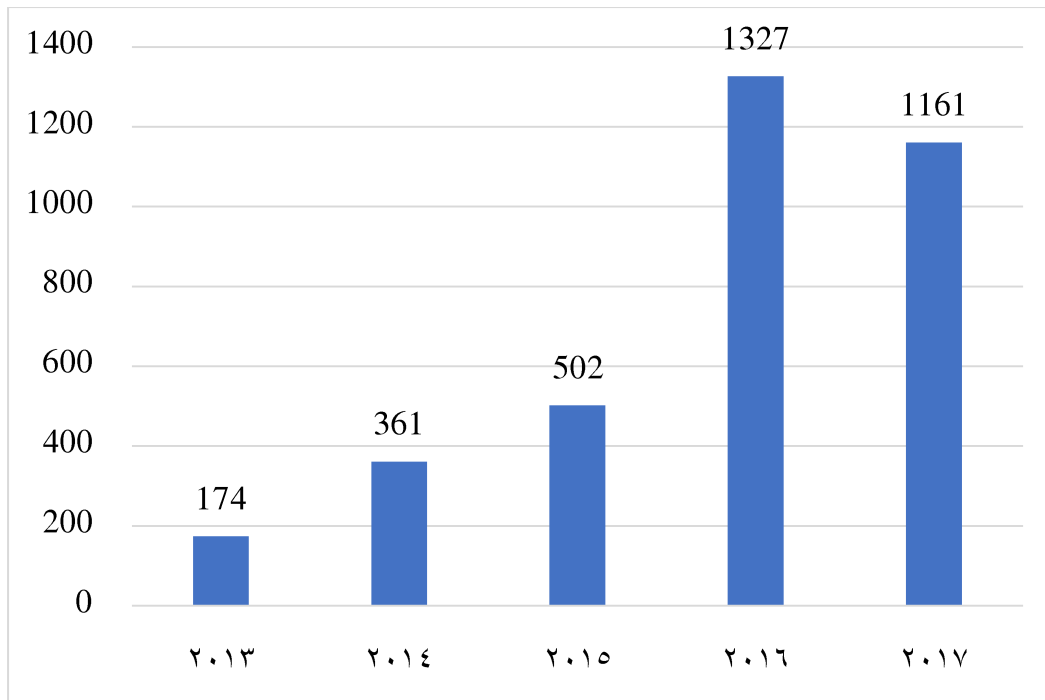
4. شكاوى الجرائم الإلكترونية ما بين 2013 - 2017

يبين الشكل رقم (1) عدد الشكاوى التي وصلت وحدة الجرائم الإلكترونية ما بين 2013 - 2017، حيث بلغ عددها 174 في العام 2013، وفي العام 2014 وصل إلى 361 شكوى بزيادة مقدارها 51.8%، وارتفع في العام 2015 إلى 502 شكوى بنسبة زيادة 65.3%، في حين وصلت في العام 2016 إلى 1327 شكوى بزيادة 86.9%، ومنذ بداية العام 2017 ولغاية 14.8 قُدمت 1161 شكوى³، كما يتبين من الشكل رقم (1)، ويلاحظ بأن الجرائم الإلكترونية أصبحت ظاهرة منتشرة ومتزايدة في فلسطين يجب الحد منها ومكافحتها.

¹ مقابلة أجراها الباحث مع مدير وحدة الجرائم الإلكترونية التابعة لإدارة المباحث في جهاز الشرطة الفلسطيني سامر الهندي بمدينة رام الله بتاريخ 14.8.2017.

² مقابلة أجراها الباحث مع مدير وحدة الجرائم الإلكترونية التابعة لإدارة المباحث في جهاز الشرطة الفلسطيني سامر الهندي بمدينة رام الله بتاريخ 14.8.2017.

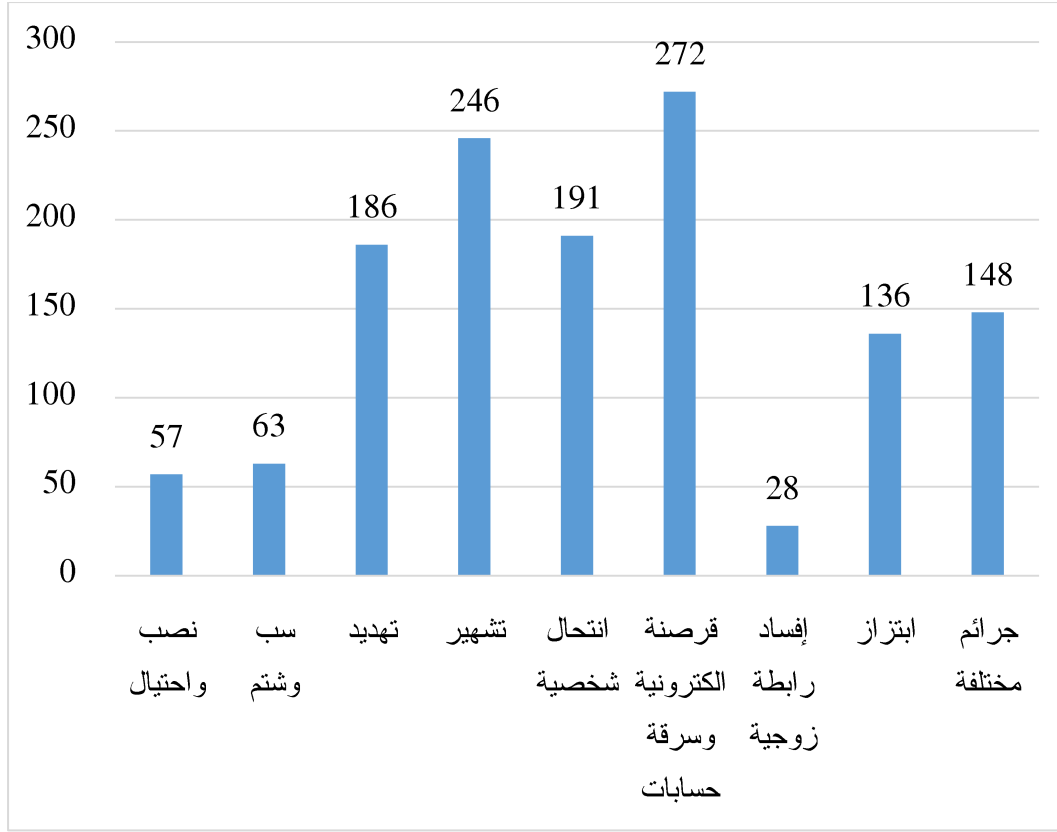
³ إحصائية حصل عليها الباحث من إدارة البحوث والتخطيط والتطوير في جهاز الشرطة الفلسطيني (غير منشورة).



الشكل رقم 1: أعداد الشكاوى المقدمة لدى وحدة الجرائم الإلكترونية في جهاز الشرطة الفلسطيني للأعوام 2013 حتى 14.8.2017.

صنفت وحدة الجرائم الإلكترونية في جهاز الشرطة الشكاوى الواردة لديها حسب نوع الجريمة المرتكبة للعام 2016 كما يلي: احتلت المركز الأول القرصنة الإلكترونية وسرقة الحسابات وبلغ عددها 272 قضية، يليها التشهير حيث وصل عددها إلى 246 قضية، واحتلت انتحال الشخصية المرتبة الثالثة بواقع 191 قضية، وفي المرتبة الرابعة التهديد بلغت 186 قضية، يليها الجرائم المختلفة 148 قضية، والابتزاز 136 قضية، والسب والشتم 63 قضية، والنصب 57 قضية، وإفساد الرابطة الزوجية 28 على التوالي كما يتبين من الشكل رقم (2). ومن الجدير ذكره أن عدد الجرائم الواقعة على الذكور بلغت 59%، وعلى الإناث 36%، و5% على المؤسسات¹.

¹ إحصائية حصل عليها الباحث من وحدة الجرائم الإلكترونية في جهاز الشرطة الفلسطيني (غير منشورة).



الشكل رقم 2: تصنيف الجرائم الإلكترونية الواردة إلى وحدة الجرائم الإلكترونية في جهاز الشرطة الفلسطيني حسب نوعها وعددها للعام 2016.

يلاحظ أن المادة 33 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية منحت النيابة العامة أو عضو الضبط القضائي المنتدب صلاحية تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات المتعلقة بالجريمة، كما أجازت المادة 40 لجهات التحري والضبط طلب الأذن من النائب العام أو أحد مساعديه بحجب المواقع الإلكترونية حال قيام أفعال تهدد الأمن القومي والسلم الأهلي والنظام العام والآداب العامة ويقدمها لمحكمة الصلح خلال 24 ساعة¹. منحت هذه النصوص النيابة العامة وهي "خصم في الدعوى الجزائية" اختصاص قضائي مما يشكل مساساً بضمانات الحق في الوصول إلى المعلومة، وإن أمر التفتيش الصادر عن النيابة العامة غير مقترن بمدة زمنية محددة وأجازت تجديده لأكثر من مرة طالما مبررات وأسباب إجراءات التفتيش قائمة شريطة أن يكون مأمور الضبط القضائي مؤهلاً للتعامل مع طبيعة

¹ المواد 33 و40 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية.

الجرائم الإلكترونية، كما منح النيابة العامة صلاحية حجب المواقع والاطلاع على أسرار المهنة دون الحصول على حكم قضائي مما يشكل مخالفة للمعايير الدولية¹. مما يستدعي تعديل هذا النص وتقيد مدة إذن التفتيش وحصر صلاحية حجب المواقع بحكم قضائي.

ثانياً: دور النيابة العامة

تعتبر النيابة العامة جزءاً أساسياً من منظومة السلطة القضائية، وهي تمثل المجتمع والحق العام من أجل الحفاظ على أمنه واستقراره، ومحاربة الجريمة والتصدي لها والتحقيق فيها وملاحقة مرتكبيها وإحالتهم إلى القضاء، وانطلاقاً من رؤيتها وفق خطتها الاستراتيجية بمجتمع فلسطيني يسوده القانون ومبدأ فصل السلطات واحترام الحقوق والحريات، قامت النيابة العامة بإنشاء نيابات متخصصة، ومنها نيابة حماية الأسرة من العنف، ونيابة الأحداث، ونيابة دعاوى الحكومة، ودائرة الجرائم الدولية والتعاون القضائي الدولي، وحديثاً نيابة مكافحة الجرائم المعلوماتية "الإلكترونية"².

1. تشكيل نيابة خاصة بالجرائم المعلوماتية

تنتشر ظاهرة الجرائم الإلكترونية في فلسطين بشكل متزايد مما يستدعي ضرورة التوقف عندها لمكافحتها والحد منها، لتحقيق ذلك أنشأت وحدة نيابة الجرائم الإلكترونية بقرار من النائب العام بتاريخ 2016/3/20، وتم تعيين 26 عضواً مختصين تقنياً وفنياً في التحقيق بجرائم تقنية المعلومات بين وكلاء ومعاونين نيابة في كل محافظة، وتتبع وتعمل تحت إشراف مباشر من قبل النائب العام³.

¹ ملاحظات مؤسسة الحق على القرار بقانون بشأن الجرائم الإلكترونية رقم 16 لسنة 2017، بتاريخ 2017/10/2، رام الله، ص15.

² التقرير السنوي السابع للنيابة العامة لدولة فلسطين لعام 2016، الصادر في آذار من العام 2017، ص17.

³ مقابلة أجراها الباحث مع رئيسة نيابة الجرائم الإلكترونية نسرین رشموي في النيابة العامة الفلسطينية بمدينة رام الله بتاريخ 2017/8/10.

2. آلية عمل نيابة الجرائم الإلكترونية

تعمل هذه الوحدة على التحقيق في الجرائم التي ترتكب باستخدام الوسائل التقنية والمعلوماتية وتختلف آلية التحقيق باختلاف الوسيلة المستخدمة بارتكاب هذه الجرائم، وإذا ارتكبت عبر الحواسيب فيتم التعامل معها والتحقيق فيها من قبل وحدة الشرطة المركزية. وهذه التحقيقات لا تشكل أي انتهاك للخصوصية أو السرية للمواطن إلا إذا كانت تتعلق بجريمة تفيد مصلحة التحقيق، وللنائب العام فقط صلاحية الكشف عنها. وهناك بعض الاحتياجات لا تتم إلا بقرار من قاضي محكمة الصلح للسماح بالاطلاع أو اختراق خصوصية معينة¹.

3. آلية تقديم الشكوى في الجرائم المعلوماتية

تقدم شكاوى الجرائم الإلكترونية كأى شكوى تقليدية إلى النيابة العامة، ويتم سماع شهادة المشتكى تحت تأثير القسم القانوني ومن ثم تحديد الاحتياجات اللازمة للتحقيق من قبل عضو النيابة المختصة، ويقوم بمخاطبة النائب العام لمخاطبة شركات الاتصالات ومزودي الإنترنت لكل شكوى وحسب نوع الجريمة وبأى وسيلة تمت، أو من خلال وحدة الجرائم الإلكترونية إذا كانت تتعلق بضبط جهاز أو فحصه أو استخراج البيانات وصور، ويتم تجميع الملف ومراسلة النيابة التي تقوم بالتحقيق لبناء الملف التحقيقي وإحالته للمحكمة المختصة وفقاً للقانون والأصول².

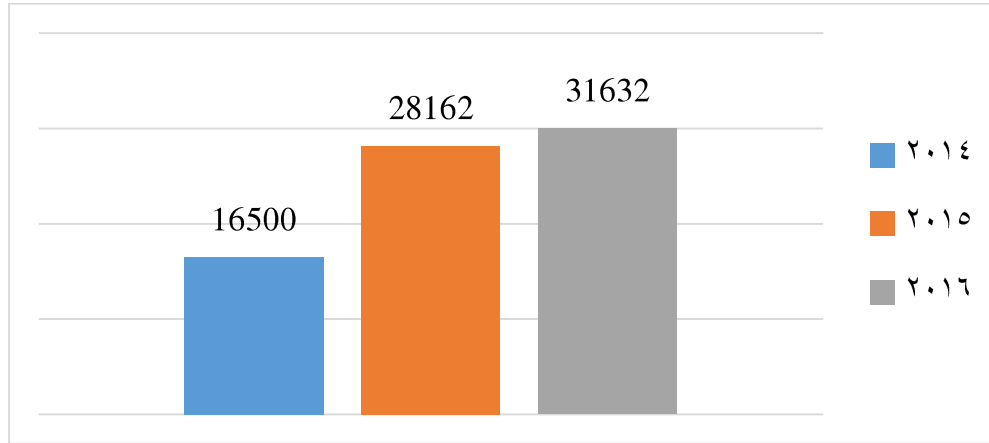
4. شكاوى الجرائم الإلكترونية ما بين 2014 - 2016

تشير الإحصائيات الواردة في التقرير السنوي السابع للنيابة العامة لدولة فلسطين 2016 الصادر في آذار من العام 2017 إلى أن عدد الطلبات حول الجرائم الإلكترونية والجرائم التقليدية بوسيلة الكترونية الواردة إلى نيابة مكافحة الجرائم المعلوماتية في العام 2014 بلغت 16500 شكوى،

¹ مقابلة أجراها الباحث مع رئيسة نيابة الجرائم الإلكترونية نسرین رشمای في النيابة العامة الفلسطينية بمدينة رام الله بتاريخ 2017/8/10.

² مقابلة أجراها الباحث مع رئيسة نيابة الجرائم الإلكترونية نسرین رشمای في النيابة العامة الفلسطينية بمدينة رام الله بتاريخ 2017/8/10.

وارتفعت إلى 28162 شكوى في العام 2015 أي بزيادة مقدارها 70.7%، وبلغت 31632 شكوى في العام 2016 أي بنسبة زيادة 12.3% عن العام 2015¹، مما يدل على زيادة انتشار هذه الظاهرة بشكل متزايد ومستمر مما استوجب الإسراع بإصدار قرار بقانون خاص بالجرائم الإلكترونية عوضاً عن تطبيق قانون العقوبات الأردني 1960 الذي لا يتوافق مع متطلبات التطور التكنولوجي والقانوني الحديث.



الشكل رقم 3: عدد الشكاوى حول مرتكبي الجرائم الإلكترونية التي وصلت للنسبة العامة في الأعوام 2014 و2015 و2016.

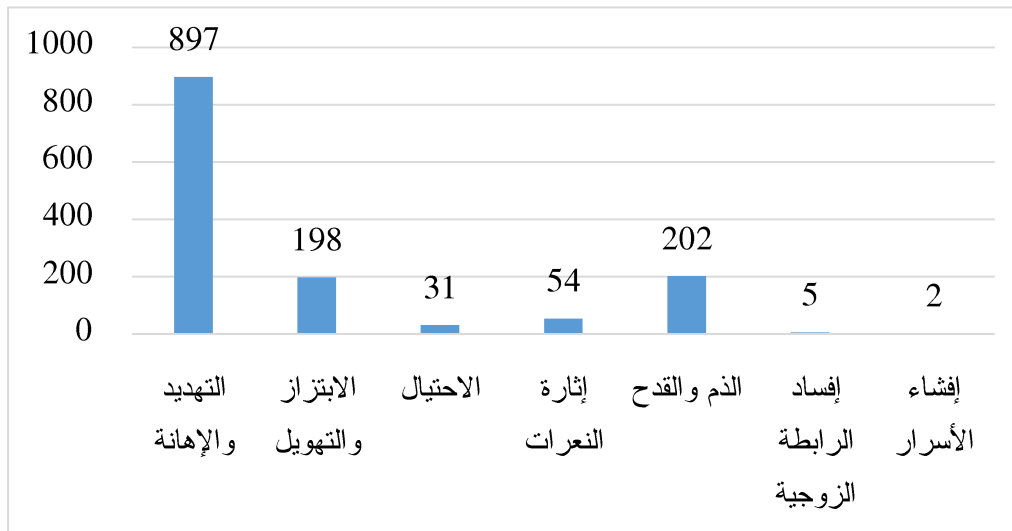
يتضح من الجدول رقم (1) والشكل رقم (4) أن مجموع قضايا الجرائم الإلكترونية حسب التكيف القانوني للهمم الواردة إلى النيابة العامة للعام 2016، بلغت 1389 قضية موزعة على النحو الآتي، احتلت جرائم التهديد والإهانة المرتبة الأولى وبلغ مجموعها 897 بنسبة 64.4%، يليها في المرتبة الثانية جرائم الذم والقذف وبلغ مجموعها 202 قضية بنسبة 14.5%، وفي المرتبة الثالثة جرائم الابتزاز والتهويل وبلغ مجموعها 198 قضية بنسبة 14.3%، وفي المرتبة الرابعة إثارة النعرات عبر وسائل الاتصالات السلكية واللاسلكية وبلغ مجموعها 54 قضية بنسبة 3.9%، وفي المرتبة الخامسة قضايا الاحتيال وبلغ مجموعها 31 قضية بنسبة 2.2%، وفي المرتبة السادسة قضايا إفساد الرابطة الزوجية وبلغ مجموعها 5 بنسبة 0.4% وفي المرتبة

¹ التقرير السنوي السابع للنسبة العامة لدولة فلسطين لعام 2016، الصادر في آذار من العام 2017، ص112.

الأخيرة قضايا إفشاء الأسرار وبلغ مجموعها قضيتين بنسبة 0.1% من المجموع الكلي للجرائم المعلوماتية للعام 2016¹.

جدول رقم 1: عدد القضايا الواردة للنيابة العامة المتعلقة بالجرائم المعلوماتية "الإلكترونية"

نوع القضية	عدد القضايا	النسبة المئوية
التهديد والإهانة	897	64.6%
الابتزاز والتهويل	198	14.3%
الاحتيال	31	2.2%
إثارة النعرات	54	3.9%
الذم والقذح	202	14.5%
إفساد الرابطة الزوجية	5	0.4%
إفشاء الأسرار	2	0.1%
المجموع	1389	



الشكل رقم 4: عدد القضايا الواردة للنيابة العامة المتعلقة بالجرائم المعلوماتية "الإلكترونية" للعام 2016.

¹ التقرير السنوي السابع للنيابة العامة لدولة فلسطين لعام 2016، الصادر في آذار من العام 2017، ص 113 – 114.

أعطت المادة 34 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية النيابة العامة الحق في الحصول مختلف الوسائل والأدوات والبيانات والمعلومات المتعلقة بمحتوى الجريمة الإلكترونية وضبطها والتحفظ عليها لتساعد في كشف الحقيقة، واشترطت المادة 35 الحصول على إذن القاضي لمراقبة المحادثات والمحادثات الإلكترونية، كما فرضت المادة 36 اتخاذ كافة التدابير والإجراءات للمحافظة على سلامة مختلف الوسائل الإلكترونية والبيانات والمعلومات لحين صدور حكم قضائي نهائي، ومنحت المادة 37 المحكمة إصدار امر بالاعتراض على محتوى الاتصالات، والزمّت الجهات المختصة بعدم استبعاد أي دليل ناتج عن وسائل تكنولوجيا المعلومات ما دام تم الحصول عليها ضمن الإجراءات القانونية والقضائية الدولية وفق أحكام المادة 38 و39 من القرار بقانون¹.

قد تشكل هذه المواد انتهاكاً للخصوصية في حال تم إجراء تفتيش وسائل تقنية المعلومات دون الحصول على إذن من المحكمة المختصة، أو تم ذلك دون حضور المتهم على الرغم من عدم النص عليها، ولم يحدد بناءً على طلب النائب العام أو أحد مساعديه أو نوع الجريمة، ولم تشترط تسبب أذن المراقبة ومدته، بمعنى أن المشرع تراجع عن الضمانات الممنوحة وفق نص المادة 51 من قانون الإجراءات الجزائية فيما يخص تنظيم إجراءات ضبط المراسلات ومراقبة المحادثات السلوكية واللاسلكية بأن يكون الإذن بناءً على طلب من النائب العام أو أحد مساعديه وفي الجنايات أو الجناح المعاقب عليها بمدة لا تقل عن سنة، لكنه توسع في مدة الرقابة لثلاثة شهور قابلة للتجديد لمرة واحدة بشكل يتعارض مع قانون الإجراءات الجزائية، كما خلت تلك النصوص من إتلاف البيانات والمعلومات أو إعادتها لمصدرها الأصلي بعد استيفاء الغرض منها، ولم ينص على استبعاد أي دليل ناتج عن المراقبة غير المشروعة². وهذا يوجب إعادة صياغة هذه النصوص بما تتوافق مع الضمانات الممنوحة وفق قانون الإجراءات الجزائية الفلسطيني والمعايير الدولية.

¹ المواد 34 - 39 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية.

² ملاحظات مؤسسة الحق على القرار بقانون بشأن الجرائم الإلكترونية رقم 16 لسنة 2017، بتاريخ 2017/10/2، رام الله، ص16 و ص17.

ثالثاً: دور القضاء

يشكل الجهاز القضائي الفلسطيني أحد أسس وأركان المنظومة القانونية الفلسطينية، وانطلاقاً من دوره بتطبيق أحكام القانون لحماية الحقوق والحريات العامة، ومن أجل تطبيق أحكام القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، لا بد من تطوير القضاء بما يتناسب مع التطورات والتغيرات التكنولوجية وما ينجم عنها من آثار اجتماعية وقانونية¹.

قبل صدور القرار بقانون بشأن الجرائم الإلكترونية كانت المحاكم الفلسطينية تطبق قانون العقوبات الأردني رقم 16 لسنة 1960 وتطويع النصوص القانونية للجريمة العامة على الجريمة التي تقع عبر الوسيلة الإلكترونية فمثلاً تسند نصوص جرائم التشهير والذم والقدح والتحقير والتهديد والاحتيال والتزوير العادية على هذه الجرائم إذا ارتكبت بوسيلة الكترونية، وهذه النصوص والعقوبات لا تتناسب مع الجريمة العصرية بسبب قدم القانون. وأصبح الآن يطبق القرار بقانون بشأن الجرائم الإلكترونية على كافة الملفات التي تحال من النيابة العامة إلى المحاكم، باعتباره قانوناً خاصاً بدلاً من قانون العقوبات الذي أصبح قانوناً عاماً. وأكثر الجرائم المعلوماتية انتشاراً في فلسطين التشهير والابتزاز والاحتيال².

يعتبر القرار بقانون بشأن الجرائم الإلكترونية قانوناً عصرياً وحديثاً يوازي القوانين في الدول الأخرى ومستمد من اتفاقية بودابست ولا يتعارض مع الحريات العامة، وأي قانون يصدر حديثاً لا بد أن يأخذ فترة زمنية في التطبيق العملي حتى يثبت مدى ملاءمته للواقع واكتشاف نقاط ضعفه وتصويبها. ومن أجل تفعيل دور القضاء في الفضاء الإلكتروني لا بد من تنظيم دورات متخصصة للقاضي الجزائي حول الجرائم المعلوماتية لتطبيق أحكام القانون بكفاءة واقتدار³.

¹ مقابلة أجراها الباحث مع القاضي أيمن ظاهر، قاض محكمة صلح رام الله بتاريخ 2017/9/12 بمدينة رام الله.

² مقابلة أجراها الباحث مع القاضي أيمن ظاهر، قاض محكمة صلح رام الله بتاريخ 2017/9/12 بمدينة رام الله.

³ مقابلة أجراها الباحث مع القاضي أيمن ظاهر، قاض محكمة صلح رام الله بتاريخ 2017/9/12 بمدينة رام الله.

الفرع الثالث: ملاحظات عامة حول القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية

يهدف هذا القرار بقانون بشأن الجرائم الإلكترونية إلى مكافحة الجريمة الإلكترونية في فلسطين، وتحديد النصوص القانونية الواجبة التطبيق على القضايا ذات العلاقة ومن أجل سرعة الفصل فيها، وتعزيز ثقة المواطنين بالجهاز القضائي والنيابة العامة، وتعزيز ثقة المواطن للتعامل مع الوسائل الإلكترونية، والمساهمة في تطوير الاقتصاد الوطني من خلال تفعيل الأنشطة الاقتصادية والعقود التجارية التي تتم من خلال الوسائل الإلكترونية¹. ووضع هذا القرار بقانون حداً للتعامل مع الجرائم الإلكترونية كجرائم عادية وفق تطبيق نصوص الجرائم التقليدية في قانون العقوبات الساري المفعول، ويعتبر مكملاً لقانون العقوبات الساري المفعول ولا يمكن فصله عنه. وجاء هذا التشريع ليضع حداً لعدم إفلات المجرم المعلوماتي من العقاب، ولمعاقبة أصحاب الجرائم الذين يوظفون مختلف الوسائل التكنولوجية لارتكاب جرائمهم، والحد من الظواهر المجتمعية السلبية التي قد تلحق أضراراً مادية ومعنوية بالمجتمع والمستخدمين².

يحمل هذا القانون في بعض مواده المحافظة على الخصوصية فعلى سبيل المثال ما ورد في المادة 4 منه نصت على حظر الدخول بدون وجه حق على وسيلة أو نظام أو موقع الكتروني أو شبكة الكترونية أو المعلومات أو التجاوز وعدم الحاق الضرر بالمستخدمين أو المستفيدين، وما جاء في المادة 8 تجريم فك أي بيانات مشفرة للأشخاص والهيئات المعنوية، ونصت المادة 12 على تجريم استخدام الشبكة الإلكترونية أو احدى وسائل تقنية المعلومات في الوصول دون وجه حق إلى أرقام أو بيانات وسائل التعامل الإلكتروني أو التلاعب بها، وما نصت عليه المادة 27 على تجريم قيام الموظف العام أو موظف مزود الخدمة بارتكاب الجرائم الإلكترونية مستغلاً سلطاته وصلاحياته أثناء تأدية عمله أو بسببه أو سهل ذلك لغيره. ولا يجوز للنيابة العامة الاعتراض أو التمتصت أو جمع البيانات إلا بقرار من المحكمة المختصة، وبالتالي فرض

¹ المادة 2 من مسودة قرار بقانون الجرائم الإلكترونية بلا رقم لسنة 2016 والمعد من قبل النيابة العامة بتاريخ 2016/3/16.

² مداخلة د. حسن الطراونة، أستاذ القانوني الجنائي في كلية الحقوق في الجامعة الأردنية ضمن برنامج ملف اليوم بعنوان "قانون الجرائم الإلكترونية بين الأهمية والتطبيق" أجريت على تلفزيون فلسطين بتاريخ 2017/7/12، رام الله.

المشرع الفلسطيني ضمانات منها رقابة القضاء على النيابة العامة لضمان حماية الحقوق والحريات العامة. وهذا يتفق مع أحكام القانون الأساسي الذي كفل حرية الرأي والتعبير ضمن الحدود التي رسمها القانون، وحظر الرقابة على الإعلام من أجل الحفاظ على العمل الصحفي بصفتها السلطة الرابعة¹.

يحتوي هذا القرار بقانون على المصطلحات العلمية ذات الدلالة القانونية ويبين الإجراءات التي يجب أن يستخدمها المحقق والنيابة العامة أثناء عملية التحقيق أو المحاكمة كتفتيش وضبط المعلومات والأدلة الإلكترونية التي تشكل جريمة، حتى لا تثير جدلاً قانونية في شرعيتها ومشروعيتها أمام النيابة العامة والمحكمة ولعدم ترتب البطلان على هذه الإجراءات، وكيفية استخراج واستخدام الدليل المشروع وغير المشروع من أجل صيانة الحقوق والحريات، والعقوبات، وبالإضافة إلى الالتزامات المترتبة على مزودي خدمة الإنترنت والتعاون الدولي في هذا المجال. كما تناول هذا القرار بقانون مجموعة من الإجراءات القضائية منها تشكيل وحدة الجرائم الإلكترونية لدى جهاز الشرطة الفلسطينية والنيابة العامة والمحاكم. وقد جاء هذا القرار بقانون منسجماً في العديد من مواد مع متطلبات الاتفاقية العربية لمكافحة جرائم تقنية المعلومات واتفاقية بودابست لمكافحة الجرائم المعلوماتية من ناحية ومتناقضاً مع نصوصها في العديد من مواد من ناحية أخرى مما أثار جدلاً وردود فعل واسعة عليه من حيث الشكل والمضمون من قبل مؤسسات المجتمع المدني والمفوض العام لحماية الحقوق والحريات في هيئة الأمم المتحدة كما يتبين أدناه:

أولاً: ردود الفعل الفلسطينية غير الرسمية

ومن ناحية ردود الأفعال الفلسطينية على القرار فقد قامت الهيئة المستقلة لحقوق الإنسان "ديوان المظالم" ومؤسسات المجتمع المدني الأعضاء في اللجنة المشتركة (نقابة الصحفيين الفلسطينيين، مؤسسة الحق، شبكة المنظمات الأهلية، مجلس حقوق الإنسان، المركز الفلسطيني للتنمية

¹ مقابلة أجريت على تلفزيون فلسطين مع النائب العام لدولة فلسطين د. أحمد براك ضمن برنامج ملف اليوم بعنوان "قانون الجرائم الإلكترونية بين الأهمية والتطبيق" بتاريخ 2017/7/12، رام الله.

والحريات الإعلامية "مدى"، مركز المرأة للإرشاد القانوني والاجتماعي، الائتلاف من أجل النزاهة والمساءلة "أمان"، مركز تطوير الإعلام في جامعة بيرزيت، المركز الفلسطيني لاستقلال المحاماة والقضاء "مساواة"، ومنتدى مناهضة العنف ضد المرأة) بتقديم مذكرة قانونية إلى عضو اللجنة التنفيذية لمنظمة التحرير الفلسطينية وعضو المجلس التشريعي الفلسطيني حنان عشراوي حول القرار بقانون رقم (16) لسنة 2017 بشأن الجرائم الإلكترونية، حيث عبرت هذه المؤسسات عن رفضها لهذا القرار بقانون للأسباب التالية: استخدام كلمات فضفاضة وعامة وتوسع غير مبرر في التجريم، وتهديد الخصوصية وحرمة الحياة الخاصة، وحجب المواقع الإلكترونية، وقسوة الجزاءات، وغياب النصوص القانونية التي توفر حماية عامة لحقوق الإنسان وحياته الأساسية. وبالاستناد إلى هذه الأسباب، والتي طالت جل نصوص القرار بقانون، وتعزيزاً وحماية لحقوق المواطنين وحياتهم الأساسية، وتنفيذاً للالتزامات دولة فلسطين الدولية، فإن هذه المؤسسات ترى بأن القرار بقانون رقم (16) لسنة 2017 بشأن الجرائم الإلكترونية، لا يشكل أساساً لتشريع ناظم لمكافحة الجرائم الإلكترونية¹.

ثانياً: ردود الفعل الدولية

على الصعيد الدولي وبناءً على المعلومات الواردة إلى ديفيد كاي المقرر الخاص في الأمم المتحدة لتعزيز وحماية الحقوق وحرية الرأي والتعبير دعا الحكومة الفلسطينية باتخاذ خطوات ضرورية لمراجعة بعض بنوده ليتماشى مع الالتزامات المترتبة عليها وفق الاتفاقيات الدولية لحقوق الإنسان وذلك خلال سنتين يوماً من تاريخ 2017/8/16².

ثالثاً: ردود الفعل الفلسطينية الرسمية

فيما يتعلق بردود الفعل الرسمية فقد قرر مجلس الوزراء الفلسطيني في جلسته رقم (183) المنعقدة بتاريخ 2017/12/19 إحالة مشروع قرار بقانون الجرائم الإلكترونية لوضعه في قلبه

¹ مذكرة قانونية إلى د. حنان عشراوي حول القرار بقانون رقم (16) لسنة 2017 بشأن الجرائم الإلكترونية، رئيس دائرة الثقافة والإعلام في منظمة التحرير الفلسطينية، بتاريخ 2017/9/17، المنشورة على www.musawa.ps.

² مقال بعنوان "الأمم المتحدة تطالب الحكومة الفلسطينية بالرد خلال شهرين حول قانون الجرائم الإلكترونية"، نشر على صحيفة العربي الجديد بتاريخ 2017/08/29، <https://www.alaraby.co.uk>، تاريخ الزيارة 2107/11/10.

القانوني المناسب لإقراره في الجلسة القادمة تمهيداً للتنسيب بها إلى السيد الرئيس لإصدارها حسب الأصول¹.

إضافة إلى ما تقدم يمكن إبراز أهم الملاحظات القانونية الشكلية والجوهرية الأخرى على هذا القرار بقانون:

- صادق رئيس دولة فلسطين على هذا القرار بقانون استناداً لصلاحياته التشريعية الاستثنائية وفق أحكام المادة 43 من القانون الأساسي الفلسطيني لسنة 2003 وتعديلاته بسبب تعطل المجلس التشريعي عن ممارسة أعماله، والتي تشترط وجود حالة ضرورة لمباشرة تلك الصلاحيات الاستثنائية والذي قد تنتفي توفرها في هذا القانون.
- عدم طرح هذا القرار بقانون للنقاش المجتمعي للاستئناس برأي المؤسسات الحقوقية ومؤسسات المجتمع المدني والشركات المزودة لخدمة الإنترنت وأصحاب الاختصاص.
- ورود بعض المصطلحات الواسعة والفضفاضة خلافاً لمبدأ شرعية الجرائم والعقوبات مثل أمن الدولة، تهديد الأمن القومي، النظام العام والآداب العامة.
- قد يستخدم هذا القرار بقانون كأداة قانونية لانتهاك حقوق المواطنين وحرياتهم الأساسية.
- لم يتناول هذا القرار بقانون التعويض عن الأضرار المعنوية للمتضررين من هذه الجرائم.
- يخلوا من أي نصوص قانونية حول انتهاك أي حق من حقوق الملكية الفكرية.
- غياب اللائحة التفسيرية لهذا القرار بقانون مما يتطلب الإسراع في إصدارها.

¹ اجتماع مجلس الوزراء في جلسته رقم (183) بتاريخ 2017/12/19، المنشورة على الموقع www.palestinecabinet.gov.ps

• تجاوز عدد الجرائم الإلكترونية الواردة في كل من اتفاقية بودابست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات فينبغي أن يبنى وفق معايير هذه الاتفاقيات.¹

• تعاقب معظم بنوده على القصد "الركن المعنوي الذي يصعب إثباته" دون تحقيق الركن المادي.

وهذا يستوجب إعادة مراجعة صياغة بعض بنوده أو إضافة مواد جديدة من قبل جهات الاختصاص وخبراء القانون ومؤسسات المجتمع المدني من أجل الوصول إلى قانون يغطي معظم الملاحظات آنفة الذكر، وإضافة نص قانوني جديد يحظر تفسير أو تأويل أي نص بشكل يخالف أو يتعارض مع الحقوق والحريات العامة والحق في الخصوصية، وإصدار اللائحة التفسيرية الخاصة بالقرار بقانون بشأن الجرائم الإلكترونية وصولاً إلى قانون عصري وحديث منسجماً مع متطلبات الاتفاقيات الدولية والعربية بهذا الخصوص.

المبحث الثاني: التحديات التشريعية ودور المؤسسات في الوقاية من الجرائم المعلوماتية

يواجه المشرع الفلسطيني مجموعة من التحديات بسبب انتشار هذه الجرائم في فلسطين بشكل متزايد، وتعمل العديد من مؤسسات الدولة على مواجهتها والحد منها. وبناءً على ما تقدم يتناول هذا المبحث مطلبين، يشتمل المطلب الأول على التحديات التي تواجه المشرع الفلسطيني في ملاحقة مرتكبي الجرائم المعلوماتية، أما المطلب الثاني يبحث دور المؤسسات في الوقاية منها ومكافحتها.

¹ ملاحظات مؤسسة الحق على القرار بقانون بشأن الجرائم الإلكترونية رقم 16 لسنة 2017، بتاريخ 2017/10/2، رام الله، ص2.

المطلب الأول: التحديات التي تواجه المشرع الفلسطيني في ملاحقة مرتكبي الجرائم المعلوماتية

من أبرز التحديات التي تواجه المشرع الفلسطيني في ملاحقة ومتابعة مرتكبي الجرائم التقنية وردعهم

الفرع الأول: وضع استراتيجية تشريعية فلسطينية

على الرغم من تقدم وتطوير بعض القوانين الفلسطينية إلا أن العملية التشريعية في فلسطين تعاني من أوجه الضعف تحد من كفاءتها وفعاليتها، بسبب تعطل المجلس التشريعي عن أعماله مما يتيح للسلطة التنفيذية إصدار قرارات بقانون، وهذا يؤدي إلى تداخل صلاحيات السلطة التنفيذية مع السلطة التشريعية خلافاً لمبدأ الفصل بين السلطات¹. هذا الوضع يتطلب ضرورة إعادة انعقاد جلسات المجلس التشريعي الفلسطيني وتفعيل دوره في إصدار التشريعات والقوانين النازمة لمختلف مجالات الحياة، وفق الرؤية الاستراتيجية لبناء دولة المؤسسات والقانون. ونتيجة لانتشارها في دولة فلسطين يتوجب وضع خطة استراتيجية وطنية شاملة للوقاية والحد منها، قائمة على ضمان سيادة القانون وحقوق الإنسان وحماية الحقوق والحريات العامة وتعزيز تنفيذ الأحكام القضائية وتسهيل الحصول على خدمات قطاع العدالة للأفراد، وتعزيز التعاون بين المؤسسات ذات العلاقة وتطوير النظام القانوني ليتناسب مع احتياجات مختلف شرائح المجتمع، وتنظيم العلاقة بين قطاع العدالة وقطاع الأمن وتعزيزها مع وسائل الإعلام، بالإضافة إلى تمكين مؤسسات قطاع العدالة القيام بدورها بشكل فعال وتعزيز مبدأ الرقابة والمساءلة والشفافية في عمل تلك المؤسسات².

¹ البيان الختامي لمؤتمر عقده معهد الحقوق في جامعة بيرزيت بعنوان "مقومات الإصلاح التشريعي: التحولات والتحديات"، بتاريخ 2010/11/1.

² التقرير السنوي السابع للنيابة العامة لعام 2016 الصادر في آذار من العام 2017، رام الله، ص 15.

وينبغي أن تركز هذه الاستراتيجية على وضع برامج توعية وإرشادية للوقاية والحد من الجرائم الإلكترونية بالتركيز على المناهج الدراسية ووسائل الإعلام الهادفة والأسرة، وتوحيد التشريعات الداخلية بما تتناسب مع التطورات الحديثة وتدريب أفراد العدالة الجنائية على التعامل مع هذه الجرائم وإيجاد نظام جنائي وإجرائي لحماية شبكات وأنظمة المعلومات والبيانات، وتعزيز دور البحث العلمي في مجال الجرائم المستحدثة بشكل عام وفي الجرائم الإلكترونية بشكل خاص للعمل على الحد من مخاطرها وأثارها.

الفرع الثاني: تحديات قانونية

تتمثل التحديات القانونية في الجوانب الموضوعية من ناحية والإجرائية من ناحية أخرى، ومن التحديات الموضوعية صعوبة تحديد مفهوم الجرائم المعلوماتية باعتبارها جرائم مستحدثة، بالإضافة إلى ظهور أنماط جديدة لسوء استغلال مختلف وسائل تقنية المعلومات، وصعوبة تحديد مصدر ارتكابها لقيام فاعلها بإخفاء الدليل الرقمي مع تزايد التطور التكنولوجي، كذلك ضعف البحث العلمي حول الجرائم التقنية والمعلوماتية¹.

أما التحديات الإجرائية التي تواجه وحدة الجرائم الإلكترونية في جهاز الشرطة الفلسطينية في أداء وتنفيذ مهامه لملاحقة مرتكبي الجرائم المعلوماتية تتمثل في ضعف البنية التحتية الإلكترونية، وانخفاض عدد الموظفين ذوي الاختصاص في متابعة الجرائم الإلكترونية، وصغر حجم مختبر الأدلة الرقمية والذي لا يتناسب مع عدد هذه الجرائم وانتشار الشرائح 3G الإسرائيلية، وضعف التعاون المجتمعي مع جهاز الشرطة في مجال الجرائم الإلكترونية².

كما تواجه نيابة الجرائم الإلكترونية العديد من التحديات والصعوبات في التحقيق بجرائم تقنية المعلومات منها نقص الكوادر البشرية المختصة تقنياً وفنياً في التعامل مع الجرائم المعلوماتية، وضعف القوانين سارية المفعول (قانون العقوبات وقانون الاتصالات السلكية واللاسلكية) عن

¹ عابنة، محمود أحمد: مرجع سابق، ص 147 و ص 153.

² مقابلة أجراها الباحث مع مدير وحدة الجرائم الإلكترونية التابعة لإدارة المباحث في جهاز الشرطة الفلسطيني سامر الهندي بمدينة رام الله بتاريخ 14.8.2017.

ملاحقة مرتكبيها وردعهم لفراغهم من النصوص القانونية التي تجرم هذه الأفعال، بالإضافة إلى تطبيق النصوص التقليدية على الجرائم الإلكترونية قبل صدور القرار بقانون بشأن الجرائم الإلكترونية. ولم تتطرق النصوص الحالية في قانون الإجراءات الجزائية الفلسطيني إلى مسألة البحث والتحري وجمع الاستدلالات والتفتيش وضبط التقنيات الخاصة من أجل إثباتها والمحافظة على الأدلة¹. وجاء القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية ليضع خارطة طريق قانونية لملاحقة مرتكبيها.

أما القضاء الفلسطيني قبل صدور القرار بقانون بشأن الجرائم الإلكترونية واجه صعوبات قانونية بتحديد الجرائم الواقعة على أجهزة الحاسوب ذاتها فمثلاً قانون العقوبات لا يغطي التكيف القانوني لتدمير الجهاز نفسه أو اختراق البريد الإلكتروني التي كانت تشكل مشكلة حقيقية في تكيف التهم وإسنادها للمتهم، أما بعد صدور القرار بقانون بشأن الجرائم الإلكترونية فقد غطى معظم الجرائم التي تقع على الأجهزة الإلكترونية والأشخاص. ومن أهم المشاكل الفنية تواجهها المحاكم تتمثل في تقديم الدليل الرقمي الذي يثبت الجريمة الإلكترونية من خلال المختبر الجنائي باعتباره مختبراً مركزياً والذي لا يعتبر كافياً لبنيتها الأساسية من مباني وأجهزة وكوادر بشرية كافية ومختصة، لتقديم التقرير الوافي والشامل للقضاء حول الدليل الرقمي من قبل أصحاب الاختصاص وفي الوقت المناسب².

الفرع الثالث: تطبيق القانون وإنفاذ قرارات المحاكم

يواجه القضاء الفلسطيني والنيابة العامة والشرطة الفلسطينية العديد من التحديات التي قد تؤثر على أدائه ومهامه، منها سيطرة الاحتلال الإسرائيلي على المناطق الفلسطينية التي تشكل عائقاً في أداء دورهم القانوني، بالإضافة إلى ضعف البنية التحتية والتقنية القضائية وغياب استقرار التشريعات والقوانين³. وهذا يستدعي من أصحاب العلاقة ضرورة تطويرها في التعامل مع

¹ مقابلة أجراها الباحث مع رئيسة نيابة الجرائم الإلكترونية نسرین رشموي في النيابة العامة الفلسطينية بمدينة رام الله بتاريخ 2017/8/10.

² مقابلة أجراها الباحث مع القاضي أيمن ظاهر، قاض محكمة صلح رام الله بتاريخ 2017/9/12 بمدينة رام الله.

³ الشلادة، مرجع سابق، ص 12.

طبيعة الجرائم الإلكترونية، بما يتناسب مع متطلبات القرار بقانون بشأن الجرائم الإلكترونية. كما يشكل سيطرته على قطاع الاتصالات والفضاء الإلكتروني الفلسطيني عائقاً أمام عمليات التحقيق في هذه الجرائم لملاحقة ومتابعة مرتكبيها لفرارهم داخل المناطق التي لا تخضع للسيطرة الفلسطينية ويعيق الوصول إلى الأدلة الجنائية الرقمية. إضافة إلى ذلك لا يوجد سيادة وسلطة قانونية للقضاء والنيابة العامة والشرطة على المتهمين من حملة الهوية الزرقاء الإسرائيلية¹.

الفرع الرابع: مواكبة التطورات الإقليمية والدولية

بعد حصول فلسطين على عضو مراقب في هيئة الأمم المتحدة، وانضمامها إلى الاتفاقيات والمعاهدات الدولية في مجال الجرائم المعلوماتية، ونتيجة الالتزامات المترتبة عليها بموجب أحكام هذه الاتفاقيات صدر قرار بقانون بشأن الجرائم الإلكترونية، وجاءت مواده منسجمة مع هذه الاتفاقيات الدولية والإقليمية بما في التعاون الدولي²، وهذا يتطلب تعزيز إجراءات التحقيق والملاحقة القضائية الدولية وتسليم المجرمين، وتبادل الخبرات الفنية والقانونية بين أعضاء العدالة الجنائية في مجال الجرائم التقنية.

الفرع الخامس: تعزيز المشاركة المجتمعية

أثارت مؤسسات المجتمع المدني العديد من الانتقادات بعد إصدار القرار بقانون بشأن الجرائم الإلكترونية في فلسطين انطلاقاً من دورها في ممارسة الرقابة الشعبية ومنها: عدم دستوريتها باعتباره صادر عن السلطة التنفيذية وهي جهة غير مختصة بإصداره وإنما يدخل من اختصاص السلطة التشريعية. ويشكل انتهاكاً لحرية الرأي والتعبير والحرية الصحفية والعمل الإعلامي والحق في الوصول إلى المعلومة والحق في حماية الخصوصية التي كفلها القانون الأساسي الفلسطيني والمعاهدات الدولية والإقليمية التي وقعت وانضمت إليها فلسطين. عدم طرح القرار بقانون للنقاش المجتمعي بمشاركة خبراء قانونيين وصحفيين والشركات المزودة لخدمة الإنترنت،

¹ التقرير السنوي السابع للنيابة العامة لعام 2016 الصادر في آذار من العام 2017، رام الله، ص 123.

² مقابلة أجراها الباحث مع رئيسة نيابة الجرائم الإلكترونية نسرین رشناوي في النيابة العامة الفلسطينية بمدينة رام الله بتاريخ 2017/8/10.

ومنح النيابة العامة صلاحية واسعة كمراقبة وحجب المواقع الإلكترونية وتفتيش الأجهزة الإلكترونية ومراقبة الاتصالات والمحادثات مما يتطلب تقيد هذه الصلاحيات. يتضمن القرار بقانون عبارات ومصطلحات عامة دون تحديدها أو تعريفها مثل "الآداب العامة في المادة 20، والأمن الداخلي والخارجي وتعرض سلامة الدولة للخطر في المادة 24، وإثارة النعرات العنصرية في المادة 24"، مما يجعل هذه النصوص قابلة للتفسير والتأويل وتشكل انتهاكاً لمبدأ شرعية الجرائم والعقوبات، والتوسع في نطاق التجريم والتشديد في العقوبات لأفعال لا تتناسب مع طبيعة المعطيات الرقمية. ومنح القرار بقانون شركات مزودي خدمة الإنترنت الحفاظ بالبيانات الخاصة بالمشاركين وتقديم أي معلومات من أجل كشف الحقيقة، التي قد تشكل انتهاكاً لخصوصية وسرية المشاركين في حال تزويدها لجهات دولية أخرى نتيجة الالتزامات المترتبة على فلسطين وفق الاتفاقيات الموقع عليها في هذا المجال. ولا ينص على حماية المبلغين والشهود وعلى استبعاد الأدلة المعلوماتية بعد استخدامها كإتلافها أو إعادتها لمصدرها، وفرض عقوبات متشددة بالحبس والغرامات المالية الباهظة التي لا تتناسب مع الواقع الفلسطيني، وشكل مخالفة للقاعدة القانونية "العلم بالقانون" أي لم يمنح الأفراد فترة زمنية من أجل الاطلاع عليه بعد نشره بالجريدة الرسمية¹.

تأسياً على ما تقدم تطالب مؤسسات المجتمع المدني إعادة النظر في بعض بنوده ومناقشتها للأخذ بأرائهم وملاحظاتهم للوصول إلى قانون يكفل حرية الرأي والتعبير والحرية الصحفية والعمل الإعلامي والمحافظة على الخصوصية والسرية بشكل يتناسب وينسجم مع المعاهدات الدولية والإقليمية التي انضمت ووقعت عليها فلسطين.

جاءت العديد من ملاحظات مؤسسات المجتمع المدني منسجمة مع متطلبات القانون الأساسي والمعايير الدولية بخصوص حقوق الإنسان من ناحية وخلطت ما بين نصوص القرار بقانون وسوء استخدامها من قبل السلطة التنفيذية من ناحية أخرى، وقد تزول معظم هذه الملاحظات والتخوفات عند إصدار اللائحة التفسيرية للقرار بقانون بشأن الجرائم الإلكترونية.

¹ المذكرة القانونية حول القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، الصادرة عن الهيئة المستقلة لحقوق الإنسان "ديوان المظالم" في مدينة رام الله، بتاريخ 2017/8/7.

المطلب الثاني: دور المؤسسات في الوقاية من الجرائم المعلوماتية ومكافحتها

يختلف دور مؤسسات المجتمع في مواجهة هذه الجرائم، فبعضها يلعب دوراً وقائياً كمؤسسات الإعلام والأسرة والتعليم والثقافة، والأخرى تعمل على مكافحتها كالمؤسسات الأمنية والنيابة العامة والقضاء، يتناول هذا المطلب دور المجلس التشريعي والمؤسسات الأمنية، والإعلامية، والدينية، والأسرة، والتعليمية والثقافية للوقاية منها¹.

الفرع الأول: المجلس التشريعي

نظراً لغياب دور المجلس التشريعي الفلسطيني في إصدار التشريعات منذ أكثر من 10 سنوات جاء القرار بقانون بشأن الجرائم الإلكترونية لسد الفراغ التشريعي التي عانت منه السلطة التنفيذية والقضائية.

تكفل التشريعات والقوانين أمن واستقرار المجتمعات وتشكل الضمانات الأساسية لحقوق الأفراد، وهذا يتطلب سن تشريعات أو استحداث القوانين الجزائية التقليدية لتتلاءم مع التطورات التكنولوجية والتقنية والاقتصادية والاجتماعية، لملاحقة مرتكبي تلك الجرائم من أجل تحقيق الردع العام والخاص من خلال فرض عقوبات صارمة تساهم في الحد من أثارها السلبية على الأفراد والمؤسسات².

الفرع الثاني: المؤسسة الأمنية

تقوم المؤسسة الأمنية بمواجهة الجرائم الإلكترونية من خلال تأهيل كوادر أمنية متخصصة باستخدام التقنيات الحديثة والفضاء الإلكتروني في عمليات البحث والتحري والمراقبة لمنعها وضبطها، والتوعية الثقافية الأمنية حول مخاطر انتشارها³، وتحفيز الأفراد والمؤسسات على

¹ الردايدة، عبد الكريم: الجرائم المستحدثة واستراتيجية مواجهتها. دار ومكتبة الحامد للنشر والتوزيع، الطبعة الأولى، الأردن، 2013، ص 100.

² الردايدة، عبد الكريم: مرجع سابق، ص 263.

³ حمدان، هاني: دور العلاقات العامة لدى الأجهزة الأمنية في التوعية الأمنية، مجلة الدراسات الأمنية، أكاديمية الشرطة الملكية، عمان، الأردن، العدد 1، 2004، ص 37.

إبلاغ الجهات المختصة عنها¹، بالإضافة إلى تعزيز الأبحاث العلمية الشرطية والأمنية حولها وتحليلها مع مواكبة التطور العلمي والتكنولوجي. وتعزيز التعاون الأمني إقليمياً ودولياً خلال تبادل الخبرات القانونية والإجراءات الفنية والتقنية².

الفرع الثالث: المؤسسة الإعلامية

يساعد الإعلام كسلطة رابعة على ترسيخ أمن المجتمع والتأثير فيه من خلال إثارة الرأي العام لمواجهة الجرائم بكافة أشكالها، من خلال تسليط الضوء على الأفعال والتصرفات السلبية وتوعية المجتمع بهذه الجرائم ومخاطرها للوقاية منها، بواسطة الصحافة الإلكترونية وإصدار الصحف والمجلات التوعوية ونشرها في أروقة المجتمع. ولإنجاح ذلك يتطلب وضع خطة إعلامية من أجل التعرف على ظاهرة الجرائم المعلوماتية في المجتمع لمواجهتها وتنمية الوعي المجتمعي بمخاطرها. وحث المواطنين على إبلاغ الجهات المختصة حال تعرضه لهذه الجرائم وتعاونهم من الجهات المختصة. وبالإضافة إلى نشر وتركيز الجهود على أداء المؤسسات الأمنية والقضائية في مجال مكافحة هذه الجرائم³.

الفرع الرابع: المؤسسة الدينية

تلعب المؤسسات الدينية دوراً مهماً في الوقاية من هذه الجرائم من خلال التربية الأخلاقية وتقوية الإيمان بين أفراد المجتمع والتنشئة السليمة للأفراد عبر وسائل التوعية الدينية المختلفة، ومن خلال وضع مؤلفات وكتب ذات بعد ديني عن مخاطرها⁴، وتنظيم دورات ومحاضرات إرشادية حول هذه الجرائم في أماكن العبادة والمدارس والجامعات وغيرها من المؤسسات، وتعزيز دور خطباء المساجد بالتعاون مع وزارة الأوقاف بتوعية الناس حول هذه الظواهر، وبيان المخاطر

¹ مرسى، محمد محمود السيد: تفعيل دور الشرطة في تحقيق الاستقرار الأمني، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة، 2004، ص55.

² الجبال، محمد علي: دور الشرطة الوقائي في انحسار جرائم العنف، مجلة الأمن العام المصرية، عدد 136، ص 65.

³ الشناوي، محمد: استراتيجية مكافحة جرائم النصب المستحدثة، القاهرة، 2006، ص 264.

⁴ الدباس، عبد الفتاح: دور العقيدة الإسلامية في الحد من الجرائم . أكاديمية الشرطة الملكية، الأردن، عمان، 2002، ص 10 - 11.

التي تنشئ عن السلوكيات التي تتعارض مع الدين الإسلامي ومبادئ الشريعة الإسلامية، والمساهمة في تعزيز تنمية الوازع الديني والأخلاقي¹.

الفرع الخامس: الأسرة

تساهم الأسرة في مواجهة هذه الجرائم باعتبارها أكثر تأثراً بوصفها المؤسسة الأولى التي تؤثر في تحديد سلوك الطفل وشخصيته، ومن خلال تنشآت وتربية وتوعية أفرادها وتوجيههم نحو السلوكيات الإيجابية وإبعادهم عن الجريمة، وتقديم النصائح لهم حول مخاطر هذه الجرائم، كما تساهم الأسرة في مواجهة ومكافحة الجرائم المعلوماتية عن طريق معاقبة أفرادها حال وقوعها من قبل أحدهم، ويفرض هذا الدور على مختلف الدول وضع برامج أسرية ضمن خططها التنموية والاجتماعية من أجل بناء جيل صالح².

الفرع السادس: المؤسسة التعليمية والثقافية

تلعب المؤسسات التعليمية والثقافية دوراً رئيسياً في مواجهة الجرائم الإلكترونية، وتحد من انتشار السلوك غير المرغوب فيه مجتمعياً، وتمنع انحراف الأشخاص نحو ارتكاب الجرائم وتوجيههم إلى السلوك الاجتماعي الصحيح وتعزيز القيم والأخلاق من خلال الإخلاص بالعمل وحسن التربية والتوجيه، وفرض الرقابة والمتابعة على أفرادها لرصدها ولمعرفة أسبابها من أجل الوصول إلى طرق ووسائل علاجها، والتركيز بالمنهج الدراسي الابتدائية على الأخلاق الحميدة كون الطفل أكثر استجابة في هذه المرحلة، وتساهم هذه المؤسسات من خلال إيجاد مقررات تعليمية تعمل على توعية أفراد المجتمع، ونشر الكتب والمجلات حول هذه الجرائم ومخاطرها³.

¹ حوري، عمر محي الدين: الجريمة أسبابها ومكافحتها "دراسة مقارنة" في الشريعة والقانون والعلوم الاجتماعية، دار الفكر، دمشق، الطبعة الأولى، 2003، ص 33.

² الردايدة، عبد الكريم: مرجع سابق، ص 212 - ص 215.

³ الشناوي، محمد: مرجع سابق، ص 261.

الفصل الثالث

إجراءات الدراسة والتحليل الإحصائي

مقدمة

جاء الاستبيان بعد صدور قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية للوقاية من مخاطرها والحد منها وانتشارها في المجتمع الفلسطيني، وفي الفترة التي لا زال يشهد فيها هذا القرار بقانون نقاشاً واسعاً وجدلاً كبيراً واجتهادات قانونية لمدى ملاءمة مواده للواقع الفلسطيني، وإثراءً علمياً لرسالة الماجستير بالبيانات والمعلومات الأولية. تناول الاستبيان آراء الشارع الفلسطيني حول الجرائم الإلكترونية في فلسطين من حيث مدى تعرض الفرد لجريمة الكترونية وما هو نوعها وعدد المرات التي ارتكبت ضده، وهل تقدم الفرد بشكوى للجهات المختصة أم لا ومدى رضاه عن تلك الشكوى، وحول معرفة الأفراد بالقرار بقانون 16 لسنة 2017 بشأن الجرائم الإلكترونية، وأفضل الإجراءات الواجب اتخاذها للحد من الجرائم الإلكترونية في فلسطين.

منهجية الاستبيان

تم إعداد مسودة الاستبيان من خلال مراجعة الدراسات والأبحاث المنشورة حول الجرائم الإلكترونية، ثم

تم عرض الاستبيان على محكمين من حملة درجة الدكتوراه في القانون والإحصاء¹ ثم تم إجراء بعض التعديلات والإضافات عليها. بعد ذلك تم إعداد الاستبيان إلكترونياً باستخدام (Google Forms) حيث تم توزيع 20 استبانة كتجربة أولى و30 استبانة كتجربة ثانية، وبعد أن تم إجراء كافة التعديلات عليها تم نشرها وتوزيعها على الشبكة العنكبوتية من خلال موقع

¹ المحكمين هم: د. حسين أحمد، مدير مركز استطلاعات الرأي والدراسات المسحية، جامعة النجاح الوطنية، نابلس، د. نائل طه، برنامج القانون العام / دراسات عليا / جامعة النجاح الوطنية، د. أنور جاني، نائب لعميد كلية القانون بجامعة النجاح الوطنية ومدير مركز التدريب القانوني.

التواصل الاجتماعي فيسبوك. بعد ذلك تم إجراء تحليل الاستبيان باستخدام (Google Forms) وبرنامج SPSS حيث تم الاستعانة بخبير تحليل احصائي¹.

صدق وثبات أداة الدراسة

بعد إعداد الاستبيان الدراسة بصورتها الأولية وللتحقق من صدقها، تم عرضها على المشرف وعلى مجموعة من ذوي الاختصاص بهدف التأكد من صدق محتوى الأسئلة المكونة للاستبانة، ومدى ملاءمتها لأهداف الدراسة ومتغيراتها، وقد أشاروا إلى صلاحية أداة الدراسة. ولقياس ثبات أداة الدراسة تم استخدام معامل ثبات هذه الدراسة باستخدام معادلة كرونباخ الفا (Cronbach Alpha)، وقد بلغت قيمة معامل الثبات (0.73) كما في الجدول رقم 2 وهو معامل ثبات جيد يفي بأغراض البحث العلمي.

جدول رقم (2): نتائج معامل كرونباخ الفا (Cronbach Alpha) باستخدام برنامج SPSS.

		N	%
Cases	Valid	516	100.0
	Excluded	0	.0
	Total	516	100.0
Reliability Statistics			
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items	
.726	.802	21	

مجتمع الدراسة

يتكون مجتمع الدراسة من أفراد المجتمع الفلسطيني في الضفة الغربية وقطاع غزة ممن لديهم نفاذ لشبكة الإنترنت ومواقع التواصل الاجتماعي للفترة الواقعة ما بين (18 - 24) آب 2017 والمقدر عددهم (2,537,600) بناءً على تقرير وسائل التواصل الاجتماعي في فلسطين 2016 الصادر عن سوشال ستوديو².

¹ أحمد دابوقي، خبير تحليل البيانات، مشروع مجتمعات مزدهرة، نترا تيك، رام الله.

² تقرير وسائل التواصل الاجتماعي في فلسطين 2016 الصادر عن سوشال ستوديو بالشراكة مع شركة الاتصالات الفلسطينية والمنشور على الموقع www.socialstudio.me.

عينة الدراسة

استخدام الباحث برنامج¹ Raosoft Sample size calculator، لاختيار عينة عشوائية ممثلة أفراد المجتمع الفلسطيني في الضفة الغربية وقطاع غزة ممن لديهم نفاذ لشبكة الإنترنت ومواقع التواصل الاجتماعي، وقد بلغ حجم عينة الدراسة (601) فرد. وبهامش خطأ 4% ومستوى ثقة 95%، كما بلغت نسبة الاستجابة على الاستبيان من مجتمع الدراسة (86%) أي ما يعادل (516) فرد.

الفرع الأول: خصائص العينة

يبين الجدول رقم (3) حجم عينة الدراسة وخصائصها وفق المتغيرات المستقلة (الجنس، مكان السكن، العمر، المهنة، المستوى العلمي) حيث بلغ عددها 516 موزعة على النحو الآتي 51.7% من حجم العينة إناث، و48.3% ذكور، ومن حيث مكان السكن فإن 47.3% يعيشون في المدينة، و41.5% في القرية، و11.2% في المخيم، وتوزيعها حسب متغير العمر بنسبة 1.9% أقل من 18 سنة، و65.1% أعمارهم ما بين 18 – 29، و28.5% تتراوح أعمارهم ما بين 30 – 49، و4.1% لمن أعمارهم ما بين 50 – 64، و0.4% لمن تزيد أعمارهم عن 65 سنة، وتصنيفها وفقاً للمهنة فإن 30.2% طلاب، و12.6% موظفي قطاع عام، و18.8% موظفي قطاع خاص، و12.4% موظفي قطاع أهلي، و14.3% يعمل لحسابه الخاص في حين أفاد 11.6% بأنهم عاطلون عن العمل. وعلى صعيد التحصيل العلمي فقد أفاد 1.6% بأنهم أقل من ثانوي، و6.2% ثانوي، و4.5% معهد، و66.1% يحملون شهادة البكالوريوس، في حين أن 21.7% يحملون شهادات الدراسات العليا.

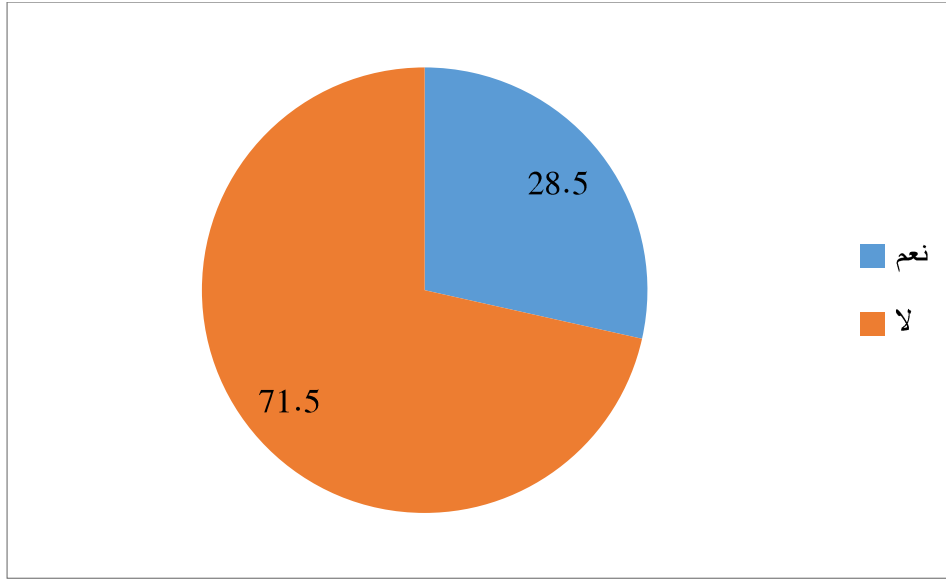
¹تم استخدام الحاسبة الإلكترونية على الموقع <http://www.raosoft.com/samplesize.html> وتم الدخول للموقع بتاريخ 2018/01/24.

جدول رقم (3): توزيع أفراد عينة الدراسة تبعاً لمتغيرات الدراسة المستقلة.

المتغيرات	الفئة	العدد	النسبة المئوية
الجنس	ذكور	249	48.3
	إناث	267	51.7
	المجموع	516	100
مكان السكن	مدينة	244	47.3
	قرية	214	41.5
	مخيم	58	11.2
	المجموع	516	100
العمر	أقل من 18	10	1.9
	18 – 29	336	65.1
	30 – 49	147	28.5
	50 – 64	21	4.1
	65 فأكثر	2	0.4
	المجموع	516	100
المهنة	طالب	156	30.2
	موظف قطاع عام	65	12.6
	موظف قطاع خاص	97	18.8
	قطاع أهلي	64	12.4
	عاطل عن العمل	60	11.6
	يعمل لحسابه	74	14.3
	المجموع	516	100
المستوى العلمي	أقل من ثانوي	8	1.6
	ثانوي	32	6.2
	معهد	23	4.5
	بكالوريوس	341	66.1
	دراسات عليا	112	21.7
	المجموع	516	100

الفرع الثاني: تعرض أفراد العينة إلى جريمة الكترونية

بلغ عدد الذين تعرضوا إلى جريمة الكترونية 147 فرداً أي ما نسبته 28.5% من أفراد العينة، في حين بلغت نسبة الذين لم يتعرضوا إلى جريمة الكترونية 71.5%. كما يبين من الشكل رقم (5)، ومن حيث مكان السكن تشكل نسبة الذكور الذين تعرضوا إلى جرائم الكترونية 43.8% في المدن 47.5% في القرى و36.4% في المخيمات، مقارنة مع الإناث 56.3% في المدن و52.5% بالقرى و63.6% في المخيمات، ووفقاً للفئة العمرية للذكور فإن 39.4% لمن تتراوح أعمارهم ما بين 18 – 29 تعرضوا لجرائم الكترونية و47.7% لمن يتراوح أعمارهم ما بين 30 – 49، و85.7% للذين تبلغ أعمارهم من 50 – 64، وأما الإناث فإن 60.6% تعرضن لجرائم الكترونية لمن تتراوح أعمارهن ما بين 18 – 29، و52.3% للفئة العمرية من 30 – 49، و14.3% من 50 – 64، وحسب طبيعة المهنة للذكور فإن 31.8% من الطلاب تعرضوا لجريمة الكترونية و55% موظف من القطاع عام و46.9% موظف من القطاع خاص و25% موظف من القطاع أهلي و43.8% من العاطلين عن العمل و73.7% لمن يعمل لحسابه الخاص، وبالمقارنة مع الإناث فإن 68.2% من الطالبات تعرضن لجريمة الكترونية و45% من موظفات القطاع عام و53.1% من موظفات القطاع الخاص و75% من موظفات القطاع الأهلي و56.3% من العاطلات عن العمل و26.3% ممن يعملن لحسابهن الخاص، ووفقاً للمستوى العلمي للذكور فإن 66.7% من حملة الثانوية العامة تعرضوا لجرائم معلوماتية و75% حملت شهادات المعهد و35.9% من حملت شهادات البكالوريوس و63.3% من الحاصلين على دراسات عليا، أما بالنسبة للإناث 33.3% من الحاصلات على الثانوية العامة و25% ممن يحملن شهادة المعهد و64.1% حاصلات على درجة البكالوريوس و36.7% من حاملات الدراسات العليا، ودلت النتائج على أن ما يزيد على ربع المجتمع الفلسطيني قد تعرض إلى جريمة الكترونية. وهذا يشير إلى انتشار ظاهرة الجرائم الإلكترونية بين أفراد المجتمع الفلسطيني بشكل يثير القلق مما يستوجب اتخاذ الإجراءات الكفيلة للوقاية والحد منها.



الشكل رقم (5): مدى تعرض أفراد العينة إلى جريمة الكترونية

الفرع الثالث: عدد المرات التي تعرض فيها أفراد العينة لجريمة الكترونية

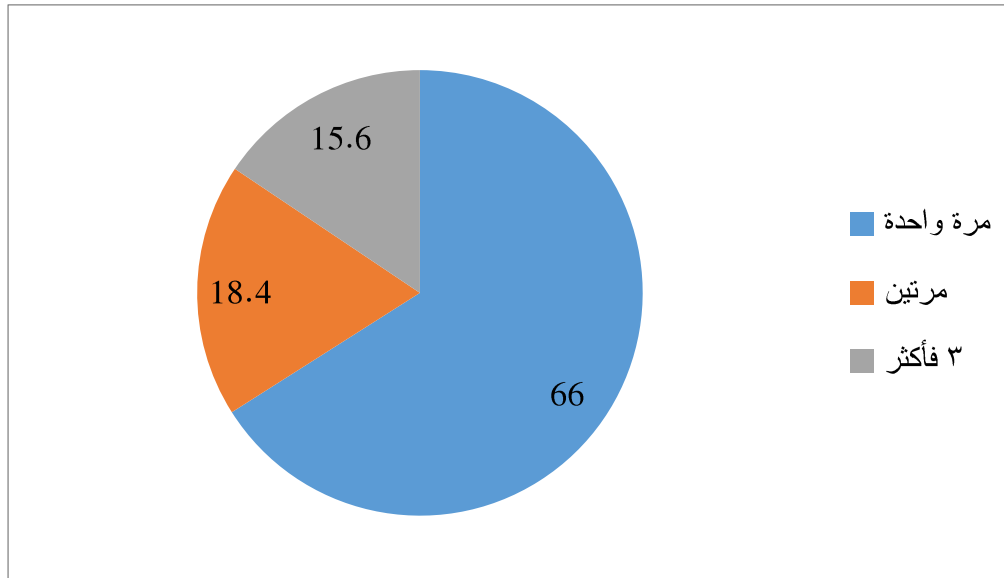
بينت نتائج الاستبيان أن 66% من أفراد العينة تعرضوا إلى جريمة الكترونية لمرة واحدة، في حين أفاد 18.4% تعرضوا لها مرتين، و15.6% تعرضوا لها ثلاث مرات فأكثر كما يتبين من الشكل رقم (6)، بلغت نسبة الذكور الذين تعرضوا لجريمة الكترونية لمرة واحدة 45.4% مقابل 54.6% من الإناث، و55.6% من الذكور تعرضوا لمرتين مقابل 44.4% من الإناث، و26.1% من الذكور تعرضوا ثلاث مرات أو أكثر مقابل 73.9% من الإناث. ويلاحظ من هذه النتائج أن تعرض الإناث لجريمة الكترونية مرة واحدة وثلاث مرات نسبتها أعلى مقارنة مع الذكور في حين أن الذكور تعرضوا مرتين بنسبة أعلى من الإناث، وهذا يشير إلى أن الجرائم الإلكترونية أكثر انتشاراً بين الإناث من الذكور وقد يعود ذلك إلى استخدام الإناث للشبكة المعلوماتية ووسائل التواصل الاجتماعي أكثر من الذكور وكذلك الوعي القانوني بمخاطر الجرائم الإلكترونية لدى الذكور أعلى من الإناث.

بلغت نسبة الذكور الذين تعرضوا لجرائم الكترونية 44.6% مقابل 55.4% من الإناث، ويسكنون 53.6% منهم في المدن و40.2% بالقرى و6.3% في المخيمات، وبلغت نسبة الجرائم التي ارتكبت مرة واحدة في المدن 70% و20% مرتين و10% ثلاث مرات فأكثر،

وفي القرى بلغت 73.3% مرة واحدة و13.3% مرتين و13.3% ثلاث مرات فأكثر، وفي المخيمات 71.4% مرة واحدة و28.6% مرتين، وحسب المؤهل العلمي فإن 82.1% ممن يحملون شهادة البكالوريوس تعرضوا لجريمة إلكترونية لمرة واحدة و13.1% دراسات عليا و2.4% أقل من ثانوي و1.2% ثانوي و1.2% معهد، أما بخصوص الذين تعرضوا مرتين لتلك الجرائم فإن 75% من حملة البكالوريوس و10% دراسات عليا و10% أقل من ثانوي و5% ثانوي و0% معهد، وأما الذين تعرضوا لثلاثة مرات فأكثر 80% بكالوريوس و10% أقل من ثانوي و10% من حملة الدراسات العليا، وحسب طبيعة المهنة فإن 69.6% طلاب و10% يعملون لحسابه الخاص و8% من موظفي القطاع الخاص و5.4% من العاطلين عن العمل و3.6% من القطاع الأهلي و2.7% من القطاع العام، أما الذين تعرضوا لجريمة إلكترونية مرة واحدة 77.5% من الطلاب و8.8% من القطاع الخاص و6.3% يعمل لحسابه الخاص و3.8% من القطاع الأهلي و3.8% من العاطلين عن العمل، أما بخصوص الذين تعرضوا مرتين لتلك الجرائم أفاد 65% بأنهم طلاب و15% من العاطلين عن العمل و5% من موظفي القطاع الأهلي و5% يعمل لحسابه الخاص و0% موظفي قطاع خاص. وبخصوص الذين تعرضوا لجريمة إلكترونية ثلاث مرات فأكثر فإن 50% من يعمل لحسابه الخاص و25% من الطلاب و16.7% موظف قطاع خاص و8.3% موظف قطاع عام، وحسب الفئة العمرية فإن 3% من تقل أعمارهم عن 18 و90% تتراوح أعمارهم 18 - 29 و6% من 30 - 49 و1% ما بين 50 - 64، والذين ارتكبت بحقهم جريمة إلكترونية لمرة واحدة 1.3% أقل من 18 و93.8% ما بين 18 - 29 و3.8% من 30 - 49 و1.3% ما بين 50 - 64، وبخصوص من تعرض مرتين فإن 10% أقل من 18 و75% ممن بلغت أعمارهم 18 - 29 و15% لمن يتراوح 30 - 49 والذين تعرضوا ثلاث مرات فأكثر فإن 92% لمن بلغت أعمارهم ما بين 18 - 29 و8% لمن يتراوح عمره من 30 - 49.

يتضح من النتائج تعرض الإناث أكثر من الذكور لجرائم إلكترونية، وتنتشر بشكل أوسع على من يسكنون المدن يليها القرى والمخيمات، ويحتل سكان القرى المرتبة الأولى في الجرائم المرتكبة لمرة واحدة والمخيمات لمرتين والمدن لثلاث مرات فأكثر، كما أن هذه الجرائم أكثر

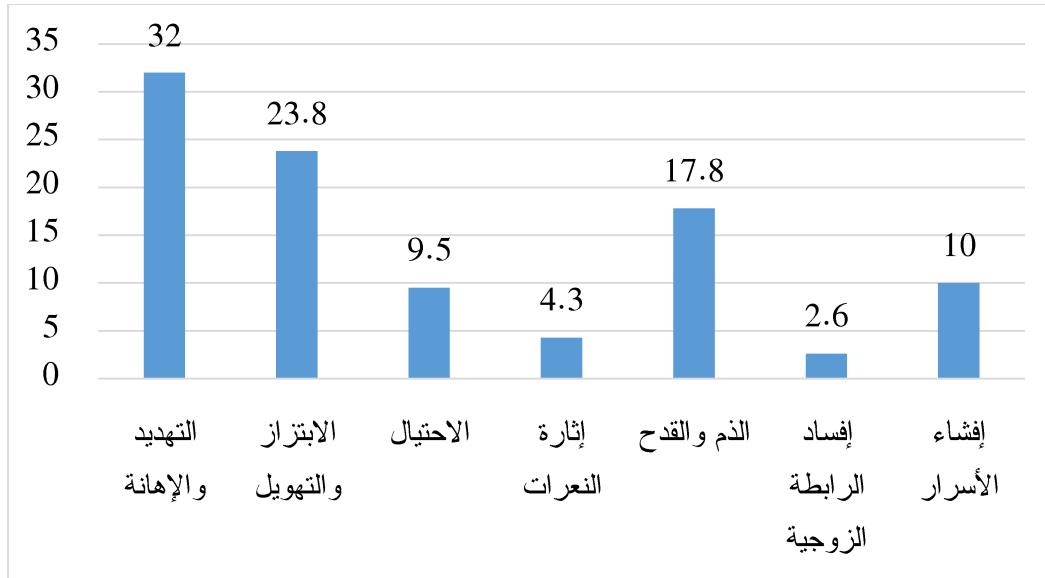
انتشاراً بين الطلاب ومن حملة شهادة البكالوريوس والفئة العمرية 18 – 29. وقد يعود ذلك إلى انتشار استخدام الشبكة المعلوماتية في المدن بشكل أوسع وأكثر انفتاحاً من القرى والمخيمات وكذلك تركز تواجد الجامعات والمعاهد والكليات في المدن بالإضافة إلى أن فئة الشباب هي من أكثر الفئات استخداماً لوسائل التواصل الاجتماعي.



الشكل رقم (6): عدد المرات التي تعرض فيها أفراد العينة لجريمة إلكترونية.

الفرع الرابع: نوع الجريمة الإلكترونية التي تعرض لها أفراد العينة

احتلت جريمة التهديد والإهانة مركز الصدارة بنسبة 32%، تلتها جريمة الابتزاز والتهويل بنسبة 23.8%، ثم الذم والقذح بنسبة 17.8%، وإفشاء الأسرار بنسبة 10%، يليها الاحتيال بنسبة 9.5%، ثم إثارة النعرات بنسبة 4.3%، وأخيراً إفساد الرابطة الزوجية بنسبة 2.6%. كما يوضح الشكل رقم (7).

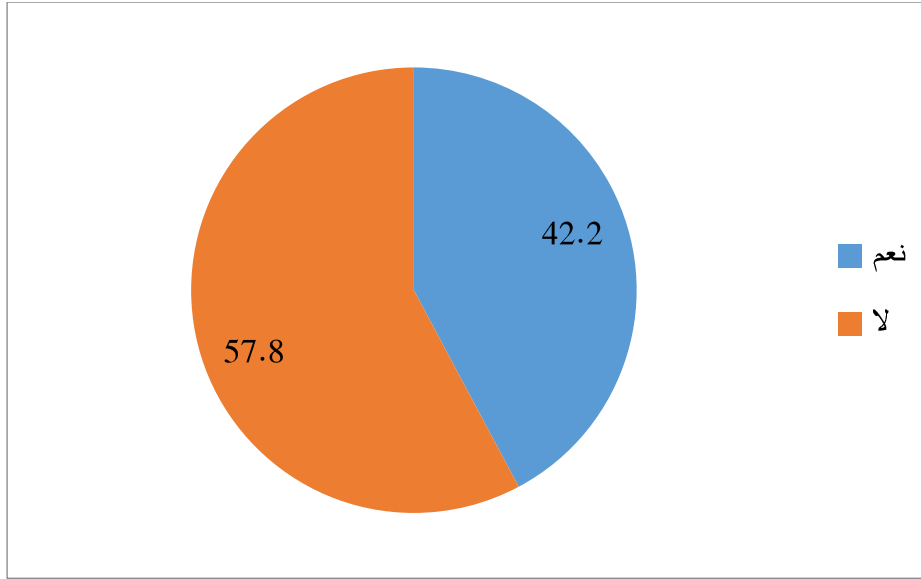


الشكل رقم (7): نوع الجريمة الإلكترونية التي تعرض لها أفراد العينة.

تشير هذه النتائج إلى أن أكثر أنواع الجرائم الإلكترونية انتشاراً في فلسطين هي التهديد والإهانة والابتزاز والتهويل والذم والقذح حيث تشكل ما نسبته 73.6% من مجموع الجرائم الإلكترونية المرتكبة.

الفرع الخامس: تقديم الشكاوى لدى الجهات المختصة

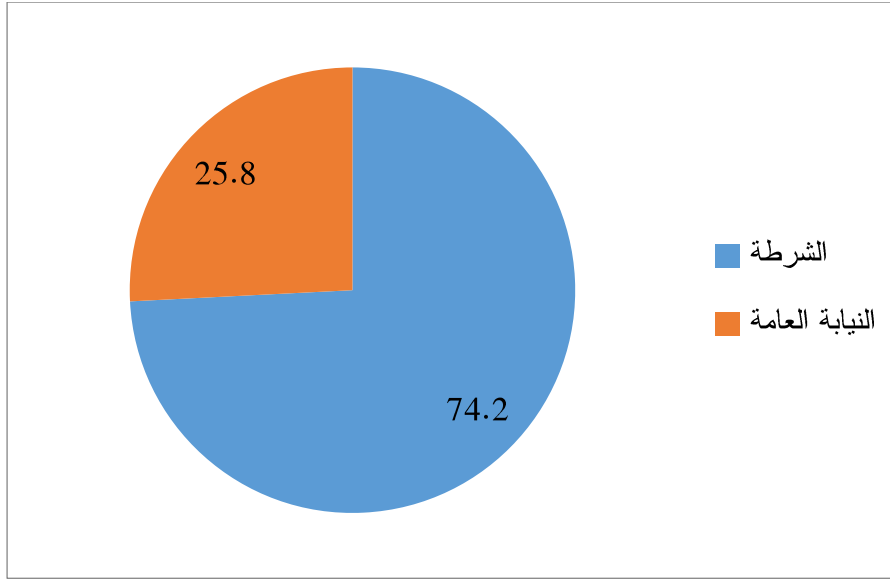
عند سؤال المستطلع آراؤهم ممن تعرضوا لجريمة الكترونية وهم 147 فرداً من حجم العينة حول إذا ما قاموا بتقديم شكوى لدى الجهات المختصة فقد أفاد 57.8% بأنهم لم يقوموا بتقديم شكوى، في حين أفاد 42.2% بأنهم قاموا بتقديم شكوى لدى الجهات المختصة. كما يبين الشكل رقم (8).



الشكل رقم (8): تقديم الشكاوى لدى الجهات المختصة.

تشير النتائج أن الغالبية العظمى ممن تعرضوا إلى جرائم إلكترونية لم يتقدموا بشكاوى إلى الجهات المختصة مما يتطلب نشر الثقافة القانونية وتوعية الجمهور بالمخاطر الناجمة عن عدم تقديم الشكاوى وملاحقة مرتكبيها.

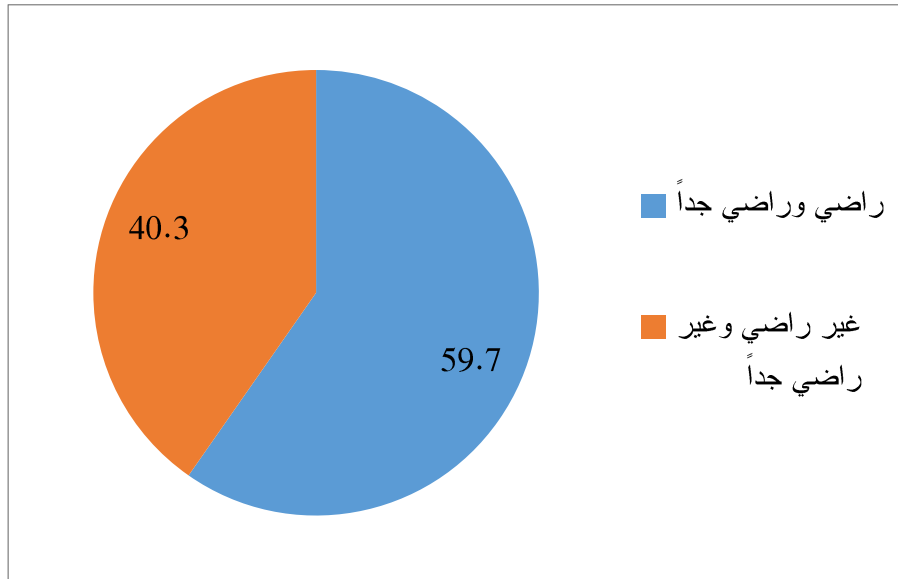
بينت نتائج الاستبيان أن 74.2% من أفراد العينة تقدموا بشكاوهم للشرطة الفلسطينية مقابل 25.8% قدموها للنيابة العامة. كما يوضح الشكل رقم (9)، وأفاد 72.4% من الذكور بتقديمهم الشكاوى لدى جهاز الشرطة وان 27.6% منهم تقدموا بشكاوى لدى النيابة العامة، أما بخصوص الإناث فان 75.8% قد تم تقديمها إلى جهاز الشرطة و 24.2% للنيابة العامة. تشير هذه النتائج إلى أن معظم الشكاوى من الذكور والإناث قُدمت إلى جهاز الشرطة الفلسطيني، مما يشير إلى ثقة المواطن بأداء جهاز الشرطة الفلسطيني وعمله الدؤوب في ملاحقة مرتكبي الجرائم الإلكترونية.



الشكل رقم (9): الجهات التي قدمت إليها الشكاوى.

الفرع السادس: مدى رضا أفراد العينة عن نتائج الشكاوى

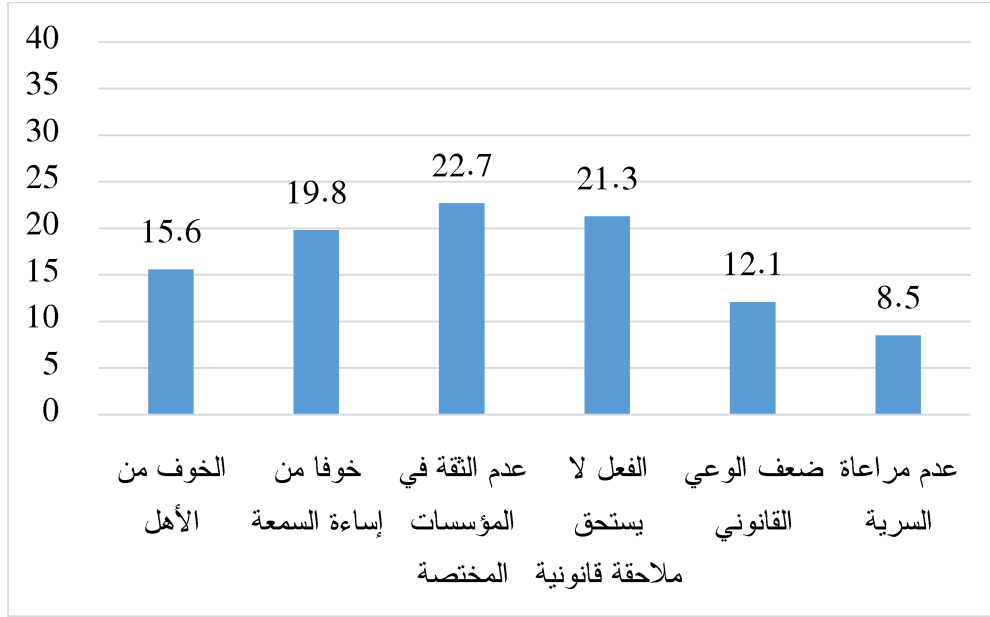
وحول نتيجة رضى أفراد العينة عن نتائج متابعة الشكاوى التي تقدموا بها أفاد 59.7% بأنهم راضون وراضون جداً في حين أن 40.3% بأنهم غير راضون وغير راضون جداً عن نتائج متابعة الشكاوى. كما يظهر في الشكل رقم (10)، أفاد 57.1% من الذكور مقابل 60% من الإناث بأنهم راضون عن نتائج الشكاوى المقدمة لدى جهاز الشرطة، في حين أن 42.9% من الذكور مقابل 40% من الإناث بأنهم غير راضون عن نتائج الشكاوى المقدمة لدى جهاز الشرطة، أما بخصوص النيابة العامة فقد أفاد 62.5% من الذكور مقابل 50% من الإناث برضاهم عن نتائج الشكاوى المقدمة لدى النيابة العامة. وان 37.5% من الذكور مقابل 50% من الإناث غير راضين من نتائج الشكاوى المقدمة لدى النيابة العامة. دلت هذه النتائج على رضى الإناث بنسبة أعلى من رضى الذكور في الشكاوى المقدمة لجهاز الشرطة مقابل رضى الذكور بنسبة أعلى من رضى الإناث في الشكاوى المقدمة لدى النيابة العامة. وتفيد هذه النتائج على اهتمام الشرطة والنيابة العامة بمتابعة الشكاوى التي يقدمها المواطن والعمل على سرعة إنجازها لمحاربة تلك الظاهرة في المجتمع الفلسطيني.



الشكل رقم (10): مدى رضا افراد العينة عن نتائج الشكاوى.

الفرع السابع: الأسباب التي حالت دون تقديم الشكاوى من قبل أفراد العينة لدى الجهات المختصة ضد مرتكبي الجرائم الإلكترونية

عند سؤال من تعرضوا لجريمة الكترونية ولم يتقدموا بشكاوى لدى الجهات المختصة حول الأسباب التي دفعتهم لعدم تقديمها أفاد 22.7% بعدم الثقة في المؤسسات المختصة، و21.3% بأن الفعل لا يستحق ملاحقة قانونية، و19.8% خوفاً من إساءة السمعة، و15.6% خوفاً من الأهل، و12.1% بضعف الوعي القانوني في حين أفاد 8.5% بعدم مراعاة السرية. كما يبين الشكل رقم (11)، وتشير هذه النتائج إلى ضرورة قيام الجهات المختصة بتعزيز ثقة المواطن بعملها وأدائها، ونشر الثقافة القانونية وتعزيزها بين أفراد المجتمع، وعدم الخوف من إساءة السمعة وضرورة تعزيز الثقة والانفتاح بين أفراد الأسرة وتطمئنه المواطن بوجود السرية في العمل.

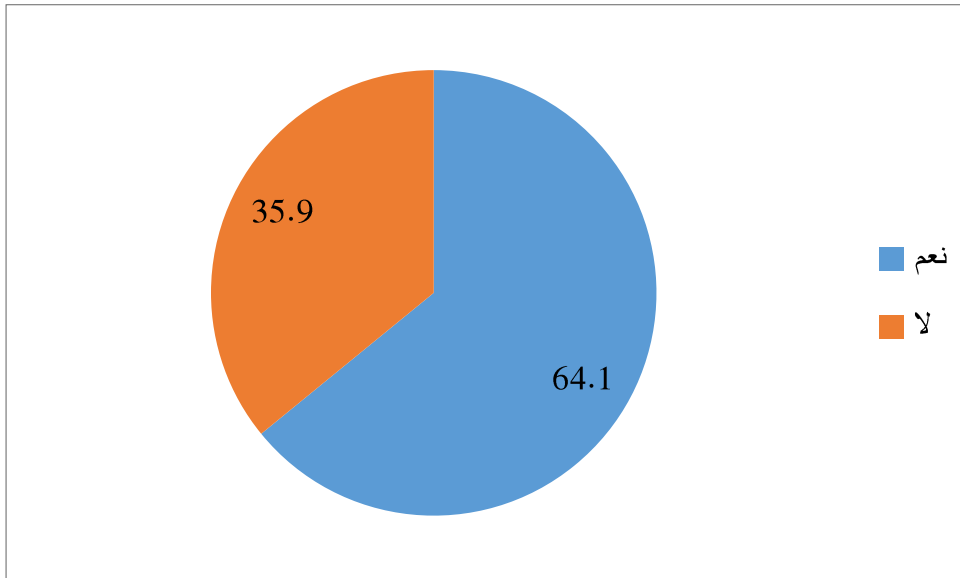


الشكل رقم (11): الأسباب التي حالت دون تقديم الشكوى من قبل افراد العينة لدى الجهات المختصة ضد مرتكبي الجرائم الالكترونية

الفرع الثامن: مدى معرفة أفراد العينة بالقرار بقانون بشأن الجرائم الإلكترونية

حول مدى معرفة أفراد العينة بالقرار بقانون بشأن الجرائم الإلكترونية أفاد 64.1% بأنهم على معرفة به في حين أفاد 35.9% بأنهم لا يعرفون هذا القانون. كما يوضح الشكل رقم (12)، بلغت نسبة الذكور الذين لديهم معرفة بهذا القرار بقانون 51.1% مقابل 48.9% من الإناث، وقد بينت النتائج أن 69.2% ممن تراوح أعمارهم بين 18 – 29 وأن 25.4% ممن بلغت أعمارهم ما بين 30 – 49 وأن 3.9% من الفئة العمرية 50 – 64 لديهم معرفة بالقرار بقانون بشأن الجرائم الإلكترونية، وحسب مكان السكن أفاد 45.6% ممن لديهم معرفة بالقرار بقانون هم من سكان المدن و45% من سكان القرى و9.4% من سكان المخيمات، ووفقاً للمستوى العلمي أفاد 4.8% شهادة الثانوية و4.2% معهد و67.4% بكالوريوس و22.7% دراسات عليا يعرفون بالقرار بقانون، أما بخصوص المهنة أفاد 33.2% من الطلاب و12.4% من موظفي القطاع العام و15.7% من موظفي القطاع الخاص و11.5% من موظفي القطاع الأهلي و9.1% من العاطلين عن العمل و18.1% ممن يعملون لدى حسابهم الخاص بمعرفتهم به. دلت هذه النتائج على المعرفة بالقرار بقانون بشأن الجرائم الإلكترونية لدى الذكور أعلى من الإناث،

والمدن أعلى من القرى والمخيمات، وبين الفئات العمرية التي تتراوح ما بين 18 - 29 و30 - 45، وكذلك الطلاب وحاملي شهادة البكالوريوس والدراسات العليا لديهم معرفة بالقرار بقانون بشأن الجرائم الإلكترونية أكثر من باقي فئات وأفراد المجتمع الفلسطيني. وتدل هذه النتيجة على حجم الوعي والثقافة لدى أفراد المجتمع اتجاه القرار بقانون بشأن الجرائم الإلكترونية وهم يمثلون الفئة الأكثر استخداماً للوسائل التقنية ومواقع التواصل الاجتماعي، وأهمية وجود مثل هذا القانون في فلسطين لمحاربة هذه الجريمة كونه يمس شرائح واسعة من المجتمع الفلسطيني. وينبغي تكثيف جهود المؤسسات ذات العلاقة بالتواصل مع أكثر من ثلث أفراد المجتمع الذين لا يعرفون على هذا القرار بقانون لتعميمه ونشره.

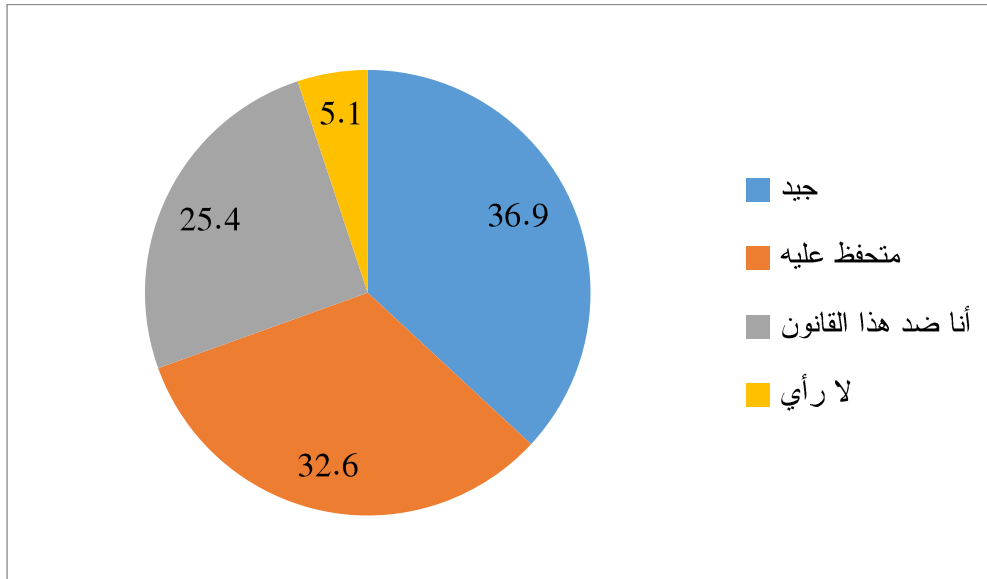


الشكل رقم (12): مدى معرفة افراد العينة بالقرار بقانون بشأن الجرائم الإلكترونية.

الفرع التاسع: رأي أفراد العينة بالقرار بقانون بشأن الجرائم الإلكترونية

يرى 36.9% من أفراد العينة بأن القرار بقانون بشأن الجرائم الإلكترونية جيد، و32.6% متحفظون عليه، و25.4% ضد هذا القانون، في حين أفاد 5.1% لا رأي لهم بهذا القانون. كما يتبين من الشكل رقم (13)، يتضح من النتائج أن 63.1% من أفراد العينة متحفظون وضد ولا رأي لهم بهذا القرار بقانون، مما يستدعي تكثيف جهود السلطة التنفيذية والتشريعية لتوعية

الجمهور بمواده وأهدافه من خلال تضافر الجهود مع أصحاب الاختصاص ومؤسسات المجتمع المدني.



الشكل رقم (13): رأي افراد العينة بالقرار بقانون بشأن الجرائم الإلكترونية.

بلغت نسبة الذكور الذين أبدوا آراءهم حول القرار بقانون بشأن الجرائم الإلكترونية 49.3% مقابل 50.7% من الإناث، موزعين حسب مكان السكن 46% يسكنون في المدن و 44.9% في القرى و 9.1% في المخيمات، وحسب الفئة العمرية فان 69.2% ممن تراوحت أعمارهم 18 – 29 و 25% لمن بلغت أعمارهم ما بين 30 – 49 و 4% لما كانت أعمارهم 50 – 64، فيما يخص المستوى العلمي فان 5.1% ممن ادلو بأرائهم يحملون شهادة الثانوية و 4.3% معهد و 66.3% بكالوريوس و 23.2% دراسات عليها، من حيث المهنة فان من عبروا عن آرائهم 33.7% من الطلاب و 13.4% من موظفي القطاع العام و 16.7% من موظفي القطاع الخاص و 11.2% من موظفي القطاع الأهلي و 8.7% من العاطلين عن العمل و 16.3% ممن يعملون لحسابه الخاص. دلت هذه النتائج على أن معرفة الإناث القرار بقانون بشأن الجرائم الإلكترونية أكثر من الذكور، وان الفئات العمرية الأكثر معرفه به ما بين 18 – 29 و 30 – 49، والمدن الأعلى معرفة مقارنة مع القرى والمخيمات، وان الطلاب يحتلون المرتبة الأولى بمعرفتهم بهذا

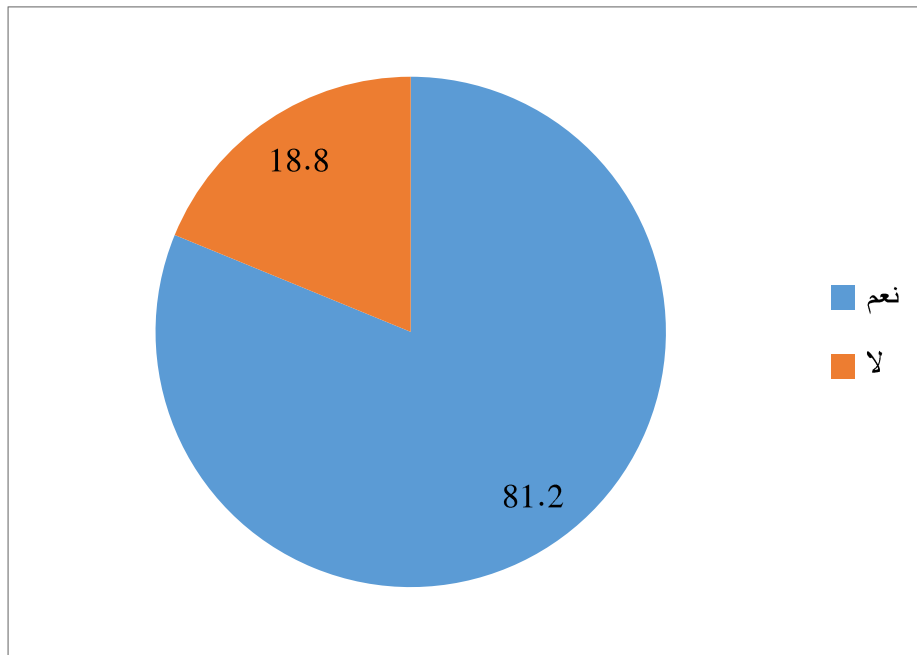
القرار بقانون، أما حملت شهادة البكالوريوس والدراسات العليا فانهم أكثر معرفة ممن يحملون شهادة المعهد والثانوية العامة.

أفاد 52% ممن بلغت أعمارهم ما بين 18 - 29 بأنهم ضد القرار بقانون بشأن الجرائم الإلكترونية و41% لمن تراوحت أعمارهم 30 - 49 و4% للفئة العمرية 50 - 64 و4% لمن تقل أعمارهم عن 18، وأما الذين أفادوا بأنه جيد 80% لمن تراوحت أعمارهم 18 - 29 و18% ممن تراوحت أعمارهم 30 - 49 و3% من بلغت أعمارهم ما بين 50 - 64، أما الذين تحفظوا عليه 65% ممن بلغت أعمارهم 18 - 29 و26% من الذين بلغت أعمارهم 30 - 49 و6% لمن تراوحت أعمارهم 50 - 64 و2% لمن تقل أعمارهم عن 18 و1% لعمر 65 فأكثر. وبخصوص الذين لا رأي لهم به فإن 80% من الذين تتراوح أعمارهم 18 - 29 و20% ممن بلغت أعمارهم 30 - 49 و6% ممن بلغ 50 - 64.

الفرع العاشر: مدى استعداد أفراد العينة لتقديم شكوى لدى الجهات المختصة ضد مرتكبي الجرائم الإلكترونية

بعد صدور القرار بقانون بشأن الجرائم الإلكترونية أفاد 81.2% بأن لديهم الاستعداد لتقديم شكوى في حال تعرضهم إلى جريمة إلكترونية في حين أجاب 18.8% بأنهم ليس لديهم الاستعداد لتقديم شكوى بعد صدور هذا القانون كما يبين في الشكل رقم (14). بلغت نسبة الذكور الذين لديهم استعداد لتقديم شكوى 47.3% مقابل 52.7% من الإناث، وحسب مكان السكن فإن 47.5% ممن يسكنون المدن و42.5% في القرى و10% في المخيمات لديهم استعداد لتقديم شكوى حال تعرضهم لجريمة إلكترونية، أما وفق الفئة العمرية فإن 66.3% ممن تتراوح أعمارهم ما بين 18 - 29 و27.2% تراوحت أعمارهم 30 - 49 وان 4.1% بلغت أعمارهم من 50 - 64 لديهم استعداد لتقديم شكوى، وبخصوص المهنة أفاد 31.3% من الطلاب و12.6% من موظفي القطاع العام و20.3% من موظفي القطاع الخاص و11.2% من موظفي القطاع الأهلي و11.5% من عاطلين عن العمل و13.1% ممن يعملون لحسابه الخاص استعدادهم لتقديم شكوى. دلت هذه النتائج على أن استعداد الإناث لتقديم شكوى ضد

مرتكب جريمة إلكترونية أعلى من الذكور، وكذلك الذين يسكنون في المدن ومن الحاصلين على مؤهل البكالوريوس والدراسات العليا وفئة الطلاب والفئة العمرية من 18 – 29 أعلى من باقي أفراد وفئات المجتمع الفلسطيني. تشير هذه النتائج إلى أهمية وجود القانون كمحفز أساسي لدفع المواطنين وتشجيعهم على تقديم الشكاوى ضد مرتكبي الجرائم الإلكترونية.

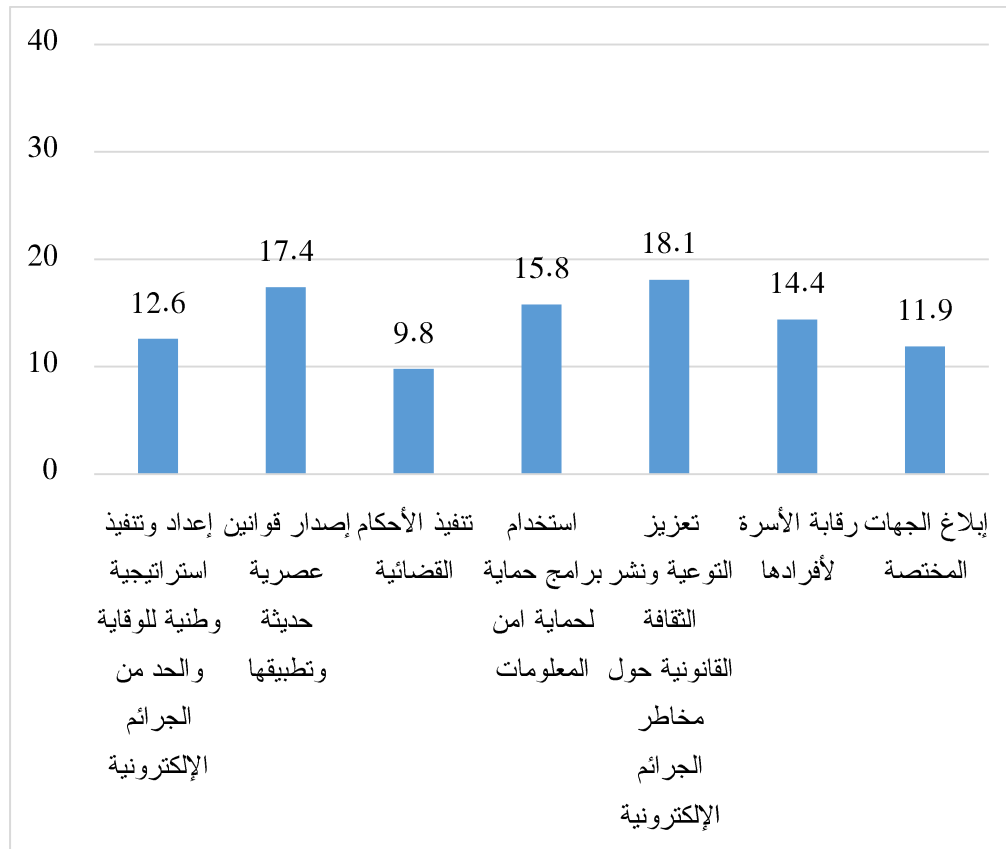


الشكل رقم (14): مدى استعداد أفراد العينة لتقديم شكوى لدى الجهات المختصة ضد مرتكبي الجرائم الإلكترونية بعد صدور القرار بقانون بشأن الجرائم الإلكترونية.

الفرع الحادي عشر: الإجراءات الواجب اتخاذها حسب أفراد العينة للحد من الجرائم الإلكترونية في فلسطين

يرى أفراد العينة أن الإجراءات الواجب اتخاذها للحد من الجرائم الإلكترونية في فلسطين تتمثل في تعزيز التوعية ونشر الثقافة القانونية حول مخاطر الجرائم الإلكترونية ونسبة 18.1%، وإصدار قوانين عصرية حديثة وتطبيقها بنسبة 17.4%، واستخدام برامج حماية لحماية أمن المعلومات بنسبة 15.8%، ورقابة الأسرة لأفرادها بنسبة 14.4%، وإعداد وتنفيذ استراتيجية وطنية للوقاية والحد من الجرائم الإلكترونية بنسبة 12.6%، وإبلاغ الجهات المختصة بنسبة 11.9%، وتنفيذ الأحكام القضائية بنسبة 9.8%. كما يبين الشكل رقم (15)، تشير هذه النتائج

إلى ضرورة تعزيز ونشر التوعية والثقافة القانونية حول مخاطر الجريمة الإلكترونية، وإصدار قوانين عصرية وحديثة وتطبيقها، وإعداد وتنفيذ استراتيجية وطنية للوقاية والحد من الجرائم الإلكترونية، وتعزيز رقابة الأسرة لأفرادها، وتشجيع المواطنين على إبلاغ الجهات المختصة حال وقوع هذه الجرائم.



الشكل رقم (15): الإجراءات الواجب اتخاذها حسب أفراد العينة للحد من الجرائم الإلكترونية في فلسطين

أظهرت نتائج الاستبيان أن 28.5% من أفراد العينة تعرضوا إلى جرائم الكترونية، وأكثرها انتشاراً كانت ما بين الفئات العمرية 18 – 49، ونسبة ارتكابها بين الإناث أعلى من الذكور، أما من حيث المهنة احتل الطلاب مركز الصدارة في انتشارها، وحسب المؤهل العلمي فكان حملة البكالوريوس الأكثر تعرضاً لهذه الجرائم، كما بينت الدراسة أن 66% من أفراد العينة تعرضوا لها لمرة واحدة و18.4% مرتين و15.3% ثلاث مرات فأكثر، أما أكثرها انتشاراً في فلسطين كانت التهديد والإهانة يليها الابتزاز والتهويل، الذم والقدح، إفشاء الأسرار، الاحتيال، إثارة النعرات، وإفساد الرابطة الزوجية على التوالي، وأظهرت الدراسة أن 57.8% لم يقدموا

شكاوى ضد مرتكبي الجرائم الإلكترونية، بسبب ضعف الثقة بالمؤسسات ذات العلاقة، الجريمة لا تستحق ملاحقة قانونية، الخوف من إساءة السمعة، الخوف من الأهل، ضعف الوعي القانوني، وعدم مراعاة السرية، وبخصوص المعرفة بالقرار بقانون بشأن الجريمة الإلكترونية أفاد 64.1% من أفراد العينة لديهم معرفه به، ورأى 36.9% بأنه جيد مقابل 63.1% ما بين ضد ومتحفظ ولا رأي له، وحسب وجهة نظر أفراد العينة فإن الإجراءات الواجب اتخاذها للحد من الجرائم المعلوماتية في فلسطين تمثلت في نشر التوعية والثقافة القانونية حول مخاطر الجريمة الإلكترونية، إصدار قوانين عصرية وحديثة وتطبيقها، إعداد وتنفيذ استراتيجية وطنية للوقاية والحد من الجرائم الإلكترونية، تعزيز رقابة الأسرة لأفرادها، وإبلاغ الجهات المختصة.

ويتضمن الملحق رقم 1 الأسئلة التفصيلية لأداة الدراسة وكذلك التحليل التفصيلي لنتائجها، بينما يتضمن الملحق رقم 2 أداة الدراسة.

اختبار فرضيات الدراسة

❖ نتائج الفرضية الأولى

من أجل دراسة صحة الفرضية القائلة بأنه "لا يوجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متغير (التعرض لجريمة الكترونية) والمتغيرات الديموغرافية (الجنس، مكان السكن، العمر، المستوى العلمي)"، أي أن متغيرات مستقلة، فقد تم استخدام اختبار كاي تربيع - Chi-Square للمتغيرات المستقلة وذلك لأن المتغيرات اسمية وكانت النتائج كما هو مبين في الجداول (4، 5، 6، 7).

أ- لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متغير (التعرض لجريمة الكترونية) ومتغير الجنس.

الجدول (4): نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين متغير التعرض لجريمة الكترونية ومتغير الجنس.

		الجنس		المجموع
		ذكر	أنثى	
هل تعرضت إلى جريمة الكترونية	نعم	65	82	147
	لا	184	185	369
المجموع		249	267	516
نتائج اختبار مربع كاي (Chi-Square Tests) بين متغير تعرض لجريمة الكترونية ومتغير الجنس				
	Value	df	Asymptotic Significance (2-sided)	
Pearson Chi-Square	1.342 ^a	1	.247	
Continuity Correction ^b	1.126	1	.289	
Likelihood Ratio	1.345	1	.246	
Fisher's Exact Test				
Linear-by-Linear Association	1.340	1	.247	
N of Valid Cases	516			
a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 70.94.				
b. Computed only for a 2x2 table				

يتبين من الجدول السابق، أن قيمة مستوى الدلالة هي 0.247 وهذه القيمة أكبر من القيمة المحددة في الفرضية وهي (0.05)، ولذلك فإننا نقبل صحة الفرضية ونقول بأنه "لا يوجد علاقة بين متغير (التعرض لجريمة الكترونية ومتغير الجنس)"، أي أن المتغيرين مستقلان. ومن الجدول السابق نلاحظ أن فئة الإناث أكثر تعرضاً للجريمة من الذكور حيث بلغت نسبة الإناث اللواتي تعرضن لجريمة الكترونية 31%، بينما بلغت هذه النسبة لدى الذكور 26%.

ب- لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متغير (التعرض لجريمة الكترونية) ومتغير مكان السكن.

الجدول (5): نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين متغير التعرض لجريمة الالكترونية ومتغير مكان السكن.

		مكان السكن			المجموع
		مدينة	قرية	مخيم	
هل تعرضت إلى جريمة الالكترونية	نعم	64	61	22	147
	لا	180	153	36	369
المجموع		244	214	58	516
نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين متغير التعرض لجريمة الالكترونية ومتغير مكان السكن					
	Value	df	Asymptotic Significance (2-sided)		
Pearson Chi-Square	3.150 ^a	2	.207		
Likelihood Ratio	3.021	2	.221		
Linear-by-Linear Association	2.518	1	.113		
N of Valid Cases	516				
a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 16.52.					

يبين الجدول رقم 5، أن قيمة مستوى الدلالة هي 0.207 وهذه القيمة أكبر من القيمة المحددة في الفرضية وهي (0.05)، ولذلك فإننا نقبل صحة الفرضية ونقول بأنه "لا يوجد علاقة بين متغير التعرض لجريمة الالكترونية ومتغير مكان السكن"، أي أن المتغيرين مستقلان. ومن الجدول السابق نلاحظ أن سكان المخيم أكثر تعرضاً للجريمة الالكترونية بنسبة بلغت 38% بينما بلغت هذه النسبة لدى سكان المدن والقرى — 26%، 29% على التوالي.

ت- لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متغير (التعرض لجريمة الالكترونية) ومتغير العمر.

الجدول (6): نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين متغير التعرض لجريمة الكترونية ومتغير العمر

		العمر					المجموع
		من 18 أقل	18 - 29	30 - 49	50 - 64	65 فأكثر	
هل تعرضت إلى جريمة الكترونية	نعم	2	94	44	7	0	147
	لا	8	242	103	14	2	369
المجموع		10	336	147	21	2	516
نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين متغير التعرض لجريمة الكترونية ومتغير العمر							
		Value	df	Asymptotic Significance (2-sided)			
Pearson Chi-Square		1.586 ^a	4	.811			
Likelihood Ratio		2.148	4	.709			
Linear-by-Linear Association		.276	1	.599			
N of Valid Cases		516					
a. 3 cells (30.0%) have expected count less than 5. The minimum expected count is .57.							

يبين الجدول رقم 6، أن قيمة مستوى الدلالة هي 0.811 وهذه القيمة أكبر من القيمة المحددة في الفرضية وهي (0.05)، ولذلك فإننا نقبل صحة الفرضية ونقول بأنه "لا يوجد علاقة بين متغير التعرض لجريمة الكترونية ومتغير العمر"، أي أن المتغيرين مستقلان. ومن الجدول السابق نلاحظ أن أفراد العينة الذين تراوحت أعمارهم من 50 لغاية 64 سنة أكثر تعرضاً للجريمة الكترونية بنسبة بلغت 33%، في حين وجد أن 30% ممن تراوحت أعمارهم من 30 لغاية 49 عام قد تعرضوا لجريمة الكترونية. بينما لوحظ أن 28% ممن تراوحت أعمارهم من 18 لغاية 29 عام تعرضوا للجريمة الكترونية. وبلغت نسبة التعرض للجريمة الكترونية لدى الفئة العمرية أقل من 18 عام بـ 20%.

ث- لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متغير (التعرض لجريمة الكترونية) ومتغير المستوى العلمي.

الجدول (7): نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين متغير التعرض لجريمة الكترونية ومتغير المستوى العلمي.

		المستوى العلمي					المجموع
		أقل من ثانوي	ثانوي	معهد	بكالوريوس س	الدراسات العليا	
هل تعرضت إلى جريمة الكترونية	نعم	1	9	4	103	30	147
	لا	7	23	19	238	82	369
المجموع		8	32	23	341	112	516
نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين متغير التعرض لجريمة الكترونية ومتغير المستوى العلمي							
		Value		df	(2-Asymptotic Significance sided)		
Pearson Chi-Square		3.049 ^a		4	.550		
Likelihood Ratio		3.362		4	.499		
Linear-by-Linear Association		.325		1	.569		
N of Valid Cases		516					
a. 1 cells (10.0%) have expected count less than 5. The minimum expected count is 2.28.							

يتبين من الجدول السابق، أن قيمة مستوى الدلالة هي 0.550 وهذه القيمة أكبر من القيمة المحددة في الفرضية وهي (0.05)، ولذلك فإننا نقبل صحة الفرضية ونقول بأنه "لا يوجد علاقة بين متغير (التعرض لجريمة الكترونية ومتغير المستوى العلمي)"، أي أن المتغيرين مستقلان. ومن الجدول السابق نلاحظ أن حملة شهادات البكالوريوس أكثر تعرضاً للجريمة بنسبة 30% من أفراد العينة، وفي حين وجدت هذه النسبة لدى حملة شهادة الثانوي فما دون 41% (انظر الجدول 7).

❖ نتائج الفرضية الثانية

من أجل دراسة صحة الفرضية القائلة بأنه "لا يوجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متغير (المعرفة عن القرار بقانون بشأن الجرائم الإلكترونية) ومتغيرات الديموغرافية (الجنس، مكان السكن، العمر، المستوى العلمي)"، أي أن متغيرات مستقلة، فقد تم استخدام اختبار كاي تربيع - Chi-Square للمتغيرات المستقلة وذلك لأن المتغيرات اسمية وكانت النتائج كما هو مبين في الجداول (8، 9، 10، 11).

أ- لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متغير المعرفة عن القرار بقانون بشأن الجرائم الإلكترونية ومتغير الجنس.

الجدول (8): نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين بين متغير المعرفة عن القرار بقانون بشأن الجرائم الإلكترونية ومتغير الجنس.

		الجنس		المجموع
		ذكر	أنثى	
هل لديك معرفة عن القرار بقانون بشأن الجرائم الإلكترونية؟	نعم	169	162	331
	لا	80	105	185
المجموع		249	267	516
نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين متغير المعرفة عن القرار بقانون بشأن الجرائم الإلكترونية ومتغير الجنس				
	Value	df	(2-Asymptotic Significance sided)	
Pearson Chi-Square	2.902 ^a	1	.088	
Continuity Correction ^b	2.598	1	.107	
Likelihood Ratio	2.909	1	.088	
Fisher's Exact Test				
Linear-by-Linear Association	2.896	1	.089	
N of Valid Cases	516			
a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 89.27.				
b. Computed only for a 2x2 table				

يبين من الجدول رقم 8، أن قيمة مستوى الدلالة هي 0.088 وهذه القيمة أكبر من القيمة المحددة في الفرضية وهي (0.05)، ولذلك فإننا نقبل صحة الفرضية ونقول بأنه "لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متغير المعرفة عن القرار بقانون بشأن الجرائم الإلكترونية ومتغير الجنس"، أي أن المتغيرين مستقلان. ومن الجدول السابق نلاحظ أن 68% من الذكور لديه معرفة عن القرار بقانون بشأن الجرائم الإلكترونية، بينما لوحظ أن 60% من الإناث لديهم معرفة عن القرار بقانون بشأن الجرائم الإلكترونية.

ب- لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متغير المعرفة عن القرار بقانون بشأن الجرائم الإلكترونية ومتغير مكان السكن.

الجدول (9): نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين بين متغير المعرفة عن القرار بقانون بشأن الجرائم الإلكترونية ومتغير مكان السكن.

		مكان السكن			المجموع
		مدينة	قرية	مخيم	
هل لديك معرفة عن القرار بقانون بشأن الجرائم الإلكترونية؟	نعم	151	149	31	331
	لا	93	65	27	185
المجموع		244	214	58	516
نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين متغير المعرفة عن القرار بقانون بشأن الجرائم الإلكترونية ومتغير مكان السكن:					
	Value	df	(2-Asymptotic Significance sided)		
Pearson Chi-Square	6.223 ^a	2	.045		
Likelihood Ratio	6.192	2	.045		
Linear-by-Linear Association	.009	1	.926		
N of Valid Cases	516				
a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 20.79.					

يتبين من الجدول السابق، أن قيمة مستوى الدلالة هي 0.450 وهذه القيمة أقل من القيمة المحددة في الفرضية وهي (0.05)، ولذلك فإننا نرفض صحة الفرضية ونقول بأنه "توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متغير المعرفة عن القرار بقانون بشأن

الجرائم الإلكترونية ومتغير مكان السكن"، أي أن المتغيرين غير مستقلان. حيث لوحظ أن هناك تأثير لمكان السكن على المعرفة عن القرار بقانون بشأن الجرائم الإلكترونية. وجد أن سكان القرى أكثر معرفة من غيرهم من سكان المدن والمخيمات. وبينت نتائج أن 70% من سكان القرى لديهم معرفة عن القرار بقانون بشأن الجرائم الإلكترونية.

ت- لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متغير المعرفة عن القرار بقانون بشأن الجرائم الإلكترونية ومتغير العمر.

الجدول (10): نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين متغير المعرفة عن القرار بقانون بشأن الجرائم الإلكترونية ومتغير العمر.

		العمر					المجموع
		من أقل 18	18 - 29	30 - 49	50 - 64	65 فأكثر	
هل لديك معرفة عن القرار بقانون بشأن الجرائم الإلكترونية؟	نعم	4	229	84	13	1	331
	لا	6	107	63	8	1	185
المجموع		10	336	147	21	2	516
نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين متغير المعرفة عن القرار بقانون بشأن الجرائم الإلكترونية ومتغير العمر							
		Value	df	(2-Asymptotic Significance sided)			
Pearson Chi-Square		8.237 ^a	4	.083			
Likelihood Ratio		8.062	4	.089			
Linear-by-Linear Association		2.107	1	.147			
N of Valid Cases		516					
a. 3 cells (30.0%) have expected count less than 5. The minimum expected count is .72.							

يبين من الجدول رقم 10، أن قيمة مستوى الدلالة هي 0.083 وهذه القيمة أكبر من القيمة المحددة في الفرضية وهي (0.05)، ولذلك فإننا نقبل صحة الفرضية ونقول بأنه لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متغير المعرفة عن القرار بقانون بشأن الجرائم الإلكترونية ومتغير العمر"، أي أن المتغيرين مستقلان. ومن الجدول السابق نلاحظ أن

أفراد العينة الذين تراوحت أعمارهم من 18 لغاية 29 عام أكثر معرفة عن القرار بقانون بشأن الجرائم الإلكترونية من غيرهم من الفئات العمرية الأخرى، وجد أن 68% منهم لديهم المعرفة عن القرار بقانون بشأن الجرائم الإلكترونية. في حين أن هذه نسبة المعرفة انخفضت لدى الفئات العمرية الأخرى.

ث- لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متغير المعرفة عن القرار بقانون بشأن الجرائم الإلكترونية ومتغير المستوى العلمي.

الجدول (11): نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين بين متغير المعرفة عن القرار بقانون بشأن الجرائم الإلكترونية ومتغير المستوى العلمي.

		المستوى العلمي					المجموع
		أقل من ثانوي	ثانوي	معهد	بكالوريوس س	الدراسات العليا	
هل لديك معرفة عن القرار بقانون بشأن الجرائم الإلكترونية؟	نعم	3	16	14	223	75	331
	لا	5	16	9	118	37	185
المجموع		8	32	23	341	112	516
نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين متغير المعرفة عن القرار بقانون بشأن الجرائم الإلكترونية ومتغير المستوى العلمي							
		Value	df	(2-Asymptotic Significance sided)			
Pearson Chi-Square		5.980 ^a	4	.201			
Likelihood Ratio		5.736	4	.220			
Linear-by-Linear Association		4.855	1	.028			
N of Valid Cases		516					
a. 1 cells (10.0%) have expected count less than 5. The minimum expected count is 2.87.							

يتبين من الجدول السابق، أن قيمة مستوى الدلالة هي 0.201 وهذه القيمة أكبر من القيمة المحددة في الفرضية وهي (0.05)، ولذلك فإننا نقبل صحة الفرضية ونقول بأنه "لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متغير المعرفة عن القرار بقانون بشأن الجرائم الإلكترونية ومتغير المستوى العلمي"، أي أن المتغيرين مستقلان. ويبين الجدول أن فئة

الدراسات العليا أكثر معرفة عن القرار بقانون بشأن الجرائم الإلكترونية بنسبة بلغت 67%، في حين بلغت وجد أن 65%، 61% من حملة شهادات بكالوريوس والدبلوم (المعهد) لديهم معرفة عن القرار بقانون بشأن الجرائم الإلكترونية، بينما قلت هذه النسبة لدى حملة شهادة الثانوية وما دون ذلك.

❖ نتائج الفرضية الثالثة

من أجل دراسة صحة الفرضية القائلة بأنه "لا يوجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متغير (الاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية) ومتغيرات الديموغرافية (الجنس، مكان السكن، العمر، المستوى العلمي)"، أي أن متغيرات مستقلة، فقد تم استخدام اختبار كاي تربيع - Chi-Square للمتغيرات المستقلة وذلك لأن المتغيرات اسمية وكانت النتائج كما هو مبين في الجداول (12، 13، 14، 15) التالية:

أ- لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين الاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية ومتغير الجنس.

الجدول (12): نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين الاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية ومتغير الجنس.

		الجنس		المجموع
		ذكر	أنثى	
بعد صدور القرار بقانون بشأن الجرائم الإلكترونية في حال تعرضك لجريمة الكترونية هل لديك استعداد لتقديم شكوى لدى الجهات المختصة؟	نعم	198	221	419
	لا	51	46	97
المجموع		249	267	516
نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين الاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية ومتغير الجنس				
	Value	df	(2-Asymptotic Significance sided)	
Pearson Chi-Square	.893 ^a	1	.345	
Continuity Correction ^b	.693	1	.405	
Likelihood Ratio	.893	1	.345	
Fisher's Exact Test				
Linear-by-Linear Association	.892	1	.345	
N of Valid Cases	516			
a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 46.81.				
b. Computed only for a 2x2 table				

يبين من الجدول رقم 12، أن قيمة مستوى الدلالة هي 0.345 وهذه القيمة أكبر من القيمة المحددة في الفرضية وهي (0.05)، ولذلك فإننا نقبل صحة الفرضية ونقول بأنه "لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين الاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية ومتغير الجنس"، أي أن المتغيرين مستقلان. ومن الجدول السابق نلاحظ أن 83% من الإناث لديهم لاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية. بينما انخفضت هذه النسبة لدى الذكور لتصل إلى 80%.

ب- لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين الاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية ومتغير مكان السكن.

الجدول (13): نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين الاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية ومتغير مكان السكن.

		مكان السكن			المجموع
		مدينة	قرية	مخيم	
بعد صدور القرار بقانون بشأن الجرائم الإلكترونية في حال تعرضك لجريمة إلكترونية هل لديك استعداد لتقديم شكوى لدى الجهات المختصة؟	نعم	199	178	42	419
	لا	45	36	16	97
المجموع		244	214	58	516
نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين الاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية ومتغير مكان السكن					
	Value	df	(2-Asymptotic Significance sided)		
Pearson Chi-Square	3.502 ^a	2	.174		
Likelihood Ratio	3.236	2	.198		
Linear-by-Linear Association	.990	1	.320		
N of Valid Cases	516				
a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 10.90.					

يتبين من الجدول السابق، وأن قيمة مستوى الدلالة هي 0.174 وهذه القيمة أكبر من القيمة المحددة في الفرضية وهي (0.05)، ولذلك فإننا نقبل صحة الفرضية ونقول بأنه "لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين الاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية ومتغير مكان السكن"، أي أن المتغيرين مستقلان. ويبين الجدول أن سكان القرى لديهم الاستعداد لتقديم شكوى لدى الجهات

المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية أكثر من غيرهم من سكان المدن والمخيمات. وجد أن 83% من سكان القرى لديهم الاستعداد لتقديم شكوى، بينما بلغت هذه النسبة لدى سكان المدن والمخيمات — 82%، 72% على التوالي.

ت- لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين الاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية ومتغير العمر.

الجدول (14): نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين الاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية ومتغير العمر.

		العمر					المجموع
		أقل من 18	18 – 29	30 – 49	50 – 64	65 فأكثر	
بعد صدور القرار بقانون بشأن الجرائم الإلكترونية في حال تعرضك لجريمة إلكترونية هل لديك استعداد لتقديم شكوى لدى الجهات المختصة؟	نعم	9	278	114	17	1	419
	لا	1	58	33	4	1	97
المجموع		10	336	147	21	2	516
نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين الاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية ومتغير العمر							
		Value	df	(2-Asymptotic Significance sided)			
Pearson Chi-Square		3.587 ^a	4	.465			
Likelihood Ratio		3.333	4	.504			
Linear-by-Linear Association		2.295	1	.130			
N of Valid Cases		516					
a. 4 cells (40.0%) have expected count less than 5. The minimum expected count is .38.							

يتبين من الجدول السابق، أن قيمة مستوى الدلالة هي 0.465 وهذه القيمة أكبر من القيمة المحددة في الفرضية وهي (0.05)، ولذلك فإننا نقبل صحة الفرضية ونقول بأنه "لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين الاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية ومتغير العمر"، أي أن المتغيرين مستقلان. ويبين الجدول أن أفراد العينة الذين تراوحت أعمارهم ما دون 18 عام لديهم الاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية أكثر من غيرهم من الفئات العمرية الأخرى. وجد أن 90% من هذه الفئة العمرية لديهم الاستعداد لتقديم شكوى، بينما انخفضت هذه النسبة وخاصة لدى الذين تراوحت أعمارهم ما فوق 65 عام حيث بلغت 50% فقط لديهم الاستعداد لتقديم شكوى.

ث- لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين الاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية ومتغير المستوى العلمي.

الجدول (15): نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين الاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية ومتغير المستوى العلمي.

		المستوى العلمي					المجموع
		أقل من ثانوي	ثانوي	معهد	بكالوريوس	الدراسات العليا	
بعد صدور القرار بقانون بشأن الجرائم الإلكترونية في حال تعرضك لجريمة الكترونية هل لديك استعداد لتقديم شكوى لدى الجهات المختصة؟	نعم	7	25	17	278	92	419
	لا	1	7	6	63	20	97
المجموع		8	32	23	341	112	516
نتائج اختبار (كاي تربيع - Chi-Square) لفحص العلاقة بين الاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية ومتغير المستوى العلمي							
		Value	df	(2-Asymptotic Significance sided)			
Pearson Chi-Square		1.295 ^a	4	.862			
Likelihood Ratio		1.244	4	.871			
Linear-by-Linear Association		.198	1	.656			
N of Valid Cases		516					
a. 2 cells (20.0%) have expected count less than 5. The minimum expected count is 1.50.							

يبين من الجدول رقم 15، وأن قيمة مستوى الدلالة هي 0.862 وهذه القيمة أكبر من القيمة المحددة في الفرضية وهي (0.05)، ولذلك فإننا نقبل صحة الفرضية ونقول بأنه "لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين الاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية ومتغير المستوى العلمي"، أي أن المتغيرين مستقلان. ومن الجدول السابق نلاحظ أن 88% من حملة شهادة الثانوي فما دون

لديهم الاستعداد لتقديم شكوى لدى الجهات المختصة بعد صدور القرار بقانون بشأن الجرائم الإلكترونية. بينما انخفضت هذه النسبة لدى أفراد العينة حسب المستوى العلمي، حيث وجد أن 74% من حملة شهادة الدبلوم (المعهد) لديهم الاستعداد لتقديم شكوى. وكما أن 82% من حملة شهادة البكالوريوس لديهم الاستعداد لتقديم شكوى.

النتائج

1. عجز النصوص الجزائية التقليدية في مواجهة الجرائم المعلوماتية.
2. تواجه الأدبيات المتعلقة بالجرائم المعلوماتية العديد من الصعوبات الموضوعية والإجرائية في تحديد مفهوم الجرائم المعلوماتية واكتشافها وإثباتها.
3. يوجد نقص في الكوادر البشرية المؤهلة فنياً وتقنياً وضعف البنية التحتية في مجال الجرائم المعلوماتية لدى جهاز الشرطة والنيابة العامة والقضاء.
4. لا يوجد سيادة فلسطينية كاملة على الفضاء الإلكتروني في فلسطين بسبب سيطرة الاحتلال الإسرائيلي عليه.
5. يوجد صعوبات في التعاون القضائي الدولي في الجرائم المعلوماتية وإشكالية القانون الواجب التطبيق والمحكمة المختصة بنظر هذه الجرائم باعتبارها دولية عابرة للحدود.
6. الجرائم الإلكترونية ظاهرة حديثة الانتشار في فلسطين وهي في تزايد مستمر.
7. أكثر الجرائم الإلكترونية انتشاراً في فلسطين هي التهديد، الإهانة، والابتزاز، والتهويل، والذم والقدح.
8. يوجد ضعف في عملية نشر التوعية والثقافة القانونية حول مخاطر الجريمة الإلكترونية.
9. غياب الاستراتيجية الوطنية الشاملة للوقاية والحد من الجرائم الإلكترونية.

التوصيات

1. يفضل من أصحاب الاختصاص الاتفاق على مفهوم للجريمة المعلوماتية.
2. تعزيز التنسيق والتعاون بين المؤسسات القانونية الإقليمية والدولية من أجل ملاحقة مرتكبي الجرائم المعلوماتية وتقديمهم للعدالة.
3. ضرورة زيادة الكوادر البشرية المختصين فنياً وتقنياً ومتطلبات البنية التحتية التكنولوجية الحديثة في مجال الجرائم المعلوماتية لدى جهاز الشرطة والنيابة العامة الفلسطينية والجهاز القضائي.
4. العمل على إصدار اللائحة التفسيرية للقرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية.
5. ضرورة إصدار أدلة إجرائية للمؤسسات الأمنية والقضائية للتعامل مع الجرائم المعلوماتية.
6. ضرورة بسط السيادة الفلسطينية على فضاءها الإلكتروني.
7. نشر الثقافة والمعرفة ورفع درجة الوعي القانونية بمخاطر الجرائم المعلوماتية.
8. رفع مستوى التأهيل والتدريب لأفراد الشرطة والنيابة العامة والقضاة للتعامل مع طبيعة الجرائم الإلكترونية.
9. استخدام الأنظمة المعلوماتية الآمنة والمحمية للمحافظة على سلامة وسرية البيانات والمعلومات.
10. ضرورة إشراك المختصين ومؤسسات المجتمع المدني في مناقشة القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية قبل تعديله.
11. إعداد وتنفيذ خطة استراتيجية وطنية شاملة للوقاية والحد من الجرائم المعلوماتية في فلسطين.

قائمة المصادر والمراجع

المصادر

- قرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، الصادر في مدينة رام الله عن رئيس دولة فلسطين بتاريخ 2017/6/24، منشور في الجريدة الرسمية الفلسطينية، ممتاز عدد 14، بتاريخ 2017/7/9.
- قرار بقانون رقم 15 لسنة 2017 بشأن المعاملات الإلكترونية، الصادر في مدينة رام الله عن رئيس دولة فلسطين بتاريخ 2017/6/15، منشور في الجريدة الرسمية الفلسطينية، ممتاز عدد 14، بتاريخ 2017/7/9.
- القرار بقانون رقم (15) لسنة 2009 بشأن الهيئة الفلسطينية لتنظيم قطاع الاتصالات، صدر في مدينة رام الله بتاريخ 2009/6/4، عن الرئيس محمود عباس، نشر في الجريدة الرسمية الفلسطينية في العدد 82، بتاريخ 2009/8/22.
- قانون رقم 3 لسنة 1996 بشأن الاتصالات السلكية واللاسلكية، صدر في مدينة غزة، بتاريخ 1996/1/18، عن الرئيس ياسر عرفات، منشور في جريدة الوقائع الفلسطينية في العدد 12، بتاريخ 1996/4/23.
- قانون العقوبات الأردني رقم 16 لسنة 1960.
- المرسوم الرئاسي رقم 9 لسنة 2011 الصادر عن رئيس دولة فلسطين بتاريخ 2011/6/27 بمدينة رام الله بشأن المصادقة على تعديل الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (منشور على المقتفي).
- قانون التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات رقم 19 لسنة 2012، المنشور على صفحة رقم 2580 من عدد الجريدة الرسمية رقم 5162 بتاريخ 2012/6/17.

- مشروع قرار بقانون الجرائم الإلكترونية رقم (بلا) لسنة 2016، الصادر عن النيابة العامة في مدينة رام الله بتاريخ 2016/3/16 (غير منشور).

المراجع

- الصغير، جميل عبد الباقي، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، ط1، دار النهضة العربية، القاهرة، 1992.
- عباينة، محمود أحمد: جرائم الحاسوب وأبعادها الدولية، الطبعة الثانية، عمان، دار الثقافة، 2009.
- المومني، نهلا عبد القادر: الجرائم المعلوماتية، الطبعة الثانية، عمان، دار الثقافة، 2010.
- فكرى، أيمن عبد الله: جرائم نظم المعلومات - دراسة مقارنة، دار الجامعة الجديدة للنشر، الإسكندرية، 2007.
- فوريستر، توم: مجتمع التقنية العالي، قصة ثورة تقنية المعلومات، ترجمة محمد كامل عبد العزيز، نشر مركز الكتاب الأردني، عمان، الطبعة الأولى، 1989.
- عرب، يونس: دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والإنترنت، الجزء الأول، اتحاد المصارف العربية، ط1، بيروت، 2002.
- قشقوش، هدى: جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، بدون طبعة، ط1، القاهرة، 1992.
- رستم، هشام: الجرائم المعلوماتية أصول التحقيق الجنائي التقني، مجلة الأمن والقانون، دبي، كلية الشرطة، عدد4، 1999.
- الشوا، سامي محمد: ثورة المعلومات وانعكاساتها على قانون العقوبات، ط2، بدون طبعة، دار النهضة العربية، القاهرة، 1994.

- قوره، نائلة: جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي، دار النهضة العربية، ط1، القاهرة، 2004.
- المناعسة، أسامة والزعبي، جلال: جرائم تقنية نظم المعلومات الإلكترونية - دراسة مقارنة، دار الثقافة للنشر والتوزيع، الطبعة الثانية، عمان، 2015.
- إبراهيم، خالد ممدوح: الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط1، 2009.
- رمضان، مدحت عبد الحلیم: الحماية الجنائية للتجارة الإلكترونية - دراسة مقارنة، دار النهضة العربية، القاهرة، 1994.
- الهيتي، محمد حماد: التكنولوجيا الحديثة والقانون الجنائي، بدون طبعة، دار الثقافة للنشر والتوزيع، ط1، عمان، 2004.
- منصور، محمد حسين: المسؤولية الإلكترونية، دار النهضة العربية، ط2، القاهرة، 2004.
- حجازي، عبد الفتاح بيومي: الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، ط1، القاهرة، 2002.
- صالح، نائل عبد الرحمن: الجرائم الاقتصادية في التشريع الأردني، دار الفكر للنشر والتوزيع، الطبعة الأولى، الجزء الأول، عمان، 1990.
- السراج، عبود: قانون العقوبات الاقتصادي، منشورات جامعة دمشق، الطبعة السابعة، 1998.
- الجبور، محمد: الوسيط في قانون العقوبات - القسم العام، دار وائل، عمان، 2010.
- حسني، محمود نجيب: النظرية العامة للقصد الجنائي، دار النهضة العربية، ط2، القاهرة، 1971.

- موسى، مصطفى محمد: دليل البحث والتحري عبر شبكة الإنترنت، دار الكتب القانونية، مصر، 2010.
- سرور، أحمد فتحي: الوسيط في قانون العقوبات - القسم العام، الطبعة الخامسة، دار النهضة العربية، القاهرة، 1991.
- حسني، محمود نجيب: شرح قانون العقوبات - القسم العام، الطبعة السادسة، دار النهضة العربية، القاهرة، 1989.
- السعيد، كامل: شرح الأحكام العامة في قانون العقوبات والقانون المقارن، دار الفكر للنشر والتوزيع، ط2، عمان، 1983.
- جميعي، حسن: إثبات التصرفات القانونية التي يتم إبرامها عبر الإنترنت، دار النهضة العربية، القاهرة، بدون سنة طبعة.
- الردايدة، عبد الكريم: الجرائم المستحدثة واستراتيجية مواجهتها، دار ومكتبة الحامد للنشر والتوزيع، الطبعة الأولى، الأردن، 2013.
- الشناوي، محمد: استراتيجية مكافحة جرائم النصب المستحدثة، دار البيان، الطبعة الأولى، القاهرة، 2006.
- الدباس، عبد الفتاح: دور العقيدة الإسلامية في الحد من الجرائم، أكاديمية الشرطة الملكية، الأردن، 2002.
- حوري، عمر محي الدين: الجريمة أسبابها ومكافحتها "دراسة مقارنة" في الشريعة والقانون والعلوم الاجتماعية، دار الفكر، دمشق، الطبعة الأولى، 2003.

رسائل دكتوراه وماجستير

- مرسى، محمد محمود السيد: تفعيل دور الشرطة في تحقيق الاستقرار الأمني، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة، 2004.
- العجمي، عبد الله دغش: المشكلات العلمية والقانونية للجرائم الإلكترونية - دراسة مقارنة، رسالة ماجستير، جامعة الشرق الأوسط، الأردن، 2014.
- الردايده، عبد الكريم: دور أجهزة العدالة الجنائية في حماية حقوق ضحايا الجريمة، رسالة ماجستير، جامعة عمان العربية للدراسات العليا، الأردن، عمان، 2006.

أوراق عمل والأبحاث

- المذكرة القانونية حول القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، الصادرة عن الهيئة المستقلة لحقوق الإنسان "ديوان المظالم"، بتاريخ 2017/8/7، رام الله.
- ملاحظات مؤسسة الحق على القرار بقانون بشأن الجرائم الإلكترونية رقم (16) لسنة 2017، بتاريخ 2017/10/2، رام الله.
- مقال بعنوان " الأمم المتحدة تطالب الحكومة الفلسطينية بالرد خلال شهرين حول قانون الجرائم الإلكترونية"، نشر على صحيفة العربي الجديد بتاريخ 2017/08/29، www.alaraby.co.uk.
- الشلالدة، محمد فهاد ربيعي، عبد الفتاح أمين، الجرائم الإلكترونية في دولة فلسطين المحتلة في ضوء التشريعات الوطنية والدولية، بحث مقدم إلى المؤتمر العلمي الحادي عشر لكلية القانون في جامعة جرش حول الجرائم المعلوماتية من 5-2015/5/7، نيسان 2015.
- مطر، كامل: الجريمة الإلكترونية، ورقة عمل مقدمة إلى المؤتمر الأول لمكافحة الجرائم الإلكترونية في فلسطين، جامعة النجاح الوطنية، نيسان، 2016.

- الدبري، عبد العال: الجريمة الإلكترونية بين التشريع والقضاء في الدول الغربية، 2013.

- المطردي، مفتاح بوبكر، الجريمة الإلكترونية والتغلب على تحدياتها، ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان المنعقد في 23-25 / 2012 / 9.

- عاشي، سميرة: ماهية الجرائم المعلوماتية، بحث منشور في مجلة المنتدى القانوني، العدد السابع، جامعة محمد خضير بسكرة، الجزائر، 2011.

- الشوا، محمد سامي: جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم في المؤتمر الدولي السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25-28 أكتوبر، 1993.

- رستم، هشام محمد: ورقة عمل بعنوان "جرائم الحاسب كصورة من صور الجرائم المستحدثة"، مجلة الدراسات القانونية، تصدرها كلية الحقوق بجامعة أسيوط، العدد السابع عشر، القاهرة، 1995.

- القطاونة، مصعب: الإجراءات الجنائية الخاصة في الجرائم المعلوماتية، بحث مقدم لشبكة قانوني الأردن، 2010.

- الجرائم الإلكترونية بين الواقع والتشريع، إعداد هنادي كرسوع، إعلام الشرطة الفلسطينية، www.police.ps.

- جرائم الحاسب الآلي، ورقة عمل مقدمة من الأمانة العامة لمجلس التعاون الخليجي لاجتماع اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم الإلكترونية "الإنترنت" الأول والذي انعقد بمقر الأمانة العامة بالرياض خلال الفترة من 4 - 5/4/2004.

- حمدان، هاني، دور العلاقات العامة لدى الأجهزة الأمنية في التوعية الأمنية، مجلة الدراسات الأمنية، أكاديمية الشرطة الملكية، عمان، الأردن، العدد 1، 2004.
- الجمال، محمد علي، دور الشرطة الوقائي في انحسار جرائم العنف، مجلة الأمن العام المصرية، عدد 136.
- البياتي، هلال عبود: الوسائل الفنية لحماية البرامج ودور التشريعات في حماية المعلومات، بحث منشور في مجلة أبحاث الحاسوب، المجلد الأول، العدد الأول، تصدر عن الأمانة العامة لاتحاد مجالس البحث العلمي العربي، 1996.
- الرواشدة، سامي والهيجنة، أحمد: مكافحة الجريمة المعلوماتية بالتجريم والعقاب، بحث منشور في المجلة الأردنية في القانون والعلوم السياسية، جامعة مؤتة، المجلد (1)، العدد (3)، الأردن، 2009.

المقابلات

- مقابلة الباحث مع السيدة نسرین رشمای رشماوي رئيسة نيابة الجرائم الإلكترونية في النيابة العامة الفلسطينية بمدينة رام الله بتاريخ 2017/8/10.
- مقابلة الباحث مع السيد سامر الهندي مدير وحدة الجرائم الإلكترونية في جهاز الشرطة الفلسطيني بمدينة رام الله بتاريخ 2017/8/14.
- مقابلة الباحث مع سعادة القاضي أيمن ظاهر قاضي محكمة صلح رام الله بمدينة رام الله بتاريخ 2017/9/12.
- مقابلة د. أحمد براك النائب العام لدولة فلسطين مع صحيفة دنيا الوطن، رام الله، بتاريخ 2017/1/3، www.pgp.ps
- مقابلة أحمد براك النائب العام لدولة فلسطين على تلفزيون فلسطين ضمن برنامج ملف اليوم بعنوان "قانون الجرائم الإلكترونية بين الأهمية والتطبيق"، رام الله، بتاريخ 2017/7/12.

- مقابلة د. حسن الطراونة، أستاذ القانوني الجنائي في كلية الحقوق في الجامعة الأردنية ضمن برنامج ملف اليوم بعنوان "قانون الجرائم الإلكترونية بين الأهمية والتطبيق" على تلفزيون فلسطين، رام الله، بتاريخ 2017/7/12.

المواقع الإلكترونية

- مجلس القضاء الأعلى الفلسطيني www.courts.gov.ps .
- النيابة العامة الفلسطينية www.pgp.ps/ar/Pages/default.aspx .
- جهاز الشرطة الفلسطيني www.palpolice.ps .
- مجلس الوزراء الفلسطيني www.palestinecabinet.gov.ps .
- المركز الفلسطيني لاستقلال المحاماة والقضاء "مساواة" www.musawa.ps .
- الهيئة المستقلة لحقوق الإنسان "ديوان المظالم" www.ichr.ps .
- المركز العربي لأبحاث الفضاء الإلكتروني www.accronline.com .

الملاحق

ملحق رقم (1): أسئلة الاستبيان وتحليلها

هل تعرضت إلى جريمة إلكترونية	الإجابة	عدد الإجابة	النسبة المئوية
	نعم	147	28.5
	لا	369	71.5
	المجموع	516	100
في حال الإجابة بنعم عدد المرات التي تعرضت لجريمة إلكترونية	عدد المرات	عدد الإجابة	النسبة المئوية
	مرة واحدة	97	66
	مرتين	27	18.4
	3 فأكثر	23	15.6
	المجموع	147	100
	نوع الجريمة	عدد الإجابة	النسبة المئوية
نوع الجريمة الإلكترونية التي تعرضت لها	التهديد والإهانة	74	32
	الابتزاز والتهويل	55	23.8
	الاختيال	22	9.5
	إثارة النعرات	10	4.3
	الذم والقدح	41	17.8
	إفساد الرابطة الزوجية	6	2.6
	إفشاء الأسرار	23	10
	المجموع	231	100

هل تقدمت بشكوى إلى الجهات المختصة		
الإجابة	عدد الإجابة	النسبة المئوية
نعم	62	42.2
لا	85	57.8
المجموع	147	100
ما هي الجهة التي تقدمت إليها بشكوى		
الإجابة	عدد الإجابة	النسبة المئوية
الشرطة	46	74.2
النيابة العامة	16	25.8
المؤسسة التي أعمل بها	0	0
المجموع	62	100
مدى رضاك عن نتائج الشكوى التي تقدمت بها		
الإجابة	عدد الإجابة	النسبة المئوية
راضي	24	38.7
غير راضي	18	29
راضي جداً	13	21
غير راضي جداً	7	11.3
المجموع	62	100
راضي وراضي جداً	37	59.7
غير راضي وغير راضي جداً	25	40.3
المجموع	62	100
في حال عدم تقديم شكوى ما هي الأسباب التي حالت دون تقديم الشكوى لدى الجهات المختصة		
الإجابة	عدد الإجابة	النسبة المئوية
الخوف من الأهل	22	15.6
خوفاً من إساءة السمعة	28	19.8
عدم الثقة في المؤسسات المختصة	32	22.7

21.3	30	الفعل لا يستحق ملاحقة قانونية	
12.1	17	ضعف الوعي القانوني	
8.5	12	عدم مراعاة السرية	
100	141	المجموع	
النسبة المئوية	عدد الإجابة	الإجابة	هل لديك معرفة بالقرار بقانون بشأن الجرائم الإلكترونية
64.1	331	نعم	
35.9	185	لا	
100	516	المجموع	
النسبة المئوية	عدد الإجابة	الإجابة	ما رأيك بالقرار بقانون بشأن الجرائم الإلكترونية
36.9	122	جيد	
32.6	108	متحفظ عليه	
25.4	84	أنا ضد هذا القانون	
5.1	17	لا رأي	
100	331	المجموع	
النسبة المئوية	عدد الإجابة	الإجابة	
81.2	419	نعم	
18.8	97	لا	بعد صدور القرار بقانون بشأن الجرائم الإلكترونية في حال تعرضك لجريمة الإلكترونية هل لديك استعداد لتقديم شكوى لدى الجهات المختصة
100	516	المجموع	
النسبة المئوية	عدد الإجابة	الإجابة	
12.6	260	إعداد وتنفيذ استراتيجية وطنية للوقاية والحد من الجرائم الإلكترونية	
17.4	359	إصدار قوانين عصرية حديثة	برأيك ما هي أفضل أربعة إجراءات يجب اتخاذها للحد من الجرائم الإلكترونية في فلسطين

		وتطبيقها			
9.8	203	تنفيذ الأحكام القضائية			
15.8	327	استخدام برامج حماية لحماية امن المعلومات			
18.1	373	تعزيز التوعية ونشر الثقافة القانونية حول مخاطر الجرائم الإلكترونية			
14.4	297	رقابة الأسرة لأفرادها			
11.9	245	إبلاغ الجهات المختصة			
100	2064	المجموع			
هل تعرضت إلى جريمة الكترونية					
			مدينة	قرية	مخيم
ذكر	43.8%	47.5%	36.4%		
أنثى	56.3%	52.5%	63.6%		
مجموع	100.0%	100.0%	100.0%		
عدد المرات التي تعرضت فيها لجريمة الكترونية					
			مرة	مرتين	ثلاث مرات فأكثر
ذكر	45.4%	55.6%	26.1%		
أنثى	54.6%	44.4%	73.9%		
مجموع	100.0%	100.0%	100.0%		

تعرض للجريمة وفقا للفئة العمرية						
	اقل من 18	18-29	30-49	50-64	65+	
ذكر	50.0%	39.4%	47.7%	85.7%	0.0%	
أنثى	50.0%	60.6%	52.3%	14.3%	0.0%	
مجموع	100.0%	100.0%	100.0%	100.0%	0.0%	
تعرض للجريمة حسب المهنة						
	طالب	موظف قطاع عام	موظف قطاع خاص	موظف قطاع أهلي	عاطل عن العمل	يعمل لحسابه
ذكر	31.8%	55.0%	46.9%	25.0%	43.8%	73.7%
أنثى	68.2%	45.0%	53.1%	75.0%	56.3%	26.3%
مجموع	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
تعرض للجريمة حسب المؤهل العلمي						
	أقل من ثانوي	ثانوي	معهد	بكالوريوس	دراسات عليا	
ذكر	50%	66.7%	75.0%	35.9%	63.3%	
أنثى	50%	33.3%	25.0%	64.1%	36.7%	
مجموع	100.0%	100.0%	100.0%	100.0%	100.0%	
المعرفة بالقرار بقانون بشأن الجرائم الإلكترونية (بعد صدوره)						
الجنس	ذكر	أنثى				
	51.1%	48.9%				
مكان السكن						
مدينة	قرية	مخيم				
45.6%	45.0%	9.4%				

حسب الفئة العمرية						
65+		50-64		30-49	18-29	أقل من 18
0.3%		3.9%		25.4%	69.2%	1.2%
حسب المهنة						
يعمل لحسابه		عاطل عن العمل	موظف قطاع أهلي	موظف قطاع خاص	موظف قطاع عام	طالب
18.1%		43.8%	25.0%	46.9%	55.0%	31.8%
حسب المؤهل العلمي						
دراسات عليا		بكالوريوس	معهد	ثانوي	أقل من ثانوي	
22.7%		67.4%	4.2%	4.8%	0.9%	
بعد صدور القرار بقانون بشأن الجرائم الإلكترونية هل لديك استعداد لتقديم شكوى						
أنثى				ذكر	الجنس	
52.7%				47.3%		
مكان السكن						
مخيم				قرية	مدينة	
10.0%				42.5%	47.5%	
حسب الفئة العمرية						
65+			50-64	30-49	18-29	أقل من 18
0.2%			4.1%	27.2%	66.3%	2.1%
حسب المهنة						
يعمل لحسابه		عاطل عن العمل	موظف قطاع أهلي	موظف قطاع	موظف قطاع عام	طالب

			خاص		
13.1%	11.5%	11.2%	20.3%	12.6%	31.3%
حسب المؤهل العلمي					
دراسات عليا		بكالوريوس	معهد	ثانوي	أقل من ثانوي
22.0%		66.3%	4.1%	6.0%	1.7%
إجراءات الحد من الجرائم الإلكترونية					
أنثى			ذكر	الجنس	
51.7%			48.3%		
مكان السكن					
مخيم			قرية	مدينة	
11.2%			41.5%	47.3%	
حسب الفئة العمرية					
65+		50-64	30-49	18-29	اقل من 18
0.4%		4.1%	28.5%	65.1%	1.9%
حسب المهنة					
يعمل لحسابه	عاطل عن العمل	موظف قطاع أهلي	موظف قطاع خاص	موظف قطاع عام	طالب
14.3%	11.6%	12.4%	18.8%	12.6%	30.2%

حسب المؤهل العلمي				
أقل من ثانوي	ثانوي	معهد	بكالوريوس	دراسات عليا
1.6%	6.2%	4.5%	66.1%	21.7%
أقل من 18				
الجنس	ذكر	أنثى		
	50%	05%		
مكان السكن				
مدينة	قرية	مخيم		
70.0%	20.0%	10.0%		
حسب المؤهل العلمي				
أقل من ثانوي	ثانوي	معهد	بكالوريوس	دراسات عليا
40.0%	40.0%	0.0%	20.0%	0.0%
المهنة				
طالب	موظف قطاع عام	موظف قطاع خاص	موظف قطاع أهلي	عاطل عن العمل
90.0%	10.0%	0.0%	0.0%	0.0%
من 19 – 29				
الجنس	ذكر	أنثى		
	44.9%	55.1%		
مكان السكن				
مدينة	قرية	مخيم		
47.6%	43.8%	8.6%		

حسب المؤهل العلمي					
أقل من ثانوي	ثانوي	معهد	بكالوريوس	دراسات عليا	
0.9%	4.2%	3.3%	75.9%	15.8%	
المهنة					
طالب	موظف قطاع عام	موظف قطاع خاص	موظف قطاع أهلي	عاطل عن العمل	يعمل لحسابه
43.8%	8.6%	13.1%	7.1%	11.9%	15.5%
من 30 – 49					
الجنس	ذكر	أنثى			
	55.1%	44.9%			
مكان السكن					
مدينة	قرية	مخيم			
44.2%	40.8%	15%			
حسب المؤهل العلمي					
أقل من ثانوي	ثانوي	معهد	بكالوريوس	دراسات عليا	
0.0%	8.8%	6.1%	51.0%	34.0%	
المهنة					
طالب	موظف قطاع عام	موظف قطاع خاص	موظف قطاع أهلي	عاطل عن العمل	يعمل لحسابه
0.0%	19.7%	34.0%	25.2%	8.8%	12.2%
من 50 – 64					

الجنس		ذكر	أنثى	
		47.6%	52.4%	
مكان السكن				
مدينة	قرية	مخيم		
52.4%	23.8%	%23.8		
حسب المؤهل العلمي				
أقل من ثانوي	ثانوي	معهد	بكالوريوس	دراسات عليا
0.0%	4.8%	14.3%	42.9%	38.1%
المهنة				
طالب	موظف قطاع عام	موظف قطاع خاص	موظف قطاع أهلي	عاطل عن العمل
0.0%	23.8%	14.3%	14.3%	33.3%
يعمل لحسابه				
14.3%				
65 فأكثر				
الجنس		ذكر	أنثى	
		100.0%	0.0%	
مكان السكن				
مدينة	قرية	مخيم		
50.0%	0.0%	50.0%		
حسب المؤهل العلمي				
أقل من ثانوي	ثانوي	معهد	بكالوريوس	دراسات عليا
50.0%	0.0%	0.0%	0.0%	50.0%

المهنة					
طالب	موظف قطاع عام	موظف قطاع خاص	موظف قطاع أهلي	عاطل عن العمل	يعمل لحسابه
0.0%	50.0%	0.0%	0.0%	0.0%	50.0%
تقديم الشكوى ومدى الرضا					
ذكور	راضي جدا	راضي	غير راضي	غير راضي جدا	
شرطة	19.0%	38.1%	19.0%	23.8%	
نيابة عامة	12.5%	50.0%	37.5%	0.0%	
إناث	راضي جدا	راضي	غير راضي	غير راضي جدا	
شرطة	20.0%	40.0%	28.0%	12.0%	
نيابة عامة	25.0%	25.0%	37.5%	12.5%	
نوع الجريمة التي تعرض لها					
الجنس	ذكر	أنثى			
	44.2%	55.8%			
مكان السكن					
مدينة	قرية	مخيم			
44.2%	41.5%	14.3%			
حسب المؤهل العلمي					
أقل من ثانوي	ثانوي	معهد	بكالوريوس		دراسات عليا
0.7%	6.1%	2.7%	70.1%		20.4%

المهنة						
طالب	موظف قطاع عام	موظف قطاع خاص	موظف قطاع أهلي	عاطل عن العمل	يعمل لحسابه	
29.9%	13.6%	21.8%	10.9%	10.9%	12.9%	
العمر						
أقل من 18	18 – 29	30 – 49	50 – 64	65 فأكثر		
0.7%	63.9%	29.9%	4.1%	1.4%		
نوع الجريمة						
التهديد والإهانة	الابتزاز والتهويل	الاحتيال	إثارة النعرات	الذم والقدح	إفساد الرابطة الزوجية	إفشاء الأسرار
50.3%	37.4%	15.0%	6.8%	27.9%	4.1%	15.6%
رأي أفراد العينة بالقرار بقانون بشأن الجرائم الإلكترونية						
الجنس	ذكر		أنثى			
	49.3%		50.7%			
مكان السكن						
مدينة	قرية	مخيم				
46%	44.9%	9.1%				
حسب المؤهل العلمي						
أقل من ثانوي	ثانوي	معهد	بكالوريوس	دراسات عليا		
1.1%	5.1%	4.3%	66.3%	23.2%		

المهنة					
طالب	موظف قطاع عام	موظف قطاع خاص	موظف قطاع أهلي	عاطل عن العمل	يعمل لحسابه
33.7%	13.4%	16.7%	11.2%	8.7%	16.3%
العمر					
أقل من 18	18 – 29	30 – 49	50 – 64	65 فأكثر	
1.4%	69.2%	25.0%	4.0%	0.4%	
	أقل من 18	18 – 29	30 – 49	50 – 64	
ضد هذا القانون	4%	52%	41%	4%	
جيد	0%	80%	18%	3%	
متحفظ عليه	2%	65%	26%	6%	
لا رأي	0%	80%	20%	0%	
عدد المرات التي تعرض فيها لجريمة الكترونية					
الجنس	ذكر	أنثى			
	44.6%	55.4%			
مكان السكن					
مدينة	قرية	مخيم			
53.6%	40.2%	6.3%			
عدد المرات	مدينة	قرية	مخيم		
مرة	70%	73.3%	71.4%		
مرتين	20%	13.3%	28.6%		

0.0%			13.3%	10%	ثلاث فأكثر	
100.0%			100.0%	100%		
المستوى العلمي						
دراسات عليا		بكالوريوس	معهد	ثانوي	أقل من ثانوي	
12.5%		82.1%	0.9%	0.9%	3.6%	
دراسات عليا	بكالوريوس	معهد	ثانوي	أقل من ثانوي	عدد المرات	
13.1%	82.1%	1.2%	1.2%	2.4%	مرة	
10.0%	75.0%	0.0%	5.0%	10.0%	مرتين	
10.0%	80.0%	0.0%	0.0%	10.0%	ثلاث فأكثر	
المهنة						
يعمل لحسابه		عاطل عن العمل	موظف قطاع أهلي	موظف قطاع خاص	موظف قطاع عام	طالب
10.7%		5.4%	3.6%	8.0%	2.7%	69.6%
يعمل لحسابه	عاطل عن العمل	موظف قطاع أهلي	موظف قطاع خاص	موظف قطاع عام	طالب	عدد المرات
6.3%	3.8%	3.8%	8.8%	0.0%	77.5%	مرة
5.0%	15.0%	5.0%	0.0%	10.0%	65.0%	مرتين
50.0%	0.0%	0.0%	16.7%	8.3%	25.0%	ثلاث

						فأكثر
العمر						
فأكثر 65		50 - 64		30 - 49	18 - 29	أقل من 18
0%		1%		6%	90%	3%
فأكثر 65	50 - 64		30 - 49	18 - 29	أقل من 18	عدد المرات
0.0%	1.3%		3.8%	93.8%	1.3%	مرة
0.0%	0.0%		15.0%	75.0%	10.0%	مرتين
0%	0%		8%	92%	0%	ثلاث فأكثر

ملحق (2) استبيان حول الجرائم الإلكترونية في فلسطين

استبيان حول الجرائم الإلكترونية في فلسطين									
أولاً: البيانات الشخصية									
V1. الجنس	1. ذكر	2. أنثى	V2. مكان السكن	1. مدينة	2. قرية	3. مخيم			
V3. العمر	1. أقل من 18	2. 18 – 29	3. 30 – 49	4. 50 – 64	5. 65 فأكثر				
V4. المهنة	1. طالب	2. موظف قطاع عام	3. موظف قطاع خاص	4. قطاع أهلي	5. عاطل عن العمل	6. يعمل لحسابه			
V5. المستوى العلمي	1. أقل من ثانوي	2. ثانوي	3. معهد	4. بكالوريوس	5. الدراسات العليا				
ثانياً: الأسئلة									
Q1	هل تعرضت إلى جريمة إلكترونية		1. نعم	2. لا	Q2	في حال الإجابة بنعم، ما هو عدد المرات التي تعرضت لجريمة إلكترونية؟		1. مرة	2. 3 فأكثر
Q3	ما هو نوع الجريمة الإلكترونية التي تعرضت إليها؟								
Q3.1	التهديد والإهانة		1. نعم	2. لا	Q3.2	الابتزاز والتهويل		1. نعم	2. لا
Q3.3	الاحتيال		1. نعم	2. لا	Q3.4	إثارة النعرات		1. نعم	2. لا
Q3.5	الذم والقدح		1. نعم	2. لا	Q3.6	إفساد الرابطة الزوجية		1. نعم	2. لا
Q3.7	إفشاء الأسرار		1. نعم	2. لا					
Q4	هل تقدمت بشكوى إلى الجهات المختصة؟		1. نعم	2. لا					
Q5	في حال الإجابة بنعم، ما هي الجهة التي تقدمت بشكوى إليها؟		1. الشرطة	2. النيابة	3. أخرى				
Q6	ما مدى رضاك عن نتائج الشكوى التي تقدمت بها؟		1. راضي جداً	2. راضي	3. غير راضي	4. غير راضي جداً			
Q7	في حال الإجابة بلا (عدم تقديم شكوى) ما هي الأسباب التي		1. الخوف من الأهل	1. نعم	2. لا	2. خوفاً من إساءة السمعة		1. نعم	2. لا

		3. عدم الثقة في المؤسسات المختصة	1. نعم	2. لا	4. الفعل لا يستحق الملاحقة القانونية ضد مرتكبه	1. نعم	2. لا	
		5. ضعف الوعي القانوني	1. نعم	2. لا	6. عدم مراعاة السرية	1. نعم	2. لا	
Q8	هل لديك معرفة عن القرار بقانون بشأن الجرائم الإلكترونية؟ (بعد صدوره)	1. نعم	2. لا					
Q9	ما رأيك بالقرار بقانون بشأن الجرائم الإلكترونية؟	1. جيد	2. متحفظ عليه	3. أنا ضد هذا القانون	4. لا رأي			
Q10	بعد صدور القرار بقانون بشأن الجرائم الإلكترونية في حال تعرضك لجريمة الكترونية هل لديك استعداد لتقديم شكوى لدى الجهات المختصة؟	1. نعم	2. لا					
Q11	برأيك ما هي أفضل 4 إجراءات يجب اتخاذها للحد من الجرائم الإلكترونية في فلسطين؟	1. إعداد وتنفيذ استراتيجية وطنية للوقاية والحد من الجرائم الإلكترونية	2. إصدار قوانين عصرية وحديثة وتطبيقها	3. تنفيذ الأحكام القضائية	4. استخدام برامج محمية لحماية أمن المعلومات	5. تعزيز التوعية ونشر الثقافة القانونية حول مخاطر الجرائم الإلكترونية	6. رقابة الأسرة لأفرادها	7. إبلاغ الجهات المختصة عند وقوع الجريمة

An – Najah National University

Faculty of Graduate Studies

Cybercrimes Concept and Their Legislative Challenges in Palestine

By

Nabeel Mahmoud Abu Al-Rub

Supervised

Dr.Anwar Janem

**This Thesis is Submitted in Partial Fulfillment of the Requirements for
The Degree of Master of Public Law, Faculty of Graduate Studies,
An-Najah National University, Nablus – Palestine.**

2018

Cybercrimes Concept and Their Legislative Challenges in Palestine

By

Nabeel Mahmoud Abu Al-Rub

Supervised

Dr. Anwar Janem

Abstract

The study aims to analyze the cybercrimes concept and their legislative challenges in Palestine through defining the nature of cybercrimes, examining the appropriateness of Palestinian legislations and laws and the challenges faced the Palestinian legislator to limit them, identifying mechanisms to prosecute the perpetrators by the police, prosecution and judiciary, and study their reality in Palestine. The study also aimed to contribute to raise awareness and legal culture about the dangers of cybercrimes among Palestinian society.

The study concluded that there are objective and procedural difficulties in defining the concept, detection and proving the cybercrime, and the vacuum of existing penal laws from analysis, investigation, collection, search and seizure of evidence. Cybercrime is an increasingly widespread phenomenon in Palestine in light of the reliance on traditional laws that do not meet the minimum requirements for their control and limitation. In this regard, the Law No. 16 of 2017 on cybercrime came to fill the legal gap without issuing its executive regulations, which still raises a wide debate about its clauses and its relevance to the Palestinian reality of prevention and reduction of cybercrimes and deter the perpetrators. Also, the study

concluded that there is a limited institutionalization for prosecute the perpetrators of cybercrimes, the lack of qualified staff, the lack of standard procedural manuals in the police and prosecution for complaints mechanism and methods of investigation to prosecute and follow-up the perpetrators, the lack of training for criminal justice personnel on the construction of the digital information guide and how to deal with modern technical means of proving cybercrimes, and the Palestinian judiciary modernity in dealing with these crimes, and there is no national strategic plan for the prevention and reduction of cybercrimes, and the weak role of institutions in spreading awareness and legal culture about cybercrimes risks.

